6-16-2016

Performance Optimization of Network Protocols for IEEE 802.11s-based Smart Grid Communications

Nico Saputro
Florida International University, nsapu002@fiu.edu

DOI: 10.25148/etd.FIDC000767

FLORIDA INTERNATIONAL UNIVERSITY

Miami, Florida

PERFORMANCE OPTIMIZATION OF NETWORK PROTOCOLS FOR IEEE 802.11S-BASED SMART GRID COMMUNICATIONS

A dissertation submitted in partial fulfillment of the
requirements for the degree of
DOCTOR OF PHILOSOPHY
in
ELECTRICAL ENGINEERING
by
Nico Saputro

2016

To: Interim Dean Ranu Jung
College of Engineering and Computing

This dissertation, written by Nico Saputro, and entitled Performance Optimization of Network Protocols for IEEE 802.11s-based Smart Grid Communications, having been approved in respect to style and intellectual content, is referred to you for judgment.

We have read this dissertation and recommend that it be approved.

Ismail Guvenc

Nezih Pala

A. Selcuk Uluagac

Leonardo Bobadilla

Kemal Akkaya, Major Professor

Date of Defense: June 16, 2016

The dissertation of Nico Saputro is approved.

Interim Dean Ranu Jung
College of Engineering and Computing

Andrés G. Gil
Vice President for Research and Economic Development
and Dean of the University Graduate School

Florida International University, 2016

DEDICATION

I dedicate my dissertation to my parents, my spouse, and my children. A great reverence for my parents, Tjoek Koentjoro and Honny Megawati. Your determination and perseverance through the hard times in the past year were the biggest push for my tenacity to finish this work. A special feeling of gratitude to my spouse, Ida Imelda, and my children, Kevin and Devin, for being there for me throughout the entire doctorate program. Without your love, patience, and understanding, the completion of this work would not have been possible.

ACKNOWLEDGMENTS

I would like to express my deepest appreciation to my committee members who were very helpful and supportive throughout the dissertation process. A special thanks to Dr. Kemal Akkaya, my advisor, for his thoughtful comments and countless hours of support and encouragement. Without his mentorship, this dissertation could not have been completed.

My graduate school experience in the United States was enabled by so many people and institutions. I would like to express my sincere gratitude to them. In particular, I am very grateful to the American Indonesian Exchange Foundation (AMINEF) and International Institute of Education (IIE), which administer the Fulbright scholarship program in Indonesia and the United States. Without the Fulbright Presidential Scholarship, my tremendous graduate journey would not have been possible. I am also grateful for the generous support from the rector and staff of Parahyangan Catholic University, the dean of the Faculty of Information Technology and Sciences, and the head of the Department of Informatics.

Finally, this research was supported in part by the U.S. National Science Foundation under the Grant #1550313: TWC TTP: Small: Collaborative: Privacy-Preserving Data Collection and Access for IEEE 802.11s-Based Smart Grid Applications.

ABSTRACT OF THE DISSERTATION

PERFORMANCE OPTIMIZATION OF NETWORK PROTOCOLS FOR IEEE 802.11S-BASED SMART GRID COMMUNICATIONS

by

Nico Saputro

Florida International University, 2016

Miami, Florida

Professor Kemal Akkaya, Major Professor

The transformation of the legacy electric grid to Smart Grid (SG) poses numerous challenges in the design and development of an efficient SG communications network. While there has been an increasing interest in identifying the SG communications network and possible SG applications, specific research challenges at the network protocol have not been elaborated yet. This dissertation revisited each layer of a TCP/IP protocol stack which basically was designed for a wired network and optimized their performance in IEEE 802.11s-based Advanced Metering Infrastructure (AMI) communications network against the following challenges: security and privacy, AMI data explosion, periodic simultaneous data reporting scheduling, poor Transport Control Protocol (TCP) performance, Address Resolution Protocol (ARP) broadcast, and network interoperability. To address these challenges, layered and/or cross-layered protocol improvements were proposed for each layer of TCP/IP protocol stack. At the application layer, a tree-based periodic time schedule and a time division multiple access-based scheduling were proposed to reduce high contention when smart meters simultaneously send their reading. Homomorphic encryption performance was investigated to handle AMI data explosion while providing security and privacy. At the transport layer, a tree-based fixed Retransmission Timeout (RTO) setting and a path-error aware RTO that exploits rich information of IEEE 802.11s data-link layer path selection were proposed to address higher delay due to TCP mechanisms. At the network layer, ARP requests create broadcast storm problems in IEEE 802.11s due to the use of MAC addresses for routing. A secure piggybacking-based ARP was proposed to eliminate this issue. The tunneling mechanisms in the LTE network cause a downlink traffic problem to IEEE 802.11s. For the network interoperability, at the network layer of EPC network, a novel UE access list was proposed to address this issue. At the data-link layer, to handle QoS mismatch between IEEE 802.11s and LTE network, Dual Queues approach was proposed for the Enhanced Distributed Channel Access. The effectiveness of all proposed approaches was validated through extensive simulation experiments using a network simulator. The simulation results showed that the proposed approaches outperformed the traditional TCP/IP protocols in terms of end to end delay, packet delivery ratio, throughput, and collection time.

TABLE OF CONTENTS

CHAPTER PAGE

LIST OF TABLES

TABLE PAGE

LIST OF FIGURES

FIGURE PAGE

CHAPTER 1

Introduction

1.1 Motivation

The transformation of the legacy electric grid to Smart Grid (SG) which enables two-way flow of information among different SG components, poses numerous challenges in the design and development of an efficient SG communications infrastructures for connecting different components of the SG. In addition to the currently used underlying networks and protocols, new wired/wireless approaches are being planned for deployment for different components/applications of the SG. The proposed SG communications infrastructures will have many interconnected systems with a variety of ownership and management to provide end-to-end services among stake holders as well as among intelligent devices. This communications infrastructure is referred to as *SG communications network* hereafter.

Over the past few years, there has been a growing interest in identifying the SG communications network [4], in particular for the Advanced Metering Infrastructure (AMI) application. AMI is considered as one of the six key priorities for SG [5]. It is designed to collect, measure, and analyze energy consumption data of consumers through smart meters (SMs) in order to pave the way for dynamic and automatic power pricing. In AMI, home appliances report to a SM, SMs report to a data aggregation point such as a gateway in distribution substation, and then the aggregation point relays these reports to the utility center. Given the span of AMI, the SG AMI communications network will be a multi-tier [4] that consists of a Home Area Network (HAN), a Neighborhood Area Network (NAN), and a Wide Area Network (WAN). HAN is located in the customer domain and provides access to in-home appliances. NAN connects SMs to local access points, and WAN provides communications link between local access points to the utility center. Each tier may use different communications technologies (e.g., wireless, wired) [6], different protocol standards (e.g., open standards, proprietary), and may be owned by different entities (e.g., consumer, utility company, cellular provider). The decision of which communications technology will be adopted depends on various factors such as network characteristics, cost, geographical needs, task objectives, and types of applications and services to consumers [7].

Recently, many utility companies have chosen and implemented wireless mesh technologies for large-scale AMI communications networks [8]. Among wireless mesh options, IEEE 802.11s [9] is one of the viable wireless mesh NAN options for AMI. IEEE 802.11s extends IEEE 802.11 standard by adding self-forming multi-hop mesh networking capability into the Medium Access Control (MAC) layer of IEEE 802.11. Instead of using the Internet layer routing, IEEE 802.11s incorporates routing at the MAC layer (i.e., cross-layer approach [10]) called Hybrid Wireless Mesh Protocol (HWMP). It also supports Quality of Service (QoS) traffic by incorporating IEEE 802.11e standard [11]. However, since IEEE 802.11s is recently approved as an amendment to IEEE 802.11 standard in 2012, the large-scale real-life deployments of IEEE 802.11s-based SG communications network are limited and performance issues with the increase of the network diameter have not been well investigated [12].

Furthermore, TCP/IP protocols [13] are initially designed and optimized for wired network. An extensive research has suggested that TCP/IP protocols do not provide optimal performance for wireless network. Wireless networks have four major characteristics that distinguish them from wired networks [14]: (1) channel contention; (2) signal fading; (3) mobility; and (4) limited power and energy. Although a variety of optimization protocol improvements have been proposed for wireless network, some of which may involve cross-layer optimizations [15, 16, 10], these improved protocols may not adequate when they are implemented for SG communications network due to the specific SG requirements in terms of Reliability, Security, and Privacy. Even though there have been some initiatives to improve the TCP/IP protocol for SG wireless communications network in recent years, but the works are limited to the routing protocols for SG [4] and only few works on other TCP/IP protocol layers [17, 18].

Therefore, it is imperative to identify protocol operations in each TCP/IP protocol stack that can contribute to the performance degradation of IEEE 802.11s-based SG communications network and propose novel or improved approaches. These proposed approaches can be validated and verified through thorough simulations using a network simulator before real-life deployments can be realized. This will test and verify the conceptual integrity of the proposed approaches in a controlled and reproducible manner before the added complexity of the harsh SG environment.

1.2 The Purpose of Study

The aim of this study is to revisit the TCP/IP protocol stack and propose novel or improved TCP/IP protocols that will be used in an IEEE 802.11s-based SG communications network when it is deployed as the Neighborhood Area Network of AMI application.

Although the IEEE 802.11s-based SG communication network is the focal point in the study, since interoperability between networks is also a very important factor in order to meet SG requirements [4], a Long Term Evolution (LTE) cellular network [19, 1] is considered as the WAN for AMI application. Obviously, there may be advantages and disadvantages of this option compared to other options, such as using WiMax or powerline communications. However it is not the scope of this study to compare these options as such works already exist [20].

In particular, the study addresses the following specific SG challenges: (1) security and privacy, (2) AMI data explosion, (3) periodic simultaneous data reporting scheduling, (4) poor Transport Control Protocol (TCP) performance, (5) Address Resolution Protocol (ARP) broadcast, and (6) network interoperability.

1.3 Performance Metrics

The effectiveness of all proposed approaches in the study are validated through extensive simulation experiments using *ns3* discrete network simulator. Throughout the study, four performance metrics are used:

1. *Packet Delivery Ratio (PDR)* which indicates the number of packets received at the data collector divided by the number of packets transmitted by all the SMs. This metric is crucial in understanding the positive impact of the proposed method for packet delivery.

2. The average *End-to-end (ETE) delay* of all packets at the application layer. This metric indicates the average ETE delay of all packets from smart meters to the gateway or utility company.

3. *Throughput* which indicates the number of bits received at the gateway or utility company divided by the total simulation time.

4. The average *Collection Time* which indicates the total collection time from all rounds of sending readings divided by the number of rounds during the simulation time. The collection time of each round is measured as the time of the latest reading that is received at the gateway or utility company for that round minus the earliest time schedule for that round. Let $\overline{CT}$ be the average

collection time, **m** be the number of round, **N** be the number of SMs, $\mathbf{Tx}_{ji}$ be the time schedule of SM_j to send its report at round **i**, $\mathbf{Rx}_{ji}$ be the receiving time of report sent from SM_j at the gateway for round **i** where **i**=1,2,...,**m**, and **j**=1,2,..,**N**. The average *Collection Time* follows Eq. 1.1:

$$\overline{CT} = \frac{\sum_{i=1}^{m} \left(\max_{1 \le j \le N} (Rx_{ji}) - \min_{1 \le j \le N} (Tx_{ji}) \right)}{m} \tag{1.1}$$

Note that PDR, ETE delay, and Collection Time are measured at the application layer since the goal is to measure all delays since the packet is sent by SMs. Throughput however, is measured at the transport layer since the goodput (i.e., the application layer throughput) excludes the protocol overheads.

1.4 SG AMI Communications Network

Fig. 1.1 shows the SG AMI communications network investigated in the study. Each SM, which is installed in every house, is equipped with IEEE 802.11s radio device. A large number of SMs in vicinity are grouped together into a NAN. Each NAN is headed by a gateway node which can further relay the data collected from SMs to utility company through the LTE network. A gateway with dual interfaces, IEEE 802.11s interface and LTE interface, is used in this SG AMI communications network to support bi-directional traffic flow between network tiers. For IEEE 803.11s-based NAN, the gateway acts as the Mesh Portal Point (MPP) and the root node for tree-based routing of Hybrid Wireless Mesh Protocol (HWMP), the default IEEE 802.11s path selection protocol. As the root node, the gateway periodically broadcast proactive path request (PREQ) to create and maintain a logical spanning tree rooted at the gateway. In this way, a path to each SM is always available through the gateway and each SM can reach the gateway in multi-hop fashion through other

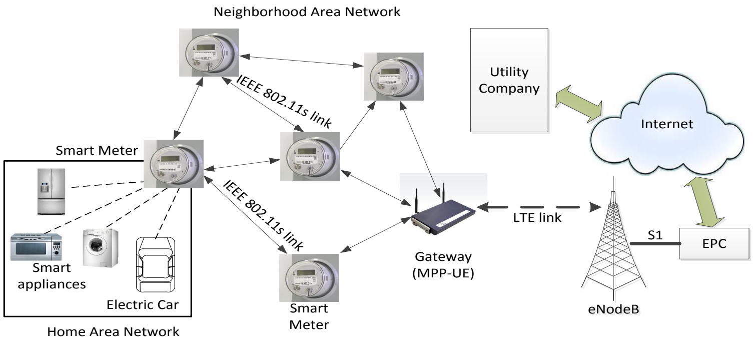


Figure 1.1: SG communications network investigated in the study

SMs. For LTE network, this gateway acts as a User Equipment (UE) and can communicate with utility company through a base station (i.e., eNB) and an Evolved Packet Core (EPC) access network which serves as the LTE gateway to external network (i.e., Internet).

Throughout the dissertation, the SG AMI communications network that consists of IEEE 802.11s and LTE cellular network as the NAN and WAN respectively, is referred to as *hybrid AMI network* while IEEE 802.11s-based SG NAN for AMI application is referred to as *IEEE 802.11s-based AMI network* hereafter.

1.5 Network Protocols Optimization Classifications

In the study, the proposed approaches can be classified into two groups: (1) Layered protocol approaches, and (2) Cross-layer approaches. The first category exploits the traditional layered-protocol architecture. Each layer in the protocol stack hides the complexity of the layer below and provides services to the layer above it. The latter category on the other hand, requires some exchange of information between different protocol layers.

1.5.1 Layered Protocol Approaches

Five layered protocol approaches that address different TCP/IP protocol layer issues are proposed. At the application layer, meter reading data can be collected from SMs in real time at different time-interval for different purposes in addition to billing purpose. In this way, the availability and the amount of power consumption data increase significantly and enable many new applications which were very difficult to accomplish in the past such as dynamic pricing, demand response, demand forecasting, and fraud detection [21]. Moreover, SMs can also be used to collect other data such as power quality, outage notification, restoration after outage notification, etc. To address this data explosion as well as the security and privacy issues that arise due to the availability of rich-information of collected data, two different application layered protocol approaches are proposed and presented in Chapter 4 and Chapter 5. In Chapter 4, three different data aggregation approaches are evaluated to reduce the number of traffic that passing through IEEE 802.11s-based AMI network while taking into account the security and privacy concerns. In Chapter 5, three novel spanning-tree based scheduling and two novel time division multiple access scheduling strategies are presented to address simultaneous data reporting that burden IEEE 802.11s-based AMI network.

Layered protocol approach at the transport layer that based on spanning tree is presented in Chapter 6 to address the poor TCP performance and setting that degrade performance [15]. In Chapter 9 the network interoperability of Hybrid AMI network is investigated. A novel UE access list mechanism is proposed at the network layer of Evolved Packet Core (EPC) access network to handle the downlink traffic to IEEE 802.11s-based AMI network issue due to the tunneling mechanism between packet data gateway (P-GW) at the EPC network to the LTE base-station (i.e., eNB). A layered approach at the data-link layer that proposed dual-queues (DQs) instead of single queue in each access class (AC) of Enhanced Distributed Channel Access (EDCA) in IEEE 802.11e is also presented in Chapter 9.

1.5.2 Cross-Layer Protocol Approaches

Three cross-layer approaches are proposed in this dissertation. In Chapter 7, a path-error aware retransmission timeout (PEARTO), a cross-layer approach between transport and data link layer, is presented. This approach handles the poor TCP performance by taking into account the path error information from the data link layer when RTO timer expires. A secure piggybacking Address Resolution Protocol (ARP), a cross-layer approach between network and data link layer, to address ARP broadcast problem by piggybacking ARP to proactive Path Request (PREQ) of HWMP path selection mechanism is discussed in Chapter 8. Finally, a cross layer approach between the application and network layer is presented in Chapter 9 for privacy-preserving data collection activity in hybrid AMI network when utility company is assumed to be untrusted.

1.6 Contribution

The contributions on this dissertation can be summarized as follows:

1. The performance comparison of three data aggregation techniques to reduce the number of data passing through a SG communications network (i.e., SG data explosion). In the study, three criteria suitable for AMI data aggregation are identified and several homomorphic cryptosystems are evaluated based on those criteria. Paillier partially homomorphic encryption, the selected cryptosystem based on those criteria, is employed for secure hop-by-hop data concatenation and end-to-end data aggregation. Their performance is compared

to a non-secure hop-by-hop data aggregation approach in term of data size and ETE delay. In addition, the computation time of two different multiplication algorithms for homomorphic encryption are investigated for varying operand data size.

2. Three novel data collection mechanisms to set the periodic reporting time of each SM to improve TCP performance in IEEE 802.11s-based AMI network are proposed. The first idea is based on the nature of HWMP, the default IEEE 802.11s path selection protocol. Each SM is assigned a reporting time based on its location in the spanning tree network. The second idea is inspired by the time division multiple access (TDMA) methods where each SM is given a separate slot. The third idea is based on both previous ideas and clustering to increase the number of SMs that can send at the same slot. In addition, a heuristic gateway placement mechanism based on *p*-center facility problem to minimize data delivery delay is proposed.

3. Two TCP retransmission mechanisms are proposed to reduce the packet delay in IEEE 802.11s-based AMI network when simultaneous data reporting is employed. Typically, TCP handles packet losses by retransmitting them again when the corresponding acknowledgments (ACKs) are not received within a certain time interval. This time interval is referred to as *retransmission timeout* (RTO). The RTO value will be doubled each time within this time interval, an ACK is not received. The first proposed mechanism is a spanning-tree based layered protocol approach to set the initial RTO value individually and limit the number of doubling the RTO value when an acknowledgment (ACK) is not received. Instead of having the same initial RTO value for all SMs, each SM is assigned different initial RTO value based on its location in the spanning-tree network (i.e., based on the distance from the gateway) and set

the upper-bound limit of the RTO value in advanced (i.e., the upper bound number of doubling the RTO). The second proposed mechanism is a novel heuristic cross-layer protocol between transport layer and data link layer. In the proposed mechanism, the decision to double the RTO value or not is determined based on the link failure information from HWMP that releases path error (PERR) packets when there is a link failure. These PERR packets will be used to distinguish whether the retransmission timeout is due to congestion or non-congestion event.

4. A novel cross-layer approach between the network layer and the MAC layer called **PARP-S**, a secure piggybacking-based Address Resolution Protocol (ARP), is proposed to eliminate the ARP broadcast storm in IEEE 802.11s-based AMI network. Broadcast ARP requests are piggybacked in the periodic broadcast proactive path request (PREQ) and path reply (PREP) packets that are used by HWMP to build and maintain paths to all SMs in this IEEE 802.11s-based AMI network. In this way, the MAC address resolution is handled during routing tree creation/maintenance and hence the broadcasting of ARP requests from SMs to learn the MAC address of the data collector (i.e., the gateway/root node) is completely eliminated. To protect against ARP cache poisoning attacks, Elliptic Curve Digital Signature Algorithm (ECDSA) is employed.

5. In this study, a hybrid AMI network is proposed by extending the functionality of UE, which basically the end terminal of the LTE network, as the gateway to IEEE 802.11s-based AMI network. A network interoperability issue that causes downlink traffic to any SM in the IEEE 802.11s-based AMI network cannot be delivered due to the GPRS tunneling mechanism of LTE network is identified, and two different approaches are proposed to address this issue. The

first approach is privacy-preserving cross-layer approach between application and internet layer that strives to disassociate IP address of the SM from SG data so that utility company will not be able to find any correlation between these two while overcomes the network interoperability issue. The second approach is an internet layer approach by proposing a novel UE access list to the Packet Data Gateway (P-GW) of the EPC network. This list is used to find the IP address mapping between the network IP address of an IEEE 802.11s-based AMI network and its corresponding UE IP address that acts as the gateway to this AMI network.

6. Another network interoperability issue of hybrid AMI network due to the mismatch of Quality of Service (QoS) capabilities between IEEE 802.11s and LTE network is also identified. IEEE 802.11s employs IEEE 802.11e contention-based Enhanced Distributed Channel Access that has four Access Category (AC) First In First Out (FIFO) queues while LTE network has nine Quality Class Identifiers (QCIs). To address this issue, a modification to the number of queue in each AC of EDCA is proposed. Instead of a single queue in each AC as in the existing IEEE 802.11e standard, dual-queues (DQs), namely a priority and non-priority queue, are proposed for each existing EDCA's AC. In this way, within the same AC, two differentiate services can be provided. The traffic in the priority queue has higher priority over the non-priority queue. In addition, a configurable QoS mapping list is proposed at the gateway of the hybrid AMI network to ensure the appropriate mapping between QCIs and the modified AC in IEEE 802.11s-based AMI network.

1.7 Organization

The motivation and the background information for the network protocol performance optimizations for IEEE 802.11s-based SG Communications Networks are provided in this chapter. The rest of the dissertation is organized as follows: Chapter 2 presents the related work regarding the problem motivated in Chapter 1. Chapter 3 presents the background on hybrid AMI network and TCP/IP protocols. The next two chapters present TCP/IP layered protocol approaches at the application layer. While data aggregation and concatenation for AMI networks are discussed in Chapter 4, the gateway placement and scheduling strategies for periodic data reporting for IEEE 802.11s-based AMI network are investigated in Chapter 5. Chapter 6 discusses another layered protocol approach, a tree-based minimum RTO setting and limit the doubling mechanism of back-off algorithm when the RTO timer expires. The next two chapters present the cross-layered approaches. Chapter 7 discusses a heuristic cross-layer approach for the doubling mechanism of RTO timer while Chapter 8 discusses the cross-layer approach that addresses the ARP broadcast storm issue. In Chapter 9, two network interoperability issues for hybrid AMI network and the proposed approaches to handle these issues are discussed in this chapter. Finally, Chapter 10 provides the conclusion remark about this study.

CHAPTER 2

Related Works

In this chapter, the published works related to the contributions of this dissertation are explained. These published works have been classified based on the relevant TCP/IP protocol stack in which the dissertation is going to address and presented in a top down manner in the following order: application layer section, transport layer section, internet/network layer section, and finally data link layer section. In addition, the published works on hybrid wireless and LTE networks for SG communications network is also presented in this chapter.

2.1 Application Layer Related Work

2.1.1 Data Collection in SG

Typically, the data collection activities in SG are in the form of many to one communications pattern known as *convergecast*. These activities involve a wide variety of intelligent data generating devices, such as sensors and SMs, which are used by SG applications in different SG venues, from the generation to the transmission and distribution networks. There have been many research efforts in the literature that address different aspects of SG data collection activities. Among those efforts, the works on AMI-based multi-hop Wireless Mesh Networks (WMNs) in [22][23] that address the presence of simultaneous traffic due to unpredictable emergency events such as outage, are close to the work in this dissertation. For such unpredictable events, the research community on WMNs typically handles this issue by scheduling the transmission at the MAC layer. This type of scheduling can be viewed as an integrated problem that consists of many sub-problems such as finding the feasible routing, channel assignment for efficient utilization of available channel, and feasible interference-free link scheduling [24]. In both [22] and [23], traffic scheduling that attempts to find a better route in order to reduce overall network delay is pursued. In [22], a single-class back-pressure routing that takes into account the hop-count and queue length in each mesh node is proposed for a multi-gate mesh network. In [23], a random switching approach that takes into account the traffic load of each node (i.e., the total amount of data that needs to be sent by a node) and path load (i.e., the maximum traffic load of all nodes along a path), is proposed to balance the data collection tree. The work in [25] addresses the simultaneous traffic in SG that causes very high network contention since a huge number of SMs are trying to send data at the same time. To handle simultaneous traffic, a different time schedule is created for each SM to reduce the number of competing SM at a time. This can be done by introducing a random delay to the schedule of each SM [25]. The proposed approach in the dissertation is different since the periodic predictable events such as meter reading is handled at the application layer by proposing several mechanisms to assign different time-schedule based on SM location in the data collection tree.

2.1.2 Gateway Placement

The placement of gateway nodes that act as the integration points between multi-hop WMNs and other networks has been investigated extensively. The main goal is to maximize the network throughput while ensuring certain QoS requirements such as bandwidth and delay [26] [27], minimum average hop counts [28], or per node fairness [29]. Typically, the proposed approaches strive to find the minimum number of gateways and their locations by partitioning the network into clusters and selecting a cluster head in each cluster as the gateway [26] [27] [28], or dividing the whole network area into grid of certain size and the cross points on the grid are considered as the candidate locations [29].

In the clustering-based approaches, a spanning tree rooted at the gateway is constructed at each cluster and the depth of the tree must satisfy the radius constraint. Each non-root node in a cluster may serve as a relay node for a limited number of its descendant nodes in the tree (i.e., relay-load constraint). In [26] and [27], the radius constraint represents the delay constraint since delay is considered as the function of the number of hop from the source to the gateway while in [28] the radius constraint is related to the number of mesh routers in the cluster. In addition to those constraints, each cluster can have a total bandwidth constraint [26], cluster size constraint [27], or minimum average hop count [28]. All these approaches however, address the placement of multiple gateways while the IEEE 802.11s-based AMI network used in this dissertation requires only a single gateway. Thus, the similarity of the work in the dissertation is providing the best network performance in terms of ETE delay by assuming the gateway as the root of the spanning tree.

For single gateway placement for WMNs, three heuristics have been proposed in [30]. These heuristics strive to minimize hop count, transmission power, and the sum of the weights of all the shortest paths from all the nodes to the potential gateway respectively. They mainly take into account the physical layer attributes and do not require any knowledge on traffic or on scheduling/routing being used. However, they are based on conflict-free scheduling access protocol such as in WIMAX (IEEE 802.16) and not based on random access (i.e., IEEE 802.11) as in the case of the dissertation. The closest works to this study are conducted for the applications of Wireless Sensor and Actuator Networks (WSANs). For instance, in COLA [31], vertex 1-center approach has been used with the aims of maximizing the coverage area while minimizing the end-to-end delay. In this approach, vertex 1-center selects the first found node as the gateway even when there is more than one candidate. The calculation of the number of hops is based on the assumption that the number of intermediate nodes is always available and therefore, the number of hops is calculated by dividing the Euclidean distance of these nodes with the transmission range. In this study, the selection criterion is different due to the nature of data traffic in AMI networks. Basically, the vertex 1-center selects the gateway location based on the number of directly connected neighboring nodes in the tree topology rooted at the gateway.

2.1.3 Privacy Preserving Data Aggregation for SG

Two types of approaches are proposed for data aggregation for encrypted data: (1) hop-by-hop concatenation [32], and (2) end-to-end encryption via homomorphic approach [33] [21]. The first type of approach just performs concatenation of the encrypted packets when doing aggregation at the aggregator nodes. Two different symmetric key-pairs are used. The first key pair is for end-to-end encryption between the SM and the utility company while the second key pair is for hop-by-hop authentication between a SM and its one-hop parent node. Even though there is some additional overhead due to the implementation of hop-by-hop security, data aggregation via packet concatenation mechanism still gives some bandwidth saving while providing privacy protection when the data is in transit. Nonetheless, there is not real saving on the size of the data sent since the data are concatenated. The only saving is on the header count. In addition, when the channel is lossy the packet drop rate would be higher since larger packets are traveling.

The second approach is based on homomorphic encryption schemes where arithmetic operation (i.e. multiplication) is performed on ciphertext. An aggregation tree that covers all SMs in the neighborhood is constructed in [33]. Every SM in the aggregation tree encrypts its energy consumption data, takes inputs from its children nodes, aggregates them by multiplication operations, and then the aggregated result is forwarded to its parent node. The root of the tree multiplies all the incoming data and then decrypts the result to obtain the final result (i.e., total power consumption). Hence, the privacy of household power consumption is maintained since the aggregation operation is performed on the ciphertext. Another approach in [21] also employs homomorphic encryption and an additive secret sharing mechanism for leakage/fraud detection of power consumption usage in a neighborhood without revealing any information about the individual energy consumption.

2.2 Transport Layer Related Work

TCP in wireless networks has been widely studied. Various approaches have been proposed to improve its performance in wireless networks and address its different aspects. Summaries of these approaches can be found in [14] [34] [35]. From the protocol stack point of view, these approaches may involve the adjustment of individual protocol layer (i.e., layered approaches), or require the interaction between layers (i.e., cross-layer approaches).

2.2.1 Layered Approaches

An adaptive minimum Retransmission Timeout (RTO) [36] is proposed to identify TCP packets whose ACKs will possibly be delayed to avoid spurious RTO timeouts. Actually, delayed ACK is an effort to improve TCP performance by decreasing the number of transmitted ACKs which in turn reduces the channel contention. This delayed ACK can be based on certain criteria, such as until after two consecutive TCP packets are received or a specific time limit is exceeded[37], the number of segments [38], channel condition [39], and the path length [40]. However, this receiver action eventually may cause spurious RTOs at the sender side, and therefore a fixed extended minimum RTO is used at the sender for those identified TCP packets.

In this way, the sender will have a longer waiting time for delayed ACK to arrive. Note that all of these approaches focus on TCP throughput improvement and thus may bring additional delay which is contradicting with the goal of this study of improving the ETE delay.

Recently, a number of layered approaches specific to SG applications have been proposed for different goals (i.e. different than the ETE delay) [17][18]. The work in [17] focuses on the reliability and throughput performance of TCP in a large-scale setting. The main goal is to aggregate the TCP traffic from SMs at certain regional aggregators. The domain of the work in [18] is the monitoring aspect of the SG. Phasor Measurement Units (PMUs) which are sent real-time are considered as the data traffic sources. The work addresses issues regarding reliability along with security.

2.2.2 Cross-layer Approaches

Typically, TCP requires the route failure information from the network layer when a cross-layer approach is pursued. A number of cross-layer approaches that have been proposed were mainly for Mobile Ad Hoc Networks (MANETs) where on-demand routing is employed and mobility is the major cause of route failures. Explicit Link Failure Notification (ELFN) [41], Ad hoc TCP (ATCP) [42], TCP Buffering capability and Sequence Information (TCP-BuS) [43], and TCP Feedback (TCP-F) [44] are some examples of these approaches. Basically, these approaches prevent the TCP to initiate congestion control and require new feedback mechanism to be added so that the intermediate nodes can notify the sender about a route failure. However, these feedback-based approaches may not be better than the standard TCP when they are used in static networks [45]. The IEEE 802.11s SG AMI network, on the other hand, has different network characteristics. It is a static network where every

SM is stationary attached to a household location. It employs path selection at the MAC layer instead of the network layer. Furthermore, to compensate the added complexity from the cross-layer approaches, the margin of improvement should be significant [46]. Thus, these approaches cannot be used in this study.

2.3 Internet Layer Related Work

2.3.1 ARP Broadcasting Overhead in WMNs

In general, broadcast messages (e.g., for MAC address resolution or path discovery) in shared wireless medium such as WMNs may lead to frequent contention and collision among neighboring nodes. With the possible effects of interference and hidden terminal problems, WMNs may lose up to 50% loss of throughput at each hop when a real world environment is considered [47]. This is still the case even with the new IEEE 802.11n MAC standard that has better data rates and transmission range [12]. To alleviate this issue, one proposed solution is to use multiple radios and communicate via different channels [48]. Multi-radio multi-channel WMNs have been the focus of the research community recently [49]. While these types of WMNs can boost the bandwidth, they still need to address joint channel assignment and routing issues in large-scale as well as the inter-flow interference. In addition, they will be more expensive as they require additional hardware.

ARP broadcast problem has been initially considered in small scale WMNs where each node is assumed to talk to every other node randomly [50]. The authors propose to use a gratuitous ARP sent from each node to the root node (if any) so that this root node can act as a central database for all IP and MAC address mappings. In this way, when there is an ARP request from any node in the network, it can respond to these requests. While this study shares the same goal of reducing the ARP broadcasts, the approach in [50] still allows a lot of ARP request and reply messages which cannot be tolerated in a large-scale AMI network. The proposed approach in this dissertation is very different since it exploits IEEE 802.11s to completely eliminate all ARP request by piggybacking this information within PREQ messages in advance.

2.3.2 ARP Attacks

ARP cache poisoning is a well-known attack and a number of ways that involve detection and prevention mechanisms have been proposed in the past to address it. For instance, there are detection mechanisms that work by monitoring ARP packets and alerting administrators through passive detection (e.g., arpwatch [51]), active detection [52] and Intrusion Detection Systems (IDS) (e.g., snort [53]). However, these approaches will not be applicable to the proposed approach in this study due to the size of AMI applications and unavailability of administrators. The prevention mechanisms which rely on additional networks devices such as switches where the prevention is bound to these devices (e.g., Port security [54] and Dynamic ARP Inspection (DAI) [54]) are also not applicable to the proposed approach since it embed ARP within the PREQ and PREP.

A game theoretic approach based on voting mechanisms is proposed to mitigate the ARP cache poisoning problem in [55]. In this approach, each node has a long term table to store all the address mapping information in the neighborhood. When a node cannot find an address mapping in its long-term table, first it will try to resolve it through the normal ARP procedure (i.e., broadcast ARP request and unicast ARP reply mechanism). However, when there is an address mapping conflict that cannot be resolved by the node itself, voting mechanism is used to resolve this conflict. During the voting, each node will vote based on its long term table information. This approach contradicts with the goal of alleviating broadcast messages in WMNs since the voting requests are issued in broadcast and hence would create additional overhead, especially in large-scale.

Due to inapplicability of the above approaches, alternative solutions, which are based on cryptographic approaches, are pursued. One of such approaches is replacing the ARP protocol with a new protocol that involves a secure server [56]. The secure server keeps the IP to MAC address mapping database and shares secret keys with all nodes. In this approach, all nodes periodically and securely report their IP and MAC addresses to the secure server using shared secret keys. All ARP requests and replies for any address resolution occur between a node and the secure server. This approach alleviates broadcast ARP requests but it is not be feasible in an AMI application since the communication between SMs and server may not be possible.

The ultimate solutions to cache poisoning problem are to provide authentication for ARP replies. Secure ARP (S-ARP) [57] and Ticket-based ARP [58] fall into this category. S-ARP provides a defense against ARP cache poisoning using asymmetric cryptography. S-ARP uses DSA to provide authentication scheme for ARP replies and prevents ARP poisoning attacks. An additional ARP header that consists of 12 bytes S-ARP header and a variable length payload is added at the end of the ARP protocol standard to carry the authentication information. A variable length payload is also added at the end of the ARP replies in ticket-based ARP (TARP) approach. This payload contains a ticket as a proof of IP address ownership. This ticket is generated and signed by the Local Ticket Agent (LTA) as authentication proof of the association between IP and MAC addresses. The ticket also has an issue timestamp and expiration time which are used to identify when the ticket was generated and how long it is valid. The issue timestamp is also used for ticket revocation. TARP uses RSA with 1024-bit key. The proposed approach in this study is also based on authentication but does not use DSA or RSA due to their overheads. Elliptic curve version of digital signature (ECDSA) is pursued to not only address the issues regarding scalability and performance but also for easy integration of the proposed approach with IEEE 802.11s. This is because elliptic curve has already been implemented in IEEE 802.11s for password-based authentication called Simultaneous Authentication of Equals (SAE) [9][59].

2.4 Data Link Layer Related Work

2.4.1 IEEE 802.11s Performance Improvement

In the past, there has been some research on IEEE 802.11s in terms of improving its performance. For instance, [60] strived to achieve more reliability by employing multiple-gateways and multipath routing. [61] proposed a new routing metric called link error rate metric and utilized multiple reserved paths to handle route instability. [62] studied delay-tolerant traffic management in IEEE 802.11s-based WMNs. Finally, a recent study focused on the ping pong effect of the Airtime routing metric of HWMP and presented its correlation to the underlying rate control algorithms [63]. None of these approaches concerned with the ARP broadcast problem in WMNs.

2.4.2 IEEE 802.11s Security Protection

IEEE 802.11s does not specify security in routing and hence HWMP is vulnerable to routing attacks such as Path Request (PREQ) flooding, route redirection and routing loop formation [64]. While path request (PREQ) flooding is a Denial-of-Service (DoS) attack, the other two attacks are performed by modifying the mutable fields of HWMP's control packet. These mutable fields (i.e., hop count, TTL and metric) are modified at each hop by the intermediate nodes before forwarding control packet to the next hop. To tackle these attacks, hop-by-hop authentication on the mutable fields using Merkle tree has been proposed [64]. The Merkle tree is a binary tree which concatenates the hash values of mutable elements in a hierarchical manner. Eventually at the root, one hash-value is obtained for all the mutable fields. Non-mutable fields of the routing packet are protected using symmetric encryption. The approach assumes the availability of keys via IEEE 802.11s Mesh Security Architecture and utilizes IEEE 802.1X for initial authentication. Moreover, there have been some claims on the collision resistance of Merkle trees in the past [65].

As another approach, Identity Based Cryptography (IBC) is used to authenticate HWMP control messages, i.e. route request (PREQ) and route reply (PREP) messages by creating digital signature of the mutable fields [65]. In IBC, given an identity of a node, public and private keys are generated using a hash function. Before sending control messages, the digital signature of the mutable fields is calculated using the private key. This signature is included in the control packet. When a node receives a control message, it verifies the digital signature using the transmitter's public key. If it is not correct, the packet is dropped. However, this approach only addresses the attacks from external nodes.

2.4.3 IEEE 802.11e QoS Amendment

After being approved, a variety of studies have been conducted to improve the performance of IEEE 802.11e. However, most of these studies are based on a single-hop Wireless LANs such as the study to fine tuning the parameters (e.g., Contention window minimum/maximum, transmission opportunity limit (TXOP Limit) and arbitration inter-frame spacing number (AIFSN)) [66], the investigation on the effects of the minimum backoff window size and retransmission limit [67], and collision management in Enhanced Distributed Channel Access (EDCA) [68]. In the multi-hop environment, an effort to improve the end-to-end delay for multimedia and real time traffic is conducted in [69]. The authors propose dynamic ReAllocative Priority (ReAP), Adaptive-TXOP (A-TXOP), and TXOP-sharing schemes to achieve this goal. This dissertation differs from these studies in both the network type and the way it handles the performance issues. In this research, IEEE 802.11e standard in IEEE 802.11s-based mesh networks, which can cover a larger area than WLANs and can enable point-to-point multi-hop communication, is investigated. In addition, this study proposes to modify the data structures used in IEEE 802.11e instead of fine-tuning the system parameters.

2.5 Hybrid Wireless and LTE cellular Networks for SG

Several studies have investigated the use of hybrid wireless network and LTE cellular network for SG [70] [25] [71] [72]. A hybrid WiFi mesh/LTE network is proposed in [70], even though the investigation is only on the performance of geographic routing protocol used in the mesh. In other studies, a hybrid IEEE 802.15.4-based Wireless Sensor Network (WSN) and public LTE network is proposed and compared with public LTE network as the sole communications network under simultaneous emergency traffic [25] and two-way demand response application traffic [71]. In these studies, clusterheads in WSN are equipped with dual-interfaces. In [72], control channel and random access channel performance of LTE network are measured and compared from three types of communications networks: LTE network, a hybrid IEEE 802.11/LTE network, and a hybrid IEEE 802.11s/LTE network. The wireless networks in these hybrid networks are used to aggregate local traffic.

CHAPTER 3

Background on Hybrid AMI Network

In this Chapter, the background related to the hybrid AMI network and the TCP/IP protocols, in particular ARP and TCP protocols, are provided. In addition, homomorphic cryptosystem which is very important for privacy-preserving data aggregation is also explained.

3.1 IEEE 802.11s

3.1.1 Overview

IEEE 802.11s is the amendment to IEEE 802.11 standard by bringing multi-hopping capability to wireless LANs. This standard covers various functions, such as mesh discovery, peering, security, and mesh path selection and forwarding. The nodes in IEEE 802.11s WMN are given names based on their roles. All mesh routers are Mesh Points (MP) and are able to provide connectivity at the data link layer between other MPs. If an MP also provides connectivity to another network such as the Internet or a wired LAN, it is termed a Mesh Portal Point (MPP). An MP becomes a Mesh Access Point (MAP) if it connects wireless clients (e.g., Mesh Station (Mesh STA)) to the mesh network. Fig. 3.1 shows IEEE 802.11s naming convention.

3.1.2 Forming A Mesh Network

A Mesh network is formed through discovery and peering mechanisms. The discovery process uses passive and active scanning mechanism to find other mesh nodes. After the discovery, two neighbor mesh nodes need to agree to establish a mesh peering to each other. After successful mesh peering, they become peer mesh stations and can communicate directly one another. A mesh node can establish a mesh

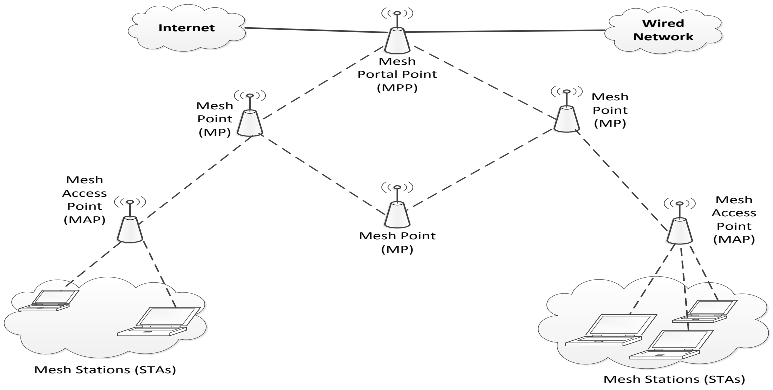
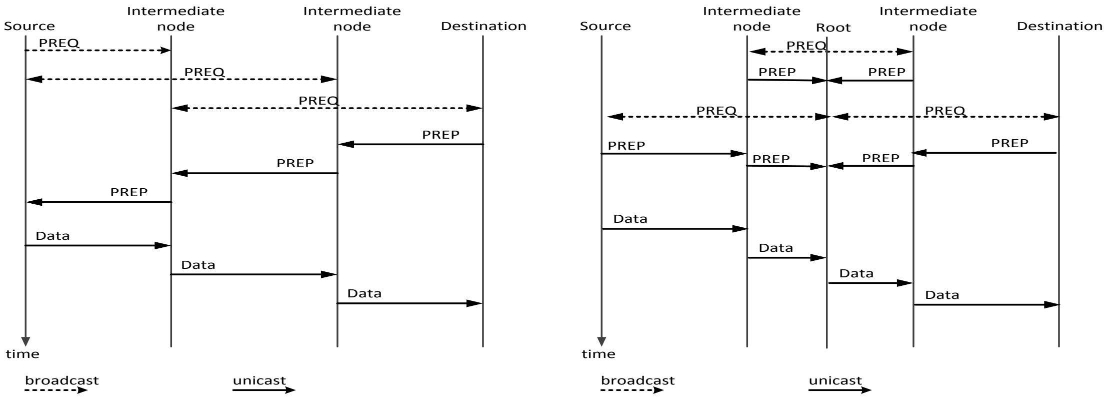


Figure 3.1: IEEE 802.11s architecture components

peering with multiple neighbor mesh nodes. Peering mechanism has two modes: (1) a secure peering mode, called Authenticated Mesh Peering Exchange (AMPE); and (2) a non-secure peering mode, called Mesh Peering Management (MPM). A secure peering requires a Shared Pairwise Master Key (PMK) which can be derived from IEEE 802.1X or from Simultaneous Authentication of Equals (SAE). While 802.1X requires the presence of an Authentication server, SAE does not need it as explained next.

3.1.3 Simultaneous Authentication of Equals

In addition to the previously defined authentication methods, IEEE 802.11s amendments adopted a protocol to simultaneously authenticate two arbitrary peers, called Simultaneous Authentication of Equals (SAE) [9][59]. SAE requires a shared password and a set of domain parameters either from Finite Field Cryptography (FFC) or Elliptic Curve Cryptography (ECC) to achieve authentication and key agreement. As the name implies, the parties that involve in the exchange are equals, each side is able to initiate the protocol, and does not have to be direct neighbors. The initiator (i.e., the node initiating the protocol) is the one that discovers its neighbor(s) first.



(a) Reactive mode

(b) Proactive PREQ mode

Figure 3.2: Reactive and Proactive mode of HWMP protocol

3.1.4 Mesh Path Selection

HWMP is the default path selection mechanism in IEEE 802.11s WMN. It combines two modes of path selection operations: 1) on-demand; and 2) proactive tree building. The first mode is always present while the later depends on the presence of a root node in the WMN. The on-demand mode allows mesh nodes to communicate through peer-to-peer paths while the proactive mode builds a tree that connects all nodes in the mesh to a root node. In this way, a path is always available between all the mesh nodes via the root. Both modes use the metric cost of the link to determine which paths HWMP builds. They also use the same processing rules and three common messaging: 1) *Path Request* (PREQ), 2) *Path Reply* (PREP); and 3) *Path Error* (PERR) message. Fig. 3.2 illustrates the operations of reactive mode and proactive mode of HWMP protocol.

In on-demand mode, a source node broadcasts a PREQ message indicating the MAC address of destination to find a path to a destination. All nodes receiving PREQ message create/update its path to this source node when 1) the PREQ sequence number is greater than the current path to the source; or 2) when the sequence number is the same as the current path but it offers a better metric. *Target Only (TO)* flag in PREQ message determines whether only the destination or any intermediate node that knows a path to destination may reply to PREQ. Only the destination is allowed to reply when TO=1. Otherwise, the first intermediate node that responds to PREQ re-broadcasts PREQ with the updated metrics and sets TO flag to 1 in order to prevent all intermediate nodes sending other replies. Once the destination node (or any allowed intermediate node) receives PREQ message, it sends to the source a unicast PREP. If the destination node receives further PREQ with a better metric (and same or greater sequence number), it sends a new PREP along the updated path. The same rule as in PREQ is used when the source node receives more than one PREP.

Proactive mode has two mechanisms to announce a root node: 1) proactive PREQ; and 2) Root Announcement (RANN) messages. While the first is intended to create paths between all mesh nodes and a root mesh proactively, the later is intended to distribute path information for reaching the root mesh node with no forwarding information creation. When using proactive PREQ message, the root node broadcasts a proactive PREQ message periodically with an increasing sequence number. Each node may receive multiple copies of PREQ each traversing different paths from the root node to the receiving node. The processing rules are the same as in on-demand mode. In case of RANN, there are three messages involved. The root issues pro-active RANN, SM replies with unicast PREQ and the root replies with unicast PREP.

3.2 LTE Network

Long-Term Evolution (LTE) is designed to support unified Internet Protocol packet-switched services for both voice and data. LTE, which refers to E-UTRAN (Evolved Universal Terrestrial Radio Access Network), consists of user equipments (EUs) and base stations called enhanced Node B (eNB). LTE is connected to an IP-based multi-access core network called Evolved Packet Core (EPC). These two systems together are called as Evolved Packet System (EPS). EPC has the responsibility to provide overall control of the user equipment and bearers establishment. EPC uses separate components for control-plane and user-plane. Mobility Management Entity (MME) is a control-plane component that handles mobility and network access for thousands of eNBs. Serving Gateway (S-GW) is a user-plane component that handles data bearers when a UE moves between eNBs, and Packet Data Network Gateway (P-GW) is a user-plane component that handles IP management in LTE network and communication with external data network. These gateways may be implemented in one physical node or separated physical node [19].

A bearer in LTE network is basically a set of network parameters that defines how IP traffic is treated across LTE network. As depicted in Fig. 3.3, to deliver downlink IP traffic to an appropriate UE for example, an IP packet is encapsulated using EPC-specific protocol (i.e., EPS bearer) and tunneled from P-GW to the appropriate eNB using General Packet Radio Service (GPRS) tunneling protocol for user plane (GTP-U). This EPS bearer has to travel across multiple interfaces (e.g., S5/S8, S1, and radio interfaces). Across each interface, EPS bearer is mapped into a lower layer bearer (e.g., S5/S8 bearer, S1 bearer, and radio bearer).

When a UE is first attached to an LTE network, an IP address is assigned by P-GW and a default bearer that provides an always-on best effort service IP

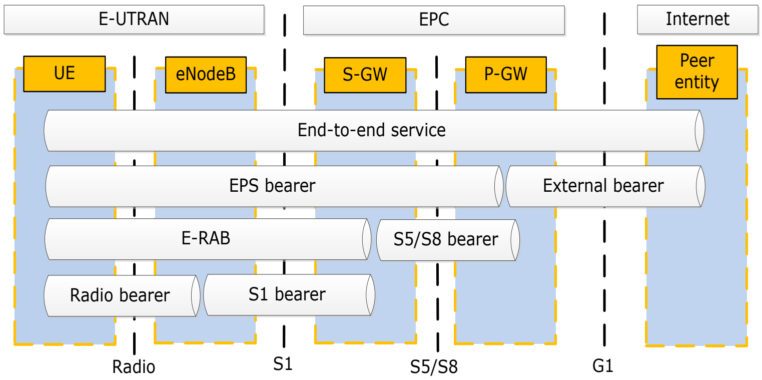


Figure 3.3: EPS bearer service architecture [1]

connectivity is established between UE and P-GW. An additional bearer called dedicated bearer that runs on top of default bearer and provides a specific QoS service can be created anytime for specific traffic. Nine QoS class of identifiers (QCIs) with different set of parameters such as packet delay budget, packet error loss rate, and the resource types (e.g., Guaranteed Bit Rate (GBR) or non-GBR) are available for dedicated bearer.

To assign to a dedicated bearer, packet filtering based on Traffic Flow Templates (TFTs) can be conducted. TFTs use IP header information (e.g., source and destination, port number) to filter packet so that each traffic can be assigned to an appropriate dedicated bearer. Uplink and downlink traffic can have different TFTs. For downlink traffic, packet filtering is performed by P-GW while UE is responsible for uplink traffic.

The interworking of the LTE network (i.e., E-UTRAN) and other 3GPP radio access (e.g., 3G and 2G) and non-3GPP radio access (WLAN, WiMAX) are well studied and handled in the EPC. EPC has different components to handle the mobility issue. For instances, Service Gateway (S-GW) component in the EPC serves as the mobility anchor for interworking with other 3GPP technologies such as GPRS and UMTS, while Packet Data Network Gateway (P-GW) serves as the mobility anchor for interworking with non-3GPP technologies such as CDMA and WiMax networks.

3.3 Address Resolution Protocol (ARP)

3.3.1 Overview of ARP

Each node in an Internet Protocol (IP)-based network is recognized by its IP address. However, whenever an Ethernet frame is sent from one node to another on the same network, the physical address (i.e., MAC address) determines to which interface the frame is destined, not the IP address. ARP provides IP-to-MAC address mapping. Each node maintains an ARP table locally to keep these mappings. Parts of ARP are the ARP Request and Reply messages when the MAC address for a node is not known. Typically, when a node needs to learn the MAC address of a certain destination, it broadcasts an ARP Request message to the network. The node who has the MAC address replies with an ARP Reply message which includes the MAC address. This address is then stored in the ARP table. ARP uses three parameters to control the ARP operations:

1. *ARP AliveTimeOut* defines the minimum time a dynamic ARP entry remains in the ARP table before it is being refreshed (i.e., an ARP request will be issued for the corresponding entry).
2. *ARP MaxRetries* defines the maximum number of times that a node can send the same ARP request before declaring a destination to be unreachable and the corresponding entry of the destination's IP address in the ARP table is marked as **dead**.

3. *ARP WaitReplyTimeOut* defines the number of seconds a node waits for ARP reply in response to an ARP request.

In IEEE 802.11s-based AMI network, as opposed to typical use of ARP at the data link layer, ARP is employed above the HWMP protocol to get the MAC address of the data collector node. Typically, the data collector gateway is set as the root of the WMN. Every SM sends its power consumption data periodically to the gateway at the same pre-defined time intervals. However, since the ARP table of each SM would be empty at the beginning of data collection, all SMs will broadcast an ARP request for learning the gateway MAC address and then find a path to the gateway. Similar ARP requests will be sent periodically when the ARP *AliveTimeOut* of the gateway in the ARP table expires. These requests are forwarded via the intermediate nodes until they reach the gateway node. Once the MAC address is found, it is passed to layer-2 so that it can be used by HWMP.

3.3.2 Attacks on ARP

Since ARP is a widely deployed protocol in every system, it has been subject to various attacks [52]. ARP cache poisoning is one of such attacks at the MAC layer in which an attacker modifies the address mapping in the ARP table by sending a malicious ARP reply message to the victim machine. In this way, the attacker diverts the traffic towards that machine to another machine (possibly itself). It can also perform a man-in-the middle attack by modifying the ARP tables of two victim machines and control their conversations. Finally, it can modify the ARP message in any way. These attacks are also valid in the context of IEEE 802.11s. Any adversary can send malicious ARP replies to one of the SMs in the network and change its ARP table. Since HWMP will be using the information in the ARP table, the created routes will not be valid.

3.4 Transmission Control Protocol

TCP is a window-based transport layer protocol that provides connection oriented, end-to-end reliable data delivery. TCP uses a three-way handshake (i.e. SYN, SYN-ACK, and ACK) for connection establishment and a four-way handshake (i.e. FIN, ACK, FIN, ACK) for connection termination. With the four-way handshake, each side will close independently. A half-open connection may occur when one side has terminated its connection while the other side has not. The terminating side cannot send anymore segment (i.e., TCP-layer data packet) but is still able to receive until the other side terminates as well.

TCP uses sequence numbers for data transmission by numbering each byte of data with a unique sequence number. Then, TCP packs the data into data segment and put the sequence number of the first byte of the data segment and transmits them to a destination. When the destination receives them, it replies to the sender with an ACK. An ACK serves for several purposes. First of all, the ACK informs the sender that the data have been received correctly by putting the sequence number of next expected data byte in the ACK. The receiver also puts information about the amount of data the receiver is willing to accept and the amount of data a sender can transmit to a receiver without receiving any ACK from the receiver. While the former is called an advertised window or a receiver window (rwnd), the latter is called a congestion window (cwnd). The sender will send data based on the minimum between these two windows.

Among several purposes, an ACK can also be used to identify segment loss. When a receiver knows that it received an out of order data segment based on the sequence number of the received data segment, the receiver sends an ACK to identify the missing data segment for retransmission. The sender may receive more than one

ACK that identify the same missing segment for retransmission. This is called a duplicate ACK. The sender determines a segment loss and retransmits the missing segment after it receives three duplicate ACKs.

TCP also uses retransmission timeout (RTO) timer to identify segment loss. Whenever a sender sends a data segment to a destination, an RTO timer is activated. The RTO timer is calculated based on the approach given in RFC 6298 [73]. TCP assumes a segment loss when the RTO expires before receiving the ACK. TCP retransmits the segment and initiates the *slow start* algorithm. This algorithm is the first phase of the TCP congestion algorithm. It increments the *cwnd* exponentially each time a non-duplicate ACK is received until it reaches the slow start threshold. Following the slow start is congestion avoidance algorithm such as TCP Reno, Tahoe, Vegas, and New Reno.

3.5 Homomorphic Cryptosystems

Homomorphic cryptosystems use either symmetric or asymmetric key for encryption and decryption. Even though symmetric key homomorphic cryptosystem is faster, but the asymmetric key are widely used since these cryptosystems are more secure. There are two types of homomorphic crytosystems:

1. **Additive homomorphic encryption**. Suppose that m_1 and m_2 be two values of plaintext, then the result of addition operation on plaintext values can be obtained by decrypting the result of multiplication operation on the corresponding encrypted values.

$$m_1 + m_2 = D_{PK}\left(E_{PUB}\left(m_1\right) \times E_{PUB}\left(m_2\right)\right)$$

2. **Multiplicative homomorphic encryption**. The result of multiplication operation on plaintext values can be obtained by decrypting the result of multiplication operation on the corresponding encrypted values.

$$m_1 \times m_1 = D_{PK}\left(E_{PUB}\left(m_1\right) \times E_{PUB}\left(m_2\right)\right)$$

Many homomorphic cryptosystems and their variants can be found in the literature. A summary of a selection of homomorphic cryptosystems can be found in [74]. A more comprehensive review can be found in [75] and in [76] [77] for elliptic curve versions.

CHAPTER 4

Performance Evaluation of Data Aggregation in AMI Network

In this chapter, three data aggregation methods to reduce traffic in SG communication networks while providing security and privacy to SG data are evaluated. In particular, the impact of homomorphic encryption on data size and latency metrics is investigated. These metrics are chosen since SG is expected to deliver huge amount of SG data. How homomorphic encryption increases or reduces the amount of data to be transmitted and the ETE delay performance of data delivery via aggregation need to be investigated given real-time requirements of SG to prevent power failures or handle demand response.

4.1 Preliminaries

4.1.1 Problem Motivation

While the aim of attacks in the conventional meter reading is energy theft through physical tampering of the analog meter to prevent it from recording the energy consumption accurately, AMI has more targets for attacks. The attacks can be performed not only at SM, but also at the SG communications network and the utility company. In all of these venues, several types of importance data can travel or be stored. For instance, in addition to energy consumption data, SM stores critical data such as password, encryption keys, and firmware that controls SM operations. The energy consumption data also travel through SG communications network, and store at the utility company.

Availability of such data on different venues provides opportunities for several new attacks. In addition to various attacks on integrity, availability and accountability [78], the most serious concerns are on privacy. Privacy in SG is related to

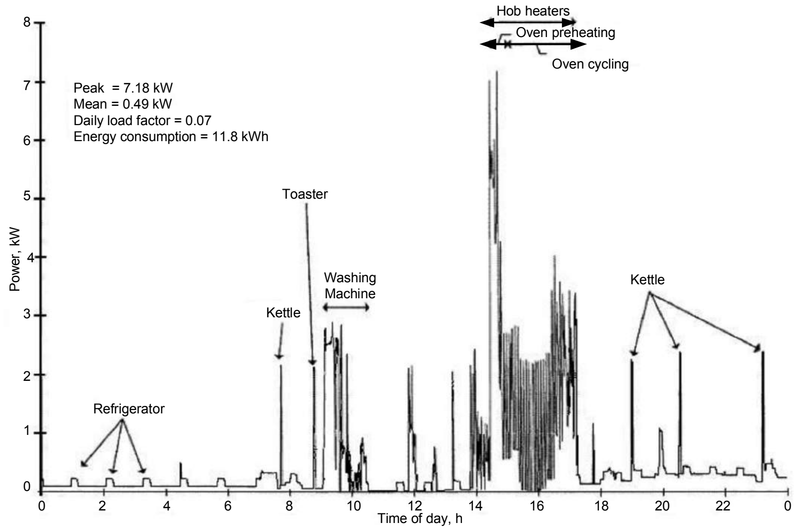


Figure 4.1: Power Usage to Personal Activity Mapping [2]

confidentiality of user identity and consumption data. There are two types of attacks that can pose privacy threats: 1) Attacks on SG communications network to capture the consumption data in transit (i.e., from SM to utility and/or from utility to other parties) and; 2) Attacks on the stored data (i.e., in SM, utility company or other third parties). Once the data are captured, there may be several scenarios that can pose privacy threats. This is because the captured consumption data can easily be disaggregated into individual appliance-level information using Non-Intrusive Load Monitoring (NILM) [79]. Analyzing this data over a period of time can provide a forecast about the household activities as depicted in Fig. 4.1.

Privacy issues also arise from data aggregation. Data aggregation is needed to reduce the traffic and save the total bandwidth used. Instead of sending individual data to destination, aggregating the data and sending aggregated data will reduce the total bandwidth used. In fact, in many cases, this type of aggregated data is needed for statistical purposes. However, data aggregation also requires the performing node to have access to the data in order to do the aggregation operation. This obviously violates the privacy. To overcome this issue, recently homomorphic encryption has been employed [33] [80]. The idea is based on data processing on the encrypted data rather than the plaintext. In this way, an intermediate node will not be able to access the content of the data. Given the important role of homomorphic encryption to provide privacy-preserving for SG data aggregation, there is a need to evaluate its performance under a variety of network conditions to access its suitability to meet SG requirements.

4.1.2 Choices for homomorphic cryptosystem for AMI

The selection of homomorphic cryptosystem for AMI data aggregation needs to consider three criteria: (1) functionality, (2) security, and (3) performance. Given that data aggregation requires a sum function, additive homomorphic cryptosystems are the possible candidates while asymmetric key based encryption is preferred due to SG high security requirement. For the performance, two metrics that need to be considered are:

1. *Message Expansion Factor*: It shows the size of ciphertext compare to the plaintext. For instance, the message expansion factor of 2 means that 10-bytes plaintext become around 20-bytes ciphertext.
2. *Computational Overhead*: Several factors may affect computational overhead. Encryption and decryption computational costs should be minimal to reduce the processing delay. Larger ciphertext requires a more intensive arithmetic computation during the data aggregation operation. Different choices of algorithms for the cryptographic computation may also affect the computational overhead [81].

Among many homomorphic cryptosystems as shown in Table 4.1, Paillier can be considered as the preferred choice for privacy-preserving ETE aggregation due to

Table 4.1: Homomorphic cryptosystems

Cryptosystem	Homomorphic Operation		Type of Key	Message Expansion Factor	Security Remark
	Add.	Mul.			
Paillier [82]	✓		Asymmetric Key	2	semantically secure (IND-CPA)
Okamoto-Uchiyama [83]	✓		Asymmetric Key	3	provable secure equivalent to difficulty of the factorization problem
Naccache-Stern [84]	✓		Asymmetric Key	≥ 4	provable secure under the prime residuosity assumption
RSA [85]		✓	Asymmetric Key	1	not semantically secure
El-Gamal [86]		✓	Asymmetric Key	2	semantically secure (IND-CPA)
Domingo-Ferrer [87]	✓	✓	Symmetric Key	2	vulnerable to known plaintext attack
Castelluccia, Mykletun, Tsudik [88]	✓		Symmetric Key	add a small number of bits	provable secure
Elliptic Curve El Gamal [77]	✓		Asymmetric Key	4	Elliptic Curve Discrete Logarithm Problem (ECDLP)

its small message expansion factor, security, and functionality. Its encryption cost is not too high and has an efficient decryption [75]. Furthermore, Paillier is also non-deterministic since it uses a random number that makes the encryption of the same plaintext can produce different ciphertext.

Another possible choice is the Elliptic Curve El-Gamal (EC-EG). It is additive, has the same security level as El-Gamal cryptosystem, and has the benefit of the small key size. An EC over a 163-bit field gives the same level of security as a 1024-bit RSA modulus or Diffie-Hellman prime [89]. Nonetheless,EC-EG has the message expansion factor of 4 since each message needs to be mapped to an elliptic curve point (x,y) and then encrypt this point into two ciphertexts. Moreover, there are two issues that need to be addressed before implementing EC-EG for AMI applications: (1) EC parameters selections such as the underlying finite field and the coordinate system, and (2) the mapping function from a message to an EC point and vice versa. This mapping function should be deterministic such that the same plaintext always maps to the same EC point and has the following property [90]:

$$\boldsymbol{map}(\mathbf{m}_1 + \mathbf{m}_2 + ... + \mathbf{m}_n) = \boldsymbol{map}(\mathbf{m}_1) + \boldsymbol{map}(\mathbf{m}_2) + ... + \boldsymbol{map}(\mathbf{m}_n)$$

Unfortunately, there are not many existing works on mapping plaintext message to an EC point. The mapping functions are probabilistic algorithms [91] that are based on brute force approaches. When the search space is large, the brute-force approaches consume a lot of resources to find an EC point for each message.

4.2 Network Model

The network model is a mesh network of SMs for AMI applications. For in-network data aggregation, three types of nodes are involved: sink node, aggregator, and leaf node. A sink node initiates query and acts as the end destination of the aggregation results. An aggregator node is an intermediate node that receives and combines meter readings from its child nodes, and then forwards a single intermediate result to its parent node. A leaf node performs data reading and forwards them to its parent node. An SM can be a leaf node or an aggregator node depends on its position on the aggregation tree topology. This aggregation tree is assumed to be static and known in advanced. As an aggregator, an SM can do both data reading and data aggregation. Fig. 4.2 shows the network model, a multilevel network tree topology (i.e., acyclic) that consists of one gateway as the sink node and many SMs.

4.3 Data Collection Protocol

The sink node initiates data aggregation by periodically sending a query to the network. SMs at the lower layer (leaf nodes) send their encrypted power consumption

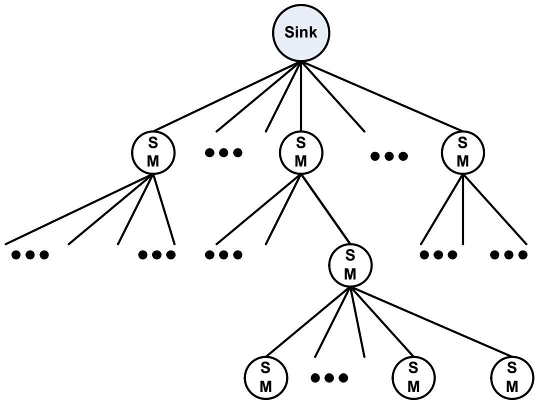


Figure 4.2: Multilevel network tree

data to their parent SM at the upper layer. These intermediate SMs, depending on the type of encryption operations, perform aggregation operation on the ciphertext before sending the result to the parent SM or to the sink. These nodes are referred to as *aggregator* in the rest of this chapter. SM will be used to refer to leaf nodes in the communication tree. The sink node computes the average power consumption by doing a division on the total sum which is in plaintext.

4.3.1 Assumption

The following assumptions are used as part of the data collection protocol:

1. The communication channels are assumed to be perfect and lossless so that there is no packet loss.
2. Key generation and distribution are performed before the sink node initiates a query. Hence, each node already has its appropriate keys based on its role. An aggregator has both public and private key, while a leaf node only has a public key.

3. Data aggregation is performed at an intermediate SM using the sum operator and the result is transmitted as soon as the aggregator SM receives data from all of its children.
4. Each aggregator already has the ID list of its direct child SMs.

4.3.2 Security Considerations

The protocol can also handle the following attacks in addition to providing privacy:

1. ***Eavesdropping:*** Eavesdropping attack may take place in AMI applications when data are in transit on the communication network by overhearing the transmission to obtain privacy information.
2. ***Data Pollution:*** Data pollution may take place in AMI when an external attacker performs false data injection attack or when previous meter readings from some internal nodes reach an aggregator (i.e., data freshness attack). This data freshness attack may tamper the current aggregation result.
3. ***Node Failure:*** A node failure may occur when an SM or an aggregator fails to respond queries or fails to forward its reading or the intermediate aggregation results. In this way, the sink node will receive an incorrect aggregation result.

The three threats mentioned above are addressed as follows: Each SM has a unique ID. Each packet sent from a downstream node has this ID in the packet. The aggregator node verifies this ID using a simple look-up mechanism on its ID list. If the incoming packet comes from an authorized node, the receiving packet will be included in the aggregation operation. This mechanism also avoids data pollution from external attacker (i.e., false data injection attack).

A timestamp is used to overcome data freshness attack. If the timestamp of a packet is less than the timestamp assigned in the node, the operation or the data received will be discarded. A timeout is used to avoid an aggregator waiting indefinitely in case some of its child nodes are unable to report. Initially, the sink node announces its timeout value to its first level aggregator nodes. Subsequently, depending on its position in the aggregation tree, an aggregator will adjust its timeout value according to the timeout value of its parent node as follows:

(maximum sink timeout limit - tree depth × minimum delay between depth levels).

To handle inaccurate aggregation results in case of node failures, the number of readings is sent to the sink node and compares it with the actual SM count. Note that for each SM, either a leaf node or intermediate SM, a two-tuple of information is sent: (1) An encrypted power consumption or an encrypted aggregate power consumption, and (2) An encrypted number of power consumption data. For a leaf node, the number of data is always one while the number of data at an intermediate SM depends on the number of its child nodes. The sink node verifies the received number of power consumption data before it calculates the average power consumption. When the number of data is less than the registered customers, then this means that there is a node failure.

4.3.3 Communications Protocol

As part of the protocol, four operation codes are defined as shown in Table 4.2. OPCODE is the type of operation used to specify the operation that needs to be performed by each SM. ID is the identity of the sender node. TIMESTAMP is used for the data freshness. DATA is a two-tuple of information that represents different information based on OPCODE as defined in the Table 4.2.

Table 4.2: Operation Code definition

OPCODE	Type of operation	DATA
K	Public Key distribution to all nodes, initiated by the Sink node	public key: $\mathbf{N}\|\|\mathbf{g}$
P	Private Key distribution to the aggregator nodes, initiated by the Sink node	private key: $\lambda \|\| \mu$
S	Data Request to all nodes, initiated by the Sink node	parent node timeout (see assumption 5)
R	Data Reporting from all nodes to the sink in response to data request operation, generated by SMs	at the leaf node: $E(\mathbf{m})\|\|E(1)$ at the aggregator node: $\sum_{i=1}^{\mathbf{n}} E(\mathbf{m}_i)\|\|E(\mathbf{n})$, $\mathbf{n}$=number of nodes involved in the aggregation

4.4 Performance Evaluation

4.4.1 Baselines and Performance Metrics

A Java-based application was created for the privacy-preserving data aggregation simulation. The goal is to assess performance of privacy-preserving homomorphic data aggregation while being able to resist or detect the aforementioned attacks. The approach is represented as ETE-H in the graphs and tables. The performance of ETE-H is compared to two other protocols:

1. *HBH Aggregation (HBH-A)*: HBH-A basically decrypts the data, performs aggregation on the plaintext and encrypts the aggregated data before sending it. Therefore, it exposes the data to the intermediate nodes. In order to provide user privacy, pseudonyms are used instead of real IDs. Pseudonyms are associated with the IDs of SMs but this association is known only by the sink node as done in [92]. As a result, even if the data is exposed to intermediate nodes, it cannot be associated with a real ID.
2. *HBH Concatenation (HBH-C)*: One other alternative to homomorphic encryption is to perform concatenation of encrypted packets at the intermediate nodes

and send the concatenated packet to the upper level as used in [32]. This is somewhat similar to ETE homomorphic encryption but there is no operation on the packets. They are just concatenated and a larger packet is created. The final packet is decrypted and the aggregation function is performed at the sink node.

For performance evaluation, the following performance metrics were used:

- *ETE latency*: This is the elapsed time between the sink node sending a query and receiving the final average value. The time spent for source authentication is assumed to be very small than the arithmetic operation and can be ignored in the ETE delay calculation. Moreover, this authentication process has the same effect whether it is in ETE-H, HBH-A, or HBH-C.
- *Encrypted data size*: This metric measures the average message generated from the leaf nodes and from the aggregator nodes in bits. The sizes of messages affect the number of bits/packets required to transmit them.

Four experiments were conducted to observe the effect of the following parameters on ETE latency and data size for ETE-H, HBH-A and HBH-C: (1) Key size; (2) Depth of the tree; (3) The total number of aggregators per level; and (4) The effect of multiplication algorithm on homomorphic encryption.

The following parameters remained constant during the experiments: the network topology has 36 SMs, the minimum communication delay between nodes on different depth levels=50ms and the power consumption data size= 16 bits. The sink generates 2000 queries to collect power consumption data. Except the key-size experiment, 64-bits keys were used for all other experiments.

In experiment 1, a two-level network topology that has 2 aggregators at each level was used. Each aggregator has 8 SMs and 9 SMs at level-one and two respectively. A balanced network tree was used in experiment 2. The experiment started from a flat network with a depth of 1, 2 aggregators, and 17 leaf nodes per aggregator. Then tree depth was increased by one, maintained the number of SMs per aggregator as 2 for each level, and repeated the experiments until tree-depth of 5. For experiment 3, the number of SMs per level was changed while the depth was kept constant. Experiment 4 was performed at the sink node only assuming 36 SMs sensing messages to the sink node at any configuration. Table 4.3 summarizes the network topology configurations and the key size.

Table 4.3: Network Topology Configurations and Key size for the Experiments

Experiment Type	***Network Topology Configuration***				***Key size (bits)***
	tree depth	***#agg. per level***	***#SMs per agg***	$\sum$ ***SMs***	
Exp. 1	2	2	8/9	36	varies
Exp. 2	1 - 5	2	varies	36	64
Exp. 3	1	2-10	varies	36	64

4.4.2 Experiment Results and Discussion

4.4.2.1 Exp. 1: Effect of Key Size:

The effects of using different key sizes in aggregation to latency and data size are shown in Fig. 4.3 and Table 4.4 respectively. Several observations can be made from these results.

Table 4.4: Data size comparison for different key sizes, SM= Smart Meter, AGG = Aggregator

Key size (bits)	***average encrypted message size (in bits)***								
	ETE-H			***HBH-A***			***HBH-C***		
	SM	***AGG***	***%***	***SM***	***AGG***	***%***	***SM***	***AGG***	***%***
64	125.2	1746.0	1295%	125.4	125.4	0%	125.3	1753.8	1300%
128	253.2	3538.2	1297%	253.4	253.4	0%	253.5	3549.5	1300%
256	509.8	7130.9	1299%	509.0	509.0	0%	509.3	7130.5	1300%
512	1021.7	14296.7	1299%	1021.2	1021.2	0%	1021.2	14296.71	1300%
1024	2045.6	28632.3	1300%	2045.3	2045.3	0%	2045.3	28634.3	1300%

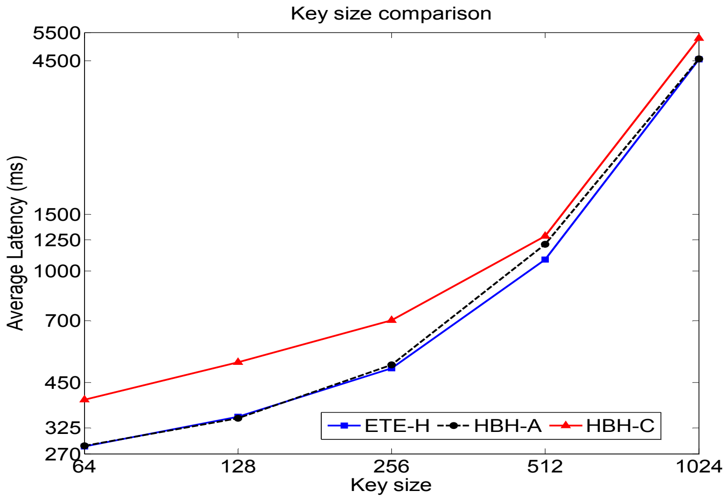


Figure 4.3: The effect of key size on end-to-end latency

While larger key size can provide better protection, it is at the expense of exponential increase in the latency for all three approaches as shown in Fig. 4.3. HBH-C has a higher ETE latency than ETE-H and HBH-A which have a similar latency for a given key size. They provide 16% to 40% reduction in the ETE latency compared to HBH-C.

The increase in the key size, which is by a factor of 2, provides a linear increase in the average size of the encrypted message of the SMs and aggregators by the same factor as seen in Table 4.4. The results indicate that both ETE-H and HBH-C have a similar percentage increase even though they have different operations. This can be attributed to the fact that homomorphic encryption eventually generates a new packet whose size is the total number of bits in both packets. This is also same in concatenation when two packets are combined. There may be only some additional information bits which are not a major increase. There is no increase in the size of data in HBH-A since before the aggregation is performed at the intermediate SMs, the received packets are decrypted first.

Given the fact that HBH-A approach does not increase the message size, it is quite interesting to see that ETE-H is providing similar ETE latency. And similarly, the latency of ETE-H approach is lower although its message size is very close that of HBH-C. These can be explained as follows: HBH-A performs decrypt-aggregation-encrypt at every aggregator including the sink which takes a lot of time and this time should be much more than the time spent by ETE-H approach to perform homomorphic multiplication at each node and decryption at the sink. Otherwise, given that HBH-A has smaller messages to transmit and thus the transmission delay of messages is much less, HBH-A should have provided lower ETE delay. HBH-C also suffers from the overhead of decryption at the sink where it performs decryption of all the data messages (embedded in big packet) before it performs aggregation.

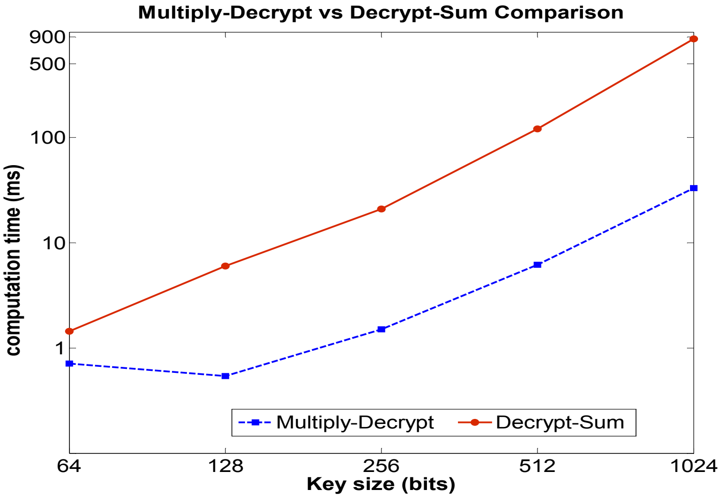


Figure 4.4: Delay Overhead of Multiplication-Decryption vs Decryption-Summation operations at the sink, n=36

To show that this is really the justification of the superior performance of ETE-H, a separate experiment for the sink was conducted. The cost of multiplying n encrypted messages followed by decryption at the sink was investigated and compared it with the result of decrypting n messages and then summing them in HBH-C for various data sizes. Fig. 4.4 indicates that *Multiplication-Decryption* approach is much faster than *Decryption-Sum* approach at the sink. This is mainly due to higher overhead of decryption compared to multiplication. In the former approach,

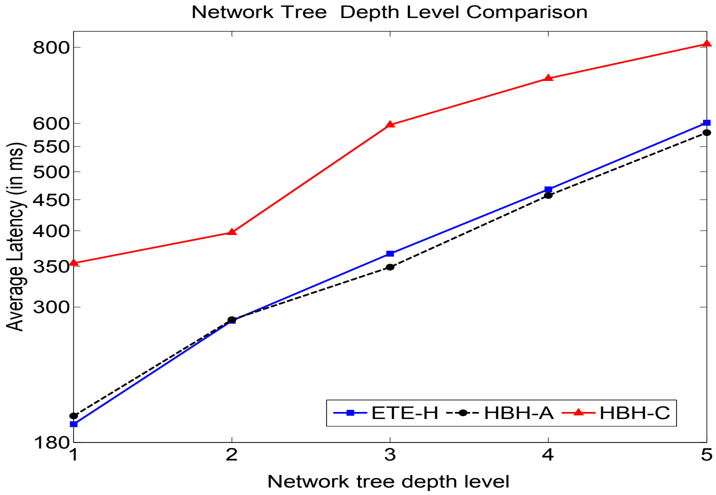


Figure 4.5: Latency comparison for different depth-levels

there are n multiplications and 1 decryption while in the latter, there are n decryptions and 1 summation. This outcome explains why HBH-C is experiencing more delay at the sink and why ETE-H is faster although it performs multiplication at the aggregator nodes.

4.4.2.2 Exp. 2: Effect of the Depth of the Tree

The impact of the depth of the tree on the ETE latency performance is shown in Figure 4.5. ETE latency increases with the increased depth in all approaches. This is because there will be more transmission delay in the data when arrived at the sink. The pattern in ETE latency is similar to that of Fig. 4.3 due to the same reasons. HBH-C performs around 20% worse than the other approaches at all depth levels. Note that the same performance ratio is maintained due to the fact that the total number of SMs is not changing in the network. The total number of SMs affects the overhead at the sink which may significantly change the ETE latency.

However, in terms of message size, while the average data size generated from the aggregator nodes in HBH-A remains constant, both ETE-H and HBH-C show a

Table 4.5: Data size comparison with different network tree depth levels

tree	***average encrypted message size (in bits)***								
depth	***ETE-H***			***HBH-A***			***HBH-C***		
(level)	***SM***	***AGG***	***%***	***SM***	***AGG***	***%***	***SM***	***AGG***	***%***
1	125.2	2244.3	1693%	125.2	125.2	0%	125.4	2257.4	1700%
2	125.2	1746.0	1295%	125.4	125.4	0%	125.3	1753.8	1300%
3	125.5	1500.8	1095%	125.3	125.3	0%	124.7	1495.9	1100%
4	125.6	1501.3	1096%	125.1	125.1	0%	125.0	1500.6	1100%
5	125.4	1498.9	1096%	125.2	125.2	0%	125.1	1501.6	1100%

significant increase in the data size with the increase of the tree depth-level as shown in Table 4.5. Hence, ETE-H and HBH-C consume more bandwidth than HBH-A.

Considering the tree depth and processing times, the findings in this subsection can be summarized as follows: The transmission time from the leaf nodes to an aggregator has small contribution to ETE latency since the data size of the encrypted message from leaf nodes is typically small. The transmission time from an aggregator to its parent node will have a significant contribution if the data size is larger. In addition, there will be significant processing. The processing times at an aggregator, from the highest to the lowest, are in the following order: HBH-A, ETE-H, and HBH-C; while at the sink node it is HBH-C, HBH-A, and ETE-H respectively.

4.4.2.3 Exp. 3: Effect of the # Aggregators per Tree Level

The aim of this experiment is to analyze the effect of spreading the load to more aggregators on performance. Looking at the ETE latency, ETE-H and HBH-A perform better than HBH-C when the # of aggregators is smaller (see Fig. 4.6). As the number of aggregators increases, there will be more operations performed at the sink due to increased number of children reporting. This increases the processing delay for both multiplication and decryption and thus the delay of ETE-H and HBH-A becomes similar to that of HBH-C at increased number of aggregators. For HBH-C, the total number of decryptions will not change but it takes the advantage of

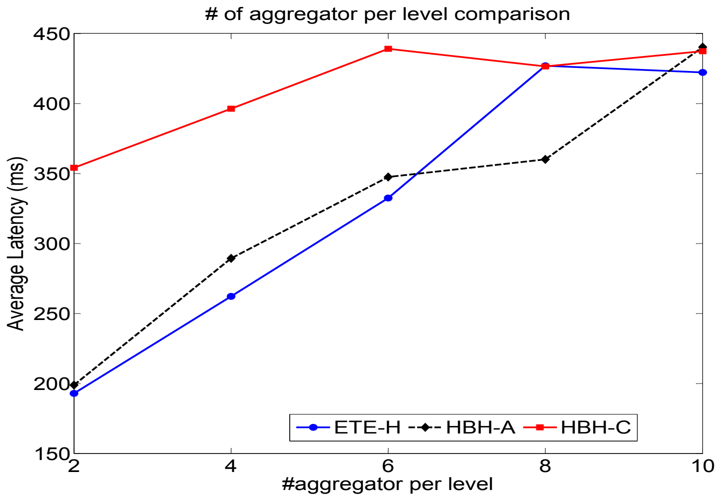


Figure 4.6: Latency comparison for different number of aggregators per tree level

more parallelism among the increased number of aggregators performing aggregation which helps to maintain a flat latency. Regarding data size, the results indicate that with the increased number of aggregators per tree level, the average message size generated by aggregators is decreased as shown in Table 4.6.

Table 4.6: Data size comparison for different number of aggregators per level

#agg per level	***average encrypted message size (in bits)***								
	ETE-H			***HBH-A***			***HBH-C***		
	SM	***AGG***	***%***	***SM***	***AGG***	***%***	***SM***	***AGG***	***%***
2	125.2	2244.3	1693%	125.2	125.2	0%	124.8	2246.2	1700%
4	125.4	1124.8	797%	125.3	125.4	0%	125.2	1126.8	800%
6	125.1	748.4	498%	125.3	125.3	0%	125.2	751.4	500%
8	125.3	561.9	349%	124.8	124.8	0%	125.5	564.9	350%
10	125.4	450.3	259%	125.0	125.0	0%	125.7	452.4	260%

4.4.2.4 Exp. 4: Using a Different Multiplication Algorithm in ETE-H

In the above experiments, the default Java multiplication operation is used for ETE-H. Since different computation algorithms may produce different results, the aim of this experiment is to investigate the performance of Karatsuba multiplication algorithm [93], shown in Alg. 1, compared to the Java's default multiplication. In the implementation of Karatsuba's algorithm, a cutoff value is used to limit the

Algorithm 1 kmultiply(**X,Y,cutoff**)

```
1. if $\mathbf{X} \leq$ cutoff and $\mathbf{Y} \leq$ cutoff then return $\mathbf{XY}$
2. else split $\mathbf{X}$, $\mathbf{Y}$ in half
   $\mathbf{X} = 2^{n/2}X_1 + X_2$
   $\mathbf{Y} = 2^{n/2}Y_1 + Y_2$
3. $X_1Y_1$ = kmultiply($X_1$,$Y_1$,cutoff)
4. $X_2Y_2$ = kmultiply($X_2$,$Y_2$,cutoff)
5. $\mathbf{W}$ = kmultiply($X_1 + X_2$,$Y_1 + Y_2$,cutoff)
6. return $2^{\mathbf{n}}X_1Y_1 + 2^{\mathbf{n/2}}(\mathbf{W}\text{-}X_1Y_1\text{-}X_1Y_2) + X_2Y_2$
```

number of recursive operations. **K-n** is defined as the cutoff value that is equal to the maximum bit length of the operands divided by $2^{\mathbf{n}}$. Hence, the cutoff value of Karatsuba-1 (K-1) to K-3 are the half size, the one-fourth size, and the one-eighth size of the maximum bit length of the operands.

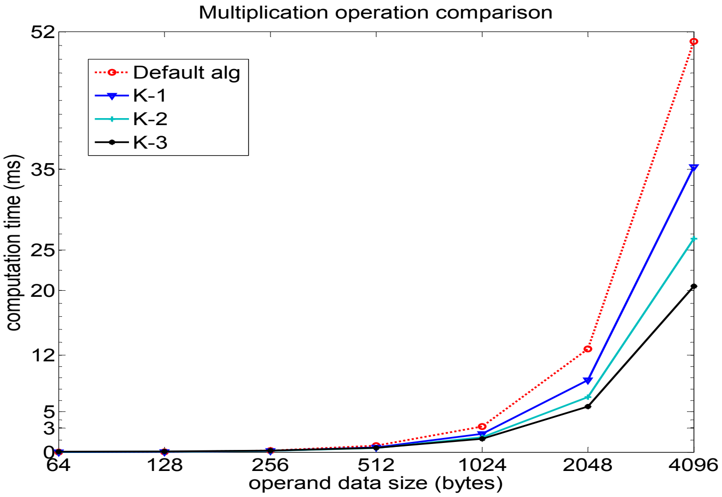


Figure 4.7: Computational time comparison of Karatsuba algorithm and Java's default multiplication for ETE-H

Fig. 4.7 shows that when the data (operand) size is bigger (e.g., ≥ 1024 bytes), Karatsuba performs better than Java's default multiplication algorithm. Therefore, the algorithm can be employed at the sink or at the nodes that are near the sink.

This is because, the sink and aggregators near the sink will receive bigger data compared to the leaf SMs or the aggregators near the leaf SMs. This will speed up the multiplication process at the upper level SMs.

4.5 Summary

In this chapter, the performance of widely recommended privacy preserving data aggregation approaches was evaluated using the message size and ETE latency metrics. Three data aggregation approaches (end-to-end homomorphic data aggregation (ETE-H), hop-by-hop homomorphic data aggregation (HBH-A), and hop-by-hop concatenation data aggregation (HBH-C)) were compared. Overall, the results indicated that ETE-H provides comparable ETE latency when compared to HBH-A that does not provide privacy by itself. In addition, its performance is superior to HBH-C in terms of ETE latency due to fastness of homomorphic multiplication compared to decryption at the sink. However, both ETE-H and HBH-C increase the message size to be transmitted significantly and thus their bandwidth requirements will be higher. As a result, ETE-H can be a preferred solution if the underlying network traffic will not be significant. Otherwise, HBH-A can be picked provided that it is complemented by a separate privacy mechanism.

CHAPTER 5

Investigation of Gateway Placement and Smart Meter Data Reporting Strategies for IEEE 802.11s-based AMI Network

In this chapter, designing efficient and reliable IEEE 802.11s-based AMI network is investigated, in particular the placement of the gateway that collects data from SMs and periodic data reporting strategy. Given that fine-grained regular data collection from large-scale SMs in the IEEE 802.11s-based AMI network may create a lot of traffic and interference, it is critical to pick the suitable data collection strategy to meet some SG requirements. The location of the gateway is also important since it may also add to this interference by impacting the length of routes.

5.1 Problem Motivation and Description

An IEEE 802.11s-based AMI network is expected to serve a number of applications in addition to meter reading data collection such as outage detection, demand response, electric vehicle charging coordination, security certificate distributions, etc. This means there will be an increased traffic on IEEE 802.11s-based AMI networks as the new applications of the SG come to life. Note that periodic operations of IEEE 802.11s such as establishing and maintaining peering between SMs, building the network topology, and maintaining the proactive paths to all SMs through the gateway already create significant amount of traffic. The situation is compounded with the upper protocol layer operations. For instance, as can be read in Chapter 8, the operation of Address Resolution Protocol increases the contention and eventually causes the network performance degradation. Considering all of these at the same time, IEEE 802.11s-based AMI network may experience a lot of congestion and interference which may increase the data delay as well as the packet loss. Such performance metrics can be critical in meeting certain quality of service (QoS) requirements such as demand response or distribution side state estimation. Therefore, there is a need to alleviate the traffic congestion.

A lot of different aspects can be studied to achieve this goal from the networking perspective. Since these studies have already been employed in the context of other applications, this chapter focuses on SG features that can give us leverage to reduce data delay. Such leverage is in the form of data transmission scheduling and gateway location. For instance, the way we collect data from SMs can be adjusted. The SMs can be organized to transmit their power readings at predetermined times to reduce contention in the network. Similarly, previous research showed that the gateway locations in Wireless Mesh Networks (WMNs) can have a significant impact on the network throughput [30], however finding the solution for the gateway locations is NP-hard [28]. Thus, there is a need to evaluate the performance of this network on a variety of different gateway locations before the real deployment is done.

The problem can be defined as follows: ”Given a certain number of SMs, their locations in a NAN, and the periodic data collection frequency, the first goal is to find the location of a single Mesh Portal Point (MPP) (i.e., gateway) for the IEEE 802.11s-based AMI network, that minimizes the end-to-end delay. Then, based on the chosen gateway location and the data collection frequency, the second goal is to come up with a mechanism to reduce the contention and thus the end-to-end delay when TCP is employed.”

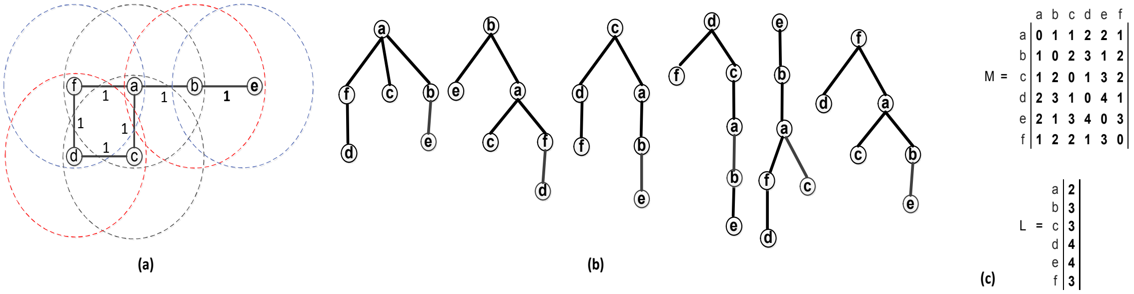
To this end, the gateway placement based on HWMP operations and setting the periodic reporting time individually for each SM rather than setting the same periodic reporting time for all are proposed in this chapter.

5.2 Gateway Placement for IEEE 802.11s-based AMI network

The proposed solution is adapted from the Network facility location problems (NFLPs) domain that studies placing one or more facilities in certain locations in a network that consists of nodes and links. The network demand points can be nodes or nodes and links simultaneously. NFLPs can be classified into five main categories [94]: median, center, covering, hub location, and hierarchical location problems. The objective is to find the facility locations that optimize a specific metric from demand points to the nearest facility (i.e., cost minimization or profit maximization).

The network demand points in this case are SMs. The periodic data traffic generated from every SM is of equal importance, and the network coverage is not an issue due to the multi-hopping capability of IEEE 802.11s. The objective is to find the location for a single gateway that acts as the MPP and the root node for the proactive tree-based routing of IEEE 802.11s. Since there will be infinite number of possible locations to place a single gateway in a NAN, the goal is to place the gateway in one of the household's locations to narrow the solution domain. For this reason, the gateway placement problem is considered as a 1-vertex center problem [31]. The goal in this type of problem is to minimize the maximum distance from all SMs to the gateway (i.e., minimax). However, since multi-hop routes are used, the distance needs to be expressed in terms of hop count. Therefore, a two-stage heuristic 1-vertex center approach based on minimum spanning tree (MST) which can be formed by exploiting the default proactive tree-based path selection in IEEE 802.11s is proposed.

In the proposed heuristic approach, the IEEE 802.11s-based SG AMI network is represented as undirected graph $G(V,E)$ which is called connectivity graph. Each node $v \in V$ represents an SM with a transmission range r. The direct neighborhood



$$M = \begin{array}{c|cccccc|} & a & b & c & d & e & f \\ a & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{2} & \mathbf{1} \\ b & \mathbf{1} & \mathbf{0} & \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{2} \\ c & \mathbf{1} & \mathbf{2} & \mathbf{0} & \mathbf{1} & \mathbf{3} & \mathbf{2} \\ d & \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{0} & \mathbf{4} & \mathbf{1} \\ e & \mathbf{2} & \mathbf{1} & \mathbf{3} & \mathbf{4} & \mathbf{0} & \mathbf{3} \\ f & \mathbf{1} & \mathbf{2} & \mathbf{2} & \mathbf{1} & \mathbf{3} & \mathbf{0} \end{array}$$

$$L = \begin{array}{c|c|} a & \mathbf{2} \\ b & \mathbf{3} \\ c & \mathbf{3} \\ d & \mathbf{4} \\ e & \mathbf{4} \\ f & \mathbf{3} \end{array}$$

Figure 5.1: two-stage heuristic 1-vertex center based MST approach example. a) connectivity graph of SMs, the weight of all links are assumed equal to 1. b) for every node v, an MST is built. c) Minimum distance matrix M and maximum hop list L. Each row v in M represents hop count of every other nodes to a node v. The minimum value in L is in the first row of L. This row corresponds to node a. Thus, node a is selected as the gateway. $\mathbf{N}(a)$=(f,c,b),$\overline{H}(a)$=(1+1+1+2+2)/5=1.4

of v, denoted by $\mathbf{N}(v)$, is the set of SMs that reside within the transmission range of v. A wireless link that exists between v and every neighbor $u \in \mathbf{N}(v)$ is denoted by an edge $e(u,v) \in E$.

In the first step, the heuristic approach is similar to the ordinary 1-vertex center approach by creating the minimum distance matrix M that contains the minimum number of hops for every node v to all other nodes. However, to determine the number of hops for each node v to all other nodes, an MST rooted at a node v, denoted by $\mathbf{T}(v)$, is established using the Prim's MST algorithm [95]. In addition, two MST statistics are collected, the size of $\mathbf{N}(v)$ (i.e., the number of 1-hop node), and the average hop count $\overline{H}(v)$. To find the minimax value in M, a maximum hop list L is used to store the maximum number of hop from each row in M. The chosen gateway location corresponds to the entry in L that has the lowest value. In case there is a tie (i.e., more than one entry in L that have the lowest value), the heuristic mechanism chooses the location that has the minimum size of $\mathbf{N}(v)$. When there is another tie, the second level heuristic criterion is based on the minimum average hop count.

The pseudo code of gateway placement is shown in Alg. 2. An example of 1-vertex approach is given in Fig. 5.1.

Algorithm 2 Two-stage heuristic 1-vertex center

```
for every candidate gateway location $v \in V$ do
    $\mathbf{T}(v)\leftarrow$ a minimum spanning tree rooted at $v$
    $\mathbf{N}(v)\leftarrow$ directly connected neighbor of $v$
    $\overline{H}(v)\leftarrow$ the average hop count in $\mathbf{T}(v)$
    for every node $w \in V$ do
        $\mathbf{M}(v,w)\leftarrow$ the hop count from $v$ to $w$ in $\mathbf{T}(v)$
    end for
    $\mathbf{L}(v)\leftarrow$ the maximum hop count in $\mathbf{M}(v)$
end for
MinCostNodes $\leftarrow$ nodes with the minimum hop count in $\mathbf{L}$
if $|MinCostNodes| > 1$ then
    for every node $k$ in MinCostNodes do
        $minNeighbors \leftarrow$ nodes with the lowest $|\mathbf{N}(\mathrm{k})|$
    end for
    if $|minNeighbors| > 1$ then
        for every node $k$ in minNeighbors do
            $minAvgHop \leftarrow$ nodes with the lowest $|\overline{H}(\mathrm{k})|$
        end for
        Gateway location $\leftarrow$ first node in $minAvgHop$
    else
        Gateway location $\leftarrow$ $minNeighbors$
    end if
else
    Gateway location $\leftarrow$ $MinCostNodes$
end if
```

5.3 Data Report Scheduling for IEEE 802.11s-based AMI network

In this section, three approaches for data collection scheduling in IEEE 802.11s-based AMI network are discussed. Note that these approaches are proposed at the application layer. The first approach exploits a spanning tree based solution, the second is motivated from the TDMA-type medium access, and the third combines the first two approaches and clustering method.

5.3.1 Spanning-tree Based Scheduling

Due to the location of SMs in the network, some SMs will be close to the gateway and thus will have shorter packet delay compared to others. Therefore, a data collection approach based on the locations of SMs in the network topology was proposed. To identify the unique location of each SM, a minimum spanning tree (MST) for the network was built. An MST traverses every node in the network starting from the root node. The goal is to assign different time slots for each SM based on its position in the ST. For this purpose, three options related to the position of node in the ST are explored.

5.3.1.1 MST-based Nearest Node First Scheduling (MST-NNFS)

In this approach, a node that is closest to the root of the ST (i.e., the gateway) is scheduled first while the leaf nodes are scheduled last. A leaf node is the one that does not act as a relay for any of the other SMs. The time schedule allocation for each SM is based on Equation 5.1.

$$TS(i) = sTime + (depth(i) - 1) \times \delta \tag{5.1}$$

where, $TS(i)$ represents the time slot for SM_i, $sTime$ represents the initial time that is the same for all SMs, $depth(i)$ represents the network depth of SM_i, δ is a constant value, and i = 1,2, ..., n. n is the number of SMs.

5.3.1.2 MST-based Farthest Node First Scheduling (MST-FNFS)

In this approach, the leaf nodes are scheduled first for transmission while the nearest nodes to the root are scheduled last as in Equation 5.2.

$$TS(i) = sTime + (maxDepth - depth(i)) \times \delta \tag{5.2}$$

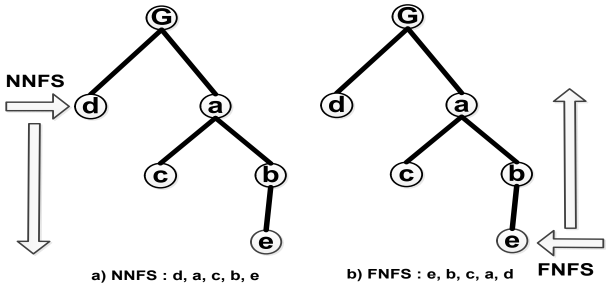


Figure 5.2: An example of spanning tree scheduling based on node position in the tree.

where $maxDepth$ represents the maximum depth level of the ST. Fig. 5.2 illustrates the different between NNFS and FNFS.

5.3.1.3 MST-based Randomly Assigned Scheduling (MST-RAS)

In MST-FNFS and MST-NNFS, SMs at the same network depth level will have the same time slot assignments which may create contentions. Therefore, a random time slot is assigned for each SM in MST-RAS. However, there will be a large number of possibilities for time slot assignment for each SM. Therefore, the proposed approach still uses the spanning tree by considering the SM's position in the ST in the assignment. As a matter of fact, either MST-NNFS or MST-FNFS approaches can be chosen as the starting point and then add a random value to each SM's schedule. Eq. 5.3 shows an example of MST-RAS scheduling that uses MST-NNFS as the starting point.

$$TS(i) = sTime + (depth(i) - 1) \times \delta + \delta_i \tag{5.3}$$

where δ_i is a random value in a certain range.

5.3.2 TDMA Scheduling

The ST-based scheduling may help reduce the contention but depending on the size of the network and traffic patterns, there will still be contention at different locations of the network. To completely eliminate these contentions, a TDMA-based approach which allows only one SM to transmit at a time slot T is proposed. Within this time slot, only one SM is allowed to access the channel that reports to the same gateway node. Eq. 5.4 represents the time schedule allocation for SM_i. For N SMs, there will be N time slots for each data collection cycle.

$$TS(i) = sTime + T \times (i - 1) \tag{5.4}$$

5.3.3 k-degree TDMA Scheduling

Setting a TDMA scheduling to each SM raises an important issue related to the channel utilization since only one SM is allowed to send at a time slot T. To increase the channel utilization, the number of SMs that allow to send simultaneously at a time slot T can be increased. In this case, for each data collection cycle, the total number of time slots of N SMs when k SMs are allowed to send simultaneously at a time slot T, $k \leq N$, is shown in Eq. 5.5.

$$totalTS = (N \text{ div } k) + (N \bmod k) \tag{5.5}$$

For the first time slot, there will be $\mathbf{C}(N,\, k)$ possible combinations of k SMs. Since these k SMs are only allowed to send one time in each data collection cycle, the possible combinations of k SMs for the second time slot is $\mathbf{C}(N-k,\, k)$. Subsequently, there will be $\mathbf{C}(N-2k,\, k)$ possible combinations of k SMs for the third time slot, and so forth. Eq. 5.6 shows the total possible combinations of k SMs assignments.

$$\prod_{i=1}^{N \text{ div } k} \mathbf{C}(N-(i-1)k, k) \tag{5.6}$$

However, not all of these combinations are feasible for the k-degree TDMA scheduling since the goal is to minimize the contention among SMs. The k SMs for every time slot t_j should be selected in such a way so that the contention between these k SMs is minimized.

Assigning k unique SMs to a time slot t_j, $1 \leq j \leq totalTS$, can be considered as a variation on classical vertex coloring problems (VCPs) that are known to be NP-hard combinatorial optimization problem [96]. VCP has been widely studied for years and applied for a variety of real world problems such as timetabling, scheduling, and frequency assignment problems. In VCP, the aim is to assign a color to every vertex in such a way so that no two adjacent vertices have the same color and the minimum number of colors is used. For the k-degree TDMA scheduling case, a vertex represents an SM_i, a color represents a time slot t_j, and an edge represents a wireless link between two SMs. The goal is to assign a time slot t_j to an SM_i so that two adjacent SMs (i.e., two SMs that are connected with an edge) do not have the same time slot t_j. However, unlike VCP that strives to minimize the number of colors for a given graph, in the k-degree TDMA scheduling case the number of time slots has been determined to be as in Eq. 5.5 and each time slot t_j will be assigned to k SMs. The only exception is when $(N \bmod k) > 0$. In this case, the last time slot in each data collection cycle will be assigned to $(N \bmod k)$ SMs.

While there have been many proposed algorithms for solving VCPs, heuristic approaches are more popular than exact approaches since the latter approaches were only able to solve consistently for a small number of vertices (e.g., up to 80 vertices) [96]. Given that an IEEE 802.11s-based AMI network is expected to support a much bigger number of SMs, a heuristic k-degree TDMA-based scheduling approach to increase the degree of parallel transmission in each time slot is proposed. The proposed heuristic approach is based on the nature of traffic flow in an IEEE 802.11s-based AMI network. The proactive tree-based path selection of IEEE 802.11s causes the traffic from all SMs to flow multihop toward the gateway by following a path

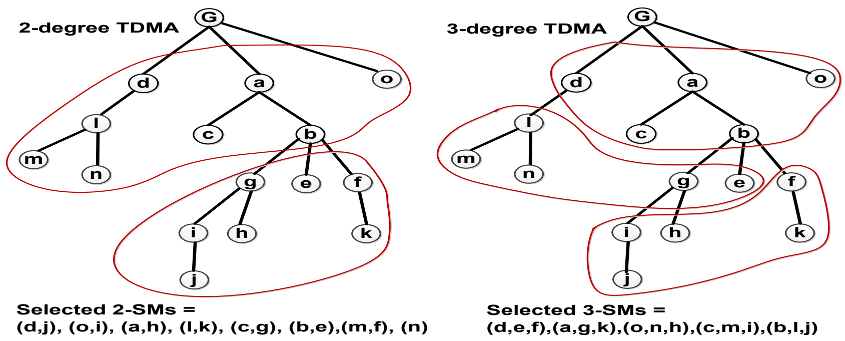

2-degree TDMA
G
d
a
o
l
c
b
m
n
g
e
f
i
h
k
j
Selected 2-SMs =
(d,j), (o,i), (a,h), (l,k), (c,g), (b,e),(m,f), (n)
3-degree TDMA
G
d
a
o
l
c
b
m
n
g
e
f
i
h
k
j
Selected 3-SMs =
(d,e,f),(a,g,k),(o,n,h),(c,m,i),(b,l,j)

Figure 5.3: Examples of k-degree TDMA

upwards in a tree structure. Therefore, the proposed approach used an MST of the network topology rooted at the gateway g and assigns a time slot t_j to k SMs based on their locations in the ST. In the context of VCPs, instead of assigning colors to graph $G(V,E)$, the proposed approach strives to assign colors to vertices of a spanning tree subgraph $T(V,E_T)$ of G. This vertex coloring of a spanning tree is known as backbone coloring [97].

To assign a time slot t_j to k SMs, the MST is divided into k clusters, each cluster has an equal number of SMs. The SMs in each cluster are sorted based on their tree depth in such a way so that SMs in the odd cluster(s) are sorted based on the ascending order of their tree depths while SMs in the even cluster(s) are sorted based on the descending order of their tree depths. An SM from each sorted cluster is selected to form a group of k-SMs for each time slot t_j. Fig. 5.3 shows examples of 2-degree and 3-degree TDMA scheduling. The pseudo code of the k-degree TDMA is depicted in Alg. 3. An array list, denoted by $SList$, is used to store the list of 2-tuple (SMID,depth) in ascending order of the tree depth. Hence the length of the array list will be equal to N, the number of SMs. Each $cluster(j)$ has the length of $totalTS$ and the index in each $cluster(j)$ represents the time slot t_j.

The only exception can be in the last cluster. When (N mod $TotalTS$) > 0, the length of the last cluster will be (N mod $TotalTS$).

Algorithm 3 k-degree TDMA

```
$totalTS \leftarrow (N\ div\ k) + (N \bmod k)$;
$\mathbf{T}(g) \leftarrow$ the MST rooted at the gateway $g$;
$maxDepth \leftarrow$ the maximum tree depth of $\mathbf{T}(g)$;
for $1 \leq t \leq maxDepth$ do
    $SList \leftarrow$ append 2-tuple(s) (SMID,t) where the SMs in $\mathbf{T}(g)$
                are $t$ edge(s) from $g$;
end for
for $1 \leq j \leq k$ do
    if $|SList| \geq totalTS$ then
        $n = totalTS$;
    else
        $n = |SList|$;
    end if
    $cluster(j) \leftarrow$ the first $n$ 2-tuples (SMID,depth) from
                $SList$;
    $SList \leftarrow (SList - cluster(j))$;
    if ($j \bmod 2 = 0$) then
        sort $cluster(j)$ in descending order of tree depth;
    end if
end for
for $1 \leq x \leq TotalTS$ do
    for $1 \leq j \leq k$ do
        if (x $\leq |cluster$(j)$|$ ) then
            $timeslot(x,j) \leftarrow cluster(j,x)$.SMID;
        end if
    end for
end for
```

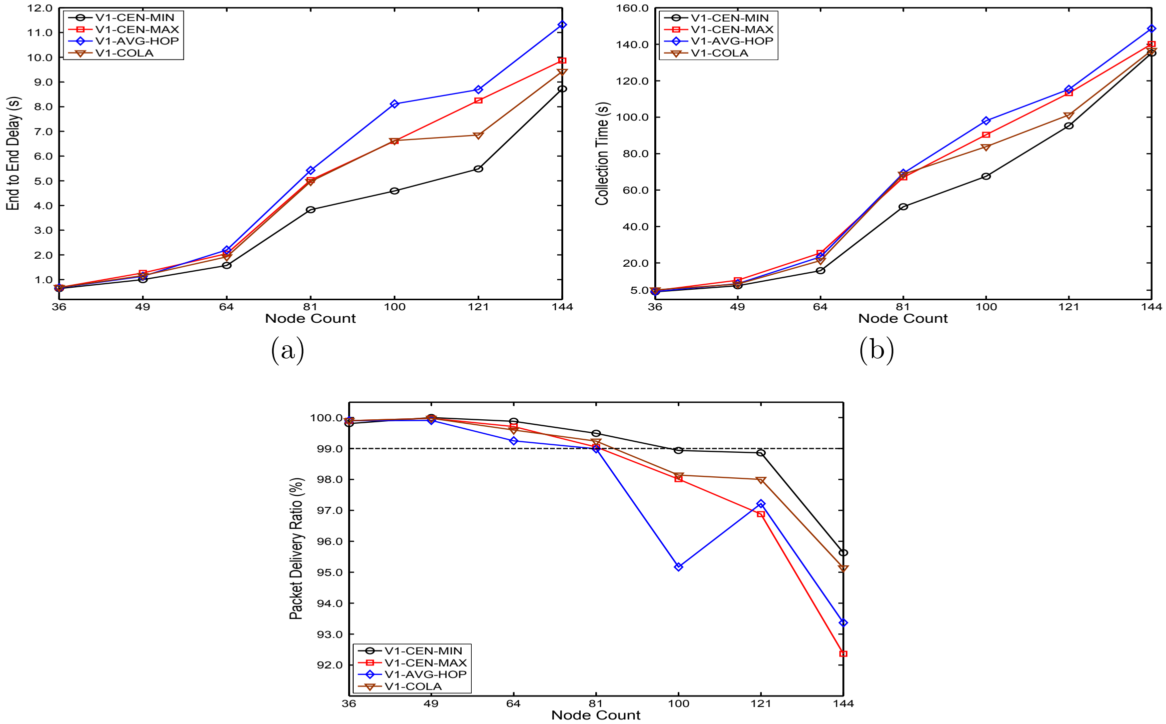
5.4 Performance evaluation

5.4.1 Experiment Setup

The network simulator ns-3 version 3.22 was used to evaluate the performance of the proposed approaches in random network topology of IEEE 802.11s-based AMI network that consists of N mesh nodes, $N \in$ [36,49,64,81,100,121,144]. For each N, 30 network topologies were created. For each topology, one node was selected as the gateway of the network and the (N - 1) remaining nodes represented SMs.

Given that the location of a SM is attached to a consumer's house location, the distance between SMs should follow the distance between houses. Therefore, to represent a realistic SM network, there should be a minimum distance between nodes in the created random network topologies. For this reason, a realistic topology generator called NPART [98] was used. Unlike other topology generators that strive to put the nodes within a given area and tend to create a dense connected network that does not guarantee a minimum distance between nodes, NPART enables the network to grow to meet the minimum distance requirement. Moreover, the NPART algorithm was built based on the observation from the real world user-defined network topologies and thus, it creates network topologies that have the properties similar to these real networks.

The following specifications were used: IEEE 802.11g as the underlying MAC, 120m transmission range for each node, and 75m minimum distance between nodes. In the experiments, TCP protocol was employed for reliable data delivery and a much higher load was used in order to stress test the IEEE 802.11s-based AMI network for the proposed approaches evaluations. Given that the meter reading data size may vary depending on the detailed information that needs to be included and the use of security and privacy mechanisms, 512-bytes was chosen as the meter reading data size to cover worst cases. This data size was also chosen to maximize the default 532 bytes TCP segment size. In this way, the TCP protocol does not need to fragment the data and still be able to send it as one segment. The meter reading was transmitted periodically every 15secs [62] at the same time by all SMs, assuming it was a commercial and industrial smart meter. The results were presented in graphs as the average from 30-topologies.



(a)

(b)

(c)

Figure 5.4: Gateway Placement evaluation.

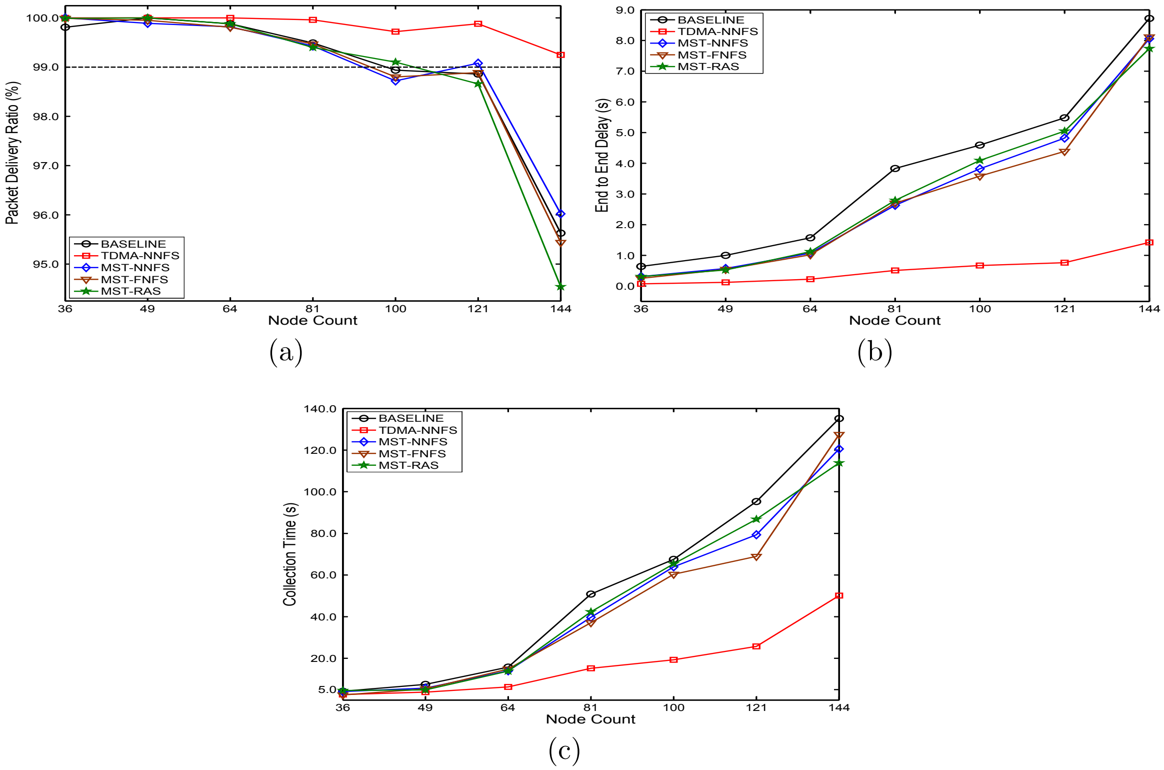
5.4.2 Gateway Placement Evaluation

In this section, the proposed two-stage heuristic 1-vertex center based MST approach was evaluated under the peak traffic (i.e., all SMs send simultaneously). Two versions of the approach were considered, minimizing and maximizing the number of 1-hop neighbors. These approaches were compared with two existing approaches that attempt to minimize the delay: (1) Vertex 1-center approach used in COLA [31]; and (2) Minimum hop count approach [28] [30]. These approaches were labeled in the graphs as V1-CEN-MIN, V1-CEN-MAX, V1-COLA, and V1-AVG-HOP respectively.

The simulation results are depicted in Fig. 5.4 and demonstrate some interesting results. First, V1-CEN-MIN outperforms all other approaches in terms of ETE delay while V1-AVG-HOP approach is the worst. On average for all node counts, the ETE delay discrepancy between these two approaches is 37.6%. When compared to V1-CEN-MAX and V1-COLA, V1-CEN-MIN also improves the ETE delay 29.0% and 21.6% respectively.

Second, it is expected that minimizing the average hop count can reduce overall traveling time and thus the ETE delay. Similar expectation is also valid for V1-CEN-MAX. However, the results indicate that these are not the case. In order to minimize the average hop count, V1-AVG-HOP approach tends to pick a gateway location on a flat tree network (i.e., a network with smaller depth). Hence, the number of 1-hop predecessor nodes per relay node increases. Similar situation arises in V1-CEN-MAX approach, the number of 1-hop predecessor nodes per gateway increases. As a result, each relay node and/or the gateway will suffer from the increased contention and interference that may lead to retransmissions. Hence, this increases delay and eliminates the benefit of shorter traveling time of smaller hop count.

Third, when compared to V1-COLA, V1-CEN-MIN also shows a significant improvement and is able to find a better gateway position that reduces the ETE delay. Fourth, V1-CEN-MIN outperforms all other approaches in term of Collection Time. The performance improvement of V1-CEN-MIN on average of all node counts compared to V1-AVG-HOP, V1-CEN-MAX, and V1-COLA are 25.5%, 29.0%, and 19.9% respectively. And finally, V1-CEN-MIN while showing a significant improvement compared to the other approaches in both ETE delay and collection time, these improvements do not have any effect on the PDR. As a matter of fact, it is slightly higher than all other approaches in term of PDR. On average of all node counts, the following improvement is achieved compared to V1-AVG-HOP, V1-CEN-MAX, and V1-COLA : 1.3%, 1.0%, and 0.4% respectively. Due to it superiority to other



(a) (b)

(c)

Figure 5.5: Scheduling Performance Evaluation.

approaches, for the remaining experiments, the gateway location will be selected by V1-CEN-MIN approach.

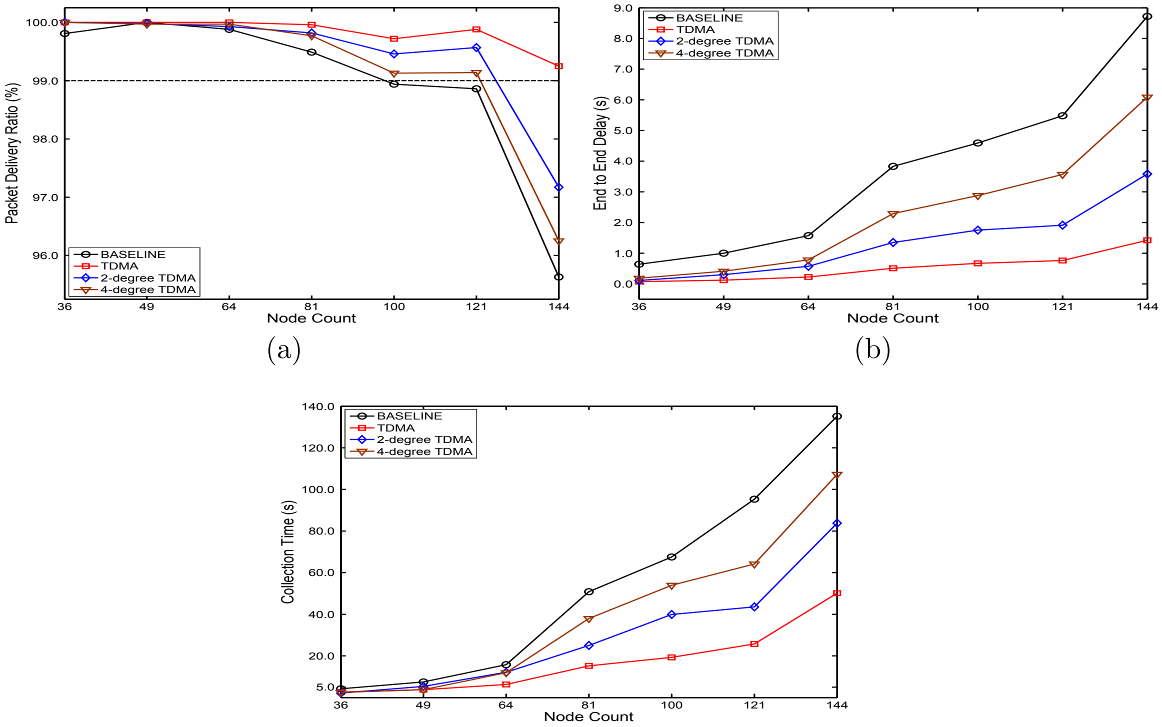
5.4.3 Scheduling Performance Evaluation

The following arbitrary values were used for the experiments: δ and timeslot $T =$ 50ms and $\delta_i \in$ [1ms,10ms]. For TDMA scheduling, since for N SMs there will be N factorial possible time schedule assignments, MST-based time scheduling assignment was used by assigning the time slot to the nearest node first (i.e., NNFS). This TDMA approach was labeled as TDMA-NNFS in the graphs and compared with the BASELINE when all SMs have the same time schedule (i.e., simultaneous scheduling).

As depicted in Fig. 5.5, the results indicate that the network performance can be further improved by giving a different time schedule to SMs which in turn relaxing the contention. When compared to the BASELINE, on average the results are in the following order: MST-RAS (26.6%), MST-NNFS (27.9%), MST-FNFS (31.6%), and TDMA-NNFS (86.4%). The similar order exists the Collection Time: MST-RAS (12.0%), MST-NNFS (13.4%), MST-FNFS (21.0%), and TDMA-NNFS (60.6%).

When comparing the results, the performance improvements from MST-based approaches are not as attractive as TDMA-NNFS. Moreover, even though MST-FNFS outperforms the other MST-based approaches, they perform very close to each other. This can be attributed to the presence of intra-path interference [24] (i.e., interference from other traffic along the same path) and inter-path interference [24] (i.e., interference from nearby traffic that following different path). In TDMA-NNFS, since only a single SM is allowed to transmit in a certain amount of time, interferences caused by other SMs are low compared to the MST-based approaches. Thus, significant improvements can be achieved. In MST-based approaches on the other hand, these interferences are higher due to parallel transmission of several SMs at the same depth level (MST-NNFS and MST-FNFS) or due the close time schedule in MST-RAS as a result of small δ_i.

The results also show that MST-RAS that randomly assigns a unique time schedule to each SM is not a good choice compared to orderly assigned time schedule as in MST-NNFS or MST-FNFS, since it might increase inter-path and intra-path interference in the network. Note that the proposed approaches attempt to avoid simultaneous contention among neighboring SMs when they are sending at the same time. However, the route to the gateway from any SM in multi-hop fashion is guided by HWMP based on Airtime Link metric. This routing metric takes into account the amount of channel resources consumed and is not aware of any possible interference.



(a) (b)

(c)

Figure 5.6: k-degree TDMA evaluation.

5.4.4 Further Evaluation of TDMA-based Scheduling

Based on the simulation results, TDMA scheduling seems a reasonable approach to be used in real-life AMI applications. Instead of letting SMs send their periodic reports simultaneously, by employing TDMA scheduling for the periodic events can reduce the burden on the IEEE 802.11-based SG AMI network and thus lower ETE delay and collection can be achieved when compared to simultaneous transmissions. In this subsection, the performance when more than one SM was allowed to send at any given time was further explored.

As depicted in Fig. 5.6, the simulation results show that as the degree of parallel transmission increases, the network performance decreases. On average, the ETE delay and Collection Time increase around 20% when 2-degree TDMA is used. When

4-degree TDMA is employed, the network performance decreases further, the ETE delay and Collection Time increase 40% and 30% respectively. These results indicate that while the network utilization can be increased, *k*-degree TDMA does not bring the same performance as the TDMA-based approach due to the increased inter-path and intra-path interferences as the number of parallel transmissions increases. Therefore, the tradeoff needs to be considered when selecting the right approach for an application.

5.5 Summary

In this chapter, the problem of data collection in IEEE 802.11s-based AMI network in terms of data scheduling and gateway placement were discussed. A variety of gateway locations were investigated. In particular the gateway selections that were based on the minimum hop count and the number of directly connected nodes to the gateway (either minimum or maximum). The simulation results showed that the gateway location is crucial for the network delay performance. Among the investigated gateway placement methods in this study, the proposed heuristic vertex 1-center based approach provides gateway locations with better ETE delay performance.

Instead of simultaneous periodic data reporting from SMs, three scheduling approaches were proposed. The idea of the approaches was to set the time schedule for every SM individually in order to reduce the ETE packet delay. Both MST-based and TDMA-based approaches were proposed. These approaches were implemented and compared with the strategy of setting the same time schedule for all SMs. The results indicated that the proposed approaches outperform the same time schedule and significant reductions in the delay can be achieved. TDMA-based scheduling provides the best performance.

CHAPTER 6

Spanning Tree based RTO Design for Reduced Packet Delay in IEEE 802.11s-based AMI Networks

In this chapter, the TCP operations that may cause the problem of increased delay in a large-scale multihop IEEE 802.11s-based AMI network are identified. Two proposed TCP layered-protocol approaches to reduce this problem are presented. The first approach is based on the idea of proper setting of RTO values for SMs. Instead of setting each SM with the same recommended RTO values as defined in RFC 6298 as in the traditional networks, the RTO value of each SM is set based on its location in the spanning tree of the network topology. The second approach is based on the idea of limiting the number of doubling when the RTO timer expires. This is motivated from the fact that doubling the RTO increases the RTO value too much that negatively affects the packet delay.

6.1 Problem Motivation and Definition

An IEEE 802.11s-based AMI network introduces a lot of contention when used with TCP. This is because the contention is not only between the transmission of upstream data packets with their downstream acknowledgments (ACKs), but also from the management and control frames of IEEE 802.11s. These contentions eventually cause collision and packet loss which increase the delay. Another major issue is the retransmissions of the packets. The TCP data streams in IEEE 802.11s-based AMI network are performed in a multi-hop manner towards the gateway. This may create several issues. First, there will be traffic bottlenecks and this will increase the chance of packet collisions. Second, the probability of packet drops due to wireless environment characteristics will increase due to increased hop counts.

Finally, the TCP streams may be received at out-of order at the destinations. All these problems contribute to increasing number of retransmissions and thus end-to-end delay.

The problem of retransmissions can introduce additional delays in IEEE 802.11s-based AMI network because of the increased frequency of data collections. Recall that the data collection frequency in some AMI applications can vary from 5secs to 30 secs. In such a case, it is important to collect all the required SM readings for each round so that this data can be used for real-time objectives such as state estimation. However, there is a risk for some of the segments not to be received by the destinations before the next round of data collection begins. This is mainly due to retransmissions as detailed below.

Initially, the RTO timer is equal to a predefined initial RTO value since there is no measured sample. This RTO timer, however, may not be suitable for AMI's data reporting application. Specifically, all SMs will have the same RTO timer since they send their readings at the same time. The network contention for media access is also high and heavy congestion may occur when all SMs sending their data readings. As a result, some SMs may not receive ACKs for their reading either due to packet loss or the RTO timer expires. These SMs will retransmit their data at the same time again and will have the same new RTO timer. Typically, when the RTO timer expires and ACK has not been received, the RTO timer is doubled by TCP. As a consequence, when some of the SMs still do not receive any ACKs, the similar problem persists: These SMs will retransmit again at the same time and have the same new RTO timer's value and so on.

Doubling the RTO timer when the RTO timer expires may pose additional delay, especially when its value exceeds the next power reading reporting time. To assess the seriousness of the problem, some experiments were conducted to measure the

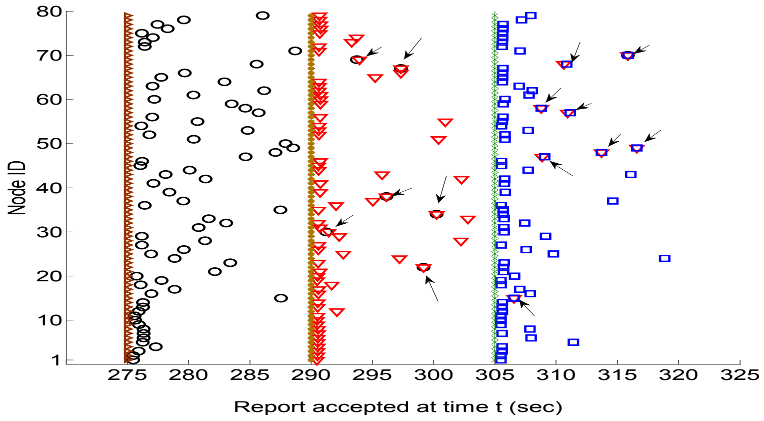


Figure 6.1: Arrival time for some of the readings exceed the next reading schedule. These are shown by arrows in the figure. The reporting is done every 15 secs (e.g., at time 275secs, 290secs, and 305secs).

number of segments that cannot be transmitted until the next round. The result depicted in Fig. 6.1 indicates that there are indeed a good number of segments which could not be transmitted.

In such a case, the next data reporting action at an SM must wait for the previous reading to be acknowledged first. In case of waiting too much, the RTO timer may expire before an SM can send its reading to the gateway. In case the timer expires, this next reading can be sent together with the previous reading, either partially or in a whole, depending on the window size. However, since TCP sends data in byte streams, there is no definite boundary between the previous and the next data readings. Hence, the receiver must know exactly the data size in order to recover both readings individually. The receiver also needs a temporary storage when the next reading is partially sent due to the window size limitation. This partial reading must be stored until the next segment arrives and the whole reading can be recovered.

These results indicate that retransmissions not only will increase the delay but also complicate things in order to handle failed readings. Therefore, it is important to address this problem in IEEE 802.11s-based AMI networks. The problem can be defined as follows: “Given an IEEE 802.11s-based AMI network with a certain number of SMs, their locations, topology and data collection frequency, the goal is to propose a mechanism to reduce the number of retransmissions and thus the end-to-end delay when TCP is employed.”

6.2 Spanning-tree based Approach

In this section, two proposed changes to TCP protocol are discussed in order to reduce the delay as detailed below.

6.2.1 Spanning-tree Based RTO Setting

RFC 6298 [73] defines the standard algorithm that TCP senders are required to use to compute and manage their retransmission timer. It is computed when an ACK is received at a sender with the following equation:

$$RTO = SRTT + 4 \times RTTVAR \tag{6.1}$$

where, SRTT represents smoothed Round Trip Transmission (RTT) delay of the measured samples, and RTTVAR represents the RTT variation. Note that the RTT samples must not be taken from packets that were retransmitted. The RFC also specifies three parameter values related to an RTO value:

1. The initial RTO value when there is no measured sample RTT. The recommended value is now 1sec rather than 3secs as in the previous version (i.e., RFC 2988 [99]).
2. The minimum RTO value. Note that whenever the computed RTO (using Eq. 6.1) is greater than this minimum RTO, then that value is used as the minimum RTO. The suggested minimum RTO value is 1sec.

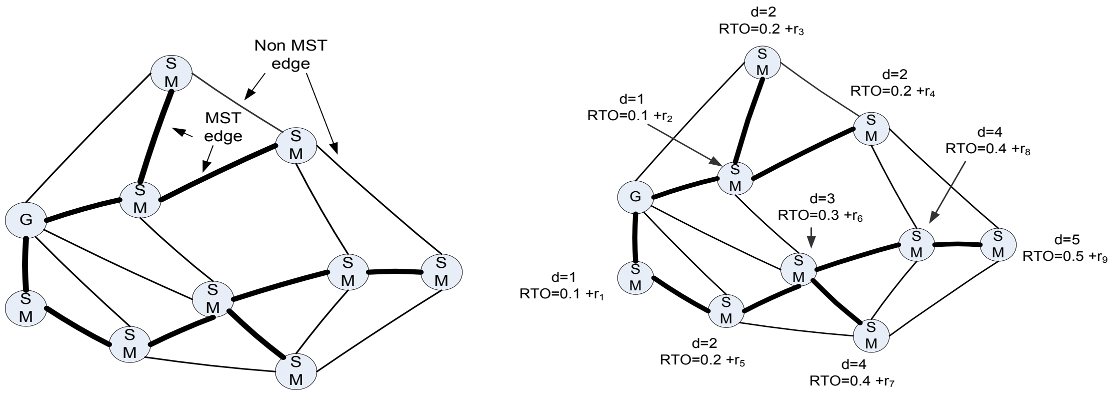
3. The new RTO value is set when the RTO timer expires. The RTO value must be doubled each time the RTO timer expires.

These values are used as follows: when a sender sends a data segment, an RTO timer is activated. The value of the RTO timer can be equal to the initial RTO value when there is no sample of RTT, or the minimum RTO value when the computed RTO is less than this minimum RTO. Otherwise, it will equal to the computed RTO.

Several things need to be considered when using the recommended values in RFC 6298 for an IEEE 802.11s-based AMI Network since the way RTOs are set may affect the delay performance of the network due to the unique characteristics of SG AMI applications. First of all, the SMs send their power readings at the same time, creating a lot of contention in the network. Second, the frequency of data collection can be very high for some applications and thus there is a risk for some of the packets not to be received before the next cycle for data collection starts, creating a lot of overhead. Finally, the routes will include multiple hops which increase the possibility of packet loss due to wireless environments.

Therefore, the tree-based minimum RTO allocation mechanism that takes into account the location of SM and IEEE 802.11s path selection mechanism is proposed for AMI applications. Typically, the location of a SM is attached to a certain household location. Hence, its location is known a priori. IEEE 802.11s on the other hand, employs a proactive tree-base path selection to build proactive route from SMs to the gateway. Hence, each SM has an associate node's position in the network tree topology. To this end, depending on the node's position on the tree, each SM has a different hop count to the gateway. It takes longer time to send to and receive data from the gateway as the SM's hop count increases.

Building a spanning tree (ST) for an IEEE 802.11s-based AMI network is proposed to identify the unique location of each SM in the network. An ST of a con-



(a) (b)

Figure 6.2: Minimum Spanning Tree (MST). a) An example of MST, the thick lines are MST edges, the thin lines are non MST edges. b) Assigned RTOs for the nodes based on ST locations.

nected graph $G(V,E)$ can be defined as a maximal set of edges of G that contains no cycle, or as a minimal set of edges of G that connects all vertices. A sample is given in Fig. 6.2a. Determining the minimum ST of a network has been widely studied in the literature (e.g., Prim's MST Algorithm [95]) and this can be done by the gateway node after collecting the MAC addresses of SMs in the IEEE 802.11s-based AMI network.

The goal is to assign a different minimum RTO for each SM based on its position in the ST. Specifically, SMs at the same ST depth level will have a similar minimum RTO while SMs that are further away from the gateway (i.e., has a higher network tree depth level) will be assigned a higher minimum RTO. The following formula is used for setting the minimum RTO for a particular SM i at level d_i:

$$minRTO^i_d = 0.1 \times d_i + r_i \tag{6.2}$$

where r_i represents a random value introduced for each depth level so that SMs at the same depth level will have different RTO values. With this assignment, the RTO values for the SMs in Fig. 6.2a will be as shown in Fig. 6.2b.

6.2.2 Freezing RTO

The RFC 6298 does not specifically define the upper bound of the doubling mechanism when the RTO timer expires. I also follow an idea for stopping the doubling of RTO timer when the ACK is not received. Basically, if an ACK is not received after the first doubling of RTO timer, then the timer is not re-doubled but frozen until the ACK is arrived. In this way, whenever RTO timer expires again after that, the retransmission interval for the corresponding packet remains constant.

6.3 Performance evaluation

6.3.1 Experiment Setup

The performance of the proposed approaches was evaluated using ns-3 which has the realistic protocol settings for the behavior of the IEEE 802.11s mesh and TCP/IP protocol stacks. IEEE 802.11s-based AMI networks that consist of **N** by **N** nodes were created, $N \in [5,6,7,8,9,10,11,12]$. One node acted as the data collector while the rest acted as the SMs. The transmission range between the nodes was assumed to be 120m. The underlying MAC was assumed to be IEEE 802.11g. HWMP proactive mode was used to determine the paths among the SMs and gateway. The power readings were put in a packet size of 512 bytes and these packets were transmitted every 15secs which is consistent with some of the real SMs on the market [100]. The packets were assumed to be sent at the same times by all the SMs since this data will be used by the utility to do real-time state estimation.

The baseline approach was based on the basic operations of HWMP and TCP/IP protocol stacks in ns3.18. The initial and minimum RTO of 1sec as suggested in RFC 6298 were used for the baseline. The experiments were conducted to assess the ETE delay, throughput and PDR compared to this baseline.

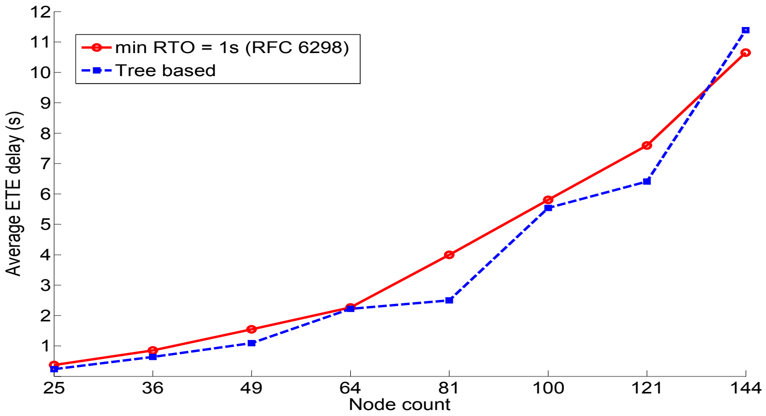


Figure 6.3: Tree-based min RTO allocation

6.3.2 ETE Delay Performance

As depicted in Fig. 6.3, on average the proposed approach improves the ETE delay around 18% when compare to min RTO=1s. However, there are fluctuations in the results and the improvement is not very significant. First of all, the ETE delay of the proposed approach is less than that of the baseline approach except for 144 nodes. Further investigation revealed that there is one SM that not able to establish a TCP connection with the gateway due to Address Resolution Protocol (ARP) issues. Basically, ARP requests could be lost and some of the SMs may not establish a TCP connection as shown in the previous study [101]. This may result in less traffic and thus less contention in the network, reducing the ETE delay for the baseline. In the proposed approach, however, all SMs are able to establish TCP connections with the gateway and send their readings.

Additionally, further analysis about the behavior of RT setting and timeouts was conducted by using the topology of 81 nodes. The maximum depth level for this topology was 16 and hence the highest minimum RTO based on Eq. 6.2 would be around 2secs. Fig. 6.4 shows the snapshot of the arriving packets and RTO expiration times. The results show that the variation in RTO timer values is very

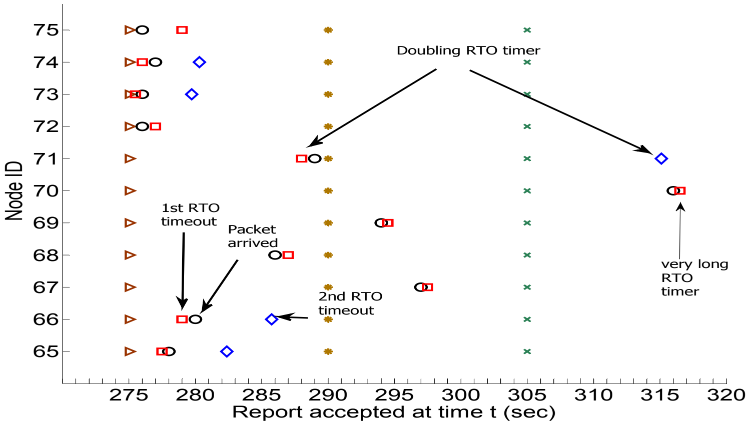


Figure 6.4: Doubling the RTO timer exceeds the next reading schedule. The figure only shows for packets sent at 275secs

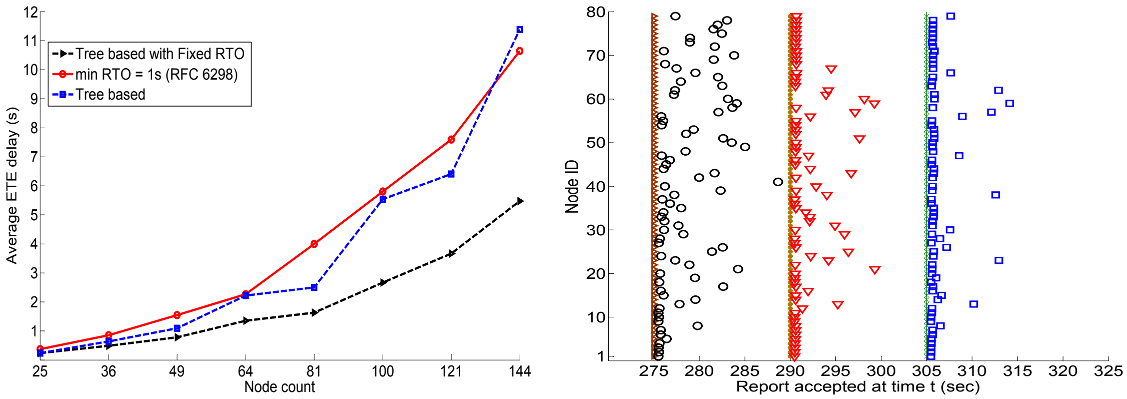
high. In fact, some of the RTO values are higher than 2secs. This indicates that the network was previously having high contention and collision that causes the RTTs of previous sending reports were high. The RTT estimator, which calculates the RTO based on Eq. 6.2, estimates that the current report most likely will having the same issue and thus higher RTO value is used.

I argue that estimating the RTO value is critically important since its value is expected to be the reflection of the network conditions. For instance, when the actual packet is not lost, a small RTO value may trigger a packet retransmission due to network congestion which eventually increases the ETE delay. However, when the packet is actually lost, a small RTO value gives the benefit of a fast retransmission and hence reduces the ETE delay. On the other hand, a longer RTO may prevent a packet retransmission since it will be sufficient to receive the ACK. The negative side of a longer RTO timer is when the packet is actually lost and the sender needs to wait long enough before it can retransmit the packet. These situations increase the ETE delay and can be observed in Fig. 6.4. For instance, five packet retransmissions have occurred (e.g., node ID 65, 66, 71, 73, and 74) and the gateway receives those packets not long after the RTO expires. The node ID

73 and 74 have a smaller RTO timer compared to the others and thus they have lower ETE delay.Recall that doubling the RTO value when the RTO expires poses a problem when the value encompasses the next data reading scheduled. For instance, the node with the ID 71 has the second highest RTO value that exceeds the next two data reading scheduled. Fortunately, the data reading has been received by the gateway and its acknowledgment also has been received by the sender before the next scheduled so that the node can send its next scheduled report as planned. On the other hand, node with ID 70 has a very long RTO value that exceeds the next two scheduled. Hence, the next two packets are held until the previous packet has been received and acknowledged. These increase the ETE delay significantly. Based on this result, freezing RTO value at the SMs is proposed to reduce ETE delay as discussed next.

6.3.3 ETE Performance with Frozen RTO

The same experiments as in Section 6.3.2 were repeated but by applying the idea of RTO freezing. Basically, after an RTO timer was doubled, it stopped there and no more doubling was performed. When compared to the baseline and the tree-based approach as depicted in Fig. 6.5a, the results indicate that freezing the RTO significantly help reducing the ETE delay. Overall, this approach reduces the ETE delay around 48% (on average of all node count) and 41% compared to baseline and tree-based approach respectively. This is attributed to the fact that retransmissions are forced and thus a sender does not have to wait too long for the congested packets which really need for retransmission. Eventually, the ETE delay is reduced. To confirm the effectiveness of the improvement when the frozen RTO approach was employed, the snapshot of the arrival times of readings when the frozen RTO



(a) (b)

Figure 6.5: Tree based min RTO allocation with Fixed RTO approach when RTO timer timeout. a) The ETE delay comparison, b) Arrival time when fixed RTO is employed, no more reading exceeds the next scheduled report.

Table 6.1: Packet Delivery Ratio (PDR)

Grid Topology	*minRTO=1s*	*Tree-based*	*Tree-based with FRTO*
5x5	100.00	100.00	100.00
6x6	100.00	100.00	100.00
7x7	99.54	100.00	100.00
8x8	99.06	99.21	100.00
9x9	99.57	99.45	100.00
10x10	99.24	99.46	99.87
11x11	97.97	97.21	99.76
12x12	97.51	97.36	99.54

is depicted in Fig. 6.5b. The snapshot indicates that all packets were able to be received by the gateway before the next reading cycle starts.

6.3.4 PDR and Throughput Performance

The other two performance metrics also verify that the proposed approaches did not impose any adverse effect. As depicted in Table 6.1, the PDR results indicate that both the tree-based and the combined approaches are as better as the baseline. The PDR stays 100% for smaller network sizes. For larger network sizes, the PDR is still close to 100% and the tree-based approach along with freezing performs even slightly better, which is promising. Similar situation is observed for the throughput

Table 6.2: Throughput (kbps)

Grid Topology	*minRTO=1s*	*Tree-based*	*Tree-based with FRTO*
5x5	6.59	6.59	6.57
6x6	9.59	9.59	9.60
7x7	12.96	13.08	13.15
8x8	16.75	16.84	17.10
9x9	21.27	21.39	21.49
10x10	26.30	26.30	26.58
11x11	31.70	31.23	31.74
12x12	37.36	37.36	38.01

as depicted in Table 6.2. The proposed approaches do not impact the throughput. On the contrary, in large-scales the throughput is even slightly higher.

6.4 Summary

In this chapter, an improved TCP that can be used for an IEEE 802.11s-based AMI network to support a variety of applications was proposed. The idea of the approach was to set the RTOs of each SM in order to reduce the end-to-end packet delay. The setting was done by considering the distance of each SM from the gateway in the network. Specifically, distant SMs were provided with longer RTOs so that their RTO will not expire quickly and thus retransmission of data segments can be prevented. A freezing the RTO mechanism was also proposed to further reduced the ETE delay. The proposed approaches were implemented and compared with the traditional TCP in terms of packet delay, throughput and PDR. The results indicated that significant reductions in the delay can be achieved regardless of the network size. In addition, the proposed approaches do not negatively impact the PDR and throughput performances.

CHAPTER 7

Path Error-Aware RTO Design for Smart Meter Data Traffic in IEEE 802.11s-based AMI Network

While in Chapter 6 layered protocol approaches to reduce the ETE delay are discussed, in this chapter a heuristic cross-layer approach between the data-link layer and transport layer is proposed to tackle the RTO problem. The main idea is to incorporate the rich information from the data link layer in the TCP operations at the transport layer, in particular in the decision of doubling the RTO value when the RTO timer expires.

7.1 Problem Motivation and Definition

IEEE 802.11s standard enables the self-formation and self-healing of multi-hop wireless mesh networks. To this end, it adds new functionalities to the MAC layer of IEEE 802.11 standard such as Peering Management Protocol (PMP) for forming the mesh network and Hybrid Wireless Mesh Protocol (HWMP) for finding the best paths between a source to the destination mesh node in the mesh networks [9]. PMP suggests that each mesh node sends periodic beacon messages to its one-hop neighbors in order to maintain the wireless links among themselves.

These functionalities bring many advantages. However, they also introduce additional overhead to the MAC layer operations which may in turn disturb the operation of the upper network protocol layers. For instance, when an active peer link between two mesh nodes is suddenly closed by PMP because of a lack of a beacon message on time or beacon collisions, both mesh nodes will not be able to forward any frame to each other. When one of the mesh nodes at one end wants to forward a data frame to the other end, it will identify this as a link failure, determine that the destination is unreachable, and trigger HWMP to issue a path error (PERR) frame to notify precursor(s) about it. Each intermediate precursor that receives this PERR will invalidate the broken path from its path table and forward the PERR back to the next precursor until it reaches the originator of the frame. Upon the reception of the PERR frame, the originator starts a path discovery to find a new path to the destination.

These processes may eventually cause the RTO timer to expire when TCP is employed at the transport layer. Note that each time TCP sends a segment, an RTO timer is kicked in. When it expires, TCP will assume that there is congestion in the network and initiate a congestion control mechanism and increase the waiting time for receiving any feedback from the destination by doubling the RTO timer. This is a well-known phenomenon in TCP wireless research [34]. The inability to detect the actual cause of the timeout would eventually increase the ETE delay for the packets.

Given that IEEE 802.11s-based SG AMI networks are also used to support delay-sensitive applications in SG, such as distribution state estimation [102] [103] and demand response, there is a need to reduce ETE packet delay to meet the delay requirements by handling the above issue. The problem can be defined as follows: "Given an IEEE 802.11s-based wireless mesh network that operates as a Neighborhood Area Network for AMI applications, the goal is to come up with a mechanism to minimize the ETE data delay by handling the way TCP reacts to non-congestion events caused by the path disruption in IEEE 802.11s." To this end, a novel cross-layer heuristic approach, called Path Error Aware Retransmission Timeout (PEA-RTO), is proposed. This approach changes the retransmission timeout mechanism so that TCP will be aware of non-congestion events caused by link failures.

7.2 Path Error Aware Retransmission Timeout (PEA-RTO) Approach

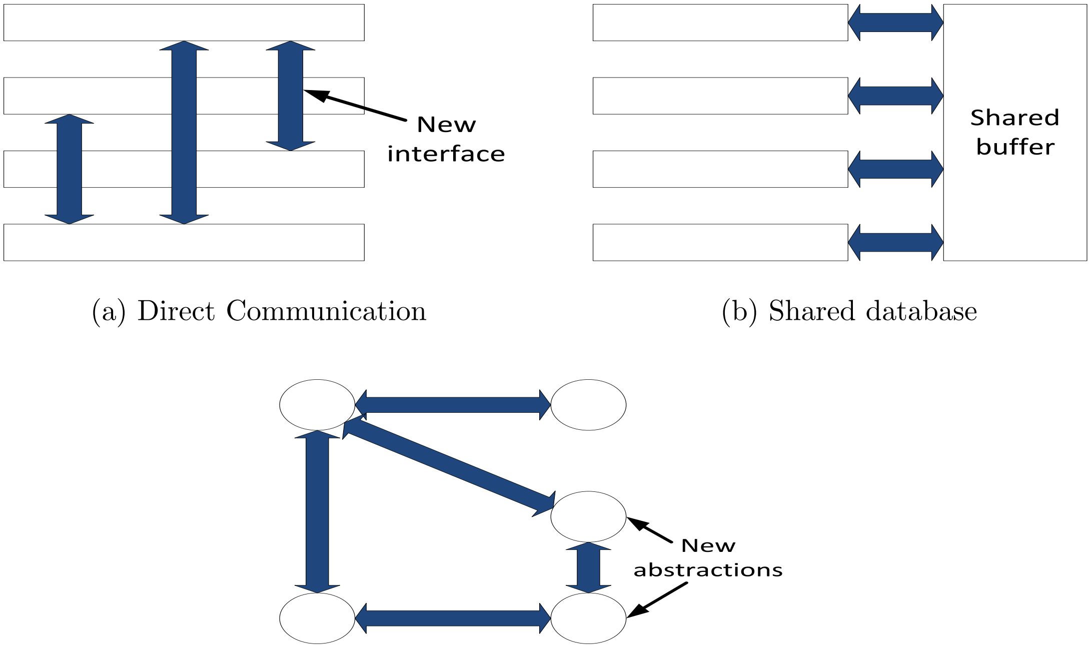
7.2.1 Overview

PEA-RTO is a lightweight heuristic cross layer approach which involves the data link layer and transport layer of the protocol stack. Unlike other existing feedback-based approaches (e.g., Explicit Link Failure Notification (ELFN) [41], Ad hoc TCP (ATCP) [42], TCP Buffering capability and Sequence Information (TCP-BuS) [43], and TCP Feedback (TCP-F) [44]) that need to add additional mechanism to enable intermediate nodes to inform the sender, PEA-RTO is lightweight since it utilizes the available information about path disruption events from HWMP at the data link layer to make decisions on RTO timer doubling mechanism at the transport layer. The idea is to make the right decision on RTO timer in order to minimize the ETE delay. The doubling of RTO is not done automatically but based on the feedback from the data link layer which handles path creation in IEEE 802.11s. The approach includes the design of a shared buffer and adjustment of RTO timer as detailed below.

7.2.2 Cross-layer Mechanism for a Shared Buffer

In designing a cross-layer approach, there are three possible options for layer interactions in the TCP/IP model [3]: (1) direct communication between layers; (2) a shared database across layers; and (3) completely new abstractions. Fig. 7.1 shows these tree possible options. While the last category may offer novel organization of protocols and flexibility, it requires major changes in the protocol stack and therefore is not preferred.

Direct communication allows run-time information sharing between layers while shared database allows optimization among multiple layers at once. Since the goal



(a) Direct Communication

(b) Shared database

(c) New abstraction

Figure 7.1: Three possible options for cross layer interaction [3]

is to provide the information of non-congestion events to the TCP so that it can react accordingly when the RTO timer expires, an upward information flow of non-congestion related PERR information through direct communication can facilitate this goal. However, since this PERR information can arrive anytime at the transport layer, a shared storage will be needed to keep this information so that it can be used when there is a need for it. Note that this information is only needed when the RTO timer expires in order to assist in the decision on the timer doubling mechanism. Hence, instead of adding more complexity at the transport layer for maintaining a buffer, the idea of a shared buffer is more attractive for the proposed cross-layer approach.

A shared buffer that acts as a shared database across layers is used to store the time of issuance of the PERR frames. To interact with the shared buffer, both the data link and transport layers need to be modified. In addition, the RFC-6298 [73]

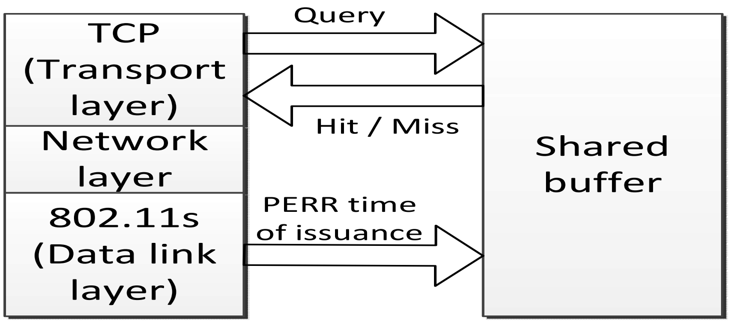


Figure 7.2: Cross layer approach between TCP and HWMP

that defines the standard algorithm for the TCP senders to compute and manage the retransmission timer also needs to be modified. In particular, modification is needed to the action that will be taken when retransmission timer expires. Fig. 7.2 shows the interaction between layers for sharing PERR information.

The link-layer supplies the shared buffer with the time of issuance of a PERR and the time when the originator receives the propagated PERR frame. Note that the originator is the final receiver of the propagated PERR frame and hence it does not need to issue any propagated PERR frames. The transport layer, on the other hand, sends a query to the shared buffer when the RTO timer expires, asking whether there is any PERR frame that has been issued between the time when the RTO timer kicks in (i.e. the time when the packet is transmitted) and the RTO timer expires. The shared buffer returns a **Hit** when there is any PERR frame issued within the given time interval and a **Miss** if otherwise.

The shared buffer itself will have three main operations: (1) add operation for adding time of issuance for the PERR frame; (2) search operation for finding whether there is a PERR frame issued within a given time interval; and (3) delete operation for erasing the shared buffer content when there is a Hit event to save some space and speed up the searching process.

7.2.3 Setting the RTO Timer

In addition to the design and implementation of this shared buffer, a heuristic mechanism for the retransmissions when the RTO timer expires is proposed at the transport layer. Specifically, the proposed mechanism acts based on the response it gets from the shared buffer as follows: (1) to set the new RTO timer equal to the previous value when a **Hit** is received; or (2) to double the RTO timer as defined in the RFC-6298 when a **Miss** is received. The pseudo-code of the retransmission mechanism is shown in Alg. 4.

Algorithm 4 Retransmission Mechanism

```
$x \leftarrow$ timer starting time
if retransmission timer expires then
    $y \leftarrow$ timer ending time
    $ret \leftarrow$ Query(x,y)
    if $ret = Hit$ then
        new timer = old timer
    else
        new timer = old timer $\times$ 2
    end if
end if
```

Keeping the old RTO timer when there is a **Hit** is based on the fact that the timer expiration was not due to congestion but due to a link failure. In this case, HWMP of IEEE 802.11s standard will start a new path discovery to find an alternative path to the destination and, when this path is found, the packet can be sent immediately. Eventually, the ETE packet delay can be reduced since TCP would try to retransmit the packet by doubling the RTO timer otherwise. On the other hand, when the network is congested, the path is assumed to be still alive, and either the packet or the response is still in transit and it has been delayed due to a lot of traffic using the same path. In this case, doubling the RTO timer will help in succeeding the transmission of the packet.

7.2.4 Further Optimization

In the proposed approach, there is no upper bound limit for the RTO timer value. This means, when a packet experiences multiple RTO timeouts, the waiting time of the sender to receive an ACK increases exponentially for each RTO timeout. The longer waiting time may increase the receiving time of a packet at the receiver which eventually delays the whole data collection process. Note that the data collection process at each round depends on the longest receiving time of a packet. As discussed in Chapter 6, by specifying an upper bound limit to the RTO timer can further reduce the ETE delay. Therefore, similar approach by adding an upper bound limit to the RTO timer is proposed to further decrease the delays. In the experiments, the number of times an RTO is doubled will be limited to two. This means, in case of successive multiple timeouts, the doubling mechanism will only be in effect twice.

7.3 Performance Evaluation

7.3.1 Experiment Setup

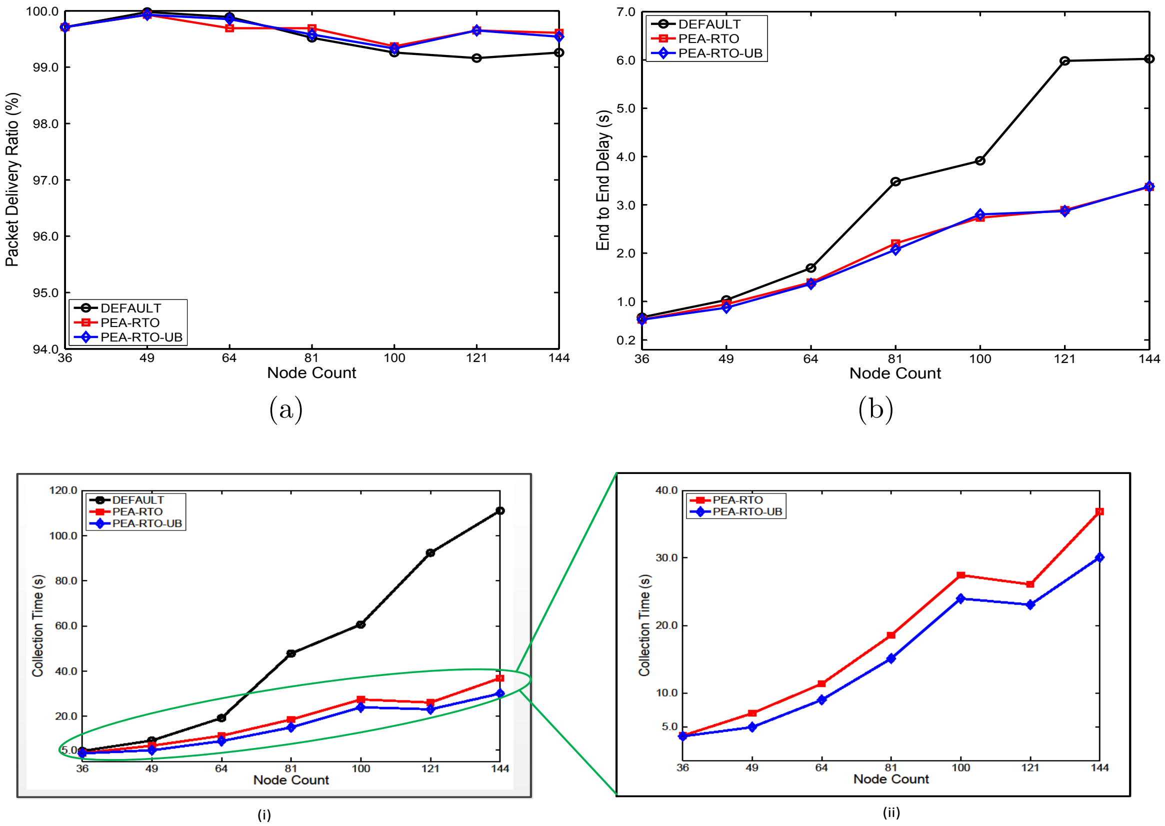
The discrete-event network simulator ns3 version 3.22 that has the implementation of IEEE 802.11s [104] was used to evaluate the performance of PEA-RTO. A realistic network topology generator called NPART [98] was used to create 30 random connected network topologies for IEEE 802.11s-based AMI network. Each random topology consists of **N** nodes, $\mathbf{N} \in [36,49,64,81,100,121,144]$. One node in each topology was selected as the data collector while the rest acted as SMs. The data collector was also the root of the IEEE 802.11s-based AMI network. The minimum distance between nodes was 60m, the transmission range was assumed to be 120m, and the underlying MAC protocol was IEEE 802.11g. Each SM generated periodic simultaneous data traffic with the packet size of 512 bytes every 15secs [105]. The simulation time was 500secs.

The background traffic was the Address Resolution Protocol (ARP) operations. In the beginning of the simulation, each node has an empty ARP table and therefore, before the TCP connection establishment, broadcast ARP requests were issued from all SMs to find the MAC-IP address mapping for their ARP table. Two ARP parameters, *ARP AliveTimeOut* and *ARP WaitReplyTimeout*, were configured to be 120secs and 4secs, respectively. Note that *ARP AliveTimeOut* determines the number of occurrence of broadcasts ARP requests in the network for ARP table maintenance while *ARP WaitReplyTimeout* defines the number of seconds a node must wait for ARP reply in response to its ARP broadcast request. The latter parameter is sensitive to the network size, 4secs waiting time is acceptable for the network size of up to 144 nodes [106].

Simultaneous data traffic running on an IEEE 802.11s-based AMI network was used as the baseline for comparison. This baseline was labeled as **DEFAULT** in the graphs while the path error-aware retransmission timeout without upper bound limit was labeled as **PEA-RTO** in the graphs. Further optimized approach with upper limit was labeled as **PEA-RTO-UB**. The upper limit was set to 2.

7.3.2 Simulation Results

The results depicted in Fig. 7.3 indicate that using the proposed mechanisms significantly improve the performance in terms of ETE delay and collection time for all network sizes when they are compared to the **DEFAULT**. Looking at the PDR performance in Fig. 7.3a, all three approaches achieve very high PDR values, above 99% for all node count. These results are expected as TCP employs retransmission



(a)

(b)

(i)

(ii)

(c)

Figure 7.3: PEA-RTO performance comparison. a) PDR, b) ETE delay, c) Collection Time

mechanisms for the lost packets and indicate that TCP is suitable for SG applications that require high reliability.

However, significant improvements are observed for the other two metrics when **PEA-RTO** is employed. As depicted in Fig. 7.3b and Fig. 7.3c, TCP induces high ETE delay and collection time proportional to the network scale in the **DEFAULT** approach. This makes TCP unattractive for some real-time SG applications that need low ETE delay and collection time. The poor performance of TCP is due to the fact that TCP reacts to link failures by triggering its congestion control algorithms which brings extra overhead and delay. This is not the case for **PEA-RTO** that reduces the ETE delay and collection time on average of all node count, by 28% and 49% respectively. Moreover, the reduction on both metrics increases with the network scale. This can be explained in the way how the RTO timer reacts to the presence of non-congestion events that makes a significant different to the ETE delay and collection time. Specifically, **PEA-RTO** approach provides a faster retransmission response to the non-congestion related packet loss, instead of waiting a longer time to provide the retransmission response as in the **DEFAULT** approach.

When comparing **PEA-RTO** and **PEA-RTO-UB** in terms of PDR and ETE delay, their performance is very much similar. However in terms of the collection time, **PEA-RTO-UB** outperforms **PEA-RTO** as can be seen in Fig. 7.3c. By employing an upper bound to the RTO timer, an additional collection time reduction of around 20% can be achieved. The collection time is decreasing proportionally as the network scales. This result indicates that there were still some multiple timeouts when **PEA-RTO** was used. Limiting the doubling mechanism to a certain number such as 2, further improves the TCP performance. In this way, the RTO timer is not doubled unnecessarily and eventually this saves some times when sending all the packets to the gateway.

7.4 Summary

In this chapter, a novel heuristic cross-layer path error aware retransmission timeout for IEEE 802.11s SG AMI Networks was proposed. The idea of this approach was to take advantage of the rich information generated by IEEE 802.11s at the data link layer, specifically from the path selection and maintenance mechanism, for the adaptive decision of the retransmission timeout timer value at the transport layer. This heuristic was based on the observation of the path error and the hit rate of the issuance of path error within an active RTO timer. The simulation results indicated that, even though the proposed cross-layer approach adds additional complexity to the network protocol operations, the margin of performance improvement is much more significant than the complexity. The simulation results also suggested that for SG applications that require low collection time metric, setting an upper bound to the doubling mechanism can lower the collection time.

CHAPTER 8

A Secure Piggybacking-based ARP for IEEE 802.11s-based AMI Network

An efficient and secure cross-layer approach between data link layer and network layer that addresses the overhead of Address Resolution Protocol (ARP) broadcast in large scales IEEE 802.11s-based AMI networks is presented in this chapter. The proposed approach, called Piggybacked ARP Secure (PARP-S), efficiently eliminates the broadcast storm issue of the ARP broadcast by piggybacking the ARP to the default path selection mechanism of IEEE 802.11s that operates at the data link layer.

8.1 Problem Motivation and Definition

In IEEE 802.11s-based AMI networks, typically the data collector gateway and SMs have two different external networks to communicate with as depicted in Fig. 8.1. As such, both gateway and SMs will need to support IEEE 802.11s to form the WMN and TCP/IP to communicate with WAN or HAN respectively. This is needed to provide bi-directional communications between customers and utility

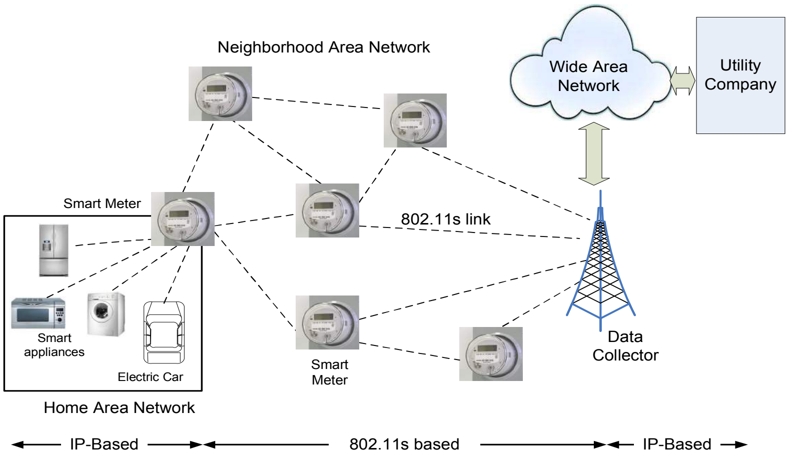


Figure 8.1: AMI two-way communications

company. For instance, the utility company may need to talk to some of the other intelligent devices at the house such as sensors, gas meters which are part of the HAN for demand response and dynamic pricing applications. The reverse is also true. Each of the other intelligent devices that are part of HAN should be able to send data to the utility company when needed. Since the utility company and the devices that are part of HAN utilize TCP/IP stack for communication, they utilize IP addresses of destinations. As a result, even though IEEE 802.11s is employed for communication between SMs (i.e., no need for IP addresses), each SM also needs to employ TCP/IP protocols on top of IEEE 802.11s to support communication to both sides (utility or HAN).

When TCP/IP is employed (i.e., either TCP or UDP is used) at SMs, the communication between the utility and the SMs or any of the HAN devices, are based on IP addresses of destinations. Hence, when the gateway receives a request from the utility company to send data to a particular destination IP, it faces the problem of associating the IP address with a MAC address. This is because IEEE 802.11s utilizes MAC addresses only and the MAC address of the destination node needs to be used for communication within the mesh. As a result, there needs to be an ARP table to keep the IP-MAC associations. When the required MAC address for a destination can not be found in the ARP table, a broadcast ARP request is issued. This broadcast message floods the mesh network. Note that this is not a one-time operation since such broadcast messages are also sent during the periodic maintenance phase of ARP tables.

I claim that the broadcasting of ARP requests in IEEE 802.11s-based WMNs can be a major overhead when the network scales as in the case of SG applications such as AMI. To justify this case, a preliminary testing to demonstrate the effects of the ARP broadcasts in larger scales is performed. For this purpose, a controlled grid

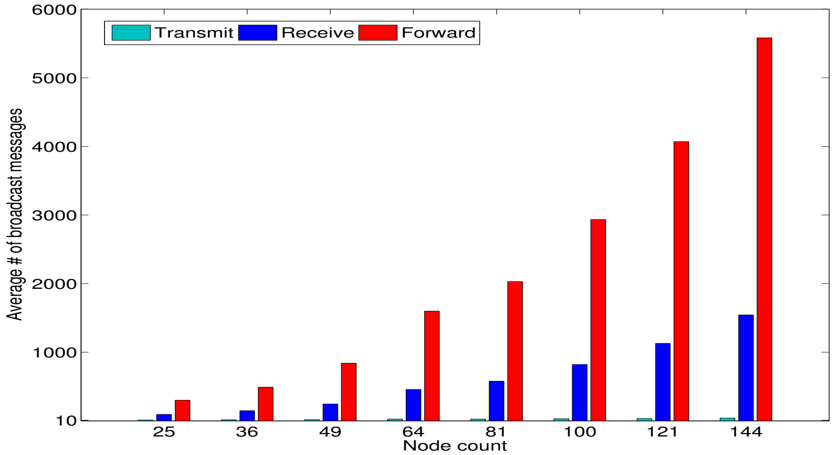


Figure 8.2: Average # of broadcast messages sent per node in HWMP for ARP.

topology in which each node can communicate with a maximum of four neighbors in the vertical and horizontal directions is used. Since the default ARP *AliveTimeOut* is varied between operating systems as summarized in [50], the default ARP *AliveTimeOut* from Windows XP (i.e., 120 secs) is used.

Fig. 8.2 shows the average number of broadcast messages per node triggered by ARP with increased SM count. By default, each node will send an ARP broadcast message when the *AliveTimeOut* expires. The results indicate that even though each node only sends a small number of broadcast messages, the number of received and forwarded broadcast messages per node is much higher which creates the major broadcast storm. With the increased hop count, this is expected since the ARP request messages will be forwarded in the network. Note that ARP replies are also a concern for creating additional traffic but since they are unicast messages, the effect is not as significant as ARP requests messages. The bottom line is that larger networks experience greater broadcast storm than smaller networks that needs to be taken into account in IEEE 802.11s-based AMI networks.

Obviously, these broadcast ARP requests to the same destination are not efficient and consume a significant amount of bandwidth that may affect throughput and prevent the reported data to arrive to the gateway in a timely manner. The timely arrival can be crucial when demand response applications need to use the IEEE 802.11s-based AMI network. Note that configuring a static ARP in each node may alleviate this problem. Nevertheless, this is not an efficient approach considering the number of SMs involved when trying to keep them up to date in case of hardware changes at the gateway node. Therefore, a mechanism that will address this problem in an efficient and secure manner is needed. Next, the details of the proposed approach are explained.

8.2 Piggybacked-based ARP Approach

To alleviate the broadcast storm problem, the modification of HWMP for piggybacking the ARP information is first proposed. Specifically, during the proactive routing formation and maintenance of HWMP in which the gateway node broadcasts a PREQ message, an IP-to-MAC address mapping of the root node is piggybacked in the proactive PREQ message. Every SM that receives this extended proactive PREQ message, in addition to its basic PREQ receiving process, will create or update its ARP table. The decision to create or update is based on the freshness of the PREQ message (i.e., based on the PREQ sequence number).

Nonetheless, this approach works with UDP where there is no need for acknowledgment from the gateway [107] [101]. For TCP protocol or for demand response applications where the gateway node needs to reply with acknowledgments or sends messages to certain SMs, there will be ARP request messages across the network transmitted by the gateway node. This node will issue an ARP request message when it can not find the MAC address of the final destination in its ARP table. Therefore, the previous approach in [107] [101] is extended by adding piggybacked ARP on PREP message in response to the piggybacked ARP in proactive PREQ message. Every SM that receives a piggybacked proactive PREQ, will piggyback its address mapping information in its PREP message to the gateway. On receiving the piggybacked ARP in PREP message, the gateway node creates or updates its ARP table.

8.2.1 Security Considerations

While the aforementioned approach helps reducing the broadcast storm, it becomes vulnerable to ARP cache poisoning attacks more easily since there is no mechanism to handle malicious piggybacked ARP messages. Specifically, an adversary can launch the following attacks:

1. Cache Poisoning Attacks: An adversary can capture the PREQ/PREP message and simply modify the MAC address mapping.
2. ARP Spoofing Attacks: An adversary can issue a fake PREQ/PREP message to divert the traffic of an SM to itself or to another destination including a broadcast MAC address. In addition, it can divert the traffic of an SM and gateway to itself by acting as an intermediary (i.e., man-in-the-middle attack). In this way, it can control every message between the SM and gateway.

To address these attacks, two security goals are set: 1) To authenticate each PREQ/PREP message for verification of sender; 2) To provide integrity of the packets when they are in transmit. In the following subsections, the details of the proposed approach are discussed.

8.2.2 PREQ/PREP Format Changes

Two additional fields for both PREQ/PREP messages are added in the proposed approach: 1) an address mapping field; and 2) a signature field. For the address mapping field, there are two possible choices, either to include: 1) only an IP address; or 2) both IP and MAC addresses. The first choice comes from the fact that the MAC address of the PREQ originator has been included in the PREQ message. PREQ message has the MAC address of the gateway node in the *Originator Mesh STA Address* field. Hence, it reduces the overhead. On the other hand, putting both IP and MAC addresses in the MAC address resolution message is more flexible at the expense of an additional overhead of at least 48-bits (i.e., the length of MAC address). The flexibility is due to possible future changes in the network architecture such as the addition of new nodes with new IP addresses. In that case, the mapping will be already in the packet and the IP-MAC pair will be entered in the ARP table as a new entry. Therefore, the second choice is chosen in the approach and both addresses are stored in the following order: (MAC address, IP address).

To address the aforementioned security goals in Section 8.2.1, a digital signature is added to each of the piggybacked messages. This signature is used to ensure that the IP-to-MAC address mapping at the extended proactive PREQ/PREP message comes from a legitimate node and its integrity is maintained. Each node (either an SM or the gateway) will not update its ARP table unless the signature in the received message is valid. The signature field is used to store the digital signature. Its length varies depending on the length of the signature.

ECDSA, which is the elliptic curve version of DSA [77], is used to create the digital signature. ECDSA has been included as the digital signature scheme in ANSI X9.62, FIPS 186-2, IEEE 1363-2000 and ISO/IEC 15946-2 standard. ECDSA as well as other ECC methods require all parties to have the same elliptic curve domain parameters. These parameters describe an elliptic curve $\mathbf{E}$ defined over a finite field F_q, a base point $\mathbf{P} \in \mathbf{E}(F_q)$, and its order $\mathbf{n}$. However, a domain parameters generation algorithm is optional for elliptic curve based applications.

The ECC domain parameters will be used to obtain the public and private keys. ECDSA uses a private key of a sender to generate the signature and a receiver node uses the sender public key for the signature verification.

Since IEEE 802.11s also uses SAE for authentication, the required ECC domain parameters for ECDSA can be obtained via SAE. SAE stores an identifying number in the authentication algorithm field of an 802.11 authentication frame to identify an elliptic curve domain parameter in the Internet Assigned Numbers Authority (IANA) repository. IANA maintains a repository of finite cyclic groups for the Internet Key Exchange (IKE) [108]. In this way, the proposed ECDSA-based signature approach does not need to handle the domain parameters agreement and distribution and thus uses the same domain parameters as in SAE. Moreover, it does not need to add an additional field in the extended PREQ message to record the signature size for varying key size. Based on the domain parameters, the signature size can be calculated and stored in the SM. This calculation is assumed to be performed during the SAE authentication.

A final change to message format is to be able to distinguish between former PREQ/PREP and the extended PREQ/PREP packets when they are received. To this end, the reserved bit in the *Flags* field is used as the identifier of these two additional fields. The last bit of the *Flags* field is used as the *ARPTag* subfield. These two additional fields are present when $ARPTag = 1$. The extended structure of both proactive PREQ and PREP messages are shown in Fig. 8.3 and Fig. 8.4 respectively.

8.2.3 HWMP Protocol Modifications

With the new packet formats and the involvement of ARP, the operations of HWMP also need to be modified. Before the gateway node sends an extended proactive

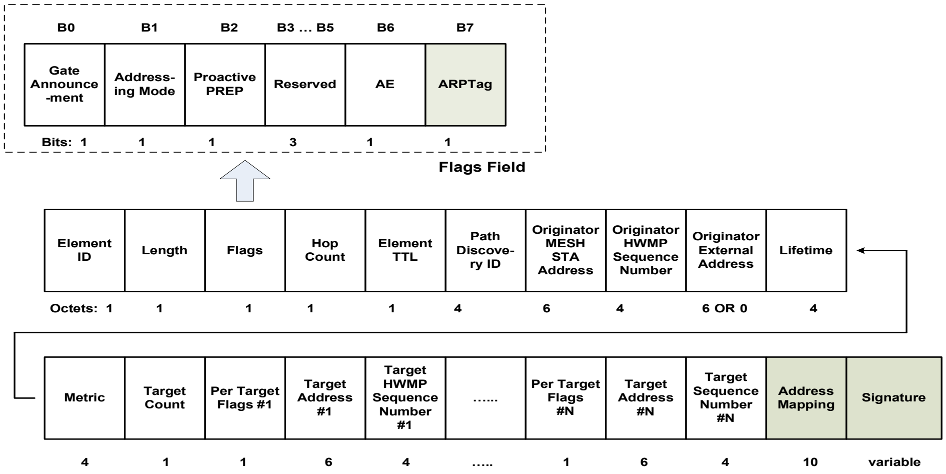


Figure 8.3: Proposed extended PREQ message format for Piggybacked ARP in HWMP

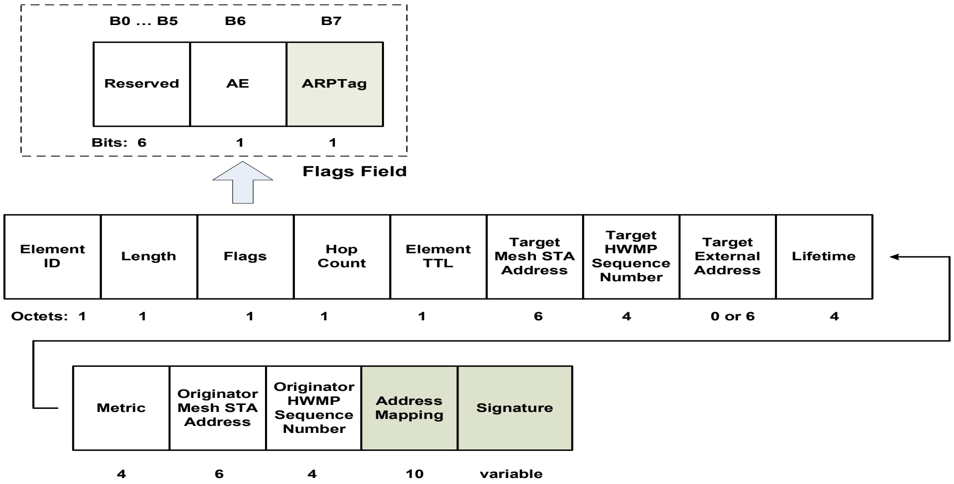


Figure 8.4: Proposed extended PREP message format for Piggybacked ARP in HWMP

PREQ, it signs the address mapping with its private key. When a node receives a PREQ message, first it checks for the additional field based on the Flags field value. If this is an extended PREQ message, the node verifies the digital signature of the message with the gateway node's public key. When the signature is verified, the node performs the following: (1) Creates or updates its ARP table; (2) Creates an extended PREP message, sets the *ARPTag* subfield of the extended message, and signs the extended PREP message with its private key. On receiving this extended PREP message, the gateway node verifies the signature with the sender's public key and creates or updates its ARP table when the signature is valid. The modification of HWMP for the gateway and SM are shown in Algorithm 5 and Algorithm 6 respectively. Algorithm 7 is used for both the gateway and SMs.

Algorithm 5 Send Proactive PREQ

```
if (Is-Time-to-send-PREQ()) then
    Preq-msg ← Create-Proactive-PREQ()
    $ARPTag_{(PREQ)} \leftarrow 1$
    osn ← PREQ originator sequence number
    Address mapping field ← (MAC||IP)
    Signature field ← sign(MAC||osn||IP )
    Preq-msg ← Append(Preq-msg||Address mapping field||signature field)
    Broadcast(Preq-msg)
    Set-Next-Time-to-Send-PREQ()
end if
```

Note that a receiving node may receive multiple copies of PREQ / PREP messages. However, since one of the acceptance criteria in the original HWMP operations is freshness, this feature also ensures that the newest address mapping information will be used for creating / updating an ARP table.

8.3 Performance Evaluations

The description of the detail implementations and an extensive experimental analysis of the approach with respect to several baselines are presented in this section.

Algorithm 6 Receive PREQ

```
Preq-msg ← **Receive-Preq()**
lPassed ← **Verify-Acceptance-Criteria**(Preq-msg)
**if** (lPassed) **then**
    **Update-Routing-Table**()
    Prep-msg ← **Create-Prep**()
    **if** ($ARPTag_{(PREQ)} = 1$) **then**
        $ARPTag_{(PREP)} \leftarrow 1$
        osn ← PREP originator sequence number
        Address mapping field ← (MAC||IP)
        Signature field ← **sign**(MAC||osn||IP )
        Prep-msg ← **Append**(Prep-msg||Address mapping field||signature field)
        osn2 ← PREQ originator sequence number
        sgnt ← PREQ signature field
        lsucceed ← **verify**(sgnt||osn2)
        **if** (lsucceed) **then**
            **Update-ARP-table**()
        **end if**
    **end if**
    **Send-unicast**(Prep-msg)
    **Forward**(Preq-msg)
**end if**
```

Algorithm 7 Receive PREP

```
msg ← **Receive-Prep**()
**if** (**Is-the-Destination**(msg)) **then**
    lPassed ← **Verify-Acceptance-Criteria**(msg)
    **if** (lPassed) **then**
        **Update-Routing-Table**()
        **if** ($ARPTag_{(PREP)} = 1$) **then**
            osn ← PREP originator sequence number
            sgnt ← PREP signature field
            lsucceed ← **verify**(sgnt||osn)
            **if** (lsucceed) **then**
                **Update-ARP-table**()
            **end if**
        **end if**
    **end if**
**end if**
```

8.3.1 Experiment Setup

Network simulator (NS-3) [104] was used to implement and test the proposed approaches. The flow monitor module [109] was used to collect data for performance evaluation. The Crypto++ library 5.6.1 was used for the implementation of authentication part. An **N** by **N** mesh network of SMs using IEEE 802.11g, UDP protocol, and TCP protocol in an area of 1200mX1200m was considered. The transmission range for the nodes was assumed to be 120m. One node was selected as the data collector to communicate with the utility company (e.g., root/gateway) while the rest of the nodes acted as SMs. Note that the area mimics the size of a neighborhood that will be using a single gateway to communicate with the utility company. As a result, node counts in relatively smaller values were used to reflect a rough estimate of households in such a neighborhood. The node count will be increased during the experiments for assessing the performance with the increased of network size and node density. For each node count, 30 random network topologies were created. The results were presented as the average from these 30 topologies for significance. The experiment results were stayed within 4.5%-11% of the average with 90% confidence interval. The confidence intervals were not shown in the figures for the figures clarity. HWMP also uses several parameters to control its operations. While the default HWMP parameters were mostly used, specifically *dot11Mesh-HWMPnetDiameterTraversalTime* parameter was set to 2sec to accommodate various depths of the network topologies and prevent HWMP to retransmit broadcast PREQ packet for path discovery too early.

8.3.2 Performance Baselines

The proposed approach was compared to several baselines by using both UDP and TCP protocols. The experiment results were presented in the graphs using the following names:

1. **Base-A** represents the basic operation of HWMP where there is no piggybacking of ARP and the ARP table of all nodes are initially empty with the default value of *ARP AliveTimeout*. The entries of the ARP table are created

during ARP creation phase and are updated periodically during ARP table maintenance phase.

2. **Base-NA** represents the ideal condition in which there is no ARP broadcast packets during the simulation time. Every node is pre-configured with all required address mapping information by storing the address mapping in the ARP table manually (i.e. static ARP). Static ARP does not need ARP table maintenance phase.

3. **PARP-NS** represents the piggybacked ARP in which the address mapping of the gateway node is piggybacked in every broadcast proactive PREQ to populate the address mapping of the gateway node to all SMs. In response to these proactive PREQ broadcast packets, every node will piggyback its address mapping information in the PREP packet. However, there is no security protection for the piggybacked ARP.

4. **PARP-S** represents the secure version of piggybacked ARP where a digital signature is added in every piggybacked ARP either in proactive PREQ or PREP packets.

The goal in the experiments is threefold: 1) To tune the ARP parameters and find the parameters for the optimal performance; 2) To understand the overhead of the proposed approach in terms of the updated management frames and signatures; and 3) To compare the performance of PARP-NS and PARP-S with the existing approaches.

8.3.3 Tuning ARP Parameters

Before starting to evaluate the proposed approach, the experiments with the baseline to determine the optimal ARP parameters, specifically *ARP WaitReplyTimeout*

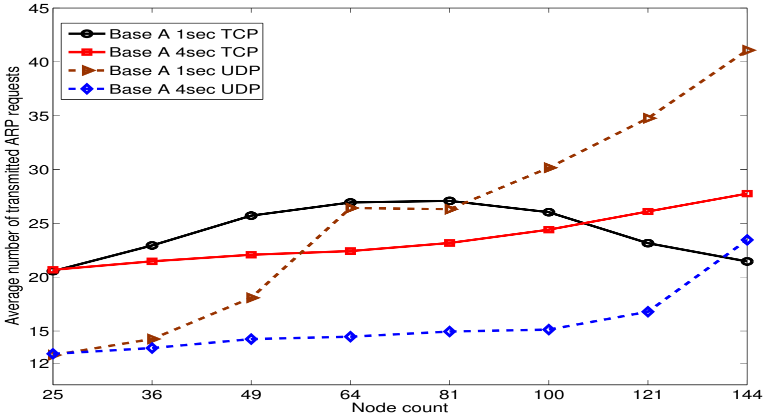


Figure 8.5: Average number of transmitted ARP requests per node

and *ARP AliveTimeout*, were first conducted. Recall that *ARP AliveTimeout* determines the number of occurrance of broadcast ARP requests in the network during the simulation time. The longer the *ARP AliveTimeout* is, the less the ARP requests occur in the network. While the focus was more on *ARP WaitReplyTimeout* since it is sensitive to the network size, the *ARP AliveTimeout* in two extreme cases, namely **Base-A** and **Base-NA**, were presented. *ARP WaitReplyTimeout* was set to two different values, specifically 1sec and 4secs. The baseline with *ARP WaitReplyTimeout* value set to 1sec was represented as **Base-A-1sec** while with the value 4sec was represented as **Base-A-4sec** in the graphs. Next, the performance of these two approaches in terms of ARP request count was investigated. Their PDR, delay and throughput performance were also compared by considering **Base-NA** as a baseline. In this way, the aim is to pick the most appropriate *ARP AliveTimeout* value for the rest of the experiments.

8.3.3.1 Number of ARP Requests

As depicted in Fig. 8.5, basically **Base-A-1sec** transmits more broadcast ARP requests than **Base-A-4sec** since the *ARP WaitReplyTimeout* is too short which

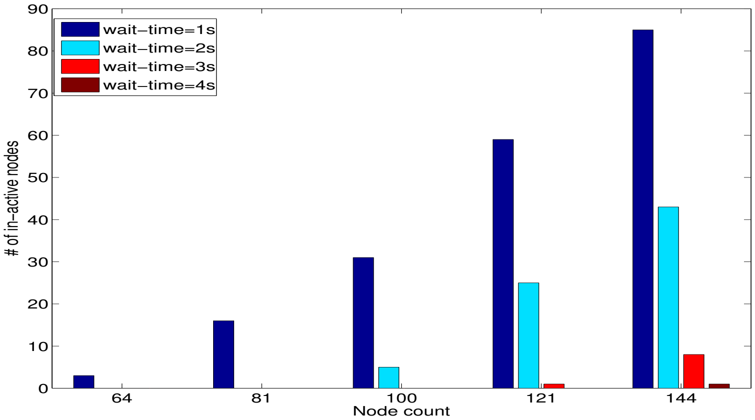


Figure 8.6: Inactive SM count for various *ARP WaitReplyTimeout* values when using TCP.

forces **Base-A-1sec** to re-transmit broadcast ARP requests. Note that if the number of retries exceeds the limit and a node still fails to receive the address mapping information, the corresponding entry in the ARP table is marked as **dead** and this node, which is called as *inactive* node hereafter, is unable to send its data to the intended destination.

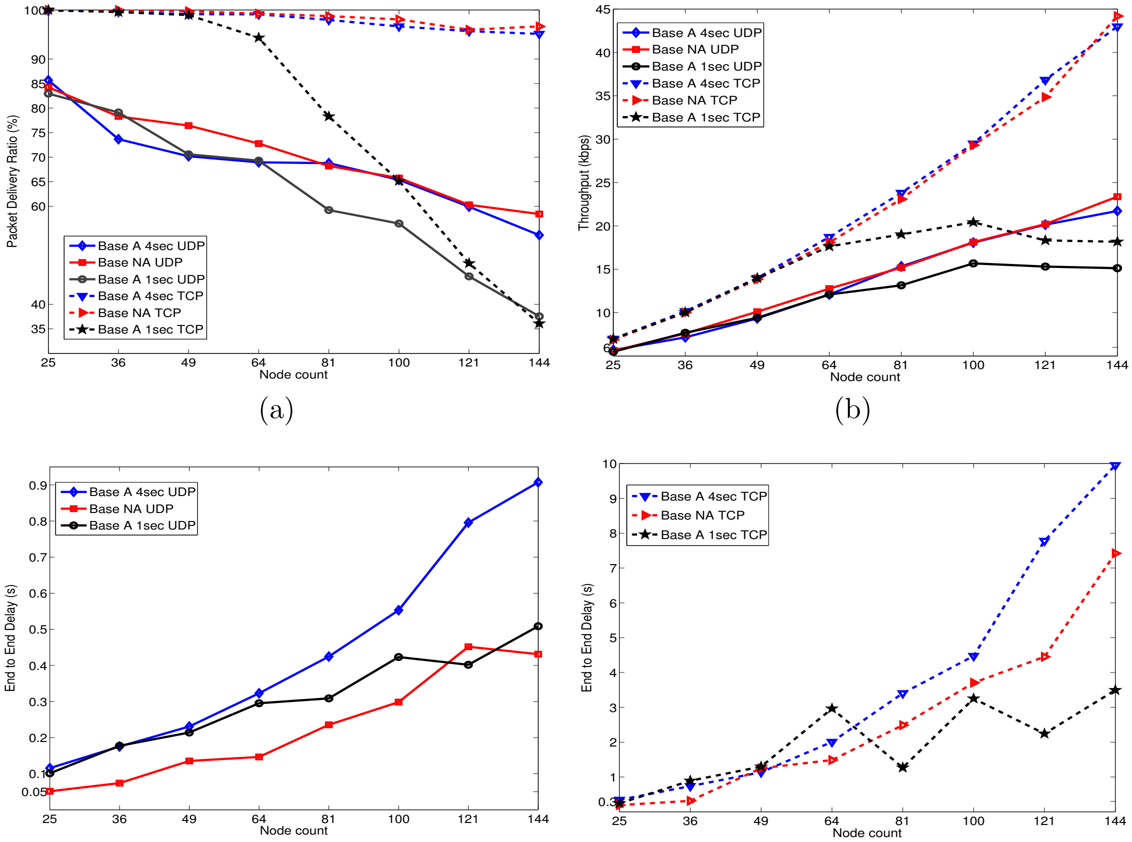
The number of broadcast ARP requests is different between UDP and TCP protocols due to the different characteristics of those protocols. This is attributed to the fact that in UDP ARP Requests are used for the purpose of sending data while in TCP they are used for connection establishment (i.e., SYN-SYN/ACK-ACK). Therefore, the gateway node is also involved and needs to send ARP requests to talk to the SMs. As a result, TCP is expected to produce more broadcast ARP requests than UDP.

Looking at Fig. 8.5 again, while the number of transmitted ARP requests for UDP is increasing as the network scales, this is not the case for TCP. For instance, the number of transmitted ARP requests for **Base-A-1sec** starts to drop after 64 nodes and becomes even less than that of **Base-A-4sec** after 121 nodes. This is an interesting outcome that may not be expected. I argue that this is due to the increasing number of *inactive* nodes in TCP as the network scales. Basically, the gateway becomes a bottleneck with too many SMs sending ARP requests at the same time and cannot reply to them to establish the TCP connection. To verify this argument, the number of *inactive* nodes for TCP is depicted in Fig. 8.6. Note that for these *inactive* nodes, TCP is unable to establish connection between those nodes and the gateway that eventually reduces the number of ARP broadcasts. In UDP, however, there is no *inactive* nodes and all the nodes are able to send their data to the gateway. The results in general indicate that increasing the *ARP WaitReplyTimeout* reduces the number of ARP requests for both protocols. It also reduces the number of inactive nodes for TCP.

8.3.3.2 Performance Assessment

Fig. 8.7 shows the impact of two different *ARP WaitReplyTimeout* values on the **Base-A** performance in terms of PDR, ETE Delay and throughput.

For PDR and throughput, **Base-A-4sec** is doing as good as **Base-NA** in both TCP and UDP which is promising (see Fig. 8.7a - 8.7b). The PDR and throughput for **Base-A-1sec** is much less especially for increased network size. For instance, starting from 64 nodes, in TCP, there is a dramatic decrease in PDR and throughput. This is mainly due to increased number of ARP broadcasts which create additional traffic and contention. In addition, this can also partially be attributed to the existing of inactive nodes as explained before. When inactive node count increases, an increased number of nodes cannot contribute to the data transmissions which in turn reduces the throughput. For **Base-A-4sec**, the effect of ARP broadcasts is minimized and thus more data can be transmitted successfully to the gateway node. Note that PDR and throughput for UDP is much less compared to TCP because of the nature of TCP (i.e., retransmissions).



(a)

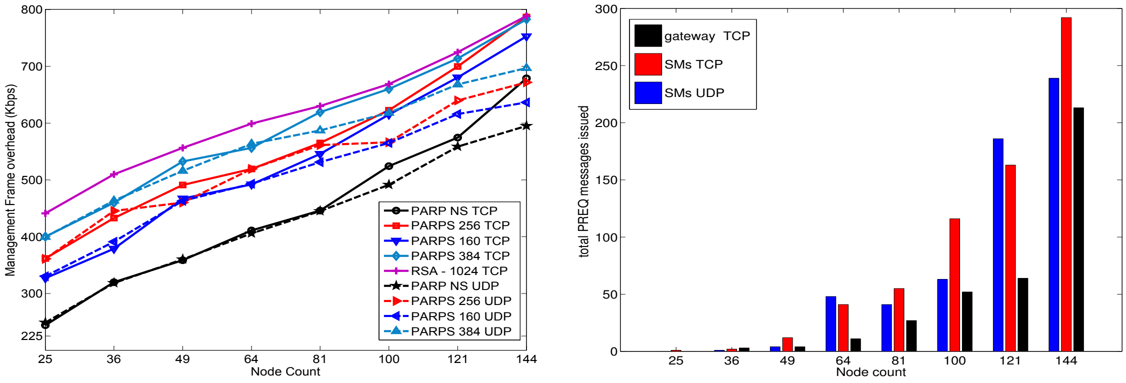
(b)

(c)

(d)

Figure 8.7: Comparison for different *ARP WaitReplyTimeOut* under different SM count a) PDR, b) Throughput, c) ETE delay for UDP, d) ETE delay for TCP

Considering the ETE delay, there are a number of observations (see Fig. 8.7c - 8.7d). First of all, ETE for UDP is much less compared to TCP because of the lack of retransmissions and connection establishment phase. Second, in all cases, **Base-NA** has the least ETE delay due to lack of ARP broadcasts. The ETE delay for **Base-A-4sec** is higher than that of **Base-NA** because of the contention introduced by ARP broadcasts especially when the network scales. While **Base-A-1sec** ETE delay seems a bit reduced for increased node count (e.g., after 64 nodes), this result is not reflecting the actual situation. When looking at PDR and throughput, **Base-A-1sec** should not be used after 64 nodes due to significant drop in PDR and



(a) (b)

Figure 8.8: Overhead evaluations for PARP-NS and PARP-S based on: a) key size b) on demand PREQ

throughput (i.e., because of *inactive* nodes). The decrease in ETE delay can be explained as follows: For UDP, due to large number of ARPs, the number of data packets from further nodes (with respect to the gateway) decreases significantly. This reduces the overall ETE delay since mostly closer nodes to the gateway will be able to send their data. For TCP, due to the existing of too many *inactive* nodes, the number of contending nodes for accessing the medium decreases which eventually reduces the ETE delays. Note that for **Base-A-4sec**, all the nodes are able to send data to the gateway when the network size is up to 121 while only one *inactive* node when network size was 144. Hence, there is still a lot of contention among all the nodes in the network which increases medium access and queuing delay.

Looking at the overall results, the *ARP WaitReplyTimeout* of 4secs were used for the rest of the experiments since it provided better reliability in terms of PDR and throughput.

8.3.4 PARP Evaluations

The proposed piggyback approaches, **PARP-NS** and **PARP-S**, were evaluated for UDP and TCP protocols in this subsection.

8.3.4.1 Overhead Evaluations

As previously discussed, piggybacking ARP information in proactive PREQ and PREP packets adds additional overhead to the management frames. This extra overhead comes from the addition of fixed-size address mapping field and variable-size signature field. While the fixed-size address mapping field is used in **PARP-NS**, **PARP-S** has both overheads. In addition, there is an additional cryptographic computation time at each node for signing and verification of the content of the signature field when the security protection is employed.

Two experiments to measure these overheads and observe their impact on the performance were conducted. First, the signature field overhead was investigated and the total overhead (of all packets) for each node count was reported. This overhead was investigated by considering three different key-sizes in ECC: 160 bits, 256 bits, and 384 bits. These keys created the signature size of 42 bytes, 64 bytes, and 96 bytes respectively. As depicted in Fig. 8.8a, **PARP-NS** has the lowest overhead as expected, while the overhead in **PARP-S** increases as the key size increases, either for UDP or TCP. The overhead of RSA 1024 bit key is also used as the comparison and it shows that the overhead of RSA is the highest.

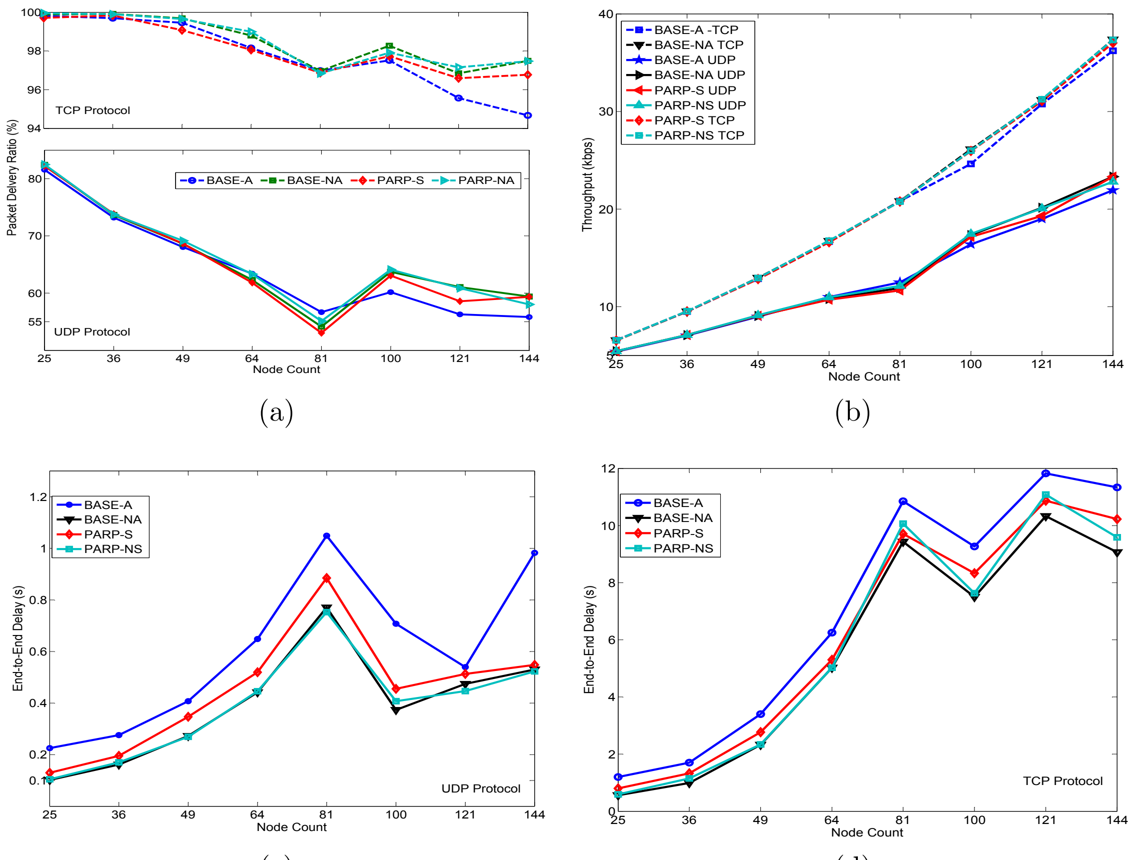
The results also show that TCP overhead is more than UDP especially when the node count increases beyond 81. This indicates that TCP uses more management frames than UDP. This can be explained as follows: Since both UDP and TCP operate on the same environment and hence the amount of proactive PREQ and PREP packets they sent are similar, the higher overhead in TCP comes from PERR and/or additional PREQ packets. As mentioned before, HWMP has two modes of operations: proactive mode and reactive mode. Even though proactive mode is used, when a sender cannot find a route to a destination, reactive mode will kick in and start broadcasting PREQ packets to find a route. To verify this observation, the number of PREQ packets from all nodes was measured. Fig. 8.8b shows the total on demand PREQs issued for **PARP NS** in UDP and TCP protocols. Note that the gateway does not need to send any information when UDP protocol is used and thus there is no on demand PREQs. On the other hand, the gateway needs to send an acknowledgment for every packet received when TCP is employed. A higher number of on demand PREQ packets from the gateway indicates that the gateway needs to delay the acknowledgments to some senders until the routes to these senders are found. The delay for the acknowledgment may trigger packet retransmission from a sender if it causes the retransmission timeout to expire for that packet. Hence, the number of PREQ packets will increase for TCP. The similar situation also arises for SMs. Some SMs need to buffer their data packet to the gateway and wait for the reactive mode to find the route to destination.

For the rest of the experiments, the results from 256 bits key size are presented since this key size has the security equivalent to 3072 bits RSA [110].

8.3.4.2 PARP-NS and PARP-S vs Others

Several experiments were conducted to assess the performance of **PARP-NS** and **PARP-S** compared to **Base-A** and **Base-NA**. The experiment results show that the performance of the proposed approaches is similar to that of **Base-NA** for all tested scenarios (UDP and TCP protocols) as depicted in Fig. 8.9.

In particular, the results indicate that **PARP-NS** and **PARP-S** match the performance of **Base-A** and **Base-NA** in terms of PDR and throughput for both UDP and TCP. However, the main advantage of the proposed approaches is that they significantly reduce the ETE delay compared to the existing solution, namely **Base-A**. The reduction becomes more dramatic when the network scales. For UDP,



(a)

(b)

(c)

(d)

Figure 8.9: PARP-NS and PARP-S using UDP and TCP protocols a) PDR (UDP and TCP) b) Throughput (UDP and TCP) c) ETE delay (UDP) d) ETE delay (TCP)

the improvement almost doubles while TCP improvement becomes more obvious with increased network size. Obviously, this is due to decrease of ARP requests which reduces contention for the nodes to access the channel. The results also show that **PARP-NS** and **PARP-S** perform even as good as **Base-NA**, which are the best that can be achieved. There are a number of other observations that can be made out of these results. First of all, TCP always performs better than UDP in terms of PDR. This is due to the reliable data delivery operation of TCP. Second, the throughput for all approaches does not change since the total bits received

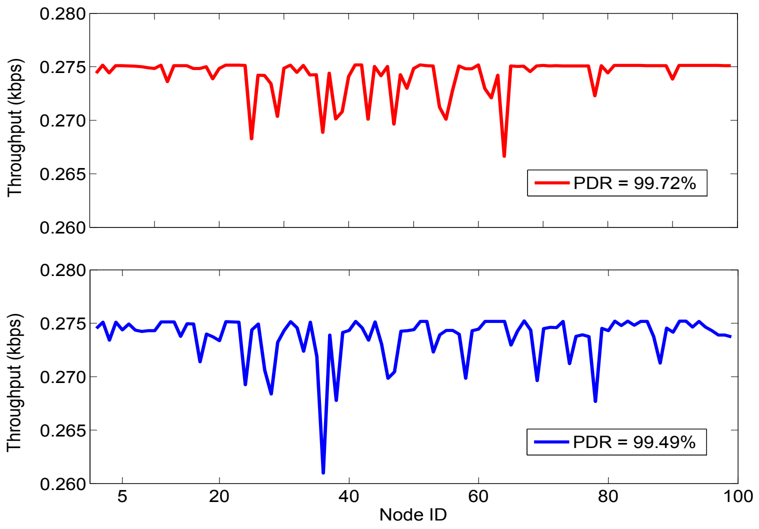


Figure 8.10: Per-node throughput for 100 nodes topology

at the gateway is measured. However, the throughput of TCP is much higher than UDP even though the application layer of both protocols generates the same amount of data. This is because of higher number of packets received at the gateway with the reliability service provided by TCP through error control. In addition, some packets may arrive more than once due to being sent by the senders when their retransmission timers timeout. In terms of fairness, Fig. 8.10 shows per-node throughput for two sample of 100 nodes topology. It shows that all nodes are able to send to the gateway and the fluctuation is typically due to the variation of the link quality between nodes.

Comparing **PARP-NS** and **PARP-NS**, the results depicted in Fig. 8.9 indicate that the overhead of signing and verification the signature is almost negligible. As far as the PDR is concerned, **PARP-S** almost matches the performance of **PARP-NS** especially for TCP. In case of UDP, the PDR is slightly less due to slight increases in the ETE delay that causes some of the packets to be retransmitted and eventually dropped. The throughput for both approaches is almost identical in all cases.

The ETE delays are also very similar in particular for TCP. Some fluctuations in TCP ETE delay of **PARP-NS** can be attributed to the retransmission timeout problem in TCP. More specifically, each time TCP sends a packet, a retransmission timeout is set for the packet. When an acknowledgment is received from the destination before the timeout expires, the timeout is canceled. However, if the sender does not receive an acknowledgment until the retransmission timeout expires, the sender retransmits the data and the transmission timeout value is increased by a certain amount. When this retransmission timeout value exceeds the next packet transmission schedule, this next packet will be buffered until successful delivery of the current packet (at the transport layer). Even if only a few SMs experience this problem, they eventually significantly affect the average delay of all tested SMs. I speculate that this is the case that occurs for some of the specific SMs in **PARP-NS** which overall increases the average ETE at some specific node counts.

Overall, it can be concluded that **PARP-S** is a secure and efficient approach whose performance is as good as **PARP-NS** and significantly outperforms **Base-A**.

8.4 Summary

IEEE 802.11s-based AMI network is prone to ARP broadcast storm problem that may cause significant impact on the performance of AMI applications. In this study, a mechanism to tackle this broadcast storm problem by piggybacking the MAC address resolution in the proactive PREQ message of HWMP was proposed. The proposed mechanism causes several changes to HWMP and the packet format of IEEE 802.11s. Piggybacking the MAC address resolution in proactive PREQ however, poses security threats such as ARP cache poisoning attack. To address this security issue, an authentication mechanism based on ECDSA was proposed.

An extensive simulation study to investigate the performance improvement as well as the optimal parameters for ARP in IEEE 802.11s-based AMI network was conducted. Specifically, by adjusting the *ARP WaitReplyTimeOut* parameter, the destination unreachable problem due to smaller *ARP WaitReplyTimeout* values can be alleviated. By using these parameters, the performance of the proposed approach with and without authentication components was evaluated. The simulation results indicated that the proposed piggybacking idea significantly decreases the ETE delay while maintaining the same PDR and throughput, these results are crucial in reliable data collection for large-scale AMI applications. The secure version, namely *PARP-S* introduced only a slight overhead in terms of ETE delay and thus can be considered as a feasible mechanism to be employed for SG AMI applications.

CHAPTER 9

Addressing Network Interoperability in Hybrid AMI Network

In this chapter, to ensure two-way traffic flow in the hybrid AMI network, two network interoperability issues due to different network characteristics in each network tier are identified. For the first issue, a proposed cross-layer privacy preserving solution and a layered non-privacy solution are discussed. A modification to IEEE 802.11e standard is proposed to address the second issue.

9.1 Problem Motivation and Definition

The problem motivation and definition can be separated into two parts based on two network interoperability issues in hybrid AMI network. The first part is related to the extension of the end terminal of LTE network as the gateway to IEEE 802.11s-based AMI network, while the second part is related to the number of QoS classes in each network tier as detailed next.

9.1.1 Ensuring Two-way Traffic Flow in Hybrid AMI Network

When a hybrid AMI network is deployed, to ensure two-way flow of traffic between network tier, each network tier requires a gateway to the other network. In this study, a gateway that has dual interfaces, one interface for IEEE 802.11s network and the other interface for LTE network are proposed. While MPP has been defined as the gateway to the other network in IEEE 802.11s, gateways in LTE network are defined in the Evolved Packet Core (EPC) access network (e.g., P-GW and S-GW). In this study, since these gateways, in particular P-GW is used as the gateway to the Internet which connects the LTE network to utility company, user equipment which basically the end terminal of LTE network, is proposed to be the gateway for IEEE 802.11s by extending its functionality.

One critical design decision in hybrid AMI network is related to IP addressing of each network tier. Different network ownership (e.g., when public LTE network is chosen for WAN while NANs are private networks owned by a utility company), may cause IEEE 802.11s-based AMI network and LTE network to be in a different IP subnetwork. Moreover, even if they are in the same IP subnetwork, the interoperability issue related to downlink traffic intended to any SM in the IEEE 802.11s-based AMI network still persists. This is because in LTE network, unidirectional General Packet Radio Service (GPRS) tunneling protocol (GTP) is used between a base station (i.e., eNB) and P-GW for packet delivery as depicted in Fig. 9.1. For each packet delivery direction (e.g., uplink or downlink), each UE has its own GTP tunnel and this tunnel is uniquely identified using a tunnel endpoint ID (TEID). When the destination IP in the IP packet is unknown (e.g., the IP of a SM in IEEE 802.11s-based AMI network), P-GW will drop the IP packet since it cannot find the corresponding TEID for this IP packet.

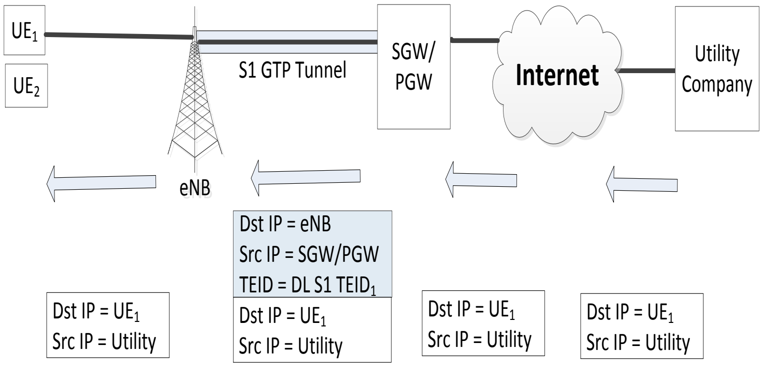


Figure 9.1: GTP Tunnel used between eNB and S-GW/P-GW.

9.1.2 QoS Classes Mismatch in Hybrid AMI Network

Another interoperability issue is related to the number of QoS classes in each network tier. IEEE 802.11s has fewer QoS classes than LTE. The four QoS classes in IEEE

802.11s may not be adequate since there are a wide variety of activities that can be performed by using SMs, such as [111]: (1) remote meter reading, (2) remote service switching, (3) tamper detection and notification, (4) outage detection and notification, and (5) voltage and power quality (PQ) monitoring. Besides periodic and emergency traffic initiated by SMs, periodic and on-demand traffic initiated by utility company that can be bidirectional may pass through this hybrid network. For instances, power price information are sent periodically to SMs for automated DR application. An action command to turn on/off SM remotely is sent by utility company for DR or service switching to assist firefighters when there is an emergency situation in the consumer side (e.g., fire). Utility company can send a query to SM(s) for on-demand meter reading to address billing or other consumer issues, outage restoration verification, or on-demand voltage and PQ information. Finally, there is the traffic associated with network management and security/privacy. For instance, IEEE 802.11s broadcasts periodic beacons to form and maintain mesh peering between the nodes, use routing messages, etc. All of these traffic types may have different QoS requirements. For the reliable, high performance, and secure SG communications network, it is very important to meet these QoS requirements, in particular to the stringent delay and priority requirements of mission critical control SG applications as well as grid measurement and monitoring applications [112]. However, since the available QoS AC classes in IEEE 802.11s are limited to four (lowest to highest) : background (AC-BK), best effort (AC-BE), video (AC-VI), and voice (AC-VO), typically some of those traffic classes are mapped to the same QoS class [113]. This may eventually affect the performance compared to the case when the traffic types are in different classes.

To show the impact of serving heterogeneous traffic in the same class and different classes in IEEE 802.11s, a preliminary experiment was performed in a controlled grid

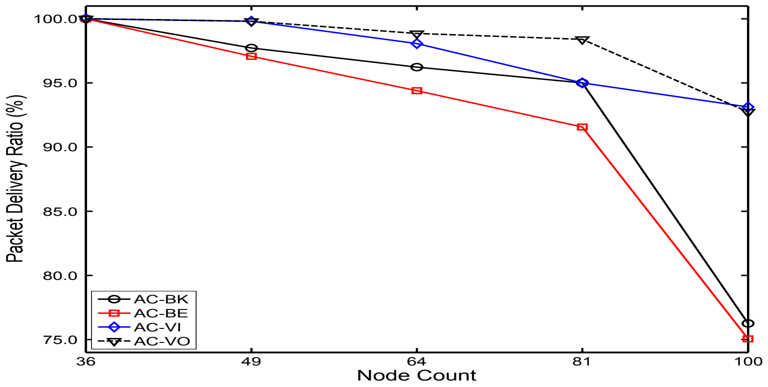


Figure 9.2: PDRs of SG traffic when the management frames are using separate QoS classes than Best Effort (merged case).

topology where each mesh node can have utmost four directly connected neighbor nodes in the vertical and horizontal direction. The packet delivery ratio (PDR) of heavy SG traffic that was assigned to the best effort class (AC-BE), was measured for varying QoS classes for IEEE 802.11s management frames (i.e., mesh management frames for peering and routing). As shown in Fig. 9.2, the worst PDR is when both SG traffic and management frame are using AC-BE (joint usage). However, when the management frame traffic is assigned to different QoS class while SG traffic remains in AC-BE, the PDR improves even though management frame traffic is assigned to AC-BK (the lowest priority QoS class). Moreover, as the node count increases, it is observed that the most significant PDR improvement is achieved when management frame traffic is assigned to AC-VO.

This can be explained as follows: Besides the shortest backoff value in AC-VO, management frame traffic does not have to compete with SG traffic since they are using different ACs. On the other hand, when management frame and SG traffic are in the same AC, they must compete in First In First Out (FIFO) basis. As a result, when there is a path selection issue (e.g., when a path error occurs), IEEE 802.11s may not be able to provide a quick response since the management frame may need to be in-line in the queue. Similar situation exists when management frame is assigned to AC-BK. Even though the management frame does not need to compete with other traffic in AC-BK, since the priority is lower than SG traffic when both ACs have the same backoff value (i.e., virtual collision between ACs), SG traffic that has higher priority than the management frame traffic will be given access to the medium. This result indicates that giving higher priority QoS class exclusively to certain traffic (e.g., management frame traffic) can improve the network performance. However, when there are more than four traffic classes then some of them need to be merged in IEEE 802.11s even though LTE can handle such classes.

Therefore, in this study, the goals are twofold: to ensure two-way flow of QoS traffic in hybrid AMI network while providing a flexible QoS mapping between tiers and to devise a new IEEE 802.11s architecture that expands the existing QoS classes to accommodate a wide variety of SG QoS traffic and IEE 802.11s operations.

9.2 Proposed Approaches for Two-way Traffic Flow

Two different approaches are pursued to ensure the two-way traffic flow in hybrid AMI network. The first approach is motivated by the need of user privacy protection since the appliance-level information can be derived from the fine-grained meter readings by means of non-intrusive load monitoring (NILM) applications [114]. The consumer behavior can then be deduced based on this appliance-level information. This approach is cross-layer approach between application and network layer. It does not need any modification to the LTE network while the second approach is a non-privacy layered protocol approach at the network layer of the EPC network (i.e., LTE modification).

9.2.1 Privacy-preserving Gateway Address Translation

Employing the Network Address Translation (NAT) [115] at the gateway does not solve the problem since the GPRS tunneling is attached to a UE (i.e., mapping between UE IP address and downlink Tunnel ID (TEID)). NAT cannot map multiple SM's IP address into a single IP address and still be able to identify each unique SM. A special case of NAT called Network Address Port Translation (NAPT) or commonly known as Port Address Translation (PAT) can be used since PAT allows all IP addresses in an IEEE 802.11s AMI network to be mapped into a single IP address (i.e., the UE IP address) and a unique source port number. However this can be used only when the downlink traffic to SMs are direct response to unlink traffic from SMs (e.g., ACK). This will not work when utility company is the initiator of the downlink traffic.

Therefore, pseudonyms are proposed as the unique consumer identity embedded in SMs. This pseudonym is used each time an SM sends data such as meter reading, outage notification, or power quality to utility company. All SMs must register their pseudonyms and IP addresses to the trusted gateway first so that the gateway address translation approach will be able to map the SM's IP address to the UE's IP address. This approach consists of two processes, the registration process and the address translation process as detailed next.

9.2.1.1 IP Address Registration

In the IP address registration process, a SM registers its pseudonym and IP address to the trusted gateway by sending a small registration packet that consists of SM's pseudonym and its IP address. The registration is performed after an SM joins the IEEE 802.11s-based AMI network through a successful peering mechanism with other SMs. A secure peering by means of Authenticated Mesh Peering Exchange (AMPE) is assumed. The required shared Pairwise Master Key (PMK) for AMPE is derived from Simultaneous Authentication of Equals (SAE) [59], one of the authentication methods that has been adopted in IEEE 802.11s standard. It does not need an authentication server and uses a shared password and a set of Elliptic Curve Cryptography (ECC) domain parameters to do authentication and key agreement. As the name implies, each side in the exchange is able to initiate the protocol, and does not have to be direct neighbors. The initiator is the one that discovers its neighbor(s) first.

The proposed approach exploits the presence of ECC domain parameter in IEEE 802.11s to ensure that the registration packet comes from a legitimate SM and its integrity is maintained. To this end, a digital signature is added to the packet and Elliptic Curve Digital Signature Algorithm (ECDSA) [77] is used to create and verify the signature. A sender SM uses its private key to generate the signature and the gateway verifies this signature using the SM public key. These keys are obtained from the ECC domain parameters that have been provided in the mesh network for SAE. When the registration packet passes the authentication verification, the gateway will store the pseudonym and the IP address in its mapping table for address translation operations.

9.2.1.2 Gateway Address Translation

The gateway address translation operations are depicted in Fig. 9.3. An SM sends their data to the utility company through the trusted gateway. When the gateway receives a packet from the IEEE 802.11s-based AMI network, instead of using the original source IP address of the sender, the UE gateway IP address is used to replace the source IP address of the sender before the packet is forwarded through

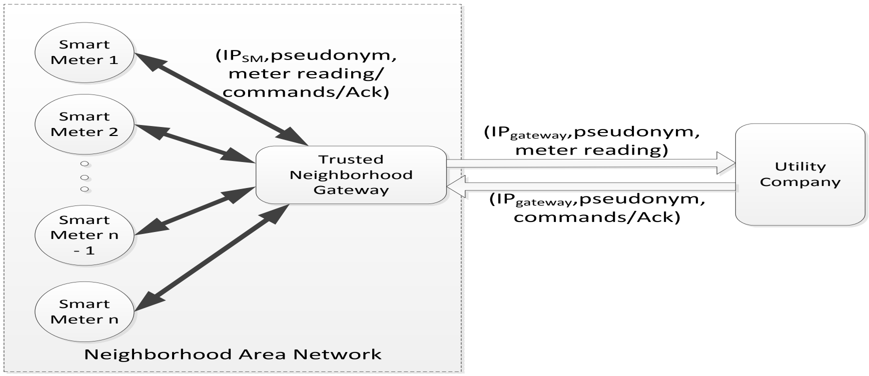

Smart Meter 1
Smart Meter 2
Smart Meter n - 1
Smart Meter n
(IP_SM,pseudonym, meter reading/ commands/Ack)
Trusted Neighborhood Gateway
(IP_gateway,pseudonym, meter reading)
(IP_gateway,pseudonym, commands/Ack)
Utility Company
Neighborhood Area Network

Figure 9.3: The gateway address translation mechanism

the LTE network to the utility company. In this way, the original source IP address is hidden from utility company. Utility company cannot relate the consumer ID to the sender IP address since this source IP address is belong to the gateway IP address.

When the received packet requires a response from utility company, such as an acknowledgment for TCP packet, utility company will send it to the trusted gateway through the LTE network. The P-GW will be able to identify the destination IP address (i.e., UE's IP address) and employs the appropriate bearer to the destination UE. When the gateway corresponding to this UE receives the packet, it will check its mapping table to find the intended SM IP address based on the pseudonym information in the packet. Note that whenever the gateway changes the source IP address of the in-transit packets, the TCP/UDP and IP checksums of the packet also need to be recalculated using the new source IP address since the old checksums are calculated based on the old source IP address. Typically the destination receiver will validate the integrity of the received packets by calculating the checksums of the received packet.

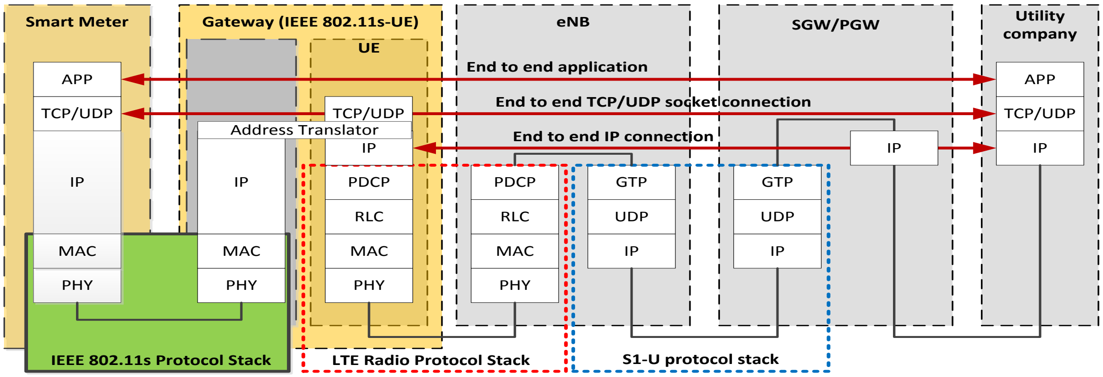
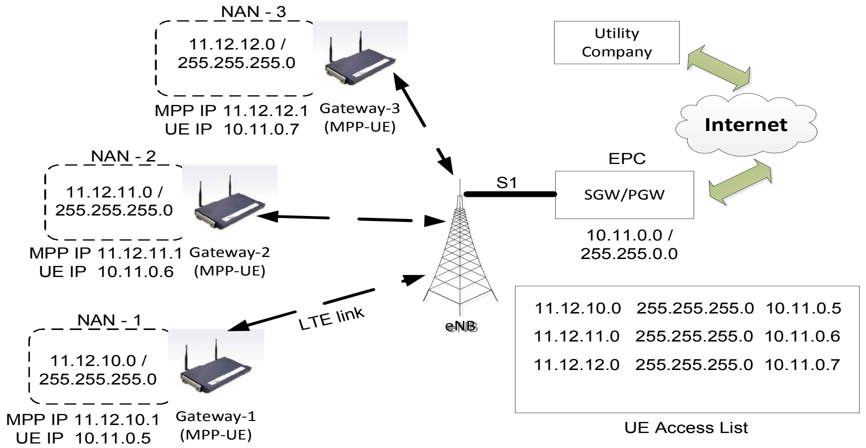


Figure 9.4: SG user plane communications network from smart meter to utility company. The S-GW and P-GW are implemented in a single physical node

Fig. 9.4 shows that end-to-end IP connection from utility company and the UE is still maintained as in the default LTE network operations, while the end-to-end transport and application layers connections from utility company and SMs can be enabled by the gateway address translation mechanism.

9.2.2 UE Access List mechanism

In this section, a UE access list is proposed for two-way flow traffic in the hybrid AMI network. This list consists of network base address and subnet mask of IEEE 802.11s-based AMI network and its corresponding UE gateway IP address that serves this IEEE 802.11s-based AMI network. Fig. 9.5 illustrates an example of the content of a UE access list. Instead of discarding a downlink IP packet when the destination IP address is unknown, in our approach P-GW will check in its UE access list to see whether this unknown IP address is associated to one of IEEE 802.11s-based AMI networks. Since there will be thousands of UEs that act as gateways to IEEE 802.11s-based AMI networks, a sorted list is used and binary search [95] based on the packet destination IP address to find the corresponding UE



11.12.10.0	255.255.255.0	10.11.0.5
11.12.11.0	255.255.255.0	10.11.0.6
11.12.12.0	255.255.255.0	10.11.0.7

Figure 9.5: An example of UE access list content for three IEEE 802.11s NANs. Each NAN is assumed to have a maximum of 254 SMs. When downlink traffic to 11.12.11.11 is received for instance, P-GW will check this list. The IP address is in the list (i.e., base network 11.12.11.0), P-GW will know the associated UE IP address (i.e., 10.11.0.6).

gateway is employed. The average and worst case time complexity of this searching algorithm is O(log N).

When an IP address is associated to an IEEE 802.11s-based AMI network, the appropriate UE IP address can be retrieved from the UE access list. This UE IP address is then used to find the corresponding TEID. This process is shown in Alg. 8. Note that eNB has the mapping between TeID and an RBID (Radio Bearer ID) which will be used to deliver the IP packet from eNB to a UE that acts as the gateway to an IEEE 802.11s-based AMI network. At the UE, the appropriate QoS class for this traffic in the an IEEE 802.11s-based AMI network can be assigned based on the information in the QoS mapping list as explained next.

9.3 QoS mapping and extension

A QoS mapping list at the gateway of hybrid AMI network is proposed to map downlink QoS traffic from the LTE network to its corresponding QoS class in IEEE

Algorithm 8 Received From Outside Network

```
for every downlink IP packet received at P-GW do
    ipAddr ← destination IP address of the packet;
    succeeded ← VerifyIfIpAddressInLteNetwork(ipAddr);
    if (not succeeded) then
        ipUe ← BinarySearchInUeAccessList(ipAddr);
        if (ipUe == nil) then
            Discard the packet;
            Return;
        end if
        ipAddr = ipUe;
    end if
    enBAddr ← FindEnBAddress(ipAddr);
    teID ← FindBearerInformation(ipAddr);
    SendPacketToEnB(packet, enBAddr, teID);
end for
```

802.11s. Each time the gateway receives downlink traffic, it consults this list to determine what would be the appropriate QoS class for the received traffic. This mapping list consists of a pair of QCIs of LTE network and its corresponding QoS class in IEEE 802.11s.

A sequential search is adequate for this list since utmost only nine QoS classes are available. The worst case time complexity of this algorithm is O(N). When the gateway receives downlink traffic from the LTE network, based on from which bearer this traffic is coming from, the gateway will find the corresponding QoS identifier for IEEE 802.11s in the QoS mapping list. Note that the QoS mapping list is only used for the downlink traffic. For the uplink traffic from SM(s), the ordinary packet filtering at the UE that uses Traffic Flow Templates (TFTs) is used to assign the uplink traffic to an appropriate bearer.

To address the mismatch, QoS classes in IEEE 802.11s are extended by employing dual queues (DQs) called non-priority and priority queues for each AC instead of a single queue as defined in IEEE 802.11e standard. The DQs within the same AC have the same EDCA parameters as depicted in Fig. 9.6. In this way, eight QoS classes are available in IEEE 802.11s. When an AC has the right to access

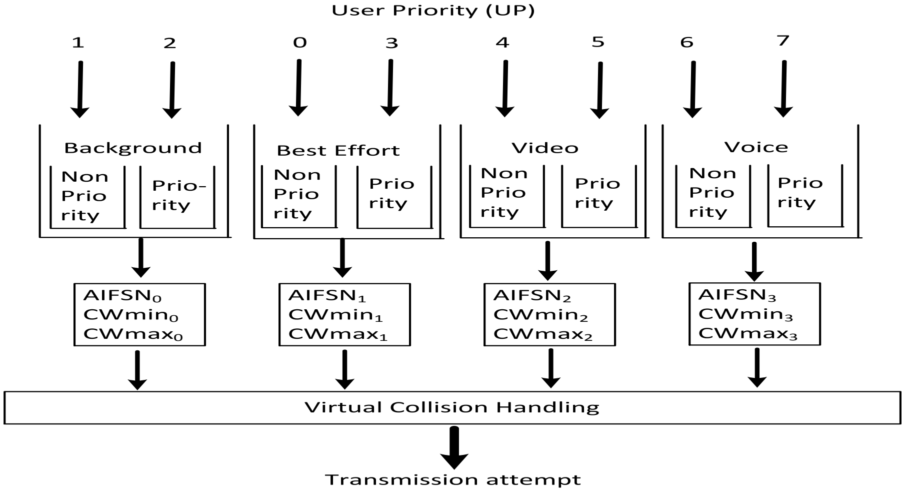


Figure 9.6: Proposed EDCA modification with dual queues.

the medium, the priority queue in this AC will be checked first. When it is not empty, the packet from this queue is granted to access the medium. Otherwise, the non-priority queue is given the access to the medium.

9.4 Performance Evaluation

Performance evaluations were conducted separately for Gateway Address Translation and UE access list. While the goal for gateway translation was to access the overhead of pseudonyms processing and gateway translation operations at the gateway which is the critical point to ensure two-way traffic flow between tier, for UE access list the evaluation was combined with QoS mapping list and extension to ensure two-way heterogeneous QoS traffic flow between tier.

The following parameters were used in both evaluations: the transmission range for each SM was assumed to be 120m. The underlying MAC protocol was assumed to be IEEE 802.11g. The distance from the gateway of the hybrid AMI network to the base station of the LTE network was 3000m. Simultaneous data report scheduling was used, an SM generated uplink TCP data traffic every 15secs, the packet size was 512 bytes, and the simulation time was 500secs.

9.4.1 Gateway Address Translation Evaluation

9.4.1.1 Experiment Setup

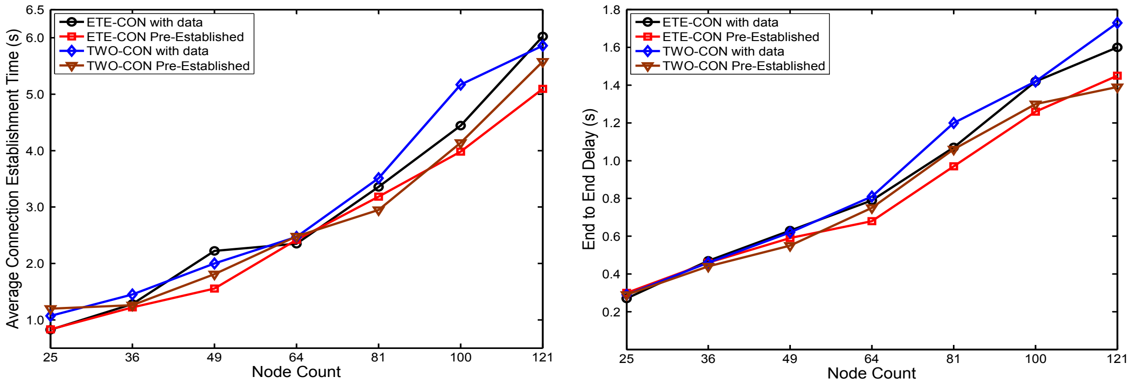
An **N** by **N** grid topology was used in the experiment, $\mathbf{N} \in$ [5,6,7,8,9,10,11]. The distance between SMs was 100m. The last mesh node ID (i.e., mesh node ID (N^2-1)) was used as the gateway of the hybrid AMI network.

Besides ETE delay and PDR metrics, *connection establishment time* metric was used for performance assessment. This metric indicates how long it takes to establish an end-to-end connection between a SM and utility company through the hybrid AMI network.

9.4.1.2 Performance Evaluation Results

The gateway address translation that enables end-to-end TCP connection was compared with a baseline where TCP connection establishment was performed in two steps. First, SMs performed connection establishment to the mesh root (i.e., the gateway), and then the second TCP connection was established between the gateway and utility company. In the figures, end-to-end- TCP connection was labeled as ETE-CON while the baseline was labeled as TWO-CON.

In the experiments, two different scenarios were used. In the first scenario, the TCP connection was established on *a need-basis.* In the second scenario, TCP connection was *pre-established* so that when an SM wanted to send its reading, the TCP connection will already be active. These scenarios were shown as *with data* and *pre-established* labels in the figures.



(a) (b)

Figure 9.7: Performance under different meter count: a) Average connection establishment time b) ETE delay.

The connection establishment in the *pre-established* TCP connection scenario provides slightly better performance than that of TCP which is used on *a need basis* as depicted in Fig. 9.7a. This is because in the *pre-established* scenario, the TCP handshaking mechanism for establishing the TCP connection is performed when there is not many data traffic in the network. In the need-basis scenario on the other hand, the handshaking mechanism is also competing with the transmission of the meter readings from SMs that have successfully established the TCP connection to utility company. However, for AMI scenario, a need-basis can still be applicable despite the slight performance degradation in order to keep the network idle when there are no data communications.

Note that TWO-CON approach reduces the number of connection establishment from the gateway to utility company. In the TWO-CON approach, each SM establishes a TCP connection to the gateway and thus multiple TCP connections are established while the gateway only requires a single TCP connection to utility company. Furthermore, the TCP connection establishment from the gateway to utility company can also be performed independently from the TCP connection establishment from SMs to the gateway when the pre-established scenario is chosen. When ETE-CON approach is employed on the other hand, there will be many handshaking packets for TCP connection establishment passing through the LTE network from SMs to utility company. Hence these handshaking packets will take a longer route to utility company compare to TWO-CON approach. Given this situation, ECE-CON performance is promising to be use in AMI while preserving the privacy.

Fig. 9.7b. shows the ETE delay of our ETE-CON approach compare to the TWO-CON approach in both connection establishment scenarios. The results indicate that the ETE-CON approach produces similar result compared to TWO-CON approach despite the overhead of pseudonym processing and the gateway address translation operations. While both approaches have a similar performance in term of the ETE delay, it is also important to check the PDR whether there are any packet losses at the gateway due to the address translation operations. For all approaches and node count, 100% PDR are achieved.

9.4.2 QoS Mapping and Extension Evaluation

9.4.2.1 Experiment Setup

A random realistic topology of N nodes, $N \in [36,49,64,81,100]$ was created. In the experiments, the results from 30 topologies for each N were collected and the average of these results were calculated. UE access list was used in this experiment as depicted in Fig. 9.8.

Table 9.1 shows the details of applications (OMS, GO and DR) that were used for performance evaluation. Since the goal was to assess the proposed approaches under heavy security traffic overhead, two encryption mechanisms were used in the simulation, AES-128 and Fully Homomorphic Encryption (FHE) [116]. The AES-128 was used for data traffic that do not need any in network processing such as

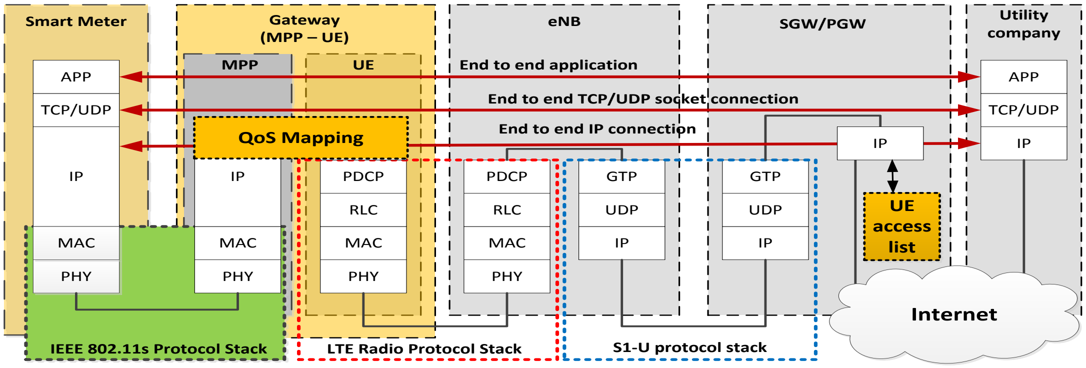


Figure 9.8: QoS Mapping List and UE Access List

OMS and DR while FHE was employed for SM data traffic privacy that may need in network processing while in-transit due to its large packet size. Note that: (1) FHE is a new technology that allows computation on encrypted data and thus is being considered for user privacy in AMI applications, (2) in addition to the downlink traffic from DR to SMs, by employing TCP protocol in all simulations, there is a downlink acknowledgment (ACK) to SM from utility company to acknowledge a received packet.

Table 9.1: SG Applications used for performance evaluation

SG Application	*Data size (bytes)*		*Data Sampling*	*Security*
	plaintext	*ciphertext*		
OMS (from SMs to OMS)	64	80	60secs	AES-128
Grid Operations (GO) (meter usage)	4	12,660	30secs	FHE
DR (commands to SMs)	4	16	on-demand	AES-128

In the experiments, four traffic allocation scenarios were compared as follows :

1. *Single AC-based.* GO, OMS, and IEEE 802.11s management frames were using AC-BE. In the graphs, the scenarios for GO and OMS were labeled as GO-Baseline and OMS-Baseline respectively.

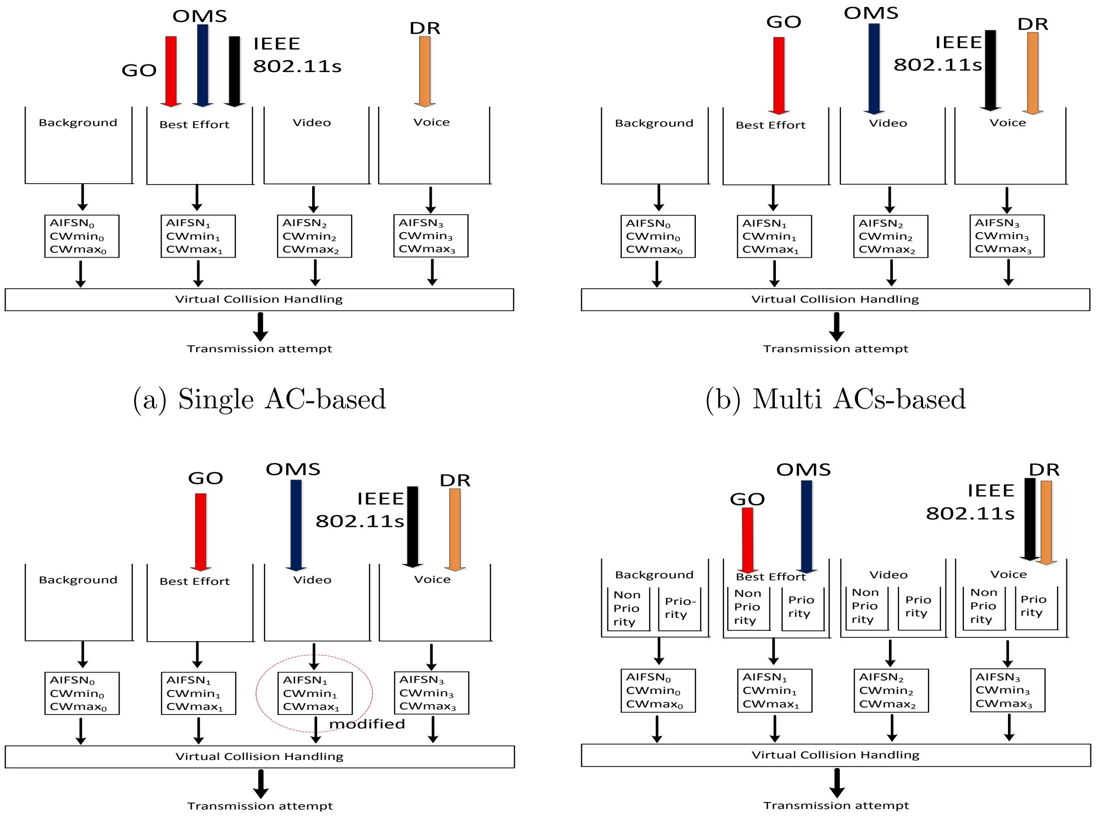
2. *Multi ACs-based.* IEEE 802.11s management frames were using AC-VO. GO was using AC-BE and

    (a) OMS was using AC-VI. In the graph, OMS traffic was labeled as OMS-VI and GO as GO-OMS-VI to indicate GO's performance in AC-BE when OMS was using AC-VI.

    (b) OMS was using AC-VI but with modified EDCA parameters. The EDCA parameters were set equal to that of AC-BE. Similarly, OMS and GO were labeled as OMS-VI-mod and GO-OMS-VI-mod.

3. *Dual Queues-based.* IEEE 802.11s management frames were using AC-VO. OMS was using AC-BE Priority Queue (PQ) and GO was using AC-BE Non Priority (NP) Queue. OMS and GO were labeled as OMS-DQ-BE-PQ and GO-DQ-BE-NP.

Fig. 9.9 illustrates all experiment scenarios. For all scenarios, the downlink on-demand DR randomly selected several SMs (e.g., 10% from SMs) and sent DR commands several time at random to these SMs. The DR downlink traffic was assigned to a dedicated bearer (e.g., QCI 9) in LTE network and mapped it to AC-VO of IEEE 802.11s network. While the uplink traffic (e.g., GO and OMS) were assigned to the default bearer for fair comparison. Note that the DR results were not showed for figures clarity due to small data size and random occurrence of the traffic. For GO and OMS traffic in all scenarios, periodic reporting in SG at the worst case scenario (i.e., simultaneous) was used. In this scenario all SMs sent their report at the same time schedule which may cause heavy contention in the network.


OMS
GO
IEEE 802.11s
DR
Background
Best Effort
Video
Voice
Non Prio rity
Prio- rity
AIFSN$_0$ CWmin$_0$ CWmax$_0$
AIFSN$_1$ CWmin$_1$ CWmax$_1$
AIFSN$_2$ CWmin$_2$ CWmax$_2$
AIFSN$_3$ CWmin$_3$ CWmax$_3$
modified
Virtual Collision Handling
Transmission attempt

(a) Single AC-based

(b) Multi ACs-based

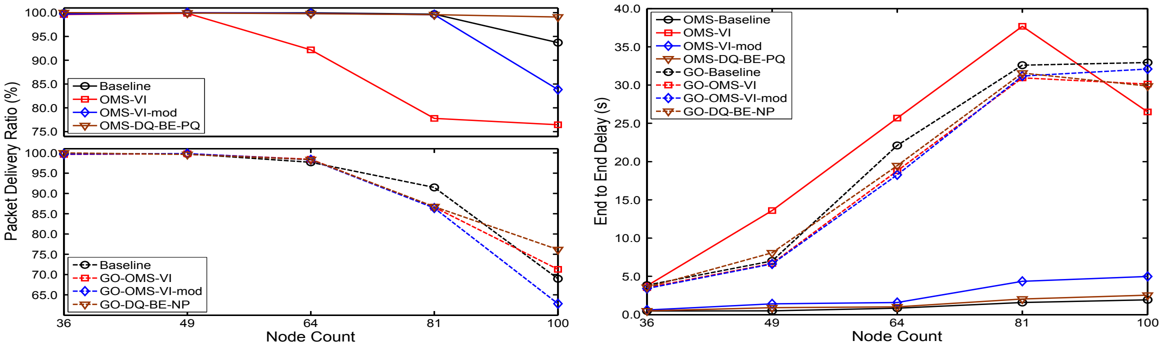
(c) Multi ACs-based with modified EDCA parameters

(d) Dual Queues-based

Figure 9.9: Four experiment scenarios for QoS mapping and extension evaluation

9.4.2.2 Performance Evaluation Results

Fig. 9.10 shows some interesting results. When compared the OMS-Baseline with OMS-AC-VI, the result is very surprising. By assigning to a higher priority AC, the expectation is we will get a higher PDR and a lower ETE delay for the OMS data traffic. On the contrary, the simulation results show that PDR drops and ETE delay rises as the node count increases. Even worst, the average ETE delay of OMS traffic is higher than that of GO traffic. This can be explained as follows: Within the same SM, OMS traffic that has a shorter backoff value than GO may have access to the



(a) (b)

Figure 9.10: Performance evaluation of different QoS Class assignments for priority traffic.

medium. However, due to the interference from other SMs that might transmit GO traffic, this SM is not able to transmit since the medium is not idle. As a result, OMS traffic may need to wait longer in order to access the medium and thus ETE delay increases as shown in Fig. 9.10. This indicates that the standard EDCA parameters for AC-VI are not suitable for heavy security overhead traffic.

Tuning the parameters might be an option to improve the performance in the above cases. Indeed, the simulation results for OMS-VI-mod confirm this. Both metrics of OMS-VI-mod are improved significantly when compared to OMS-VI, in particular the ETE delay reduces significantly. Moreover, these improvements do not have a significant impact on GO traffic. Both PDR and ETE delay of GO-OMS-VI-mod are similar to GO-OMS-VI until 81 nodes while the performance of GO-OMS-VI-mod drops afterward. However, further efforts are needed to fine-tune the parameters to improve the performance of the high priority traffic.

OMS-VI-mod approach is basically having two queues with the same parameters similar to the DQ approach. When the results are compared with OMS-DQ-BE-PQ results, both PDR and ETE delay metrics of OMS-DQ-BE-PQ are better than OMS-VI-mod approach. This is due to the fact that when both OMS and GO traffic are present, OMS traffic in DQ approach is guaranteed to have access to the medium first. This is not the case for OMS-VI-mod. Note that in OMS-VI-mod, even though both ACs have the same CW range, the actual CW value selected at a time in each AC may be different due to random CW selection. Moreover, the impact of DQ approach on GO traffic is minimal when compared to OMS-VI-mod. The PDR of GO traffic is even better in DQ approach than in OMS-VI-mod.

Comparing OMS-DQ-BE-PQ and OMS-Baseline, even though the ETE delay of OMS traffic is slightly higher when DQ approach is used, this comes from the increase in PDRs of the OMS traffic. Moreover, the impact on GO traffic is minimal than the baseline. The PDR and ETE delay of GO traffic for DQ approach are also outperforming the baseline.

As a result, the following can be concluded: Normally, multiple queues are expected to be better than single queue carrying all the traffic. However, when FHE is used, this prevents us achieving improved results with multiple queues. This is because FHE creates a lot of retransmissions which does not leave any space for neighboring SMs to access the medium even if their OMS has a higher priority class. With a single queue, the problem is similar in the sense that FHE traffic dominates the medium. However, with single queue, PDRs are worse which causes to slightly reduce the ETE delay. Thus, while DQs may offer flexibility in types of different QoS classes without any additional overhead, FHE overhead still needs be carefully addressed by focusing on both parameter tuning and packet size optimization.

9.5 Summary

In this chapter, two network interoperability issues in hybrid AMI network were presented. A privacy-aware gateway address translation was proposed to overcome the tunneling mechanism in the LTE network that prevents downlink traffic to be delivered to the appropriate gateway while preserving user privacy. This approach required no modification in the LTE network. It extended UE functionality with gateway address translation function that can change the source IP address of the uplink data with its IP address in order to hide the SM IP address for privacy purpose and to be able to employ the LTE features. At the downlink direction, the packet sent from utility company can be identified by P-GW and the appropriate tunnel id (TEID) can be assigned to this packet since the packet was destined to the UE. At the UE, the gateway address translation will find the IP address of the destination SM based on the consumer identity in the received packet. The implementation and evaluation of this privacy-aware approach for TCP protocol has shown that it was feasible and even slightly reduced the ETE and connection establishment delays.

A different approach was also proposed to overcome the tunneling issue. A novel UE access list mechanism was proposed to find the address mapping between the network address from an IEEE 802.11s AMI network and the corresponding gateway IP address (i.e., UE IP address) at the P-GW of EPC network. When the corresponding UE IP address was found, the downlink traffic can be processed as in the regular P-GW to eNB operations.

Another network interoperability issue related to QoS classes mismatch between tiers and how the QoS assignment between tier was handled at the IEEE 802.11s by proposing dual-queues (DQs) to extend the available QoS classes of EDCA from four QoS classes to eight QoS classes. A QoS mapping list was then used at the gateway to map QCIs from the LTE network to these new QoS classes to ensure end-to-end QoS within the hybrid network for the downlink traffic intended to SM(s) in the IEEE 802.11s-based AMI network. In this study, the proposed approaches were implemented and their performance was evaluated. The performance of DQs approach was compared with several traffic allocation strategies under heavy security/privacy overhead. The performance evaluation indicated that while DQs can provide flexibility in terms of increased QoS classes and improve performance, their benefits were not obvious when FHE-like security overhead exists.

CHAPTER 10

Concluding Remarks and Future work

AMI is one of the prominent SG applications that revolutionizes data collection activity at the distribution subsystem and enables new SG applications. Besides fine-grained meter reading, a variety of two-way flow data traffic can be collected through AMI communications network as well. The availability of huge amount of these fine-grained data in different venues: in the smart meter, at the AMI communications network while they in transit, and at utility company or other third parties; may pose security and privacy issues. Furthermore, due to the importance of these fine-grained AMI data for some SG applications, a reliable AMI communications network is also paramount importance. This communications network must be able to accommodate traffic with different priority and Quality of Service (QOS) requirements. Given that there are a variety of options for the communication technologies for AMI communications network, in this study a hybrid AMI network that consists of IEEE 802.11s-based Neighborhood Area Network and LTE cellular network as the Wide Area Network was investigated.

This study revisited every layer of TCP/IP protocol stack. The protocol operations that can degrade the protocol performance when they are used in this hybrid AMI network, in particular in IEEE 802.11s-based AMI network were identified; and novel or improve TCP/IP protocol approaches were proposed to meet the SG requirements in terms of security, privacy, and reliability. In Chapter 4, the security and privacy issues due to AMI data explosion and the availability of these AMI data in different venues were first investigated. The study surveyed some well known homomorphic cryptosystems and assessed their main features, in particular their functionality, security, and performance. The assessment showed that among other homomorphic cryptosystems, Paillier cryptosystems is the best candidate since it has the lowest message expansion factor and reasonable computation overheads. Two privacy-preserving data aggregation approaches that based on Paillier, which are called as End-to-end Homomorphic Encryption and Hop-by-hop aggregation, were evaluated through extensive simulations and compared with the non-secure hop-by-hop concatenation data aggregation approach. Different aspects of network topology and key size were thoroughly investigated for these approaches.

This study however, is limited to partially homomorphic encryption (PHE) that only able to perform addition or multiplication operations. In recent years, a new type of homomorphic encryption that enables to perform both operations on a ciphertext called fully homomorphic encryption (FHE) has emerged. Given that many new SG applications can be developed in the future, the use of FHEs for SG applications and their performance can be explored as the future work.

In Chapter 5, the gateway placement for the hybrid AMI network was first discussed. The gateway has important role to enable two-way traffic flow from IEEE 802.11s-based AMI network and LTE network. Several gateway placement proposals were evaluated through thorough simulations. The simulation results indicated that gateway placement is very important since different gateway location may create different path-length for every SM in the network and thus may affect the ETE packet delay. Among the evaluated gateway placement strategies, the novel two-stage heuristic vertex 1-center approach that attempts to pick the gateway location with the minimum number of directly connected SMs to the gateway showed a promising result, since it can reduce the ETE packet delay when compared to other gateway placement strategies such as the gateway placement based on the average minimum path length of all SMs to the gateway or maximizing the directly connected SMs to the gateway.

The study presented in Chapter 5 also showed that managing the present of fine-grained AMI data in the IEEE 802.11s-based AMI network can have a significant impact to the network performance. Letting SMs in neighborhood area to send their meter readings to utility company simultaneously was not a good choice since this strategy burdened the network and increased the ETE packet delay. Five data collection strategies were proposed to manage the present of these AMI data. The idea was to set a time schedule for every SM individually. These strategies can be based on the SM's position in the spanning tree of the network topology rooted at the gateway (e.g., NNFS, FNFS, and RAS), or imitated the time-division multiple access idea (e.g., TDMA and k-degree TDMA scheduling). The performance evaluation through extensive simulations showed that all proposed data collection strategies outperformed the simultaneous strategy. Among the proposed strategies, time-division multiple access-based scheduling showed the best performance.

The study investigated TCP protocol which offers a reliable data delivery in Chapter 6 and Chapter 7. Two different aspects of TCP protocol were explored and a novel approach was proposed for each aspect to improve the TCP performance in IEEE 801.s-based AMI network. These aspects were setting the minimum retransmission timeout (RTO) value and the decision to doubling the RTO value when it is expired. Typically, the minimum RTO value is the same for all SMs as in the traditional network. However since simultaneous AMI data transfer may appear in the network, this setting may increase contention. By assigning the minimum RTO value to each SM based on its location in the spanning tree rooted at the gateway, the ETE packet delay can be reduced. The reduction was more significant when an upper bound of the number of doubling the RTO value was implemented. The second investigated aspect was the inherent poor performance of TCP protocol in wireless network since it cannot distinguish whether the delay was due to congestion or other causes. To address this issue, a novel heuristic cross-layer path aware retransmission timeout approach was proposed. The approach uses the path error information from IEEE 802.11s path selection mechanism for an adaptive decision to double the RTO value. The simulation results showed that this novel approach can improve the network performance significantly at the cost of additional complexity to the network protocol.

In Chapter 8, the impact of the Address Resolution Protocol (ARP) broadcast request in an IEEE 802.11s-based AMI network was investigated. The initial extensive simulation experiments indicated that broadcast in a mesh network indeed burdened the network and degraded the network performance due to the broadcast storm in the network. The proposed solution exploited the HWMP operations, in particular the optimized broadcast mechanism for creating and maintaining proactive paths to all of SMs. The ARP broadcast request was piggybacked to the proactive path request. For this purpose, several modifications to the HWMP and packet format of IEEE 802.11s were proposed. In addition, security threads that may arise in this approach was also identified and a security protection through authentication mechanism using elliptic curve cryptography was employed.

Two network interoperability issues between IEEE 802.11s and LTE in the AMI hybrid network were identified and three proposed approaches were discussed in Chapter 9. In an AMI hybrid network, the function of user equipment was extended as the gateway to the IEEE 802.11s-based AMI network. This extension however, caused the downlink traffic cannot be delivered to an SM in the IEEE 802.11s-based AMI network due to the tunneling mechanism in the LTE network. Two distinct approaches were proposed to address this interoperability issue. The first approach was taking into account the privacy issue. A privacy-aware gateway address translation mechanism was proposed for the hybrid AMI network. This was a cross-layer approach between the application and the internet layer. Pseudonyms were used at the application layer to disassociate user identity and power consumption information. These pseudonyms are then used for utility company and the gateway in the address translation processes. When there was uplink traffic to the utility company, the trusted gateway changes the IP address of the sender to its IP address (i.e., the IP address of SM is hidden from utility company). On receiving this traffic, the utility company can send downlink traffic to the gateway, and the gateway will use the pseudonyms in the traffic to identify the corresponding SM. The second approach was a layered protocol approach at the internet layer of the EPC network. A novel UE access list was proposed for the mapping between the subnetwork of IEEE 802.11s-based AMI network and the corresponding gateway IP address (i.e., UE IP address).

The second interoperability issue was related to the QoS mismatch between IEEE 802.11s and LTE network. While LTE supports nine QoS class identifiers (QCIs), IEEE 802.11s that incorporates IEEE 802.11e standard, only supports four differentiated services. To address this mismatch, dual-queues (DQs) that consists of a priority and non priority queue, was proposed for each EDCA access category. In this way, eight differentiated services were available in IEEE 802.11s. In addition, a QoS mapping list was added at the gateway to ensure the appropriate QoS mapping between these networks.

Even though a hybrid AMI network was considered in this study, the focus of TCP/IP protocol improvements were mainly on the IEEE 802.11s-based AMI network while the LTE network was only considered for the interoperability issues with the IEEE 802.11s. Given that there will be thousands of IEEE 802.11s-based AMI networks that can be served by a base-station (i.e., eNB) of the LTE network, the overall performance of this hybrid AMI network has not been investigated yet, in particular the LTE network performance. Recently, preliminary study has been conducted in [72] for the LTE performance. Nevertheless, there are many aspects of LTE network that can be explored and investigated for this hybrid AMI network as the future work.

Moreover, the proposed approaches were based on the operations of HWMP, the default path selection mechanism in IEEE 802.11s standard. Given the flexibility of the IEEE 802.11s standard to accommodate other path selection mechanisms, investigating the TCP/IP protocol performance when other path selection mechanisms are used, can be the future work of this study. RPL [117], a routing protocol for low-power and lossy network, can be considered as one of the viable options for the future work. RPL is intended for the network where the interconnections between nodes are characterized by high loss rates, low data rates, and instability. It supports traffic flows that are suitable for AMI such as point-to-multipoint, and multipoint-to-point traffic flows.

BIBLIOGRAPHY

[1] 3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2 (3GPP TS 36.300 version 9.4.0 Release 9)."

[2] E. Quinn, "Privacy and the new energy infrastructure," *Social Science Research Network (SSRN)*, February 2009.

[3] V. Srivastava and M. Motani, "Cross-layer design: a survey and the road ahead," *Communications Magazine, IEEE*, vol. 43, pp. 112–119, Dec 2005.

[4] N. Saputro, K. Akkaya, and S. Uludag, "A survey of routing protocols for smart grid communications," *Comput. Netw.*, vol. 56, pp. 2742–2771, July 2012.

[5] D. of Energy, "Communications requirements of smart grid technologies," Oct. 2010.

[6] A. Zaballos, A. Vallejo, and J. Selga, "Heterogeneous communication architecture for the smart grid," *Network, IEEE*, vol. 25, pp. 30 –37, september-october 2011.

[7] C.-H. Lo and N. Ansari, "The progressive smart grid system from both power and communications aspects," *Communications Surveys Tutorials, IEEE*, vol. 14, pp. 799–821, Third 2012.

[8] G. Neichin and D. Cheng, "2010 u.s. smart grid vendor ecosystem," 2010.

[9] "Ieee standard for information technology–telecommunications and information exchange between systems–local and metropolitan area networks–specific requirements part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications amendment 10: Mesh networking," *IEEE Std 802.11s-2011 (Amendment to IEEE Std 802.11-2007 as amended by IEEE 802.11k-2008, IEEE 802.11r-2008, IEEE 802.11y-2008, IEEE 802.11w-2009, IEEE 802.11n-2009, IEEE 802.11p-2010, IEEE 802.11z-2010, IEEE 802.11v-2011, and IEEE 802.11u-2011)*, pp. 1 –372, 10 2011.

[10] I. Akyildiz and X. Wang, "Cross-layer design in wireless mesh networks," *Vehicular Technology, IEEE Transactions on*, vol. 57, pp. 1061–1076, March 2008.

[11] "Ieee standard for information technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications amendment 8: Medium access control (mac) quality of service enhancements," *IEEE Std 802.11e-2005 (Amendment to IEEE Std 802.11, 1999 Edition (Reaff 2003)*, pp. 1 –189, 2005.

[12] T. Imboden, K. Akkaya, and Z. Moore, "Performance evaluation of wireless mesh networks using ieee 802.11s and ieee 802.11n," in *Communications (ICC), 2012 IEEE International Conference on*, pp. 5675–5679, IEEE, 2012.

[13] F. Baker and D. Meyer, "Rfc 6272 - internet protocols for the smart grid," 2011.

[14] K. C. Leung and V. O. K. Li, "Transmission control protocol (tcp) in wireless networks: issues, approaches, and challenges," *IEEE Communications Surveys Tutorials*, vol. 8, pp. 64–79, Fourth 2006.

[15] D. Benyamina, A. Hafid, and M. Gendreau, "Wireless mesh networks design a survey," *Communications Surveys Tutorials, IEEE*, vol. 14, pp. 299–310, Second 2012.

[16] F. Foukalas, V. Gazis, and N. Alonistioti, "Cross-layer design proposals for wireless mobile networks: A survey and taxonomy," *Communications Surveys Tutorials, IEEE*, vol. 10, pp. 70–85, First 2008.

[17] T. Khalifa, A. Abdrabou, K. Naik, M. Alsabaan, A. Nayak, and N. Goel, "Split- and aggregated-transmission control protocol (sa-tcp) for smart power grid," *Smart Grid, IEEE Transactions on*, vol. 5, pp. 381–391, Jan 2014.

[18] Y.-J. Kim and M. Thottan, "Sgtp: Smart grid transport protocol for secure reliable delivery of periodic real time data," *Bell Labs Technical Journal*, vol. 16, no. 3, pp. 83–99, 2011.

[19] 3GPP, "General Packet Radio Access (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (3GPP TS 23.401 version 12.8.0 Release 12)."

[20] W. Wang, Y. Xu, and M. Khanna, "A survey on the communication architectures in smart grid," *Computer Networks*, vol. 55, no. 15, pp. 3604 – 3629, 2011.

[21] F. D. Garcia and B. Jacobs, "Privacy-friendly energy-metering via homomorphic encryption," in *Proceedings of the 6th international conference on Security and trust management*, STM'10, (Berlin, Heidelberg), pp. 226–238, Springer-Verlag, 2011.

[22] H. Gharavi and C. Xu, "Traffic scheduling technique for smart grid advanced metering applications," *Communications, IEEE Transactions on*, vol. 60, pp. 1646–1658, June 2012.

[23] S. Shao, S. Guo, X. Qiu, L. Meng, Y. Jiao, and W. Wei, "Traffic scheduling for wireless meter data collection in smart grid communication network," in *Computing, Communication and Networking Technologies (ICCCNT), 2014 International Conference on*, pp. 1–7, July 2014.

[24] V. Gabale, B. Raman, P. Dutta, S. Kalyanraman, B. Raman, P. Dutta, and S. Kalyanraman, "A classification framework for scheduling algorithms in wireless mesh networks," *Communications Surveys Tutorials, IEEE*, vol. 15, pp. 199–222, First 2013.

[25] J. Markkula and J. Haapola, "Impact of smart grid traffic peak loads on shared LTE network performance," in *Communications (ICC), 2013 IEEE International Conference on*, pp. 4046–4051, June 2013.

[26] Y. Bejerano, "Efficient integration of multihop wireless and wired networks with qos constraints," *Networking, IEEE/ACM Transactions on*, vol. 12, pp. 1064–1078, Dec 2004.

[27] B. Aoun, R. Boutaba, Y. Iraqi, and G. Kenward, "Gateway placement optimization in wireless mesh networks with qos constraints," *Selected Areas in Communications, IEEE Journal on*, vol. 24, pp. 2127–2136, Nov 2006.

[28] B. He, B. Xie, and D. P. Agrawal, "Optimizing deployment of internet gateway in wireless mesh networks," *Computer Communications*, vol. 31, no. 7, pp. 1259 – 1275, 2008. Special Issue: Resource Management and routing in Wireless Mesh Networks.

[29] F. Li, Y. Wang, and X.-Y. Li, "Gateway placement for throughput optimization in wireless mesh networks," in *Communications, 2007. ICC '07. IEEE International Conference on*, pp. 4955–4960, June 2007.

[30] S. N. Muthaiah and C. P. Rosenberg, "Single gateway placement in wireless mesh networks," in *Proceedings of the 8th International Symposium on Computer Networks (ISCN08)*, pp. 5–10, 2008.

[31] K. Akkaya and M. Younis, "Cola: A coverage and latency aware actor placement for wireless sensor and actor networks," in *Vehicular Technology Conference, 2006. VTC-2006 Fall. 2006 IEEE 64th*, pp. 1–5, Sept 2006.

[32] A. Bartoli, J. Hernandez-Serrano, M. Soriano, M. Dohler, A. Kountouris, and D. Barthel, "Secure lossless aggregation for smart grid m2m networks," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pp. 333 –338, oct. 2010.

[33] F. Li, B. Luo, and P. Liu, "Secure information aggregation for smart grids using homomorphic encryption," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pp. 327 –332, oct. 2010.

[34] A. Al Hanbali, E. Altman, and P. Nain, "A survey of TCP over ad hoc networks," *Communications Surveys Tutorials, IEEE*, vol. 7, pp. 22–36, Third 2005.

[35] W.-Q. Xu and T.-J. Wu, "TCP issues in mobile ad hoc networks: Challenges and solutions," *Journal of Computer Science and Technology*, vol. 21, no. 1, pp. 72–81, 2006.

[36] I. Psaras and V. Tsaoussidis, "On the properties of an adaptive {TCP} minimum {RTO}," *Computer Communications*, vol. 32, no. 5, pp. 888 – 895, 2009.

[37] R. Braden, "Rfc 1122 - requirements for internet hosts – communication layers," October 1989.

[38] E. Altman and T. Jimnez, "Novel delayed ack techniques for improving tcp performance in multihop wireless networks," in *Personal Wireless Communications* (M. Conti, S. Giordano, E. Gregori, and S. Olariu, eds.), vol. 2775 of *Lecture Notes in Computer Science*, pp. 237–250, Springer Berlin Heidelberg, 2003.

[39] R. de Oliveira and T. Braun, "A dynamic adaptive acknowledgment strategy for tcp over multihop wireless networks," in *INFOCOM 2005. 24th Annual*

Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE, vol. 3, pp. 1863–1874 vol. 3, March 2005.

[40] J. Chen, M. Gerla, Y. Z. Lee, and M. Y. Sanadidi, "Tcp with delayed ack for wireless networks," *Ad Hoc Netw.*, vol. 6, pp. 1098–1116, Sept. 2008.

[41] G. Holland and N. Vaidya, "Analysis of TCP performance over mobile ad hoc networks," in *Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking*, MobiCom '99, (New York, NY, USA), pp. 219–230, ACM, 1999.

[42] J. Liu and S. Singh, "ATCP: TCP for mobile ad hoc networks," *Selected Areas in Communications, IEEE Journal on*, vol. 19, pp. 1300–1315, Jul 2001.

[43] D. Kim, C.-K. Toh, and Y. Choi, "TCP-BuS: improving TCP performance in wireless ad hoc networks," in *Communications, 2000. ICC 2000. 2000 IEEE International Conference on*, vol. 3, pp. 1707–1713 vol.3, 2000.

[44] K. Chandran, S. Raghunathan, S. Venkatesan, and R. Prakash, "A feedback-based scheme for improving TCP performance in ad hoc wireless networks," *Personal Communications, IEEE*, vol. 8, pp. 34–39, Feb 2001.

[45] J. P. Monks, P. Sinha, and V. Bharghavan, "Limitations of TCP-ELFN for ad hoc networks," *MOMUC00*, 2000.

[46] I. Akyildiz and X. Wang, "Cross-layer design in wireless mesh networks," *Vehicular Technology, IEEE Transactions on*, vol. 57, pp. 1061–1076, March 2008.

[47] S. Systems, "solving the wireless mesh multi-hop dilemma," *Acces One Network White Paper*, 2010.

[48] M. Alicherry, R. Bhatia, and L. E. Li, "Joint channel assignment and routing for throughput optimization in multi-radio wireless mesh networks," in *Proceedings of the 11th annual international conference on Mobile computing and networking*, pp. 58–72, ACM, 2005.

[49] I. F. Akyildiz and X. Wang, "A survey on wireless mesh networks," *Communications Magazine, IEEE*, vol. 43, no. 9, pp. S23–S30, 2005.

[50] S.-H. Lee and Y.-B. Ko, “An efficient multi-hop arp scheme for wireless lan based mesh networks,” in *Operator-Assisted (Wireless Mesh) Community Networks, 2006 1st Workshop on*, pp. 1–6, Sept.

[51] LBNL, “Arp watch.” Lawrence Berkeley National Laboratory.

[52] V. Ramachandran and S. Nandi, “Detecting arp spoofing: an active technique,” in *Proceedings of the First international conference on Information Systems Security*, ICISS’05, (Berlin, Heidelberg), pp. 239–250, Springer-Verlag, 2005.

[53] Snort, “Snort user manual 2.9.3.” The Snort Project, May 2012.

[54] Cisco, “Cisco unified wireless network architecture base security features,” in *Enterprise Mobility 7.3 Design Guide*, Cisco Systems Inc, 2013.

[55] S. Y. Nam, S. Djuraev, and M. Park, “Collaborative approach to mitigating {ARP} poisoning-based man-in-the-middle attacks,” *Computer Networks*, vol. 57, no. 18, pp. 3866 – 3884, 2013.

[56] M. G. Gouda and C.-T. Huang, “A secure address resolution protocol,” *Computer Networks*, vol. 41, no. 1, pp. 57–71, 2003.

[57] D. Bruschi, A. Ornaghi, and E. Rosti, “S-arp: a secure address resolution protocol,” in *Computer Security Applications Conference, 2003. Proceedings. 19th Annual*, pp. 66–74, Dec.

[58] W. Lootah, W. Enck, and P. McDaniel, “Tarp: Ticket-based address resolution protocol,” *Computer Networks*, vol. 51, no. 15, pp. 4322 – 4337, 2007.

[59] D. Harkins, “Simultaneous authentication of equals: A secure, password-based key exchange for mesh networks,” in *Sensor Technologies and Applications, 2008. SENSORCOMM ’08. Second International Conference on*, pp. 839 –844, aug. 2008.

[60] H. Gharavi and B. Hu, “Multigate mesh routing for smart grid last mile communications,” in *Wireless Communications and Networking Conference (WCNC), 2011 IEEE*, pp. 275 –280, march 2011.

[61] J.-S. Jung, K.-W. Lim, J.-B. Kim, Y.-B. Ko, Y. Kim, and S.-Y. Lee, “Improving ieee 802.11s wireless mesh networks for reliable routing in the smart

grid infrastructure," in *Communications Workshops (ICC), 2011 IEEE International Conference on*, pp. 1 –5, june 2011.

[62] J. Kim, D. Kim, K.-W. Lim, Y.-B. Ko, and S.-Y. Lee, "Improving the reliability of ieee 802.11s based wireless mesh networks for smart grid systems," *Communications and Networks, Journal of*, vol. 14, no. 6, pp. 629–639, 2012.

[63] R. M. Abid, T. Benbrahim, and S. Biaz, "Ieee 802.11s wireless mesh networks for last-mile internet access: An open-source real-world indoor testbed implementation," *Wireless Sensor Network*, vol. 2, no. 10, pp. 725–738, 2010.

[64] M. S. Islam, Y. J. Yoon, M. A. Hamid, and C. S. Hong, "A secure hybrid wireless mesh protocol for 802.11s mesh network," in *Proceeding sof the international conference on Computational Science and Its Applications, Part I*, ICCSA 08, (Berlin, Heidelberg), pp. 972–985, Springer-Verlag, 2008.

[65] J. Ben-Othman and Y. Benitez, "On securing hwmp using ibc," in *Communications (ICC), 2011 IEEE International Conference on*, pp. 1 –5, june 2011.

[66] J. Villalón, P. Cuenca, and L. Orozco-Barbosa, "On the effectiveness of ieee 802.11 e qos support in wireless lan: a performance analysis," in *High Performance Computing and Communications*, pp. 605–616, Springer, 2005.

[67] Y. Xiao, "Performance analysis of priority schemes for ieee 802.11 and ieee 802.11 e wireless lans," *Wireless Communications, IEEE Transactions on*, vol. 4, no. 4, pp. 1506–1515, 2005.

[68] M. E. Masri, "Ieee 802.11 e: the problem of the virtual collision management within edca," in *INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings*, pp. 1–2, IEEE, 2006.

[69] T. B. Reddy, J. P. John, and C. S. R. Murthy, "Providing mac qos for multimedia traffic in 802.11 e based multi-hop ad hoc wireless networks," *Computer Networks*, vol. 51, no. 1, pp. 153–176, 2007.

[70] G. Rajalingham, Q.-D. Ho, and T. Le-Ngoc, "Evaluation of an efficient smart grid communication system at the neighbor area level," in *Consumer Communications and Networking Conference (CCNC), 2014 IEEE 11th*, pp. 426–431, Jan 2014.

[71] J. Markkula and J. Haapola, "Lte and hybrid sensor-lte network performances in smart grid demand response scenarios," in *Smart Grid Communications*

(SmartGridComm), 2013 IEEE International Conference on, pp. 187–192, Oct 2013.

[72] F. Koohifar, N. Saputro, I. Guvenc, and K. Akkaya, "Hybrid wi-fi/lte aggregation architecture for smart meter communications," in *Smart Grid Communications (SmartGridComm), 2015 IEEE International Conference on*, Nov 2015.

[73] V. Paxson, M. Allman, J. Chu, and M. Sargent, "Rfc 2988 - computing tcp's retransmission timer," June 2011.

[74] N. Saputro and K. Akkaya, "On preserving user privacy in smart grid advanced metering infrastructure applications," *Security and Communication Networks*, vol. 7, no. 1, pp. 206–220, 2014.

[75] C. Fontaine and F. Galand, "A survey of homomorphic encryption for non-specialists," *EURASIP J. Inf. Secur.*, vol. 2007, pp. 15:1–15:15, Jan. 2007.

[76] P. Paillier, "Trapdooring discrete logarithms on elliptic curves over rings," in *Proceedings of the 6th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology*, ASIACRYPT '00, (London, UK, UK), pp. 573–584, Springer-Verlag, 2000.

[77] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography.* Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2003.

[78] F. Cleveland, "Cyber security issues for advanced metering infrastructure (ami)," in *Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE*, pp. 1 –5, july 2008.

[79] G. Hart, "Nonintrusive appliance load monitoring," *Proceedings of the IEEE*, vol. 80, pp. 1870 –1891, dec 1992.

[80] D. Seo, H. Lee, and A. Perrig, "Secure and efficient capability-based power management in the smart grid," in *Parallel and Distributed Processing with Applications Workshops (ISPAW), 2011 Ninth IEEE International Symposium on*, pp. 119–126, May 2011.

[81] O. Ugus, D. Westhoff, R. Laue, A. Shoufan, and S. A. Huss, "Optimized implementation of elliptic curve based additive homomorphic encryption for wire-

less sensor networks,” *2nd Workshop on Embedded Systems Security (WESS)*, 2007.

[82] P. Paillier, “Public-key cryptosystems based on composite degree residuosity classes,” in *Proceedings of the 17th international conference on Theory and application of cryptographic techniques*, EUROCRYPT’99, (Berlin, Heidelberg), pp. 223–238, Springer-Verlag, 1999.

[83] T. Okamoto and S. Uchiyama, “A new public-key cryptosystem as secure as factoring,” in *Advances in Cryptology EUROCRYPT’98* (K. Nyberg, ed.), vol. 1403 of *Lecture Notes in Computer Science*, pp. 308–318, Springer Berlin Heidelberg, 1998.

[84] D. Naccache and J. Stern, “A new public key cryptosystem based on higher residues,” in *Proceedings of the 5th ACM conference on Computer and communications security*, CCS ’98, (New York, NY, USA), pp. 59–66, ACM, 1998.

[85] R. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Communications of the ACM*, vol. 21, pp. 120–126, 1978.

[86] T. El Gamal, “A public key cryptosystem and a signature scheme based on discrete logarithms,” in *Proceedings of CRYPTO 84 on Advances in cryptology*, (New York, NY, USA), pp. 10–18, Springer-Verlag New York, Inc., 1985.

[87] J. Domingo-Ferrer, “A provably secure additive and multiplicative privacy homomorphism,” in *Proceedings of the 5th International Conference on Information Security*, ISC ’02, (London, UK, UK), pp. 471–483, Springer-Verlag, 2002.

[88] C. Castelluccia, E. Mykletun, and G. Tsudik, “Efficient aggregation of encrypted data in wireless sensor networks,” in *Mobile and Ubiquitous Systems: Networking and Services, 2005. MobiQuitous 2005. The Second Annual International Conference on*, pp. 109 – 117, july 2005.

[89] K. Lauter, “The advantages of elliptic curve cryptography for wireless security,” *Wireless Communications, IEEE*, vol. 11, pp. 62 – 67, feb 2004.

[90] E. Mykletun, J. Girao, and D. Westhoff, “Public key based cryptoschemes for data concealment in wireless sensor networks,” in *Communications, 2006. ICC ’06. IEEE International Conference on*, vol. 5, pp. 2288 –2295, june 2006.

[91] B. King, "Mapping an arbitrary message to an elliptic curve when defined over gf (2 n)," *International Journal of Network Security*, vol. 8, no. 2, pp. 169–176, 2009.

[92] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pp. 238 –243, oct. 2010.

[93] X. Fang and L. Li, "On karatsuba multiplication algorithm," in *Proceedings of the The First International Symposium on Data, Privacy, and E-Commerce*, ISDPE '07, (Washington, DC, USA), pp. 274–276, IEEE Computer Society, 2007.

[94] A. B. Arabani and R. Z. Farahani, "Facility location dynamics: An overview of classifications and applications," *Computers & Industrial Engineering*, vol. 62, no. 1, pp. 408 – 420, 2012.

[95] T. H. Cormen, C. Stein, R. L. Rivest, and C. E. Leiserson, *Introduction to Algorithms*. McGraw-Hill Higher Education, 2nd ed., 2001.

[96] E. Malaguti and P. Toth, "A survey on vertex coloring problems," *International Transactions in Operational Research*, vol. 17, no. 1, pp. 1–34, 2010.

[97] H. Broersma, F. V. Fomin, P. A. Golovach, and G. J. Woeginger, "Backbone colorings for graphs: Tree and path backbones," *Journal of Graph Theory*, vol. 55, no. 2, pp. 137–152, 2007.

[98] B. Milic and M. Malek, "NPART-node placement algorithm for realistic topologies in wireless multihop network simulation," in *Proceedings of the 2nd International Conference on Simulation Tools and Techniques*, p. 9, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2009.

[99] V. Paxson and M. Allman, "Rfc 2988 - computing tcp's retransmission timer," November 2000.

[100] "Korean electric power research institute," 2013.

[101] N. Saputro and K. Akkaya, "An efficient and secure arp for large-scale ieee 802.11s-based smart grid networks," in *ADHOCNETS 2013, LNICST 129*

(A. Mellouk, M. H. Sherif, J. Li, and P. Bellavista, eds.), pp. 214–228, Springer, 2014.

[102] M. Baran and T. McDermott, "Distribution system state estimation using AMI data," in *Power Systems Conference and Exposition, 2009. PSCE '09. IEEE/PES*, pp. 1–3, March 2009.

[103] J. Peppanen, M. Reno, M. Thakkar, S. Grijalva, and R. Harley, "Leveraging AMI data for distribution system model calibration and situational awareness," *Smart Grid, IEEE Transactions on*, vol. PP, no. 99, pp. 1–1, 2015.

[104] K. Andreev and P. Boyko, "Ieee 802.11 s mesh networking ns-3 model," *IITP, WNS3, March*, 2011.

[105] N. Saputro and K. Akkaya, "Periodic data reporting strategies for IEEE 802.11s-based smart grid AMI networks," in *Smart Grid Communications (SmartGridComm), 2014 IEEE International Conference on*, pp. 314–319, Nov 2014.

[106] N. Saputro and K. Akkaya, "PARP-S: A secure piggybacking-based ARP for IEEE 802.11s-based smart grid AMI networks," *Computer Communications*, vol. 58, no. 0, pp. 16 – 28, 2015. Special Issue on Networking and Communications for Smart Cities.

[107] N. Saputro and K. Akkaya, "An efficient arp for large-scale ieee 802.11s-based smart grid networks," in *Local Computer Networks (LCN), 2013 IEEE 38th Conference on*, pp. 723–726, Oct 2013.

[108] D. Harkins and D. Carrel, "Rfc 2409 - the internet key exchange (ike)," 1998.

[109] G. Carneiro, P. Fortuna, and M. Ricardo, "Flowmonitor: a network monitoring framework for the network simulator 3 (ns-3)," in *Proceedings of the Fourth International ICST Conference on Performance Evaluation Methodologies and Tools*, VALUETOOLS '09, (ICST, Brussels, Belgium, Belgium), pp. 1:1–1:10, 2009.

[110] NSA, "The case for elliptic curve cryptography," *Report*, 2009.

[111] D. of Energy, "Operations and maintenance savings from advanced metering infrastructure - initial results," 2012. [Online] Accessed: 2015-05-05.

[112] J. G. Deshpande, E. Kim, and M. Thottan, "Differentiated services qos in smart grid communication networks," *Bell Labs Technical Journal*, vol. 16, no. 3, pp. 61–81, 2011.

[113] K. C. Budka, J. G. Deshpande, T. L. Doumi, M. Madden, and T. Mew, "Communication network architecture and design principles for smart grids," *Bell Labs Technical Journal*, vol. 15, no. 2, pp. 205–227, 2010.

[114] M. Zeifman and K. Roth, "Nonintrusive appliance load monitoring: Review and outlook," *Consumer Electronics, IEEE Transactions on*, vol. 57, pp. 76–84, February 2011.

[115] P. Srisuresh and M. Holdrege, "Rfc 2663 - ip network address translator (nat) terminology and considerations," 1999.

[116] S. Tonyali, N. Saputro, and K. Akkaya, "Assessing the feasibility of fully homomorphic encryption for smart grid ami networks," in *Ubiquitous and Future Networks (ICUFN), 2015 Seventh International Conference on*, pp. 591–596, July 2015.

[117] T. Winter, P. Thubert, A. Brandt, T. Clausen, J. Hui, R. Kelsey, P. Levis, K. Pister, K. Struik, and J. Vasseur, "Rpl: Ipv6 routing protocol for low power and lossy networks," 2011.

VITA

NICO SAPUTRO

	Born, Solo, Indonesia
1994	B.Eng., Electrical Engineering Institut Teknologi Bandung (ITB) Bandung, Indonesia
2000	M.Eng., Industrial Engineering Institut Teknologi Bandung (ITB) Bandung, Indonesia
2009-2012	Fulbright Presidential Scholarship
2011-2014	PhD. Candidate, Computer Science Southern Illinois University Carbondale, Illinois
	Graduate Assistantship Information Technology Service Center Southern Illinois University Carbondale, Illinois
2014-2016	Graduate Assistantship Electrical and Computer Engineering Florida International University Miami, Florida

PUBLICATIONS AND PRESENTATIONS (selected articles)

Kohifar,F., Saputro,N., Guvenc,I., and Akkaya,K, *”Hybrid Wi-Fi/LTE Architecture with Aggregation for Smart Meter Communications”*. IEEE International Conference on Smart Grid Communications (SmartGridComm), Miami, FL, Nov. 2015.

Mahmoud,M., Saputro,N., Akula,P., and Akkaya,K, *”Privacy-Preserving Power Injection over a Hybrid AMI/LTE Smart Grid Network”*. IEEE Internet of Things Journal, 2016. (to appear).

Saputro,N., Yurekli,A.I., Akkaya,K., and Uluagac,A.S., *”Privacy-preservation for IoT in Smart Buildings”*. Book Chapter In Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations, ed. Fei Hu, Apr. 2016, CRC-Press.

Saputro,N., and Akkaya,K., *”PARP-S: A Secure Piggybacking-based ARP for IEEE 802.11s-based Smart Grid AMI Networks”*. Computer Communications, vol. 58, pp. 16-28, Mar. 2015, Elsevier.

Saputro,N., and Akkaya,K., *”On Preserving User Privacy in Smart Grid Advanced Metering Infrastructure Applications”*. Security and Communication Networks 7(1), pp. 206-220, Jan. 2014, John Wiley & Sons.

Saputro,N., Akkaya,K., and Uludag,S., *”A Survey of routing protocols for smart grid communications”*. Computer Network 56(11), pp. 2742-2771, Jul. 2012, Elsevier.

Saputro,N., Akkaya,K., and Yurekli,A.I., *”Path Error-Aware RTO Design for Smart Meter Data Traffic in IEEE 802.11s-based AMI Networks”*. IEEE International Conference on Smart Grid Communications (SmartGridComm), Miami, FL, Nov. 2015, pp. 211-216.

Saputro,N., Akkaya,K., and Guvenc,I., *”Privacy-aware Communication Protocol for Hybrid IEEE 802.11s/LTE Smart Grid Architectures”*. The 11th IEEE International Workshop on Performance and Management of Wireless and Mobile Networks (P2MNet), Clearwater Beach, FL, Oct. 2015, pp. 905-911.

Saputro,N., and Akkaya,K., *”Periodic Data Reporting Strategies for IEEE 802.11s-based Smart Grid AMI Networks”*, The 5th IEEE International Conference on Smart Grid Communications (SmartGridComm), Venice, Italy, Nov. 2014, pp. 314-319.

Saputro,N., and Akkaya,K., *”An Improved TCP for Reduced Packet Delay in IEEE 802.11s-based Smart Grid AMI Networks”*, in N. Mitton, A. Gallais, M.E. Kantarci, and S. Papavassiliou (Eds.), Ad Hoc Networks, LNICST Vol 140, Chap. 8, pp. 86-97, Nov. 2014, Springer.

Saputro,N., and Akkaya,K., *”An efficient and Secure ARP for Large-scale IEEE 802.11s-based Smart Grid Networks”*, in M.H. Sherif, A. Mellouk, J. Li, and P. Bellavista (Eds.), Ad Hoc Networks, LNICST Vol. 129, Chap. 14, pp 214-228, Jan. 2014, Springer.

Saputro,N., and Akkaya,K., *”An efficient ARP for Large-scale IEEE 802.11s-based Smart Grid Networks (short paper)”*, The 38th IEEE Conference on Local Computer Networks (LCN), Sidney, Australia, Oct. 2013, pp. 723-726.

Saputro,N., and Akkaya,K., *”Performance Evaluation of Smart Grid Data Aggregation via Homomorphic Encryption”*, IEEE Wireless Communications and Networking Conference (WCNC), Paris, France, Apr. 2012, pp. 2945-2950.