3-30-2017

Development of a Remotely Accessible Wireless Testbed for Performance Evaluation of AMI Related Protocols

Utku Ozgur
Florida International University, uozgu001@fiu.edu

DOI: 10.25148/etd.FIDC001799

FLORIDA INTERNATIONAL UNIVERSITY

Miami, Florida

DEVELOPMENT OF A REMOTELY ACCESSIBLE WIRELESS TESTBED FOR PERFORMANCE EVALUATION OF AMI RELATED PROTOCOLS

A thesis submitted in partial fulfillment of the

requirements for the degree of

MASTER OF SCIENCE

in

COMPUTER ENGINEERING

by

Utku Ozgur

2017

To: Interim Dean Ranu Jung
College of Engineering and Computing

This thesis, written by Utku Ozgur, and entitled Development of a Remotely Accessible Wireless Testbed for Performance Evaluation of AMI Related Protocols, having been approved in respect to style and intellectual content, is referred to you for judgment.

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

A. Selcuk Uluagac

Alexander Pons

Kemal Akkaya, Major Professor

Date of Defense: March 30, 2017

The thesis of Utku Ozgur is approved.

Interim Dean Ranu Jung
College of Engineering and Computing

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

Florida International University, 2017

ACKNOWLEDGMENTS

I would like to thank Advanced Wireless and Security Lab (ADWISE) group and their members, my family and friends for being supportive and helpful during my studies and to the Department of Electrical and Computer Engineering, FIU for providing me with this opportunity.

I would also like to acknowledge the support of my thesis by Department of Energy and National Science Foundation. This thesis is partially based upon work supported by the Department of Energy under Award Number DE-OE0000779 and by US National Science Foundation under the grant number CNS-1550313.

ABSTRACT OF THE THESIS

DEVELOPMENT OF A REMOTELY ACCESSIBLE WIRELESS TESTBED FOR PERFORMANCE EVALUATION OF AMI RELATED PROTOCOLS

by

Utku Ozgur

Florida International University, 2017

Miami, Florida

Professor Kemal Akkaya, Major Professor

Although smart meters are deployed in many countries, the data collection process from smart meters in Smart Grid (SG) still has some challenges related to consumer privacy that needs to be addressed. Referred to as Advanced Metering Infrastructure (AMI), the data collected and transmitted through the AMI can leak sensitive information about the consumers if it is sent as a plaintext.

While many solutions have been proposed in the past, the deployment of these solutions in real-life was not possible since the actual AMIs were not accessible to researchers. Therefore, a lot of solutions relied on simulations which may not be able to capture the real performance of these solutions. In this thesis, two 802.11s wireless mesh-based SG AMI network testbeds are developed with Beaglebone Black and Raspberry Pi 3 boards to provide a baseline for the simulations. The Raspberry Pi 3 testbed is also configured to be remotely accessible.

TABLE OF CONTENTS

CHAPTER PAGE

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

Smart Grid (SG) is the system that makes power distribution efficient and effective [Wen09]. This is achieved through different components at the generation, transmission and distribution levels that enable bidirectional communication. One of these components is the Advanced Metering Infrastructure (AMI) where smart meters (SMs) and other intermediate devices are deployed for ensuring communication between the users and the utility company. SMs are used to collect consumer power usage data which is sent to the utility company for billing and analysis purposes.

For the healthy progression of the SG system, a stable and efficient method of communication between SMs and the respective companies is needed. Because of its practicality and low cost [YMG08], wireless communication networks can be an alternative of the wired networks such as a power-line communication (PLC) that is mostly preferred in SG AMI networks [JBL$^+$11]. Different wireless mesh protocols and standards are employed for this purpose. IEEE 802.11s standard is preferred as it integrates mesh networking services and protocols with existing IEEE 802.11 protocols at the MAC layer.

Another thing to consider in these networks is the privacy of the collected data [GXL$^+$12, SA14]. Although at first it may seem like simple collected data, such as power consumption of a household, wouldn't mean anything to an attacker that intercepts it, this data can actually be used to gain insight about that particular household after monitoring the collected data for some time. In order to avoid this, various approaches are proposed in recent years. [TSA15a, TCA$^+$16a, TASU16]

Despite the diversity of these solutions, one major issue is the lack of actual deployment and testing in real AMI environments. This was partially due to infeasibility of using existing utility AMI systems and insufficient resources to develop such testbeds at academic environments. Therefore, bulk of the research relied on simulations to evaluate the feasibility, performance and overhead of privacy-preserving methods. However, simulation-based tools have their own issues, particularly for wireless environments, in terms of their ability to capture the channel characteristics and simulate the protocols. Therefore, there is a need to assess how realistic the simulation-based tools are in the context of AMI applications when different privacy-based computations are performed. This thesis aims to fulfill the need by creating an actual secure AMI testbed using Beaglebone Black boards (BBBs) [Col13] with TP-Link TL-WN722N wireless adaptors [TL16] to evaluate the performance of AMI related protocols. Specifically, the proposed system takes advantage of different encryption algorithms for privacy which are partially homomorphic encryption algorithm called Paillier cryptosystem (PHE) [Pai99], secure multi-party computation (SMPC) [KPS13, TAS$^+$17], and fully homomorphic encryption (FHE) [TSA15b, TASU16]. For message integrity and identity check, two-factor authentication with OpenSSL [Ope16] certificates and Elliptic Curve Digital Signature Algorithm (ECDSA) [JMV01] signatures are used. In order to test FHE, another testbed is created by replacing BBBs with Raspberry Pi 3 (RP3) [RW12] devices. Another aim of this work is to make this testbed remotely accessible so that interested researchers can access and use the system for research purposes without needing to create their own testbed.

CHAPTER 2

BACKGROUND INFORMATION

2.1 Smart Grid

SG is a cyber-physical system that is expected to replace the traditional power grid still in use. [CMAU16] In order to understand what smart grid offers and what is different in smart grid, a comparison between traditional power grid and smart grid is made in the next subsection. Then, smart grid and its domains are explained in detail.

2.1.1 Smart Grid versus Traditional Power Grid

Traditional power grid is a physical system that is currently being used for power generation and transmission. The system has four different interconnected domains as seen in Fig. 2.1. These domains are called generation, transmission, distribution, and customer domain. In this grid, generation domain is responsible for generation of power that will be used inside the grid. Transmission domain is responsible of getting the power generated from the generation domain and transmitting it using High Voltage (HV) lines. Distribution domain gets the power transmitted through the HV lines, transforms it to Low Voltage (LV) and distributes this power using LV lines to the customer domain. Customer domain is the domain that consumes the power generated. Although this grid is used for a long time without major problems, it started to get old with the introduction of new technologies. This created a need for an upgrade on the grid. As the traditional power grid is not upgradeable because of its nature, smart grid is proposed to take over it.

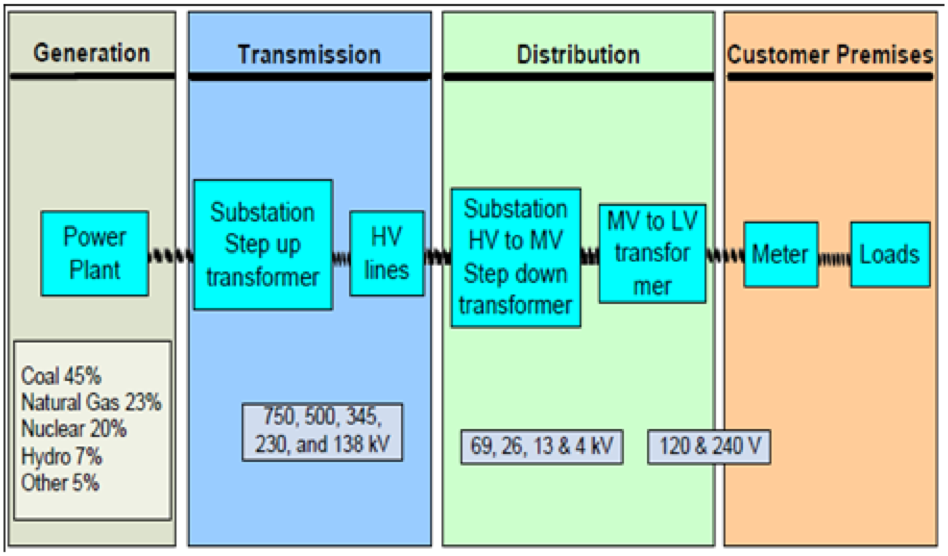
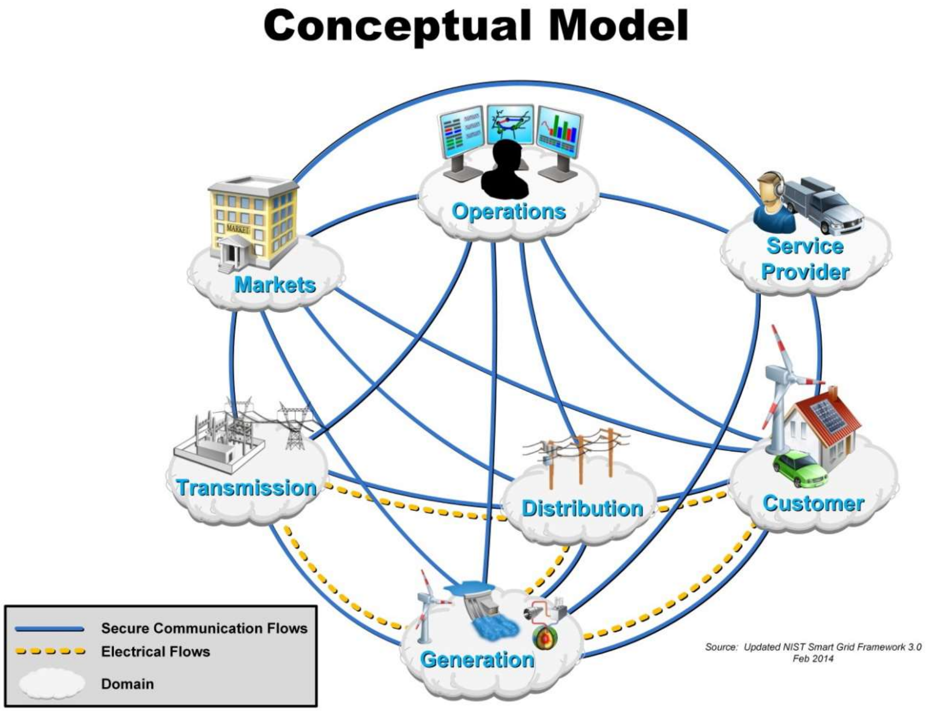


Figure 2.1: Traditional Power Grid Model with its Domains

SG aims to take over by addressing the weaknesses of the traditional power grid and fixing them. One of the weaknesses that is addressed is the type of the system. Traditional power grid is a physical system, whereas SG is a cyber-physical system. [FMXY12] Cyber system is established in SG by creating a communication network on top of the physical system. This cyber system also introduces three new domains in SG. [GWP$^+$14] Apart from the four classic domains, SG also includes service provider, operation and market domains which are different than the traditional power grid. The representation of the SG with its domains can be seen in Fig. 2.2.

Another weakness that is addressed by SG is communication between domains. In the traditional power grid, communication is one way and. Power is generated, transmitted, distributed and then used. It is not possible for the customer domain to communicate with other domains. This is not the case for SG. In SG, communication is two-way. This is achieved by changing the centralized generation in the traditional power grid (only generation domain generates energy) by distributing the power generation to the generation, transmission, distribution, and customer domains.



Source: Updated NIST Smart Grid Framework 3.0 Feb 2014

Figure 2.2: Smart Grid Model with Domains

These domains are configured to generate energy when needed in SG. The generated energy in these domains can also be shared with other domains when it is needed. Another advantage of distributed generation is that it provides more control over the grid and makes the system more tolerant to faults.

Domains of SG are explained in detail at their respective subsections below.

2.1.2 Generation Domain

Like in the traditional power grid, generation domain is mainly responsible for energy generation in SG, too. In this domain, energy is generated by using different energy sources like solar, wind, coal, etc. The additional communications added in SG to this domain are used for better control of the generation process. Operation domain uses the communication to monitor the generation to measure and record the process in order to review if needed and do the necessary protections for the system.

2.1.3 Transmission Domain

The energy generated in the generation domain is transferred with the help of the transmission domain. This transmission is made possible by using substations that transform the energy to the appropriate voltage according to the grid's needs. Like in generation domain, new communications introduced in SG is used to better control this domain. In this domain, control also includes stabilization and optimization which is needed to be done in this domain maintain the supply/demand equilibrium.

2.1.4 Distribution Domain

Distribution domain is the bridge that connects the transmission domain to the customer domain. The energy transmitted through the transmission domain is distributed to the customer domain with the help of the distribution domain. This domain works in a very similar way compared to the transmission domain. Substations get the energy transmitted from the transmission domain, then relay the energy using LV lines after it is transformed. Control mechanisms are again present with the help of communication and operations domain.

2.1.5 Operation Domain

Operation Domain is the domain that make sure the grid is operating without any problems. This includes not only the physical system but also the cyber system that is vital for the control of the physical system. In the cyber side, operation domain monitors and controls the network operations. If a fault occurs in this side, it is also analysed by this domain. In the physical side, operations domain is responsible for distribution, transmission, and customer domains. All the devices used in these domains are under control of the operations domain and any maintenance needs, upgrades, extensions, and security needs are covered by it.

2.1.6 Service Provider Domain

The energy generated in SG is not supplied to the customer directly as there is a need for a way to control the usage of the grid by customers. All users in the customer domain should be able to benefit from the grid fairly. Service provider domain is responsible for creating and providing services that can benefit from the SG and used by customers. The most popular example for a service is electricity. The providers in this domain is considered responsible for the management of the service they provide. Which means they need to manage the users (can be individuals, houses, or buildings), their accounts, and any maintenance or set up cost for the devices that are needed for use of the service. Billing the users for their usage is another responsibility of the service provider.

2.1.7 Market Domain

A service provider needs to be in control of some components of the SG to be able to provide their service. As there is not only one provider, there is a need to control how the grid components should be bought, sold, and traded. These processes are done inside the market domain.

2.1.8 Customer Domain

The whole aim of constructing a grid is to provide the energy needed by the customers in the customer domain. Customers inside this domain can be separated into three different types, which are home, building, and industrial. Energy is mostly consumed in this domain. With SG, it is also possible to generate electricity in this domain. This generation is achieved by micro-grids. Micro-grids are smaller grids that generate energy with the sources available in the customer domain. These sources can be solar, wind, and hydroelectric.

All customers have different energy needs, pricing, and usages. The control process is automated with the help of SMs located in the customer premises. This metering infrastructure is called Advanced Metering Infrastructure (AMI), which is an important system in the customer domain, and the main focus of this thesis.

2.2 AMI Network

AMI communication network consists of SMs that are connected via a wireless mesh network (WMN) with a gateway serving as a relay between SMs and the utility companies (UCs). A typical infrastructure for the considered AMI in this thesis is shown in Fig. 2.3.

In the SG context, SMs are mostly hooked on to the devices in the Home Area Network (HAN) or in the Building Area Network (BAN) that consume electricity like home appliances, electric vehicles, etc. WMN is set up with the SMs located inside a neighborhood or in other words a Neighborhood Area Network (NAN).

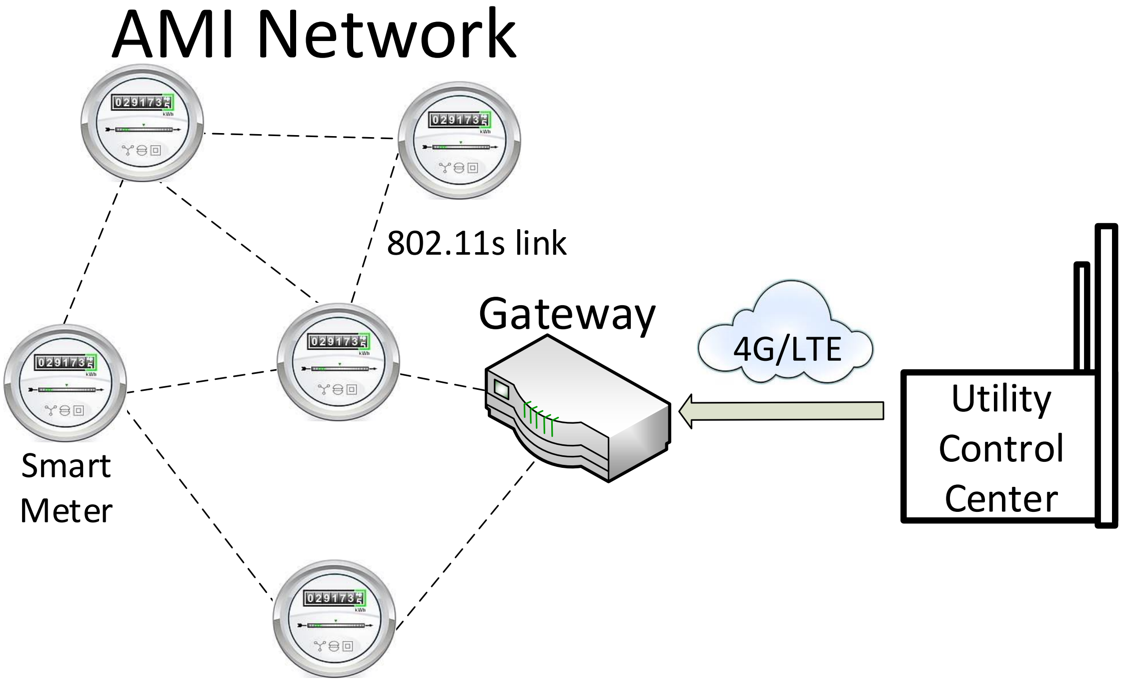


Figure 2.3: A sample AMI communication network, gateway, and long-distance communication to a utility company.

Data collected from the devices by the SMs is sent to the gateway of the WMN. Gateway collects this data and then transmits it to the UCs using a Wide Area Network (WAN) technology like 4G, LTE, etc. This data can be used for billing or statistical purposes by the UCs.

2.3 IEEE 802.11s

IEEE 802.11s standard allows mesh networking among the SMs through 802.11 MAC/PHY layer standard [HDM$^+$10]. It uses the Hybrid Wireless Mesh Protocol (HWMP) as its default routing protocol to find a multi-hop path towards the destination.

The nodes in 802.11s WMN are given names based on their roles. All nodes are considered as Mesh Points (MP) and are able to provide connectivity at the data link layer between other MPs. If an MP also provides connectivity to the Internet, it is termed a Mesh Portal Point (MPP). If one of the MPs is used as an access point, it is called Mesh Access Point (MAP).

2.3.1 Hybrid Wireless Mesh Protocol

As IEEE 802.11s standard extends 802.11 MAC layer, routing is carried out in this layer rather than in the Network Layer. Routing in MAC Layer rather than in Network Layer creates new requirements for the routing protocol that will be used in these networks [Bah06]. One of these requirements is the routing metric. Routing metrics used in the traditional routing protocols are metrics that are calculated in Network Layer, but as we are now in MAC Layer, a radio-aware routing metric is needed. Another requirement is the support for unicast, broadcast and multicast messages. These messages were sent by using IP addresses in Network Layer, but we must use MAC addresses for this purpose in WMNs. The final requirement is an efficient path selection algorithm, which can use MAC addresses for routing purposes. HWMP is defined as the default routing protocol for IEEE 802.11s-based mesh networks because it fulfills these new requirements set for WMNs [IEE06].

The routing metric used in HWMP is airtime metric. This metric gives the cost, in terms of channel resource consumed, of using a link for frame transmission [BAM12]. Value of this metric is found using the following equation:

$$C_a = [O_{ca} + O_p + B_t][r/(1 - e_{pt})] \tag{2.1}$$

In this equation, C_a is the airtime cost, O_{ca} is the overhead for channel access, O_p is overhead for protocol, B_t is the number of bits available in a test frame, r is the bit rate in Megabits per second and e_{pt} is the error rate for the frame.

Support for unicast, broadcast and multicast messages are provided in HWMP with the help of using control messages. Four different control messages are used in HWMP:

- *Root Announcement (RANN):* Informs MPs about the root MP (if present) and the distance of that MP to the root MP.
- *Route Request (RREQ):* Asks destination MPs to form a reverse route from destination to the source.
- *Route Reply (RREP):* Forms a forward route from destination to the source and verifies the reverse route.
- *Route Error (RERR):* Informs MPs that receive this message about the inavailability of a route.

The path selection mechanism is the main reason for the naming of HWMP. ”Hybrid” is used in the naming of HWMP because it uses on-demand routing and proactive routing together. The decision mechanism used by HWMP for routing method selection can be seen in Fig. 2.4.

On-demand Routing in Hybrid Wireless Mesh Protocol

As seen in Fig. 2.4, on-demand routing is used in HWMP when there is no root. Root configuration is not made if the network does not have a fixed network topology. This means that this routing is used when the network is mobile. This approach is especially efficient in mobile networks since routes are only created on-demand as the name suggests so devices that join or leave network do not cause a big problem

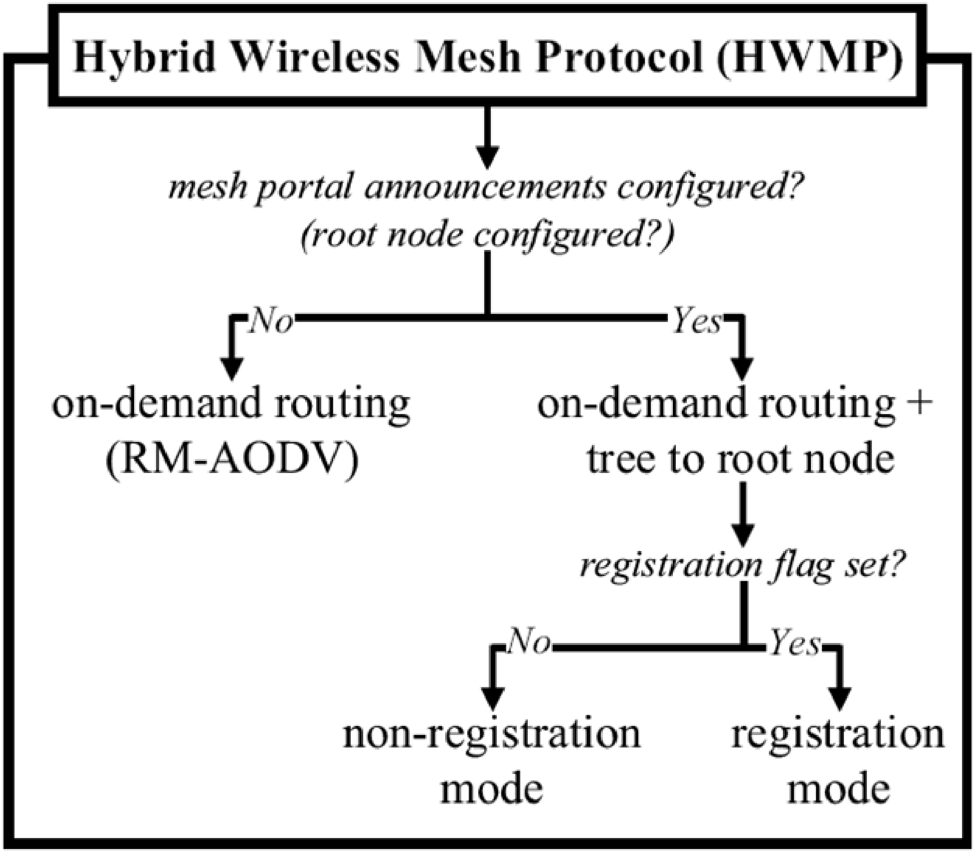


Figure 2.4: The decision mechanism of HWMP for routing method selection. (By courtesy of [Bah06])

for routing. The procedure followed for route creation between the source and the destination is as follows:

- RREQ is broadcasted by the source MP to find a route to the destination
- When RREQ is received by one of the MPs, there are two possibilities:
  - If that MP has a route to the destination, route is updated.
  - If that MP does not have a route to the destination, RREQ is forwarded.
- When a path is found, the destination sends a unicast RREP to the source.

Proactive Routing in Hybrid Wireless Mesh Protocol

As seen in Fig. 2.4, proactive routing is used in HWMP when a root MP is configured. One of the MPs is configured as root, which is responsible for the traffic going in and out of the network. Two different mechanisms can be used when proactive routing is selected in HWMP. The first one uses proactive RREQ messages (also called registration mode [Bah06]) and the second one uses proactive RANN messages (also called non-registration mode [Bah06]). The procedure for the first mechanism is:

- Root MP periodically broadcasts RREQ messages
- When an MP receives this RREQ message, it updates its path to the root and forwards it if needed

The procedure for the second mechanism looks like the first mechanism but it uses RANN messages.

- Root MP periodically floods the network with RANN messages
- When an MP receives this RANN message, if it needs to update the path, it sends a RREQ to the root
- When the root MP receives the RREQ message, it sends a unicast RREP message back to that MP.

2.4 Paillier Cryptosystem

Privacy-preserving aggregation is done using homomorphic encryption which allows some specific operations on ciphertext and provides an encrypted result that, when decrypted, is equal to the result of operations performed on plaintext.

This thesis uses a partially homomorphic encryption (PHE) algorithm called Paillier [Pai99]. This is chosen due to its addition property, smaller message expansion factor compared to others, and security features [SA12, SA14].

Below is a more formal representation of Paillier's homomorphic addition operation:

Let m_1 and m_2 be two plaintexts.

$$D_{S_K}((E_{P_K}(m_1)\, x\, E_{P_K}(m_2))\, mod n^2) = (m_1 + m_2)\, mod n \tag{2.2}$$

where n is the first component of the public key ($P_K = (n,\, g)$ where g is a random integer and $g \in Z^*_{n^2}$). Thus, one can infer that there is no need to know the private key to perform homomorphic addition operation while using Paillier cryptosystem.

2.5 Fully Homomorphic Encryption

Another homomorphic encryption solution is fully homomorphic encryption (FHE). Unlike Paillier, FHE supports multiplication operations on ciphertext. The scheme used in this thesis is called SV scheme which is proposed by Perl et al. [PBS11]

The main differences between PHE and FHE are message, key sizes, and the message expansion factor. FHE works on the data bit by bit which means it encrypts every bit and expands it size-wise. Because of this, FHE message and key sizes are huge compared to PHE sizes. Although this is a disadvantage for FHE, it is also an advantage for FHE as it provides near perfect security as long as private key isn't compromised.

2.6 Secure Multi-Party Computation

Secure multi-party computation (SMPC) is another solution for preserving privacy. Unlike PHE and FHE, secret sharing is the method used by SMPC. In this method, the secret created for the communication of the nodes (parties) in the network is divided into pieces and these pieces are given to the different parties in the network. This divide and share approach makes it harder to crack the secret as gathering one piece wouldn't be enough to get the secret itself.

In SMPC, data aggregation for a network with n nodes is done as follows:
(r_i is the secret of node i, and p is a prime number)

- A unique point (x) is picked by every node.
- Every node selects a polynomial with n - 1 degree polynomial that satisfies the equation f(0) = r_i.
- Every node shares their unique points with each other and also get the f(x) values computed by other nodes to compute F(x), which is the summation of all f(x) computations, and send to the gateway.
- Gateway uses the F(x) computations to compute a new polynomial called g(x). The constant term of g(x) gives the aggregation of the data supplied by n nodes.

2.7 ns-3

ns-3 is an open-source discrete-event network simulator that implements most of the major protocols in the TCP/IP protocol stack [316]. Ns-3 is chosen since it has been a widely used tool that can provide close-to realistic results with its rich protocol sets. Among these protocols, implementations of IEEE 802.11s also exist which makes it convenient to develop various AMI applications. It is C++ based and thus it is also very convenient to include well-known crypto libraries to be used in the implementations such as Paillier, FHE and AES.

2.8 Beaglebone Black

Beaglebone Black [Col13] is a compact board that aims to provide developers a low-cost and efficient development platform. Beaglebone Black comes with Debian operating system. It uses AM335x 1GHz ARM Cortex-A8 as its processor and it has 512 MB DDR3 RAM with 4 GB storage space. These properties make BBBs suitable for use as a SM simulator. The only thing missing in BBBs is a wireless adapter. Because of this, TP-Link TL-WN722N [TL16] wireless adaptors are used.

2.9 Raspberry Pi 3

Like BBB, Raspberry Pi [UH16] is another compact board solution that aims to give developers a sophisticated and low-cost development environment. In this thesis, the latest Raspberry Pi, Raspberry Pi 3, is used. What makes RP3 different than BBB is its specifications. Compared to BBB, RP3 comes with a more powerful components like 1.2GHz 64-bit quad-core ARMv8 CPU and 1 GB RAM. A microSD slot is also available for the developers which makes the storage of the board flexible depending on the storage capacity of the microSD card selected by the developer. Unlike BBB, RP3 comes with a wireless adaptor, but as it does not support mesh networking, TP-Link adaptors are used with RP3s, too.

CHAPTER 3

RELATED WORK

Due to their easy-to-deploy and self-healing features, wireless mesh networks attracted attention of people from both industry and academia. [AWW05] In most of these studies that focused on this topic, simulators were frequently used but a number of studies utilized real testbeds. [UIA11]

Although HWMP has a solid presence as the default routing protocol of WMNs, researchers think that there is still room for improvement for different aspects of HWMP. Security is also considered as an important property for HWMP. Security of routing and forwarding functionalities is not described thoroughly in HWMP specification; therefore, HWMP can be vulnerable to attacks. This vulnerability is targeted with different approaches in literature. SHWMP proposes extended security by suggesting cryptographic extensions [IHH09], while IBC-HWMP and Hash-HWMP discuss that security can be strengthened with identity-based cryptography or hashing [BOMB11].

Research done in literature that focus specifically on AMI Networks also prefer simulations rather than actual testbeds. Popular simulation tools used under this context is ns-3 and Matlab. Matlab is mostly used to do simulations on the security of AMI Network. In one of the studies done with Matlab, Vijayanand et al. [VDKK16] proposes a bit masking based data aggregation technique for secure data collection. ns-3 simulations are also used for testing secure data aggregation and obfuscation techniques [TCA$^+$16b, TASU16]. In addition to this, ns-3 is used to model AMI network to assess performance of wireless technologies like 802.11ah, WiMAX, and LTE in a Neighborhood Area Network [SGBP16]. Another work in literature that benefited from ns-3 focuses on the communication between data concentrator unit and AMI inside smart grid and evaluates the communication performance on different conditions [KPL16]. Although simulations are good tools to use for testing different conditions, their reliability is always questionable if they are not supported with an actual deployment or compared with one under same conditions.

The main focus of the actual deployed AMI testbeds is security and privacy issues in AMI Networks. For these issues, Qasim Ali et al. [AASD13] suggest randomization on AMI configurations. This randomization makes the behavior of AMI unpredictable, which makes it harder to analyze the network and attack it. In another study, a security analysis tool called SmartAnalyzer is proposed [RASB13]. Testbed deployed is used to assess the effectiveness of this tool against real attacks that can be done on AMI Networks. Data collection protocol of AMI Network is also investigated for improvements on the security of AMI Networks. In their work, Uludag et al. [ULRN14] introduce a new data collection protocol that is secure and efficient with the help of the developments in Machine-to-Machine communication techniques. One common thing about the testbeds mentioned above is the limited information about the components of the testbed, and how the testbed is created and deployed.

Security and privacy issues in AMI Networks are addressed in this thesis, too. A solution, that uses data aggregation with partial homomorphic encryption algorithm called Paillier and two-factor authentication (with OpenSSL certificates and ECDSA signatures), is proposed considering the previous research done in this field. As stated in its respective section in background information, what makes Paillier as the preferred homomorphic encryption algorithm to use in AMI Networks is its addition property with smaller message expansion factor, and security features compared to other algorithm options. [SA12, SA14] Another thing that can be noticed when the literature is surveyed is the amount of works that choose Paillier as the homomorphic encryption algorithm to use. [BHTS16, SZS17, MZKF15, TASU16]. This thesis differs from the other works that use Paillier by evaluating the performance of Paillier in both simulation and testbed environments. Another difference of this thesis is addition of two-factor authentication mechanism.

Unlike the aforementioned efforts, this thesis compares the performances of simulation and testbed solutions under similar conditions for different privacy-preserving protocols, and also give detailed information about the components used and the steps followed to deploy the two testbeds that are created. Additionally, the remote accessibility of the testbeds is another unique property of this work, which can attract more researchers into working on AMI networks.

CHAPTER 4

AMI TESTBED CREATION

4.1 Testbed Creation with Beaglebone Black

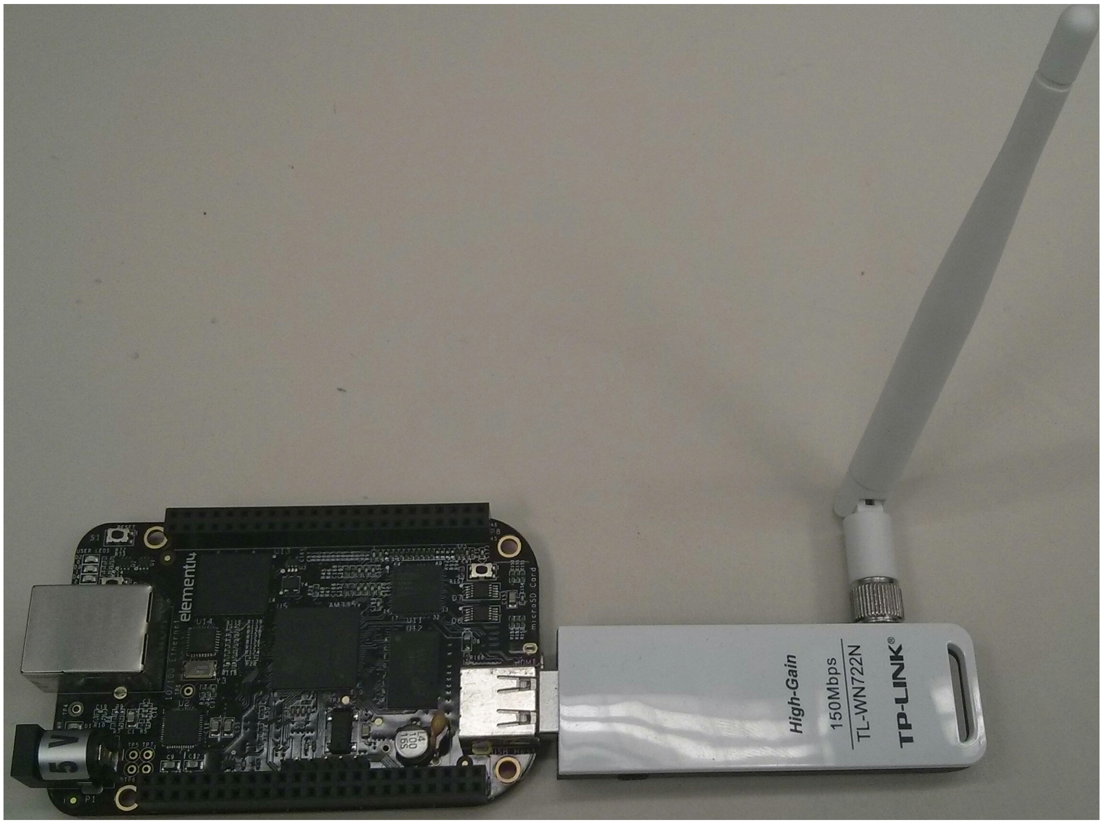


Figure 4.1: Beaglebone Black Board with the Wifi dongle

The creation of the testbed began after getting the BBBs and TP-Link TL-WN722N wireless adaptors (see Fig. 4.1). Firmware and drivers required for the adaptors are installed to the BBBs first with the following commands:

```
$ sudo apt-get install wireless-tools usbutils
$ sudo apt-get install firmware-atheros
```

BBBs were not able to support mesh networking with their initial configuration because of the kernel version (3.8) installed in them. Because of this, the kernel is upgraded to 4.1.15 on every BBB. Following commands are executed on the command line for the kernel upgrade (As kernel versions are always in development and new versions are published, following commands may return different revision or version numbers):

```
$ sudo apt-cache search linux-image | grep 4
$ sudo apt-get install linux-image-4.1.15-bone-rt-r18
$ sudo reboot
$ sudo apt-get update
```

The last step for mesh networking support on BBBs was the installation of the ’iw’ utility that is used for management of wireless interfaces in Linux systems. [IW16] JDK8 is also installed to compile and run the Java applications. These are installed with these commands:

```
$ sudo apt-get install iw
$ sudo apt-get install oracle-java8-installer
```

A laptop that runs Ubuntu 16.04 is also configured to be the gateway of the network.

After preparing the BBBs and the laptop, the 802.11s wireless mesh network is created. [o11] Linux operating system is further used in order to make the deployment of the testbed easier in case something happens to one of the nodes. Startup scripts that make devices join the mesh called ’FIUMesh’ and get an IP inside the subnet 10.1.1.0/24 and shell scripts that run the applications are also created and copied into all BBBs and the gateway with the help of Linux. One of the scripts used can be seen below:

```
#!/bin/bash
```

```
sudo killall NetworkManager
sudo ifconfig wlan0 down
sudo iw dev wlan0 interface add mesh type mp
sudo iw dev mesh set channel 11
sudo ifconfig mesh 10.1.1.3 netmask 255.255.255.0 up
sudo iw dev mesh mesh join FIUMesh
```

In order to run this script on startup, the first thing that is done is placing the script in /etc/init.d directory. After placing it into that directory, the script is made executable and then a symbolic link is created with the copy of the script named SXXmyscript in the /etc/rc3.d directory where SXX is the number of the last script in that directory with the following commands:

```
$ chmod 755 myscript
$ sudo ln −s /etc/init.d/myscript /etc/rc3.d/SXXmyscript
```

The "date" command of Linux is also used to synchronize the time of all devices in the mesh network as it will be needed for testing. [com17] Following command is executed before every test as time synchronization was critical for the tests done for performance evaluation:

```
$ sudo date −−set="$(ssh user@server date)"
```

4.2 Testbed Creation with Raspberry PI 3

RP3 testbed is deployed after the creation of BBB testbed, so it was easier to deploy with the documents created during the development of BBB testbed. Another thing that helped in the development was the better configuration of RP3 compared to BBB. TP-Link adapter is recognized automatically without the need of installing the drivers from the command line. Also, the Linux kernel that is placed on RP3s on default was already supporting mesh networking, so kernel of RP3 is not upgraded. The RP3 testbed is deployed after installing the iw and JDK and placing the scripts (the same scripts used for BBB with the change on IP addresses) that make RP3s automatically join the mesh network.

4.3 Securing the Testbed

After making sure that testbeds are working without problem, implementation of the security models started. The security model implemented initially were PHE with ECDSA signature authentication. [OTAS16] FHE and SMPC are developed afterwards. OpenSSL certificate authority (CA), certificate revocation list (CRL), and certificates are created in Linux and added to the security models in order to make the testbed more secure with two-factor authentication. [OTA16] Creation process started with the creation of root CA. Following commands are used to create the directory that store the files needed by the root CA, or will be created by the CA:

```
$ mkdir /root/ca
$ cd /root/ca
$ mkdir certs crl newcerts private
$ chmod 700 private
$ touch index.txt
$ echo 1000 > serial
```

Index and serial text files are used as a database that store the information of signed certificates. After creating the directory the configuration file called openssl.cnf is prepared. [ope] Root CA's key and certificate are created with the following commands:

```
$ cd /root/ca
$ openssl genrsa −aes256 −out private/ca.key.pem 4096
$ chmod 400 private/ca.key.pem
$ openssl req −config openssl.cnf \
              −key private/ca.key.pem \
              −new −x509 −days 7300 \
              −sha256 \
              −extensions v3_ca \
              −out certs/ca.cert.pem
$ chmod 444 certs/ca.cert.pem
```

In order to make sure that root CA is secure, second CA called intermediate CA is created. This CA is prepared with the purpose of signing created certificates on behalf of root CA so that root CA is kept secret and is not compromised. Like the root CA creation process, intermediate CA creation process also prepares the directories and files first, then openssl.cnf file is filled and intermediate CA's key is issued:

```
$ mkdir /root/ca/intermediate
$ cd /root/ca/intermediate
$ mkdir certs crl csr newcerts private
$ chmod 700 private
$ touch index.txt
$ echo 1000 > serial
$ cd /root/ca
$ openssl genrsa -aes256 \
    -out intermediate/private/intermediate.key.pem 4096
$ chmod 400 intermediate/private/intermediate.key.pem
```

Next step for intermediate CA is issuing a certificate signing request so that it can be signed by the root CA to sign certificates on root CA's behalf:

```
$ cd /root/ca
$ openssl req -config intermediate/openssl.cnf \
      -new -sha256 \
      -key intermediate/private/intermediate.key.pem \
      -out intermediate/csr/intermediate.csr.pem
```

Then, root CA can sign the intermediate CA's certificate:

```
$ cd /root/ca
$ openssl ca -config openssl.cnf \
         -extensions v3_intermediate_ca \
         -days 3650 -notext -md sha256 \
         -in intermediate/csr/intermediate.csr.pem \
         -out intermediate/certs/intermediate.cert.pem
$ chmod 444 intermediate/certs/intermediate.cert.pem
```

When both CAs are ready, CRL can be created for the storing the revoked certificates:

```
$ cd /root/ca
$ openssl ca -config intermediate/openssl.cnf \
      -gencrl -out intermediate/crl/intermediate.crl.pem
```

Contents of the CRL can be checked using the following command:

```
$ openssl crl \
        -in intermediate/crl/intermediate.crl.pem \
        -noout   text
```

After getting everything ready, certificates can be created and signed with these commands:

```
$ cd /root/ca
$ openssl genrsa -aes256 \
  -out intermediate/private/www.example.com.key.pem 2048
$ chmod 400 intermediate/private/www.example.com.key.pem
$ openssl req -config intermediate/openssl.cnf \
  -key intermediate/private/www.example.com.key.pem \
  -new -sha256 \
  -out intermediate/csr/www.example.com.csr.pem
$ openssl ca -config intermediate/openssl.cnf \
  -extensions usr_cert -days 375 -notext -md sha256 \
  -in intermediate/csr/www.example.com.csr.pem \
  -out intermediate/certs/www.example.com.cert.pem
$ chmod 444 intermediate/certs/www.example.com.cert.pem
```

Implementation of the security models are done using the Java (Paillier and SMPC) and C (FHE) programming language. During the testing of the model, BBBs and the gateway are placed to the different spots in Advanced Wireless and Security (ADWISE) Lab at Florida International University, which is a 12-by-12 office room (see Fig. 4.2). Same placement is done for RP3s, too.

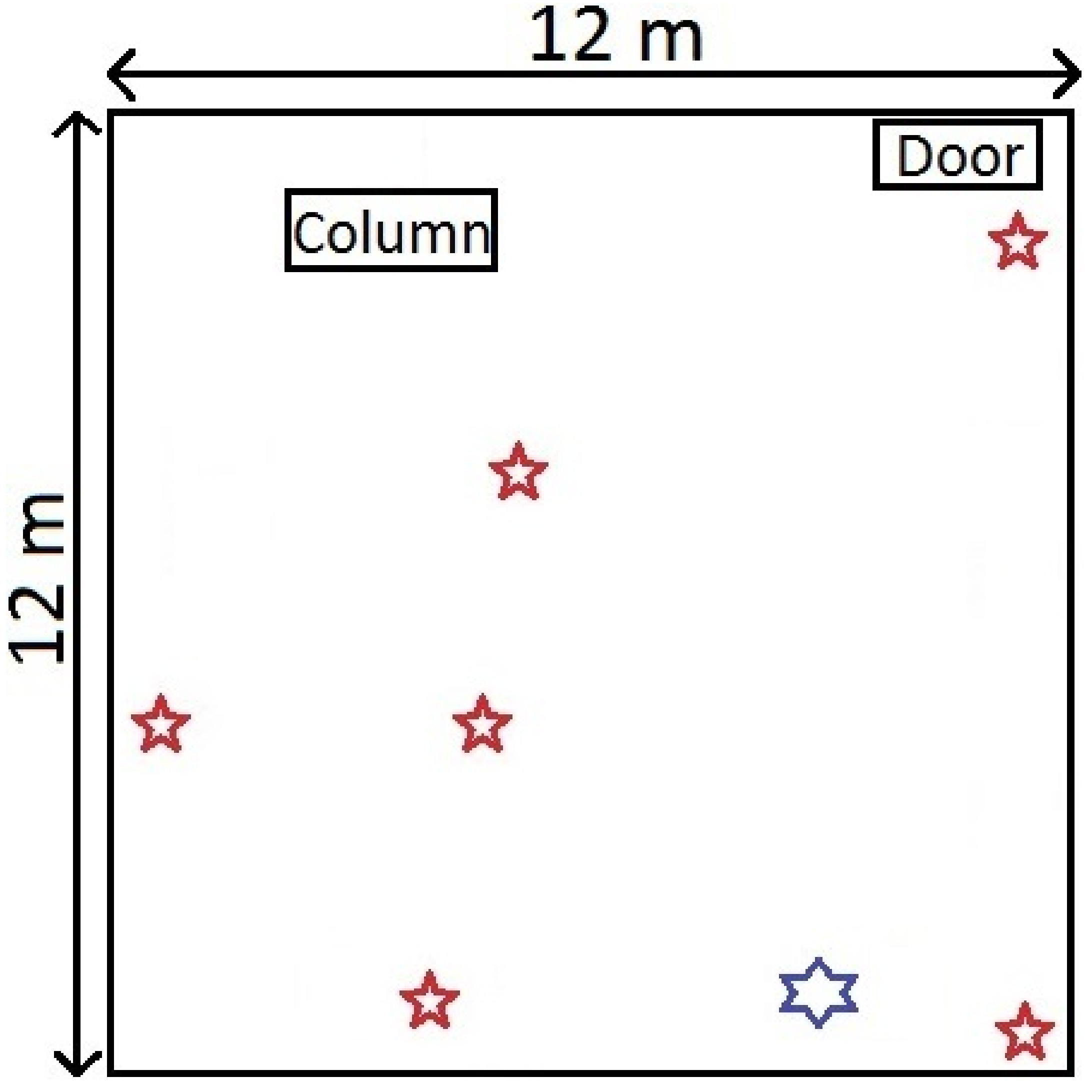


Figure 4.2: The layout of the lab which hosts the testbed.

4.4 Remote Access Setup for the Testbed

Remote access to the testbed is provided with a website. [ami] Users who are interested in using the testbed can do it by signing up for an account on the website's Sign Up page. The server that website resides is used as the gateway of the mesh network so users can access to the meters available in the network by using the interface available on the website.

CHAPTER 5

PERFORMANCE EVALUATION OF THE SECURE TESTBED

5.1 Baselines

Since one of the goals of this work is to assess the performance of AMI related privacy-preserving protocols, in addition to Paillier, SMPC and FHE, two other baselines are also implemented: 1) Plaintext; and 2) AES-based Encryption. This was done because of the difference in message overheads (can be seen in Table 5.1), and the difference in message exchange method as AES, FHE, SMPC, and Paillier do the exchange with ciphertexts and Paillier and FHE also do the aggregation on ciphertexts. The use of TCP and UDP protocols is also considered as speed is utmost concern in AMI applications. Consequently, six different approaches are implemented. Implementations for TCP and UDP applications are done in a multi-threaded client-server fashion and they were written as similar as possible in order to minimize the affect of implementations on the results.

Table 5.1: Message overhead for plaintext, 256-bit AES, Paillier, SMPC, FHE and ECDSA

Message size (in bits)	
Plaintext	16
256-AES Ciphertext	128
Paillier Ciphertext	2048
ECDSA Signature	568
FHE	more than 100000
SMPC	256

5.2 Performance Metrics

For performance evaluation, following metrics are used:

- *Packet Delivery Ratio (PDR):* The ratio of the packets that are received by the gateway to the number of packets sent to the gateway.
- *Throughput (TP):* The total data (in Kb) received by the gateway per second.
- *Average Completion Time (CT):* Average elapsed time for receiving all data from the gateway in one round. Measured at the application layer so that it takes into account the cryptosystem operations.

5.3 Performance Evaluation of Paillier with ECDSA

The first test is done to evaluate the initial privacy-preserving protocol that uses Paillier with only ECDSA signatures. PDR, TP and CT results of the first test can be seen in the next subsections.

5.3.1 PDR Results

As seen in Fig. 5.1, the PDR values for HbyH aggregation mode are 50% because of aggregation within the network. However, the values for UDP are slightly below 50%. This means there are a few lost packets which were not retransmitted because UDP does not have a retransmission mechanism whereas TCP can retransmit a lost packet. In EtoE aggregation mode, the TCP PDRs are all 100% while those for UDP are below 90%. The ratio of the lost packets increases in EtoE aggregation mode because the number of packets in the network at the same time increases. Since the meters send their data packets at the same time and at the same frequency, wireless radio frequency interference occurs and the packet(s) are lost.

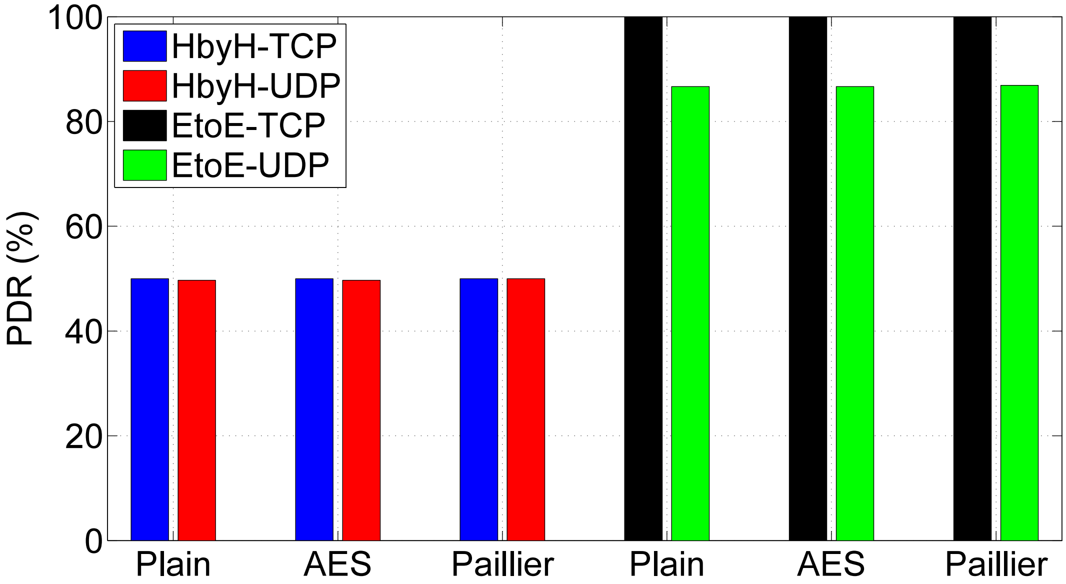


Figure 5.1: The simulation PDR results for the first test.

When we look at the results on the testbed, we see that the PDR results follow a very similar trend as in the case of ns-3 simulations. The only exception is the UDP behavior, especially under AES. The results in Fig. 5.2 indicate that in real-life UDP can achieve better PDR, but it still does not guarantee 100% delivery as in the case of TCP.

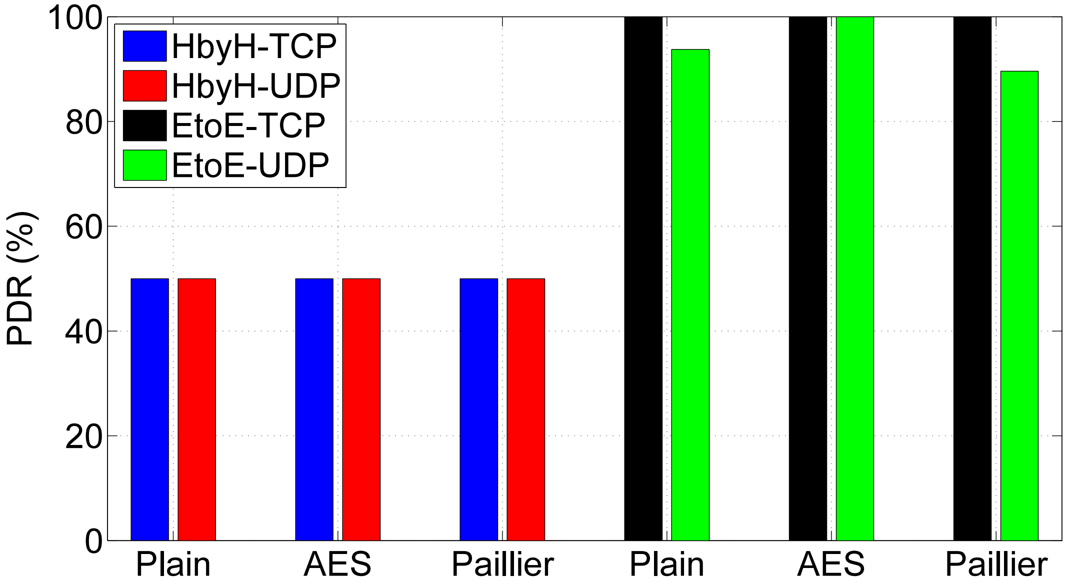


Figure 5.2: The testbed PDR results for the first test.

5.3.2 TP Results

The TP values increase as the size of the data packet transmitted increases. The values for EtoE aggregation mode are relatively higher than those for HbyH aggregation mode because the number of the data packets received by the gateway meter is threefold of the number of the data packets received by the gateway meter in EtoE aggregation mode. In EtoE aggregation mode, the values for UDP is lower than those for TCP due to lower PDR.

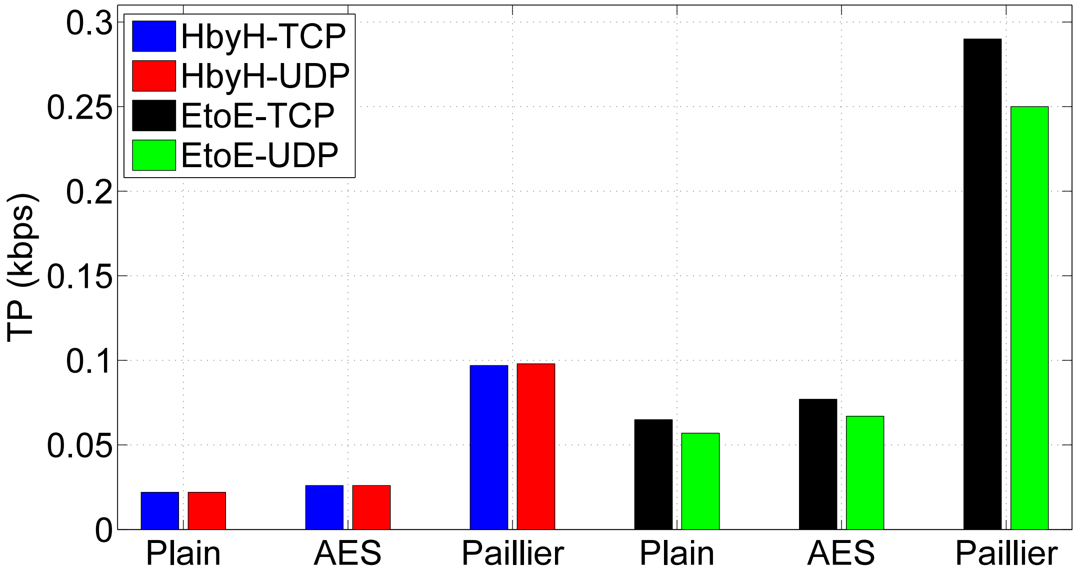


Figure 5.3: The simulation TP results for the first test.

The discrepancy in case of PDR was minor. When we check the results for TP and CT, major discrepancies can be observed between the testbed and ns-3. For instance, for TP, TCP performs poorly compared to UDP which is very surprising. In particular, the gap is huge when Paillier is used. This can be partially attributed to lower communication and processing delays in UDP which gives way to process more packets.

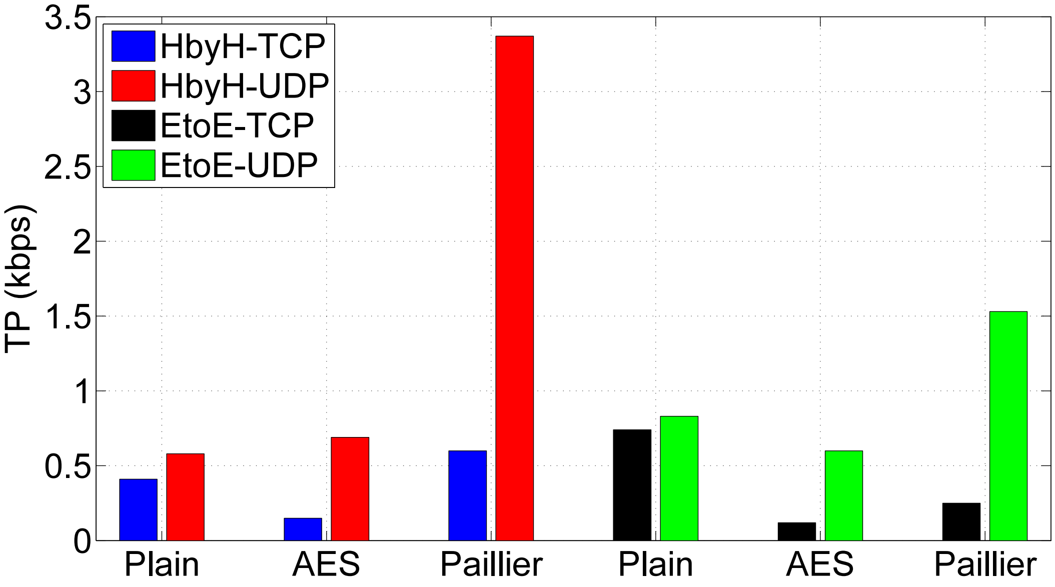


Figure 5.4: The testbed TP results for the first test.

5.3.3 CT Results

For the CT, overall, HbyH approach performs better given that there will be heavy computation at the gateway for the EtoE approach. In addition, this can also be attributed to the fact that the number of the meters that want to have access to the channel. As the number increases the number of the collisions increases. This increases the back-off time for the next channel access try and so the overall delay.

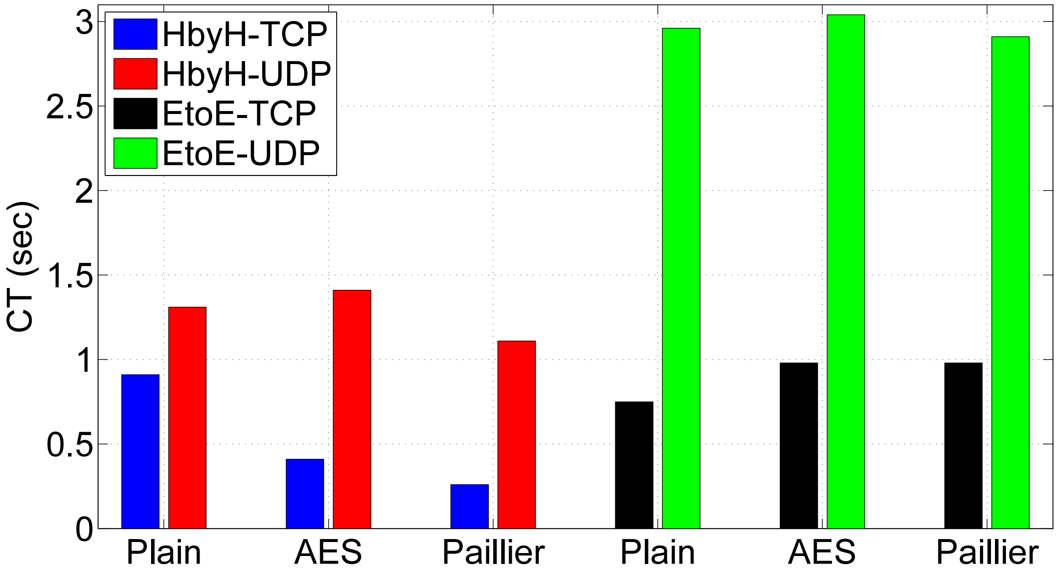


Figure 5.5: The simulation CT results for the first test.

The CT values also show very interesting results. For instance for EtoE mode, while simulation shows good performance with TCP, the testbed indicates that the performance difference is not major. On the other hand, in the HbyH mode, UDP is better in simulations while it performs worse in testbed. These are conflicting results. There can be many speculations. One reason might be the limited computational capabilities of the BBBs. For instance, in HbyH there will be more computations at intermediate nodes running TCP due to its overhead and aggregation. The computer conducting simulations may have more resources than the BBBs which makes UDP perform better in the testbed.

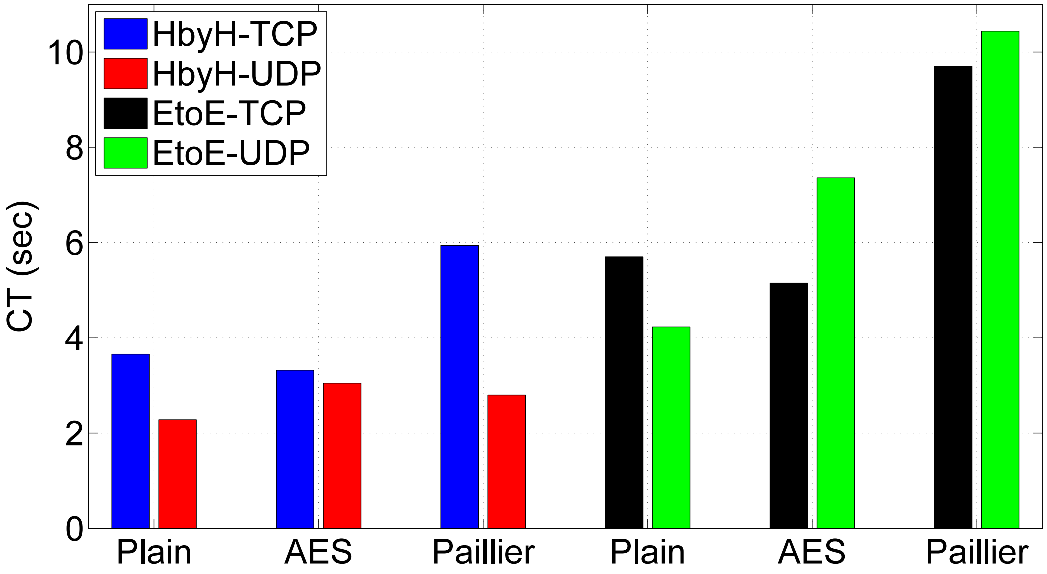


Figure 5.6: The testbed CT results for the first test.

Another speculation might be on the nature of TCP streaming process. Specifically, TCP will try and buffer the data and fill a full network segment thus making more efficient use of the available bandwidth. UDP on the other hand puts the packet on the wire immediately thus increasing the contention delay with more packets in the channel. For the testbed, the limited resource at the intermediate nodes will limit the TCP capabilities and thus the difference between UDP and TCP is not as large as the simulation case.

5.4 Performance Evaluation of Paillier with Two-Factor Authentication using ECDSA and OpenSSL Certificates

After reviewing the results of the first test, further investigation is done on the testbed and simulation implementations in order to find the cause of the discrepancies observed in the first test. Both implementations are edited to make them more consistent with each other and bug-free. Authentication mechanism is also improved by adding OpenSSL certificates to create a two-factor authentication system that is hard to break than a single authentication mechanism. Second test is done right after these developments. Results of this test are presented in the next subsections.

5.4.1 PDR Results

As seen from Figures 5.7 and 5.8, PDR results are almost the same for both testbed and simulation results. PDR values are 50% for all results collected in HbyH mode, 100% for all results collected in EtoE mode and TCP (except for testbed Paillier result), and around 85-86% for all results collected in EtoE mode and UDP. Around 85% PDR results for EtoE UDP reminds the connectionless nature of UDP and question the reliability of it in a SG AMI network.

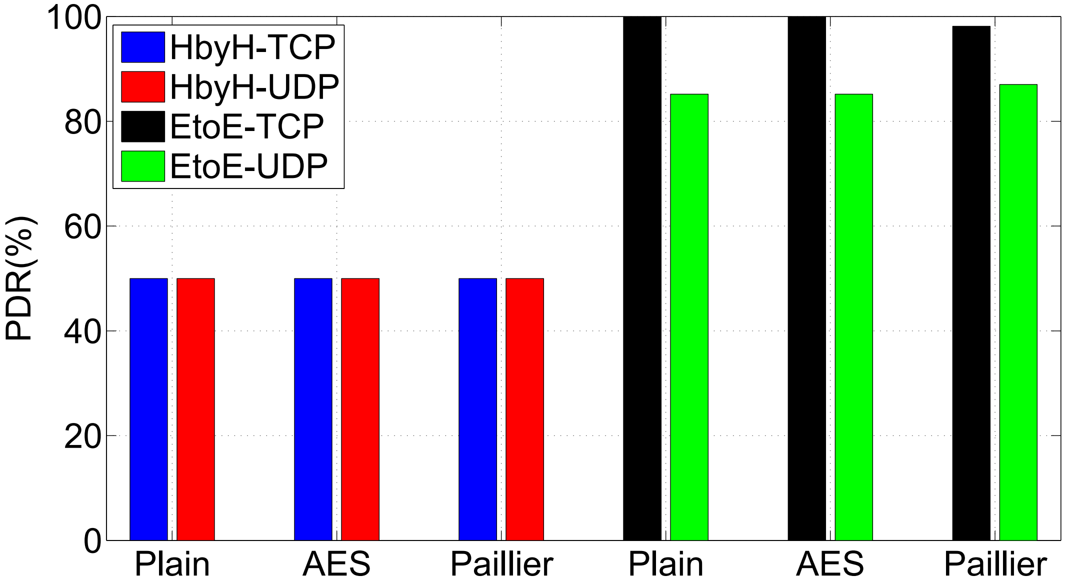


Figure 5.7: The testbed PDR results for the second test.

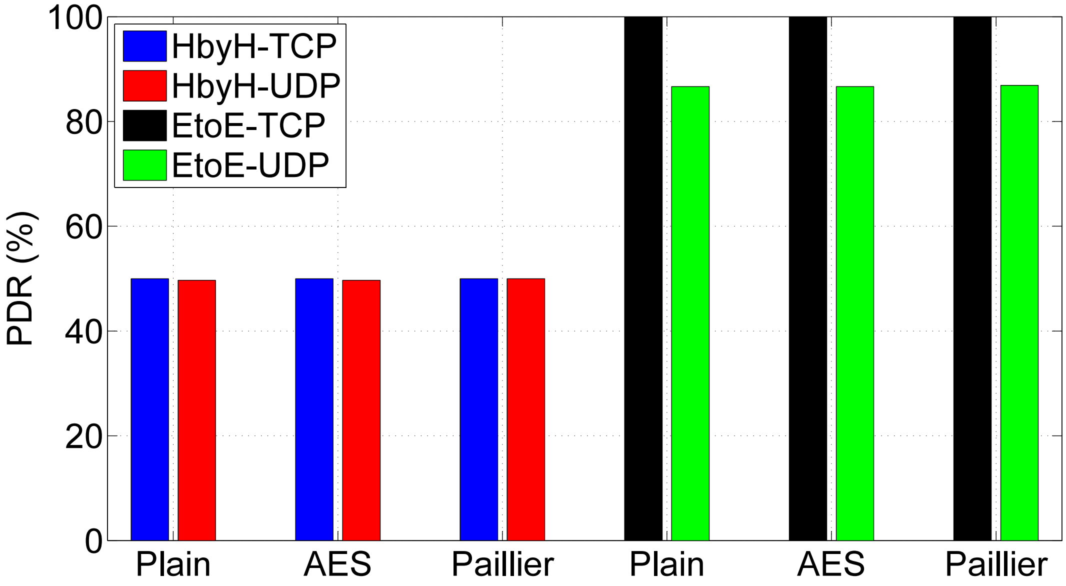


Figure 5.8: The simulation PDR results for the second test.

5.4.2 TP Results

The trend in the PDR results is also followed by the TP results. The simulation and testbed results are very similar to each other. For HbyH mode, it can be seen that TP results are really close for UDP and TCP cases with Paillier having the highest throughput followed by AES and plaintext. This result is reasonable since Paillier sends the biggest message by size, whereas message sizes for AES and plaintext are close to each other. The close performance of UDP and TCP shows that TCP is able to utilize the channel effectively with small number of collisions and back-offs which give enough advantage for it to be able to compete with UDP. For EtoE mode, Paillier again provides the highest throughput with TCP and UDP as expected.

There are conflicting results between the simulation and the testbed. For instance, for Paillier, the simulation and the testbed results are not matching. Since TCP packets have additional overhead, it may be reasonable to assume that TCP

TP will be higher, which is the case in the ns-3 simulation. However, for the testbed, UDP TP is higher. One possible explanation could be regarding the ending time of the experiments. It is possible that when the experiment is stopped, TCP is still in the process of re-transmitting some of the lost packets. Those will eventually come to increase the TP. However, this may also be the case for ns-3. Therefore, there may be differences in the parameter settings for the TCP back-off mechanism in the simulation and testbed.

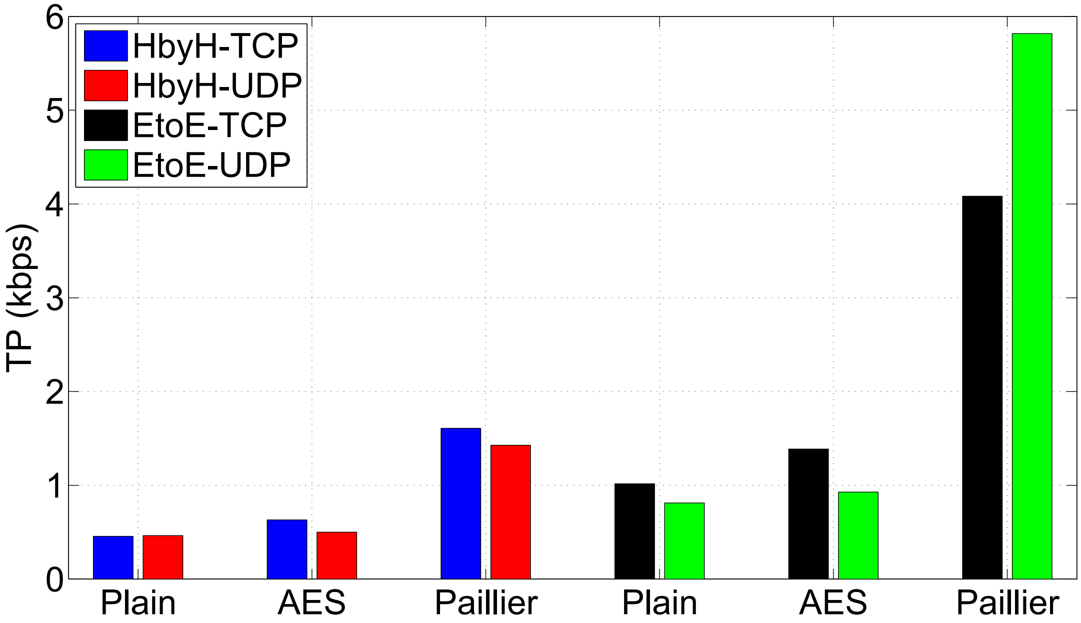


Figure 5.9: The testbed TP results for the second test.

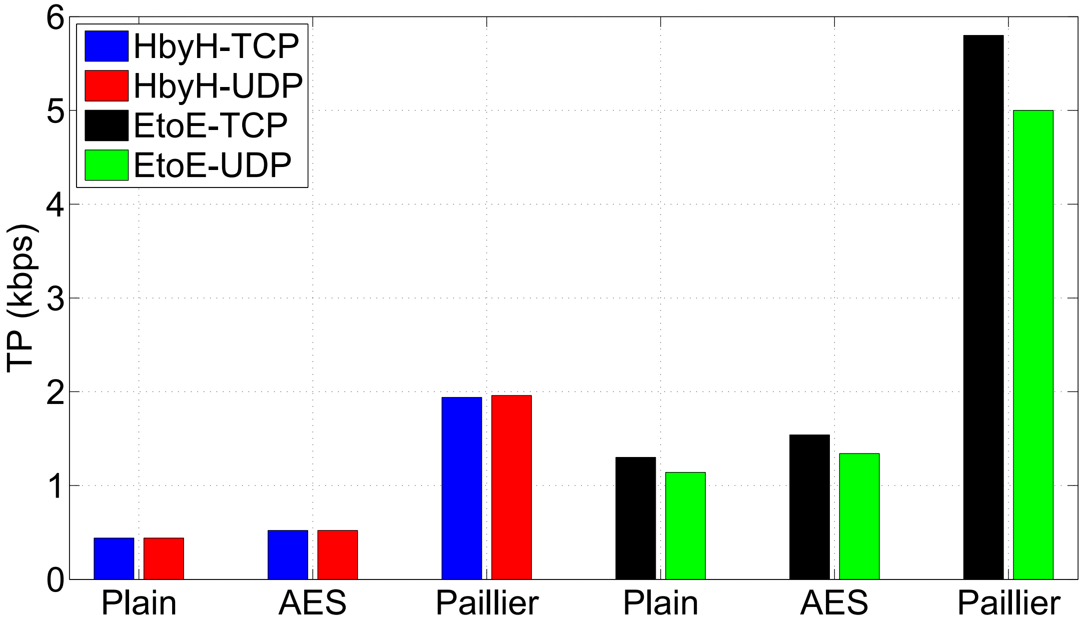


Figure 5.10: The simulation TP results for the second test.

5.4.3 CT Results

The most interesting results among all the tests are the CT results since they show a lot of differences in simulation and testbed results. Almost all the results are conflicting with respect to testbed and simulation as seen in Fig. 5.11 and 5.12.

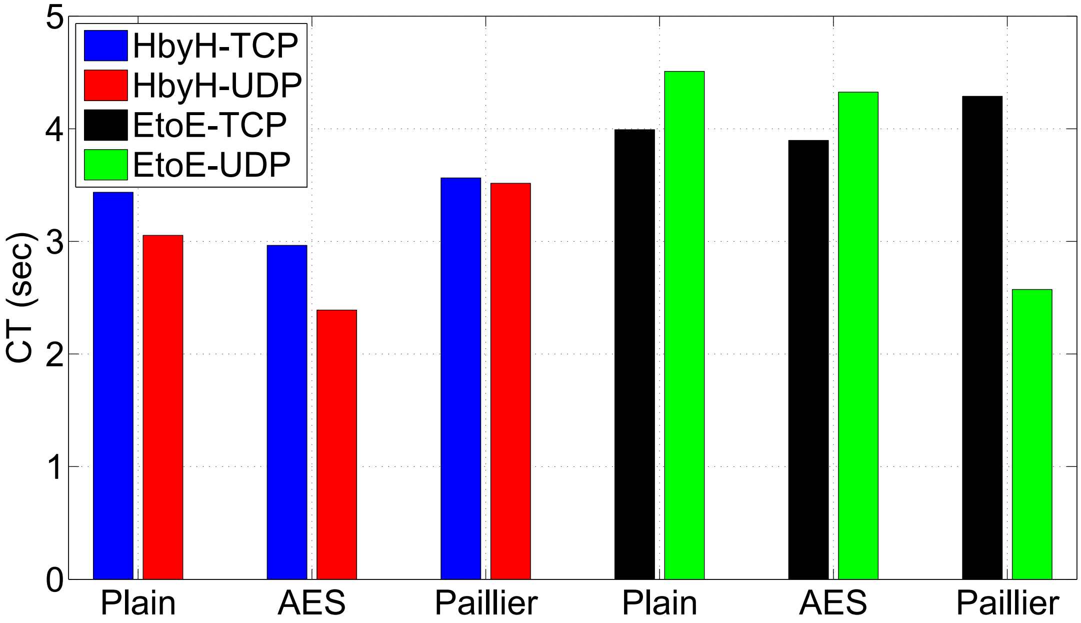


Figure 5.11: The testbed CT results for the second test.

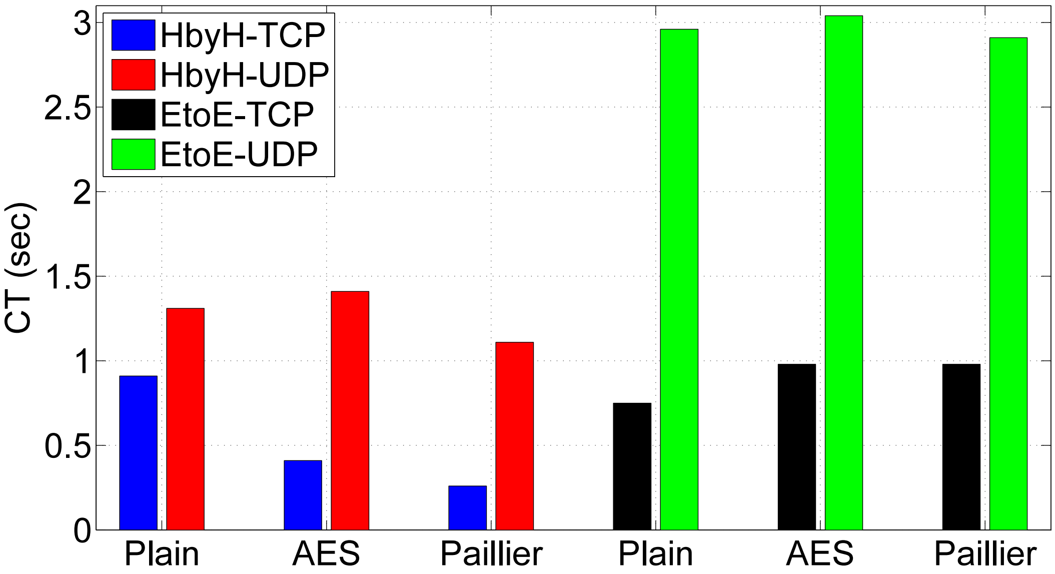


Figure 5.12: The simulation CT results for the second test.

For instance, ns-3 favors TCP over UDP in terms of CT in all approaches. This is unusual as there is a connection establishment phase for TCP and ACK messages as an overhead. In fact, the testbed results show the opposite and favors UDP in most cases, which is making more sense. For TCP there is an advantage of buffering since it can create a stream of bytes. In this way, there will be an implicit aggregation where it acts as a streaming protocol and thus in some cases it can buffer packets and reduce the number of transmissions in the network. This eventually reduces the delay in some rounds of data collection. The results show that ns-3 does a better job in terms of configuring the network for improved results. However, obviously its ability to capture the channel characteristics are limited compared to a real-testbed. It assumes an open space propagation model. This might be the reason that it performs much better in terms of CT than the testbed (simulation CT is in the orders of 1-2 secs while testbeds are at least 3secs).

The other problem is with AES and Paillier performing better than the plaintext case in ns-3. The overhead of processing at the intermediate nodes seem to give some advantage to these approaches in terms of keeping the channel less busier. While the testbed results are more meaningful in the sense that the CTs are close to each other in HbyH mode, this still does not explain why AES is better than the plaintext case.

To analyze this further, the data collection period is increased to 120 secs to see if this has any effect on the performance of the testbed. The results shown in Fig. 5.13 and Fig. 5.14 indicate minor effect for TCP but major for UDP. Since there is less overlap among different periods, this helps EtoE approaches reduce their CTs. However, the AES vs plaintext case still holds with TCP.

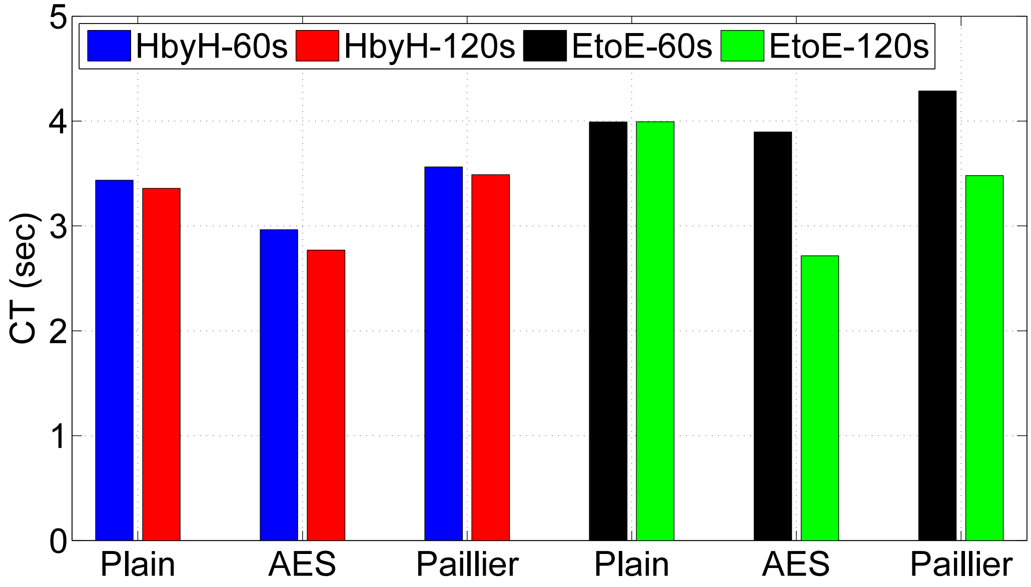


Figure 5.13: Comparison of testbed CT results for TCP under different data collection periods.

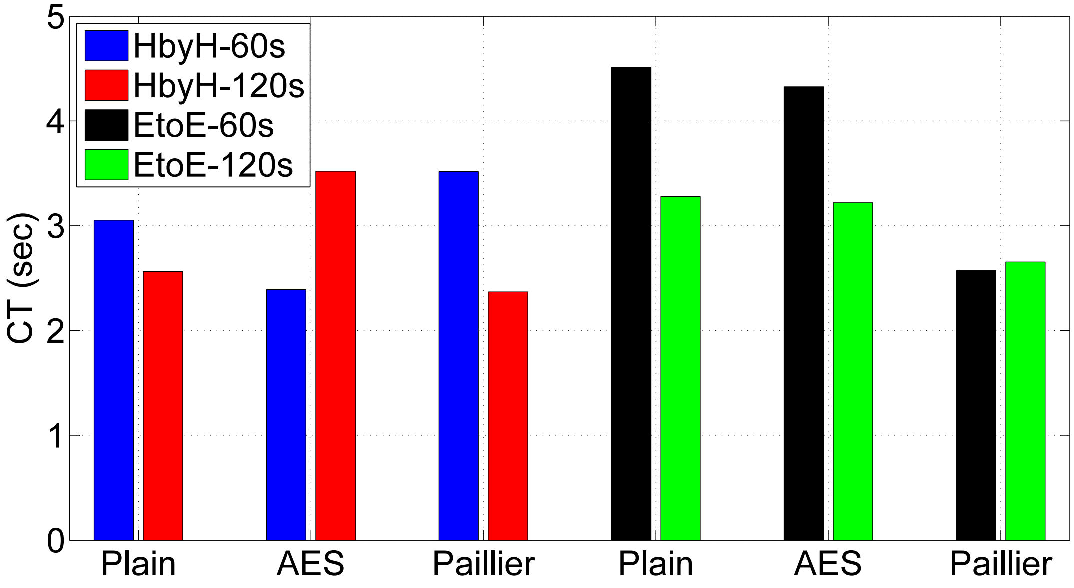


Figure 5.14: Comparison of testbed CT results for UDP under different data collection periods.

5.5 Performance Evaluation of improved Paillier with Two-Factor Authentication

After seeing that there are still discrepancies that needs solving, implementations are checked again considering the possible explanations that are discussed. AES and Paillier algorithms are examined together with the Java applications. Improvements are done to make these algorithms and the application work smoothly. Third test is done afterwards. Results can seen on sections 5.5.1, 5.5.2, and 5.5.3.

5.5.1 PDR Results

PDR results can be seen on Figures 5.15 and 5.16. As expected, TCP results are always 100% for EtoE, and 50% for HbyH modes. The percentage values are different for UDP. On HbyH mode cases, PDR values for UDP range from 38-44% which means that in every test there was a packet loss in at least one of the rounds. Another thing that can be noticed from the testbed results is that PDR values of UDP on HbyH mode follow pattern. Highest PDR value is achieved on plaintext (the case with the smallest packet size) case and lowest PDR value is achieved on Paillier (the case with the biggest packet size) case. This result can be a sign that there is a relation with the packet size and probability of losing that packet. The mentioned pattern is not observed in UDP EtoE mode cases. PDR results range from 90-100% and AES achieves the highest result and breaks the pattern. Also, lowest result is achieved by plaintext eliminating any packet size-packet loss probability relation possibility as mentioned after reviewing the HbyH mode cases' results.

Simulation results are very similar with the testbed results for the EtoE mode cases, but there are differences for the HbyH mode cases. Simulation results show that PDR is 50% for all HbyH UDP cases, which means no packet loss during the rounds. The fact that packet losses occurred on all HbyH mode cases for UDP can point to another weakness of simulations, which is the real-life conditions.

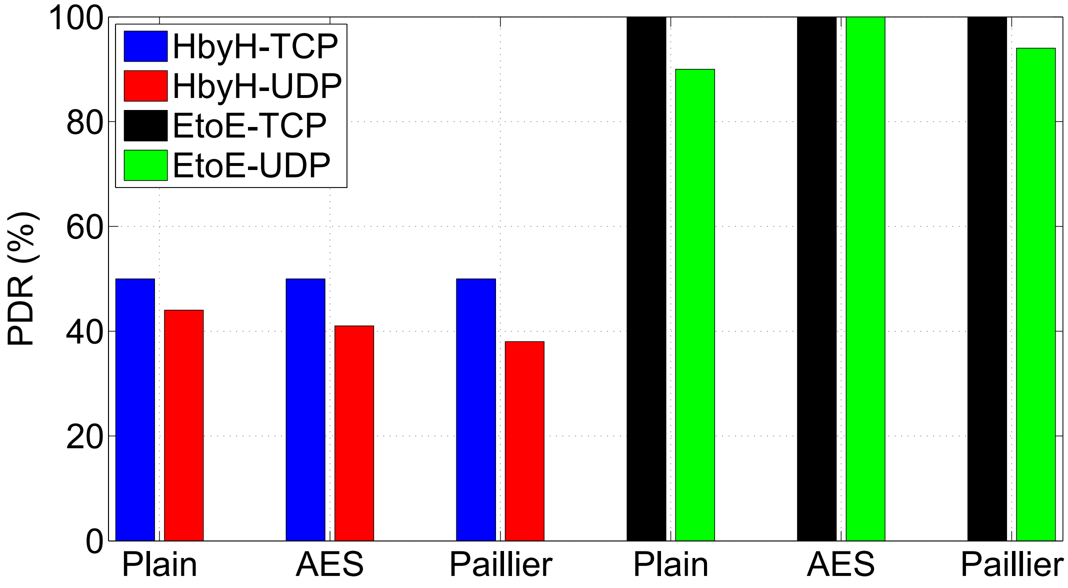


Figure 5.15: The testbed PDR results for the third test.

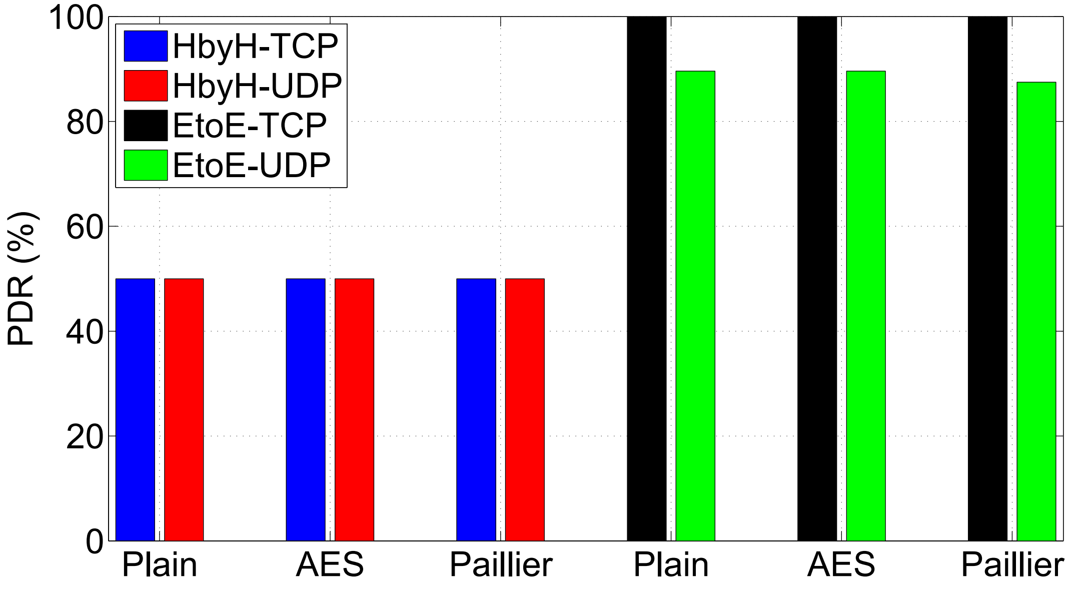


Figure 5.16: The simulation PDR results for the third test.

5.5.2 TP Results

TP results can be seen on Figures 5.17 and 5.18. As packet sizes of AES and plaintext are close to each other, TP results of these cases are also close. With its big packet size, TP results of Paillier are always the highest. Because of the packet losses for almost all cases, UDP values are smaller than TCP values with a small margin.

Simulation TP results are very close to the testbed results on TCP cases as packet size of the data sent is very close for both setups and there is no packet loss. For UDP, packet loss ratios are different for the setups. Because of this, results are not as close as the TCP results. Still, the patterns are same with the testbed results.

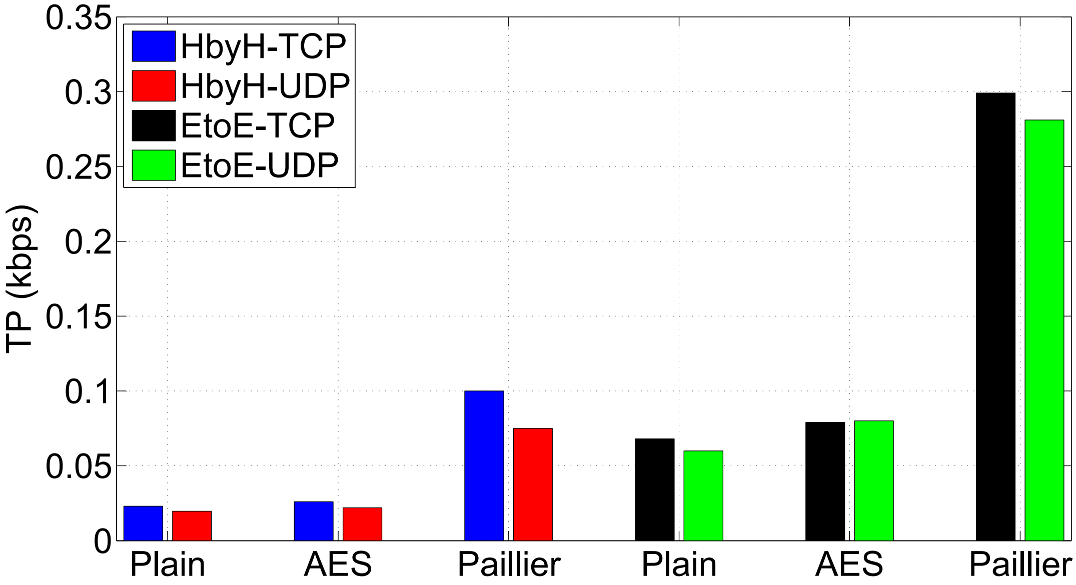


Figure 5.17: The testbed TP results for the third test.

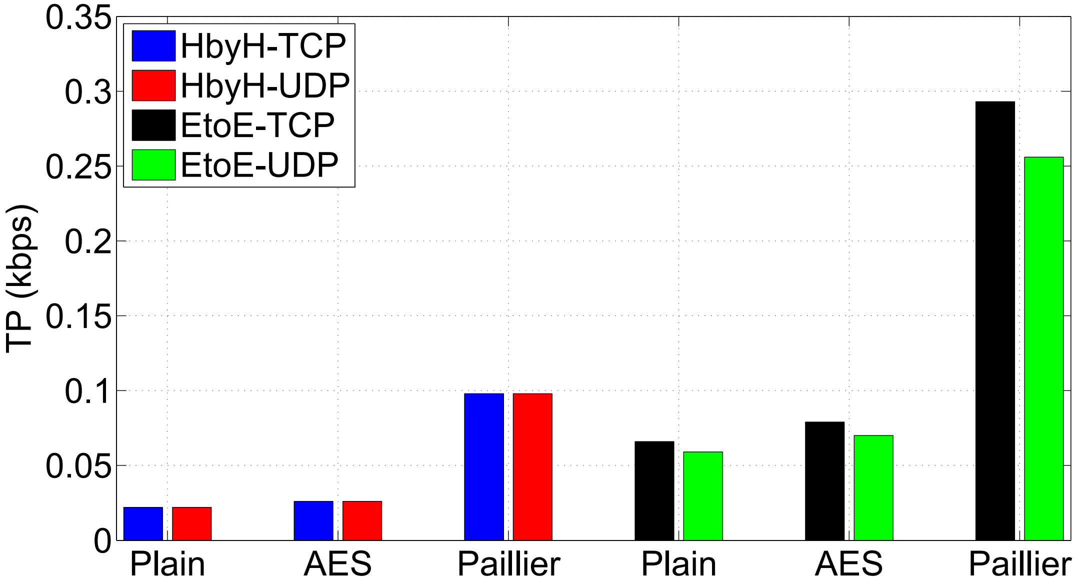


Figure 5.18: The simulation TP results for the third test.

5.5.3 CT Results

Among the previous two tests' results, CT results were the results with the most discrepancies. CT results of this test can be seen on Figures 5.19 and 5.20. Considering the testbed results, it can be said that these results are the most consistent one among the three tests' results. In all cases, TCP performs better than UDP for testbed results. This was the case for the previous test's simulation results. In the discussion of the second tests' results, it was speculated that TCP's buffering capability can be the reason for its speed. The new results gathered from the testbed support this speculation. Another consistent result that can be seen on the testbed results is that AES and Paillier cases' performance against the plaintext case. Normally, the expected result for this comparison would be plaintext case beating the other two as no encryption operation is done and packet size is smaller for plaintext case, but results show the exact opposite. The reason behind these results can be the utilization capabilities of both protocols. As bandwidth of the channel is big enough, these protocols can benefit from it and utilize even if the packet size gets bigger. In order to verify this claim, a small mesh network is set up to test TCP and UDP's performance under different packet sizes. Two different network sizes (1 BBB and laptop, 3 BBBs and laptop) and four different packet sizes (2, 100, 1024 and 10000 bytes) are used for this test. Delay results of this test can be seen on Figures 5.21 and 5.22. These results show that packet size doesn't have any effect on TCP and it affects UDP only after packet size gets huge. Considering these results, it can be said that it is possible to get better performance from encrypted systems as packet size is not a big factor, and encryption operations doesn't have a huge effect on the CT.

Unlike the testbed results, UDP performs better than TCP for all cases with a small margin in simulation results. Another difference is the mode performance. For simulation, HbyH performs better than EtoE mode. Other than these differences, simulation and testbed results are very similar to each other with AES and Paillier performing very close to plaintext in all cases. The reason for the differences mentioned about can be the channel configuration of ns-3. For EtoE and TCP to be faster, higher bandwidth is required. The testbed results show that in real life conditions this is possible as EtoE and TCP are faster than HbyH and UDP respectively. Considering this, it can be said that the channel configuration of ns-3 may need a revision to simulate the real life conditions.

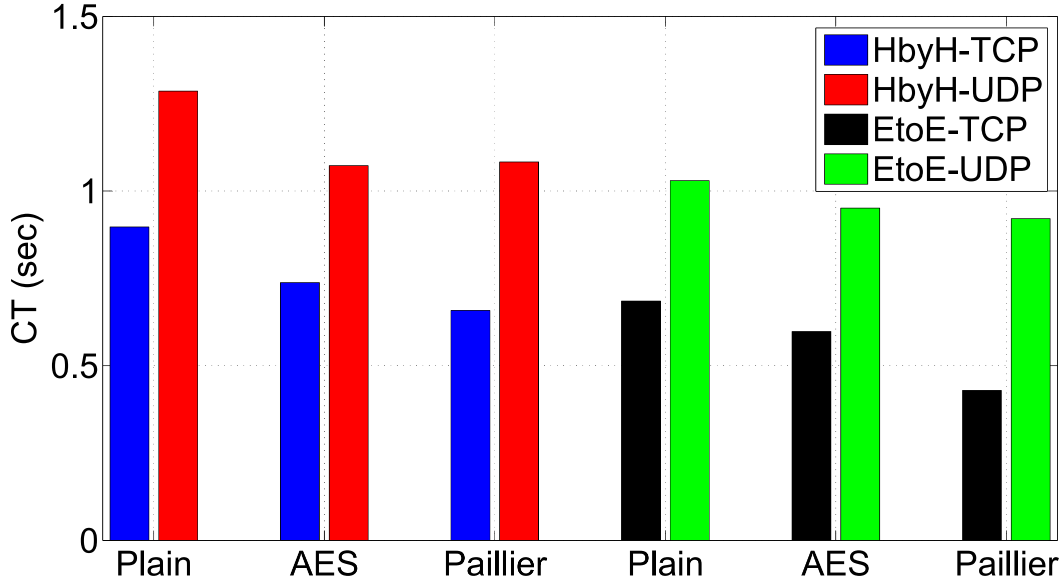


Figure 5.19: The testbed CT results for the third test.

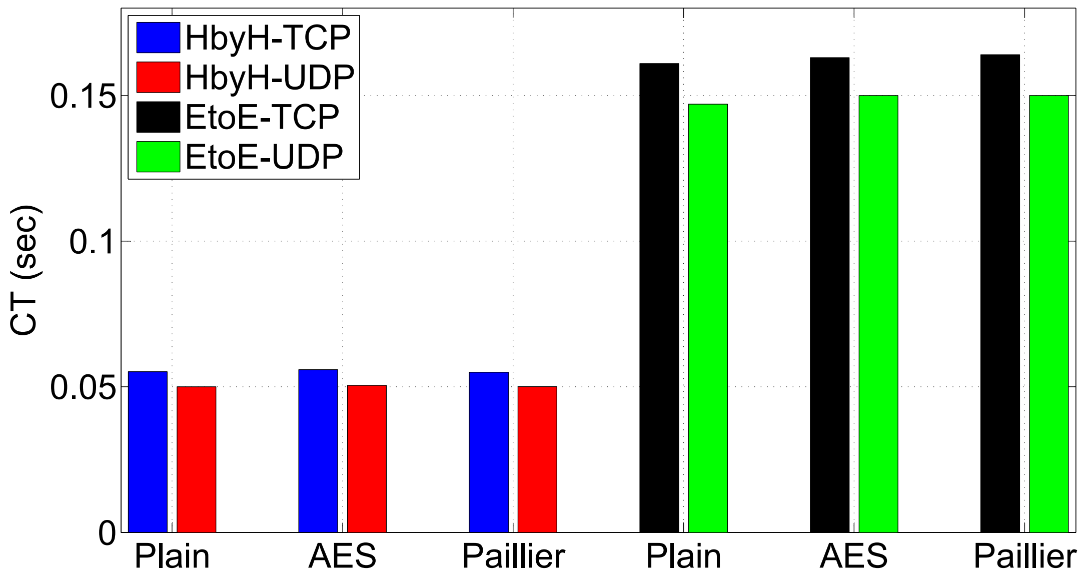


Figure 5.20: The simulation CT results for the third test.

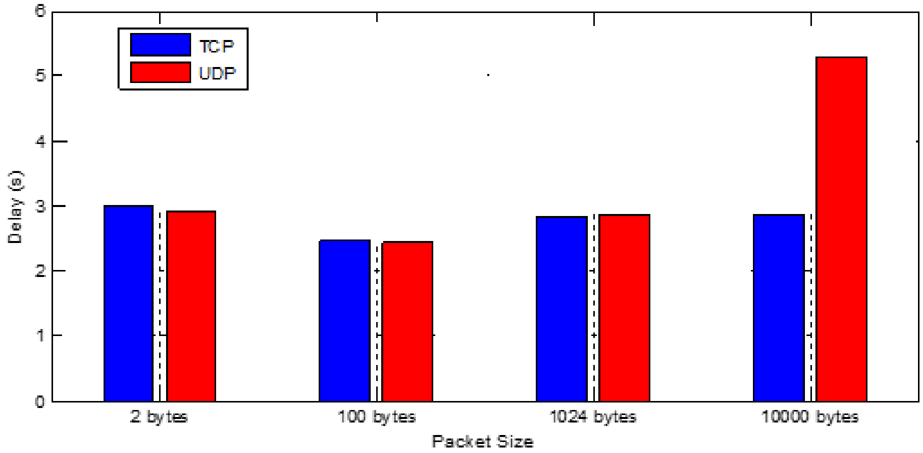


Figure 5.21: CT results for 1 BBB case

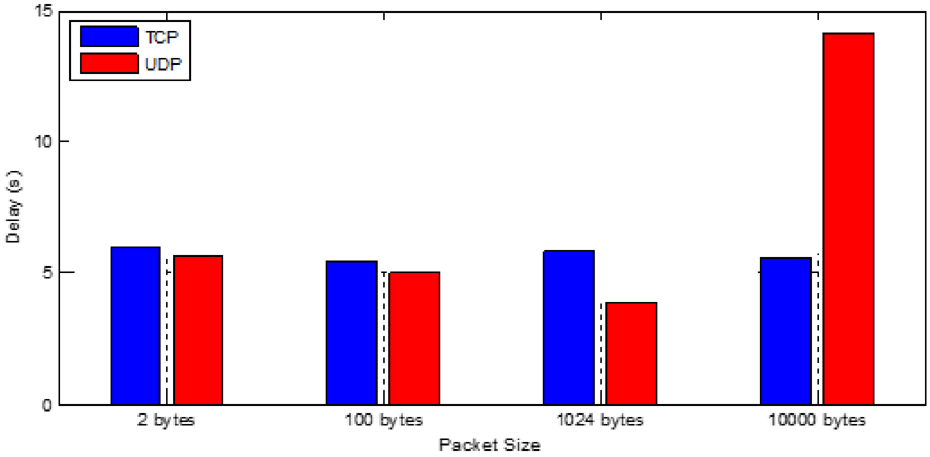


Figure 5.22: CT results for 3 BBBs case

5.6 Performance Evaluation of Paillier with Two-Factor Authentication and Gateway switched from Laptop to Beaglebone

The main problems that are faced in the previous tests were the mode and protocol performance differences in the testbed and the simulation results. In the discussion of the results, it was stated that this may be because of the channel configuration of ns-3 simulator. In order to check if this claim is true, a new test is prepared. The laptop that is used as the gateway for the testbed is a device much more sophisticated than a BBB. On the testbed, when EtoE mode is used, laptop does the aggregation operations. Whereas, when HbyH mode is used, intermediate BBBs are responsible for these operations. Because of this, in order to be fair with the simulation results and support the claims made in the previous section, for this new test, a new BBB is used as a gateway instead of the laptop used in the previous tests.

5.6.1 PDR Results

PDR results can be seen on Figures 5.23 and 5.24. As major discrepancies were not observed in the previous PDR results, we were expecting a similar result in terms of PDR for this test, and that was the case for this test. Only difference with the previous results was the PDR results of UDP cases. The switch from laptop to BBB causes the PDR values to drop to around 45% for TCP and 80% for UDP. This is different from the simulation results that show 50% for TCP and 90% for UDP as PDR results. This can be another proof to show that the ns-3 configuration is not accurate on channel characteristics.

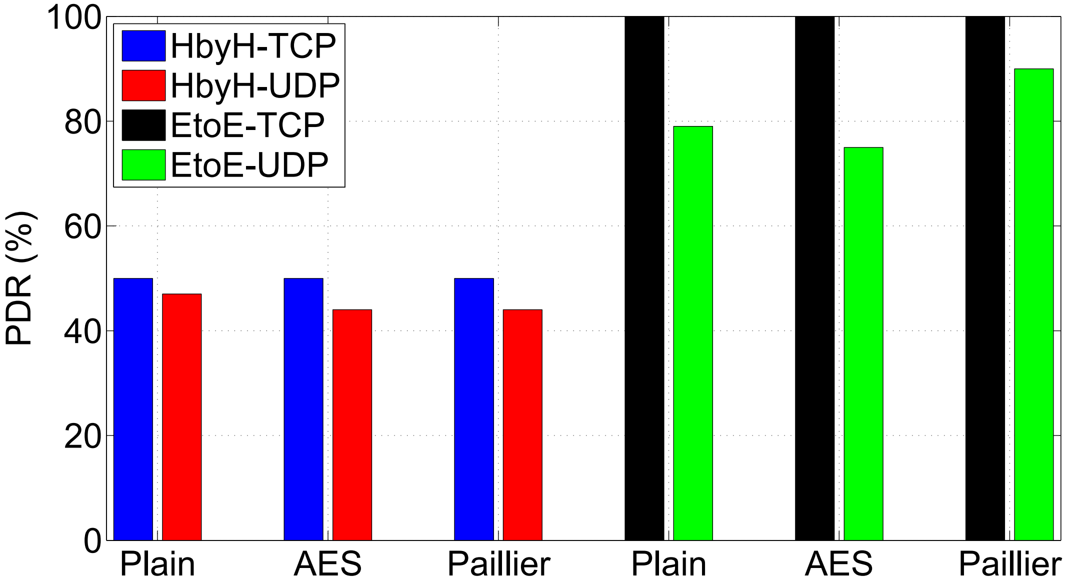


Figure 5.23: The testbed PDR results for the fourth test.

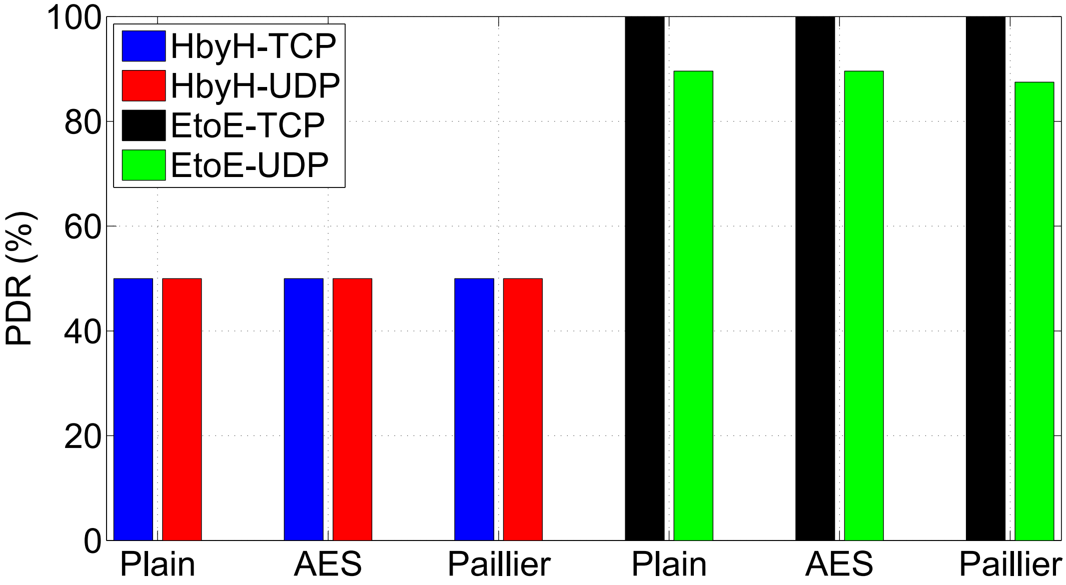


Figure 5.24: The simulation PDR results for the fourth test.

5.6.2 TP Results

TP results can be seen on Figures 5.25 and 5.26.Like PDR, TP results were also very similar. Only difference is UDP TP results. As there were more packet drops for the testbed case than the simulation case, UDP TP results are little lower than the simulation.

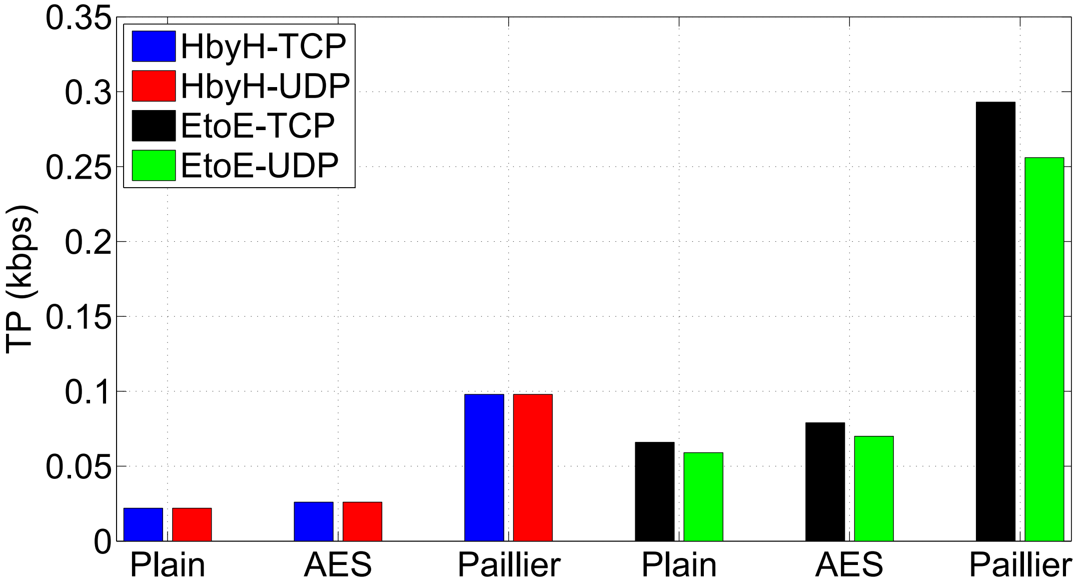


Figure 5.25: The simulation TP results for the fourth test.

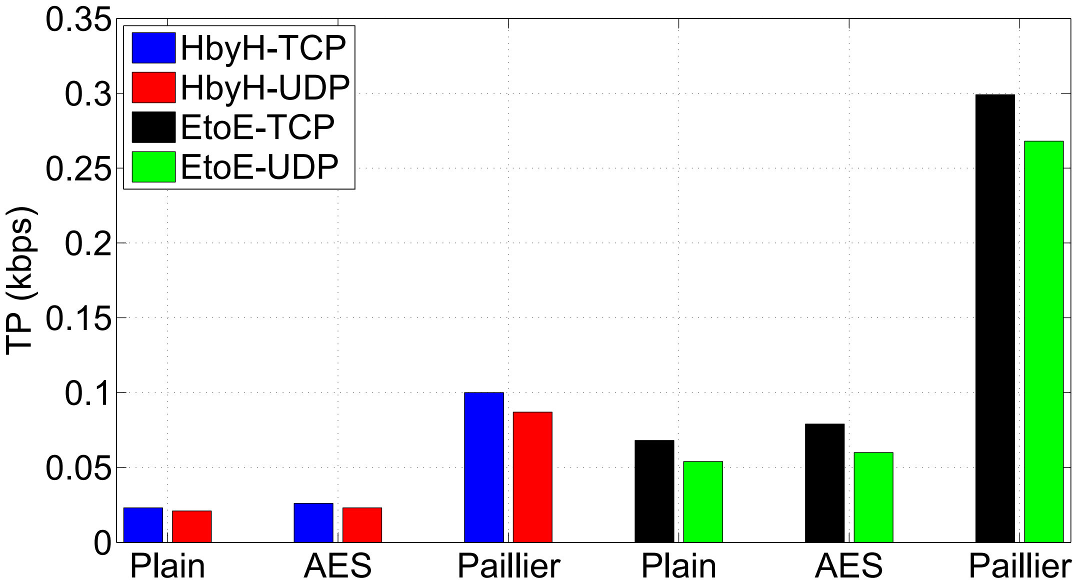


Figure 5.26: The testbed TP results for the fourth test.

5.6.3 CT Results

CT results can be seen on Figures 5.27 and 5.28. Checking the results we can say that one of the two main problems that led to this test is solved, but the other one is not. In both simulation and testbed results, UDP performs better than TCP which means that there is no discrepancy anymore for protocol performance. Although the discrepancy for the mode performance still stands with HbyH performing better in simulation, and worse in testbed, these results support the claim we made after the third test. Results show that ns-3 can not configure the communication channel correctly as better performance by EtoE shows that the bandwidth of the communication channel between BBBs is large enough for the gateway to receive data and process it quickly.

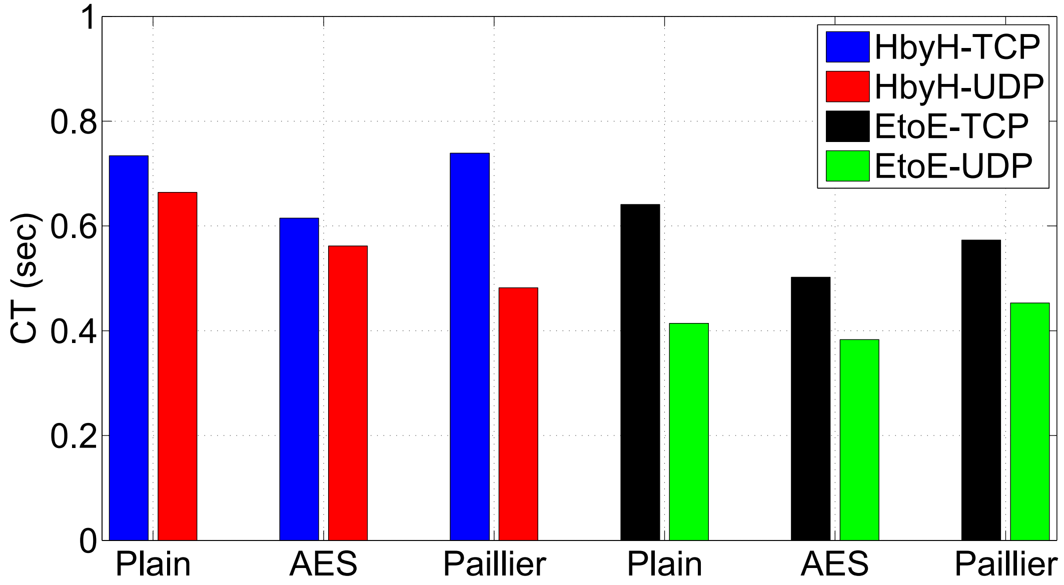


Figure 5.27: The testbed CT results for the fourth test.

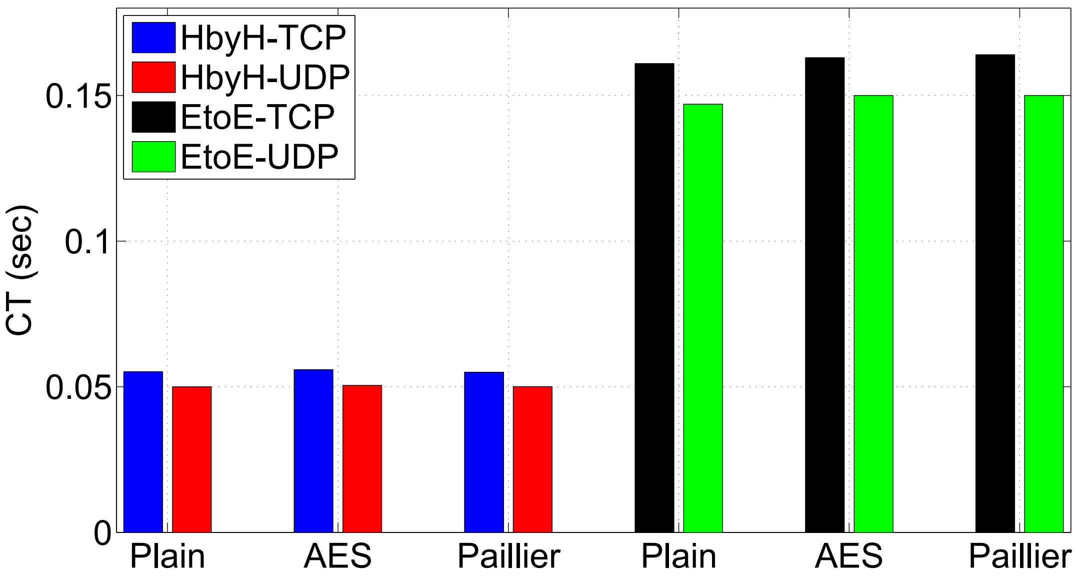


Figure 5.28: The simulation CT results for the fourth test.

5.7 Performance Evaluation of SMPC and FHE compared to Paillier

After solving the conflicts between the simulation and the testbed and seeing the performance of Paillier against other baselines, final test is done to evaluate performance of two other privacy-preserving protocol options that can be considered for AMI Networks. The protocols selected for comparison are SMPC and FHE. As BBBs were not able to deal with the computational overhead of FHE, RP3 testbed is used for this test. Same cases that are considered for the previous tests are considered again for this test (HbyH versus EtoE, and TCP versus UDP). For the testbed, FHE couldn't be tested with UDP because of the packet loss and memory problem. As FHE ciphertext size is really big, it can not be sent immediately as one packet. It is sent by using more than one packets. If one of these packets is lost, data is also lost as its integrity is damaged. When UDP is tested, random packet losses occurred on every test causing the application to crash without any results. The ns-3 implementation of FHE worked without problem. This situation suggested that FHE UDP implementation could be causing problems due to memory limitations.

5.7.1 PDR Results

PDR results can be seen on Figures 5.29 and 5.30. For testbed, there wasn't any surprising results for TCP cases as they were all 50% for HbyH and 100% for EtoE modes. For HbyH mode, UDP matches the performance of TCP, but packet losses can be seen in EtoE mode cases. Paillier PDR for UDP is around 80% and SMPC PDR is close to 98%. FHE UDP PDR values couldn't be gathered as the application crashed for both modes without outputting a result because of packet losses. This problem shows that perfect PDR wouldn't be reached by FHE UDP cases even if tests were run without problem.

The trend set by TCP in the testbed can also be seen in simulation results with 50% for HbyH and 100% for EtoE modes. The only difference between the testbed and the simulation is UDP results. Although Paillier HbyH UDP results are the same for both setups, EtoE results are different with a 6.5% margin in simulation's favor. Also, there is 3.2% difference between the SMPC HbyH UDP results of the simulation and the testbed. As packet losses are random, these margins can be expected. Another test can result in a different margin or maybe same values like HbyH mode TCP results. As there is no result for FHE UDP in testbed, it is not possible the compare the simulation values. Still, the simulation results show that UDP does not perform very well with FHE and its huge message size that results in larger packets.

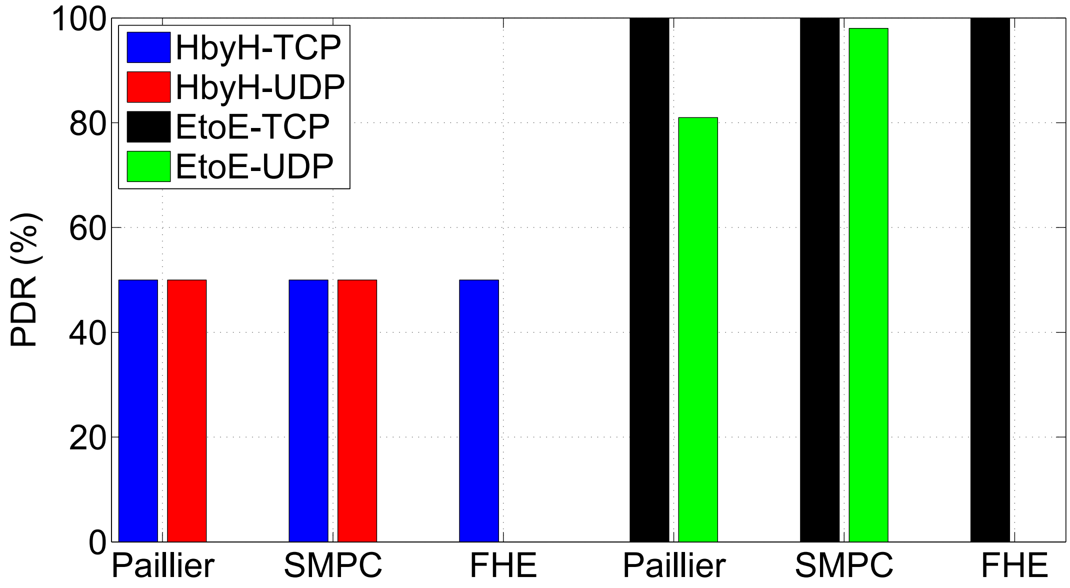


Figure 5.29: The testbed PDR results for the final test.

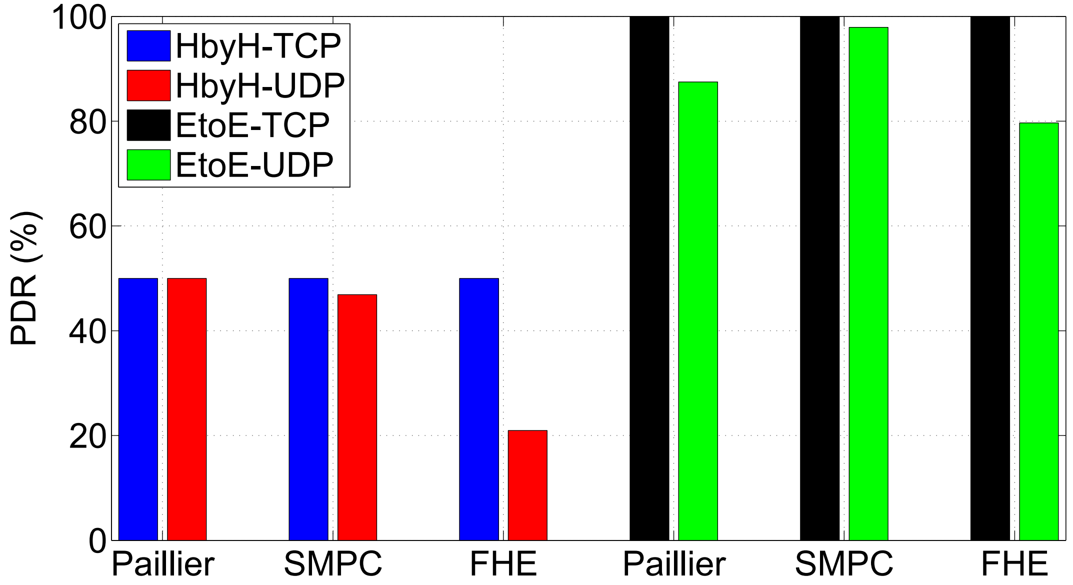


Figure 5.30: The simulation PDR results for the final test.

5.7.2 TP Results

TP results can be seen on Figures 5.31, 5.32, 5.33 and 5.34. One thing that can be noticed FHE TP values compared to other protocols. As FHE has the highest message size, its TP values are also the highest. FHE is followed by Paillier which has the second biggest message size. As more packets are received in EtoE modes, TP values are higher for this mode as expected. TP values are also not calculated for FHE UDP cases.

The simulation results are also parallel with the testbed results. FHE with TCP achieves the biggest TP values, while SMPC achieves the lowest values with UDP. As packet loss ratios are different, UDP TP values are also different, but very close to each other for the testbed and the simulation results.

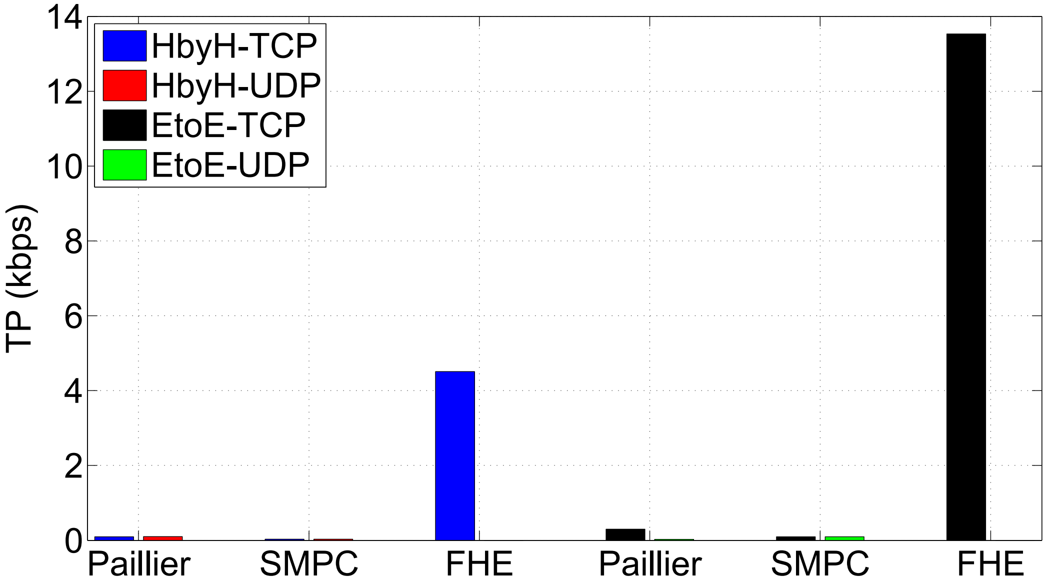


Figure 5.31: The testbed TP results for the final test.

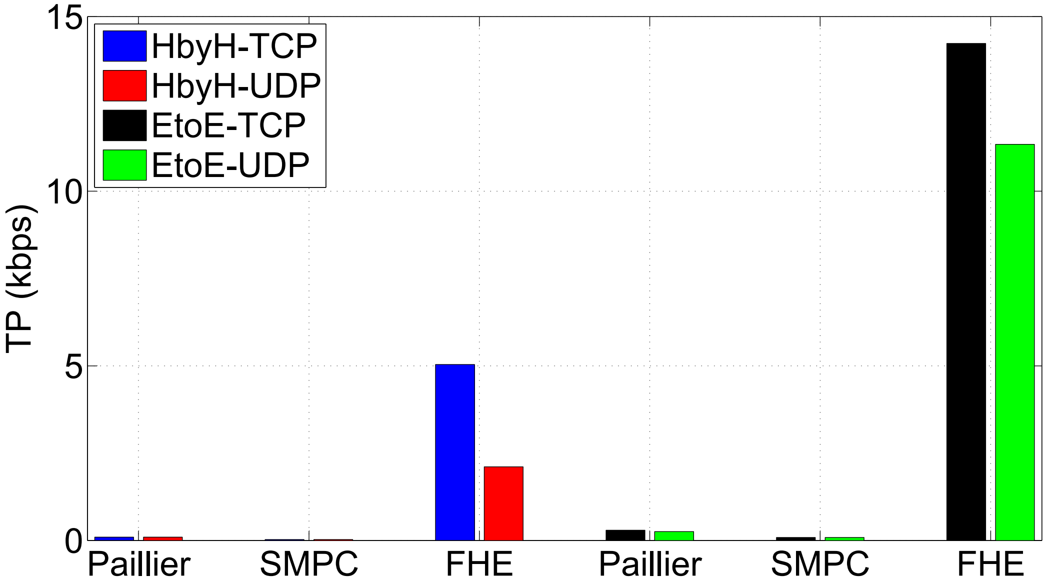


Figure 5.32: The simulation TP results for the final test.

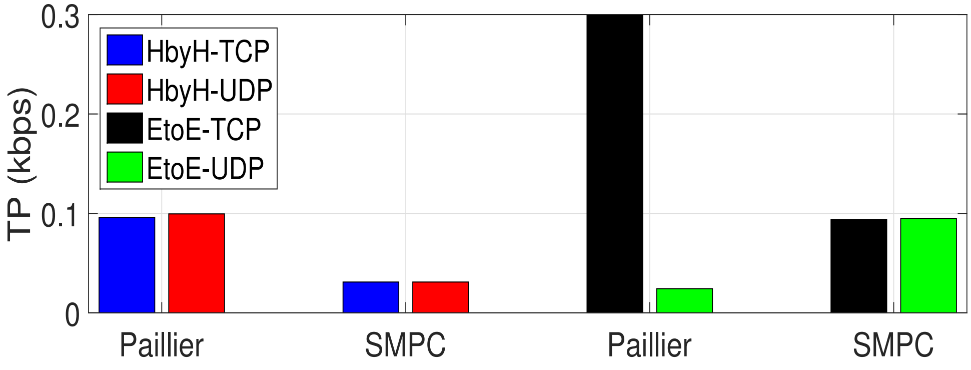


Figure 5.33: The testbed TP results of SMPC and PHE only

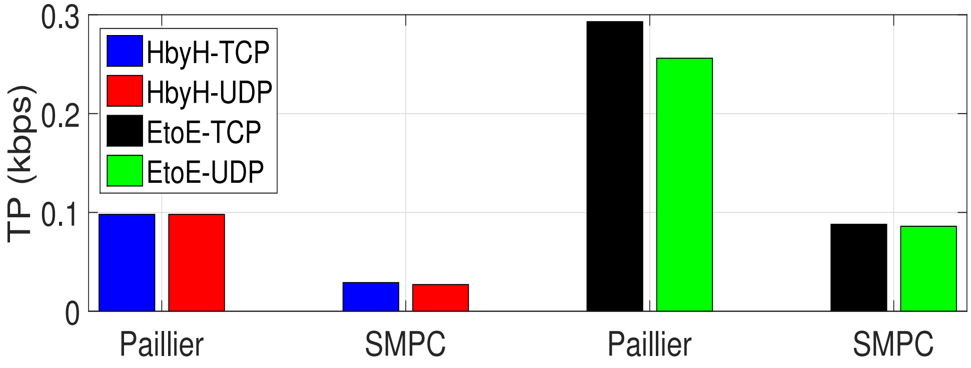


Figure 5.34: The simulation TP results of SMPC and PHE only

5.7.3 CT Results

CT results can be seen on Figures 5.35, 5.36, 5.37 and 5.38. Results are evaluated from different angles to evaluate them better.

The first evaluation is done on the transport protocols' performance. Testbed results show that UDP is faster than TCP for all cases (except FHE as UDP couldn't be tested). Simulation results confirm the testbed results and additionally show that UDP is faster for FHE, too.

The second evaluation is done on the privacy-preserving protocols' performance. With a quite big margin, FHE is the slowest protocol in the testbed. Paillier is the fastest protocol under both HbyH and EtoE modes, but the difference between

SMPC is very small for EtoE mode cases. Like the testbed results, FHE is the slowest protocol, and Paillier is the fastest one, with SMPC right behind it speed-wise in the simulation results.

Finally, data collection modes' performance is evaluated. For Paillier and SMPC, we can see that EtoE mode performs better than HbyH mode. However, the case for FHE is the exact opposite. This shows that the gateway is able to handle the computations required for Paillier and SMPC without problem, but its resources are not enough to handle the heavy computations required by FHE resulting in a poor performance compared to HbyH mode for the EtoE mode. Unlike the testbed results, the HbyH mode performs better than the EtoE mode for all of the privacy-preserving protocols' cases in the simulation results. When FHE is used, the communication channel is utilized until its limits to transfer the big ciphertext created by FHE. This results in a better performance in the testbed for HbyH as the load is split and easier to handle. This situation again supports our claim made in the third test that ns-3 channel configuration is the reason for the discrepancies observed between mode performances.

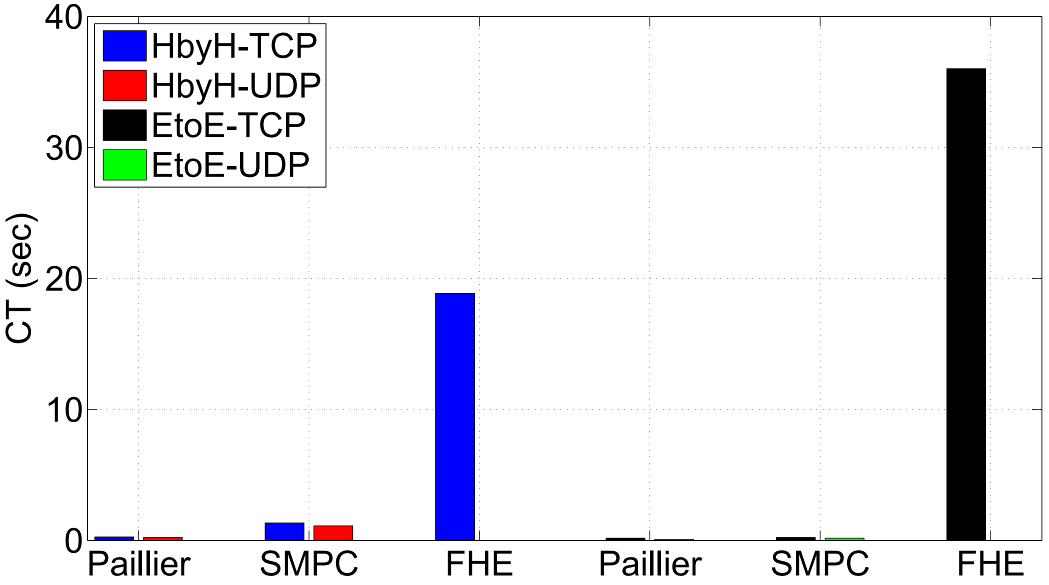


Figure 5.35: The testbed CT results for the final test.

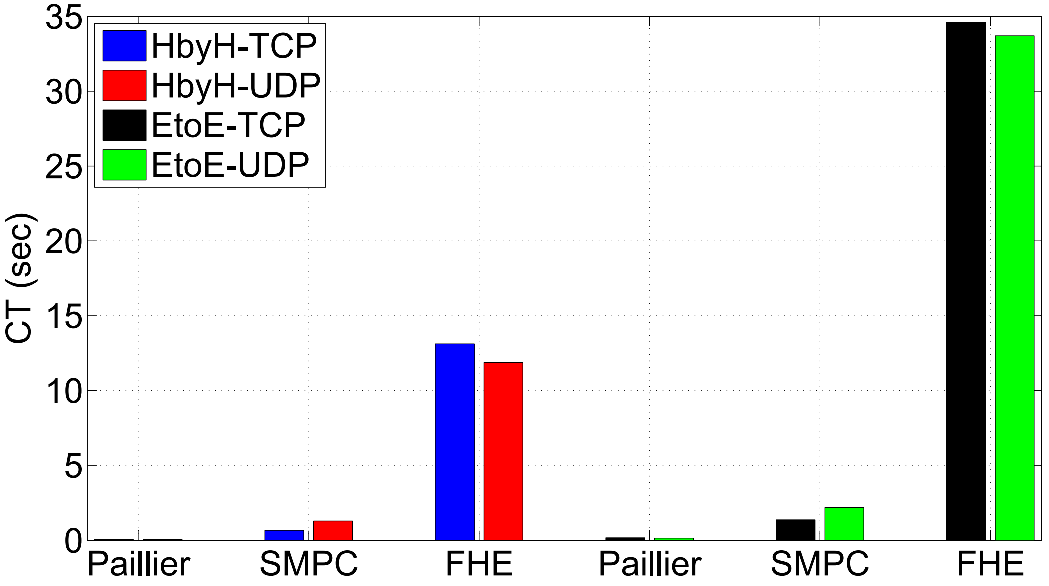


Figure 5.36: The simulation CT results for the final test.

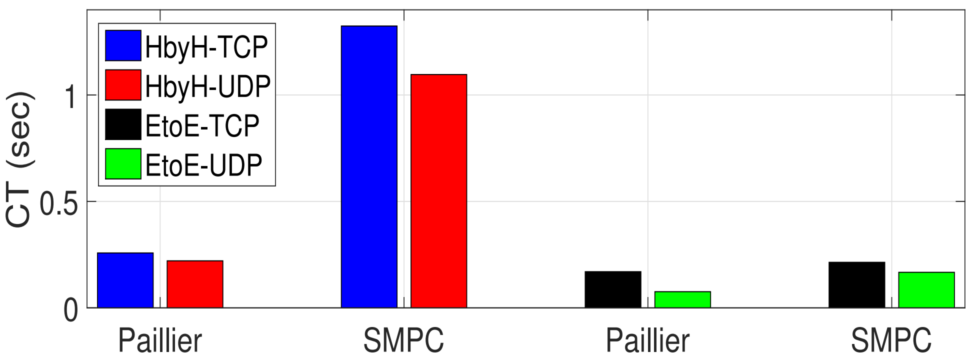


Figure 5.37: The testbed CT results of SMPC and PHE only

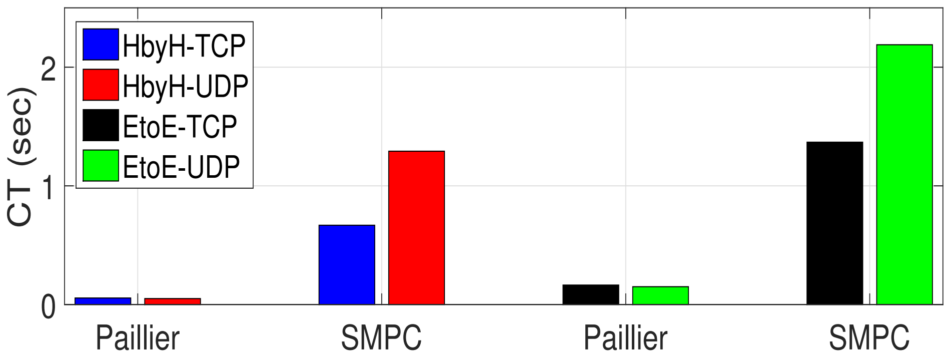


Figure 5.38: The simulation CT results of SMPC and PHE only

CHAPTER 6

CONCLUSION

In this thesis, two 802.11s wireless mesh-based SG AMI testbeds are developed. After their development, testbeds are used to evaluate the performance of privacy-preserving protocols that can be used to secure AMI network communications consisting of a combination of Paillier cryptosystem, FHE, or SMPC for privacy and ECDSA (initially only ECDSA was proposed and tested), and OpenSSL for two-factor authentication. In order to test the protocols, three test environments are created, one that uses ns-3 simulator, one that uses the testbed created with BBBs, and another one with RP3s. Remote access is also set up to provide researchers interested in AMI networks a realistic testbed solution for performance evaluation of any AMI related protocol they are working on.

The evaluations revealed several interesting results: 1) While PDR and TP mostly match with ns-3 and testbed, there is discrepancy among the two results when it comes to CT metric. The results were conflicting and suggests that any simulation result in research might not be able to capture the channel characteristics; 2) First two tests showed that HbyH approaches are much suited to be used for AMI since they reduce CT significantly, but the final tests proved that EtoE approaches actually perform better for the testbed; 3) Paillier's performance is really close to plaintext exchange performance making them feasible for use in AMI Networks, and; 4) UDP performs better than TCP in all cases for both the testbed and the simulation, but considering the packet losses in UDP and the need for reliability in AMI Networks, TCP looks like a better option for use in AMI Networks. 5) Final test showed that SMPC can also be considered as a privacy option, but FHE still needs improvement speed-wise.

[316] ns 3. ns-3: Network Simulator 3. Release 3.24.1, 2016.

[AASD13] M. Q. Ali, E. Al-Shaer, and Q. Duan. Randomizing ami configuration for proactive defense in smart grid. In *2013 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pages 618–623, Oct 2013.

[ami] Adwise lab ami testbed.

[AWW05] Ian F Akyildiz, Xudong Wang, and Weilin Wang. Wireless mesh networks: a survey. *Computer networks*, 47(4):445–487, 2005.

[Bah06] Michael Bahr. Proposed routing for ieee 802.11 s wlan mesh networks. In *Proceedings of the 2nd annual international workshop on Wireless internet*, page 5. ACM, 2006.

[BAM12] SMS Bari, Farhat Anwar, and MH Masud. Performance study of hybrid wireless mesh protocol (hwmp) for ieee 802.11 s wlan mesh networks. In *Computer and Communication Engineering (ICCCE), 2012 International Conference on*, pages 712–716. IEEE, 2012.

[BHTS16] D. Brettschneider, D. Hlker, R. Tnjes, and A. Scheerhorn. On homomorphic encryption for privacy-preserving distributed load adaption in smart grids. In *2016 IEEE International Conference on Communications (ICC)*, pages 1–6, May 2016.

[BOMB11] Jalel Ben-Othman, Lynda Mokdad, and Yesica I Saavedra Benitez. Performance comparison between ibc-hwmp and hash-hwmp. In *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*, pages 1–5. IEEE, 2011.

[CMAU16] Mehmet H Cintuglu, Osama A Mohammed, Kemal Akkaya, and A Selcuk Uluagac. A survey on smart grid cyber-physical system testbeds. *IEEE Communications Surveys & Tutorials*, 2016.

[Col13] Gerald Coley. Beaglebone Black System Reference Manual. *Texas Instruments, Dallas*, 2013.

[com17] commandlinefu. Synchronize date and time with a server over ssh, February 2017.

[FMXY12] X. Fang, S. Misra, G. Xue, and D. Yang. Smart grid #x2014; the new and improved power grid: A survey. *IEEE Communications Surveys Tutorials*, 14(4):944–980, Fourth 2012.

[GWP^{+}14] C Greer, DA Wollman, DE Prochaska, PA Boynton, JA Mazer, CT Nguyen, GJ FitzPatrick, TL Nelson, GH Koepke, AR Hefner Jr, et al. Nist framework and roadmap for smart grid interoperability standards, release 3.0. *US National Institute of Standards and Technology, Tech. Rep.*, 2014.

[GXL^{+}12] Jingcheng Gao, Yang Xiao, Jing Liu, Wei Liang, and CL Chen. A Survey of Communication/Networking in Smart Grids. *Future Generation Computer Systems*, 28(2):391–404, 2012.

[HDM^{+}10] Guido R Hiertz, Dee Denteneer, Sebastian Max, Rakesh Taori, Javier Cardona, Lars Berlemann, and Bernhard Walke. IEEE 802.11s: the WLAN Mesh Standard. *Wireless Communications, IEEE*, 17(1):104–111, 2010.

[IEE06] IEEE. *HWMP Specification*, 11 2006. Rev. 1.

[IHH09] Md Shariful Islam, Md Abdul Hamid, and Choong Seon Hong. Shwmp: a secure hybrid wireless mesh protocol for ieee 802.11 s wireless mesh networks. In *Transactions on Computational Science VI*, pages 95–114. Springer, 2009.

[IW16] IW. Linux wireless documentation, 2016.

[JBL^{+}11] Liu Jianming, Zhao Bingzhen, Geng Liang, Yuan Zhou, and Wang Yirong. Communication performance of broadband plc technologies for smart grid. In *Power Line Communications and Its Applications (ISPLC), 2011 IEEE International Symposium on*, pages 491–496. IEEE, 2011.

[JMV01] Don Johnson, Alfred Menezes, and Scott Vanstone. The Elliptic Curve Digital Signature Algorithm (ECDSA). *International Journal of Information Security*, 1(1):36–63, 2001.

[KPL16] A. Kheaksong, A. Prayote, and W. Lee. Performance evaluation of smart grid communications via network simulation version 3. In *2016 13th International Conference on Electrical Engineering/Electronics,* *Computer, Telecommunications and Information Technology (ECTI-CON)*, pages 1–5, June 2016.

[KPS13] Mario Kirschbaum, Thomas Plos, and Jorn-Marc Schmidt. On secure multi-party computation in bandwidth-limited smart-meter systems. In *Availability, Reliability and Security (ARES), 2013 Eighth International Conference on*, pages 230–235. IEEE, 2013.

[MZKF15] M. A. Mustafa, N. Zhang, G. Kalogridis, and Z. Fan. Dep2sa: A decentralized efficient privacy-preserving and selective aggregation scheme in advanced metering infrastructure. *IEEE Access*, 3:2828–2846, 2015.

[o11] open80211s.

[ope] Openssl ca.

[Ope16] OpenSSL. OpenSSL, 2016.

[OTA16] Utku Ozgur, Samet Tonyali, and Kemal Akkaya. Testbed and simulation-based evaluation of privacy-preserving algorithms for smart grid ami networks. In *Proceedings of the 41st IEEE Local Computer Networks Conference Workshops*. IEEE, 2016.

[OTAS16] U. Ozgur, S. Tonyali, K. Akkaya, and F. Senel. Comparative evaluation of smart grid ami networks: Performance under privacy. In *2016 IEEE Symposium on Computers and Communication (ISCC)*, pages 1134–1136, June 2016.

[Pai99] Pascal 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, pages 223–238, Berlin, Heidelberg, 1999. Springer-Verlag.

[PBS11] H. Perl, M. Brenner, and M. Smith. Poster: An implementation of the fully homomorphic smart-vercauteren crypto-system. In *18th ACM Conference on Computer and communications security (ACM CCS)*, pages 837 – 840, October 2011.

[RASB13] M. A. Rahman, E. Al-Shaer, and P. Bera. A noninvasive threat analyzer for advanced metering infrastructure in smart grid. *IEEE Transactions on Smart Grid*, 4(1):273–287, March 2013.

[RW12] Matt Richardson and Shawn Wallace. *Getting started with raspberry PI.* " O'Reilly Media, Inc.", 2012.

[SA12] Nico Saputro and Kemal Akkaya. Performance Evaluation of Smart Grid Data Aggregation via Homomorphic Encryption. In *Wireless Communications and Networking Conference (WCNC), 2012 IEEE Conference on*, pages 2945–2950. IEEE, 2012.

[SA14] Nico Saputro and Kemal Akkaya. On Preserving User Privacy in Smart Grid Advanced Metering Infrastructure Applications. *Security and Communication Networks*, 7(1):206–220, 2014.

[SGBP16] A. Sahu, A. Goulart, and K. Butler-Purry. Modeling ami network for real-time simulation in ns-3. In *2016 Principles, Systems and Applications of IP Telecommunications (IPTComm)*, pages 1–8, Oct 2016.

[SZS17] H. Shen, M. Zhang, and J. Shen. Efficient privacy-preserving cube-data aggregation scheme for smart grids. *IEEE Transactions on Information Forensics and Security*, 12(6):1369–1381, June 2017.

[TAS$^+$17] Samet Tonyali, Kemal Akkaya, Nico Saputro, Selcuk A. Uluagac, and Mehrdad Nojoumian. Privacy-preserving protocols for secure and reliable data aggregation in smart grid ami networks. *Future Generation Computer Systems, Special Issue on Internet of Things: Security and Forensics Trends and Challenges*, 2017.

[TASU16] Samet Tonyali, Kemal Akkaya, Nico Saputro, and A. Selcuk Uluagac. A Reliable Data Aggregation Mechanism with Homomorphic Encryption in Smart Grid AMI Networks. In *Proceedings of the 13th IEEE Annual Consumer Communications and Network Conference*. IEEE, 2016.

[TCA$^+$16a] S. Tonyali, O. Cakmak, K. Akkaya, M. M. E. A. Mahmoud, and I. Guvenc. Secure data obfuscation scheme to enable privacy-preserving state estimation in smart grid ami networks. *IEEE Internet of Things Journal*, 3(5):709–719, Oct 2016.

[TCA$^+$16b] Samet Tonyali, Ozan Cakmak, Kemal Akkaya, Mohamed MEA Mahmoud, and Ismail Guvenc. Secure data obfuscation scheme to enable privacy-preserving state estimation in smart grid ami networks. *IEEE Internet of Things Journal*, 3(5):709–719, 2016.

[TL16] TP-LINK. TP-LINK TL-WN722N, 2016.

[TSA15a] Samet Tonyali, Nico Saputro, and Kemal Akkaya. Assessing the Feasibility of Fully Homomorphic Encryption for Smart Grid AMI Networks. In *The Seventh International Conference on Ubiquitous and Future Networks 2015 - ICUFN2015*, 2015.

[TSA15b] Samet Tonyali, Nico Saputro, and Kemal Akkaya. Assessing the feasibility of fully homomorphic encryption for smart grid ami networks. In *Ubiquitous and Future Networks (ICUFN), 2015 Seventh International Conference on*, pages 591–596. IEEE, 2015.

[UH16] Eben Upton and Gareth Halfacree. *Raspberry Pi User Guide.* Wiley Publishing, 4th edition, 2016.

[UIA11] Suleyman Uludag, Tom Imboden, and Kemal Akkaya. A taxonomy and evaluation for developing 802.11-based wireless mesh network testbeds. *Wiley International Journal of Communication Systems*, 2011.

[ULRN14] S. Uludag, K. S. Lui, W. Ren, and K. Nahrstedt. Practical and secure machine-to-machine data collection protocol in smart grid. In *2014 IEEE Conference on Communications and Network Security*, pages 85–90, Oct 2014.

[VDKK16] R. Vijayanand, D. Devaraj, B. Kannapiran, and K. Kartheeban. Bit masking based secure data aggregation technique for advanced metering infrastructure in smart grid system. In *2016 International Conference on Computer Communication and Informatics (ICCCI)*, pages 1–5, Jan 2016.

[Wen09] Luan Wenpeng. Advanced Metering Infrastructure. *Southern Power System Technology*, 3(2):6–10, 2009.

[YMG08] Jennifer Yick, Biswanath Mukherjee, and Dipak Ghosal. Wireless sensor network survey. *Computer networks*, 52(12):2292–2330, 2008.