

Testbed and Simulation-based Evaluation of Privacy-preserving Algorithms for Smart Grid AMI Networks

Utku Ozgur, Samet Tonyali, and Kemal Akkaya

Department of Electrical and Computer Engineering

Florida International University

Miami, Florida 33174 USA

Email: {uozgu001, stony002, kakkaya}@fiu.edu

Abstract—Although smart meters are deployed in a lot of countries as a result of aiming to make the power grid more resilient and efficient, the data collection process from smart meters in Smart Grid (SG) has still challenges that relate to consumer privacy. Referred to as Advanced Metering Infrastructure (AMI), the data collected and transmitted through this AMI can leak sensitive information about the consumers if it is sent as plaintext. While a number of 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 performance of these solutions. In this paper, we pick a widely used homomorphic-based aggregation and implement it in a realistic testbed so that it can be compared with a simulation-based solution. Specifically, we develop a system that provides privacy with the Paillier cryptosystem and two-factor authentication with ECDSA and OpenSSL certificates. In order to test the system, an IEEE 802.11s-based SG AMI network testbed is constructed with Beaglebone Black boards that imitate the behavior of smart meters. The same network is also simulated in widely used ns-3. The results showed that ns-3 simulation and testbed results are parallel in most cases and the proposed system can perform effectively. However, there are still many differences that need to be taken into account in deploying real systems.

I. INTRODUCTION

Smart Grid (SG) is the system that makes the power distribution efficient and effective [15], [21]. This is achieved through different components at the generation, transmission and distribution levels that enable two-way information communication. One of such 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 affordable method of communication between SMs and the respective companies is needed. Thanks to the cost and easiness of the installation and the maintainability [22], wireless communication networks became an alternative of the wired networks such as a power-line communication (PLC) that is mostly preferred in SG AMI networks [8]. To this end, various wireless mesh protocols can be employed [15]. IEEE

802.11s is such an option which integrates mesh networking services and protocols with existing IEEE 802.11 protocols at the MAC layer. IEEE 802.11s-based mesh networks use Hybrid Wireless Mesh Protocol (HWMP) by default to relay data packets through the network in a multi-hop fashion [6].

However, when such mesh-based wireless communication infrastructures are used, privacy of the user becomes an issue as the users' data will travel over wireless communications through potentially others' SMs [5], [14]. Although instantaneous SM data does not expose much about the user, collecting and analyzing this data for longer periods can provide gains insight a particular household and the habits of the people living there. In order to avoid this, various approaches were proposed in recent years [14], [16]–[18]. These approaches strived to provide solutions that either hides the user identities or introduce noise to the actual data.

Despite the diversity of these solution, one major issue was the lack of actual deployment and testing in real AMI environments. This was partially due to infeasibility of using existing utility AMI systems and partially due to 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 paper aims to make that comparison by building an AMI testbed and utilizing ns-3 [10] simulations.

Specifically, we propose a system that takes advantage of a partially homomorphic encryption algorithm called Paillier cryptosystem [12] and two-factor authentication with OpenSSL [11] certificates and Elliptic Curve Digital Signature Algorithm (ECDSA) [9] signatures to provide the privacy needed in the data collection process inside a SG AMI Network. Paillier homomorphic systems can perform data aggregation on the encrypted data that will enable privacy for the user's data. The actual testbed is created with Beaglebone

Black boards (BBBs) [4] with TP-Link TL-WN722N wireless adaptors [19]. Tests are made with the help of a data collection application that is executed on every BBBs to make BBBs send data once after a period of time. A similar network topology was created using ns-3 environment which has the implementation of IEEE 802.11s. We built the same system (Paillier, OpenSSL and ECDSA) on ns-3 to have a fair comparison.

In order to evaluate and compare our system's performance, the application is run in two different modes called hop-by-hop (HbyH) and end-to-end (EtoE) aggregation. These approaches implement aggregation either at the intermediate nodes or at the gateway. We also tested plaintext data exchange and data exchange using Advanced Encryption Standard (AES) encryption algorithm on both testbed and simulation. Results are evaluated in terms of throughput (TP), completion time (CT), and packet delivery ratio (PDR). The results indicated that while testbed and simulation are agreeing in most of the test cases, there are still many discrepancies in CT, that relates to data delay, which may eventually impact various AMI applications in real life.

The rest of the paper is organized as follows: In Section II, we present the work previously done in this area. In Section III, we give background information about some terms and concepts that are discussed thoroughly in this paper. In section IV, we explain how the testbed is constructed and the testbed and simulation experiments are made. In section V, results of the experiments are discussed. Finally, we conclude the paper in Section VI.

II. RELATED WORK

Due to their easy-to-deploy and self-healing features, wireless mesh networks (WMNs) attracted attention of people from both industry and academia [3]. Consequently, there have been many studies investigating them. In most of these studies, simulators were frequently used but a number of studies utilized real testbeds [20]. Using these testbeds, different protocols and hardware have been tested. These testbeds focused on the testing of four primary research areas: Routing, Mobility, Interference, and QoS [20].

There are two major things that are missing with these existing testbeds; 1) Only a few of them utilized the IEEE 802.11s standard; and 2) They do not consider any privacy protocols on these testbeds. For instance, AAbid et al. [2] presents an open-source implementation of IEEE 802.11s-based WMN testbed. Their implementation is easy-to-deploy, and they provide the source code and deployment instructions [1]. In the paper, they identified some of the most important implementation problems and proposed feasible solutions for these problems. However, this testbed was not geared for the needs of AMI networks and there is no research on security or privacy issues.

On the privacy side, there has been numerous approaches presented in the literature [14]. These approaches differ based on the concept of anonymizing the customer identity, obfuscating and aggregation of the data. However, the incorporation

of these approaches in AMI network protocols and assessment of the performance has not been well studied.

Unlike the aforementioned efforts, in this paper, we focus on the performance of IEEE 802.11s-based networks targeting AMI environment with a privacy preservation focus. We investigate how the message overheads and the crypto-operational delays affect the performance of the network by testing them on a real testbed and a simulator. In this way, a comparison between testbed and simulation can also be done.

III. PRELIMINARIES

A. AMI Network

AMI communication network consists of SMs that are connected via a WMN with a gateway serving as a relay between SMs and the UC. A SM measures mainly the real-time electrical energy consumption of the consumers in addition to power quality and instantaneous values such as voltage and current at their connection points. A typical infrastructure for the considered AMI in this paper is shown in Fig. 1. In the current AMI systems, this data is either collected by the utility company control center or by a trusted third party (TTP).

IEEE 802.11s standard allows mesh networking among the SMs through 802.11 MAC/PHY layer standard [6]. It uses the HWMP as its default routing protocol to find a multi-hop path towards the destination. In our mesh network, the gateway collects meter readings that are sent by the SMs via multi-hop routes.

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).

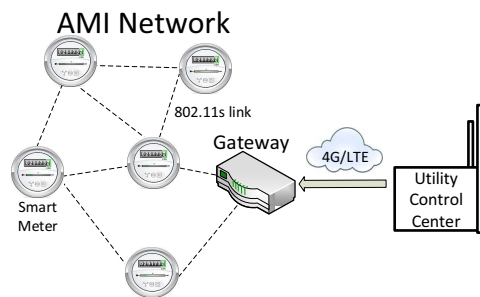


Fig. 1. A sample AMI communication network, gateway and long-distance communication to a utility company.

B. Paillier Cryptosystem

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

In this paper, we make use of a partially homomorphic encryption (PHE) algorithm called Paillier [12]. This is chosen due to its addition property, smaller message expansion factor compared to others, and security features [13], [14].

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

Let m_1 and m_2 be two plaintexts.

$$D_{S_K}((E_{P_K}(m_1) \times E_{P_K}(m_2)) \bmod n^2) = \quad (1)$$

where n is the first component of the public key ($P_K = (n, g)$ where g is a random integer and $g \in \mathbb{Z}_{n^2}^*$). Thus, one can infer that we do not need to know the private key to perform homomorphic addition operation while using Paillier cryptosystem.

For security and privacy, every SM in the AMI network holds a public key based on Paillier cryptosystem provided by the UC. In this way, all SMs are enabled to perform addition operation when aggregation is needed. For any other communication among the SMs, a symmetric key system can be used.

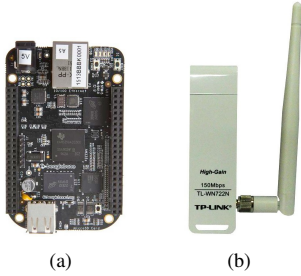


Fig. 2. (a) A Beaglebone Black board, and (b) a TP-LINK TL-WN722N Wi-Fi dongle.

C. Network Simulator-3 (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 [10]. We chose to use ns-3 in our simulations 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 and AES.

IV. PROTOCOL DEVELOPMENT ON AN AMI TESTBED

A. Protocol Description

By using BBBs and TP-Link TL-WN722N wireless adaptors (see Fig. 2), we have developed a small testbed at Advanced Wireless and Security (ADWISE) Lab at Florida International University. Specifically, we deployed nodes in a hierarchical manner and implemented to protocols that will enable data aggregation. Considering the number of BBBs and written applications, a three-level full tree network is planned as the network topology to use for our work. Fig. 3, provides the representation of the network. A laptop that runs Ubuntu 16.04 is used as the gateway of the network in order to differentiate the gateway from other meters. The application is written in order to support two different modes:

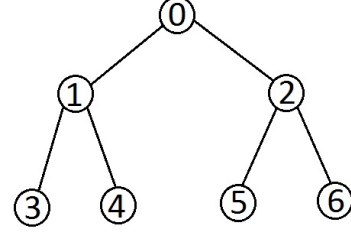


Fig. 3. The tree representation of the network we used in this study.

- *Hop-by-Hop Aggregation (HbyH)*: In this mode, leaf meters send their readings to the nodes at the middle level, which are also called aggregator meters. These meters then aggregate the readings that come from the leaf meters with their own readings and send the result to the gateway. The gateway collects all readings from the aggregator meters and like the aggregator meters, it aggregates its reading with these readings.
- *End-to-End Aggregation (EtoE)*: In this protocol, there is no aggregation performed within the network. Rather every packet is aggregated when it arrives at the gateway which acts as the data collector.

B. Setup Details

Firmware and driver required for the adaptors are installed to the BBBs first. 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, kernel is upgraded to 4.1.5 on every BBBs. 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 [7].

Linux operating system is further used in order to make the testing smoother after the planning of the network. OpenSSL certificates are created with the terminal. 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. The "date" command of Linux is also used before testing to synchronize the time of all devices in the mesh network.

All applications collect data from the meters after a given period of time. We tried different data collection frequencies, specifically 60secs and 120 secs. BBBs and the gateway are placed to the different spots in our ADWISE, which is a 12m X 12m office room as shown in Fig. 4.

This placement is also carried into the ns-3 simulation to have a fair comparison. We used the ns-3 version 24.1 for our simulations. We assumed that all required keys were exchanged between the nodes before the simulation. Each simulation was run for 500 seconds. The transmission power is 18 dBm for both simulations and the testbed experiments, and IEEE 802.11g is used as the underlying MAC implementation. Both testbed and ns-3 experiments were run for eight minutes.

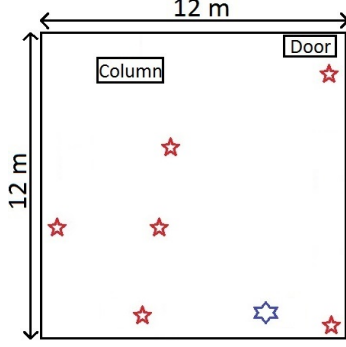


Fig. 4. The layout of the lab which hosts the testbed.

V. PERFORMANCE EVALUATION

A. Baselines

Since our goal is to assess the performance of privacy-preserving protocols, in addition to Paillier, we also implemented two other baselines: 1) Plaintext; and 2) AES-based Encryption. This was done because of the difference in message overheads (can be seen in Table I), and the difference in message exchange method as AES and Paillier do the exchange with ciphertexts and Paillier also does aggregation on ciphertexts. We also considered the use of TCP and UDP protocols as reliability is utmost concern in AMI applications. Consequently, we compared six different approaches. Implementations for TCP and UDP applications are done in a multithreaded client-server fashion and they were written as similar as possible in order to minimize the affect of implementations on the results.

TABLE I
MESSAGE OVERHEAD FOR 256-BIT AES, PAILLIER CRYPTOSYSTEM AND ECDSA

Message size (in bits)	
Plaintext	16
256-AES Ciphertext	128
Paillier Ciphertext	2048
ECDSA Signature	568

B. Performance Metrics

For performance evaluation, we used the following metrics:

- **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.

C. PDR Results

As we can see from Figures 3 and 4, 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. We should not forget that 50% PDR for HbyH mode results are not caused by packet losses as the main cause is the aggregation operation done in aggregator meters that decreases the number of packets in the network. Around 85% PDR results for EtoE UDP reminds us about the connectionless nature of UDP and makes us consider the reliability of it in a SG.

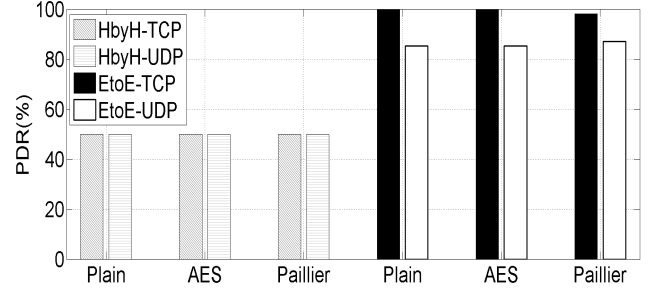


Fig. 5. The testbed PDR results.

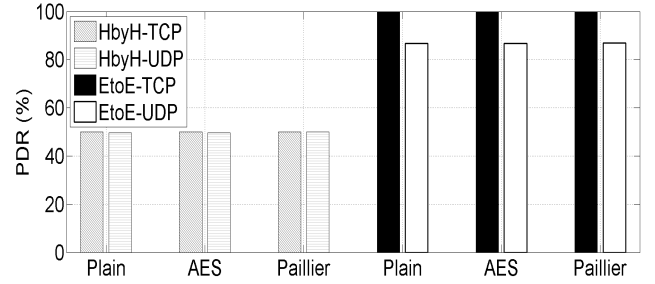


Fig. 6. The simulation PDR results.

D. 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, we see that TP results are really close for UDP and TCP cases with our system having the highest throughput followed by AES and plaintext. This result is reasonable since our system 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 a small number of collisions and backoffs which give enough advantage for it to be able to compete with UDP. For EtoE mode, our system again provides the highest throughput with TCP and UDP as expected.

There are conflicting results with respect to simulation and testbed. For instance, for Paillier, the simulation and 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

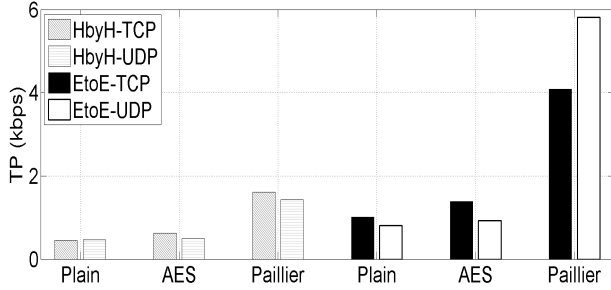


Fig. 7. The testbed TP results.

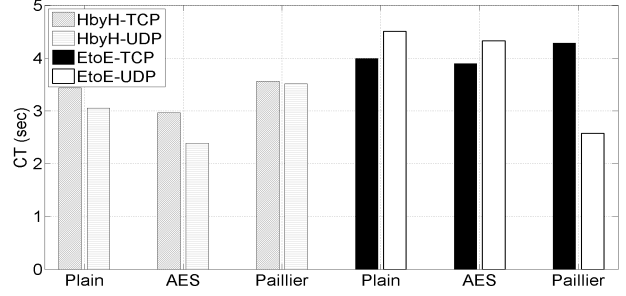


Fig. 9. The testbed CT results.

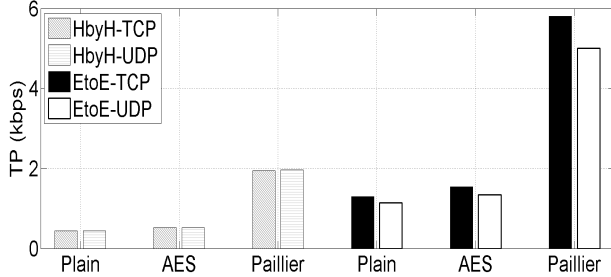


Fig. 8. The simulation TP results.

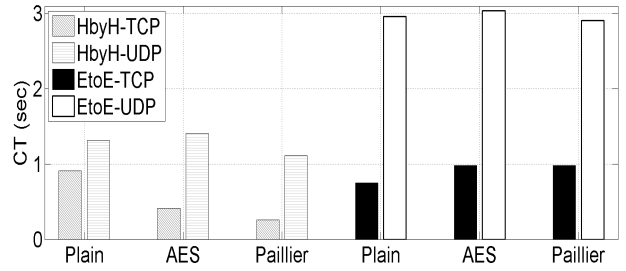


Fig. 10. The simulation CT results.

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.

E. 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. 9 and 10.

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. One of the reasons for ns-3 behavior can be attributed to the streaming nature of TCP. UDP creates individual packets and put them in the channel independently. This creates a lot of congestion in the network especially when EtoE approaches are used (since there will be more packets). However, for TCP there is an advantage of buffering since it can create a stream of bytes (not individual packets). 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 tested (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, we have then increased the data collection period to 120 secs to see if this has any effect on the performance of the testbed. The results shown in Figs. 11 and Fig. 12 indicate minor effect for TPC but major for UDP. Since there is less overlap among different periods, this helps EtoE approaches to reduce their CTs. However, the AES vs Plaintext case still holds with TCP. Overall, these show that simulation-based results are not always trustable and there is a lot of uncertainties in real-life that may effect any of the results.

VI. CONCLUSION

In this paper, we developed a privacy-preserving protocol consisting of a combination of Paillier cryptosystem and two-factor authentication that uses OpenSSL and ECDSA. In order to test the proposed system, we created two test environments, one that uses ns-3 simulator and another one that uses the testbed created with Beaglebone Black Boards that behave like smart meters in a SG AMI Network.

The evaluations revealed several interesting results: 1) While PDR and TP mostly match with ns-3 and testbed, there are major discrepancies 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 realities; 2) HbyH approaches are much suited to be used for

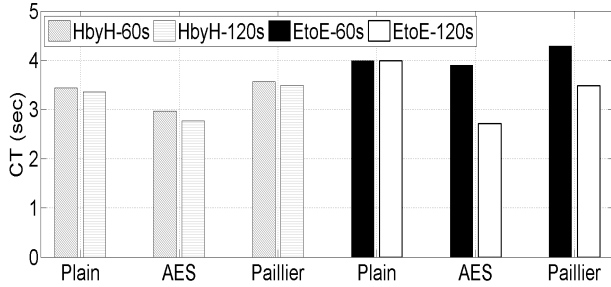


Fig. 11. Comparison of testbed CT results for TCP under different data collection periods.

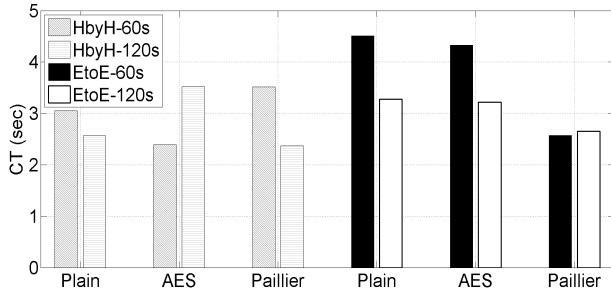


Fig. 12. Comparison of testbed CT results for UDP under different data collection periods.

AMI since they reduce CT significantly; 3) Paillier almost matches the performance of AES while providing perfect privacy. It only requires increased bandwidth and; 4) In some cases, TCP may perform faster than UDP so application needs should be carefully determined in advance.

ACKNOWLEDGMENT

This material 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.

REFERENCES

- [1] R. M. Abid, "The pre-ieee 802.11s wireless mesh network testbed at auburn university," 2010. [Online]. Available: http://www.aui.ma/personal/~R.Abid/WEB_SITE_WMNs_AUBURN/index.htm
- [2] 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, p. 725, 2010.
- [3] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey," *Computer networks*, vol. 47, no. 4, pp. 445–487, 2005.
- [4] G. Coley, "Beaglebone Black System Reference Manual," *Texas Instruments, Dallas*, 2013.
- [5] J. Gao, Y. Xiao, J. Liu, W. Liang, and C. Chen, "A Survey of Communication/Networking in Smart Grids," *Future Generation Computer Systems*, vol. 28, no. 2, pp. 391–404, 2012.
- [6] G. R. Hiertz, D. Denteneer, S. Max, R. Taori, J. Cardona, L. Berlemann, and B. Walke, "IEEE 802.11s: the WLAN Mesh Standard," *Wireless Communications, IEEE*, vol. 17, no. 1, pp. 104–111, 2010.
- [7] IW, "Linux wireless documentation," 2016. [Online]. Available: <https://wireless.wiki.kernel.org/en/users/documentation/iw>
- [8] L. Jianming, Z. Bingzhen, G. Liang, Y. Zhou, and W. Yirong, "Communication performance of broadband plc technologies for smart grid," in *Power Line Communications and Its Applications (ISPLC), 2011 IEEE International Symposium on*. IEEE, 2011, pp. 491–496.
- [9] D. Johnson, A. Menezes, and S. Vanstone, "The Elliptic Curve Digital Signature Algorithm (ECDSA)," *International Journal of Information Security*, vol. 1, no. 1, pp. 36–63, 2001.
- [10] ns 3, "ns-3: Network Simulator 3," Release 3.24.1, 2016. [Online]. Available: <http://www.nsnam.org/>
- [11] OpenSSL, "OpenSSL," 2016. [Online]. Available: <https://www.openssl.org/>
- [12] 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*, ser. EURO-CRYPT'99. Berlin, Heidelberg: Springer-Verlag, 1999, pp. 223–238. [Online]. Available: <http://dl.acm.org/citation.cfm?id=1756123.1756146>
- [13] N. Saputro and K. Akkaya, "Performance Evaluation of Smart Grid Data Aggregation via Homomorphic Encryption," in *Wireless Communications and Networking Conference (WCNC), 2012 IEEE Conference on*. IEEE, 2012, pp. 2945–2950.
- [14] —, "On Preserving User Privacy in Smart Grid Advanced Metering Infrastructure Applications," *Security and Communication Networks*, vol. 7, no. 1, pp. 206–220, 2014.
- [15] N. Saputro, K. Akkaya, and S. Uludag, "A survey of routing protocols for smart grid communications," *Computer Networks*, vol. 56, no. 11, pp. 2742 – 2771, 2012. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S1389128612001429>
- [16] S. Tonyali, K. Akkaya, N. Saputro, and A. S. 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.
- [17] S. Tonyali, O. Cakmak, M. Mahmoud, I. Guvenc *et al.*, "Secure Data Obfuscation Scheme to Enable Privacy-Preserving State Estimation in Smart Grid AMI Networks."
- [18] S. Tonyali, N. Saputro, and K. 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.
- [19] TP-LINK, "TP-LINK TL-WN722N," 2016. [Online]. Available: http://www.tp-link.com/en/products/details/cat-11_TL-WN722N.html
- [20] S. Uludag, T. Imboden, and K. Akkaya, "A taxonomy and evaluation for developing 802.11-based wireless mesh network testbeds," *Wiley International Journal of Communication Systems*, 2011. [Online]. Available: <http://dx.doi.org/10.1002/dac.1299>
- [21] L. Wenpeng, "Advanced Metering Infrastructure," *Southern Power System Technology*, vol. 3, no. 2, pp. 6–10, 2009.
- [22] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer networks*, vol. 52, no. 12, pp. 2292–2330, 2008.