Assessing Attack Threat Against ZigBee-based Home Area Network for Smart Grid Communications

Mostafa M. Fouda*†1, Zubair Md. Fadlullah†2, and Nei Kato†3
*Faculty of Engineering at Shoubra, Benha University, Egypt
†Graduate School of Information Sciences (GSIS), Tohoku University, Japan
Emails: mfouda@ieee.org1, zubair@it.ecei.tohoku.ac.jp2, and kato@it.ecei.tohoku.ac.jp3

***Abstract*—Smart Grid (SG) technology aims at bringing the world's aging electric grids into the twenty first century. To this end, the current power grids require to be overlayed with a robust communications system. Home Area Network (HAN) is an important part of the SG communications framework through which the end-users are able to communicate with the electricity provider. In a HAN, there is typically a smart-meter and a number of electric appliances. Most of the proposals to-date have agreed upon using IEEE 802.15.4 wireless technology dubbed as ZigBee for the HAN communications amongst the smart meter and the various electric appliances. Although ZigBee provides few security features, the technology still suffers from a number of security vulnerabilities, particularly in case of SG HAN. In this paper, we describe a HANIdentifier (HANId) conflict attack against ZigBee for HAN communications and demonstrate the impact of the attack on SG communications through computer simulations. Finally, we also envision an appropriate framework to prevent the attack.**

Keywords-smart grids; ZigBee; security

I. Introduction

Recent research endeavors in many countries, now, focus on transforming the existing utility grids (e.g., power lines) into "smart" ones. The Smart Grid (SG) concept is synonymous to future grid [1], and is aimed at providing the end-users (i.e., consumers) with more stable and reliable power. In a SG, the end-users' devices are expected to be able to communicate with the utility provider so that they may express their need or demand for power usage. To this end, the power provider should be able to effectively communicate with the end-users' devices. To facilitate this two-way communication, the hierarchical architecture for SG consists of the power plant, distribution stations, and different regional networks. These networks range from neighborhood and buildings to individual homes. The home area networks can service a number of electric appliances. Therefore, we need to protect the home area network systems from illegal accesses and a variety of threats. The home networks are typically based on IEEE 802.15.4 (ZigBee) wireless technology which may lead to various security vulnerabilities and attacks including Denial of Service (DoS), malicious codes, and so forth.

At a typical home, an end-user may have a huge number of electric appliances, all of which are required to be connected to the home network's coordinator, with which they may exchange information pertaining to power requirements and usage. IEEE 802.15.4 or ZigBee specification [2] delineates wireless and media access protocols for cheap and power-saving personal area networking devices. The SG community has begun using these protocols, particularly in home area networks. In addition, the 802.15.4 specification supports a number of security features through a link-layer security package. However, these security features are not designed to address some simple yet detrimental attacks. In this paper, we investigate a link-layer attack, which manipulates the HANIdentifier (HANId) conflict message and demonstrate its impact on the performance of the SG communications in the home network level. Our contribution in this paper consists in envisioning an appropriate architecture that prevents this type of attack from occurring in the first place.

The remainder of this paper is organized as follows. Section II presents relevant related researches. Section III presents the considered SG model architecture. Section IV describes the considered attack model against home networks and also provides simulation results to verify the impact of the attack. In Section V, we present a novel architecture to avoid the security vulnerability, which may lead to the considered attack. Finally, the paper concludes in Section VI.

II. Related Research Work

In order to fulfill all the requirements of a smart grid, it is an imperative to take into account many standards. In particular, the Institute of Electrical and Electronics Engineers (IEEE) launched an initiative to define these standards and provide guidelines on SG functionality. Their devised standards combined the recent advances in power engineering, communications, and Information Technology (IT). As a consequence, the IEEE P2030 group was formed and it comprised different task-forces focusing on integration of various energy sources, load side requirements, cyber security, and so forth [3]. Thus, they attempted to consider various aspects of power engineering along with IT and communications technologies. It was indicated that the IT group would investigate issues such as privacy, security, data integrity, interfaces, and interoperability in

This work is partially supported by the Government of Egypt.

SG. On the other hand, the communications technology group was assigned the responsibility to delineate the communication requirements amongst devices used in SG. The objective of the power group was to define boundaries on power generation, transmission, and distribution while considering the end-users. However, the policies designed by the above work-groups are broad in nature and should be considered as coarse design directives for enforcing security in SG communications.

Hamlyn *et al.* [4] proposed a utility computer network security management and authentication for actions and commands request in SG operations. However, their work focused on securing host area electric power systems and electric circuits. They did not consider SG communications framework in their work.

Power system communication and cyber security issues are considered to be crucial components of SG in [5]. This work suggests that numerous cyber security issues require to be addressed and solved. For example, integrated SCADA/EMS systems and administrative office IT environments may lead to evolving security threats. This work also demonstrates that broadband capabilities have opened up new ways of introducing new functionality, both at smart meters and the central system collecting metering data. The utilites are interested in transferring data to the households that may include price information and special offers. However, such data may also contain control signals, which may raise delicate issues to deal with.

Metke *et al.* point out in their work [6] that SG deployments must satisfy strict security requirements. For instance, strong authentication is considered by their work to be a requisite for all users and devices of the SG. Their work also found out that with the large number of users and devices affected, scalable key and trust management systems, tailored to the particular requirements of the utility provider will be essential.

It is worth noting that the afore-mentioned relevant works do not address the security requirements of the IEEE 802.15.4 (ZigBee) based networks tailored for home area communications in the SG. In our work, by providing a broad SG communications framework, we point out a security concern in the ZigBee-oriented home area network and try to deal with this security vulnerability in the remainder of this paper.

III. CONSIDERED SG COMMUNICATIONS ARCHITECTURE

We derive our motivation in envisioning a complete communication architecture for SG from a number of works [7], [8]. Fig. 1 depicts our considered SG communication framework. It should be noted that the SG power transmission and distribution system is separated from the communication one. In fact, the communication network is overlayed with the distributed one and Fig. 1 considers the communication overlay only.

For clarity, we first briefly describe the power Distribution Network (DN). In the considered DN in Fig. 1, power is delivered from the power plant to end-users through two components, namely the Transmission System (TS) at the power plant and a number of Distribution Systems (DSs). The former delivers power from the power plant over high voltage transmission lines (usually over 230 KV) to DSs, which are located at different regions and they are responsible for converting the electric power into medium voltage levels and distribute the same to the building-feeders, which in turn convert it into low voltage levels suitable for distribution to the consumers.

From communications point of view, the considered smart grid topology is assumed to have a number of entities, which we describe here. The TS, located at the power plant, and the Control Centers (CCs) of the DSs are connected with one another in a meshed network. This is the core communications backbone for the SG topology. We consider optical fiber technology to build this meshed network, as shown in Fig. 1, to facilitate communications with low latency and high bandwidth that are suitable for SG.

The communication framework for the lower distribution network (i.e., from CCs onward) is split into a number of hierarchical networks, namely Neighborhood Area Network (NAN), Building Area Network (BAN), and Home Area Network (HAN). For simplicity's sake, each DS is considered to cover only one neighborhood area. Thus, in Fig. 1, there are n DSs covering n neighborhoods, i.e., the number of NANs is n. Each NAN is composed of a number of BANs. For instance, $NAN1$ consists of k BANs. On the other hand, every BAN contains a number of apartments. In our illustration in Fig. 1, there are m apartments with their respective local area networks. The local area network of each apartment is referred to as a HAN. In addition, there are advanced meters called smart meters employed in the SG architecture which comprise Advanced Metering Infrastructure (AMI) for enabling an automated, two-way communication between the utility meter and the utility operator/provider. The smart meters are equipped with two interfaces, namely for reading power and for communication gateway. The smart meters used in NAN, BAN, and HAN are referred to as NAN GW (GateWay), BAN GW, and HAN GW, respectively. Consumers can be informed by these smart meters/GWs of how much power they are using so that they may be able to control their power consumption by switching on/off certain equipments. For ease of understanding, we adopt a bottom-up approach where we start describing the SG communications framework from the HAN. In addition, it is also worth mentioning that based upon the existing standards of SG, IP based communications networking is preferred in contrast with other communication protocols. The standardization of IP permits virtually effortless inter-connections with HANs, BANs, NANs, CCs, and TS.

A. Home Area Network

The Home Area Network (HAN) is a subsystem within the SG dedicated to efficiently manage the on-demand power requirements of the end-users. $HAN1$ in Fig. 1 connects the equipments (e.g., television, washing machine, oven, and so forth) in the end-user's apartment to a HAN GW, which in turn communicates with $BAN1$. We adopt Smart Energy Profile (SEP) Version 1.5 as the communication protocol in HANs that employ ZigBee radio communications. We choose

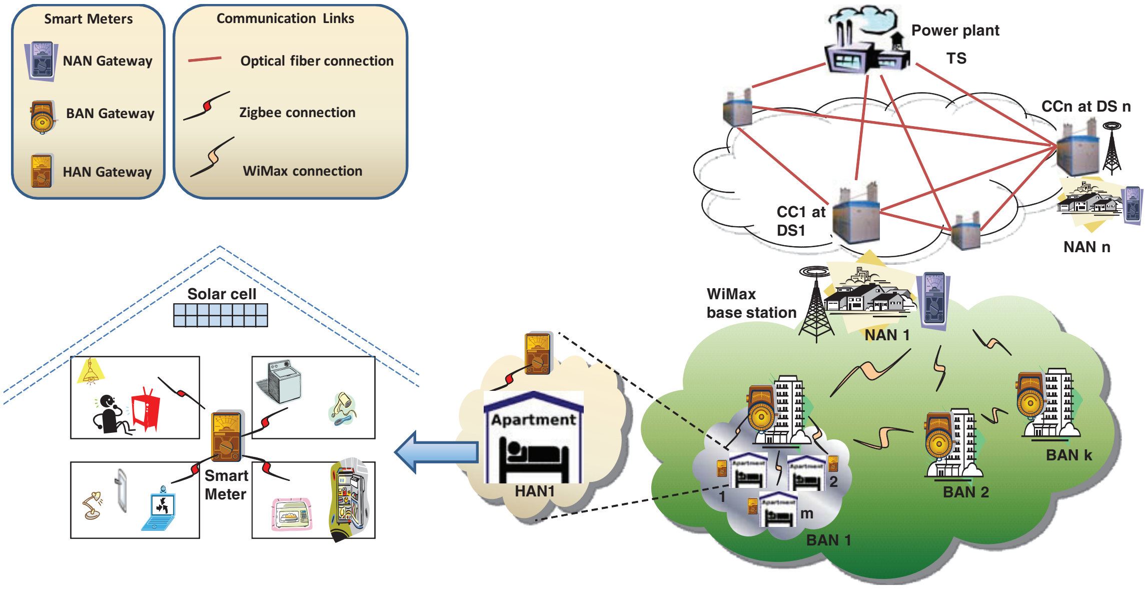


Fig. 1. Considered SG communications framework.

IEEE 802.15.4 Zigbee instead of other wireless solutions (e.g., WiFi and Bluetooth) due to its low power requirements, and simple network configuration and management. Indeed, ZigBee provides a decent communication range of 10 to 100 meters while maintaining significantly low power requirement (1 to 100 mW) and cost.

B. Building Area Network

A Building Area Network (BAN) consists of a number of apartments having HANs. The BAN smart meter/GW is typically set up at the building's power feeder. It can be used to monitor the power need and usage of the residents of the corresponding building. In order to facilitate BAN-HANs communication, WiMax may be used to cover more areas. It should be noted that 3G, 4G, and other modes of communications may also be alternative solutions for this purpose.

C. Neighborhood Area Network

Each Neighborhood Area Network (NAN) consists of a number of BANs. One or more WiMax base stations can be located in every NAN. It should be mentioned that the WiMax framework used for SG communications should be separated from the existing ones used for providing other services, e.g., Internet, to prevent network congestion and possible security threats. A NAN, thus, represents a locality or a particular region. The NAN GW can monitor how much power is being distributed to a particular neighborhood by the corresponding CC at the DS.

IV. Considered Attack Model

In this work, we address one kind of attack towards the HAN ZigBee wireless network. The attack consists in HANIdentifier (HANId) conflict. In a HAN of an apartment using ZigBee, there are a smart meter acting as the HAN coordinator and a group of nodes, which represent the electric appliances belonging to that apartment. We refer to the smart meter's unique identifier as the HANId. The members of a given HAN know their HANId. If there exists more than one HAN coordinator operating in the same operating space, a HANId conflict may occur. We derive this attack model in spirit with the one for wireless sensor networks using IEEE 802.15.4 technology [9]. If such a HANId conflict occurs, the HAN coordinator may detect the conflict through its received beacons or one of the electric appliances belonging to the HAN can notify the HAN coordinator on receiving signal from two HAN coordinators with same HANId. On notification, the HAN coordinator performs the conflict resolution procedure [2]. This mechanism mainly covers the channel scans and coordinator realignment procedure that includes choosing a new HANId and broadcasting it to all its HAN nodes. After resynchronization with beacons, the network is ready to communicate in a stable way. Thus, the conflict resolution ends. We present an attack scenario in which an adversary device can frequently send forged conflict notification messages to the HAN coordinator and enforce the coordinator to perform the conflict resolution procedure repeatedly. A smart attacker, which is able to easily produce HANId conflict notification messages by setting the related field in the message frames, can use these forged messages to prevent or greatly delay communication between the smart meter (i.e., the HAN coordinator) and the apartment's electric appliances.

In the remainder of this section, we demonstrate the impact of the HANId conflict attacks on SG communications through computer simulations in MATLAB [10]. In particular, we

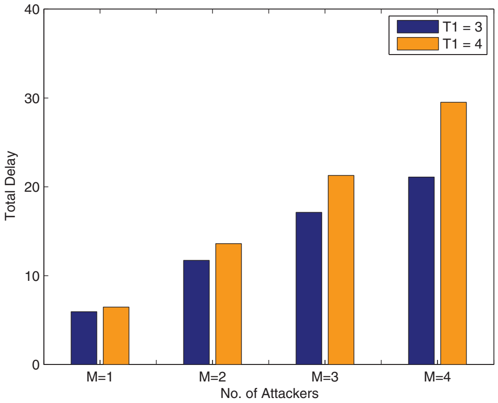


Fig. 2. Conflict resolution delay in case of using $T1$ (i.e., different threshold based detection of HANId conflict attacks) for varying number of attackers.

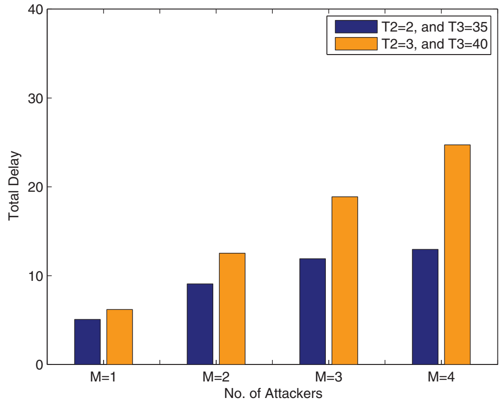


Fig. 3. Conflict resolution delay in case of using $T2$ and $T3$ (i.e., threshold based detection of HANId conflict attacks in specified time duration) for varying number of attackers.

simulate the considered HANId conflict attack to study its effect on HAN communications delay. The simulation model is typically a HAN employing IEEE 802.15.4 (ZigBee) technology. The simulated HAN consists of a HAN coordinator (i.e., smart meter) and 15 devices connected to the HAN coordinator in a star topology. Some of those devices act as malicious users (i.e., attackers) during the simulation runs. After the association process amongst the devices and the HAN coordinator, the attack-node(s) is/are assumed to send fake HANId conflict notification messages at arbitrarily chosen times. When the HAN coordinator receives a conflict notification, it performs the appropriate handling mechanism as part of the IEEE 802.15.4 specification [2].

One of the important parameters in the simulation model is the interval time between recieving a conflict at the HAN coordinator and the end of the realignment process. We set this parameter to 3 seconds as being observed in [11]. Since the HAN coordinator is not able to process any other conflict notifications during this realignment process, the HAN coordinator just ignores any HANId conflict notification during those 3 seconds period. The simulation time is set to 100 seconds within which the attacker(s) are assumed to send 10 fake HANId conflict notification messages at random times. Because the attack-node(s) may not be synchronized with one another, some attacker(s) may send the fake conflict during the realignment process of the coordinator that may lead to ignoring some conflict notifications from the attacker(s).

The HAN coordinator parameters are refered to as $T1$, $T2$, and $T3$. $T1$ is defined as the maximum number of conflicts for an attacker while $T2$ is the maximum number of HANId conflicts in a duration time ($T3$) for an attacker. Three scenarios are considered with varying numbers of attacker(s) ranging from one to four. The results are shown in Figs. 2, 3, and 4.

First, we consider a scenario whereby only $T1$ is taken into account as shown in Fig. 2. Two cases are considered, namely for $T1$=3 and $T1$=4. In the first case, when the maximum number of allowed attacks is set to three (i.e., $T1$=3), the total conflict resolution delay at the HAN coordinator continues to increase. For instance, for a single attacker model with $T1 = 3$, the detection latency is 5s in contrast with almost 20s of detection delay when there are four attackers in the system. On the other hand, when the system is relaxed to allow one more HANId conflict (i.e., when $T1$=4), the detection delay approaches approximately 30s for four attackers. This shows that even with conventional threshold-based detection schemes, multiple attackers may have a significant impact on the SG communications for nearly 20-30s, during which other legitimate devices are deprived of the utility service as they are detached from the HAN coordinator, which goes through the realignment process.

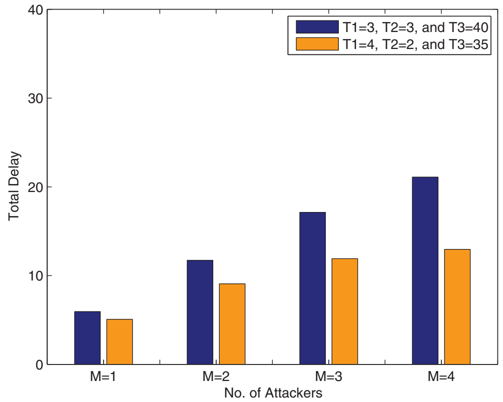


Fig. 4. Combined effect of all three considered parameters ($T1$, $T2$, and $T3$) on the HANId conflict resolution delay.

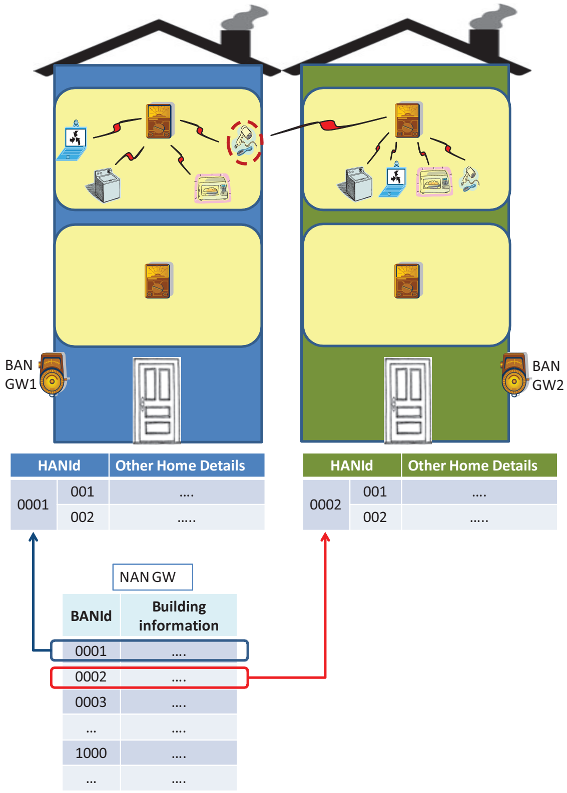
In the second scenario, only $T2$ and $T3$ are taken into account and the total conflict resolution delays are plotted for varying numbers of HANId conflict attackers as depicted in Fig. 3. When $T2$=2 and $T3$=35s, the HAN coordinator, takes approximately 5s and 13s to detect the cases comprising a single attacker and four attackers, respectively. On the other hand, when $T2$ is set to 3 for $T3$=40s, the HAN coordinator experiences much longer time (approximately 25s) to resolve the HANId conflict notifications from the four attackers. This happens because of the fact that the conflict resolution mechanism is executed by the HAN coordinator repeatedly in this case.

In the third and final scenario, we combine the effect of all the parameters (i.e., $T1$, $T2$, and $T3$) at the HAN coordinator to investigate the influence of the attack resolution on SG communications. As evident by the results presented in Fig. 4, the HANId conflict resolution delays are significant for various parameter settings and increase more with the number of attackers.

Thus, these results indicate that the HANId conflict attacks will affect the SG communications if they go unchecked. Therefore, it is essential that we prevent them from occurring in the first place by envisioning an appropriate SG communications framework.

V. Envisioned Solution

In this section, we present a SG communications framework to prevent HANId conflict attack from occurring in the first place. Our proposed framework consists in two types of data repositories at the NAN GW and the BAN GW, respectively. The NAN GW repository contains the building information and the BANIds that refer to unique identifiers to represent each BAN in the considered neighborhood area. When a new building is constructed in a neighborhood, the new BAN GW sends a request, over WiMax, to its corresponding NAN GW manager to register with the NAN GW. NAN GW creates a BANId for this new building area network by incrementing the total number of already existing buildings in its covered neighborhood by one. It is worth noting that the NAN GW may employ other information pertaining to the building (e.g., building name, owner name, and so forth) to create the BANId. It then sends the registered BANId to the appropriate BAN GW, which saves it in its own repository. In this way, the NAN GW can also track the number of buildings in a useful fashion. On the other hand, at the BAN GW, the BANId is used to construct the HANIds of all the HANs belonging to that particular BAN. For a particular apartment's HAN, the HANId consists of its BANId as the preamble following by the apartment number as shown in Fig. 5. In this simple illustration, the apartment number has been used to follow the preamble to obtain a unique HANId for each apartment. Upon activation of the HAN of a new apartment in a given buildining, the BAN GW, thus, creates a HANId and other details pertaining to the apartment. It is, again, worth mentioning that the BAN GW may use other information regarding the apartment to create its HANId. Thus, in such a managed framework, it is not possible for an apartment to obtain a duplicate HANId. This eliminates the chance of HANId conflict attacks. In other words, if a compromised device connected to a HAN attempts to send a HANId conflict attack, the HAN GW will immediately know that this HAN is the only one to subscribe that particular HANId. At this stage, the HAN GW takes the following actions.



HANId		Other Home Details
0001	001	....
	002	.....

HANId		Other Home Details
0002	001	....
	002	.....

BANId	Building information
0001	....
0002	....
0003	....
...	....
1000	....
...	....

Fig. 5. Envisioned framework to prevent occurrence of HANId attacks.

1) The HAN GW considers the node, which sent the HANId conflict message, as malicious, and ignores future HANId conflict messages from the malicious node. It should be noted that the HAN GW does not entirely block the malicious node as this may deny service to the equipment and isolate it from the power supply.
2) The HAN GW then downloads and forces secure framework update for the node deemed malicious.
3) It informs the owner (e.g., by sending a short text message to his/her cellphone) about the event so that he/she may manually check and repair the equipment.

In Fig. 5, we provide a worst-case scenario whereby there are two adjacent buildings. The portrayed apartments in these two adjacent buildings lie side by side and very close in a densely populated urban environment. In the absence of our envisioned framework, the HANs in these two buildings may be assigned the same HANId. Since the equipments in these two HANs are to operate in a work space very close to each other, they would continuously send HANId conflict messages to their respective HAN GWs. Our presented solution deals with this issue by assigning unique BANIds to each building networks that are, in turn, used to construct unique HANIds even in this exceptional case.

VI. Conclusion

In this paper, we introduced an appropriate architecture to facilitate SG communications. We then investigated IEEE 802.15.4 based Home Area Network Id conflict attacks. We studied the effect of the attack on SG communications in various attack scenarios through computer-simulations. We stress on the fact that rather than detecting the attack with a significant amount of latency, it is best to prevent the attack from taking place at all. To this end, a proper solution for this problem is envisioned.

References

[1] C. W. Gellings, The smart grid: Enabling energy efficiency and demand response. Lilburn, GA: Fairmont Press, 2009.

[2] IEEE Std 802.15.4^{TM}-2006, Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs).

[3] K. Kowalienko, "Smart Grid projects pick up speed," IEEE, The Institute, Standards, Article 06, Aug. 2009.

[4] A. Hamlyn, H. Cheung, T. Mander, L. Wang, C. Yang, and R. Cheung, "Network Security Management and Authentication of Actions for Smart Grids Operations," Proc. IEEE Electrical Power Conference, Montreal, Que, Canada, Oct. 2007.

[5] G. N. Ericsson, "Cyber Security and Power System Communication-Essential Parts of a Smart Grid Infrastructure," IEEE Trans. Power Delivery, vol. 25, no. 2, Apr. 2010.

[6] A. R. Metke and R. L. Ekl, "Smart Grid Security Technology," Proc. IEEE PES on Innovative Smart Grid Technologies (ISGT'10), Washington D. C., USA, Jan. 2010.

[7] A. Aggarwal, S. Kunta, and P. K. Verma,"A Proposed Communications Infrastructure for the Smart Grid," Proc. IEEE PES Innovative Smart Grid Technologies Conf., Gaithersburg, Maryland, USA, Jan. 2010.

[8] White paper, "The Home Area Network: Architectural Considerations for Rapid Innovation," Available at http://www.trilliantinc.com

[9] S. C. Ergen, "ZigBee/IEEE 802.15.4 Summary," Internal Report to Advanced Technology Lab of National Semiconductor, 2004.

[10] Avaliable at, http://www.mathworks.com

[11] R. Sokullu, I. Korkmaz, O. Dagdeviren, A. Mitseva, and N. R. Prasad, "An Investigation on IEEE 802.15.4 MAC Layer Attacks," Proc. of the International Symposium on Wireless Personal Media Communications (WPMC'07), Jaipur, India, Dec. 2007.