An Intrusion Detection System for Smart Grid Neighborhood Area Network

Nasim Beigi-Mohammadi and Jelena Mišić
Computer Science Dept.
Ryerson University
Emails: {nbeigimo, jmisic}@scs.ryerson.ca

Hamzeh Khazaei
Research and Development Center
IBM, Canada
Email: hamzehk@ca.ibm.com

Vojislav B. Mišić
Computer Science Dept.
Ryerson University
Email: vmisic@scs.ryerson.ca

***Abstract*—Smart grid is expected to improve the efficiency, reliability and economics of current energy systems. Using two-way flow of electricity and information, smart grid builds an automated, highly distributed energy delivery network. In this paper, we present the requirements for intrusion detection systems (IDSs) in neighborhood area network (NAN) as a component of smart grid. We propose an IDS that is implemented in a distributed fashion with respect to NAN's communication and computation needs. An analytical approach is employed for detecting Wormhole attacks. We validate our NAN IDS scheme using OPNET Modeler [1]. The analytical part of the solution is developed in Maple [2] and integrated with OPNET.**

I. Introduction

The utility industry is experiencing a major transformation that enhances energy systems by using advanced technologies and intelligent devices. According to the US department of energy (DoE) "smart grid generally refers to a class of technology that is trying to bring utility delivery systems into the 21st century." The emergence of machine-to-machine (M2M) communication has also begun in developing smart power grid. Such communication occurs among different components of smart grid such as sensors, smart meters, gateways and other intelligent devices [3]. A three-level hierarchy can be defined for smart grid communication network which includes the home area network (HAN), NAN and wide area network (WAN). Advanced metering infrastructure (AMI) makes use of the HAN, NAN and WAN for metering-related functions.

According to the electric power research institute (EPRI), security is one of the biggest challenges for widespread deployment of smart grid [4]. Physically unprotected entry points as well as wireless networks that can be easily monitored and possibly interfered pave the path for attackers. Hence, there should be security mechanisms in place intended to prevent unauthorized use of these communication paths. In addition to security mechanisms, AMI requires a reliable IDS as a second wall of defense so that in case of any security breaches, the grid can detect or deter the violation [5].

Current security solutions to protect NAN usually include physical controls (e.g., tamper-resistant seals on meters), meter authentication and encryption of all network communications, and network controls. IDSs are usually deployed inside the utility network to identify attacks against the headend [6]. This means that current intrusion detection solutions for NAN are based on a central location e.g., in the utility center, and they can suffer from scalability issues (a large-scale network can reach several million smart meters.) More importantly, security administrators have no ability to see the traffic among meters at the edge of the NAN, and they have to rely on encryption, secure key storage, and the use of protected radio frequency spectrum to prevent intrusions. As a result, NAN requires a reliable monitoring solution to detect intrusions locally.

While efforts have been made to investigate the security of AMI, there are a few works that focus on proposing and designing a reliable and efficient IDS for AMI. In [7], authors present a layered combined signature and anomaly-based IDS for HAN. Their IDS is designed for a ZigBee-based HAN which works at the physical and medium access control (MAC) layers. In [6] a specification-based IDS for AMI is proposed. The solution in [6] relies on protocol specifications, security requirements and security policies to detect security violations. However it would be expensive to deploy such an IDS because it uses a separate sensor network to monitor the AMI. Authors in [8] investigate the use of wireless mesh network (WMN) and the security framework for distribution network in smart grid. A response mechanism for smart meter network has also been proposed.

The related works discussed above either are not specifically designed for the NAN or they require a separate network for detecting intrusions in the network. In this paper, we design and implement an IDS for NAN part of AMI. In our solution, we rely on the NAN's own characteristics and propose a low cost in-band IDS that resides on network nodes running normal applications. Therefore our IDS does not require extra nodes as monitoring agents as opposed to some other related works. Depending on the type of attacks to be detected, we employ IDS on some nodes in the NAN which are powerful in terms of computation and communication capabilities. We validate our scheme using OPNET 17.1 [1] integrated with Maple 16 [2]. Our research contribution can be outlined as below:

- We propose a low cost in band solution for IDS taking into account the specifications and requirements of the NAN. Our solution is specifically tailored to detect different types of Wormhole attack which can have severe effects on the network. We introduce Delta Wormhole attack that can target the availability of the whole NAN by attacking a large number of smart meters.
- Our solution can be extended to consider other types of

attacks. In other words, due to modular design of the simulation model as well as IDS module, our solution can be considered as a framework to study the NAN and it's security threats.
- We develop a hybrid model by integrating our analytical model used to detect Wormhole attack with simulation model using OpenMaple and OPNET. To the best of our knowledge, this is the first time that Maple has been integrated into OPNET. This provides all Maple engine capabilities ready to use in OPNET.

The organization of this paper is as follows: in Section II we discuss the NAN and its communication characteristics along with its security concerns. In Section III, we explain our IDS technique and the simulation scenarios. The performance of Our IDS is illustrated in Section IV. We conclude the paper and state the future work in Section V.

II. NAN ARCHITECTURE AND IDS CHALLENGES

We adopt wireless mesh network (WMN) as the technology for NAN due to its scalability with respect to increase of the number of smart meters [9], [8]. In a NAN, smart meters send their data through single/multi-hop communication to a collector. In order to save energy in collection of data coming from smart meters, collectors forward the aggregated data to the utility center by combining the packets (saving headers) or even removing redundant information [10], [11]. Since smart meters are nodes within WMN, they are involved with forwarding and routing data packets to the collectors. Each smart meter maintains a list of peers so that in case of failure of one peer, it can switch to the next available peer. Hence, redundant paths make the network more reliable [12].

We have used AODV as the routing protocol as suggested by [13]. Although modifying our solution to utilize the most recent routing standards for NAN such as routing protocol for low power and lossy networks (RPL) [12] would be straightforward. We made smart meters keep using the discovered path (i.e., building a path tree) unless there is a problem with the path. As a result, the routing discovery takes place only once when smart meters turn on unless they loose their connection to their path tree. Such a routing scheme seems as the most suitable solution due to the limited communication and computation capabilities of smart meter networks as discussed in [14].

The primary functionality of NAN is that smart meters transmit meter readings toward collectors in one direction and on the reverse direction the utility center sends control messages to smart meters e.g., blackout a customer who is unwilling to pay his bill. There could be different incentives to attack the NAN including financial gain, personal revenge, looking for hacker community acceptance or chaos [15].

In a wormhole attack, colluding compromised smart meters can target the availability of the NAN. This attack occurs during routing through multi-hop path in NAN. In this attack, the compromised smart meters in the NAN which are not direct neighbors are connected to each other via a high-speed connection. One of the compromised smart meters sends route requests (RREQ) that it hears form its neighbors during the route discovery phase through the wormhole link to the other malicious smart meter. The other compromised smart meter which is in the vicinity of destination (collector) sends the RREQ to the collector. Since such a RREQ is the first one to reach the collector, the collector replies the route response (RREP) to the malicious smart meter and ignores later received RREQs with the same ID. Replaying RREP by the first compromised smart meter, makes the neighbor smart meters think that the wormhole path is the best path to the collector. As a result, smart meters choose the wormhole link as the best path to reach the collector.

After launching wormhole attack, compromised nodes can either act actively or passively. They can simply drop all data packets (black hole attack) or they can selectively drop packets (gray hole attack) e.g., dropping a packet after transmitting n packets, a packet every t seconds, or a randomly selected number of the packets. The attackers may also keep intercepting the packets to derive useful information e.g., information about the availability of individuals at homes for burgling purposes. In addition, when wormhole attack is performed between two neighbor NANs, some critical smart meter messages such as status messages or alarms may miss their deadline. In such an attack, initially wormhole nodes attract such traffics and intentionally make them travel longer distance (e.g., through another NAN) than their real shortest paths.

III. NAN IDS

Our proposed IDS is a hybrid of signature-based and anomaly-based detection systems. We seek for signature of attacks in the communication performed in the smart meter networks and compare it with the behavior that is expected from the nodes. If anomalies are found within the network, the IDS will generate alarms. Following the description of our proposed IDS, its architecture and detection mechanisms are explained.

A. Network Architecture and IDS Design

We develop a simulation model in OPNET which mainly focuses on the NAN part. Our simulation consists of NAN, WAN, and the utility site. Fig. 1 depicts a subnet-level view of the scenario that is used in our simulation. We have utilized the node model ip32_cloud to simulate the WAN. The ip32_cloud represents an IP cloud supporting up to 32 serial line interfaces at selectable data rate through which an IP traffic can be modeled.

For defining the application running on the smart meters, we choose automatic reading application. Automatic reading is a non-polling event where smart meters send their meter readings in a predefined frequency. For defining such an application we had to create a custom application as OPNET's default application formats did not match our need.

The proposed IDS is a distributed solution in which depending on the type of attacks to be detected, the task of intrusion detection is performed by some nodes which have enough

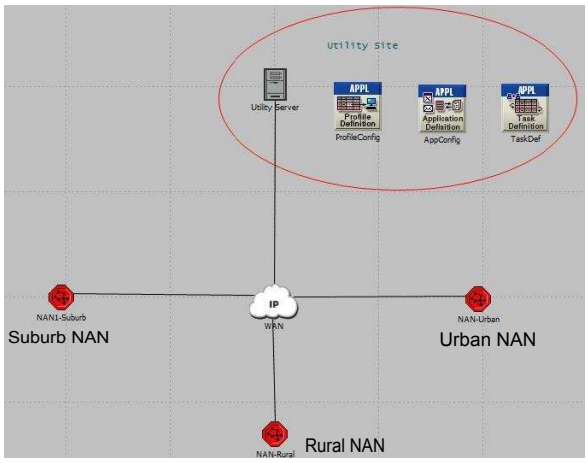

Fig. 1: High level simulation scenario.

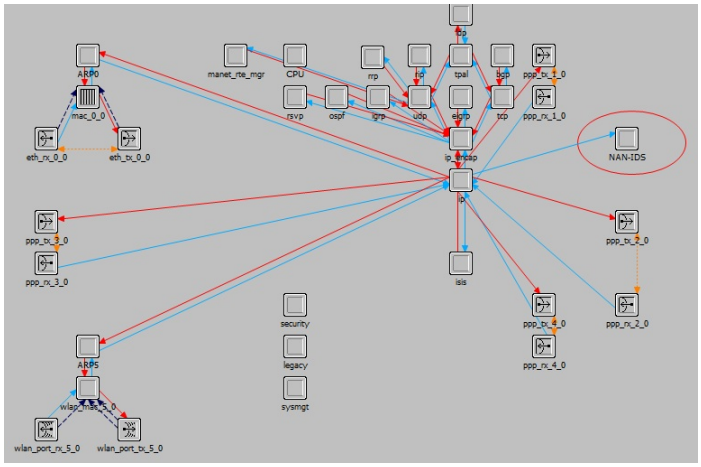

Fig. 2: Collector node model + IDS.

communication and computation capacities. We choose collectors in each NAN as monitoring nodes since they have higher capacity and computational power than smart meters and have tamper resistant hardware. As smart meters are nodes with limited communication and computation features, this seems as a suitable solution for intrusion detection in smart grid NAN. We assume that there is an end-to-end security between smart meters and collectors (as trust points) which means that collectors decrypt the smart meter data, aggregate, then re-encrypt, and forward it to the utility center over the WAN. We are aware that aggregation can be performed on the encrypted data (e.g., using additive privacy homomorphism protocols [10]), but the first approach (aggregation after decryption at collectors) better fits our IDS solution. This enhances the IDS features in several ways. The detection task is performed at a faster pace at the collectors as opposed to at the utility center. For example, false data packets can be detected sooner at the collectors rather than remaining undetected until they are decrypted at the utility center. More importantly, by distributing the IDS on collectors, we solve the problem of scalability which can occur in a central approach.

When a smart meter turns on, it starts discovering neighbors in order to connect to the NAN. After successful authentication using authentication schema such as mesh security association (MSA) [16] or simultaneous authentication of equals (SAE) [17], the smart meter needs to find the best path to the collector in order to send its data.

Fig. 2 shows the collector node model in our simulation model. We have developed a separate module called NAN-IDS shown in a circle to host our IDS engine. We have implemented new *manet_mgr* and *aodv-rte* processes to facilitate our IDS operation.

In this work, our method for detecting Wormhole attack makes use of hop count metric from [18], [19]. Our approach is based on geographical locations of smart meters. As smart meters are static nodes, we can obtain their location information easier compared to mobile ad-hoc nodes. One approach is to use global positioning system (GPS) to get the exact location of smart meters. Another approach for obtaining location of smart meters is from IDS nodes (collectors) given that nodes are registered with the collector ahead of time. Hence, geographical location can be used as a reliable measurement for estimating shortest path length between each smart meter and the corresponding collector in each NAN.

B. Hop Count Estimation

We adapt the euclidean distance estimation model in [19] for our smallest hop count estimation. The model describes the relation of euclidean distance and the corresponding hop count along the shortest path. Based on the model, given the euclidean distance between the sender and receiver, the receiver (i.e., collector) can estimate the smallest hop count to the sender (i.e., smart meter).

The collector measures the minimum euclidean distance between itself and a smart meter as

$$d = |l_c - l_s| \tag{1}$$

where l_c is the location of the collector and l_s is the location of the smart meter.

We use arbitrary $(0, 0)$ as the coordinates of a smart meter, S, and $(d, 0)$ as the coordinates of collector, C, in our calculations. The average density of the network is N_A nodes per unit area, then on the average there are $N_A * \pi r^2$ nodes in the set Φ within S's transmission range, r. For an arbitrary node i in Φ with coordinates (X_i, Y_i) the distance between i and C is:

$$euc_i = \sqrt{(X_i - d)^2 + Y_i^2}$$

in which X_i and Y_i are random variables with a uniform distribution

$$f_{(X_i,Y_i)}(x_i, y_i) = \begin{cases} 1/\pi r^2, & P_i \in \Phi \\ 0, & \text{otherwise} \end{cases} \tag{2}$$

Then the density function of EUC_i can be derived as

$$f_{EUC_i}(euc_i) = \frac{2}{\pi r^2} euc_i \cos^{-1} \frac{euc_i^2 + d^2 - r^2}{2euc_i d}$$

We assume there is a node P within S's transmission range and has the shortest euclidean distance to C. P is selected for the next hop along the shortest path to the destination. Since P is the closest node to C, we have

$$EUC_P = min\{EUC_i | i \in \Phi\}$$

Accordingly, the probability density function of EUC_P can be derived as

$$f_{EUC_P}(euc_P) = N_A \pi r^2 (1 - F_{EUC_i})^{N_A \pi r^2 - 1} f_{EUC_i}(euc_i)$$

and the mean value is obtained

$$E(euc_P) = d - r + \int_{d-r}^{d+r} (1 - F_{EUC_i}(euc_i))^{N_A \pi r^2} deuc_i \quad (3)$$

where

$$F_{EUC_i}(euc_i) = \int_{d-r}^{euc_i} f_{EUC_i}(euc_i) deuc_i$$

$E(euc_P)$ gives us our first hop and the value of hop count is increased by 1. Recursively applying the above method, we can obtain the hop count of the shortest path from the smart meter to the collector. For each recursion, we establish a new coordinate. This procedure is repeated until the remaining distance to C is no longer than r.

Using estimated shortest path, we can compute the estimated minimum hop count value, hc_e, for each flow from a smart meter to the collector. When a tunneling Wormhole attack is launched by malicious nodes, the number of hops indicated in the packet's field, hc_r, will be less than estimated minimum hop count, hc_e, as colluding malicious smart meters remove hops between the smart meters and collector.

After modeling the estimation algorithm and obtaining the estimated hop count in Maple, we need to plug it into our simulation model in OPNET. Thus, we have used OpenMaple which allows interaction with Maple engine from an external environment.

As discussed before, in reality, smart meter locations can be registered in the collectors ahead of time (e.g., when smart meters are registered within the utility center). However, in order to support high degree of scalability in our simulation, we require each smart meter to send its location information along with their RREQ packets. To this end, we have modified the RREQ packet structure in OPNET, shown in Fig. 3, to carry the location information.

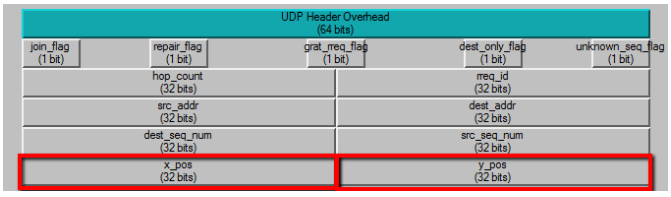

Fig. 3: Modified RREQ packet in OPNET.

When smart meters want to find the best path to the collector, they put the location information in the RREQs, sign and broadcast them. When the IDS in the collector receives the RREQs, it starts examining them. After calculating the estimated hop count, hc_e, using the location information, the IDS checks the legitimacy of the hop count in the received RREQ packets, hc_r, using following equation:

$$hc_r > \alpha hc_e \quad (4)$$

If the above condition is satisfied, the source smart meter is not under Wormhole attack, otherwise IDS flags the smart meter as being attacked. Parameter α is adjustable to the network characteristics and was set to 1 in our simulation scenarios.

C. Simulation Scenarios

We have modeled 3 real geographical regions including suburban, rural and urban areas. Fig. 4 shows the geographical image of the simulated suburb NAN. Table I represents the smart meters simulation configuration according to [11], [20]. We suppose the nodes' transmission in the NAN is perfect and signals propagate through open space, with no environmental effects. However, there are a couple of propagation models in OPNET which are neither free nor in the scope of this work.

TABLE I: Suburb Smart Meters Configuration.

Parameter	Value
Physical Channel Property	802.11g
Data Rate	24 Mbps
Transmission Power	0.005 W
Receiver Sensitivity	-95 dBm
Meter Reading Payload	512 Byte
Meter Reading Transmission Frequency	30 min
Density (N_A)	9 per $1km^2$

Fig. 4: Geographical image of the simulated suburb NAN

The chosen regions allow placing meters uniformly and placing the collector at the center of the region.

We have simulated different attack scenarios by changing the location and also the number of Wormhole end points in order to affect different parts of the network. We intend to observe how our IDS performs with respect to these scenarios. We refer to some of the Wormhole attack scenarios as Pair attacks as there is a pair of attackers.

In this work, we call the attack presented in Fig. 5 as Delta Wormhole which is comprised of three interconnected colluding attackers aiming to attack a wider range of smart meters.

Such an attack is more powerful that common Wormhole attack (i.e., consisting of two attackers) as it can bring down the availability of the whole NAN. It should be noted that the attackers can also be external nodes but should have enough credentials to communicate with the NAN nodes.

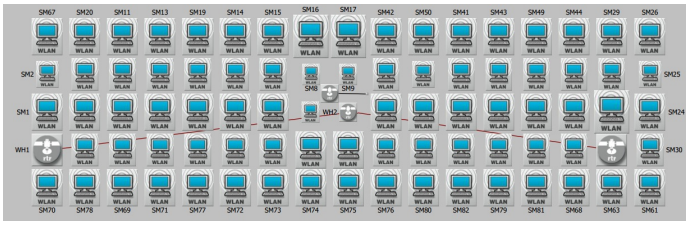

Fig. 5: Wormhole attack: Delta in suburb NAN

IV. Results From Simulation Experiments

In this section, the IDS results for suburb, rural and urban NAN scenarios are presented. We demonstrate our IDS performance for detecting Wormhole attacks by measuring false positive (FP), false negative (FN), and detection rate (DR).

The effects of Wormhole attacks on hop count distribution in suburb area are presented in Figs. 6, and 7 for a number of Pair attacks and Delta attack respectively. As can be seen Wormhole attacks decrease the number of larger hop counts and add up to the number of smaller hop counts in all attack scenarios. We have the largest decrease in hop count distribution in Delta attack because two parts of the NAN are under attack. One possible intuition that can be extracted from the hop count distribution is the possible number of colluding Wormholes in the NAN. More specifically, if the hop counts of nodes from two far corners of the NAN have decreased at the same time, the IDS will conclude that there are probably more than two attackers targeting the network.

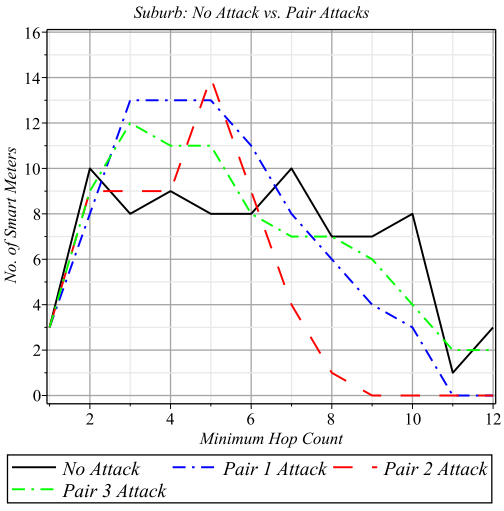

Fig. 6: Distribution of minimum hop counts of no-attack, Pair 1, Pair 2 and Pair 3 attack scenarios in suburb NAN

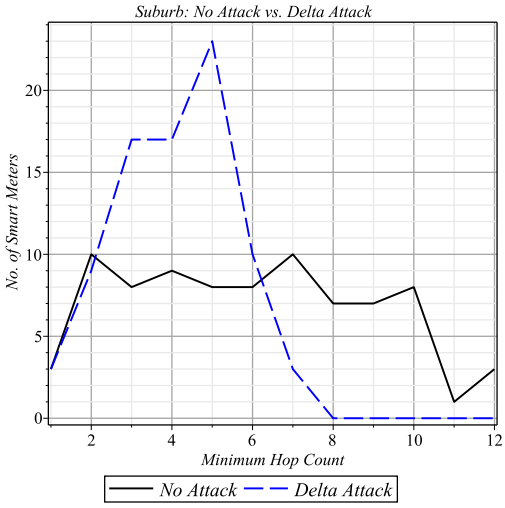

Fig. 7: Distribution of minimum hop counts of no-attack and Delta attack scenarios in suburb NAN

TABLE II: IDS result for suburb NAN

Wormhole Attack Type	FP	FN	DR	No. of Attackers
No Attack	1%	N/A	N/A	0
Pair 1	7%	5%	95%	2
Pair 2	6%	6%	94%	2
Pair 3	5%	5%	95%	2
Delta	3%	8%	92%	3
Overall	4.4%	6%	94%	2

The results of IDS detection for suburb, urban and rural areas are presented in Tables II, III and IV respectively. The simulation time was set to 12 hours and N_A was set to 9, 25 and 3.5 for suburb, urban and rural areas respectively.

TABLE III: IDS result for urban NAN

Wormhole Attack Type	FP	FN	DR	No. of Attackers
No Attack	4%	N/A	N/A	0
Pair 1	7%	5%	95%	2
Pair 2	5%	0%	100%	2
Pair 3	5%	6%	94%	2
Delta	3%	2.8%	97%	3
Overall	4.8%	3.45%	96.5%	2

TABLE IV: IDS result for rural NAN

Wormhole Attack Type	FP	FN	DR	No. of Attackers
No Attack	0%	N/A	N/A	0
Pair 1	0%	5%	95%	2
Pair 2	0%	8%	92%	2
Pair 3	0%	6%	94%	2
Delta	0%	4%	96%	3
Overall	0%	5.7%	94.2%	2

From Tables II, III, and IV it can be seen that the FP rate gets increased with density. Urban area with the average of 4.8% has the highest FP rate while rural area has average FP of 0%. This lies in the fact that when density, N_A, gets bigger in formula for calculation of estimated hop count, it tends to

give larger estimated hop count, therefore, in the equation 4, estimation hop count, hc_e tends to be larger than received hop count, hc_r. As a result, the IDS might detect more normalities as attack which leads to a larger FP rate.

On the other hand, from Tables II, III, and IV, FN is smaller in denser area, i.e., urban area, than suburb and rural areas. The reason is that when hc_e tends to be larger than hc_r, there are less number of cases where hc_e becomes less than hc_r which results in a lower FN rate in the urban area compared to rural and suburb areas. Therefore, depending on the network topology, security concerns, and administrative preferences, parameter α can be adjusted to obtain desirable FP, FN, and DR rates.

V. Conclusion and Future Work

In this work, we proposed an IDS taking into account the specifications and requirements of the NAN. Our solution detects Wormhole attack which can have severe effects on the NAN. Our detection mechanism takes advantages of an analytical model which calculates the estimated hop count between smart meters and the collector. By integrating the analytical model with the simulation model in OPNET Modeler, we evaluated our IDS for three different areas including rural, suburb and urban scenarios. The detection rates showed that Our IDS performs well in detecting wormhole attacks in all three scenarios. The FP rate in urban area was the highest due to the density and high number of nodes while the FN rate had the highest value in rural area because of less number of nodes in the network.

A number of modifications and extensions can be made to enhance the the proposed IDS:

- In our IDS, we only considered automatic meter reading traffic in the NAN. Automatic reading traffic is an uplink traffic (from smart meters to the utility center) and is only a one-way transmission. Other application traffic that can be considered (from utility center to customers) are demand response (DR), remote disconnects, firmware updates and etc.
- The main source of error in our IDS was related to the cases that the estimated hop count were equal to the received hop count. As a result, the IDS might fail in detecting real attacks. One approach that can solve this problem is to consider packet travel time in the IDS.
- Another improvements that can be made to our IDS is to add propagation model to the NAN. Such a modification will bring about the ability to evaluate the performance of the whole network along with the IDS solution.
- Our model can be modified to employ RPL [12], which is one of the recent routing protocol standard for NAN. Hence attacks specific to RPL can be studied through our simulation model and our IDS solution can be tailored to detect such attacks.

Acknowledgment

This work was supported by NSERC and Toronto Hydro Electric System Limited (THESL).

References

[1] OPNET Technologies, Inc., "OPNET Modeler 17.1," Website, Mar. 2011, http://www.opnet.com.

[2] "Maplesoft inc., Maple 16," Website, Mar. 2013, http://www.maplesoft.com.

[3] Z. M. Fadlullah, M. M. Fouda, N. Kato, A. Takeuchi, N. Iwasaki, and Y. Nozaki, "Toward intelligent machine-to-machine communications in smart grid," *IEEE Communications Magazine*, vol. 49, no. 4, pp. 60–65, Apr. 2011.

[4] NIST, "Report to NIST on smart grid interoperability standards roadmap EPRI," Jun. 2009.

[5] N. Beigi-Mohammadi, J. Mišić, V. B. Mišić, and H. Khazaei, "A framework for intrusion detection system in advanced metering infrastructure," *Wiley Journal of Security and Communication Networks*, 1939-0122 2012.

[6] R. Berthier and W. H. Sanders, "Specification-based intrusion detection for advanced metering infrastructures," in *IEEE 17th Pacific Rim International Symposium on Dependable Computing (PRDC)*, Dec. 2011, pp. 184–193.

[7] P. Jokar, H. Nicanfar, and V. Leung, "Specification-based intrusion detection for home area networks in smart grids," in *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Oct. 2011, pp. 208–213.

[8] X. Wang and P. Yi, "Security framework for wireless communications in smart distribution grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 809–818, Dec. 2011.

[9] S. McLaughlin, D. Podkuiko, S. Miadzvezhanka, A. Delozier, and P. McDaniel, "Multi-vendor penetration testing in the advanced metering infrastructure," in *Proceedings of the 26th Annual Computer Security Applications Conference*, 2010, pp. 107–116.

[10] A. Bartoli, J. Hernandez-Soriano, M. Dohler, A. Kountouris, and D. Barthel, "Secure lossless aggregation for smart grid M2M networks," in *First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Oct. 2010, pp. 333–338.

[11] K. Thambu, J. Li, N. Beigi-Mohammadi, Y. He, J. Mišić, and L. Guan, "Toronto hydro-electric system Ltd-Ryerson center for urban energy: Secure and reliable data communication for smart grid," Dec. 2012.

[12] P. Kulkarni, S. Gormus, Z. Fan, and B. Motz, "A self-organising mesh networking solution based on enhanced RPL for smart metering communications," in *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, Jun. 2011, pp. 1–6.

[13] A. Aimajali, A. Viswanathan, and C. Neuman, "Analyzing resiliency of the smart grid communication architectures under cyber attack," in *5th workshop on cyber security experimentaion and test*, Jul. 2012.

[14] C. Bennett and S. B. Wicker, "Decreased time delay and security enhancement recommendations for AMI smart meter networks," in *Innovative Smart Grid Technologies (ISGT)*, Jan. 2010, pp. 1–6.

[15] F. Skopik and Z. Ma, "Attack vectors to metering data in smart grids under security constraints," in *IEEE 36th Annual on Computer Software and Applications Conference Workshops (COMPSACW)*, Jul. 2012, pp. 134–139.

[16] I. Akyildiz and X. Wang, *Wireless Mesh Networks*, ser. Advanced Texts in Communications and Networking. Wiley, 2009.

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

[18] X. Wang and J. Wong, "An end-to-end detection of Wormhole attack in wireless Ad-hoc networks," in *31st Annual International Computer Software and Applications Conference, COMPSAC*, vol. 1, Jul. 2007, pp. 39–48.

[19] H. Wu, C. Wang, and N. Tzeng, "Novel self-configurable positioning technique for multihop wireless networks," *IEEE/ACM Transactions on Networking,*, vol. 13, no. 3, pp. 609–621, Jun. 2005.

[20] "Wi-Fi alliance, Wi-Fi for the smart grid mature, interoperable, secure technology for advanced smart energy management communications," Sep. 2010.