On Intrusion Detection in a Neighbourhood Area Network in the Smart Grid

Nasim Beigi-Mohammadi[1], Hamzeh Khazaei[2], Jelena Mišić[1], Vojislav B. Mišić[1]

[1]Ryerson University, Toronto, ON, Canada

[2]University of Manitoba, Winnipeg, MB, Canada

Contribution to the State of the Art

DOI: **10.7251/JIT1201007M** UDC **504.06+502.17**

Abstract: Smart grid, which is an upgrade of power electric system, mainly relies on powerful communication networks to provide a secure, reliable and efficient information delivery. Updating a system as complex as the electrical power grid with a large number of components has the potential of introducing new security vulnerabilities into the system. Hence, security mechanisms should be deployed to protect the smart grid as a first wall of defence against malicious attacks. As a second wall of defence, there should be intrusion detection systems in place to protect the smart grid against any security breaches. In this work, we describe an anomaly-based intrusion detection system (IDS) for neighbourhood area network whose security is of critical importance in smart grid.

Keywords: Intrusion Detection System, smart grid, Neighbourhood Area Network

Introduction

Advanced Metering Infrastructure (AMI) is a communication infrastructure that enables meters and utilities to exchange information such as power consumption, firmware updates, remote disconnects or outage awareness [1]. An AMI includes several communication networks that can be generally classified into: Home Area Network (HAN), Neighbourhood Area Network (NAN) and Wide Area Network (WAN) [18]. HAN is the network of sensors that communicate with smart meters in residential or industrial area while NAN is a network of neighbouring smart meters that communicate with collecting nodes, namely, collectors. WAN serves as a communication link between utility center and data collectors. An overview model of the AMI is shown in Figure 1. AMI introduces new security challenges since it consists of billions of low-cost commodity devices being placed in physically insecure locations. The equipment is under the control of the often disinterested, unsophisticated, or sometimes malicious users. The author in [3] discusses the security requirements and related threats of the four main components of an AMI: smart meters, the customer gateway, the communication network, and the head end. The fact that encryption and authentication alone are not sufficient to protect the infrastructure is emphasized. In AMI, availability and integrity of data take precedence over confidentiality [11][17]. Attacks targeting AMI can be classified into three categories including network compromise, system compromise and denial of service [2].

Traffic modification, false data injection and replay attacks try to compromise the network [10] while compromised node and spoofing of metering devices are examples of attacks which target the systems. Flaws or misuses of routing, configuration, and name resolution are considered as denial of service attacks. While threats discussed in [3] are required to be highly taken into account when designing security mechanisms, AMI lacks a reliable monitoring solution. One approach for designing an IDS for AMI is to leverage the existing IDS techniques that have been used in other types of networks. However, there are AMI-specific challenges that need to be aware of when designing an IDS for AMI. The IDS should be highly accurate since at the ultimate end it deals with availability which is considered to be the most critical aspect of smart grid [14]. Moreover, it should have a low communication and computation overhead on the network due to resource constraint devices in AMI. Traditional IDS mechanism including a number of lightweight agents reporting to a central management server is not applicable in such system. For instance, AMI networks may contain millions of nodes that with a central approach for monitoring and intrusion detection, the traffic load, required storage and computational capabilities at the central server could be overwhelming. Therefore, a distributed approach should be considered. In a distributed IDS, data processing is distributed among intermediate nodes and only high level data is sent to the central server [5]. In this work, an anomaly-based IDS for NAN is proposed which utilizes several rules to detect anomalies in the network.

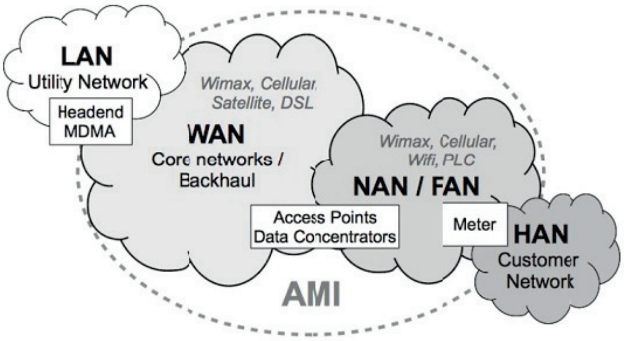

Figure 1. Overview of AMI networks (after [2]).

The rest of this paper is organized as follows: in Section 2, we briefly survey some related work. A realistic intrusion scenario is described in Section 3. Section 4 elaborates the IDS solution, while Section 6 presents the rules for the IDS. Finally, Section 5 concludes the paper and outlines some promising directions for future work.

Related Work

While many efforts have been made to investigate the security of AMI, there are a few works that focus on proposing and designing reliable and efficient IDS for AMI. Berthier, Sanders, and Khurana [2] discuss the requirements and practical needs for monitoring and intrusion detection in AMI. Kush *et al.* [7] have surveyed the gap analysis of intrusion detection in smart grid. They identify and present the key functional requirements of the IDS for smart grid environment. Jokar et al. [5] present a layered specification-based IDS for HAN. Their IDS is designed for ZigBee technology which is deployed in HAN communication. They specifically address the physical and medium access control (MAC) layers. Their work, however, is a partial solution since it only takes the two lower layers of ZigBee technology into account (i.e., considering only 802.15.4) as their feature space.

In [1], a specification-based IDS for AMI has been proposed. While the solution in [1] relies on protocol specifications, security requirements and security policies to detect security violations, it would be expensive to deploy such IDS since it uses a separate sensor network to monitor the AMI.

Roosta *et al.* [13] propose a model-based IDS working on top of the WirelessHART protocol, which is an open wireless communication standard designed to address the industrial plant application, to monitor and protect wireless process control systems. The hybrid architecture consists of a central component that collects information periodically from distributed field sensors. Their IDS monitors physical, data link and network layer in order to detect malicious behaviour. While authors provide a detailed explanation of their work, their IDS solution cannot be completely applied to NAN IDS because it is protocol-specific.

Authors in [11] investigate a technique for evaluating the security of the myriad of devices being deployed into the AMI. They show that they can leverage focused penetration efforts in one vendor to others, and explore where such evaluations must focus on the unique artefacts of a system under test. This work provides a comprehensive but high-level classification of attacks targeting AMI.

As a result, to the best of our knowledge, there is no published research that particularly addresses IDS for the NAN. In this work, IDS is proposed for the NAN which can be considered as the core part of AMI. The proposed IDS is an anomaly-based solution which considers the constraints and requirements of NAN. The IDS captures the communication overhead constraints as well as the lack of a central point to install an IDS on it by proposing a distributed IDS that is run on some nodes which are powerful in terms of memory, computation and the degree of connectivity.

Realistic Intrusion Scenarios

One of main incentive to attack smart grid is energy fraud in which attackers try to tamper with metering infrastructure so that they are not billed for the energy they consume. The attempt to disable metering-related functions falls into the denial of service (DoS) category of attacks. One of the important DoS attacks that occurs in NAN prevents meters from acting on commands such as usage queries, firmware updates and remote disconnects. Figure 2 shows a typical DoS attack on meter command execution. A realistic example for this type of an attack is when a smart meter is failed to respond to a usage query and a malicious customer takes advantage of not being billed for some amount of time. The adversary has two choices to do so; either prevents the command from execution or prevents the command from reaching to the target smart meter. In former, adversary can either exhaust the system resource e.g., allocating and maintaining the maximum allowed number of open connections or by leveraging a firmware bug causing a system hang [11]. Another situation is when the adversary tampers with the forwarding of packets away from the meter by dropping traffic destined for that meter that can happen at link and routing layer at the back haul network (WAN) and NAN. An adversary can also prevent the packets from reaching his home smart meter by malfunctioning a middle smart meter which is one of the next hops of his own meter toward utility center.

The main focus of this work is on DoS attacks that occur in NAN as a result of the en route meter nodes that may malfunction and interfere with the proper forwarding of packets (e.g., by delaying, altering, misrouting and dropping.) Such smart meters are either spoofed or under attack. DoS attacks can be launched against physical layer by using radio jamming (e.g., a source of strong noise) which may interfere with the physical channels and hinder the availability of the network. Examples of such an attack include trivial jamming, periodic jamming and reactive jamming. At the MAC layer, a compromised node may not follow the agreed-upon frequency-hopping which will result in a large number of collisions. Unprompted CTS (Clear To Send) and reactive RTS (Request To Send) jamming attacks are examples of DoS attacks that occur at the MAC layer [15]. At the network layer, black hole, grey hole and wormhole attack can be performed by a malicious node. Such attacks will cause the packets to be dropped or misrouted. Another attack that may occur in the NAN, is when the attacker transmits a flood of packets toward a target node or congests the network and reduces its performance.

Table 1 shows some of the possible threats.

Table 1: Description of possible threats.

Threat	Threat description
1	Signal jamming at the PHY level
2	Packet collision at the MAC level
3	Misrouting and packet dropping attacks (e.g., black hole, wormhole, grey hole, …)
4	Packet flooding

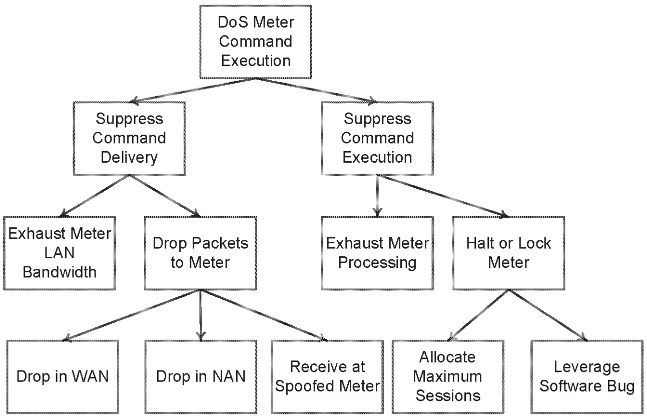
DoS Meter Command Execution
Suppress Command Delivery
Suppress Command Execution
Exhaust Meter LAN Bandwidth
Drop Packets to Meter
Exhaust Meter Processing
Halt or Lock Meter
Drop in WAN
Drop in NAN
Receive at Spoofed Meter
Allocate Maximum Sessions
Leverage Software Bug

Figure 2: DoS Meter Command Execution Tree, adapted from [11].

An IDS which acts as a second wall of defence is necessary for protecting smart grid if security mechanisms such as encryption/decryption, authentication and etc. are broken. Generally, techniques for intrusion detection are classified into three main categories:

Signature- or pattern-based, which rely on a predefined set of the so-called attack patterns or signatures to identify attacks. Such techniques are often summarized as: what is bad, is known – what is not bad, must be good.

Anomaly-based, which rely on statistical knowledge and perhaps also particular models of correct node behaviours and mark nodes that deviate from these models as malicious. Such techniques are often summarized as: what is usual, is good – what is unusual, must be bad.

Specification-based, which rely on predefined behavior (often using a set of constraints and monitor the execution of programs/protocols with respect to these constraints. Such techniques are often summarized as: what is good, is known – what is not known, must be bad.

Out of these categories, anomaly detection performs best when there is a potential for unknown attacks to occur [6]. As noted above, anomaly detection uses statistical knowledge of correct node behaviour and flags behaviour that deviates from normal system use. A typical anomaly detection system takes in audit data for analysis. The audit data is transformed to a format statistically comparable to the profile of a user. Initially, the user's profile is generated dynamically by the system and it is subsequently updated based on the user's usage. Thresholds are always associated to all the profiles. If any comparison between the audit data and the user's profile results in a deviation that crosses a set of threshold, an intrusion alarm is set [9, 16]. The fundamental reason for choosing an anomaly-based IDS for NAN is because of the existence of many unknown attacks that target the NAN and the number of such attacks will most likely increase as the smart grid becomes more widespread. Therefore, the IDS should be capable of detecting not only existing attacks but also new attacks.

Proposed IDS for NAN

Figure 3 shows a typical NAN in which smart meters are connected in an adaptive wireless mesh network and all of them can perform routing. Each node maintains a list of parents so that in case of a failure of one parent, it can switch to the next available parent. Hence, redundant paths make the network more reliable. A fully redundant routing requires both spatial and temporal diversity; spatial diversity refers to enabling each smart meter to discover multiple possible parents and then establish link to two or more. Temporal diversity refers to fail-over and retry mechanisms [13]. RPL and geographical routing protocol are two popular candidates that can be used in such a RF mesh network [4, 8].

The proposed solution is a distributed and hierarchical anomaly-based IDS. The reason for proposing a distributed IDS is that the metering network is resource constraint; smart meters have limited computation power and they cannot spend more energy monitoring their neighbours. Moreover, if all smart meters are to run IDS, they are always busy sending monitoring messages to their supervisor nodes and this is not possible in the low bandwidth network that exists between smart meters. That is why the proposed solution requires only a subset of nodes to run IDS.

The proposed IDS embraces three different IDS nodes, namely, field IDS, WAN IDS and central IDS. Field IDSs are run on the collectors as well as some smart meters whose connectivity degree is between certain thresholds. Such smart meters should also have extra memory compared to ordinary smart meters so that they can be capable of monitoring their neighbours in addition to normal functions. Note that, each smart meter should be directly connected to at least one IDS node. Field IDS nodes should be tamper resistant as nowadays most smart meters are. Field IDSs are responsible for passively monitoring the communication of the neighbour smart meters to collect trace data. They provide reports of detected attacks to central IDS in utility center. Another option is that field IDSs send detection messages to base stations residing in the WAN. The WAN base stations that act as bridges between NAN and WAN are assumed to have sufficient computational power and memory, so that they can run WAN IDSs. WAN IDSs are responsible for the incoming and outgoing traffic from and to collectors and, in case of intrusion detection, they report the malicious collectors to the central IDS. Central IDS resides in the utility center which is responsible for making global decisions based on alarms and notifications coming from the WAN and field IDSs.

The proposed IDS has three phases; data gathering, compliance check, inference that are explained in the followings. A feature set is selected from the intrinsic and observable characteristics of communications to distinguish normality from anomaly.

Phase 1 (data collection phase): in this phase, field IDSs listen on the communication of neighbour nodes and check them to see if there is any abnormal behaviour in their communication. WAN IDSs also check the communication coming from the collectors seeking for unusual activities. Central IDSs also check the communication of WAN access points and make sure about the healthiness of their communication. The communication information about each neighbour can include, but not limit to, number of transmission attempts, number of ACKs received, number of received packets and etc.

Phase 2 (compliance check phase): IDS nodes extract the data from phase 1 and perform compliance check with the normal behaviour.

Phase 3 (inference phase): After finishing phase 2, the results are sent to an inference part to derive the final decision in order to see whether the detected anomaly is a malicious attack or it is just a transient failure. To make accurate decisions in this phase, the IDS node must keep the history of the monitored nodes to distinguish between occasional network failures from real attacks.

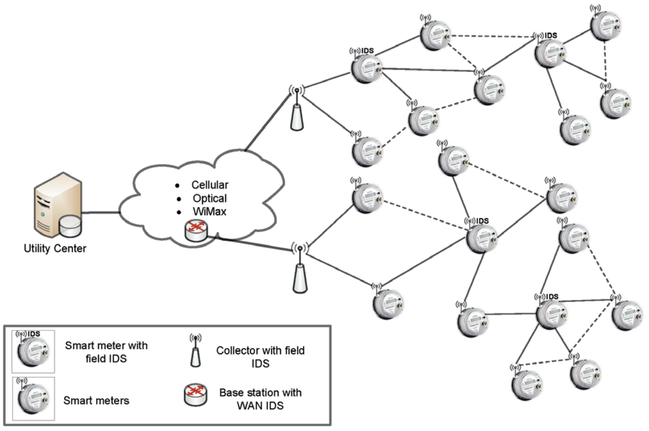

Figure 3: Neighbourhood Area Network IDS.

When an intrusion is detected, the system should take appropriate actions in response to an attack. Passive response is typical in the IDS in which the information is logged of and there is also a real-time notification. However, since NAN comprises wireless networks and the devices are located in insecure places, there should be an active response in place. If detected threat reaches a certain confidence level, required counter measures should be taken. For instance, in case of jamming attack in MAC layer, central office in substation will send a control message to the target meter to change its transmission channel.

Note that it is assumed that the communication between nodes is secure and IDS nodes are authenticated with each other using digital signatures. It is also assumed that there is an Access Control List (ACL) that all nodes have unique link keys associated with their unique IDs.

Policy Rules

In this section, we discuss in detail the policy rules which are used to detect anomalies in the system.

The IDS node should monitor the number of packets its neighbours transmit in number of bytes. Since the number of communication message types (e.g., firmware updates, usage queries and responses, offers and etc.) between smart meters and utility center is not infinite, therefore, the size of exchanged data between smart meters and utility center can be determined. Any size of data beyond the maximum value can be tagged as a suspicious message. If the number of such messages exceeds a certain threshold, IDS node should raise a flag indicating a potential threat. An example of such an attack is flooding attack. Such a rule can be implemented at field IDSs, WAN IDSs and central IDS.

Transmission power level is another parameter that can be used to detect a signal jamming attack at physical layer since the level of power for transmission is a pre-configurable parameter for deployed nodes. The IDS node can monitor its neighbour to detect any deviation from the accepted levels. Such a rule can be implemented at field IDS since the central IDS cannot monitor such a feature.

Field IDS nodes monitor the frequency/channel hopping sequence. Two nodes should agree on the frequency hopping sequence for the time slots in which they want to communicate with each other. As a result, if there is any sequence-nonconforming nodes, the node IDS should raise a flag indicating a DoS attack at MAC layer. Field IDS should apply this rule.

MAC delay transmission is another characteristic that can be monitored by the field IDS. When the utility center issues a command to a smart meter, the smart meter should respond by a certain delay. If the smart meter does not respond in the expected time frame, the field IDS should tag the smart meter node as a suspicious one and watch for more such anomalies. An example is when the smart meter is under jamming attacks and cannot transmit the data by the expected time out.

The central IDS should look for normal behaviour of smart meter applications for sending ACKs. Only the central IDS can check this feature, since the application data is encrypted in the transmission layer (e.g., using SSL) and it can be decrypted only at the utility center. Therefore, if there is a large number of missing ACKs and retransmissions, the central IDS should tag the smart meter as a suspicious one. Next, the central IDS launches an investigation to identify the source of malicious activity using lower level IDS nodes. By probing the nodes along the path to the suspicious node, the source of problem will be detected. An adversarial case is where one of the next hops of the smart meter is intentionally dropping the packets destined for that meter.

Field IDS should monitor the layer at which nodes are communicating. Since smart meters are supposed to communicate with each other only at the network layer, any smart meter's attempt to communicate with its neighbour at a different layer should raise a flag. An example of such an attack is warm hole attack in which the malicious node tries to send the traffic to some illegitimate destinations.

WAN and field IDS should monitor the request/reply pattern that is coming from the central office and smart meters. Requests must only arrive from the central office and responses must be directed to central office. If a request is coming from another source or the smart meter is trying to send the packets somewhere different from the central office, IDS nodes should alarm and notify the central office.

Table 2 links the threats listed in Table 1 with the applicable IDS detection rules outlined above.

Table 2: Threats and Corresponding Rules.

Threat	Rule 1	Rule 2	Rule 3	Rule 4	Rule 5	Rule 6	Rule 7
1	✓	✓					
2			ü	ü			
3				✓	✓	✓	✓
4	✓			ü			

Conclusion

The development of practical and efficient IDS for smart grid is highly crucial. While reasonable amount of research has been done in designing and implementing of IDS for different parts of smart grid, there is a critical need for designing an IDS for the NAN part of the smart grid. The insecure places where metering devices are located increase the potentials for intrusions within the grid. This work focuses on designing an IDS for NAN by taking the constraint of NAN into account. The proposed IDS scheme is a distributed anomaly-based solution which looks for anomalies at different layer of network stack by applying a set of rules. In case of detecting an attack, the IDS will raise an alarm highlighting the malicious activity.

In order to measure the detailed performance of the proposed IDS, such as false positive and false negative rates, detection time and the ability to differentiate between transient failures and malicious behaviours, we need a more detailed analysis of the IDS solution. Furthermore, we plan to expand the threat model to capture more adversarial cases and examine the proposed IDS using a suitable simulator such as OPNET [12].

References:

[1] Berthier, R. and Sanders, W.H. (2011) Specification-based intrusion detection for advanced metering infrastructures. *Proc. IEEE 17th Pacific Rim Int. Symp. Dependable Computing (PRDC'2011)*, pages 184–193, Dec. 2011.

[2] Berthier, R., Sanders W.H. and Khurana, H. (2010). Intrusion detection for advanced metering infrastructures: Requirements and architectural directions. *Proc. IEEE SmartGridComm*, pages 350–355, Oct. 2010.

[3] Cleveland, F.M.(2008). Cyber security issues for advanced metering infrasttructure (ami). In Power and Energy Society General Meeting -Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE, pages 1–5, Jul. 2008.

[4] Iyer, G., Agrawal, Monnerie, P. E. and Cardozo, R.S. (2011). Performance analysis of wireless mesh routing protocols for smart utility networks. *IEEE SmartGridCom*m, pages 114–119, Oct. 2011.

[5] Jokar, P., Nicanfar, H. and Leung, V.C.M. (2011). Specification-based intrusion detection for home area networks in smart grids. *IEEE SmartGridComm*, pages 208–213, Oct. 2011.

[6] Komninos, N. and Douligeris, Ch.(2009). LIDF: Layered intrusion detection framework for ad-hoc networks. *Ad Hoc Networks* **7**(1):171–182, 2009.

[7] Kush, N., Foo, E., Ahmed, E., Ahmed, I. and Clark A. (2011). Gap analysis of intrusion detection in smart grids. In Craig Valli, editor, 2nd International Cyber Resilience Conference, pages 38–46. secau-Security Research Centre, Aug. 2011.

[8] Lichtensteiger, B., Bjelajac, B., Muandller, C. and Wietfeld, C. (2010) RF mesh systems for smart metering. *IEEE SmartGridComm*, pages 379–384, Oct. 2010.

[9] Liu, Y., Li, Y. and Man, H.(2005). Mac layer anomaly detection in ad hoc networks. In Information Assurance Workshop IAW'05. pages 402–409, Jun. 2005.

[10] Lu, Z., Lu, X., Wang, W and Wang, C. (2010) Review and evaluation of security threats on the communication networks in the smart grid. *Proc. MILCOM 2010*, pages 1830–1835, Nov. 2010.

[11] McLaughlin, S., Podkuiko, D., Miadzvezhanka, S., Delozier, A. and McDaniel, P.(2010). Multi-vendor penetration testing in the advanced metering infrastructure. Proc. 26th Ann. Comp. Security Applications Conf., pages 107–116, 2010.

[12] OPNET Technologies, Inc. Opnet modeler 17.1. Website, Mar. 2011. http://www. opnet.com.

[13] Roosta, T., Nilsson, D.K., Lindqvist, U. and Valdes, A. (2008). An intrusion detection system for wireless process control systems. Proc. 5th IEEE Int. Conf. Mobile Ad Hoc Sensor Syst. MASS'2008, pages 866–872, Oct. 2008.

[14] Schuba, C.L., Krsul, I.V., Kuhn, M.G., Spafford, E.H., Sundaram, A.and Zamboni. D. (1997). Analysis of a denial of service attack on TCP. Proc. IEEE Symp. Security and Privacy, pages 208–223, May 1997.

[15] Seth, S. and Gankotiya, A.(2010). Denial of service attacks and detection methods in wireless mesh networks. In Int. Conf. Recent Trends in Information, Telecommunication and Computing (ITC), pages 238–240, Mar. 2010.

[16] Xu, R., Li, J., Zhang, F. and Levy, R. (2006). Model selection for anomaly detection in wireless ad hoc networks. 12th International Conference on Parallel and Distributed Systems ICPADS'06, (CD-ROM), 2006.

[17] Yan, Y., Qian, Y. and Sharif, H.(2011). A secure and reliable in-network collaborative communication scheme for advanced metering infrastructure in smart grid. Proc. IEEE Wireless Comm. Networking Conf. (WCNC'2011), pages 909–914, Mar. 2011.

[18] Zhang, Y., Wang, L., Sun, We., Green, R. C. and Alam, M. (2011). Distributed intrusion detection system in a multi-layer network architecture of smart grids., *IEEE Transactions on Smart Grid* **2**(4):796–808, Dec. 2011.

Submitted: April16, 2011
Accepted: June 1, 2011