A Distributed Monitoring Architecture for AMIs: Minimizing the Number of Monitoring Nodes and Enabling Collided Packet Recovery

Incheol Shin
The Attached Institute of ETRI, Korea
icshin@ensec.re.kr

Jun Ho Huh
University of Illinois at Urbana-Champaign
jhhuh@illinois.edu

Yuseok Jeon
The Attached Institute of ETRI, Korea
jys0710@ensec.re.kr

David M. Nicol
University of Illinois at Urbana-Champaign
dmnicol@illinois.edu

ABSTRACT

The electrical power grid is in the midst of a breathtaking transformation into the "Smart Grid". A key element is development of the Advanced Metering Infrastructure (AMI), which is changing the way utilities interact with smart meters at customer sites. However, with the technology comes the new risks of cyber-attacks that could exploit vulnerabilities in different parts of the communication layers, and potentially affect significant portions of the power grid. This paper proposes a novel *distributed* monitoring architecture that is capable of selecting a subset of smart meters used as intrusion detection sensors – a subset selected to *minimize* the number of meters needed while keeping the communication. Our architecture enables recovery of collided packets (that are subject to packet inspection), improving the overall reliability and accuracy of distributed monitoring.

Categories and Subject Descriptors

C.2.1 [**Network Architecture and Design**]

Keywords

Smart Grid, Advance Metering Infrastructure, Intrusion Detection System, Security

1. INTRODUCTION

The Smart Grid initiative aims to propel utilities and their electricity delivery systems into the 21st century with the aid of various information and communication technologies. The hopes are high: many believe that it will increase automation of generation, transmission, and distribution of power, ease the management for utilities, and help consumers to make better decisions. Bidirectional communication between the consumers and utilities – this is enabled through the smart meters – will facilitate more efficient usage of electricity. The infrastructure that provides the means for the smart meters at homes to reliably communicate with the utilities (sharing information about the electricity rates) is the Advanced Metering Infrastructure (AMI) in Figure 1. An AMI refers to a logical amalgamation of two core Smart Grid functionalities, "incentive-based demand responses" and "automated meter reading". The former promises to help consumers choose when to use electricity heavily (e.g., to run an electric clothes dryer) as a function of dynamically changing price. The latter improves utilization of a utility's manpower, allowing them to perform measurement and control activities that currently require a human presence at the meter.

Cyber-attacks that target AMIs cannot be taken lightly. A major concern is that the exposed infrastructure creates a much larger attack surface, creating opportunities for cyber-intruders to interfere with the network carrying data and commands between utilities and meters, and indeed, potentially gain access within the utility and out to the larger transmission and generation facilities they control. While AMI security now receives increasing research attention, we have yet to see real, practical solutions that can effectively mitigate these threats in large-scale mesh networks. Some recent studies [4], and [8] have assessed the risks associated with the threats in AMIs, but do not adequately address detection and mitigation techniques. Kush et al. in [6] highlight the lack of adequate intrusion detection systems (IDSes) for the Smart Grid and the limitations of existing systems; McLaughlin et al. [7] consider the energy theft issues in their work. Berthier et al. [3] propose an intrusion detection scheme for AMIs that monitors different communication AMI networks and detects intrusions based on protocol-level specifications. Their work, however, does not consider practical architectural issues of supporting this style of detection, missing a discussion on where and how IDS sensors should be deployed.

Grochocki et al. [1] conduct a comprehensive analysis of the potential threats to AMIs, and describe a few possible IDS deployment schemes. One of the schemes is a distributed sensing infrastructure in which the IDS sensors

SEGS'13, November 8, 2013, Berlin, Germany.

http://dx.doi.org/10.1145/2516930.2516948.

are embedded in the smart meters, inspecting all the packets that are routed via the meters. Such an infrastructure would provide a wider monitoring coverage compared to a more centralized system that relies on, for instance, a single IDS sensor deployed at a head end server. Theoretically, through those distributed, embedded sensors, the entire mesh network (also referred to as neighbourhood area network) traffic can be monitored. Any attack that is performed directly on the meters (e.g., installation of a malware on a meter) can also be monitored.

Our work builds on this idea of distributed monitoring and focuses on three integral issues that were not covered in their work: (1) minimizing the number of monitoring meters, (2) allowing recovery of collided packets that are subject to monitoring, and (3) providing support for complex IDS operations that might be too resource intensive for monitoring meters to handle. To address those issues, we propose a highly reliable and scalable monitoring architecture in a mesh network, utilizing already-existing smart meters as the IDS sensors. The key idea is the selection and connection of a minimum set of monitoring smart meters (referred to as a "monitoring tree") that provide a complete monitoring coverage for all other smart meters and their communications. This is achieved while allowing collided packets to be recovered and inspected. Any series of packets that are subject to more complex IDS monitoring (e.g., a stateful inspection based on whitelisted specifications) are forwarded to a dedicated IDS. Our packet forwarding algorithm drops any duplicating packet being forwarded, and, effectively, minimizes the load on the dedicated IDS.

The remainder of this paper is structured as follows. Section 2 presents the preliminaries and the problem definition. In section 3, we discuss the construction of a monitoring tree in smart meter mesh networks. The experimental results of our monitoring architecture are presented in section 4. Finally, our conclusions and discussion of future work are at Section 5.

2. PRELIMINARIES

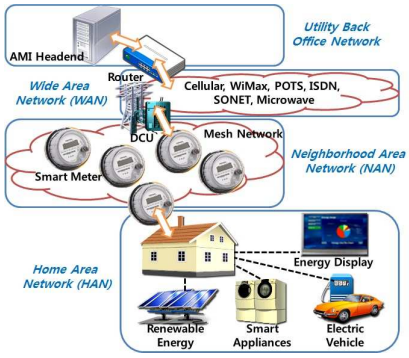


Figure 1: AMI in Smart Grid

2.1 Wireless Smart Meter Mesh Networks and Security Threats

The primary security concern about AMIs revolves around the easily accessible devices such as smart meters with the associated communication hardware, and especially, considerable number of critics have implies that lethal attacks could be initiated through smart meters. Some AMI implementations utilize mesh networks with wireless smart meters in NANs to provide self-adapting multi-path multi-hop communications between the meters with various radio technologies. Mesh networks are attractive for NANs, due to the cost-efficiency and fault-tolerance. However, insufficient emphasis of security on the wireless AMI communication technologies could result in crucial disruption of power delivery [1]. Furthermore, since smart meters with wireless devices are located in customers' premises outside of utilities' physical security perimeters, they are at high risk of compromise.

We will model a mesh network of n wireless smart meters graphically. Each wireless smart meter is assumed to have a uniform transmission radius r (although this assumption is for simplicity of exposition more than logical necessity). Under these assumptions the network can be modeled as a *Unit Disk Graph* $(UDG) G = (V, E, w)$ in a 2-dimensional plane, where V represents the set of wireless smart meters, E represents the set of wireless communication links, and w is a non-negative weight of propagation delay assigned on each edge $e = (u, v)$. Between any two smart meters $u, v \in V$ there exists an edge $(u, v) \in E$ iff $d(u, v) \leq r$ where $d(u, v)$ denotes the Euclidean distance between u and v with the transmission range r.

2.2 Threat Model

Due to the rareness of security threats to power utility systems, adversarial activities to breach into smart meter mesh networks in this work refer to the threat model in [3]. Several methods for exploiting wireless devices used in AMI networks are addressed in [5], including extracting critical data and modifying the memories to insert malicious software. These vulnerabilities suggest that meters can be compromised by an attacker, with the infection spread out throughout the various networks comprising the Smart Grid.

3. A MONITORING TREE BASED DISTRIBUTED MONITORING ARCHITECTURE

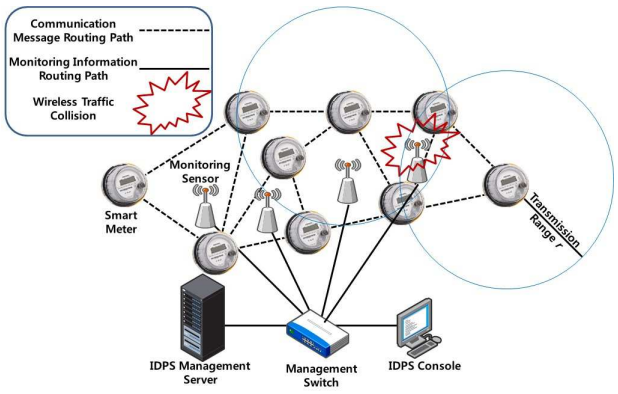


Figure 2: IDPS as described by NIST

Intrusion detection is a preventive measure aimed at identifying actions that attempt to compromise confidentiality, integrity or availability of a target resource. Scarfone et al. [10] from National Institute of Standards and Technology (NIST) describe four major components of an Intrusion Detection and Protection System (IDPS): (1) Sensors

and agents monitor and analyze activities on networks or systems; (2) Management servers and centralized devices that collect and manage information forwarded from sensors; (3) Database servers that operate as repositories for events collected from sensors and/or management servers; and (4) Consoles that provide interfaces for IDPSs' users and administrators. They also describe the following wireless monitoring sensor types:

- Dedicated Monitoring Sensors: These perform wireless IDPS functions without relaying network traffic except forwarding monitored traffic to management servers for analysis.
- Access Points (AP): IDPS capabilities are additionally implemented into APs.
- Wireless Switches: Wireless switches with IDPS capabilities as a secondary function assist administrators with monitoring wireless traffic and managing the devices.

However, there is a critical limitation with adopting this kind of IDPS: its inability to deal with packet collisions. First of all, it is not currently possible for an entirely passive IDPS sensor to monitor all wireless traffic from the neighbor smart meters due to the collision of messages, also known as the "hidden terminal problem." For instance, in a highly possible case of simultaneous transmission of any smart meters u and v where $d(u,v) > r$ and a sensor x with $d(u,x) \leq r$ and $d(v,x) \leq r$, x receives nothing but the corrupted messages from u and v by the collision. That is, due to the fact that smart meters u and v are placed in interference-free range to each other by $d(u,v) > r$, they would be able to transmit anytime in accordance with wireless communication protocols, but garbled messages occur to a sensor x from simultaneous transmission of the meters because of $d(u,x) \leq r$ and $d(v,x) \leq r$ as illustrated in Figure 2. The collision from the broadcasting nature of wireless communications decreases the number of messages that are successfully delivered to sensors for intrusion detection operations. It should be noted however that this problem is a result entirely of the sensors being passive. Standard techniques in radio protocols that prevent the hidden terminal effect will work here, if the sensor engages in the network access protocols as though it were an actively communicating node.

Another limitation is that AMIs require encrypted communication, and additional key management solutions must be deployed for monitoring systems to analyze the encrypted payloads in wireless traffic. However, we have yet to find research on efficient key agreement schemes for interaction with intrusion detection sensors; indeed, the monitoring sensors defined in [10] and [3] by design cannot communicate with the meters. Moreover, pre-distribution of secret keys is non-trivial due to the resource constraints in sensors and dynamicity/variation in the mesh networks. Consequently, this implies a clear need for research on development of new approaches for intrusion detection scheme, in the mesh networks comprised of smart meters with wireless devices.

3.0.1 Monitoring Tree(MT)

To avoid the aforementioned limitations, we propose a novel monitoring architecture based on the notion of a *Monitoring Tree (MT)*. The objective is to identify a subset of smart meters, in a topology which ensures that any transmission by any node in the network can be heard by at least one monitoring node. In addition, the MT structure is selected for efficient communication, and to supports techniques that can isolate a meter suspected of being infected, in order to limit the propagation of its communication.

We consider an IDS comprised of a set of meters that do the monitoring, an egress point for the data they collect, and an analysis infrastructure. The most significant difference from existing wireless IDS structures is the absence of separate, passive sensors. Instead we suppose that meters themselves contain software that, when the meter is selected to be a monitor, listens to traffic within its radio range, looking for signature anomalies, and reporting them.

The use of smart meters as monitoring devices has several advantages:

- Smart meters equipped with bidirectional wireless communication modules transmit messages employing collision avoidance rules in the mesh networks. This avoids the hidden terminal problem suffered by passive sensors; the access control mechanism ensures that a monitor hear at most one transmission at a time. A collision in a smart meter from MT would be able to get recovered with simple retransmission requests as described in 3
- The proposed architecture does not require any extra physical devices to be installed in the mesh networks (except for any dedicated IDS sensor used). Firmware updates can put monitoring logic into an existing infrastructure. Therefore this is a scalable, cost efficient architecture.
- Key management can be simplified to some extent. In a typical AMI, "group keys" are used to encrypt some portion of the AMI traffic. Such group keys are already available to the monitoring meters for decrypting packets and performing deep packet analysis. Packets that are encrypted using meter-specific keys would still require those keys to be shared; sketching such a key sharing mechanism is out of scope for this paper though.
- Unlike existing IDPS schemes developed in [10] and [3] which constrain allowable monitoring topologies, the MT structure is flexible. All that is required is that every node be in communication range of at least one node in the monitoring tree.

Consequently, an IDS built using a monitoring tree has variant benefits over existing IDS techniques.

As a full spanning tree over the whole network would accomplish the same objectives as a monitoring tree, it is worth pointing out the performance advantages of the MT. Intuitively, the denser a graph is, the fewer relative number of nodes are needed to ensure just that every node is connected to an MT. This intuition is borne out by theoretical work [9] on the expected number of leaves in random graphs, with the implication that the fraction of non-leaf nodes tends asymptotically towards $1/(de-1)$ percent of all nodes, where de is the average degree of a node. As an MT is basically a tree with leaves removed, this means that for dense communication graphs there are few nodes that have to serve

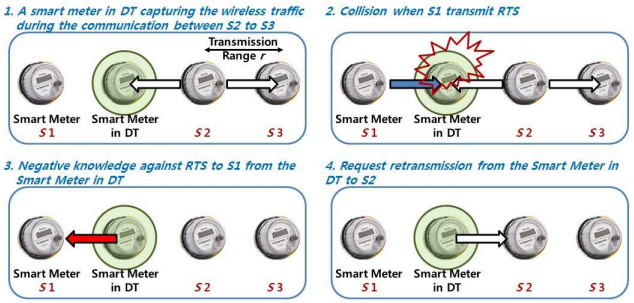


Figure 3: Collision Avoidance in MT

as monitors. This concentrates the communication infrastructure for monitoring, e.g. the monitoring load on the communication network is less. Also, and critically, since a monitoring node synchronizes with the network to avoid the hidden terminal problem (e.g., it will keep a requested transmission from a neighbour from occurring when it is hearing concurrently a different transmission that the requestor does not), the fewer the monitors, the less their synchronization impact on network.

3.0.2 *Construction of Monitoring Tree in Smart Meter Mesh Networks*

In order to construct a monitoring tree T in a smart meter mesh networks G, we leverage our previous work, the Dominating Tree (DT) Problem in [11]. Theoretically, the *Dominating Tree (DT)* problem is formally defined as follows:

DT Problem: Given an undirected weighted general graph $G = (V, E, w)$ representing a network, construct a dominating tree T' such that: (1) each node in V is either in T' or has at least one neighbor in T', (2) $w(T') = \sum w(e')\ e' \in T'$ is minimum.

In [11], we proved that DT is NP-complete and it is inapproximated within $(1-\epsilon)ln|V|, i.e.,$. Due to the reduction on the proof of NP-completeness preserving the approximation gap, we only show the reduction in the proof of inapproximability. We then present in [11] not only an approximation frame work but also a heuristic algorithm with time complexity $O(n^2 \log n)$. Clearly the monitoring tree concept we have identified can be instantiated with a dominating tree, using efficient approximation algorithms.

Figure 4 illustrates the result of computing a dominating tree on a particular topology. In this example only four meters are needed to monitor all traffic, even though there are nine nodes in the network. It is worth noting that any one of a large number of monitoring trees might be found with the property that every node in the network is within one hop of an MT node. However, this requirement does not constrain the solution to find a small number of monitoring nodes. This is the purpose served by the objective function in the DT problem formulation. Minimizing the sum of edge weights in the tree will seek solutions with few, low-cost, nodes. Indeed, if all edges have the same weight, the DT solution will identify a tree with the minimum number of nodes that have the required connectivity property.

As elaborated in Figure 5, we briefly evaluate results of MT construction using a heuristic algorithm from [11], comparing it with the so-called "Minimal Spanning Tree Minus Leaves" algorithm (which simply constructs an MST and then removes the leaf nodes).

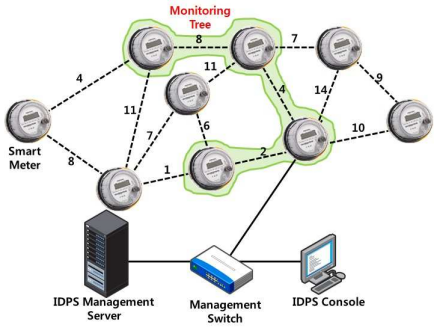
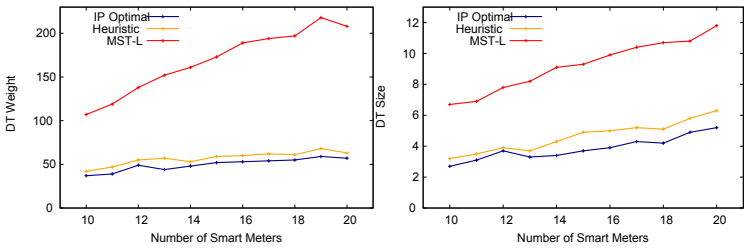


Figure 4: Intrusion Detection System with Monitoring Tree Architecture

Figure 5 compares the performance of three algorithms for computing a monitoring tree, on some randomly generated representative networks. One algorithm is the so-called "Minimal Spanning Tree minus Leaves" (MST-L) algorithm. This simply computes a minimal spanning tree (e.g. a tree over the whole graph whose sum of edge weights is minimized) and removes the leaf nodes. Another is the optimal solution to the DT problem (denoted IP Optimal). The third is a heuristic solution to the DT problem, given in [10], denoted here as "Heur Algo". The graph on the left plots the sum of monitoring tree edge weights (for a variety of graphs of increasing size.) The graph on the right plots the number of nodes in the monitoring tree. The two main conclusions to be drawn from the results are that the MST-L algorithm is significantly inferior to both of the DT solution algorithms, and that the heuristic algorithm gives solutions that are close to optimal.



(a) (b)

Figure 5: Evaluation of Heuristic Algorithm for Contructing Monitoring Trees

Other formulations of the problem as constrained optimization solutions might be considered to achieve other desirable properties of a monitoring network. For example, whereas the DT problem seeks minimization of the sum of edge weights, a desire to ensure fast response to an observed anomaly might incorporate some notion of minimizing the maximum distance from any monitoring node to the egress point. This objective function alone does not encourage solutions with small numbers of monitoring nodes, but successive solution of more constrained problems can deal with

that problem. Supposing we could specify a constraint D and seek a solution that minimizes the sum of edge weights in the monitoring tree, subject to the constraint that the longest path from monitoring node to egress point is no greater than D. By varying D and solving each problem separately, we can develop a set of solutions that give us a handle on the trade-offs between minimal longest communication path, and number of monitoring noes.

Viewed by comparison with existing wireless intrusion detection schemes, an IDS built on top of a monitoring tree has a number of advantages. First, the monitoring tree scales with increasing numbers of meters, as we have seen already, but also is easily extended to incorporate additional egress points and additional IDS servers, shortening the worst case communication path between monitoring node and some management server. Next, the monitoring tree could be fully constructed in a localized manner such that each smart meter synchronously generates the same MT structure using constraints like the need to break the ties with the same edge weight or certain number of neighbours. This requires the premise that our smart meter mesh network systems are loosely synchronized in the order of seconds, but this is reasonable since the smart meters should be timely synchronized in most environments. Finally, anticipating that attackers would seek to disable monitoring trees first, the nodes comprising an MT topology could be dynamically (and perhaps even rapidly) changed as time progress, presenting a sort of moving target to the attacker. This should be contrasted with the fixed location of IPDS sensors or expensive mobile sensors.

3.0.3 *Isolation of Adversarial Network Activities using MT*

The monitoring tree forms a backbone of the network. If we ensure that every node that routes out of the NAN is in the MT, then we are assured that every outbound communication passes through an MT node at least once. MT nodes may be given blacklisting capability, so that if a node is deemed to be suspect by any element of the IDS, its identity can be distributed throughout the MT. Whenever a message from a blacklisted source is presented to an MT node for routing, it can be dropped, insuring that no message from a corrupted meter leaves the network. Indeed, if nodes can be rapidly incorporated into an existing MT, a rogue node might be completely isolated by activating MT functionality in every node to which it can directly communicate.

4. EXPERIMENT

We conducted a series of simulation experiments to evaluate the feasibility and performance of the proposed MT architecture. Reliability of delivering readable network traffic is evaluated through a comparison against NIST's IDPS model. Performance is evaluated by comparing a simple MT of G against a "spanning tree without leaves" (MST-L) of G model. This helps in understanding how our heuristic algorithm improves the efficiency of constructing MTs.

In our simulations, weight of each edge $e = (u, v)$ is defined by $w(u, v) = C_v \cdot d_{uv}^{\gamma}$, where d_{uv} is the Euclidean distance between two smart meters, u and v. γ is predefined value to 2 because it is a typical value for unobstructed environment, and C_v is a random constant. In order to evaluate the performance of each approach, n smart meters with transmission range $r = 300m$ are randomly deployed in a predefined area size of $1000m \times 1000m$. n varies from 10 to 100 with increment of 10, and 100 network instances were investigated for each value of n, and the results were averaged.

[13] tries to alleviate the hidden terminal problem for wireless smart meter networks. The smart meters in their work, however, employ simple busy-ton multiple access protocol for the wireless networks – networks as proposed by [12]. The monitoring sensors (without wireless *transmission* techniques) that are deployed in the IDPS model deliver the captured network traffic from their wireless message receivers via wired network media destined to an IDS server [2]. Our simulations do not consider wireless message losses but they do consider message corruptions resulting from packet collisions. Those results are used to compare the performances and reliability between MT and NIST IDPS architectures.

4.1 Wireless Message Collisions

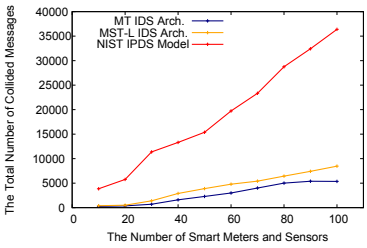


Figure 6: Total Number of Corrupted Messages from Wireless Collision

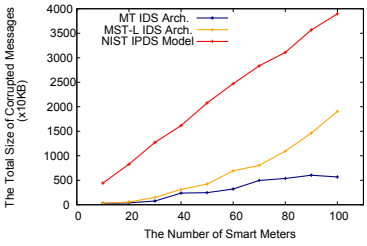


Figure 7: Total Size of Corrupted Messages from Wireless Collision

The simulation results demonstrate the effectiveness of the MT architecture in capturing and delivering the intact network traffic over the hidden terminal problem, which the IDPS model in [2] suffers from. Two performance matrices are used for this comparison: (1) total number of corrupted messages, and (2) total size of corrupted messages from the collision.

Figure 6 shows that the MT approach, on average, maintains only about 10% of the number of corrupted messages of the NIST IDPS model during the increment of first 10 meters. It is worth noting that, the curve generated by IDPS with respect to the 100% increase in the number of meters, from 50 to 100, is significantly steeper. Those observations imply that the MT technique has smaller number of wireless message collisions than IDPS in dense networks. Relatively

smaller number of monitoring meters in MT than MST-L (by the algorithm in [11]) results in 40% less number of collisions.

In addition, figure 7 depicts a curve trend similar to that of figure 6. This is rather obvious: growing number of collisions results in bigger volumes of corrupted messages. The majority of the corrupted wireless messages in MT are induced by collisions with the RTS messages in a meter that monitors the communications between two meters in the case of the advent of a new meter transmitting messages. This implies that the corrupted messages would be able to be recovered using a simple re-transmission technique from the monitoring meters in MT. In contrast, the monitoring sensors in NIST IDPS can do nothing but deliver corrupted messages to an IDS server.

It is obvious that the volume of unrecoverable corrupted messages gets bigger as the mesh network becomes more dense. This implies that he accuracy and reliability of IDSes will suffer as the number of meters in the network being monitored increases.

4.2 Message Delivery

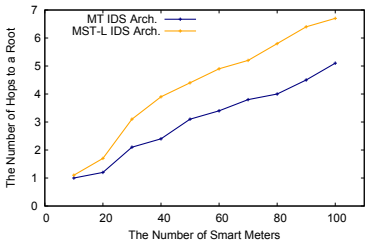


Figure 8: Total Number of Hops to IDS Server

Another important comparison between our MT architecture and NIST IDPS would be the delivery time of the messages being forwarded from the distributed sensors (monitoring meters in our architecture) to the IDS servers. But this comparison would require the knowledge of overall structure of the wired network topology that the messages travel through. Because AMI networks are located in varying sizes, estimating AMI network topologies is not easy. Instead, we look at the number of hops the messages need to travel through to reach the IDS servers are shown here. As depicted in the figure 8, the messages would be able to reach the IDS servers with less than 5 intermediate hops in the MT architecture, and at most 7 intermediate hops in the MST-L architecture.

5. CONCLUSION

A monitoring tree based IDS architecture has been proposed in this paper. It uses already-existing smart meters in the mesh networks as the IDS sensors and achieves high survivability and reliability. Any packet that is subject to a more complex IDS inspection is forward to a dedicated IDS server. Our monitoring tree architecture introduces noticeable benefits over existing proposals for Smart Grid IDSes, namely in the spaces of scalability, localization and recovery of collided packets that are subject to inspection.

Acknowledgment

This work was supported by the Power Generation and Electricity Delivery of the KETEP grant funded by the Korea government Ministry of Trade, Industry and Energy (20111030100020).

6. REFERENCES

[1] D. Grochocki, J.H. Huh, R. Berthier, R. Bobba, W. Sanders and J. Jetcheva. *AMI Threats, Intrusion Detection Requirements and Deployment Recommendations* Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on, page 395–400. 2012

[2] American National Standard Institute (ANSI). *ANSI C12.22-2008 American National Standard Protocol Specification for Interfacing Data Communication Networks.* 2008.

[3] R. Berthier, W. Sanders, and H. Khurana. *Intrusion Detection for Advanced Metering Infrastructures: Requirements and Architectural Directions.* In Proceedings of the 1st IEEE International Conference on Smart Grid Communications, pp. 350–355. IEEE, 2010.

[4] F. Cleveland. *Cyber Security Issues for Advanced Metering Infrastructure (AMI).* In Proceedings of the IEEE Power and Energy Society General Meeting: Conversion and Delivery of Electrical Energy in the 21st Century, pp. 1–5, July 2008.

[5] T. Goodspeed, R. H. Darren, and A. S. Bradley. *Low-level Design Vulnerabilities in Wireless Control Systems Hardware.* In Proceedings of the SCADA Security Scientific Symposium, 2009.

[6] N. Kush, E. Foo, E. Ahmed, I. Ahmed, and A. Clark. *Gap Analysis of Intrusion Detection in Smart Grids.* In C. Valli, editor, 2nd International Cyber Resilience Conference, August 2011.

[7] S. McLaughlin, D. Podkuiko, and P. McDaniel. *Energy Theft in the Advanced Metering Infrastructure.* In E. Rome and R. Bloomfield, editors, Critical Information Infrastructures Security, Volume 6027 of Lecture Notes in Computer Science, chapter 15, pp. 176–187. Springer Berlin, 2010.

[8] A. R. Metke and R. L. Ekl. *Security Technology for Smart Grid Networks.* IEEE Transactions on Smart Grid, 1(1):99–107, June 2010.

[9] A. Renyi, *Some Remarks on the Theory of Random Trees* MTA Mat. Ket. Imt. Kozl., pp. 73–85, 1959.

[10] K. Scarfone and P. Mell. *Guide to Intrusion Detection and Prevention Systems (IDPS).*

[11] I. Shin, Y. Shen, and M. T. Thai. *On Approximation of Dominating Tree in Wireless Sensor Networks.* Optimization Letters, 4(3):393–403, 2010.

[12] C. Wu and V. O. K. Li. *Receiver-Initiated Busy-Tone Multiple Access in Packet Radio Networks.* ACM SIGCOMM 87 Workshop: Frontiers in Computer Communications Technology, Stowe, VT, USA, pp. 11–13 Aug. 1987

[13] F. Xiaojing, W. Hao and T. Jun *An Improved Common Hopping Multiple Access Protocol for Smart Meter Wireless Networks.* Wireless Communications and Mobile Computing Conference (IWCMC), 2012 8th International. 2012