European Wireless 2012, April 18-20, 2012, Poznan, Poland ISBN 978-3-8008-3426-9 © VDE VERLAG GMBH

Security and Smart Metering

Sophia Kaplantzis and Y. Ahmet Şekercioğlu
Department of Electrical and Computer Systems Engineering
Monash University, Clayton 3800, Australia
Email: {sophia.kaplantzis, ahmet.sekercioglu}@monash.edu

***Abstract*—The 'smart grid' is an upgrade of the existing 20th century electrical power grid, promoted to address the pressing issues of end-user energy monitoring, global warming, distributed power generation and emergency response. Smart grids are quickly spawning in Australia, Europe and North America. Security in smart grids is imperative to protect the functionality of their underlying networks, the data they communicate and the privacy of their customers. However, few research efforts have focussed on security in this area and solutions adopted from traditional ad-hoc networks are not suitable, as they would need to be fully integrated with the grid and its legacy systems before they can yield positive results. The purpose of this paper is dual; to review matters of smart grid security and to examine the effect of hacker attacks on smart grid network parameters. Through simulation we investigate how malicious activity targeting the routing layer of smart grid networks can interrupt network effectiveness.**

I. Introduction

In a predominantly digital world that harbors grave concerns for climate change, it has become apparent that we need to revisit our primary sources of power and pollution and revert them to a cleaner, long term and more efficient state. This need when coupled with the rising price of primary fuels, the demand for higher quality energy and the insufficient delivery capacity of a central generation scheme, has led to the concept of the smart grid.

This smart grid is an all round improvement of the electrical grid in place today, starting from the meter at the end-users premises and spanning all the way through the transmission network, to the suppliers back office. It encompasses concepts such as smart metering, smart pricing and smart devices with the aspiration of peak load curtailment, distributed generation and effective demand response [1].

The advantages of implementing smart grids include:

- Environmental benefits resulting from efficient use of existing assets.
- Increased power quality and reliability.
- Reduction of blackout and forced outages
- Reduction in congestion cost, peak demand and restoration times
- Ability for consumers to monitor their use and reduce costs.

In order for these benefits to be realized, it is paramount for data to be transmitted quickly and accurately to all major components of the grid. This is achieved through a fully digital and omnidirectional wireless communication network, which in essence can be considered a Wireless Sensor Network (WSN) [2], with the goal of transmitting measured energy readings wirelessly to a control station, whilst dissipating control information through the network. As previously identified in [3] and [4], the security of a WSN is at jeopardy at all levels of its protocol stack. But how does this threat translate to smart metering applications?

In this article, we focus on the security of smart metering applications. Our contribution is to highlight the effects of malicious hacking activities on the routing protocol of the communication network. Specifically, we investigate the effects of selective forwarding and data spoofing attacks on network functionality for a simple geographic based routing protocol. The results presented in this paper are based on simulations of realistic topologies, using actual geographic coordinates. To the best of our knowledge this is the first simulated study examining the security of the routing layer of smart grid applications.

The remainder of the paper is structured as follows: In sections II and III we introduce the concepts behind the smart grid and the smart meter respectively. In section IV we present the security requirements and threats associated with smart metering applications. In section V we look at routing issues in smart grid networks, including security. In section VI we introduce our local neighbourhood smart metering simulator and the applied attack schemes. In section VII we summarize and discuss our simulated results and finally in section VIII we conclude the paper.

II. The Smart Grid

There are multiple definitions for what a smart grid is, most of which adhere to the following concepts: "A Smart Grid is an electric network which integrates electricity distribution and generation with communications, in order to support the generation of interactive energy and supply quality electricity to the end user" [5]. This concept is closely coupled with the use of digital technologies to control appliances at the consumer's home to save energy, reduce cost and increase reliability and transparency. The major driver behind the smart grid is to reduce consumption through demand response and customer awareness.

Many countries around the world have already deployed smart grids or are involved in investigative deployment projects. It is interesting to note here that an Italian utility, has installed 27 million smart meters, 90% of which are already monitored on a bimonthly basis. In our state of Victoria in Australia it is expected that one million smart meters will be

installed by 2013 to help minimize peak demand caused by increased use of air-conditioners during abrupt summer heat waves.

Other countries investigating the implementation of smart grids include Canada, the USA, the UK and Northern Ireland [6]. It is expected that with the growing trend of international legislative rules, many countries will soon follow.

A. Characteristics and components

Some of the characteristics [5] a successful smart grid should aspire to include:

- Providing high quality electricity
- Incorporating self-healing capabilities
- Integrating distributed energy generation sources
- Efficiently managing and maintaining assets whilst minimizing costs.
- Empowering the end user to make informed consumption decisions
- Enduring security attacks

In order to achieve the above characteristics they will need to make use of a number of enabling technologies such as sensing and measuring equipment, control systems, integrated communication and decision software in the form of artificial intelligence.

From a communication perspective a smart grid can be considered to include the following components:

1) **The smart meter**: which is the source of measured data in the network.
2) **The customer gateway:** which is the interface between the customer household appliances and the smart network
3) **The communication network:** that provides two way communication paths between the smart meters and back office.
4) **The data concentrator:** which is responsible for aggregating data sent from smart meters and for disseminating control information generated from the headend.
5) **The headend:** which receives and analyzes network data and generates control signals.

B. Smart grid & WSN analogy

From the above component description it now becomes possible to draw an analogy between a smart grid network and a WSN in the following manner:

- The smart meter is essentially a **sensor node** which is in charge of collecting data and routing this information back to a central authority
- The **phenomenon** we are looking to sense is the energy consumption at the location of the smart meter.
- The concentrator is the **sink**, which is a network entity with the specific task of receiving, processing and storing data from other sensor nodes
- The **sensor field** covers the entire power distribution network, which could cover suburbs, states or entire countries. In this fashion a smart grid can really be considered as a massively large WSN.
- The headend is associated with the **base station** (BS), which is a point of centralized control within the network with the task of extracting information from the network and disseminating control information back into the network
- The **communication infrastructure** is what connects the entities of the smart grid together, and although many mediums are currently being considered (power line carrier, ADSL, cable etc.), it seems as if the preferred choice is wireless (Zigbee, 802.11, Bluetooth, WiMAX, GSM). This brings the 'wireless' factor into our sensor network.

However all this said, there exist some major issues which have been stalling the international wide spread deployment of the smart grid. Firstly, although the technology exists to enable smart grids, successful integration of all system parts in a unison manner with existing rigid legacy systems is a non trivial task. Another problem is behavioral in the sense that consumers may have trouble operating the involved hardware and software. And lastly investor owned utilities are more likely to promote selling more electricity, rather than less, in order to maximize their profits. One would like to hope however that in the future the promised benefits will quickly outweigh these problems.

III. The Smart Meter

Smart metering in an electrical grid, often referred to as automated meter reading (AMR) or advanced metering infrastructure (AMI), is the act of facilitating real-time measurement, processing and feedback of consumer data throughout a network. The advantages of smart metering embrace multiple participants, including the end user, the metering companies, energy suppliers, grid companies, governments and the environment. Some benefits include reduced metering costs, better quality of supply, easier fraud detection, variable pricing schemes and energy savings for consumers. In fact, it is estimated that each smart meter can offer benefits of up to $60 yearly due to the reduction of labour costs associated with direct metering, call centers, billing, collections and physical disconnections of late paying customers. Also many studies have shown that consumers would use less electricity if they were aware of what they were being charged [1], as price signal is always a strong impediment to wasteful consumption.

In practise, smart metering is achieved by installing intelligent meters equipped with real-time communication capabilities, remote throughput limiters and local device interfacing at the customer's home. It is also provisioned that such meters will also be able to read other nearby commodity meters (water, gas etc). Hence the smart meter is the smart grid's replacement for the legacy electromechanical meter, which is now over one hundred years old.

The smart meter itself is comprised of three major components:

- **A meter** which is capable of recording the electricity consumed or generated by the customer

- **A computer** for logging and processing data and controlling interconnected devices
- **A modem** through which the meter can communicate with nearby meters or the network infrastructure

IV. The Importance of Security

Seeing as the smart meter is a gateway to the household, with the ability to constantly monitor attached devices but more importantly switch them on and off, security becomes a pressing issue [7]. A hacker who successfully dissimulates a smart meter can access confidential information, change control commands and deny access to legitimate systems [8]. It therefore becomes apparent that threats such as repudiation, masquerading and unauthorized access need to be addressed!

So how easy it is to compromise the security of a smart meter and hence the security of the grid as a whole? This question is investigated in [9], where the author examines various grid interfaces and their vulnerabilities. In particular he discusses hacking the communication medium used by the smart devices (wireless and Bluetooth), cracking the device's smart card, attacking the IT infrastructure of the electrical grid itself and even intercepting IP streams of devices that choose to connect via the internet.

A. Security requirements

Generally speaking, a secure smart grid, much like any other secure network, would need to uphold the following requirements whilst managing data:

1) **Confidentiality**: requires that only the sender and the intended receiver should understand the contents of a message. The confidentiality of the information generated and transmitted by the smart grid is paramount to customer privacy and grid success.
2) **Integrity**: requires that the sender and receiver want to ensure the message is authentic and has not been altered during transit without detection. In an smart grid, integrity would mean preventing changes to measured data and control commands by not allowing fraudulent messages to be transmitted through the network.
3) **Availability**: requires that all data is accessible and available to all legitimate network users. Since the smart grid is not only communicating usage information but also control messages and pricing signals, the availability of this information is crucial to the successful operation and maintenance of the grid.
4) **Non-repudiation**: requires that the sender and receiver cannot deny they were the parties involved in the transmission and reception of a message. The accountability of the members of a data transaction is critical when it comes to financial interactions. However, this may be tricky, seeing as data generated by the network can be owned by different entities (customer, data management services, billing systems, utilities) at different times of the data life-cycle.

B. Security threats

Each component of the smart grid architecture faces threats that conflict with the aforementioned security requirements [8].

1) Smart meter: The major issue here is protecting the confidentiality of the data accrued by the smart meter. The last thing paying customers want is for unauthorized entities and marketing firms to be able to gather information about their energy usage habits, such as how much energy they use, at what times they use most energy and which electric devices they have in their homes. Also in order to adhere to integrity requirements, changes should be prevented to data retrieved from the meter and control commands should reach the smart meters unaltered. Imagine a hacker issuing disconnect commands to millions of meters because there was no way of checking the integrity of these commands. Hence the data stored on these devices should be private and physical tampering of the devices (theft, smashing, smart card disturbance) should be prevented. The availability of smart meter data can be compromised by software glitches, component failure, physical damage or tampering by a customer attempting to modify the meters recordings through disconnection or other methods. If smart meter data can be repudiated then that means the basis for billing in the grid is shattered, therefore all changes to meter time/date and tariff must be accounted for.

2) Customer gateway: The customer gateway is an interface into the customers home and may be connected to critical equipment such as industrial equipment and refrigerators, airconditioning units and health monitoring devices. Hence the confidentiality and integrity of these systems must be protected. The availability of load control and pricing signals commands at the customer gateway can have financial impact on the end user. Also, the availability loss of many customer gateways could cause demand response problems which could potentially lead to blackouts. At the gateway all control commands and responses to such information must not be repudiated.

3) Communication network: Seeing as the communication network instigates all information flow within the grid, the privacy of this infrastructure is vital. Communication channels must not allow unauthorized access to data between customer hops or customer-to-customer interactions. You simply don't want your neighbor to know how much your next energy bill will be. Much like all networks and regardless of the medium being used, the smart grid network is vulnerable to attacks (DoS, eavesdropping, jamming etc.) because it is open to external and unsecured environments. The availability of mesh like communication networks can still be jeopardized by points of failure which may be the result of cut cables, radio interferences, decreased bandwidth and path losses. Admissibility of the communication network can also be caused by excessive traffic, perhaps due to flooding of alarms which in turn may limit or even hinder critical information from being dealt with in a timely fashion. Availability of the communication network is necessary to compliment the accountability of the customer.

We can't have a gateway that claims to have sent information, if the network can't guarantee that it has transferred it.

4) Concentrator: The concentrator faces the same threats as the smart meter with the only difference that the implications of a compromised concentrator are much more severe. If the confidentiality of the data processed by the concentrator is breached, the privacy of entire neighbourhoods will be jeopardized. If the integrity of the concentrator data is tainted, then actions resulting from erroneous measurements and control signals will be actuated, something which is very undesirable. If physical problems render a concentrator unavailable, then redundancy solutions will need to be in place. Since there is much at stake here, the security applied to a concentrator should be considered very carefully. The availability of the concentrator can be tested by an attacker with a large jamming radio. This would confuse and deafen nearby concentrators and stall them for transmitting important control information or gathering readings.

5) Headend: The headend is supposedly a secured environment in a utility or data management site, where standard IT security measures are used. However, customer information that is being used for billing and other operations must be kept confidential and not be disclosed to unauthorized entities. Integrity concerns also arise because data and control information is widely available to knowledgable personnel. At the headend, measured data can be modified, dropped or replaced and invalid data and control commands can be issued to reset meters, connect/disconnect meters and distributed generation devices, change pricing signals and initiate demand response. Imagine the destruction a disgruntled employee could unleash from the headend. Availability at the headend may be compromised as a result of interfacing problems between the legacy systems already in use and the new technologies that need to be used. This issue would need to be considered in the initial design phase of the backend systems. The headend gathers all information transferred to it from the communication network and determines what future operations are necessary. These decisions along with the audit logs must be non repudiable.

C. Security Constraints

Each component of the smart grid is also bounded by physical limitations that drastically affect the security solutions that can be employed.

1) Smart meter: Due to the large number of meters that need to be purchased and installed in a smart grid, it is essential that the meters themselves are cost effective [8]. The meter needs to perform a number of tasks, most of which are unrelated to security. So adding features that improve meter security such as audit logs, self diagnostics and security upgrades can increase the cost of the meter. Another problem is that smart meters are installed in places accessible to the public, making them more vulnerable to tampering attacks. In order to thwart such physical attacks, measures must be taken which increase the average cost of the meter. There is a relationship between cost and security that needs to be considered before any major decisions are made.

2) Customer gateway: Much like smart meters, customers gateways perform a number of tasks which may not be directly related to security. The gateway is owned by the consumer and is manufactured by various vendors, making a consistent solution hard to implement. The gateways are also located in insecure environments which may allow for cyber and physical attacks.

3) Communication network: The smart grid's communications network is predominantly serviced by low bandwidth wireless carriers. So solutions that call for the transmission of large encryption keys and certificates will be limited by throughput availability.

4) Concentrator: The concentrators will once again need to be cost effective because they too will be deployed at a large enough scale to not render them single points of failure. Measures should be implemented to ensure that these devices are not easily unplugged or tampered with and that missing data logs can be retrieved after an unexpected outage.

5) Headend: Although the base station of the network is most likely to be located on secured premises, there are many security requirements on the systems that access the data. Many systems (billing, curtailment and control, statistical) will be accessing vast amounts of data and each one of these systems will have to adhere to different access policies, making it hard for one security solution to service all these needs.

V. Routing in Smart Metering Applications

The routing layer of a network provides end to end packet delivery. It is responsible for finding the most efficient path for the packet to travel on its way to a destination. Some of the functions the routing layer performs include flow control, network segmentation/desegmentation and error control.

Routing protocols for WSNs can be split in three categories based on network structure [10].

- **Flat** routing protocols, in which each node plays the same role in order to complete sensing tasks. Information in such protocols is requested through queries.
- **Hierarchical** routing protocols, in which higher energy nodes (such as the concentrator) can be used to process and send information, while lower power nodes perform sensing tasks. Data aggregation and fusion are commonly used among these protocols to improve energy efficiency and scalability.
- **Location based** routing protocols, in which the network nodes are addressed by means of their locations. Distance is usually estimated by incoming signal strength. The coordinates of neighbouring nodes can be acquired by exchanging such information or by using GPS.

In this paper, we will be implementing a Minimum Transmission Energy (MTE) protocol [11], which is a combination of a flat and greedy geographical based protocol. In 'minimum-energy' routing protocols nodes need to route information destined for the base station through intermediate nodes, hence each node acts as a sensor and a router. MTE routes messages in a way which only considers the energy of the transmitters. The result of this behaviour is to have a

messages travel along n low power hops, rather that one high energy transmission.

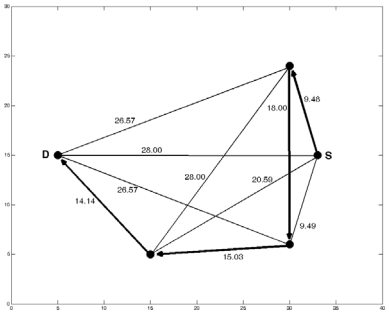


Fig. 1: Example of the MTE route selection algorithm. The elected path is highlighted in bold

A. Threats

In [12], we are informed that neglect, greed, homing, misdirection, authorization, probing, black holes and monitoring are possible routing layer attacks. In more detail, Karlof and Wagner [3], discuss specific threats to the routing layer of a WSNs, which are also very much applicable to smart grid networks. For the purpose of this paper, we investigate the effect of three variations of the following two attacks, at varying degrees of node compromise.

1) Spoofed Data: is a direct attack on routing data. By spoofing, altering or replaying routing information the attacker can complicate the network by creating routing loops, attracting or repelling traffic, generating false error messages, shortening or extending source routes or partitioning the network.

2) Selective forwarding: is an attack in which the adversary includes himself/herself in the data flow path of interest. Then the attacker may choose not to forward certain packets and drop them causing a black hole effect in the network. A variation of this attack is when the adversary only drops packets coming from specific sources or drops packets in a random fashion, whilst reliably forwarding other packets.

VI. Network Model

We simulated a large smart grid application in which the goal of the deployed network was to report energy usage data from the customer, through the network, to the headend. Each smart meter takes a reading of power usage at the costumer premises every 15 minutes, packetizes this information and sends it to the closest concentrator, using the MTE routing protocol. In turn, the concentrator forwards the readings it has received from the smart meters to the appropriate headend, for billing and control purposes. The smart meters use wireless radio to communicate among themselves and with the concentrators. Each meter has a simulated maximum radio range of 70m. The concentrators use a hardwired method (copper, power line carrier) to communicate with the headend, so transmission distance to the base station is not an issue.

The elected parameters used in our simulation are summarized in Table I.

TABLE I: Simulation Parameters

Number of smart meters	2000
Number of neighbourhood concentrators	100
Concentrator service area	200m^2
Maximum meter wireless range	70m
Number of simulated headends	1
Routing protocol	MTE

The routing protocol we simulate is Minimum Transmission Energy (MTE). We selected this protocol because of the simple way in which it selects paths. It is also an energy aware protocol which seeks to route messages from source to destination in a way that burdens the transmitting nodes the least. This is of importance for energy-aware applications, that wish to send the reading to the headend in the most cost effective way for the end-user.

In our simulations, we implemented three routing attacks:

1) A **black hole attack** in which all incoming packets are dropped.
2) A **selective forwarding attack** in which messages originating from 50% of the nodes are dropped, whilst others are forwarded faithfully.
3) A **spoofing attack** which affects message integrity by swapping source and destination pairs in a manner that causes messages to be rerouted to the source that generated them.

These attacks were launched from compromised smart meters (marked in red in Figure 2). We simulated five different scenarios for each attack, in which the network was 1%, 10%, 20%, 50% and 80% infected.

Our network topology is modeled upon a portion of a central eastern suburb of Melbourne, which in totality covers an area of 4.3km^2 and has a population of 10,000. The positions of the smart meters in this topology represent actual locations of the houses in this suburb. The concentrators are evenly spaced in a grid like fashion across the topology. Figure 2 depicts our simulated suburb at 1% and 50% hacker infiltration rates.

The platform used for this simulation is a custom combination the OMNeT++ discrete event simulator [13], C++, Matlab and Python code. Due to their sheer size, all simulations were run on the Monash Sun Grid [14], which is a Linux based computer cluster consisting of 1008 CPU cores and 2880 GB of RAM.

VII. Results & Discussion

Seeing as the smart meters are fixed non-mobile structures that are required to work autonomously, it makes sense that they would run on mains power. This makes the smart grid network more static in nature when compared with a conventional WSN, as nodes should never exhaust their energy resources. Hence measures such as node connectivity and network functionality remain constant, whilst measures such as energy dissipation and network lifetime aren't applicable.

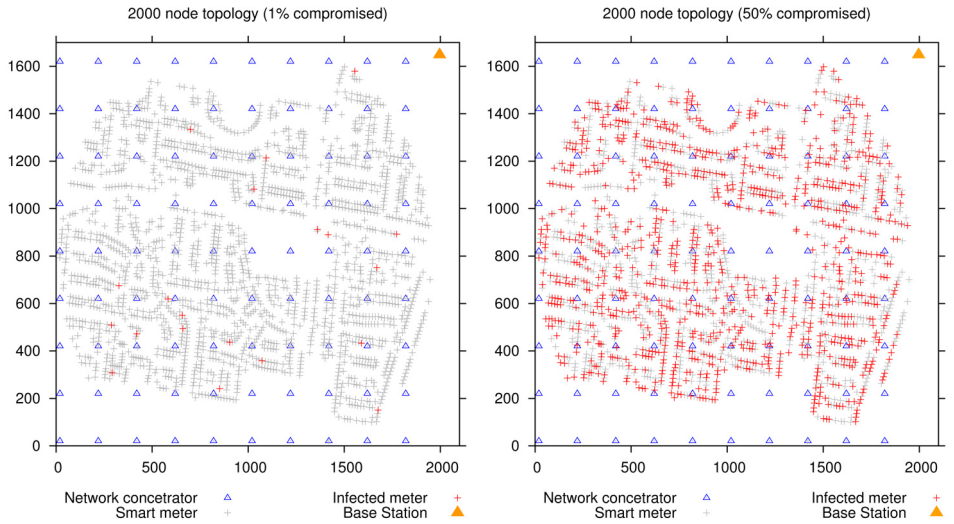


Fig. 2: Simulated smart grid topology depicting meter compromise. This topology is a direct replica of South Eastern Melbourne Suburb consisting of 2000 homes.

In order to investigate how the routing protocol is affected by the rogue nodes, we look at energy consumption, packet delivery ratio, node degree and link utilization.

A. Energy Consumption

The smart meter is a source of energy consumption in the network. The meter needs to consume power in order to measure usage patterns, store data, process control signals and most importantly transmit information via its radio. In Figure 3 we see how energy consumption varies with attack type and infection level. When the infection level is low, there is little deviation between the energy consumed for three attack types. As the infection rate increases we see larger variance between the simulated attacks. In particular, we see that under normal circumstances (no attack) the smart meters will consume more energy than when under attack. This is because the black hole is actually energy conserving, as the hacker intercepts the message before it reaches its destination, hence saving the energy that would have been dissipated transmitting the message along the remaining hops from the hacker to its destination. As the spoofing attack rebounds messages to their original sources, we see it consumes more energy than the black hole attack but less than if the messages were to be transmitted normally or intercepted by a selective forwarding node.

B. Packet Delivery Ratio

The packet delivery ratio (PDR) measures a network's ability to perform the task for which it was deployed. We measure it as the ratio of messages generated by the smart meters to those successfully received by the base station. Table II highlights that although the simulated application is 100% effective when not under attack, this changes drastically as hacks are introduced. In particular we see that the black hole and spoofing attacks are equally devastating to network functionality, as messages intercepted by the hacker, whether they are redirected or just dropped will never make it to the closest concentrator and in turn the base station. Of particular interest is that fact that even with a tiny 1% infection rate, 10% immediately gets reduced from the PDR, which in times of critical demand response could prove to be disastrous. The selective forwarding attack, which in essence is 1/2 a black hole attack, impacts packet delivery less than the black hole especially for higher infection rates. This is because the number of legitimate smart nodes ignored by the compromised meter decreases as the infection rate grows.

TABLE II: Network Effectiveness Ratio

Infection	No Attack	Black Hole	Selective Forwarding	Spoofing
1%	100%	90.85%	92.53%	90.85%
10%	100%	63.88%	79.40%	63.88%
20%	100%	46.75%	70.98%	46.75%
50%	100%	17.83%	56.46%	17.83%
80%	100%	9.50%	51.26%	9.50%

C. Node Degree

Node degree in a network is the number of connections or edges the node has to other nodes. In our simulation, the effective average network node degree is fixed at 13.04 for the measures specified in Table I. This is because the parameters that affect node connectivity, such as node density, geographic location and radio range are fixed in a smart grid application. However, the legitimate or actual node degree (not counting links to compromised nodes) varies with the number of infected nodes; As seen in Table III, node degree drops with increasing infection levels i.e. as the number of hackers increases in the network, the number of legitimate routes a node has to choose from is drastically reduced. Once again

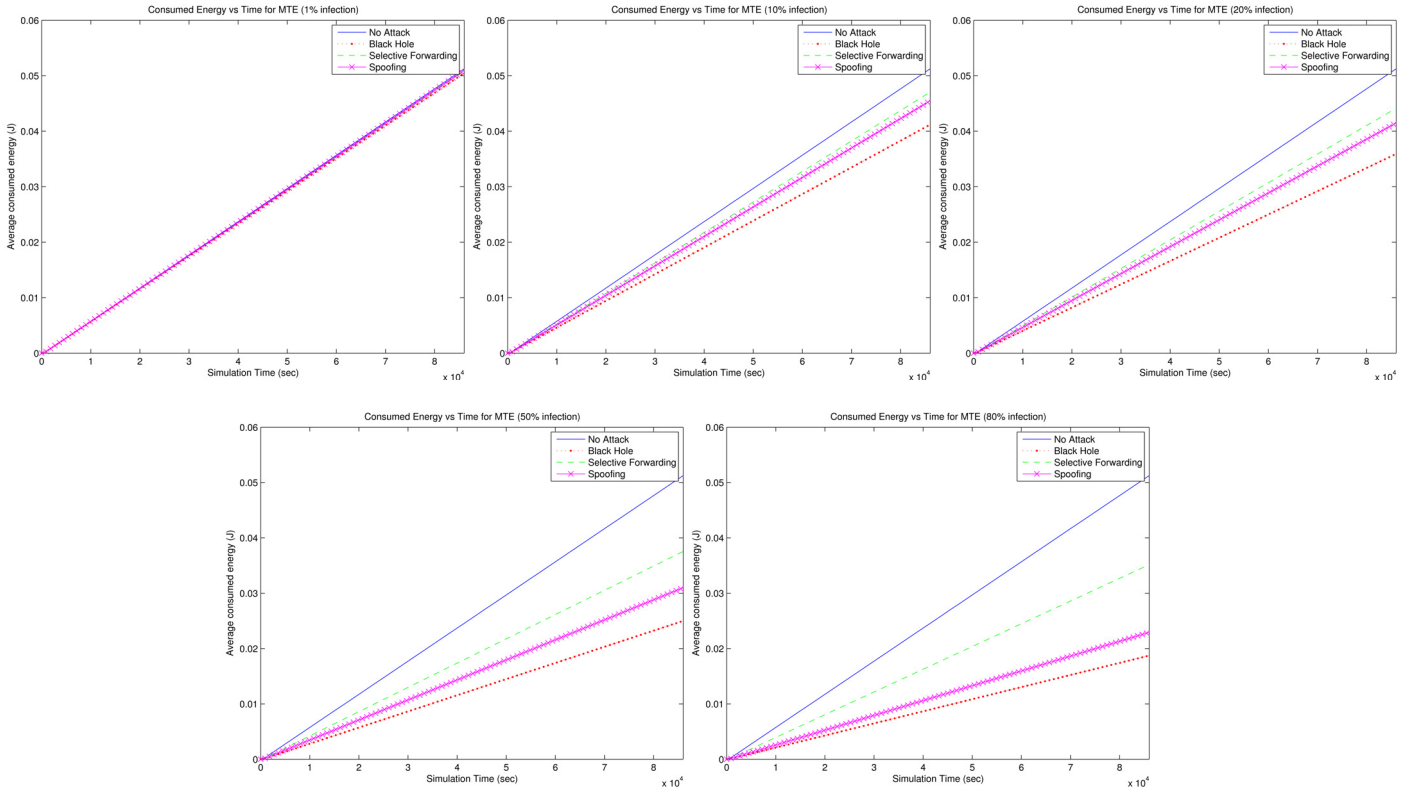


Fig. 3: Average smart meter energy consumption for varying infection levels.

we observe that the black hole attacks and spoofing attacks are more limiting than the selective forwarding attack which will actually allow one in two messages to pass through a hacker without being tainted.

TABLE III: Average Node Degree

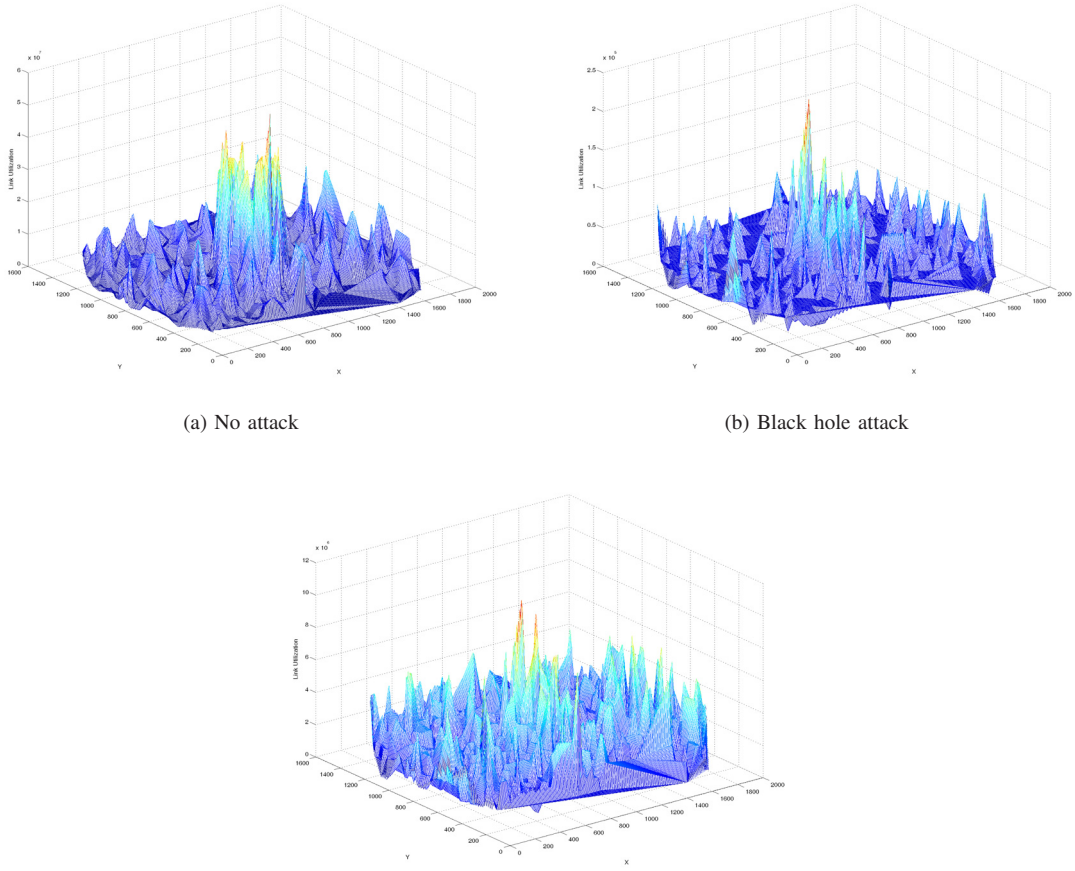
Infection	No Attack	Black Hole	Selective Forwarding	Spoofing
1%	13.04	12.95	13.00	12.95
10%	13.04	12.04	12.53	12.04
20%	13.04	10.84	12.00	10.84
50%	13.04	6.84	10.10	6.84
80%	13.04	2.77	8.10	2.77

D. Link Utilization

In Figure 4, we depict link utilization vs smart meter and concentrator location in the smart grid. This is done for the extreme case scenarios of no attack, an 80% black hole attack and an 80% spoofing attack. We plot utilization as the number of transmitted bits generated in a specific location of the topology over a 24 hour period. As expected, locations translating to the positions of concentrators, are noisy. Black holes are the quietest bandwidth attacks as they limit the amount of information being transmitted across the network. Spoofing, on the other hand is the noisiest attack still because it rebounds messages to their source, which can often be more hops away than their nearest concentrator. It is interesting to note here that the center of the network is particularly busy. This is due to the fact that there is a topological gap in the middle of the network (see Figure 2) that the nodes need to route around, as they cannot reach the concentrators in the middle of this hole. This causes them to route their messages along the edges of the hole, causing the observed burst of traffic to occur around the central concentrators. This measure would be useful in identifying 'quiet spots' and potential hacker locations, something that may be interesting when considering Intrusion Detection (ID) features.

VIII. Conclusions

Smart grids are the way of the future when it comes to dynamic service oriented future energy network infrastructure. However, these networks are still very young at heart and have a number of hurdles to overcome before they can fully flourish. One of these hurdles is security. In this article we have investigated ways in which the security of the routing layer of these grid can be compromised. We have shown that even a small number of compromised smart meters can drastically alter network connectivity and packet delivery measures. We have shown that attack and graph theory can explain the results generated from our smart meter simulator, hence confirming our simulation platform as an objective benchmark against which other protocols and attacks can be tested. We also have identified link utilization plots as a possibly useful intrusion detection measure. In the future, we would like to expand this work into a comparative study on attack resilience for



(a) No attack

(b) Black hole attack

(c) Spoofing attack

Fig. 4: Link utilization vs node location

popular WSN routing protocols. In particular, we would like to investigate the survivability of energy efficient protocols such as LEACH [11] and PEGASIS [15]. Our final vision is to use our simulator to compare existing intrusion detection methods, in an attempt to design an energy efficient and accurate Intrusion Detection System for smart grid networks.

ACKNOWLEDGMENTS

The authors would like to thank Mr Justin Young of Rio Tinto Australia, for his invaluable input to this paper through the exchange of useful conceptual ideas and programming knowledge. We also wish to thank the Monash Sun Grid [14] for allowing us the resources to run our simulations.

REFERENCES

[1] A. Vojdani, "Smart integration," *Power and Energy Magazine, IEEE*, vol. 6, no. 6, pp. 71–79, 2008.

[2] I. Akyildiz, S. Weilian, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no.8, pp. 102–114, August 2002.

[3] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," *Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols*, vol. 1, pp. 293–315, September 2003.

[4] R. Roman, J. Zhou, and J. Lopez, "On the security of wireless sensor networks," *Lecture Notes in Computer Science*, vol. 3482, no. III, pp. 681 – 690, 2005.

[5] J. R. Roncero, "Integration is key to smart grid management," in *SmartGrids for Distribution, 2008. IET-CIRED. CIRED Seminar*, pp. 1–4, 2008.

[6] R. van Gerwen, S. Jaarsma, and R. Wilhite, "Smart metering," tech. rep., July 2006.

[7] S. Karnouskos, O. Terzidis, and P. Karnouskos, "An advanced metering infrastructure for future energy networks," pp. 597–606, 2007.

[8] F. Cleveland, "Cyber security issues for advanced metering infrastructure (ami)," July 2008.

[9] S. Gold, "Not-so-smart meters?," *Network Security*, vol. 2009, no. 6, 2009.

[10] J. Al-Karaki and A. Kamal, "Routing techniques in wireless sensor networks: a survey," *Wireless Communications, IEEE*, vol. 11, pp. 6–28, Dec. 2004.

[11] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences*, p. 10, January 2000.

[12] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54 – 62, 2002.

[13] A. Varga, "OMNeT++: Community site," 2009. http://www.omnetpp.org/.

[14] M. University, "Monash sun grid (msg)," October 2009. http://www.monash.edu.au/eresearch/services/mcg/msg.html.

[15] S. Lindsey and C. Raghavendra, "Pegasis: power-efficient gathering in sensor information systems," in *Proceedings of the 2002 IEEE Aerospace Conference*, vol. 3, pp. 1125–1130, 2002.