Impact of Topology on Service Availability in a Smart Grid Advanced Metering Infrastructure

Bashar Alohali, Kashif Kifayat, Qi Shi, William Hurst
School of Computing and Mathematical Sciences,
Liverpool John Moores University, Liverpool, UK,
B.A.Alohali@2012.ljmu.ac.uk{K.Kifayat, Q.Shi, W.Hurst}@ljmu.ac.uk

***Abstract*— Over the last decade, Wireless Sensor Networks (WSNs) have brought radical changes to the means and forms of communication for monitoring and control of a large number of applications including Smart Grid (SG). Traditional energy networks have been modernized to Smart Grids to boost the energy industry in the context of efficient and effective power management, performance, real-time control and information flow using two-way communication between utility provides and end-users. However, integrating two-way communication in smart grid comes at the cost of cyber security vulnerabilities and challenges. In the context of SG, node capture is a severe security threat due to the fact that a compromised node can significantly impact the operations and security of the SG network. In this paper, node compromise attack is explored on Advance Metering Infrastructure (AMI) with smart meters for Neighbor Area Networks (NANs) in star and mesh network topologies. Simulation of node compromise/failure for a SG network, using ZigBee nodes in simulation indicates that a partial mesh topology is more resilient to node capture attacks as compared to star topology. A larger number of nodes are reachable from the control center of the SG in a partial mesh topology compared to that in a star topology.**

Keywords*- *Smart meter; Smart Grid;, Node Capture, Mesh Smart Meter, Start Smart Meter

I. INTRODUCTION

The swift development of information and communication technology (ICT) has not only changed the way we live our lives but also changed the industrial automation system including Smart Grid (SG) to an effective, efficient and reliable system. The integration of ICT has been of great importance to transform the traditional energy networks into SGs to ensure a reliable system and to overcome the limitations and challenges experienced by traditional energy networks. The U.S department of energy has defined the smart grid as an "electricity delivery system (from point of generation to point of consumption) integrated with communication and information technologies for enhanced grid operations, customers' services and environmental benefits [1]."

Recently, wireless sensor networks (WSNs) have shown great potential for various applications including in SGs. The SG applications can include a range of devices/systems such as smart meters (SMs), advance metering infrastructure (AMI), wide area measurement system (WAMS), substation automation system, common information models (CIF), and fault diagnosis to achieve seamless, efficient energy transmission and distribution, effective and reliable remote monitoring due to its easy deployment in remote locations, low cost, low date rates and low energy consumption [2-5]. Regardless of the economical and functional benefits exploited by SGs, its adoption, deployment and resiliency has been of great challenge due to potential lack of adequate security and vulnerable attacks like node capture to damage confidentiality, integrity and availability [6-7]. SMs, deployed in domestic and commercial location, required to be interconnected for communication and data flow to management entities. The deployment (i.e. star, tree, partial/full mesh) will vary as per the distribution of SMs in NANs environment and can severely impact the network resiliency due to network threats. The aim of this paper is to explore the node compromise attack on AMI and so smart meters for NANs star and mesh network topology. SG network segments in different topologies are simulated using OPNET. The simulation results show that a partial mesh topology is more resilient to node capture (NC) attacks.

The paper is organized as follows. Section 2 presents the related work followed by architecture and the functionality of SGs and its components in section 3. Section 4 describes the NC attack and its impact on NAN star and mesh topology is analyzed in section 5 and 6. Finally, Section 7 concludes the paper and future work is outlined.

II. SMART GRID OVERVIEW

A SG network permits services to have bi-directional interaction with devices on their electric grid as well with end-users and distributed power generation and storage facilities. To achieve the detailed view of the Smart Grid, it can be considered as a heterogeneous network (Fig. 1) based on the interconnection of multiple networks segments such as, the Home Area Networks (HANs) for effective energy at consumer end; the Neighborhood Area Network (NAN) for providing advance metering infrastructure; and the Wide Area Network (WAN) to distribute automation and the SG backbone [14]. The HAN interconnects to the WAN via a SM, which is part of NAN. Majority of the devices in the HAN and NAN are wireless communicating nodes. The interconnectivity of SMs into NAN is collectively referred to as advanced metering infrastructure (AMI) and is the main focus of this paper. NAN can be a network of smart meters creating a star, tree, or mesh network, which consists of smart meters and gateways that relay data.

AMI facilitates the critical communication and control functions required to implement important energy management services such as pricing schemes, demand response, automatic meter reading, and management of power quality. AMI, integrated with million number of low-cost nodes being placed in insecure, uninterested and unsophisticated locations, make smart metering vulnerable to cyber-attacks such as spoofing, eavesdropping, Denial-of-Service (DoS), man-in-the-middle attacks and node compromise [13,15]. To ensure secure communication and resiliency in SM infrastructure and so AMI is one of the critical requirements.

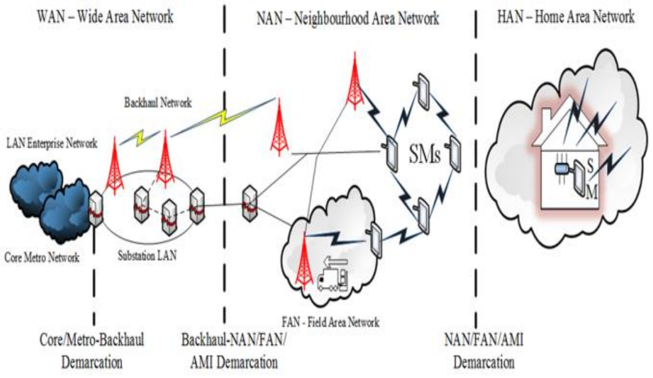

Figure 1 Smart Grid Network

III. Related Work

According to The U.S. Department of Energy, an emerging SG system must possess seven critical properties including resiliency to vulnerable attacks [8]. Over the last decade, malicious security threats on SG system have raised serious concerns. In 2003, due to Slammer worm attack from dial-up connection, Davis-Besse nuclear plant in Ohio was turned off to limit the impact of the threat [9]. In Iran, due the Bushehr power plant was infected due to one of the very first malicious coding attack known as Stuxnet worm [10]. The recent cyber-attack on Ukraine’s power network also highlighted the security and system resiliency as major requirement for smart grid [11].

In [12], a binary tree based topology has been considered to introduce an efficient and scalable key management scheme for secure unicast, multicast and broadcast communication in SGs. The scheme demands considerable manual tasks to create the binary tree and transmit it together with secret key to each node. Due to binary tree nature, this scheme is vulnerable to NC attack where a compromised node can put network resiliency at risk due to unavailability of an alternative route. In [13] tree attack has been explored on tree topology and highlighted the tree topology as vulnerable for energy theft in AMI. There have been various studies to highlight and enhance the security of Smart Grids based on encryption techniques and key management approaches against different attacks. However, the analysis of NANs resiliency considering tree and mesh topology against attacks like NC has been overlooked.

IV. Node Compromise / Capture Attack

Among various attacks in SGs, node compromise attack is a severe threat due to unattended nature of the sensor nodes. In a NC threat, an intruder can capture/compromise a node (SM) to get the access to secure cryptographic keys, node identification, communication between node and the network and monitor by re-deploying the compromised node into the network [16-17]. Once a node is compromised, it allows an intruder to execute various operations/attacks on the network and easily compromise the entire network. According to [18], there are three critical factors as mentioned below, which can lead intruder to compromise the entire network while triggering the node capture threat.

1. Cryptography technology has been of great interest to secure data transmitted across the AMI and authenticates the different entities involved in the communication flow. Node capture threat can result into a massive threat if the key(s) used to encrypt/decrypt data among neighboring nodes are deployed with weak key security and management.

2. The node deployment/topology play a critical role as it affects the scope of the node capture attacks. Generally, the scope can be defined based on the number of communication links such as, fewer the communication links between neighboring nodes (i.e. tree topology), the greater the possibility that an intruder can threat entire network. At the other end, higher the communication links between neighboring nodes (i.e. full/partial mesh topology), the smaller the possibility that an intruder can threat entire network. Therefore, node capture attacks seem to be less effective to mesh topology as compared to star topology, where there is only route from a child node to parent node.

3. The node density also plays a critical role as it affects the scope of the node capture attacks. A node compromised in the larger density network can threat the larger section of network.

Therefore, security of SM nodes and so the AMI is a critical issue to maintain the security and resiliency. Cryptography mechanisms based on symmetric (single share key) and asymmetric (public and private key) represents a crucial technology to secure the data transmitted across the nodes. A key (responsible to encrypt and decrypt data) plays a critical role and therefore an unauthorized access to key through a compromised node can threat entire network. In this paper, it is assumed the NANs use encrypted communication based on random redistribution key approach.

SMs, deployed in domestic and commercial location, required to be interconnected for communication and data flow to management entities. The deployment (i.e. star, tree, partial/full mesh) will vary as per the distribution of SMs in NANs environment. Fig. 2, 3 shows the example of star and mesh NAN topology.

Star-based network deployment is characterized by central root node, connected at the highest level in the hierarchy as show in Fig.3. Top-level node is connected to 2nd level, whereas 2nd level nodes are connected to 3rd level and so forth. The levels of the star topology can be denoted by $n \in N := \{1, 2, \ldots N\}$, where the 0^{th}level is for top root.

In a mesh network deployment, a node in each of the smart meter in NANs will communicate (transmit / receive) data by hoping from one node to another node until either the receiving node is reached or transmitted data reached to mesh gateway from node to node as shown in Fig. 3. The data from the gateway is typically transmitted to central data station via a backhaul network. The GWs are connected as start topology to backhaul network and SMs are connected as partial mesh as each SM is not directly connected to each of the other SM in the network.

V. Methodology

A. Network Security Model

It is considered that a group of Smart Meters (SMs) with one SM taking on the role of a gateway (GW) is interconnected in a manner that some SMs have a multi hop path to the gateway (GW). The GW interconnects to the central authentication point over the backhaul network. SMs that are children of other SMs use the multi-hop path to reach the GW node as shown in Fig. 2. It is assumed the NANs use encrypted communication based on random redistribution key approach. Each node is configured with a set of (K) different keys from a key pool of (P) keys. A pair of nodes with the range (R) can initiate a secure connectivity only if appropriate assigned keys are shared between them. It is also assumed that every node is deployed in a promiscuous approach and is able to recognize sources of all messages initiating from its neighboring nodes. Based on this assumption, each node will inspect only the source node ID therefore this assumption will not incur significant communication overhead.

B. Network Threat Model and Performance Metrics

It is assumed that an intruder can physically capture a limited number of SM nodes in a target region Ŗ and turn them into threat node by extracting secure keys and measured data for NAN. Considering Ç represents a set of nodes captured by intruder and for each node in set Ç, a set of secure keys are considered to be compromised. When a node is compromised, its connectivity to other nodes is affected. If the node is not an end node, a larger number of nodes lose connectivity. It allows intruder to clone a captured node and collaboratively deploy them in the NAN. The resiliency of NAN star and mesh topology in Smart Grid against NC attack will be evaluated based on following metrics; hop count, availability of SM, End to End Delay, and Energy Consumption.

C. Network Topology and Simulation Setup

To carry out evaluation of NC attacks, two NAN topologies, star and mesh as shown in Fig. 2 are considered. The NAN made of (N) nodes is deployed over a region of $(A \subseteq \mathbb{R})$. Considering that SMs in the AMI are fixed nodes, there is no mobility aspect included. Each node is assumed to be equipped with an omni-directional radio with fixed communication range (R) based on the Zigbee standard. To evaluate the resiliency of star and partial mesh topology in NAN in smart grid based on Zigbee network against node capture attack, OPNET simulation tool has been used. In both star and mesh topology simulation of NAN, network consist of a Zigbee coordinator (Gateway) and Zigbee end devices (SMs).

- ***Case 1 – Star Topology:*** In this case, Zigbee nodes are deployed in a star topology for NAN.
- ***Case 2 – Tree Topology:*** In a NAN tree topology, there is a relationship of root (GW) and child (SM) node. The child node can communicate only with their parent node whereas the parents can communicate with their child and their own parent node. Therefore, child node (SM) always depends on the parent node for data availability as there are no alternative routes for SM node to get target.
- ***Case 3 – Mesh Topology:*** In this case, Zigbee nodes are deployed as partial mesh topology for NAN. NAN Mesh topology is more flexible as it can allow each node to choose between multiple routes to transmit/receive data to the target location. It also allows the network to self-heal and search for other paths and so that data can be relay through.

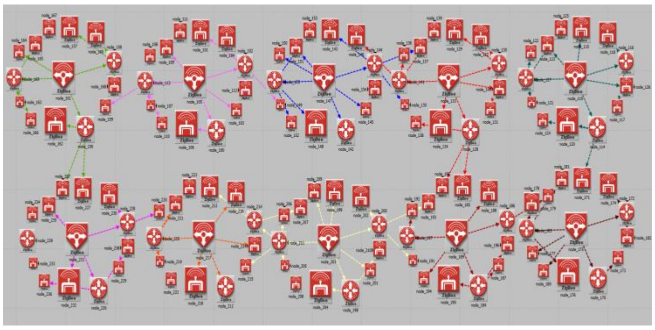

Figure 2 Mesh Topology scenarios

VI. PERFORMANCE ANALYSIS AND DISCUSSION

In this section, the OPNET simulation [19] of both star and mesh NAN topologies against node capture attacks are discussed to highlight which NAN topology is more resilient against node capture attacks.

A. Node Capture Attack and Impact on Reachability

Node capture attack involves capturing a node and incapacitating it. Often the data in the node is retrieved for malicious use, but in case of tamper-resistant hardware, the access to data on the ROM of the device is avoided. Therefore, the primary impact of a node capture is the loss of the node. In addition to the loss of the sensed data from the node, the reachability from/to the central reporting node, the NOC, is impacted. This happens when the captured node provides a path for the downstream nodes to reach the NOC.

In order to assess the impact of the reachability in the event of a node capture, star and mesh topologies are used to create a large network. For each node captured or a group of nodes captured, the number of nodes that are unreachable are noted.

A network comprising ten ZigBee coordinator nodes, thirty ZigBee router nodes and a hundred ZigBee devices are used to create the network to test the impact of the node capture attack. The topology at the coordinator node is set to mesh and star respectively for each simulation run, in its network parameters. The coordinator node sends packets to the routers and end devices in each case.

Nodes are randomly chosen to fail and the reachability from the NOC to all nodes is checked. The simulations are run for the two topologies separately and in each case, up to 9 nodes are failed. The corresponding numbers of nodes that are unreachable are noted. The figure plots the number of unreachable nodes against the number of captured nodes.

The plotted results indicate that the mesh topology of the ZigBee network fares better than the star topology. The results are dependent upon which nodes are captured in the mesh topology. If an attacker succeeds in capturing and incapacitating all the ZigBee router nodes, then the impact could be more intense. It could turn out that the mesh topology could fare worse than the star topology.

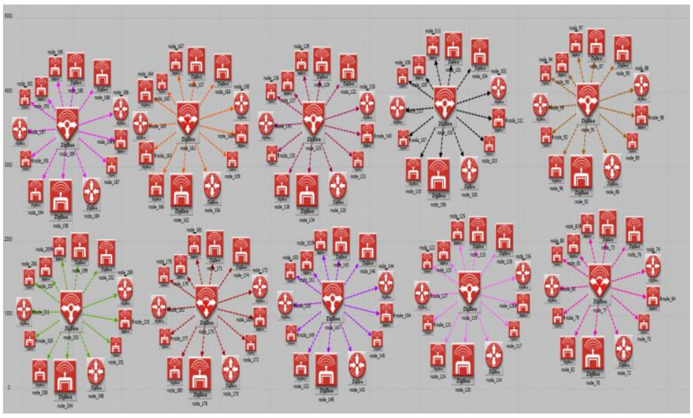

Figure 3 Star Topology scenarios

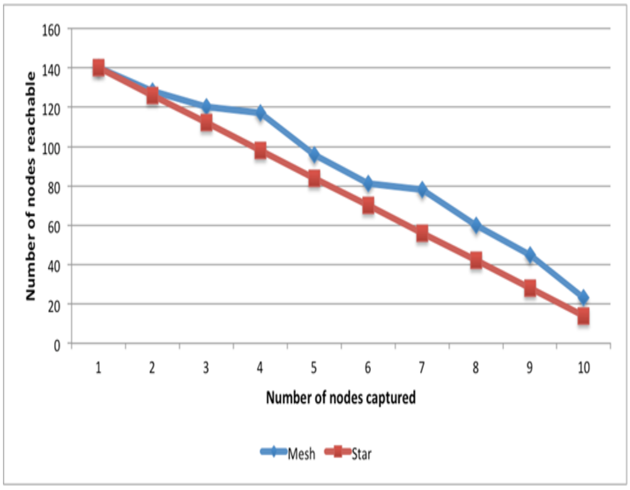

Figure 4 Reachability of nodes after node captures

VII. CONCLUSION

Node capture attacks in Smart Grid can significantly degrade network performance and threaten network security. Based on the simulation results, it is identified that partial mesh topology is more resilient topology as compared to star topology in NAN in Smart Grid against node capture attacks. As compared to NAN star, NAN mesh topology is more flexible as it can allow smart nodes to choose between multiple routes to transmit/receive data to the target location, if one of the node(s) compromised. Due to the flexibility offered by mesh topology, it is not only resilient but also an ideal solution with easy to deploy in NAN environment.

This study has been focused on simple star and partial mesh topology for NAN along with NC attack. For future work, the study will be extended to complex topology star, star and mesh topology along with advance threat model and security scheme to detect and avoid node capture attacks to enhance the network resiliency as well as security.

REFERENCES

1. Sioshansi, F. O, *Smart Grid: Integrating Renewable, Distributed & Efficient Energy*, Academic Press, 2012, p. 89.
2. V. C. Gungor, B. Lu and G. P. Hancke, "Opportunities and Challenges of Wireless Sensor Networks in Smart Grid," *IEEE Transactions on Industrial Electronics*, vol. 57, no. 10, pp. 3557-3564, 2010.
3. E. Fadel, V.C. Gungor, L. Nassef, N. Akkari, M.G. Abbas Malik, S. Almasri, I. F. Akyildiz, "A survey on wireless sensor networks for smart grid", *Computer Communications*, Vol. 1, pp. 22-33, 2015.
4. Z. Popovic and V. Cackovic, "Advanced Metering Infrastructure in the context of Smart Grids," *IEEE International Energy Conference (ENERGYCON)*, pp. 1509-1514, 2014.
5. L. Nian, C. Jinshan, Z. Lin, Z. Jianhua, and H. Yanling, "A Key Management Scheme for Secure Communications of Advanced Metering Infrastructure in Smart Grid," *IEEE*

Transactions on Industrial Electronics, vol. 60, pp. 4746-4756, 2013.

6. M. Amin, “Guaranteeing the security of an increasingly stressed grid,” *IEEE Smart Grid Newsletter*, Feb. 2011.
7. NIST, “Guidelines for Smart Grid Cybersecurity, Volume 1 - Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements, The Smart Grid Interoperability Panel – Smart Grid Cybersecurity Committee, 2014, National Institute of Standards and Technology, U.S. Department of Commerce.
8. U.S. Department of Energy, National Energy Technology Laboratory, *A Systems View of the Modern Grid*, 2007.
9. Y, Yang, T, Littler, S. Sezer, K. McLaughlin, H. F. Wang, “Impact of cyber-security issues on Smart Grid”, *2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies*, vol., no, pp.1,7, 2011.
10. D. Kushner. (2016, 8/3/2016). *The Real Story of Stuxnet*, 2013, Available: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet
11. L. Tomkiw. (2016, 8/3/2016). *Russia-Ukraine Cyberattack Update: Security Company Links Moscow Hacker Group To Electricity Shut Down*. Available: http://www.ibtimes.com/russia-ukraine-cyberattack-update-security-company-links-moscow-hacker-group-2256634
12. J. Y. Kim, and H. K. Choi, "An efficient and versatile key management protocol for secure smart grid communications," *IEEE Wireless Communications and Networking Conference (WCNC),* pp. 1823-1828, 2012.
13. S. McLaughlin, D. Podkuiko, P. McDaniel, “Energy Theft in the Advanced Metering Infrastructure”, *Critical Information Infrastructures Security*, Vol. 6027 of the series Lec Notes in Computer Science, pp 176-187, 2009.
14. W. Meng, R. Ma, and H.-H. Chen, "Smart grid neighbourhood area networks: a survey," *IEEE Network*, vol. 28, pp. 24-32, 2014
15. S.H. Seo, X. Ding and E. Bertino, "Encryption key management for secure communication in smart advanced metering infrastructures," *IEEE International Conference on Smart Grid Communications (SmartGridComm),* Vancouver, BC, pp. 498-503, 2013
16. M. V. Bharathi, R. C. Tanguturi, C. Jayakumar and K. Selvamani, "Node capture attack in Wireless Sensor Network: A survey," *IEEE International Conference on Computational Intelligence & Computing Research (ICCIC),* Coimbatore, pp. 1-3, 2012.
17. K.Venkatraman, J.Vijay Daniel, G.Murugaboopathi, "Various Attacks in Wireless Sensor Network: Survey", *International Journal of Soft Computing and Engineering (IJSCE)*, Vol. 3, No. 1, pp. 208-212, 2013.
18. K. Kifayat, M. Merabti, Q, Shi, and D. Llewellyn-Jones, *Security in Wireless Sensor Networks, Chapter 26, Handbook of Information and Communication Security*, Springer Science & Business Media, 2010.
19. RIVERBED. 2014. Riverbed Modeler Version 17.5, PL6,, Riverbed Software [Online]. Available: http://www.riverbed.com/.