Smart Grid and Renewable Energy, 2016, 7, 105-113
Published Online March 2016 in SciRes. http://www.scirp.org/journal/sgre
http://dx.doi.org/10.4236/sgre.2016.73007

SCADA Framework Incorporating MANET and IDP for Cyber Security of Residential Microgrid Communication Network

Goutham K. Chalamasetty[1], Paras Mandal[1], Tzu-Liang (Bill) Tseng[2]

[1]Department of Electrical and Computer Engineering, The University of Texas at El Paso, El Paso, TX, USA
[2]Department of Industrial, Manufacturing, and Systems Engineering, The University of Texas at El Paso, El Paso, TX, USA
Email: gchalamasetty@miners.utep.edu, pmandal@utep.edu, btseng@utep.edu

Received 23 February 2016; accepted 26 March 2016; published 29 March 2016

Abstract

This paper presents a reliable and secure supervisory control and data acquisition (SCADA) system equipped with advanced communication technologies (ACT) to enhance the operation and cyber security of the communication network in residential microgrid. The proposed approach uses the mobile ad hoc networks (MANET) for collecting data of power consumption from smart meters of residential areas and electric vehicles (EVs), and also for connecting mobile system operators to the network. Moreover, by understanding the dynamic nature of MANET and their exposure to cyber-attacks, we propose an intrusion detection and prevention (IDP) technology with secure knowledge algorithm and anomaly detection for preventing the black hole attacks, and other unknown attacks that result into packet dropping. Test results obtained by using Network Simulator (NS-2) demonstrate the effectiveness of the proposed IDP technology in preventing the cyber-attacks in the proposed residential microgrid communication network.

Keywords

ACT, Black Hole Attack, Cyber Security, MANET, Residential Microgrid, SCADA

1. Introduction

The electric power grid is going through major changes worldwide in order to become smarter, resilient, sustainable, and more reliable [1]. Power utilities are facing a major challenge in maintaining the desired reliability and security while integrating increasing loads and distributed energy resources (DER), primarily wind and solar

How to cite this paper: Chalamasetty, G.K., Mandal, P. and Tseng, T.-L. (B.) (2016) SCADA Framework Incorporating MANET and IDP for Cyber Security of Residential Microgrid Communication Network. *Smart Grid and Renewable Energy*, **7**, 105-113.
http://dx.doi.org/10.4236/sgre.2016.73007

energy. Furthermore, smart grid and/or microgrid are primary targets of cyber-attacks due to advancement in their communication networks and technologies [2] [3]. **Figure 1** shows an example of a multi-microgrid and its energy management system, termed as multi-microgrid energy management system (MMEMS), which comprises of residential, industrial, and commercial microgrids. Such microgrids can operate in connected or islanded mode with the main grid. The MMEMS is controlled by supervisory control and data acquisition (SCADA) system, which is the combination of telemetry and data acquisition [4]. SCADA plays a crucial role in controlling and ensuring a reliable and secure operation of MMEMS. Thus, it is very essential to have a SCADA system, which is persistent and also has the ability to monitor and control the system in real time to enhance the efficient operation and cyber security of the system [5]. SCADA comprises of several components such as 1) SCADA-master that sends the control commands, 2) regional terminal units (RTU), programmable logic controllers (PLC), and intelligent electronic devices (IED) that receive commands from SCADA-master, 3) human machine interface (HMI), which provides a graphical user interaction to the operator at control center, and 4) communication networks, which connect all the above mentioned components [4]-[7]. The components and sources of the MMEMS are depicted in **Figure 1** where we can observe that MCC is a major control center, which is responsible for the reliable and secure operation of MMEMS. Microgrid control centers (MGCC) are the sub control centers for individual monitoring of residential, industrial, and commercial microgrids. Moreover, each MGCC communicates with MCC to provide the entire system's state of operation. MCC also comprises of the SCADA-master that sends control commands to MGCC, and each MGCC has a sub-SCADA-master to control RTU, PLC, and IED in remote stations.

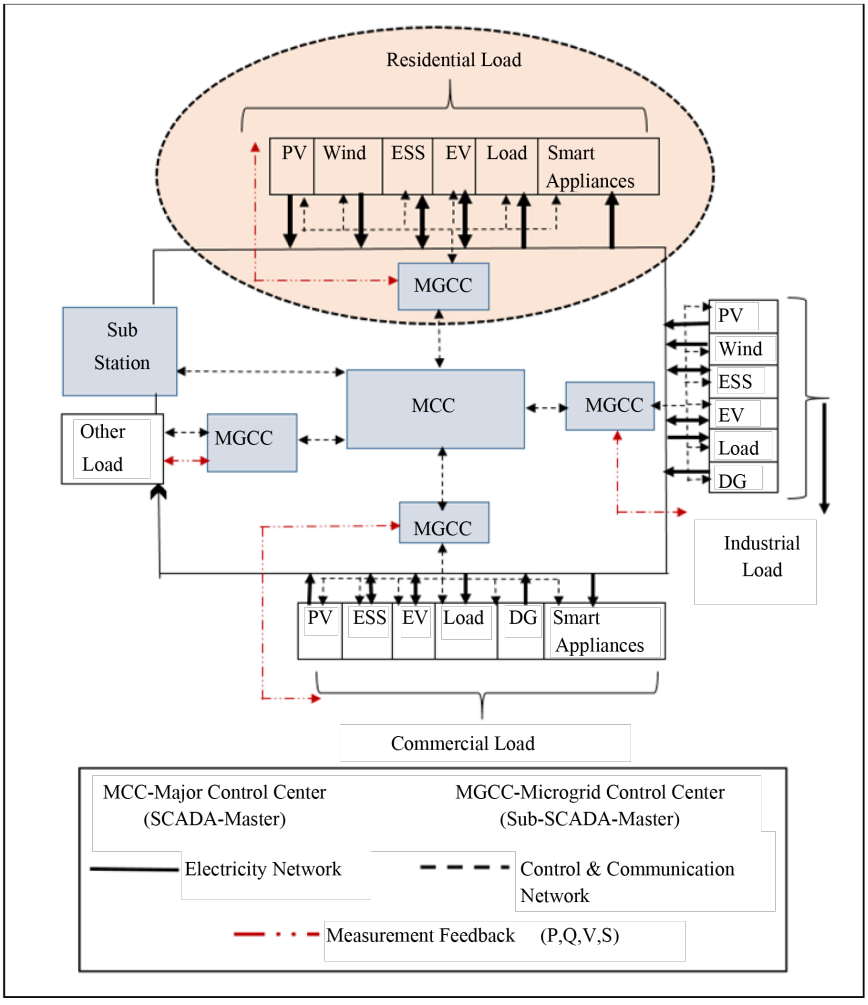

Figure 1. Architecture of MMEMS.

In general, the operation of MMEMS consists of various technologies of DER, wind, photovoltaic (PV), energy storage system (ESS), electric vehicles (EVs), loads and smart appliances (**Figure 1**). However, MMEMS can have issues, such as handling the variable output power of wind/PV, security and load sharing [8]. In addition, there are several vulnerabilities, which are discussed in detail in Section 2, in the existing SCADA system that lead to physical and cyber-attacks on the control and communication network. Hence, there is a great need to develop a reliable and secure SCADA control and communication network to enhance MMEMS operations by adopting advanced communication technologies (ACT) and providing cyber security.

This paper presents cyber security issues with focus on *communication in residential microgrid*, which is a part of MMEMS of **Figure 1**. The major contributions of this paper are: 1) we recommend to integrate ACT into existing SCADA system, 2) we propose to use mobile ad hoc networks (MANET) for residential microgrid where MANET is required to collect the information of power consumption as well as to connect with the mobile system operators, and 3) we propose an intrusion detection and prevention (IDP) technology for preventing cyber-attacks in MANET used in residential microgrid. It is emphasized that to the best knowledge of authors, this paper is the first attempt to use MANET for communication in residential microgrid.

2. Vulnerabilities in Existing SCADA System

There are numerous developments made to the SCADA system after four major blackouts in the year 2003 through United States, Canada, and Europe [9]. However, there are still many vulnerabilities such as unpatched operating systems, unencrypted data, network design vulnerabilities, lack of proper firewalls used for respective network protocols, and network configuration vulnerabilities, which lead to physical system attacks and communication system attacks [9]-[14]. The recent attack on pacific gas and electric (PG&E) substation in California in April 2013 raised questions on the vulnerabilities in the existing physical systems [15]. Study done by Federal Energy Regulatory Commission (FERC) shows that the attack on 9 substations out of 55,000 transmission substations will take down the transmission grid of the entire U.S. [16]. The attacks on communication system include extracting information from power line carrier communication (PLCC) by tapping high frequency waves with a portable current transformer, and attackers use in-band jamming and out-of-band jamming technologies to corrupt the information in optical fiber cables [14]. The present communication infrastructure used for phasor measurement units (PMU) communication is not authenticated which leads to compromise the data integrity [17]. The vulnerabilities in wireless communication technologies lead to cyber-attacks such as eavesdropping, man-in-the-middle attack, data modification, denial of service (DoS) attacks, phishing attacks, and domain name system (DNS) spoofing. In addition to these vulnerabilities, there could be an emergency situation, e.g., natural disaster, which can destroy the SCADA control and communication infrastructure, and it may result into the operators' losing their control on the system.

Furthermore, for the architecture of MMEMS (**Figure 1**), the vulnerabilities in the existing SCADA system may cause potential threats to the operation of MMEMS by performing physical attack on substation or power generating sources such as PV stations and wind farms. These vulnerabilities also benefit the cyber attackers to intrude into the system's control and communication network, which will lead to the damage of the entire system. Highly motivated by the aforementioned vulnerabilities and threats, this paper contributes to develop a reliable SCADA communication network with an application of IDP technology in order to provide cyber security for residential microgrid.

3. Proposed Work

3.1. SCADA Control and Communication Network with ACT

The advancement in technology provides many wireless communication technologies such as wireless sensor networks (WSN), MANET, and Internet that can be used in SCADA system. A recommendation is provided to incorporate the above-mentioned technologies into the present SCADA system that will help progress the smart grid by improving the system parameters such as availability, reliability, and security [18]-[20]. Integration of these ACT into the existing SCADA control and communication network have following advantages: 1) more automation into the system, which minimizes the human workers, 2) bringing mobility into the system, which will allow the operators to move from control station without losing control over the system, 3) ability for the system operator to access and control the system wherever they are in the world by using internet SCADA or

web SCADA, 4) provide collaboration with other operators, and 5) enhancement in security by an integration of ACT. WSN and MANET continuously monitor and collect the information of current, voltage, and frequency profiles, trip coil status, and battery level of ESS. Finally, this collected information will be sent periodically to the system operators through internet [21]. Integration of ACT into SCADA further provides control to the operators even in emergency situations like natural disasters. Besides the aforementioned advantages by using ACT, there are also some disadvantages in the form of cyber-attacks. Some good examples of papers that discuss about cyber security to ACT are available in [22]-[26].

The major contribution of this paper that makes it different and novel from the existing papers is that we propose to use MANET to residential microgrid as shown in **Figure 2**. In our paper, we propose to use MANETs into the SCADA for an efficient and secure communication network in residential micro grid as shown in **Figure 2**. Note that **Figure 2** is a residential microgrid, which is extracted from **Figure 1**. Implementing a communication network by using MANET is cost effective and it brings more flexibility and redundancy into the network. In the proposed network (**Figure 2**), MANET is used to acquire the power consumption information of residential houses and EVs from smart meters. Smart meters are the smart grid primary resource for providing a smart interface with consumers [27]. The power consumption pattern of EVs with respect to speed and distance is used to compare the performance of different EVs, and this data is beneficial to analyze and develop the technologies used in EVs. In our proposed residential microgrid communication network, MANET also connects mobile system operators to the network, which helps provide immediate mitigation during emergency situations such as short circuits and power outages in residential areas. Furthermore, by understanding the dynamic nature of MANET and their exposure to cyber-attacks, we propose an IDP technology, which prevents cyber-attacks.

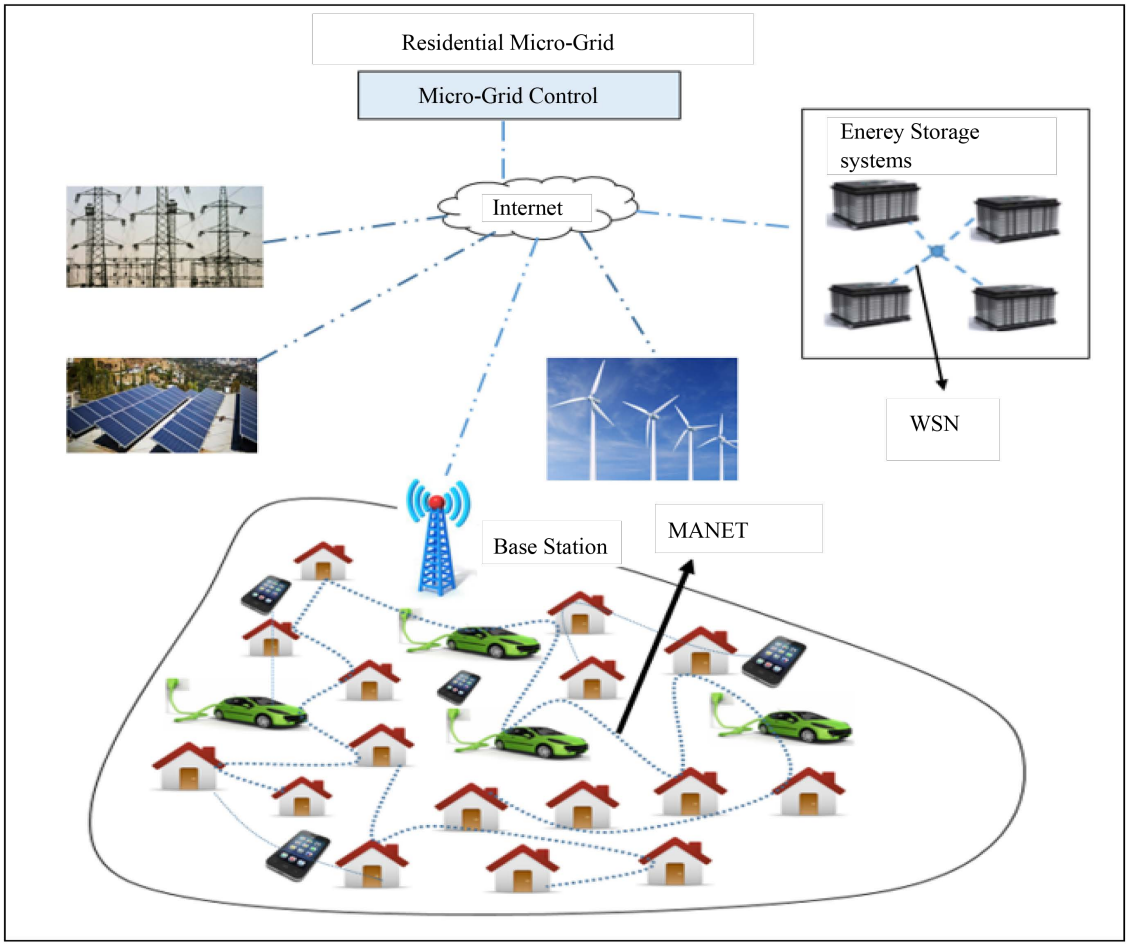

Figure 2. Architecture of SCADA control and communication network with ACT in residential microgrid.

3.2. Problem Solution for Identifying and Preventing Cyber-Attacks

By considering the benefits of identifying both known and unknown attacks discussed in [28], this paper proposes an IDP technology to prevent black hole attacks and other anomaly attacks. The information flow from source to destination node under the propose IDP technology is shown in **Figure 3**.

Black hole attack gives false information during the route discovery process while sending data from source to destination. This paper uses ad hoc on-demand distance vector algorithm (AODV) as a routing protocol in the MANET network. The routing protocol of AODV is such that when source node sends *route request* (*RREQ*) message to all the neighboring nodes, the black hole attacked node immediately sends *route reply* (*RREP*) with false information and makes the source node trust that this is an optimal route for sending data packets to destination node, and it then proceeds accordingly for data transmission. During this data transfer process, black hole node absorbs all the data packets, which result into the loss of information. To prevent these black hole attacks on MANET in our proposed network (**Figure 2**), we applied a *secure knowledge algorithm* [29], which is a simple and effective method to prevent black hole attacked nodes in the network. In this algorithm every node in the network monitors the neighboring nodes. Each node also consists of data table that provides information of 1) recent packet forwarded and 2) neighboring node related to the recently forwarded packet. The *secure knowledge algorithm* compares these two information—if they are same, there is no black hole attack; otherwise, the network is under attack. In addition to the *secure knowledge algorithm*, we include anomaly detection to prevent unknown attacks after the secure and optimal path is selected. In our proposed IDP technology, we considered the known attack as black hole that will be identified by using *secure knowledge algorithm* and unknown attacks are considered as misbehaving nodes that drop data packets during data transmission from source to destination even after the *secure knowledge algorithm* is applied. The anomaly attacks are reported by neighboring nodes, as every node monitors its neighbor node activities.

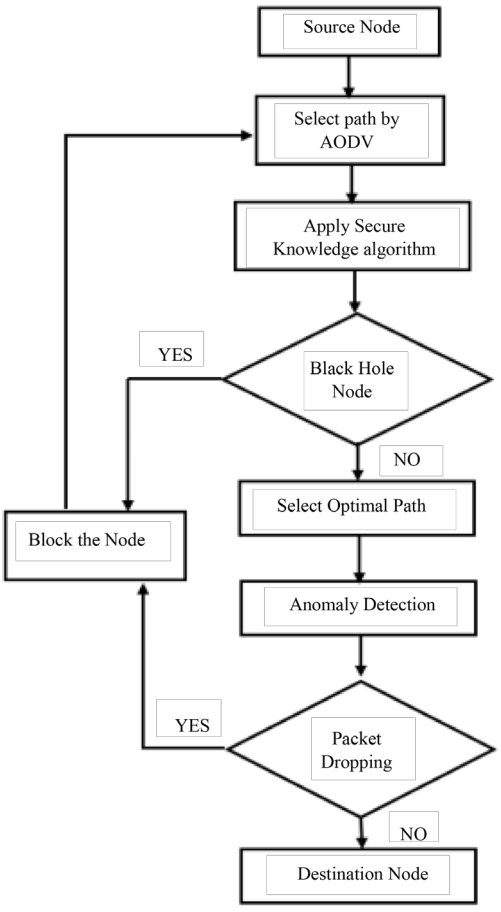

Figure 3. Data flow from source to destination.

4. Simulation and Results

We developed a communication network with MANET using Network Simulator version 2 (NS-2) as shown in **Figure 4** for our proposed residential microgrid (**Figure 2**). The parameters of the developed communication network are shown in **Table 1**. The developed network simulation is shown in **Figure 4**, which is a screen shot taken during the simulation process. The base station, which collects information from all the nodes is represented with big red circle as seen at the top right corner. The remaining nodes include residential houses, EVs, and mobile system operators.

In order to evaluate the effectiveness of the proposed IDP technology, the black hole attacked nodes and misbehaving nodes are added into the MANET network. We then applied *secure knowledge algorithm* as well as anomaly detection as presented in flowchart in **Figure 3**. Major network parameters such as network throughput, packet delivery ratio (PDR), and delay in the network are graphically represented in **Figures 5-7**.

Network throughput is the rate of data successfully delivered, PDR is defined as the ratio of number of packets delivered to the number of packets sent, and delay is total time taken to send the packets from source node to destination node. The proposed IDP technology is applied to the network, where black hole attacked nodes and misbehaving nodes are added to the developed network in NS2 simulator. From **Figures 5-7**, we can observe that network throughput and PDR are increased (**Figure 5** and **Figure 6**), and delay is decreased (see **Figure 7**), when the number of nodes in the network increased from 10 nodes to 50 nodes. Test results demonstrate that our proposed IDP technology is very efficient when there are more than 40 nodes in the network, for identifying

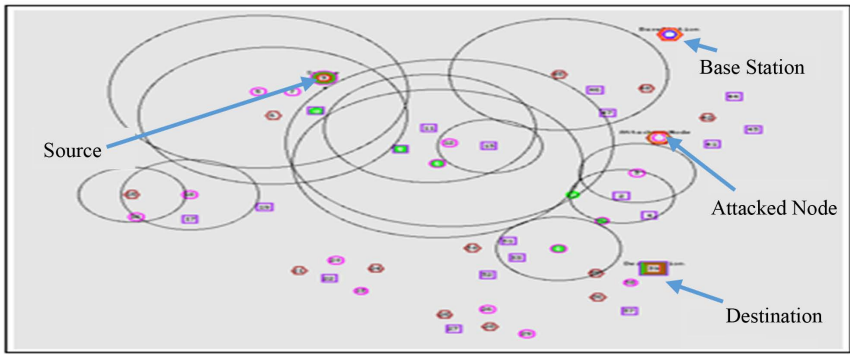

Figure 4. MANET simulation using NS-2.

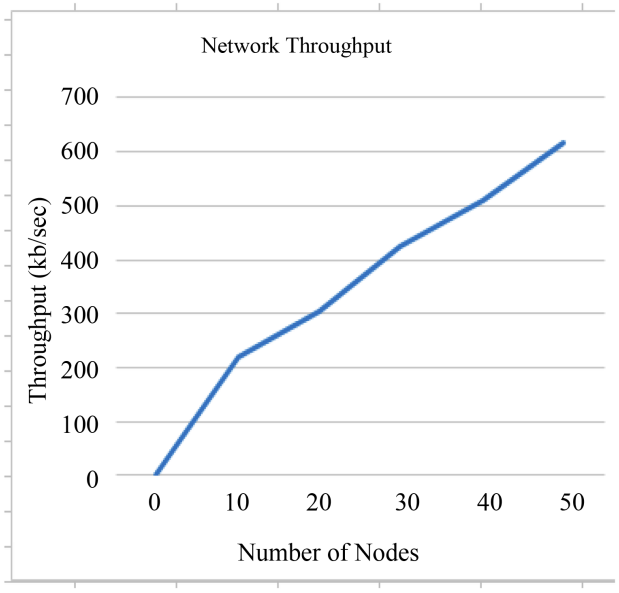

Figure 5. Network throughput vs. number of nodes.

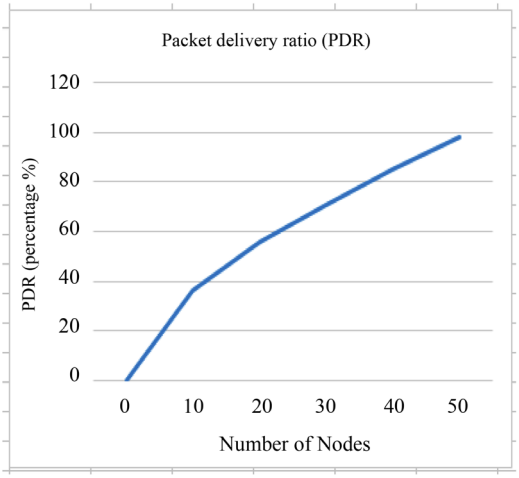

Figure 6. Packet delivery ratio vs. number of nodes.

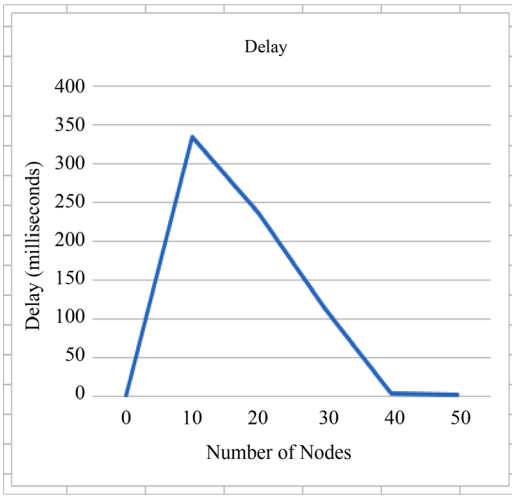

Figure 7. Delay in the network vs. number of nodes.

Table 1. Network simulation parameters.

Simulator	Network Simulator version 2
Simulation of Nodes	50
Interface Type	Phy/WirelessPhy
Channel	Wireless channel
MAC Type	Mac/802_11
Queue Type	Queue/DropTail/PriQueue
Queue Length	201 packets
Antenna Type	Omni antenna
Propagation Type	Two-ray ground
Size Of Packet	Five hundred and twelve
Routing Algorithm	AODV (ad hoc on demand distance vector algorithm)
Traffic	TCP
Simulation Time	7 minutes
Nodes Clustering	K-means algorithm

and preventing black hole attacks and other anomaly attacks that result in packet dropping. When there are only 10 nodes in the network the possibility to find a new route without attacked nodes is difficult, and when the total number of nodes increased in the network it is easy to find the new route which is optimal and secured. This will certainly enhance the cyber security for the proposed residential microgrid communication network.

5. Conclusion

This paper presented a SCADA communication network with ACT in the residential microgrid. Furthermore, IDP technology was applied to the proposed network using MANET, which collect the information of power consumption of residential areas and EVs, and also connect the network with mobile system operators. The major finding of this paper is that our proposed IDP technology, equipped with a secure knowledge algorithm and anomaly detection, was highly efficient in detecting cyber-attacks such as black hole attack and some unknown attacks, which led to create a misbehaving node that resulted into packet dropping. The future work would be interesting to examine the efficiency of multiple communication technologies when they are combined to control and operate MMEMS, and to develop viable IDP technologies that prevent cyber-attacks on the SCADA system.

Acknowledgements

This work was supported by the National Science Foundation (DUE-TUES-1246050). The authors would like to express sincere gratitude to National Science Foundation for providing financial support.

References

[1] Shafiullah, G., Oo, A., Ali, A. and Wolfs, P. (2013) Smart Grid for a Sustainable Future. *Smart Grid and Renewable Energy*, **4**, 23-34. http://dx.doi.org/10.4236/sgre.2013.41004

[2] Heydt, G.T., Liu, C.C., Phadke, A.G. and Vittal, V. (2001) Solution for the Crisis in Electric Power Supply. *Computer Applications in Power*, **14**, 22-30.

[3] Zhong, X., Yu, L., Brooks, R. and Venayagamoorthy, G.K. (2015) Cyber Security in Smart DC Microgrid Operations. *IEEE* 1*st International Conference on DC Microgrids* (*ICDCM*), Atlanta, 7 June 2015, 86-91.

[4] Kim, T.H. (2010) SCADA Architecture with Mobile Remote Components. *WSEAS Transactions on Systems and Control*, **5**, 611-622.

[5] Daoud, M. and Fernando, X. (2011) On the Communication Requirements for the Smart Grid. *Energy and Power Engineering*, **3**, 53-60. http://dx.doi.org/10.4236/epe.2011.31008

[6] Sridharan, V. (2012) Cyber Security in Power Systems. Thesis Diss., Georgia Institute of Technology.

[7] Chalamasetty, G.K., Mandal, P. and Tseng, B. (2015) Cyber Security Model for Power System Based on Game Theory. *Proc.* 5*th Southwest Energy Science and Engineering Symposium*, El Paso, 4 April 2015.

[8] Safdar, S., Hamdaoui, B., Cotilla-Sanchez, E. and Guizani, M. (2013) A Survey on Communication Infrastructure for Micro-Grids. *Proc.* 9*th International Wireless Communications and Mobile Computing Conference* (*IWCMC*), Sardinia, 1-5 July 2013, 545-550. http://dx.doi.org/10.1109/iwcmc.2013.6583616

[9] Fernandez, J.D. and Fernandez, A.E. (2005) SCADA Systems: Vulnerabilities and Remediation. *Journal of Computing Sciences in Colleges*, **20**, 160-168.

[10] Ten, C.W., Liu, C.C. and Manimaran, G. (2008) Vulnerability Assessment of Cyber Security for SCADA Systems. *IEEE Transactions on Power Systems*, **23**, 1836-1846.

[11] Wei, M. and Chen, Z. (2012) Reliability Analysis of Cyber Security in an Electrical Power System Associated WAN. *Power and Energy Society General Meeting*, San Diego, 22-26 July 2012, 1-6. http://dx.doi.org/10.1109/pesgm.2012.6345533

[12] Fovino, I.N., Guidi, L., Masera, M. and Stefanini, A. (2011) Cyber Security Assessment of a Power Plant. *Electric Power Systems Research*, **81**, 518-526. http://dx.doi.org/10.1016/j.epsr.2010.10.012

[13] Rudrapattana, S. (2013) Cyber-Security Analysis in Smart Grid SCADA Systems: A Game Theoretic Approach. PhD Diss., Texas Tech University.

[14] Mahmud, R., Vallakati, R., Mukherjee, A., Ranganathan, P. and Nejadpak, A. (2015) A Survey on Smart Grid Metering Infrastructures: Threats and Solutions. *International Conference on Electro/Information Technology* (*EIT*), DeKalb, 21 May 2015, 386-391.

[15] Tweed, K. (2014) Attack on California Substation Fuels Grid Security Debate. IEEE Spectrum. http://spectrum.ieee.org/energywise/energy/the-smarter-grid/attack-on-california-substation-fuels-grid-security-debate

[16] Tweed, K. (2014) Attack on Nine Substations Could Take Down U.S. Grid. IEEE Spectrum. http://spectrum.ieee.org/energywise/energy/the-smarter-grid/attack-on-nine-substations-could-take-down-us-grid

[17] Rihan, M., Ahmad, M. and Beg, M. (2013) Vulnerability Analysis of Wide Area Measurement System in the Smart Grid. *Smart Grid and Renewable Energy*, **4**, 1-7. http://dx.doi.org/10.4236/sgre.2013.46A001

[18] Medida, S., Sreekumar, N. and Prasad, K.V. (1998) SCADA-EMS on the Internet. *Proc. International Conference on Energy Management and Power Delivery* (*EMPD*), **2**, 656-660. http://dx.doi.org/10.1109/empd.1998.702766

[19] Kumar, N.R., Mohanapriya, P. and Kalaiselvi, M. (2014) Development of an Attack-Resistant and Secure SCADA System Using WSN, MANET, and Internet. *International Journal of Advanced Computer Research*, **4**, 627.

[20] Alcaraz, C., Lopez, J., Zhou, J. and Roman, R. (2011) Secure SCADA Framework for the Protection of Energy Control Systems. *Concurrency and Computation*: *Practice and Experience*, **23**, 1431-1442. http://dx.doi.org/10.1002/cpe.1679

[21] Grilo, A.M., Chen, J.J., Diaz, M., Garrido, D. and Casaca, A. (2014) An Integrated WSAN and SCADA System for Monitoring a Critical Infrastructure. *IEEE Transactions on Industrial Informatics*, **10**, 1755-1764. http://dx.doi.org/10.1109/TII.2014.2322818

[22] Parik, P.P., Kanabar, M.G. and Sidhu, T.S. (2010) Opportunities and Challenges of Wireless Communication Technologies for Smart grid Applications. *Power and Energy Society General Meeting*, Minneapolis, 25-29 July 2010, 1-7. http://dx.doi.org/10.1109/pes.2010.5589988

[23] Baayer, A., Enneya, N. and Elkoutbi, M. (2012) Enhanced Timestamp Discrepancy to Limit Impact of Replay Attacks in MANETs. *Journal of Information Security*, **3**, 224-230. http://dx.doi.org/10.4236/jis.2012.33028

[24] Gao, J., Xiao, Y., Liu, J., Liang, W. and Chen, C.P. (2012) A Survey of Communication/Networking in Smart Grids. *Future Generation Computer Systems*, **28**, 391-404. http://dx.doi.org/10.1016/j.future.2011.04.014

[25] Chakrabarti, A. and Manimaran, G. (2002) Internet Infrastructure Security: A Taxonomy. *Network*, **16**, 13-21.

[26] Sule, R., Katti, R.S. and Kavasseri, R.G. (2012) A Variable Length Fast Message Authentication Code for Secure Communication in Smart Grids. *Power and Energy Society General Meeting*, San Diego, 22-26 July 2012, 1-6. http://dx.doi.org/10.1109/pesgm.2012.6345622

[27] Khanna, A. (2012) Smart Grid, Smart Controllers and Home Energy Automation—Creating the Infrastructure for Future. *Smart Grid and Renewable Energy*, **3**,165-174. http://dx.doi.org/10.4236/sgre.2012.33024

[28] Tesfahun, and Bhaskari, D.L. (2015) Effective Hybrid Intrusion Detection System: A Layered Approach. *International Journal of Computer Network and Information Security* (*IJCNIS*), **7**, 35. http://dx.doi.org/10.5815/ijcnis.2015.03.05

[29] Sridevi, S.K. and Mohammed, A.A.K. (2015) Preventing Black Hole Attacks in MANETs Using Secure Knowledge Algorithm. *International Conference on SPACES*, India, 2 January 2015, 421-425.