 doi:10.20944/preprints201610.0092.v1

Review

Wireless Sensor Network Based Smart Grid Communications: Cyber Attacks, Intrusion Detection System and Topology Control

Lipi Chhaya [1,*], Paawan Sharma [1], Govind Bhagwatikar [2] and Adesh Kumar [1]

[1] University of Petroleum & Energy Studies, Dehradun 248007, India; PAAWAN.SHARMA@ ddn.upes.ac.in (P.S.); ADESHKUMAR@ddn.upes.ac.in (A.K.)
[2] SANY Group, Pune, India; gowind.india@gmail.com
* Correspondence: lipi.chhaya@gmail.com; Tel.: +91-991-337-9801

Abstract: An existing power grid is going through a massive transformation. Smart grid technology is a radical approach for improvisation in prevailing power grid. Integration of electrical and communication infrastructure is inevitable for the deployment of Smart grid network. Smart grid technology is characterized by full duplex communication, automatic metering infrastructure, renewable energy integration, distribution automation and complete monitoring and control of entire power grid. Wireless sensor networks (WSNs) are small micro electrical mechanical systems which are capable to collect and communicate the data from surroundings. WSNs can be used for monitoring and control of smart grid assets. Security of wireless sensor based communication network is a major concern for researchers and developers. The limited processing capabilities of wireless sensor networks make them more vulnerable to cyber-attacks. The countermeasures against cyber-attacks must be less complex with ability to offer confidentiality, data readiness and integrity. The address oriented design and development approach for usual communication networks requires a paradigm shift to design data oriented WSN architecture. This paper describes communication standards, various cyber-attacks and their solutions. WSN security is an inevitable part of smart grid cyber security. This paper is expected to serve as a comprehensive assessment and analysis of communication standards, cyber security issues and solutions for WSN based smart grid infrastructure.

Keywords: communication standards; cyber security; smart grid; wireless sensor networks

1. Introduction

The electrical grid is being revolutionarily transformed as Smart grid. Smart Grid is an automated and broadly distributed energy generation, transmission and distribution network. It is characterized by full duplex network with bidirectional flow of electricity and information. It is a close loop system for monitoring and response [1-4]. It can be defined in various ways as per its functional, technological or beneficial aspects. As per the definition given by U.S. department of energy, "A smart grid uses digital technology to improve reliability, security, and efficiency (both economic and energy) of the electric system from large generation, through the delivery systems to electricity consumers and a growing number of distributed-generation and storage resources" [5]. Smart Grid is an integration of electrical as well as information and communication technology to make the power grid more reliable, flexible, efficient and robust. It is an intelligent power grid with integration of various alternative and renewable energy resources by using automated monitoring, data acquisition, control and emerging communication technologies. Application of diverse set of communication standards requires analysis and optimization depending upon requirements. This requirements can be decided on the basis of area of coverage, application bandwidth requirement etc. It can be categorized as HAN, NAN and WAN as per the applications of communication technologies at various levels of deployment of smart grid [6 -9].

 doi:10.20944/preprints201610.0092.v1

1.1. Home Area Network

HAN is applicable for home automation. It is used for the consumer domain and consists of electronics appliances and wireless sensor networks [7]. These consumer electronics appliances communicate their energy consumption statistics to central or main home monitor and regulator or smart meter. Central regulator or smart meter sends it to the central electricity grid for monitoring, control, fault detection and billing purposes. Smart meters receive the commands from central power grid and they control the home appliances based on the received commands. The Home Area Networks (HANs) ranges for the coverage area of few meters. IEEE 802.15.1 (Bluetooth), IEEE 802.15.4 (Zigbee), IEEE 802.11 (WLAN/Wi-Fi), Narrowband PLC etc. standards can be used for Home area networks [8-10].

1.2. Neighborhood Area Network

The function of Neighborhood Area Network (NAN) is to communicate the information collected by smart meters with central controller [8]. The NANs may contain few hundreds of smart meters deployed in HANs. Smart meters are linked with different gateways through NANs. The coverage region of NANs is around 1-10 square miles. The requirement of data rates for NAN is around 10 - 1000 Kbps [9-12].

1.3. Wide Area Network

The Wide Area Network (WAN) connects various NANs. Data collection points are located and the collected data is forwarded to central controller. The coverage area for WAN is around thousands of square miles [13-16]. The requirements of data rate are around 10-100 Mbps. Wide area requires very high bandwidth for its operation and management. WAN is suitable for Supervisory Control And Data Acquisition (SCADA) systems for monitoring, data acquisition, control and management of power grid [17]. With the advancement in communication systems and embedded systems, wireless sensor networks have become an inevitable component of smart grid technology. They can be used to bring intelligence in power grid with their capability to collect, store, process and communicate the data [18-20].

2. Application of Wireless Sensor Networks in Smart Grid

Wireless sensor networks can be used for accurate monitoring of generation, transmission, distribution and consumption of electricity. WSN is a cost effective solution for monitoring, control, measurement and fault diagnosis at various domains of smart grid network. WSN facilitates both sensing and communication requirements [21-23]. Small sensor nodes collectively form a sensor network which is used for remote wireless communication in HAN, NAN and WAN. Large scale deployment of sensor nodes can communicate conditions various generation, transmission and distribution unites. Wireless sensor nodes can provide cost effective solution for smart microgrid monitoring which facilitates high penetration of renewable energy sources. WSN is a significant part of advanced metering infrastructure [24]. Sensing and communication are crucial for PHEV system which is one of the most inventive component of smart grid technology. An effective remote monitoring and diagnosis can prevent cascaded catastrophic events and breakdowns. A sensor node mainly contains sensors, memory, CPU, transceiver and actuators. Sensors can be used to sense various quantities like humidity, temperature, current etc. Generally WSN nodes are battery powered. Figure 1 shows the basic structure of WSN node.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 October 2016 doi:10.20944/preprints201610.0092.v1

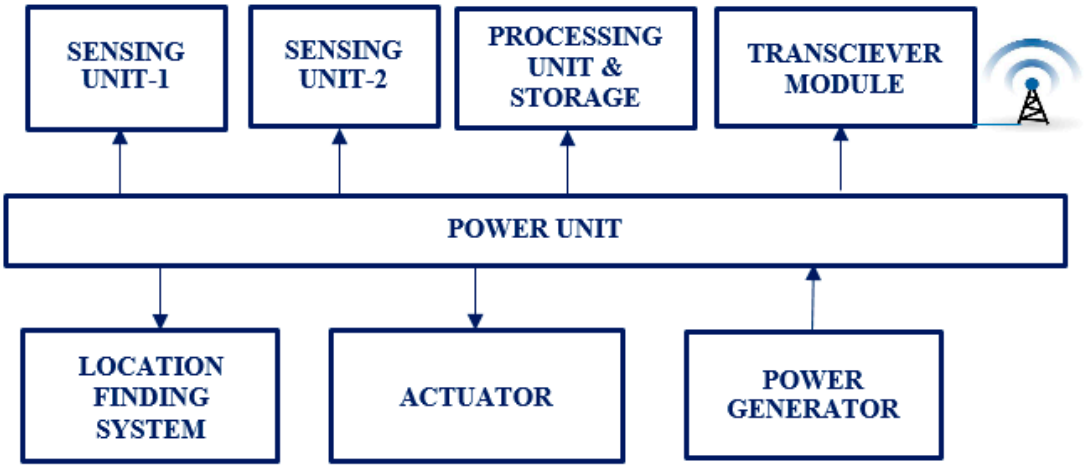

Figure 1. Architecture of WSN node

WSN is the most suitable option for HAN, NAN, WAN and smart microgrid applications for integration and operation of renewable energy sources. Figure 2 shows the application of WSN at different levels of smart grid.

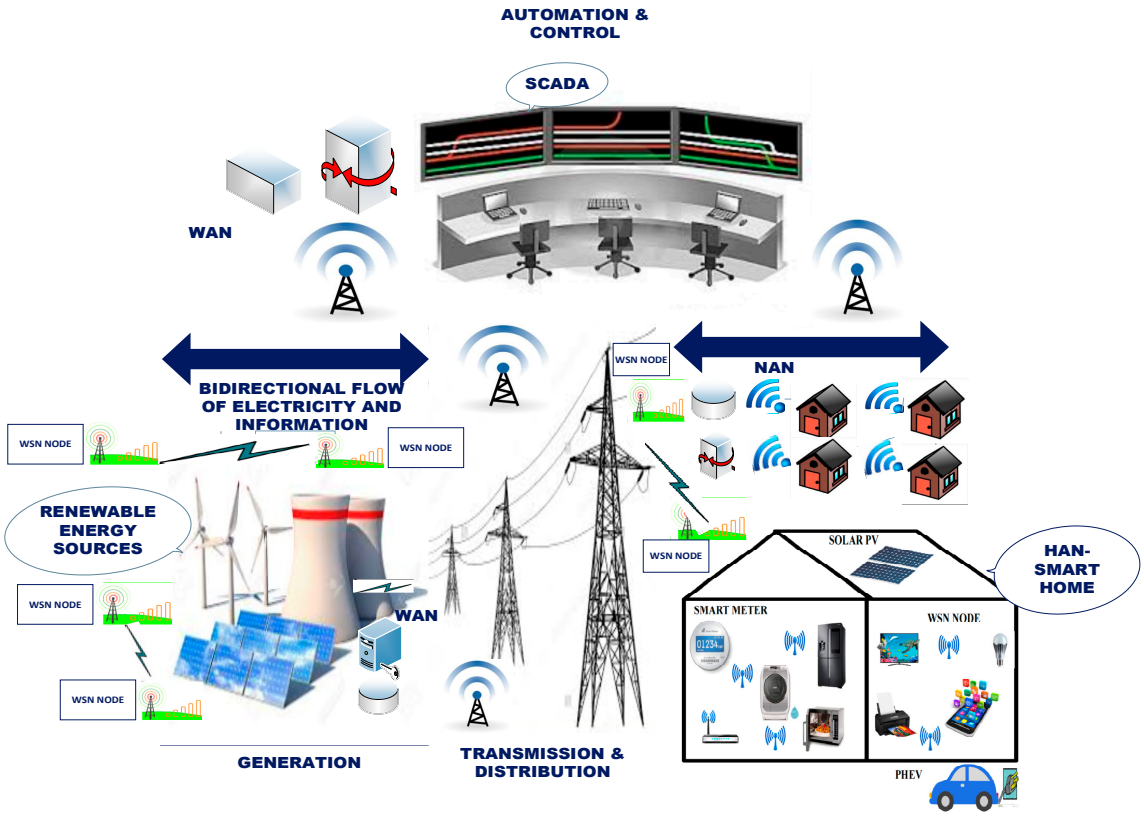

Figure 2. Application of WSN in smart grid hierarchical architecture

 doi:10.20944/preprints201610.0092.v1

Wireless sensor networks are applicable for following smart grid utilities.

- Smart power generation

Wireless sensor networks can be used at generation side for monitoring and management of energy generated. Wireless sensor networks are the prominent solution for smart microgrid applications using renewable energy resources. They can be used in solar farm, wind farm, biogas plant etc. for monitoring and control of energy. One of the objective of smart grid is to expedite the use of renewable energy sources. Renewable energy resources are situated in harsh environments and hostile locations. Moreover, their unpredictable behavior creates more challenges during their operation and management. WSN nodes are economical solutions for monitoring the behavior of renewable energy resources [25]. Various parameters of generating equipment can be effectively measured, communicated and controlled using WSN.

- Smart power transmission and distribution

Transmission and distribution of power contains various components like overhead transmission lines, underground cable network, substations and distribution transformers. WSN is an essential component for SCADA system. Real time remote monitoring of these components is inevitable to prevent power failure due to equipment breakdown or malicious attacks. Wireless sensor networks can be used for power monitoring, fault detection and isolation, location detection and outage discovery [22-25].

- Customer applications

Wireless sensor network is an effective and prominent solution for home automation systems. They can be used for complete energy management of customer premises. Consumer plays an active role in smart grid technology. Consumers have the power to decide the time of use and rates of energy usage in smart homes [23-25]. For these applications, wireless sensor networks are inevitable for communication and processing of information. WSN is a backbone of smart home applications and HAN [26].

3. Challenges of Wireless Sensor Networks in Smart Grid Applications

WSNs are a vital part of self-healing smart grid network as sensor nodes communicate parameters pertaining to conditions of various equipment and energy sources. However, there are many challenges in deployment and operation of WSN due to limitations of sensor nodes and complexity of heterogeneous smart grid network [22-26]. The challenges are summarized as below.

- Severe ecological conditions

Wireless sensor nodes can be subjected to harsh environmental condition which may cause fault of wireless sensor node.

- Various network topologies

Heterogeneous network topologies in energy distribution network due to various features and failure of sensor nodes may cause technical challenges in design of sensor nodes.

- Limited capability

Restricted processing and memory capabilities cause various challenges in design and deployment of wireless sensor networks.

- Bit errors

In communication systems, high bit error rates are observed due to high noise level. This calls for various errors detection and correction schemes. Detection and correction of error requires high memory and processing facilities which makes the design of sensor network challenging.

- Security of sensor networks

Security of wireless sensor network is an indispensable and decisive requirement. The sensor nodes must be secured from physical tampering to hacking for smooth functioning of various smart grid applications. Physical tampering is also called node capture.

- Quality of service necessities for smart grid environment

 doi:10.20944/preprints201610.0092.v1

The parameters like high data rates, latency, reliability and authenticity are vital for quality of service necessities of smart grid applications. Wireless sensor networks must fulfill these criterions for successful implementation of various applications.

4. Communication Standards for Wireless Sensor Networks

The address oriented traditional communication network is based on dedicated physical and network identification of transmitter and receiver. While WSN comprises of redundant nodes to compensate for degraded signal strengths of the nodes or node failure. Therefore in WSN, specific address of a node is of least concern. Measured values must be communicated between nodes irrespective of an address of the node. Thus, WSN communication is data oriented. WSN communication architecture design entails a conceptual paradigm shift based on applications. The communication standards applicable for WSN are describes as below.

4.1 Zigbee

Zigbee is based on IEEE 802.15.4 standard. It is an energy proficient short range wireless communication technology. It functions in the ISM band which is allocated for industrial, scientific and medical applications. Zigbee operates in the band of 2.4 GHz, 868 and 928 MHz with full duplex wireless data transmission. IEEE 802.15.4 standard describes physical layer and media access layer and Zigbee Alliance has expanded the configuration of an application layer and network layer. The maximum throughput achievable by Zigbee is 250 Kbps [15]. In the area of power automation, it is applicable for smart meters, power system monitoring and measurement of various electric parameters. Smart Grid integrates information and communication technology with existing power system to improve the power grid network with the capabilities of self-healing, disaster recovery, interoperability and compatibility, energy efficiency and security [17-20]. Zigbee can play an imperative role in operation and maintenance of power grid, data accumulation, parameter measurement, security monitoring and consumer interface.

4.2. Bluetooth

Bluetooth is a short distance wireless communication technology based on IEEE 802.15.1 standard. It uses short wavelength wireless transmission in the unlicensed ISM band from 2400 to 2480 MHz. It uses frequency hopping spread spectrum (FHSS) technology and around 1600 hops per second. Its key features are extensive availability, low power consumption and rapid data exchange. Bluetooth was initially developed in 1994 by Ericsson and then a group of firms formed a special interest group to retain and improve this technology. There are two network topologies used in Bluetooth which are termed as Piconet and Scatternet. A Piconet is created by a Personal Area Network in which one wireless client acts as a master and other wireless clients serve as slaves. Maximum eight devices can communicate with each other in one Piconet. A Scatternet is an arrangement of group of Piconets. Bluetooth is used for communications between smart consumer appliances, energy management system and smart meters. It has peak data throughput of 1 Mbps, 79 radio frequency channels and channel bandwidth of 1 MHz, nominal range of around 10 meters. Bluetooth comprises of three power classes each having a different range [15-18].

4.3. Wireless Fidelity or Wireless local area network

Wireless Fidelity (Wi-Fi) or wireless local area network technology is established on the basis of IEEE 802.11 standard. Wireless local area networks are wide spread for LAN applications with peak data rates of around 150 Mbps and extreme coverage range of 250 meters. Wi-Fi (IEEE 802.11b) operating on 2.4 GHz band achieves maximum data rates of 11 Mbps. Other versions based on IEEE 802.11a standard operates in 5.8 GHz band using Orthogonal Frequency Division Multiplexing (OFDM) and IEEE 802.11g (improved version of Wi-Fi) operates on 2.4 GHz band provides data rate up to 54 Mbps. IEEE 802.11 provides Data rates of up to 600 Mbps using Multiple Input–Multiple

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 October 2016 doi:10.20944/preprints201610.0092.v1

Output (MIMO) technology [15-19]. Security concerns for Wireless local area networks are addressed and solved in IEEE 802.11i standard (WPA-2). It uses an Advanced Encryption Standard. The main feature of Wi-Fi is existing wide support in most of the electronic devices. It is an upper layer protocol which allows communication over an Internet without using a protocol translator. Restricted number of channels can be used without an overlap in Wi-Fi/WLAN. This means that a restricted number of wireless clients can be connected in a Network. However, advantages of Wi-Fi are high data throughput, wide spread availability, IP support and network scalability. A self-healing network for HAN applications with the combination of WLAN and wireless mesh network can be developed.

4.4. Z-Wave

Z-Wave protocol is specifically designed for smart home applications. It can be adopted in Home area networks of smart grid. Z-Wave is a low data rate, short range radio frequency mesh networking standard operating on 908 MHz band. The maximum coverage area is 30 meters indoor and 100 meters outdoor. It does not require central coordinator but employs master and slave nodes. It can support 232 devices. The data rate is from 9.6 Kbps to 40 Kbps.

4.5. WirelessHART

WirelessHART protocol is designed for industrial automation and control applications. It is based on IEEE 802.15.4 compatible radio and operates on 2.4 GHz ISM band. It uses direct sequence spread spectrum technology. Besides DSSS, it uses TDMA technology in which 10 ms time slots are allocated to nodes. The range of this technology is up to 200 meters [15]. Security of communications is maintained using 128 bit AES encryption. Individual session keys as well as common network encryption key are shared among all nodes for broadcast services.

4.6. Wavenis

Wavenis is an emergent wireless communication technology for low power M to M (Machine to machine) applications. It can be used for distances up to 200 meters for various indoor applications. This technology can be used in various metering application in smart grid. It can be used in automatic meter reading, advanced metering infrastructure and remote communication applications. Wavenis operates in the bands of 868 MHz, 915 MHz, and 433 MHz. The data throughput of Wavenis ranges from 4.8 Kbps to 100 Kbps.

Wireless sensor network (WSN) uses various short distance communication technologies as they are suitable for power efficiency and wide spread availability. These communication standards use unlicensed ISM band for their operation which makes WSN both effective as well as vulnerable to attacks.

5. Security Issues in Wireless Sensor Networks

The wireless sensor networks used for smart grid applications have different characteristics than networks used for other generic applications. These characteristics are in terms of deployment topology, data processing, environmental conditions and network throughput. The security issues are related to confidentiality, authentication, availability, integrity, authorization, newness. Confidentiality deals with secrecy of data communication. Authentication is necessary for prevention of fake messages from malicious sensor nodes. It ensures data authenticity. Availability means consistency in services in presence of attacks. Integrity means the data or message is received in an unaffected form at the destination. Authorization means only authorized sensor nodes can communicate and unauthorized access of data must be prevented. Newness of data is inevitable to ensure that attackers do not replay the old data again to hinder the security of WSN [26-28]. It is very challenging to ensure the mentioned measures of data authenticity and security due to following reasons.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 October 2016 doi:10.20944/preprints201610.0092.v1

- WSNs communicate using radio transmissions and most of them use unlicensed ISM band which is used for many other applications.
- WSN nodes have very limited storage and processing capabilities.
- WSNs are deployed in potentially unsecured environments.
- WSN nodes have limited power.

Due to above reasons, sensor nodes are prone to eavesdropping or jamming attacks. Moreover, limited processing and storage capabilities of sensor nodes prevent the use of advanced cryptographic methods. Public key cryptography requires costly computation methods. Limited batteries of WSN make them prone to denial of service attacks which can further drain the energy from nodes. Tampering of sensor nodes and reprogramming of chip are the possible attacks. The security of WSN can be endangered by reverse engineering [27]. Smart grid also employs various devices and communication protocols at different network levels. So, WSN interoperability and security with other devices is also a matter of concern. The protection and privacy of WSN must be treated carefully for smart grid application which is a broad network comprising of enormous networks and protocols. The public and private security measures for WSN in various smart grid applications require costly solutions [28-30]. The cost–security tradeoff must be carefully implemented. Figure 3 shows the complete overview of applications, security issues and objectives of WSN for smart grid network.

Figure 3. An overview of applications, security issues and security measures of WSN for smart grid applications

6. Cyber Threats/Attacks in Wireless Sensor Networks

In addition to above wireless network security issues, WSNs are vulnerable to cyber-attacks on various network layers [28-31]. Figure 4 depicts various cyber-attacks in WSNs at various network layers.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 October 2016 doi:10.20944/preprints201610.0092.v1

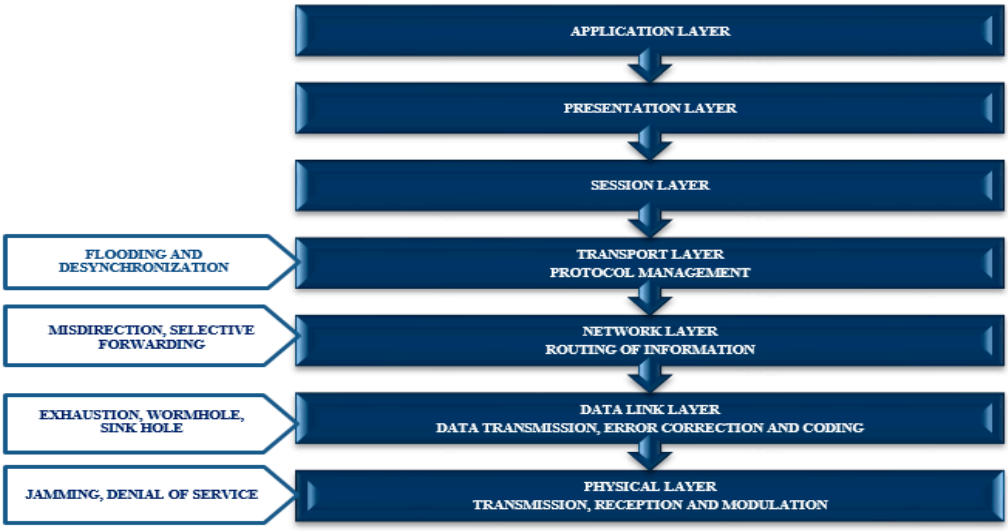

Figure 4. Attacks on various network layers

6.1. Denial of service attack

Restricted memory and computational capacity of wireless sensor network make them vulnerable of denial of service attack. In this attack, network resources are made inaccessible by network congestion [31-33].

Three types of denial of service attacks are described in literatures.

6.1.1. Physical devastation/Node capture of wireless sensor nodes

Wireless sensor nodes are deployed and distributed at various places for various applications and there are possibilities of physical damage or destruction of nodes by attackers. Node capturing may result into alteration of hardware and software of WSN node.

6.1.2. Utilization of network resources by intruders and making the scarce resources unavailable

Attackers or intruders can exploit the limited network resources and make them unavailable for actual users.

6.1.3. Alteration of configurations of wireless sensor network by attackers

The encryption and other WSN configuration aspects must be confidential and any alterations made by intruders make them in accessible for users. Jamming of network, camouflaging the wireless sensor network ambiance and physical attack on sensor node are common threats [33].

6.2. Misdirection attack

In the misdirection attack, the information is routed at fake path. It alters the routing information of network and affects the communication adversely. Misdirection is a network layer attack. Authentication techniques between transmitter and receiver, multi hop routing etc. can be used to detect misdirection attack.

6.3. Selective forwarding

Selective forwarding is a network layer attack. In this type of attack, a counterfeit node acts like an actual node and divert the packets to a wrong path but selectively drops some of the packets so that it becomes difficult to identify the intrusion. Acknowledgement based routing, multi data flow and detection based on neighboring information can be used to detect this type of intrusion.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 October 2016 doi:10.20944/preprints201610.0092.v1

6.4. Sink hole attack

It is a data link layer attack. In this attack, an intruder comes with an agreement with a sensor node or introduces a fake node in the sensor network. When a fake node attracts the network traffic, an attack is generated. Once the attack is successful the fake node can perform various malfunctions like dropping all packets, dropping selective packets and alteration of data [32, 33].

6.5. Sybil attack

In Sybil attack, a malicious sensor node takes multiple identities to perform an attack. In wireless sensor network, all the sensor nodes work complaisantly but this type of attack targets this cooperation and disturb the routing and communication process.

6.6. Wormhole attack

Wormhole attack is a data link layer intrusion. In this type of attack, a malicious or fake node records all the information and diverts it to wrong path. This attack can be formed without the knowledge of cryptography of actual wireless sensor node.

6.7. Hello flood attack

In wireless sensor networks, routing protocols use Hello packets for detection of neighbors. In this type of attack, fake packets are used to camouflage hello packets and to attract the sensor nodes [33]. Attackers with ample radio resources and processing capabilities can generate this type of attack. The victim node will identify fake hello packet as normal node.

7. Intrusion Detection System

Intrusion detection system (IDS) can be defined as a combination of hardware and software tools which are meant to detect internal or external cyber-attacks. The principle tasks of IDS are prevention and detection of attacks, situational awareness, evidence collection, and administration of connection topologies [34].

- Sensor: It collects statistics from the system being monitored.
- Detector: It analyze collected data to identify intrusions.
- Knowledge Base: It supports the detector by providing attack signatures.
- Response Manager: It manages the responses to the cyber-attacks.

The general block diagram of IDS is shown in Figure 5.

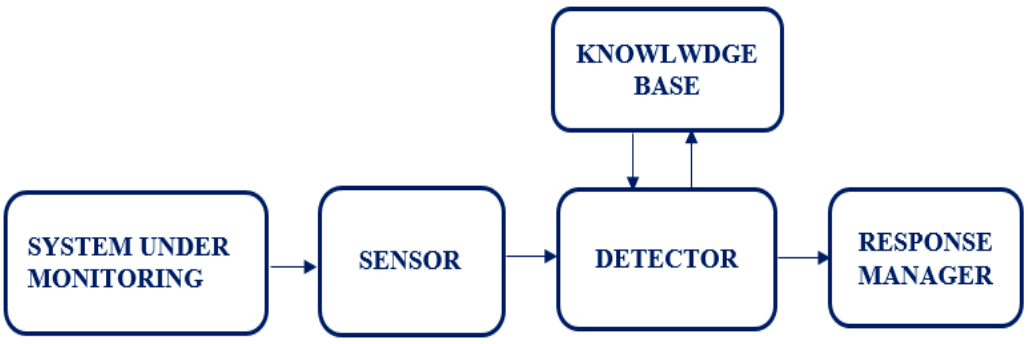

Figure 5. General block diagram of intrusion detection system

 doi:10.20944/preprints201610.0092.v1

The strategies for attacks and detection system for WSNs is different from other wireless or wired networks due to their structure and limited battery life. Intrusion detection approaches for WSN are classified as follows [33-35].

7.1. Anomaly Detection

The different types of anomalies of WSN are node anomaly, network anomaly and data anomaly as described below.

- Node Anomaly: This types of anomalies can be detected during failure of WSN node or power problems. Failure of solar panel, or fluctuations in power of different components can cause this type of anomaly. Node anomalies can be due to hardware or software issues in the WSN nodes.
- Network Anomaly: Unexpected fluctuations in the signal strength and connection problems can be used to detect network anomaly. Complete loss of connectivity or episodic connectivity can be used to detect intrusions in the network.
- Data Anomaly: An intrusion attempt can be detected from chaotic or disordered data communication.

Detection of a specific type of anomaly is very useful to decide the type and solution of cyber-attack. To detect the above mentioned anomalies, different types are approaches are applied. These anomaly detection approaches can be classified as game theoretic, statistical, machine learning, artificial immune system and data mining based approach.

7.2. Misuse Detection

Misuse detection is a signature based intrusion detection system to discover recognized attacks. The limitation of this type of detection system is that it cannot detect unknown attacks which are not predefined. Moreover, keeping signatures of attacks to generate data base is a complicated task for WSN due ti its limited memory and processing capabilities. However in very few literatures, this method has been explored using watchdog approach [8]. Watchdog approach uses the abnormal behavior of a node to detect an intrusion. All nodes watch the performance of their neighbors and communicate the information about their behavior.

7.3. Hybrid detection

An intrusion detection approach that does not qualify to be classified as either anomaly or misuse detection is called hybrid detection method. This approach is application specific and manually defined by an administrator. Hybrid approach can be a combination of anomaly and misuse detection approaches for accurate results.

8. Topology Control

Wireless sensor networks are the group of distributed sensor nodes which communicate various information for monitoring and control purpose. Sometimes it is required to place WSN nodes in unsecured and hostile environments. Due to limited battery life and restricted processing and storage capabilities of WSN nodes, security against above mentioned attacks is the biggest challenge. WSN nodes are an inevitable part of smart grid communication infrastructure. Apart from cryptographic approach as mentioned above, WSN can be designed in such a way that their topologies have specific connectivity properties [36]. Topology control can be a practical solution for WSN nodes with limited computational and communication capabilities [37-39]. An overview of various topology control schemes is described below.

8.1. Random key predistribution scheme

This scheme is extensively recognized as an appropriate solution for secured WSN communication. There are two types of random key predistribution scheme.

 doi:10.20944/preprints201610.0092.v1

8.1.1. Eschenauer–Gligor Random Key Predistribution Scheme (EG scheme)

In EG scheme, there are n number of sensors in a keying network. This scheme uses an offline pool of keys containing Pn keys. Before deployment, each sensor is assigned Kn number of discrete keys selected from pool of keys. Pn and Kn both are the functions of n for generality reasons. Kn keys in each sensor establish sensor's key ring. After deployment, two sensors can establish secured communication link only if they have at least one key (s) in common i.e. $1 \leq s \leq Kn$. Confidentiality and authenticity are achieved with symmetric key encryption mode [37].

8.1.2. s -Composite Random Key Predistribution Scheme

s -Composite Random Key Predistribution Scheme is better than EG scheme in a way that it requires minimum one overlapped key in order to establish communication between two sensors. It requires $s \geq 2$ for secured communication between sensors. It is beneficial for small scale sensor attacks but becomes vulnerable for large scale attacks. S is selected according to desired resilience of the sensor network.

8.2. Link constraint models

Various link constraint models are used to explore WSN using either EG or s- composite schemes. They are classified as follows.

8.2.1. Full visibility model

In this model, it is assumed that there is a communication link between any two sensor nodes in a network. According to this model, the two sensors can establish a secured communication link only if they have one key for EG scheme and s keys for s-composite scheme common among them [40-42]. This model requires shared keys between sensor nodes which satisfy both the schemes.

8.2.2. On-Off channel model

This model contains independent channels, each of which is either on with probability Pn or off with probability (1− Pn), where Pn is a function of n for generality. This model requires the channel between two sensors to be on for communication.

8.2.3. Disk model

This model requires sensor nodes to be within a specific radius r_n to establish a communication link between them. For the node distribution, it is considered that all n nodes are uniformly and individually deployed in a bounded area of a Euclidean plane. Such network area A is either a torus T or a square S, each of unit area, depending on whether the boundary effect exists [40]. The boundary effect arises whenever part of the transmission area of a node may fall outside the network area A. T does not have the boundary effect, whereas S has the boundary effect [41-43].

9. Conclusions

The present power grid is going through huge transformation with the deployment of smart grid technology. Smart grid is a complex hierarchical and heterogeneous network. Wireless sensor network is a prominent solution for various applications of smart grid. Wireless sensor networks are distributed collection of sensor nodes situated at various places for measurement and communication of various parameters such as temperature, voltage, current and humidity. These parameters are required for remote monitoring and control of different components of smart grid. WSNs are effective solutions for energy management system in home, industry and business applications. These small sensor nodes are extensively vulnerable to attacks as they are placed in hostile environment. Node capture results into complete control of attacker on the WSN node and tampering of hardware as well as software of WSN. The energy exhausted sensor nodes can be easily victimized. Therefore, cryptographic security is essential to protect the communication between sensor nodes as well as to detect sensor capture and to invalidate the compromised security keys. The security of dispersed WSN nodes is a crucial technical challenge due to limited memory and computational capabilities of WSN nodes.

 doi:10.20944/preprints201610.0092.v1

The data oriented design approach is required for deployment of WSN as the purpose of sensor nodes is to sense and communicate the parameters. Redundant nodes must be deployed to deal with node failures and degraded signal strengths. Traditional communication process involves physical address and IP address of a specific transmitter and receiver to establish successful communication link. This type of communication is address oriented which is different from WSN approach. As an example, consider the measurement of average temperature of some area. In this case, temperatures from each and every node is not required but an average temperature can be calculated from received readings from sensor nodes placed at various places. Identity of a specific node is secondary as soon as the readings from all areas are received. The challenges of WSN communication is different from the challenges faced by the usual communication networks.

In this paper, the analysis of various wireless communication standards, cyber security issues and solutions are discussed. Nature of various attacks must be known for detection of attacks and development of different solutions at diverse network layers. Apart from well researched solutions like IDS and cryptographic security, this paper explores topology control for cyber security of wireless sensor networks. Secured interoperability between various communication standards is inevitable for robust hierarchical smart grid infrastructure. WSN security is a multi-faceted research topic due to limitations imposed by communication standards and sensor nodes. The cost-security tradeoff must be critically analyzed and implemented for future applications of wireless sensor networks in smart grid applications.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in the paper.

AMI	Advanced metering infrastructure
CPU	Central processing unit
EG	Eschenauer–Gligor
HAN	Home area network
IDS	Intrusion detection system
IEEE	Institute of electrical and electronics engineer
ISM	Industrial, scientific and medical
MIMO	Multiple input multiple output
NAN	Neighborhood area network
PHEV	Plug in hybrid electric vehicle
PLC	Programmable logic converter
SCADA	Supervisory control and data acquisition
TDMA	Time division multiple access
WAN	Wide area network
Wi-Fi	Wireless fidelity
WSN	Wireless sensor network

References

1. Farooq, H.; Jung, L.T. Choices available for implementing smart grid communication network. In proceedings of IEEE International Conference on Computer and Information Sciences (ICCOINS), Kuala Lumpur, 2014, 1-5.
2. Feng, Z.; Yuexia, Z. Study on smart grid communications system based on new generation wireless technology. In proceedings of IEEE International Conference on Electronics, Communications and Control (ICECC), Ningbo, 2011, 1673-1678.
3. Giustina D.D.; Rinaldi S. Hybrid Communication Network for the Smart Grid: Validation of a Field Test Experience. *IEEE Trans. Power Delivery* **2015**, 30, 2492-2500.
4. Goel, N.; Agarwal, M. Smart grid networks: A state of the art review. In proceedings of IEEE International Conference on Signal Processing and Communication (ICSC), Noida, 2015, 122-126.
5. U.S. Department of Energy. Smart Grid System Report. Available online: http://energy.gov/sites/prod/files/2014/08/f18/SmartGrid-SystemReport2014.pdf (accessed on 18 August 2014).
6. Mulla, A.; Baviskar, S.; Khare, N.; Kazi, F. The Wireless Technologies for Smart Grid Communication: A Review. In proceedings of IEEE International Conference on Communication Systems and Network Technologies (CSNT), Gwalior, 2015, 442-447.
7. Kuzlu, M.; Pipattanasomporn, M.; Rahman, S. Review of communication technologies for smart homes/building applications. In proceedings of IEEE International Conference on Smart Grid Technologies - Asia (ISGT ASIA), Bangkok, 2015, 1-6.
8. Parvez, I.; Sundararajan, A.;. Sarwat,A.I. Frequency band for HAN and NAN communication in Smart Grid. . In proceedings of IEEE Computational Intelligence Applications in Smart Grid (CIASG) Symposium, Orlando, FL, 2014, 1-5.
9. Hiew, Y.K.; Aripin N.M.; Din, N.M. Performance of cognitive smart grid communication in home area network. In proceedings of IEEE Telecommunication Technologies (ISTT) symposium, 2014, Langkawi, 2014, 417-422.
10. Aalamifar, f.; Hassanein, S.; Takahara, G. Viability of powerline communication for the smart grid. In proceedings of 26th Biennial Symposium on Communications (QBSC), Kingston, 2012, 19-23.
11. Hartmann, T. Generating realistic Smart Grid communication topologies based on real-data. In proceedings of IEEE International Conference on Smart Grid Communications (SmartGridComm), Venice, 2014, 428-433.
12. Parikh, P. P.; Kanabar M.G.; Sidhu, T.S. Opportunities and challenges of wireless communication technologies for smart grid applications. In proceedings on 2010 IEEE power and energy society general meeting, 2010, 1–7.
13. Yan, Y.; Qian, Y.; Sharif, H.; Tipper, D. A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges. *IEEE Communications Surveys & Tutorials*, 2013, 15, 5-20.
14. Saputro, N.; Akkaya, K.; Uludag, S. A survey of routing protocols for smart grid communications. *Computer Networks*, **2012**, 56, 2742-2771.
15. Mahmood, A.; Javaid, N.; Razzaq, S. A Review of Wireless Communications for Smart Grid. *Renewable and sustainable reviews*, **2015**, 41, 248-260.
16. Erol-Kantarci, M.; Mouftah, H.T. Wireless multimedia sensor and actor networks for the next generation power grid. *Ad Hoc Networks*, 2011, 9, 542–551
17. Binti M. I. N.; Wei T.C.; Yatim, A.H.M. Smart grid technology: Communications, power electronics and control system. . In proceedings of IEEE International Conference on Sustainable Energy Engineering and Application (ICSEEA), Bandung, 2015, 10-14.
18. Gungor, V.V. Smart Grid Technologies: Communication Technologies and Standards. *IEEE Trans. Industrial Informatics* **2011**, 7, 529-539.
19. Amin, R.; Martin, J.; Zhou, X. Smart Grid communication using next generation heterogeneous wireless networks. In proceedings of IEEE Third International Conference on Smart Grid Communications (SmartGridComm), China, 2012, 229-234.
20. Bera, S.; Misra, s.; Obaidat, M.S. Energy-efficient smart metering for green smart grid communication. In proceedings of IEEE International Conference on Global Communications Conference (GLOBECOM), 2014 Austin, 2014, 2466-2471.

21. Monshi, M. M.; Mohammed, O.A. A study on the efficient wireless sensor networks for operation monitoring and control in smart grid applications. In proceedings of IEEE International Southeast Conference, USA, 2013, 1-5.
22. Gungor, V.V.; Lu, B.; Hancke, G. P. Opportunities and Challenges of Wireless Sensor Networks in Smart Grid, *IEEE Trans. Ind. Elec.* **2010**, 57, 3557-3564.
23. Brak, M.E.; Brak, S. E.; Essaaidi M.; Benhaddou, D. Wireless Sensor Network applications in smart grid. In proceedings of IEEE International Renewable and Sustainable Energy Conference (IRSEC), Ouarzazate, 2014, 587-592.
24. Zhang, Y.; Li, X.; Zhang, S. Zhen, Y. Wireless sensor network in smart grid: Applications and issue. In proceedings of World Congress on Information and Communication Technologies (WICT), Trivandrum, 2012, 1204-1208.
25. Erol-Kantarci, M.; Mouftah, H. T. Wireless Sensor Networks for smart grid applications. In proceedings of IEEE International Conference on Electronics, Communications and Photonics (SIECPC), Saudi, 2011, 1-6.
26. Erol-Kantarci, M.; Mouftah, H. T. Using wireless sensor networks for energy-aware homes in smart grids. In proceedings of IEEE Symposium on Computers and Communications (ISCC), Italy, 2010, 456-458.
27. Brak, M.E.; Essaaidi, M. Wireless sensor network in smart grid technology: Challenges and opportunities. In proceedings of IEEE International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), Sousse, 2012, 578-583.
28. Lu, Z.; Lu, X.; Wang, Wang, C. Review and evaluation of security threats on the communication networks in the smart grid. In proceedings of IEEE International Military Communications Conference, USA, 2010, 1830-1835.
29. Dini, G.; Tiloca, M. On simulative analysis of attack impact in Wireless Sensor Networks. In proceedings of IEEE International Conference on Emerging Technologies & Factory Automation (ETFA), Cagliari, 2013, 1-8.
30. Radmand, P.; Talevski, A.; Petersen, S.; Carlsen, S. Taxonomy of Wireless Sensor Network Cyber Security Attacks in the Oil and Gas Industries In proceedings of 24th IEEE International Conference on Advanced Information Networking and Applications, Perth, 2010, 949-957.
31. Mahmood, A.; Akbar, A. H. Threats in end to end commercial deployments of Wireless Sensor Networks and their cross layer solution. In proceedings of IEEE International Conference on Information Assurance and Cyber Security (CIACS), Pakistan, 2014, 15-22.
32. Neogy, S. Security management in Wireless Sensor Networks. In proceedings of IEEE International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), London, 2015, 1-4.
33. Can, O.; Sahingoz, O.K. A survey of intrusion detection systems in wireless sensor networks. In proceedings of 6th IEEE International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO), Turkey, 2015, 1-6.
34. Salehian, S.; Masoumiyan, F.; Udzir, N. I. Energy-efficient intrusion detection in Wireless Sensor Network. In proceedings of International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), Malaysia, 2012, 207-212.
35. Pietro, R. D.; Mancini, L. V.; Mei, A.; Panconesi, A.; Radhakrishnan, J. Connectivity properties of secure wireless sensor networks. In proceedings of ACM Workshop on Security of Ad-Hoc and Sensor Networks, Washington, DC, 53– 58, 2004.
36. Pietro, R. D.; Mancini, L. V.; Mei, A.; Panconesi, A.; Radhakrishnan, J. Redoubtable sensor networks. *ACM Trans. Info. and Syst. Security* **2008**, 11, 1–13.
37. Yağ˘an, O. Performance of the Eschenauer–Gligor key distribution scheme under an on/off channel. *Trans. Info. Theory* **2012**, 58, 3821–3835.
38. Jutla, C. S. Encryption modes with almost free message integrity In proceedings of International Conference on Theory and Applications of Cryptographic Techniques (Eurocrypt), Innsbruck,2001, 529–544.
39. Komls, J.; Szemerdi, E. Limit distribution for the existence of Hamiltonian cycles in a random graph. *Discrete Mathematics*, 1983, 43, 55–63.
40. Blackburn, S.; Gerke. S. Connectivity of the uniform random intersection graph. *Discrete Mathematics*, 2009, 16, 309-319.

 doi:10.20944/preprints201610.0092.v1

41. Bloznelis, S.M. Degree and clustering coefficient in sparse random intersection graphs. *Annals of Applied Probability*, 2013, 23(3), 1254–1289.
42. Krishnan, B.; Ganesh, A.; Manjunath, D. On connectivity thresholds in superposition of random key graphs on random geometric graphs. In proceedings of IEEE International Symposium on Information Theory (ISIT), Istanbul, 2013, 2389– 2393.
43. Krzywdzin´ski, V; Rybarczyk K. Geometric graphs with randomly deleted edges—Connectivity and routing protocols. *Mathematical Foundations of Computer Science*, 2011, 69, 544–555.