Security for Smart Distribution Grid By Using Wireless Communication

S.K.Saranya[1], Dr.R.Karthikeyan[2]

P.G Scholar, Dept of EEE, M.Kumarasamy College of Engineering, Karur, Tamilnadu, India[1]

Professor, Dept of EEE, M.Kumarasamy College of Engineering, Karur, Tamilnadu, India[2]

Abstract: In Smart Grid, the communication network plays a significant role. Wired communication adopted to ensure robustness of the backbone for power transmission network but it does not provide any flexibility. Wireless communication for power distribution grid provide more benefits such as low cost, high speed links, easy setup of connections among different devices or appliances and so on. Connecting equipment, devices and appliances through wireless communication is essential for Smart Distribution Grid (SDG). Mounting suitable wireless communication design and its security measures is extremely important for SDG. The Wireless communication design is proposed for SDG on Wireless Mesh Networks (WMNs). Its bidirectional communication and electricity flow enable both utilities and customer to monitor, forecast and handle energy usages. Yet, Wireless communication is usually susceptible to security problem. Being compromised by a malicious node is adversary would causes significant damage includes extended power outages and destruction of electrical equipment. It is crucial to security measures for SDG against intrusion of a malicious node to provide the availability of effective communication in SG.

Index Terms: Smart Grid (SG), Smart Distribution Grid (SDG), Wireless Communication, Wireless Mesh Network (WMNs).

I.   INTRODUCTION

As compared to today's power grid, smart grid is notable by several features. Smart grid is vigorous to load fluctuations and the supply-demand balance can be properly maintained via intelligent real-time dispatching mechanisms, large-capacity high-performance battery, distributed energy, and close customer-grid exchanges. Smart grid is also flexible to equipment failure, which prevents a single failure from developing into power outage or shutdown. Smart grid makes a power system more sustainable and more environmentally friendly by integrate renewable energy sources into the same grid. In smart grid, energy can be utilized efficiently through well-maintained balance between supply and demand. Smart Grid can bring various profits to customers. For example, customers can reduce the amount of power bill by harmonizing the operation time of different electric appliances to the period with best price; they can even get profit by selling power to the grid. Moreover, smart grid appreciably improves power availability and quality.

Many core technologies need to be developed to enable the above features of smart grid. Among them, one critical technology is real-time monitoring and control of a large scale power network, which demands a sophisticated communication network across the grid to fulfill two tasks: 1) exchange information acquired by distributed sensing; 2) disseminate management and control messages to electric equipment and appliances. Thus, developing novel communication technologies that meet the special requirements of a power network plays a critical role in smart grid.

Recently, smart grid (SG) is the buzz word, which has attracted attentions from engineers and researchers in both electric power and communication sectors. The concept of smart grid has appeared in recent literature in different techniques used to control the power grid operation. Some referred it is intelligent grid whereas some called it the grid of the future. The main objective of the smart grid concept is to provide the consumers with power in a more stable and

reliable manner that the aging power grids of today may not be able to provide in the near future. Smart grid can be used a two-way communication between the suppliers and consumers of electric power. The bi-directional communication indicates the ability of smart grid to enable the end users to express their power requirement demands to the utility suppliers.

In different segments of a power grid, different communication technologies are applied to meet their unique specific requirements. In a power transmission network that involves bulk power generation and power transmission, wired communications over power lines or optical cables are adopted to ensure robustness of the power backbone. However, in power distribution networks that provide power directly to customers, both wired and wireless communications should be considered. In a substation optical communication can be applied to monitor or control certain mission critical devices.

Different types of wireless networks are available, but which one is the best fit for an SDG depends on the system architecture of the SDG and varieties of communication modules and wireless connection. Moreover communication modules in an SDG may pertain heterogeneous properties in terms of communication range, computing power, and power efficiency. In an SDG, communication modules associated with electric devices are usually stationary, but mobile connections need to be supported at the customer side or on some handheld devices. The aforementioned requirements of SDG communications lie in the advantages of wireless mesh network (WMNs), so WMNs are well suited for wireless networking in an SDG. In fact, some companies have started to consider mesh links for wireless communications in a power distribution network.

II.   WIRELESS COMMUNICATION

In power distribution networks, wireless communications are preferred by many application scenarios, such as: 1) when many parameters in a substation need to be monitored, optical or power line communications can result in a costly and complicated system architecture; 2) power-line communications cannot easily bypass transformers in a power distribution network; 3) wired communications cannot provide peer-to-peer communications among electric devices in a flexible manner. In order to achieve cost effective and flexible monitoring and control of end devices, efficient dispatching of power to customers, and dynamic integration of distributed energy resources with power grid, wireless communication and networking functionalities must be embedded into electric equipments.

There exist several choices of wireless communications for connecting monitoring, control, and consumer electric devices. However, most of them (e.g., wireless local area networks (WLANs) or wireless sensor networks (WSNs) are not directly applicable to an SDG due to several issues. The first one is the flexibility in topology formation. In an SDG, various electric devices need to have peer to peer communications, so mesh networking capability is a viable option. However, a WLAN can only support one-hop point-to-multipoint (PMP) communications. Usually a WSN like a Zigbee network is also a PMP network unless mesh networking capability is added into Zigbee nodes. The second issue is that rate-distance performance is not scalable for SDG wireless communications. For example, a WLAN can support a communication rate of tens of Mbps, but it can only reliably reach a distance of tens of meters. Moreover, to achieve reasonable throughput delay trade-off, the number of nodes that can be supported within the same WLAN needs to be small. Thus, one WLAN is obviously not enough for an SDG. In theory, multiple WLANs can be adopted to support a large scale SDG. However, communications and coordination among different WLANs become difficult to manage. The better solution is to build WMNs based on WLAN technologies. The third issue is that SDG wireless communications need to support different types of wireless applications. For example, some electric nodes only need to send control or measurement information in a low frequency, so the communication capability like WSN is sufficient. However, for some other nodes like the gateway node in a home or for an entire community definitely demand a much higher communication rate and a larger communication distance. In this case, communication technologies based on

Wi-Fi with high-gain antenna may be necessary. As a result, SDG wireless networks must be capable of integrating heterogeneous wireless networks. Furthermore, in an SDG there exist PLCs that shall be utilized as much as possible, particularly to enhance reliability and security. As pointed out in wired communications can be easily integrated into WMNs
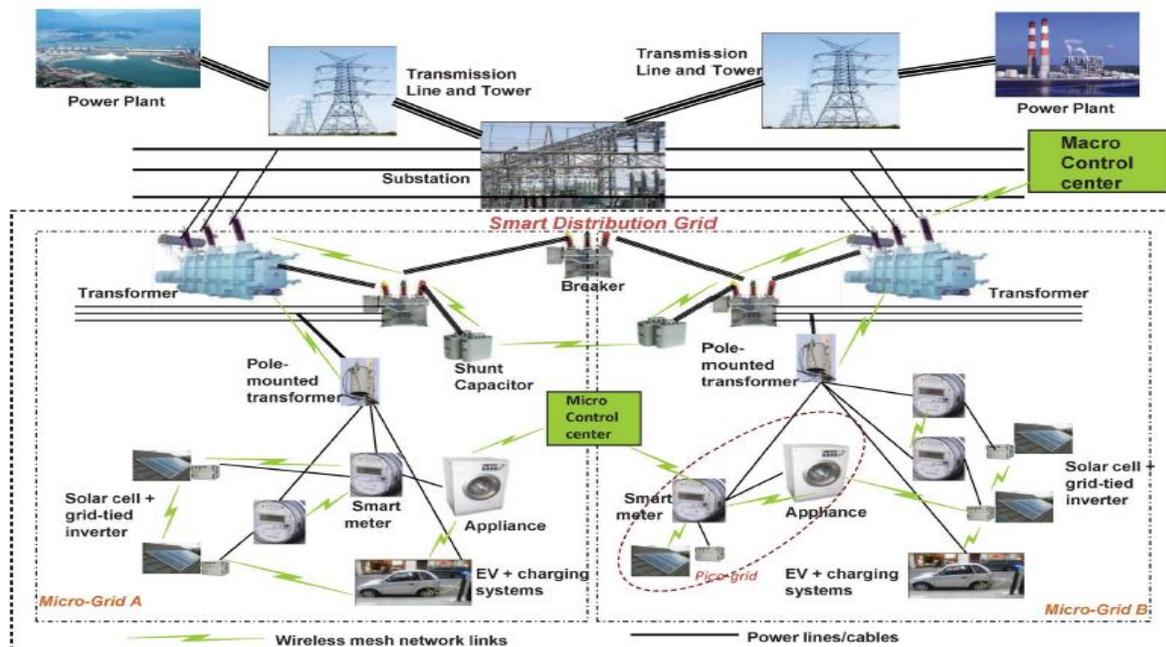

Fig. 1: Wireless communication architecture based on WMNs in smart distribution grid.

Although a cellular network like 3G can provide satisfying rate-distance performance, its network capacity may not be enough to allow SDG wireless communications as an additional service, because emerging cell phone services are currently overloading 3G networks. Moreover, coupling power supply services with telecom services downgrades reliability and complicates management of an SDG. In contrast, a wireless mesh network (WMN) does not have the afore-mentioned issues. It can be deployed and managed proprietarily by a utility company. In addition, the mesh networking capability of WMNs provides more flexible interconnection among various electric devices than a cellular network can do.

1. Wireless Mesh Network

Wireless Mesh Network (WMN), which is a communication network made up of radio nodes organized in a mesh topology, has emerged as a key technology for next-generation wireless networking. A WMN also provides basic networking infrastructure for the communication in SG. WMNs can easily integrate heterogeneous networks to fulfill different functions such as sensing, monitoring, data collection, control, pricing and so on. The system architecture that merges WMNs and power distribution networks depicted in Fig.1. An SDG below the level of substations consists of multiple Microgrids.
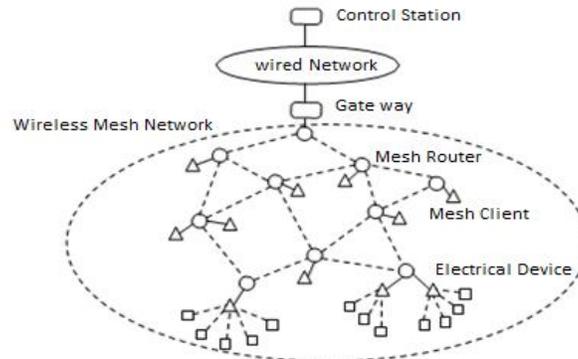
Fig 2: Wireless Mesh Network Model

Typically , a Microgrid managed by a micro control center, contains a few Picogrids. A Picogrid is usually formed by electric devices in a home or building, and it may also include some distributed energy sources like EVs or Solar Cells. Some of the benefits of using WMNs in SG are highlighted as follows:

(i)Increased communication reliability and automatic net- work connectivity.

(ii) Large coverage and high data rate.

III.   PROPOSED SYSTEM

Proposed system contains a healthy system made by 50 nodes based on AODV protocol with energy level and performance comparison of various protocol with different number of nodes are done by using NS2.

NS2 → Network simulator version2

Network simulator is a package of tools that simulates behavior of system/network. To predict the system behavior following step are followed:

- Create system/network Topologies.
- Log events that happen under ant load.
- Analyze events to understand the system/network behavior.

AODV: Ad hoc On-Demand Distance Vector

A routing protocol for ad hoc mobile networks with large numbers of mobile nodes. The protocol's algorithm creates routes between nodes only when the routes are requested by the sources nodes, giving the network the flexibility to allow nodes to enter and leave the network at will. Routes remain active only as long as data packets are travelling along the paths from the source to the destination. When the source stops sending packets. The path will time out and close.

Protocols are of different types they are AODV, DSDV, DSR. The performance of a protocols are found by comparing throughput, packet deliver ratio(PDR) and time delay of a system designed based on the various protocol.

Protocol	Number of Nodes	Throughput (Kbps)	Delay (ms)	Packet Delivery Ratio
AODV	50	547.81	123.5	99.80
DSDV	50	320.35	147.9	96.28
DSR	50	466.19	160.3	95.78

Table 1: Comparison of Protocol
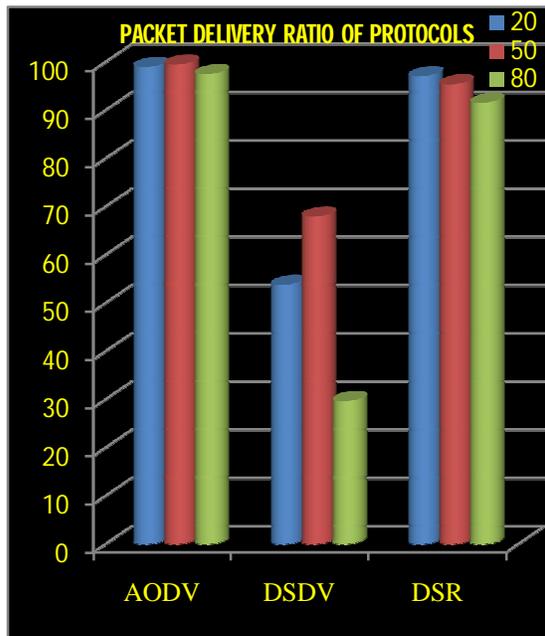
Fig 3: Comparison of protocol among

different number of nodes
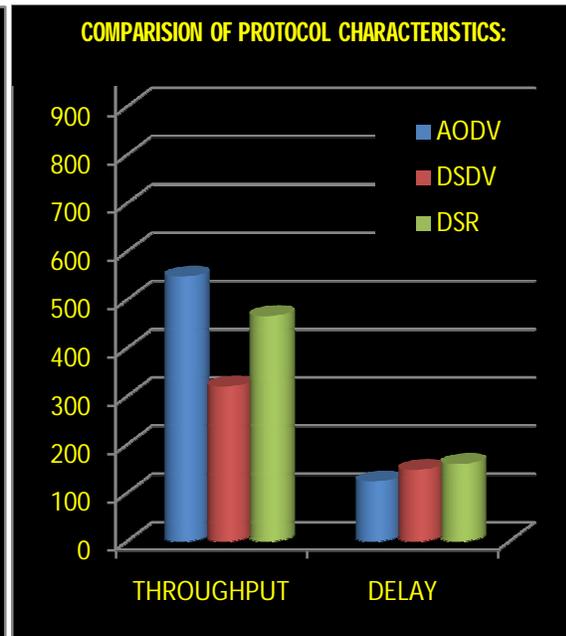
Fig 4: Comparison of protocol

Characteristics

From Table1, Fig 3 and Fig 4 it clearly explains that the AODV Protocol shows better performance among all protocols. It's having good throughput and high packet delivery ratio with low time delay. So, AODV protocol is chosen for creating system. Best system performance is also depends on the energy level of nodes. Normally, a node contains energy and it decreases while continuously sending the information from a node to another node.

The energy dropping can be noticed by color change. Each and every color intimating the energy level of node. Before, communication starts all the nodes are in green color which indicates that nodes are having full energy (i.e.,) 100%. Once, the communication happened the nodes are send data to one another. During, the communication because of continuous sending of information leads to energy level gets fall then the green color changes into yellow, red and black for further.

(i)Green → 100%

(ii)Yellow → 50%

(iii)Red → 20%

(iv)Black → 0%

The Output of proposed system is taken from the Nam. Nam is a Network Animator. A visual aid showing how the information travels in the system.

1.   Healthy System:
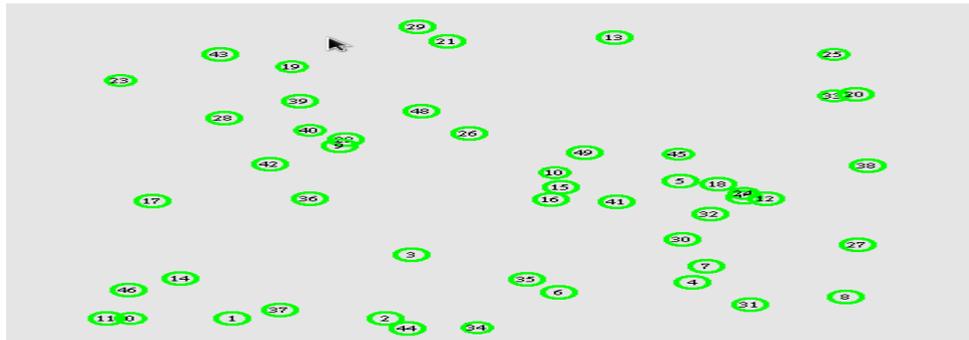
Fig 4: Healthy system with 50 nodes

A System without any problem is termed as Healthy system. Here, a Healthy system made by 50 nodes based on AODV protocol is shown in Fig 4.Here node0 is base station, it is a stable node. Where all data are send and receive. Except node0 all other nodes are utilities (i.e.,) customer, these nodes are mobile node.

At initial condition all nodes are in green color. Because, before the communication begins nodes are have full energy. As mentioned before green color indicates the full energy (i.e.,) energy level is 100%.

2. Commuinication among Nodes:
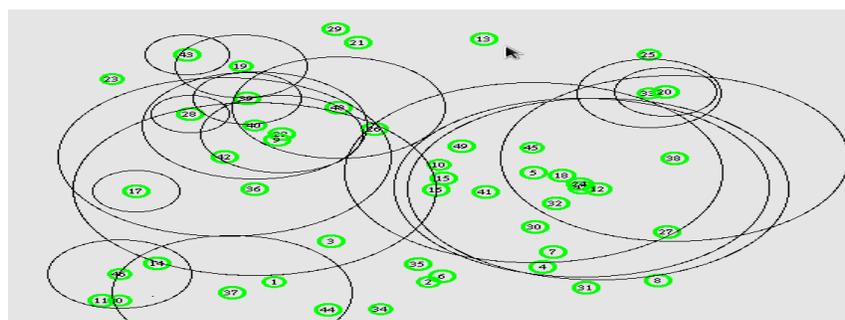
Fig 5: Nodes Communication

The communication begins among all 50 nodes which are connected based on WMN I shown in Fig 5. Times were set in the script. As per the script when the time reaches nodes will start the communication.

3. Exchanging of information:
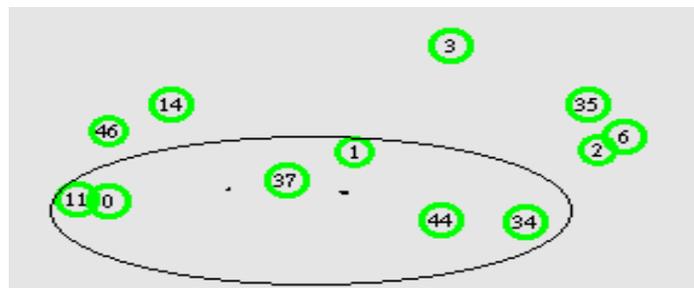
Fig 6: Information Exchanged

Fig 6 explains the data transferring between the nodes. For motion of mobile nodes, time was set in script itself. When the time reached all mobile nodes starts to move and then the data exchange among the nodes will begin. It exchanges information of Voltage, current, power demand and utilization. From the above figure it's clearly shows the data are transferring from mobile nodes (customers) to stable node say node0 (base station)

4. Drains of Energy:

Fig 7: Dropping of energy level green to yellow
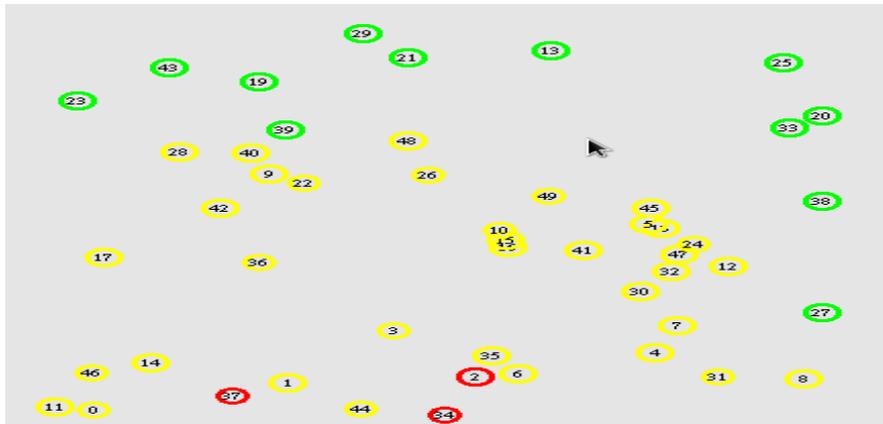
Fig 8: Dropping of energy level yellow to red

Both Fig 7 and Fig 8 Explains the energy dropping on nodes. Due, to the movement of nodes and continuous exchange of data among nodes leads to dropping of energy. Continuous exchange of information nodes with Green color falls into Yellow color is intimates that the energy levels of nodes are drops from 100% to 50% and further continuation the nodes with yellow color changed into red color is intimates that the energy levels of nodes are drops beyond from 50% to 20%.

The performance of system is showed in a graph below.
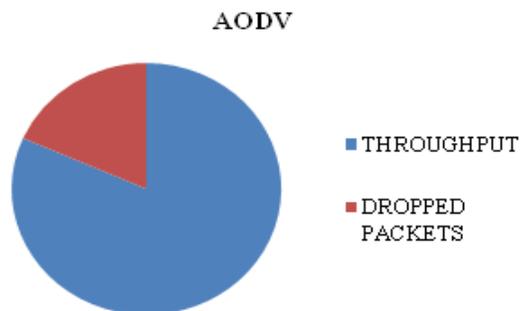
Fig 9: System Performance

Because of using AODV protocol the range information dropping get reduced and throughput of a system increased. Due to these reasons the performance of system is also increased.

IV.   CONCLUSION

A Healthy system has been created with 50 nodes. To identify the faults occurring in the system, a communication has been created among each nodes by using WMN with energy level. The proposed system is analyzed with the best protocol to provide a appreciable solution with Throughput, Packet Delivery Ratio and Delay.

Even though the Smart Grid system is stable always there are some chances for faults resulting in Blackhole. So, this work is further taken over to remove the malicious node. Finally a comparative study is provide for a secured system and un healthy system.

REFERENCE

[1]   Security Framework for Wireless Communiation in Smart Distribution Grid (Xudong Wang, Senior member , IEEE , and Ping Yi).
[2]   Wireless Sensors Network in Smart Grid: applications and Issues (Yiying Zhang and Yan Zhen).
[3]   Securing Smart Grid: Cyber Attacks, Countermeasures, and Challenges (XU Li, Inria Lille-Nord Europe, Xiaohui Liang, Rongxing Lu, and Xuemin shen, University of Waterloo).
[4]   Communication Security for Smart Grid Distribution Networks (Elias Bou-Hard. Claude Fachkha, Makan Pourzandi, Mourad Debbabi, and Chandi Assi, Concordia University).
[5]   NIST Smart Grid Cyber Security Working Group, " Guidelines For Smart Grid Cyber Security: Vol.3, Supportive analyses and references" NISTIR 7628, Aug.2010.
[6]   Y.Zhang and W.Lee, " Intrusion detection techniques for Mobile Wireless Networks" Mobile Netw. Appl.,Vol.9, no.5, pp. 545-556, 2003.