http:d2cigre.org

CONSEIL INTERNATIONAL DES GRANDS RESEAUX ELECTRIQUES
INTERNATIONAL COUNCIL ON LARGE ELECTRIC SYSTEMS

STUDY COMMITTEE D2
INFORMATION SYSTEMS AND TELECOMMUNICATION

2013 Colloquium
November 13-15, 2013
Mysore – KARNATAKA - INDIA

D2-01_18

ADAPTABILITY OF WIRELESS SENSOR NETWORK FOR INTEGRATING SMART GRID ELEMENTS IN DISTRIBUTION SYSTEM

by

Mrityunjai Tiwari*, Sasi SR Kumar, Sukumara T

ABB Global Industries and Services Ltd

(IN)

SUMMARY

The power system network comprises of generation, transmission and distribution segment where the communication network must co-exist with the power network to allow reliable flow of information. In smart grid application, the distribution segment IEDs [Intelligent Electronic Devices], RMUs [Ring Main Units] and Smart meters will require exchange of information such as Trend, system parameters, Diagnostic/Prognostic information, energy reading, load shedding/balancing commands etc. using protocols such as Modbus, DNP, IEC61850.

DERs [Distributed Energy Resources] and distribution automation devices are located geographically apart and interconnecting them through wired communication becomes tedious when considering maintenance, operational ease, future expansion etc. These difficulties can be overcome by adapting wireless technologies in this area. Various factors such as latency, network coverage, power consumption, immunity to interference, security, reliability, availability are the major challenges to wireless communication when it is adapted to the power system automation.

A prototyping pre-study that is presented in the paper focusses on various wireless communication technologies such as Zigbee [9], Bluetooth, 6LoWPAN, Wi-Fi, GSM, GPRS, UMTS, EDGE and RF and their adaptability challenges in Power System Automation which is an integral part of Smart Grid.

The paper emphasizes on our experimental results of WSN (Wireless Sensor Network) based on mesh topology and protocol stacks that can fit on the WSN physical layer framework, thereby enabling features such as self-healing, automatic role assignment, selection of frequency band which has least congestion, etc. The prototype setup simulated mesh topology based WSN consisting four Modbus slaves devices and a master device. The WSN nodes are microcontrollers with IEEE 802.5.14 interface running Modbus application on proprietary WSN stack, which can support up to 500 nodes per network and supporting 80-90 kbps bandwidth. The Modbus master and slave devices self-configure themselves as end or

* Mrityunjai Tiwari, ABB Global Industries and Services Ltd, Bhoruka Tech Park, W3-71C, Mahadevapura, Whitefield Road, Bangalore – 560 048, Karnataka, India.
Fax: + 91 80 6757 9999 e-mail: mrityunjai.tiwari@in.abb.com

coordinator nodes while forming the network and thereby ensuring continuous communication. The Modbus application running in Modbus Master Node, can open/close a switch as well as change an analog value such as a counter in any of the four slave nodes. It can also read energy meter information. The above application was tested for data latency for a given amount of data length, network range in a given terrain condition by checking the 'Packet Error Rate'(PER), ability and time taken by an isolated node to re-join the WSN. The Modbus application was chosen as an exemplary messaging format for the setup, It is possible to use other power system protocols such as IEC 60870-5-101, IEC 61850-8-1 (GOOSE) as well.

The setup was subjected to different scenarios to measure the connectivity and network coverage performance. Owing to reflections, closed areas such as within building resulted in shorter range (~300m) between two nodes when compared to the open field (~1200m). The power consumption, being an important parameter for self-powered system, was measured for different terrain conditions. The typical current consumption by the end/coordinator node is close to 30-34 mA at 3.7 volts for all types of terrain irrespective of the distance between two nodes. It is quite evident from the pre-study results that WSN is the most preferable technology in meeting the smart grid objectives.

KEYWORDS

Co-existence, congestion, deployment strategy, GOOSE, Home Area Network, Neighbourhood Area Network , key, Packet Error Rate, PAN ID, PER, Power consumption, Self-Healing, Smart Grid, Wide Area Network, Wireless Sensor Network

* Mrityunjai Tiwari, ABB Global Industries and Services Ltd, Bhoruka Tech Park, W3-71C, Mahadevapura, Whitefield Road, Bangalore – 560 048, Karnataka, India.
Fax: + 91 80 6757 9999 e-mail: mrityunjai.tiwari@in.abb.com

1. INTRODUCTION

The distribution segment in the power system has two logical divisions commonly known as primary and secondary distribution segments. The secondary distribution segment includes residential, and industrial loads. Some of the applications in this segment are load balancing & shedding, prognosis & diagnosis and energy monitoring of the power system equipment. Today these applications require some degree of human intervention. With the smart grid concepts these applications become fully automated and decentralized. For example, the load shedding concept today is for the whole outgoing feeder which can be localized to individual loads. It means that the individual residence or industry, even the individual loads can participate in the load balancing activity.

The decentralized intelligence in distribution automation segment can be realized through the help of Intelligent Electronic Devices with communication capability. These devices can network with each other for long range data communication, exchange situational awareness information and settings/parameters for realizing redundancy solutions etc. The communication technology applicable can be wireless by considering the geographical distance between these devices in the distribution automation segment.

Nowadays, wireless sensor network are getting widespread momentum in power system applications. Popular WSN technologies include WirelessHART, ZigBee, 6LoWPAN. An advantage of all of these WSN technologies from the point of view of scalability, futuristic migration towards a better technology is that they are using the common physical layer specification, i.e., IEEE 802.14.5. The network and data link layers of these protocol stacks primarily focus on network management functionalities such as maximum number of nodes, topology, network formation, self-healing mechanisms [9] and link management functions such as reliability, data integrity and security aspects of the wireless network respectively.

Network communication factors like latency, network coverage, power consumption, immunity to interference, security, reliability, availability, Internet of Things (IoT) abilities are the most important criteria for selecting the suitable WSN technology for distribution automation applications.

This paper presents the study of present deployment scheme of an electrical equipment that together with a few other devices acts as a node in the communication network. This paper also evaluates the performance of various WSN technologies against the above mentioned criteria . It presents the possibilities of adapting wireless sensor networking concepts for realizing effective integration of power system elements in secondary distribution for smart grid applications.

2. USE CASE FOR INTEGRATING SECONDARY DISTRIBUTION SEGMENT USING WSN TECHNOLOGY

Following are the two use cases that best suit the study of adapting wireless sensor network technology for integrating electrical network elements in the distribution segment.

2.1. Commercial Areas in Urban Environment

Commercial areas in a city have numerous industries, shopping and entertainment complex, etc., that are installed with Ring Main Units (RMUs) at their location. The RMU consists of switches/isolators/circuit breakers, fault indicator, protection and metering units [4]. An RMU typically has two 11KV incoming switches and one outgoing feeder breaker with a step down transformer for local use. The two switches of various RMUs are interconnected to form a ring network and ultimately connected to a main power source. Typically the distance between two RMUs in commercial areas would be approximately 100 meters.

The status information from each RMUs help identifying the load pattern, instantaneous power quality at the commercial complex along with the prognosis/diagnosis information pertaining to the local electrical equipment. It is also possible to island the fault by analysing the fault indicator status of all RMUs.

The way the information are integrated and handled at the central location determines the effective operation of the corresponding power network. Integrating the RMUs communicably using WSN technology results in advantages like two-way, lower power, low cost, scalable communication network. The reliability of the data integrated into central location is also achieved through the self- healing property [9] of the network together with the security mechanisms.

The experiment conducted as a part of the study as explained in the subsequent section analyses the feasibility of adapting such an advantageous WSN technology to this use case.

2.2. Residential Areas In Urban Environment

In the current arrangement of the RMUs in the residential areas of a city, the typical distance between two RMUs is uniform and close to 400-450 m in a planned city having proper sectorial bifurcations. The same may be non-uniform and may vary from 100 to 300 m in a city with lesser planned architecture.

The elements in RMU can provide information such as instantaneous load pattern, need for load balancing, electricity metering data for billing [4], etc., corresponding to the residential area. Integrating this information with the central station would lead to efficient energy management and many a smart grid applications.

Similarly information about the energy generation levels of nodes having renewable energy generation capability can be communicated to a decentralized decision maker. Depending upon the information, load balancing for the cluster can be executed. Information about abnormally high usage of energy at particular node can be communicated to decentralized monitoring system which can further trigger a solicited alarm to different nodes involved. Such alarms can intimate the consumer about the energy usage and also in many cases detect illegal energy theft scenarios.

The potential technologies for communicably integrating electrical equipment are WLAN and WSN. The integration of above said elements communicably involve the establishment of three communication network segments mainly Home Area Network(HAN), Neighbourhood area network(NAN) and Wide Area Network(WAN). The HAN will involve the establishment of smart meters in houses of a building. Each HAN may cover about 10-30 houses that come within the range of 30-40 m.

Further, multiple HANs shall communicate with each other through NAN. An exemplary use case of NAN will be in areas where many housing societies each having 100-150 houses are separated by a distance of 100-300 meters. In such cases the NAN will be the parent network for HAN and will gather various power measurements and billing information from the various HANs.

A city may have various NANs and all these NAN shall be a part of city wide network WAN. The nodes in WAN will be the coordinator of each NAN. These nodes when geographically placed at a uniform distance will act as a gateway to various NANs and thus HANs. The information from the elementary nodes in HAN may thus reach the nodes in WAN which can further be used for electrical billing, individual load balancing, fault detection and restoration.

3. EXPERIMENTAL SETUP FOR STUDYING THE PERFORMANCE OF WSN TECHNOLOGY

From the theoretical analysis of the features of various WSN technologies and the list of requirements for wireless technologies for their use in secondary distribution application, we found ZigBee and another proprietary WSN stack are the potential candidates for our experimental network. We eventually selected the proprietary WSN stack for our work.

The experimental setup for verifying the suitability of the WSN stack for smart grid elements in distribution automation segment consists of four protection relays, a SCADA system for acquiring data from these relays, WSN evaluation boards with proprietary WSN module & an IEEE 802.15.4 transceiver. Each of the protection devices and SCADA system interface with the WSN evaluation boards through external serial link. Thus the devices under experiment get the wireless capability. The experimental setup, shown in Figure 1, aims at successful information exchange between the protection devices and SCADA system on the WSN. The experiment setup uses Modbus Protocol over WSN frame for information exchange.

The WSN stack allows three types of roles and each of the elements in the distribution segment can be assigned with a specific role. The Coordinator performs various jobs such as selection of radio channel, network initialization, etc. The Router relays the message from one node to another. The End node essentially picks up the data from the transducer and sensor and then sends it to the intended receiver in the network via router.

In the experimental setup, as shown in Figure 1, SCADA system acts as WSN coordinator responsible for establishing the network. The protection devices can be either router or end devices. The devices with router role relay the information between source and destination, for example, relaying information from protection device to SCADA system & vice versa. Besides it can also act as end devices interacting with the coordinator.

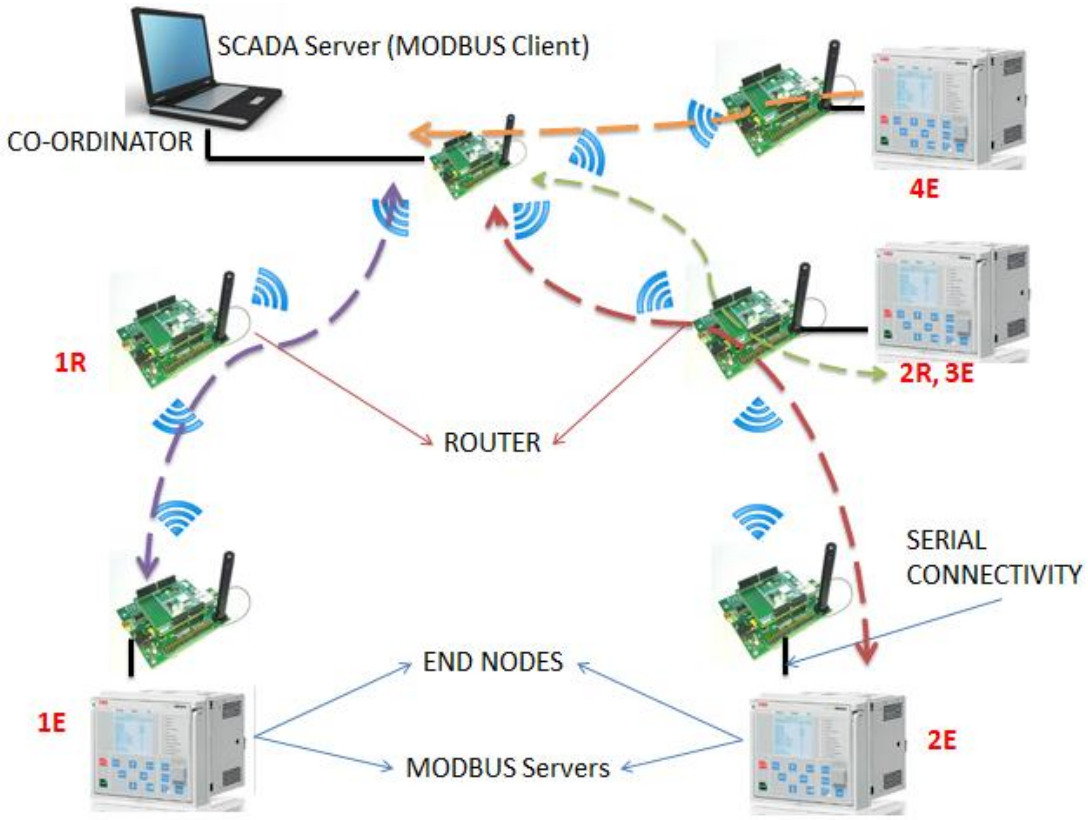

Figure 1: Experimental setup

3.1. Experimental WSN Formation

The network formation is initiated by the coordinator, i.e., SCADA system, once it is powered on. After selecting an operating frequency with least congestion [9], the coordinator sets up the network. After the network has been established the end nodes (i.e., protection devices) and the routers (i.e, protection device and/or WSN router) power on. The routers and the end nodes search for the available network bandwidth in which they can operate. Once the network's operational frequency is detected by the end node or the router, it tries to connect to the coordinator. After a successful connection is established, a unique ID is given to the network elements through which they communicate.

The network topology deployed has been indicated in Figure 1. The Modbus Master/Client (i.e, SCADA system) polls the specific Modbus slave for the measurement data. The respective protection devices present in the setup responds with the live measurement information such as phase current, phase angles and phase voltages. The Modbus frame serves as the payload for the WSN frame of size 127 bytes which was transmitted wirelessly to the SCADA system via respective parent WSN routers.

3.2. Experimentation on Network Coverage

One of the methods to evaluate the network coverage feature in WSN is calculating the Packet Error Rate (PER) at every unit of distances. PER is the ratio of the number of incorrectly received data packets to the total number of received packets. A PER of 100% signifies no frame reception and that of 0% signifies perfect frame reception.

The experimental setup was placed in a 500x300 meter open field surrounded by trees and buildings. Referring to Figure 1, the router 2R performs the role of both router and MODBUS slave. It acts as a parent router for End node 2E and also serves in the capacity of an End Node (3E) in which it acts as a MODBUS slave. The distance between the Routers 1R, 2R and the coordinator was about 100 meters. The distance between the parent router 1R and its child end node 1E was fixed at 100 m. For measuring the change in PER with reference to the distance between link partners, the distance between the router 2R and end node 2E was changed from 40 meter to 200 meter. The End Node 4E serves the role of MODBUS slave communicating directly with the Modbus master (i.e, coordinator).

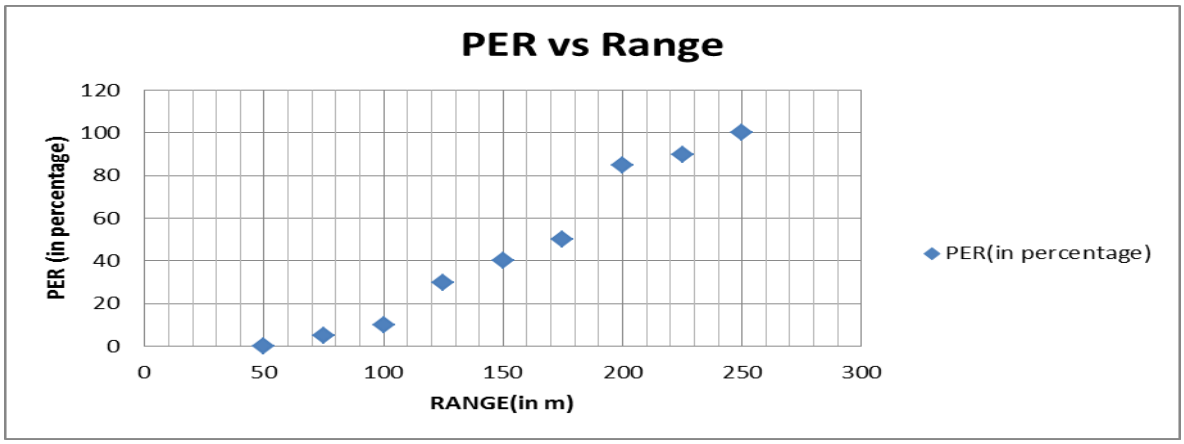

Figure 2: PER vs Range

As shown in Figure. 2, as the distance between the end- node and the router increases, the PER also increases to a point when it reaches 100% indicating complete frame loss. It is evident from the result that the maximum distance between any two nodes of the WSN under experiment is approximately 200 m. Thus deploying WSN node within every 200 m of distribution segment it would be possible to create a cluster of decentralized intelligence.

3.3. Experimentation on Self-Healing Network Characteristic

The self-healing characteristic of WSN is a notable feature for the integration of smart grid elements. In the above said experimental setup, the self-healing characteristics of the WSN are verified by switching a router node off and observing the network reconfiguration. Referring to Figure 3, one of the routers, for example, 2R was intentionally pulled out of the network by switching it off. In such arrangement, the experimental WSN responded by auto reconfiguring the network. End node 2E was assigned a new parent 1R through which the transmission of the data continued even after removal of 2R. An important aspect that should be considered while engineering the WSN is that the new parent node must exist within the reach of isolated node because of the router failure.

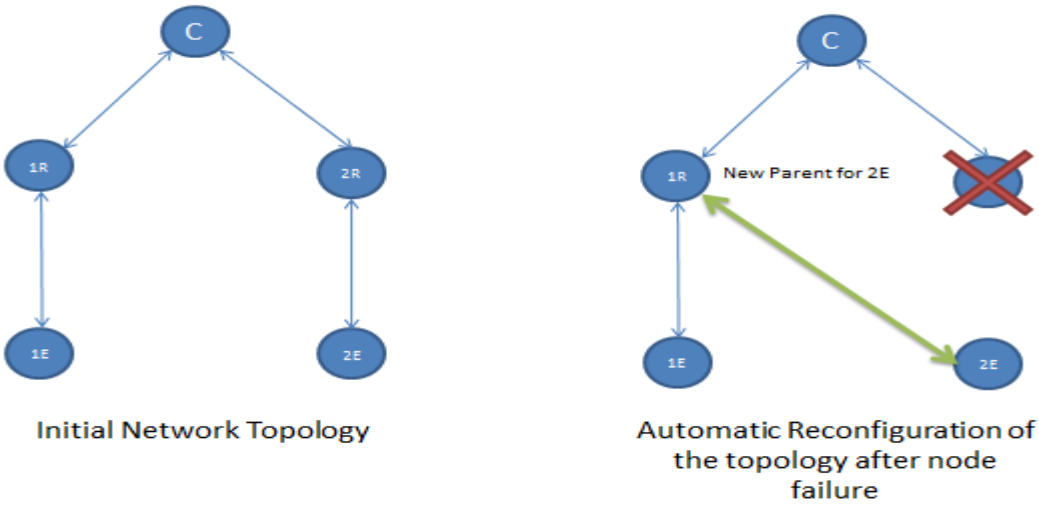

Figure 3: Experimental setup for evaluating Self- healing of WSN

Thus the auto-healing feature of WSN technology best suits the requirements of smart grid elements integration.

3.4. Experimentation on Range and Power Consumption

Power consumption of each WSN node is an important aspect while building WSN. In the experiment, the power consumption of WSN nodes is optimized by forcing the nodes to sleep mode and waking them up when needed [8][5]. The sequence of optimization steps are shown in Figure 4

Figure 4 Steps involved in data transmission from end node

The power consumption was calculated for the end node at various instances of the data acquisition and transmission cycle. The power consumption with the optimization enabled at the node level resulted in significant energy conservation as shown in Figure 5

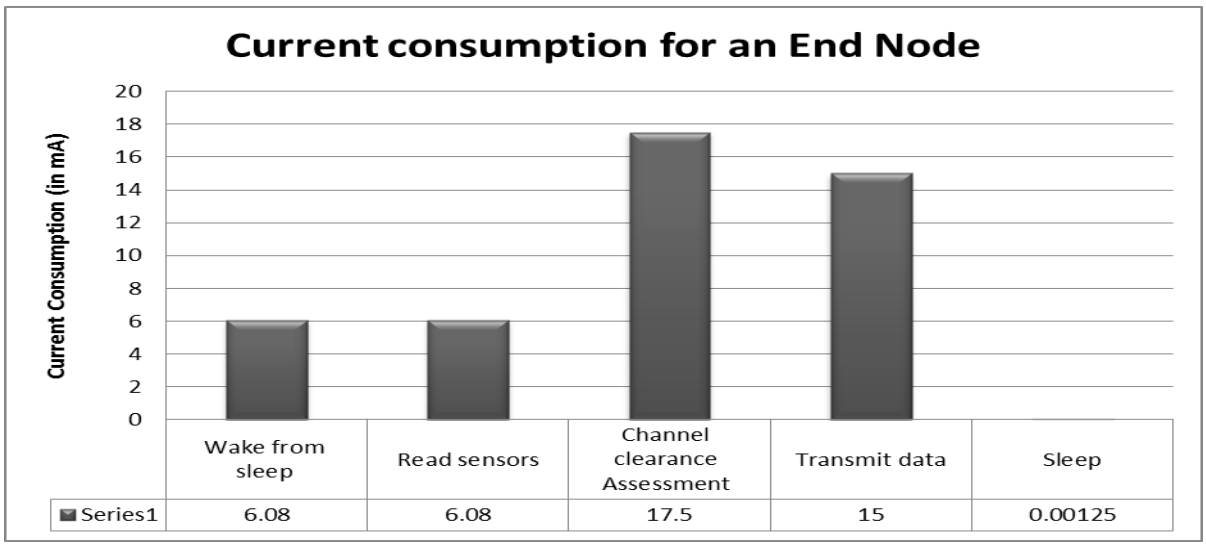

Figure 5: Current consumption at various instances in an end node [10]

The low power consumption of the end node signifies an increased battery life of the battery powering up the end nodes [9]. Many DA network applications require an end node to periodically publish prognostic information of the system or send an alarm when a particular event occurs. In such an arrangement, the end nodes sleep for majority of the time and wake only when they are scheduled to or when they data is explicitly requested from them [8][5]. Low power consumption of the end nodes will save the charge of the power source it is connected to and last longer on the same power source even if the battery is not recharged periodically [9].

Results of an experiment where the range of proprietary WSN stack for different transmit power is mentioned in Table 1.

Transmit power(mW)	Observed Indoor Range(m)	Observed Outdoor Range(m)
396	80-90	150-300
61.2	30-35	100-125
36	10-15	40-45

Table 1: Measured power consumption and range for a WSN

3.5. Experimentation on Co-Existence and Data Integrity

Distribution Automation devices are prone to many interferences from the external world as the same are subject to different types of Electro Magnetic(EM) waves and noises. Coexistence is the capability of a network to exist along with another network which is operating in a close vicinity to it [2].

The following experiment evaluates the coexistence capability and the data integrity WSN technology. The experimental setup consists of two networks of proprietary WSN that are operational within the same geographical location and the same operating frequency but different PAN IDs. Each network consists of a SCADA system (MODBUS master) which requests the data from the end nodes (Modbus slaves). Refer to figure 6, the adjacent positioning of the coordinators of network A and B and minimum distance between the end nodes EA1, EB1, EA2, EB2 and the router RA, RB ensures maximum inter network interference.

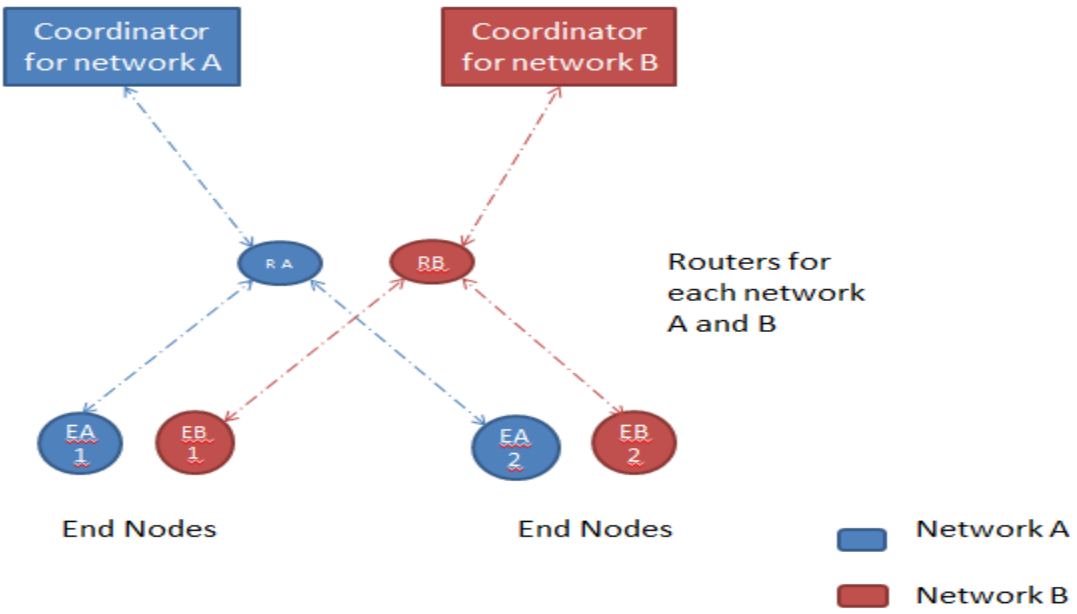

Figure 6: Experimental setup for evaluating Coexistence in WSN networks

The PER for each of the network elements remained Zero percentage even after increasing or decreasing the distance (from 20 to 50 m)between the networks and isolating them. The PER of Zero percentage for any distance between the elements of the different network provides substantial evidence for the stable data integrity of WSN. The stable PER of Zero percentage is a must for DA networks as this ensures that the data within one network is immune to interferences from the other networks operating in the same frequency range.

3.6. Experimentation on Security

For devices in electrical network, security is one of the most important criteria that a product must satisfy. The DA devices operate in areas which are more prone to intrusion, hacking and face substantial amount of threats from the external world. In case of wireless network, the possibility of attack further increases as it is easier to gain access to a wireless network than compared to a wired network.

Following experiment evaluates the security features of WSN. Refer to figure 7, the experimental setup consists of a Coordinator, two routers A and B and an End Node E. The distance between the end node E and A is less than the distance between E and router B. If a network element tries to join a WSN network it must first obtain the PAN ID that the networks coordinator assigns to the network.

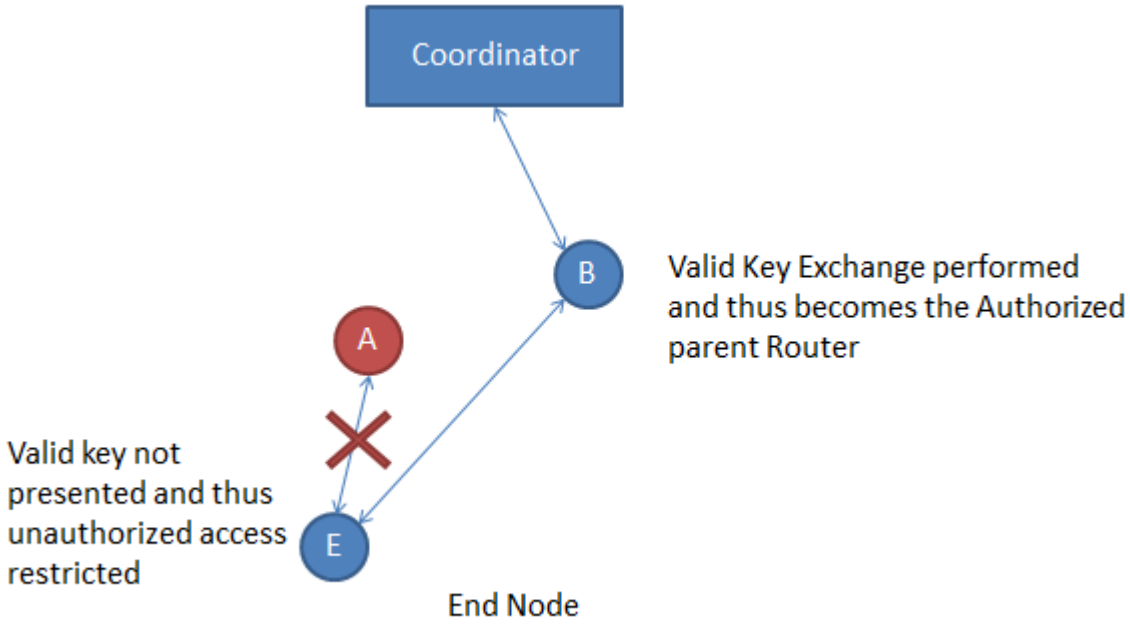

Figure 7: Experimental setup for evaluating Security in WSN

The WSN chosen for the experiment provides security features wherein the Coordinator assigns a valid PAN ID only to specific nodes whose Mac address are registered in its hash table. This ensures a first level security. In case an intrusion occurs when an end node with a registered MAC address tries to retrieve information which it is not supposed to, then WSN utilises its second level security feature of key exchange.

In the experiment conducted, unauthorised access was attempted by a router A which was in a closer vicinity to the end node and offered the end node E with a higher and better signal strength. Once the end node detected that the key exchanged by the router A was not an authentic key, it triggered an alarm throughout the system declaring an unauthorised access and also ensured that no data was exchanged with this unauthorised router. The end node continued its data exchange with the coordinator through an authorised router B even though its distance was more than that of unauthorised router.

From the experimental findings it is evident that a network protocol stack with features to block an unauthorized access to its network serves as a preferred candidate for wireless network application in DA domain.

4. ANALYSIS OF SUITABILITY OF WSN TECHNOLOGY FOR INTEGRATING SECONDARY DISTRIBUTION SEGMENT USE CASES

Following points detail the suitability of WSN technology based on the experiment findings **from** section 3 for the secondary distribution segment scenarios explained in section 2.

4.1. Range

The experimental results indicate that it is possible to use WSN technology for forming Home Area Network thereby integrating the electrical network data in an urban residential

environment. The high power WSN module can even be used for forming NAN whose spread is about a kilometre.

In WAN context, the distance between the coordinator of the two WANs may range from 300- to 2000 m. In cases where the distance between the coordinators of two networks is maximum, high power antennas are required to transmit the signals.

It is suggested to adapt high power antennas and various algorithms strategies which are commonly used in GSM networks deployment by the EC teams [7][1] to increase the communication range between any two nodes in WSN. Another deployment strategy may be the placement of high power antennas at the top of tall buildings to increase the line of sight range. Deployment strategy may include antenna selection scheme. An example of the same is the use of beam-forming antenna or switched antennas instead of fixed or directional antenna. These antennas need not be aligned manually every time but can be done electronically [6].

4.2. Security

Almost all the WSN technologies support strong security algorithms such as 128 bit AES, which make them suitable for applications such as integrating the secondary distribution network elements listed in the use cases. For IP based networks firewall implementation is possible. In order to provide greater level of security, IPsec VPNs can be used. Firewall implementation is also possible in WSN stacks [6].

4.3. Interference

The findings of the experiment on the coexistence aspects show that the IEEE 802.15 devices can coexist. However noise or impulse of high voltage/frequency could causes data corruption [2].

The obvious solution for this is to place the transmitters in an area with lowest possible noise level. For special case nodes, WSN may be coupled with optic fibre. For example, point A may have high noise level. It may be possible to keep the sensor at that location, send the signal through an optic fibre to another point B having lesser noise,where a wireless transmitter can be provide to transmit the signal to other points in the communication network.

It is suggested to implement a mechanism in each node that continuously measures the PER for the communication link connecting it with its parent node. If the PER exceeds a threshold value then it is suggested that the mechanism initiate a topology change.

Another solution is to operate in high frequency range [6][3]. However it would result in short range and increase the need for repeaters.

4.4. Power Consumption

Low power consumption nodes are available in WSN which go in a sleep mode when their operation is not required [8][5]. This saves a lot of battery life. Anyhow a deployment strategy may include battery powered operation WSN router and gateways with battery life of 1 year, which are available in market.

4.5. Capacity

This involves a number of nodes that can be present in a network. The deployment scheme must ensure that network is capable of supporting high number of nodes.

The scheme must estimate the deployment pattern by keeping in mind various factors such as the proportion of nodes functional at a time and maximum number of nodes that can be added in next 5 years [6].

4.6. Two Way Communication

The WSN must be capable of supporting full-duplex communication [6]. Full-duplex communication is an important requirement for transmitting measurement data to SCADA system and receiving commands from it. Though it's possible to use air as a full duplex medium, at the moment none of the WSN technologies support it.

4.7 Network Latency

In a mesh network, the data is transmitted from an end device to coordinator most of the time through routers. Thus data hops through multiple devices on its way to destination. This adds to the data latency. Each device in the network generates, transmits data to its destination. This in turn increases the data latency as the career must be detected before a node can begin transmission. This also increases the amount of data flowing in the channel at any given time. This paper proposes a data aggregation concept addressing the above issue.

Consider a wireless mesh network consisting of "N" nodes. For an end node to transmit the data to the destination, it must send the data to its parent router which further sends the data to destination node. A router having more than one child nodes can utilize the data aggregation concept to reduce the overall latency of the network. The proposed algorithm is based on the following parameters

a. Information type (i.e., periodic/aperiodic, real-time/non-real time)
b. The transmission intervals of periodic messages
c. Hop count (i.e., Number of routers in a given data path)
d. End-to-end message transmission delay
e. Residence time at receiver (i.e., time to decode message from descendent and encode a aggregated message)
f. Path Cost (i.e., Link delay between source and destination/parent)
g. Last link delay (transmission delay between the destination and it's immediate parent)

A parent router may have a table detailing the number of child nodes and the information about the above mentioned parameters (a) through (g) for each node.

Based on the number of child nodes and the criticality of the data to be transferred the following mathematical formula can provide the maximum number of packets that a parent router can aggregate (combine them in one packet) and send to the respective destination.

Formula

Eqn 1 $$(X) + (Y) + P_{TD} < \mathrm{T}$$

Where,

Eqn 2 $$(Y) = UP_c$$

Eqn 3 $$(X) = \sum_{j=1}^{M} \{ \sum_{p=1}^{Z} PTR_p + \sum_{i=1}^{N} PC_i \}$$

T= Total time for the data to reach the destination
PC_i = Path cost for i^{th} node
PTR_p= Residence time of a router for p^{th} packet
M= Total number of Routers
$UP_{c=}$ Uplink path cost between the destination and its immediate parent node.
PT_d= Time for processing the packet at the destination
Z= Total number of packets for aggregation at a router
N= Number of nodes the data has to travel through to reach the destination.

Using equation number 1, the maximum number of child node packets (N) that a router can aggregate and send can be found out such that the LHS is less than the RHS. With the resultant value of "p", latency of the network can be reduced. The respective value for p can be registered for respective router at the time of network initiation.

5. FUTURE WORK

Dynamically adjusting the antenna gain and employing array of directional antenna to cover as large geographical area as possible. This way power consumption is dynamically adjusted. The directional antenna demonstrates high directivity in a specific direction, very less radiating power on the sides. At the time of joining the network, a node shall identify the nodes in its vicinity; gather relative positions of nodes visible, radiation strength, etc., by exchanging handshake messages and measuring the PER. This information helps each node to identify the deployment of other nodes in its vicinity. It can then adjust the radiating pattern dynamically to establish connection with its link partner as well as optimizing energy usage. For example, a node has children nodes relatively close by, and its parent node comparatively far away. In this case, the node can adjust its radiating power such that the maximum directivity (main lobe) is towards the farthest node and can communicate with the nearest nodes using side lobes. In another embodiment, the size of the main lobe can be adjusted based on the link partner's position determined dynamically. This information helps for choosing the best link partner during network joining and failure recovery by dynamically drawing the relative position of the link partner.

6. CONCLUSION

WSN features comply with various smart grid requirements. WSN provides a network communication framework and can support the implementation of various features such as data aggregation, antenna power adjustments thereby making WSN a potential candidate for future smart grid communication.

BIBLIOGRAPHY

[1] *"RF Power Options in ZigBee™ Solutions"*, white paper, RFM, http://www.rfm.com/products/apnotes/wp_zigbeepoweroptions.pdf

[2] *"ZigBee and Wireless Radio Frequency Coexistence"*, white paper, ZigBee Alliance, June 2007

[3] Babak Karimi, Vinod Namboodiri, Visvakumar Aravinthan, Ward Jewell, *"Feasibility, Challenges, and Performance of Wireless Multi-Hop Routing for Feeder Level Communication in a Smart Grid"*, Wichita State University

[4] David Egan, *"Assessing the Popularity of ZigBee as a two way wireless communications system"*, Ember Corporation & ZigBee Alliance, 17 November 2009

[5] Johan Lönn, Jonas Olsson, *"ZigBee for wireless networking"*, Master Thesis, Linköping University.

[6] *"Wireless WAN for the Smart Grid"*, White paper, Trilliant, http://www.trilliantinc.com/library-files/white-papers/WP-WirelessWANfortheSmartGrid.pdf

[7] K. Shashi Prabh, Chinamy Deshmukh and Shikhar Sachan, *"A Distributed Algorithm for Hexagonal Topology Formation in Wireless Sensor Networks"*, Proceedings of the 14th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), 2009

[8] Dave Blissett, *"ZigBee Wireless Mesh Networking. Basic Concepts and Latest Developments"*, Telegesis (UK) Ltd.

[9] ZigBee Alliance *"ZigBee 2012 Specification 2012"*

[10] "Calculating JN5139/JN5148 Power Consumption", Jennic, 2012