ISSN Application No. 2321-6921

Global Journal of Networks and Applications

Volume No. 11

Issue No. 1

January - April 2023

ENRICHED PUBLICATIONS PVT. LTD

S-9, IInd FLOOR, MLU POCKET,
MANISH ABHINAV PLAZA-II, ABOVE FEDERAL BANK,
PLOT NO-5, SECTOR-5, DWARKA, NEW DELHI, INDIA-110075,
PHONE: - + (91)-(11)-47026006

Global Journal of Networks and Applications

Aims and Scope

Global Journal of Networks and Applications welcomes research contributions, surveys and notes in all areas relating to computer networks and applications thereof. The following list of sample-topics is by no means to be understood as restricting contributions to the topics mentioned:

- New design techniques, interesting or novel applications, components or standards.
- Interface issues including special consideration for handicapped persons.
- Computer graphics, 3-D modeling and virtual reality multi-and hypermedia including electronic publishing and digital libraries.
- Computer networks with tools such as WWW or Hyper wave.
- Emerging standards for internet presentation levels (such as XML) and Internet protocol level, new compression standards for still pictures, movies, audio and vector data, 3-D data and cartographic data.
- Work on metadata and its applications.
- Applications of networked and stand-alone multimedia systems to computer assisted presentations.
- Applications of an educational, transactional and co-operational nature.
- Gateways between databases and security, privacy and societal aspects of network and computer technology.

Global Journal of Networks and Applications

Global Journal of Networks and Applications

(Volume No. 11, Issue No. 1, January - April 2023)

Contents

A Layer-Wise Security Analysis for Internet of Things Network: Challenges and Countermeasures

Arun Kumar Bediya[*], **Dr. Rajendra Kumar**[**]

[*] *Department of computer science, Jamia Millia Islamia university , New Delhi ,India*

[**] *Department of computer science, Jamia Millia Islamia university , New Delhi ,India*

ABSTRACT

Internet of things is a vast domain, still spreading over different areas of the society, with a fast pace. The Connected IoT devices will increase in rapid pace and it is expected to extend up to 20 billion IoT devices till 2020. According to digital security firm Gemalto IoT endpoint spending will reach approximately $3tr by 2020 and has potential togenerate $19tr in next decade. IoT is combination of hardware and software, where Hardware may consists of Sensor nodes, Radio Frequency Identification (RFID), Near Field Communication (NFC) and low energy Bluetooth devices etc. Software provides middleware, information queries, data repository and data retrieval and exchange. All WSN devices turns IoT component when it is supervised using internet and significant security issues happen just when nodes are associated with the internet. This acquires a great deal of concerns identified with the privacy and security, standardization and power management. In this paper we have depicted security issues at various layers of IoT and furthermore outlined security solutions for each layer of IoT.

Keywords: IoT Architecture; IoT Layers; Security Issues in IoT.

1. Introduction

The IoT can be defined as ―an overall system of interconnected objects‖, these object must have

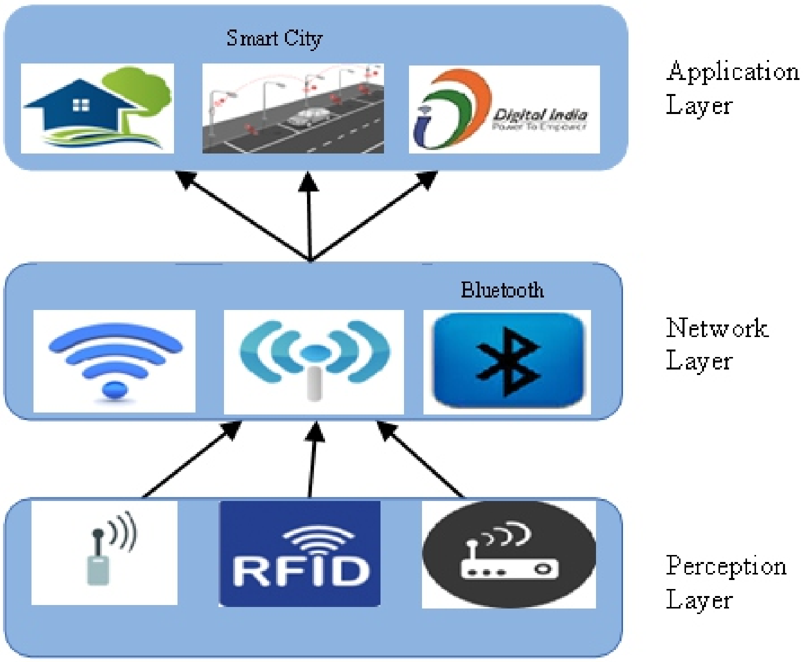
- A unique identity by which can be addressed.
- Can be accessed using internet or smart interface.
- Must be self organized and repairable.

There are numerous application areas of IoT, extending from individual to enterprise environments. IoT has numerous usage areas like agriculture, transportation, health care, production and distribution of energy. IoT devices controlled through identity management i.e. unique identity that has assigned to device, used to distinguish it from collection of homogeneous and heterogeneous devices [1] [2].

In this paper, we give a review of the IoT architecture framework (Section 2), briefly described various security issues at each layer of IoT infrastructure (Section 3), also highlighted the solutions for security issues present at each layer (Section 4), and we described a proposed mechanism to detect threats using machine learning (Section 5), and conclusion of the study (Section 6).

2. IOT ARCHITECTURE

IoT architecture functionality is based on three layers named as Perception Layer or Physical Layer, Network Layer or Middle Layer and Application Layer [3]. Whereas there is distinctive point of view with respect to the quantity the layers in IoT. This paper described three layered architecture with each layer functionality and devices that are used at each layer.



Every layer of IoT additionally has many security issues associated beside it. Fig.1 demonstrates the fundamental three layer architecture system of IoT such as devices and technologies that encompassed in each layer [4] [5] [6].

Many security frameworks have been proposed which analyzing security issues and claim to be used to used for monitoring and analyzing security of the IoT network [7][8][9] [10].

2.1 Perception Layer

In IoT, This is the layer of sensor and sometimes it is also called ―Sensors‖ layer. Basic function of this layer is to detect data, collect it and then processing. After processing information data is transferred to Network Layer. Data is collected from the environment by using sensors and actuators. Node collaboration is also performing on this layer for local network or short-range small networks.

2.2 Network Layer

This layer performs data transmission to different devices over the internet and data routing is also done by this layer. Devices like routing devices, internet gateways, switching devices, cloud computing devices are used at this layer. These devices work on technologies, for example, Wi- Fi, 3G, 4G and Bluetooth and so forth. The network gateway fills in as the intermediary amid various IoT nodes from sensors by combining, filtering, and transmission of information [11].

2.3 Application Layer

Smart Environment creation is the main purpose of this layer. This layer assures the data integrity, data authenticity and data confidentiality. Perception layer undertake on collection of information and data from various IoT devices towards web applications

3. SECURITY ISSUES IN IOT

In recent IoT botnet attacks performed like Mirai (malware), it is the biggest DDoS attack performed in the history. In October 2016 Mirai attack disturbed websites operations crosswise over North America and Europe after attackers flooded DNS service Dyn with malicious lookup requests from connected devices, like IP cameras, DVRs, switches and routers. As result various prominent websites such as Twitter, Amazon, Netflix, Airbnb, Reddit, GitHub, and many more could not navigated.

Brickerbot attack is another DDoS attack performed same as the Mirai botnet, in that it depended upon a DDoS attack and clients not changing the default username/password of their device [12] [13].

A report from F5 LABS indicated how IoT devices have been focused through botnets, numerous from a solitary facilitating supplier. As indicated by the report, IoT attacks grew 280% from the earlier half year revealing period of 2017, with a vast piece of this development coming from Mirai—malware that contaminates IoT devices and transforms them into bots [14]. In Table 1, a world's leading research and advising company Gartner predicted Worldwide Expenditure Forecast on Internet of Things security [15].

Table 1: Expenditure prediction on IoT security (in Millions of Dollars)

Year	2014	2015	2016	2017	2018
Expenditure	231.86	281.84	348.32	433.95	547.2

To secure IoT devices all kind of Security issues at different layers of IoT need to be understood. Various types of security issues at each layer are defined in brief considering the overall framework, the security issues must be settled toward the start of the design [16] [17].

3.1 Security issues at Perception Layer

Perception Layer deals with hardware's such as RFID and all sensors. Data is collected and transferred to network layer using wireless network transmission. The lack effective protection may result threat to signal as it is exposed in public place so as signal can be monitored, intercept, and disturbed easily [18] [19]. There are various types of attacks possible in IoT devices.

a) Denial of Service Attack

It is the most widely recognized attack for WSN and Internet as well. It causes waste of network assets, and frames the service out of reach from authorized users.

b) Replay Attack

Transmitting the valid data fraudulently or maliciously in repeated manner or delaying the transmission is known as Replay attack.

c) Node Capture

Capturing the node or device physically an attacker can control, leak all information, obtain security keys including group key, matching key, radio key etc. after that impact the protection of the whole framework.

d) Side Channel Attack

Electronic circuit are leaky, they produce emission as byproducts so as attacker can gather information about how data is processing and how the circuit information such as time required, energy expenditure, and electromagnetic radiation in the network. The use of emission can be used to perform reverse engineering gain the term 'side-channel analysis' or 'side-channel attack'.

e) Addition of Fake Nodes

New node inclusion to the system can be done by attackers, and feed fake date or code. This can stop system for transmitting real data by keeping busy to limited energy source; it can harm the energy source sleep, control it or can destroy the entire network.

f) Timing Information

Attacker also interested to get the information regarding the time required to obtain the key information and execution time required for encryption algorithms.

g) Attack on Routing

Routing of network transmission can be influenced by attacker utilizing fake, tampered or repeating routing information. This can contradict network transmission, create loops in routing, increment end-to-end delay, create error messages, extend or abbreviate the source way and so forth.

h) Brute force attack

Brute force attack is also most likely to suffer sensor node due to its ability of limited resource storage and computation.

I) Impersonation

Authentication in the dispersed condition is extremely troublesome to the perceptual node; taking into consideration that malicious node utilizes a fake identity to perform malicious or conspiracy attacks.

3.2 Security issues at Network Layer

Information must be secure while departing, travelling and dispatched towards web from the router. Information in travel over the system network also must be prevented against malicious movements [20].

a) Traditional Issues

Existing network for communication obtained relatively overall security assurance but there are yet many frequent issues like eavesdropping, Man in the middle attack, illegal access network, DoS attack, privacy damage, integrity damage, virus invasion, exploit attack etc. These problems can lead threat on data confidentiality and integrity.

b) Compatibility Issues

IoT network is a network of physical devices, vehicle, human, sensors, smart-phones etc. Due to heterogeneity of IoT security, coordination of network, inter-operability becoming worse. Existing web network security configuration based on human perspective, and does not certainly apply to correspondence between machines. Available security techniques will breakdowns rationale connection between IoT machines reason for compatibility issues.

c) The Cluster Security Problems

Existing IP technologies cannot be applied to large number of node identification as IoT has enormous amount of devices. Immense number of nodes traffic will probably block network if it uses the current authentication mechanism. Mutual authentication between much equipment cause literally waste of the crucial resources

d) Privacy Disclosure

Privacy information of particular user's can also be easily hacked by attackers by using social engineering and by developing information retrieval technologies.

3.3 Security issues at Application Layer

Security at application layer is the most complex and burdensome in the IoT architecture. For different environment or industrial applications different security issues are exist. Presently there is no ubiquitous standard for development of Application Layer. Following are few common security issues applicable on Application Layer

a) Software Vulnerabilities

Hacker can find out software vulnerabilities like buffer overflow vulnerabilities exist in the software due to non standard code development by software developers. It can be exploits to carry their purposes.

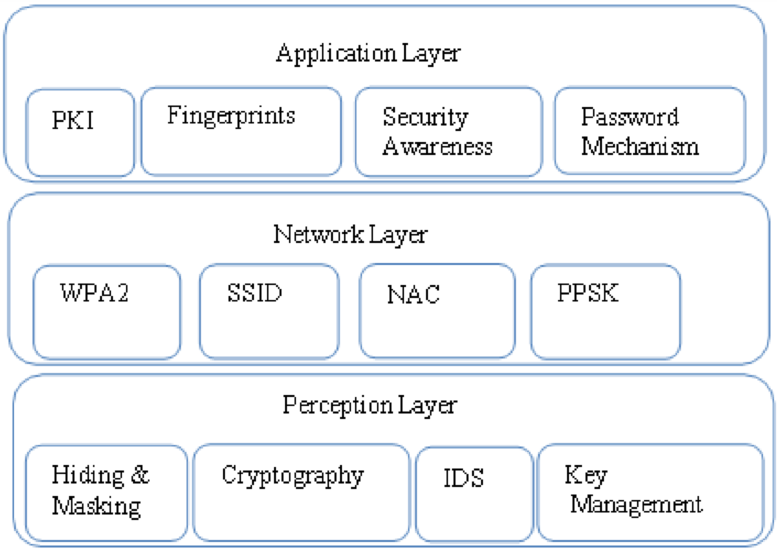


Fig. 2 Layer-wise security measures

4.1 Security Measure for Perception Layer

a) Side Channel Attack

Side Channel Attack (SCA) is a noteworthy issue in physical security. Differential Power Analysis (DPA) is a typical method for SCA. Hiding and Masking are two types of methods that can prevent DPA. Eliminating data dependencies of energy consumption is hiding mechanisms while Masking provides the middle estimations of encryption tools by randomized all the process.

b) Accessibility

Password based system can be used to protect RFID Tags and accessibility, chip security, antenna power analysis etc.

c) Cryptography

RFID can be protected by using Cryptography technology to protect confidentiality, user privacy protection, authentication and integrity of RFID systems. Hash function, Random number mechanisms, Logic Algorithm, re-encryption mechanisms and server data search algorithms are the part of security communication protocol.

d) Key Management

Security design prerequisites of Wireless sensor networks key management predominantly reflects security creation of key or algorithm modification, forward and backward protection and extensibility, source verification, freshness, and against conspiracy attacks. Four fundamental key distribution protocols are simple key distribution, hierarchical key management protocol, key pre-distribution method and dynamic key management algorithm.

e) Secret Key Algorithms

This is mainly incorporates symmetric key and asymmetric keys algorithms. Rivest-Shamir- Adleman (RAS) and Elliptic Curves Cryptography (ECC) are mainly used in Asymmetric keys algorithm, almost all current cryptographic systems internally use symmetric-key algorithms to encrypt mass messages.

f) Security Routing Protocol

An efficient routing protocol algorithm for security mainly uses following techniques Clustering, Data fusion, multiple hops routing, key management etc. For security routing mechanism SPINS security system protocols is broadly utilized, comprise of Secure Network Encryption Protocol (SNEP) and Micro Timed Efficient Streaming Loss-tolerant Authentication Protocol (µTESLA) protocol. SNEP is utilized to accomplish Confidentiality, Integrity, point to point authentication and freshness.

g) Intrusion Detection Technology

An Intrusion Detection System (IDS) is able to analyze the working of system nodes timely, and observe nodes suspicious behavior. Mechanism for protection from Cross site scripting (XSS) and cross site request forgery (CSRF) should be accomplished.

4.2 Security Measure for Network Layer

As IoT network nodes are random or irregular, autonomic, instability of energy restrictions and communication, it prompts that IoT have no foundation and dynamic topology [22].

h) Wireless Protected Access 2 (WPA2)

Wireless Protected Access 2 could settle on the organize utilization stronger unpredictable remote encryption instead of using Wireless Encryption Protocol (WEP).

i) Service Set Identifiers (SSID)

For wireless networks it is better to use many SSID instead of using only one. Thus, we may have divergent policies along each component and can allocate individual for different type of threats. Hence if any component affected by attacker, still other components will be safe.

j) Network Access Control (NAC)

Securing endpoints security technologies like antivirus, network intrusion detection system (NIDS), host intrusion prevention system (HIPS) provides better security mechanism to the network. Furthermore, it is also logical to index MAC addresses of each connected devices so that IP addresses allocate by router only to router listed devices and unknown devices can be blocked.

k) Private Pre-Shared Key (PPSK)

It is a method to connect device uniquely, securely and effortlessly in the networks. PPSK to each device connected to the network provides unique key to access network, and accessing domain might be characterized effectively to every device in the network.

l) NAT- Port Mapping Protocol Service (NAT-PMP)

The NAT-PMP is a network protocol for building settings of network address translation (NAT) and port passing configurations freely without user struggle. NAT-PMP does not follow any authentication methods and permit every host associated to the router's confined network to directly travel across the firewall. Hence, it need to be assured to examine the routers regularly regarding NAT-PMP services mis-configurations. Disabling all type of default and guest passwords from devices like routers and gateways need to be immediately finish when addition of any new network node or device. This incorporates powerful password policies, secret key management and more occasional updating of passwords.

m) IPSec Security Protocol

Authentication and Encryption can also be done using IPSec protocol. Authentication mechanisms enable the receiver to confirm the real identity of sender. Data encryption mechanisms protect data while transmission from attacker to eavesdropping and tampering data and enable confidentiality by encoding the data.

n) Authentication and Access Control

Authentication systems usually incorporate on the light weighted public key authentication techniques, random key pre-distribution authentication technology, Pre Shared Key (PSK), one- way hash functions authentication technology, utilizing auxiliary data authentication technology and so forth. Access control primarily incorporates symmetric and asymmetric cryptosystem.

4.3 Security Measure for Application Layer

There are many Utilizations application layer of IoT and it has diversity and instability. It introduce that distinctive application environment have diverse security demands.

a) Key protocol and Network Authentication

The basic mechanism are symmetric key crypto-framework, public key crypto-framework (certificates or PKI), and certificate exchange technology.

b) Privacy protection

Many techniques are available like digital water marking, fingerprint technology, threshold cryptography, anonymous authentication etc. used to protect private information.

c) Security Awareness

IoT users must be aware of correctly use of IoT services and information security importance. So that confidential information cannot be leaked.

d) Physical Security

Physical security constraint, physical resource control security, access control using password mechanism, and data management etc. Also paired devices default password must be updated. Idle time locking and maximum attempt implementation help in securing devices.

Denial of service: a common attack at each layer

DoS is an common attack that can exercise at all the three layers of IoT, Table 2 illustrated how it is significant to every layer also how to prevent and protect by this attack at each layer of IoT [23] [24].

Table 2: Solutions for DoS attacks

IoT Layer	Attack/Issues	Solutions/Methods
Perception Layer	Jamming	All or nothing Transmission , Strong Hiding Commitment Scheme, Packet Hiding ,Cryptanalysis and Steganography ,Cryptographic puzzle base scheme
	Desynchronizing attack	Double Authentication Scheme, Packet Authentication
Network Layer	UDP Flood , ICMP Flood	BCP38, Firewall Filtering
	DNS Flood	DNSSEC ,uRPF
	Smurf Attack	Block illegal ICMP Responses, Infrastructure Protection, Name Server Protection
Application Layer	Programming Attack	Parameterized Query, Input validation at server
	Path based DoS	Normalize input

5. CURRENT STATUS OF IOT SECURITY

Existing security frameworks are not addressing overall security issues and still there is scope of improvements, hence there is need to develop a security framework that not only provides security mechanism but also be able to predict possible threats or attack. As IoT is growing technology and it has various issues related to security. It has vast domain for analysis and opportunity for researcher to develop and proposed security solutions for existing issues. Detection and identification of threats is also a major problem in IoT network [25] [26] [27].

To countermeasures the issues and challenges in securing devices connected to IoT network the machine learning methods can be used inside an IoT network to secure the framework. Machine learning is a region of artificial intelligence (AI) in which computer programs are empowered to gain from experience, illustrations, and analogies. As learning happens, the abilities inside the program turn out to be more intelligent and the program ends up plainly capable of decisions making. This phenomenon can play a vital role in IoT network security.

6. CONCLUSION AND FUTURE WORK

This paper elaborated IoT layer architecture, problems, challenges and countermeasure for each layer of IoT structure. IoT network framework is combination of many layers and numerous problems originated from system concatenation and there are numerous issues which are not has a place with certain layer i.e. privacy and protection is common problem in every layer some have discussed but still there can be many more issues. This paper also described protocols of each layers of IoT and included methods, technologies and mechanism to protect from several issues at each IoT layers. In future machine learning technique can be applicable on the IoT network to protect network by various security issues and attacks.

REFERENCES

[1] Rajendra Billure, Varun M Tayur, Mahesh V, ―Internet of Things - A Study on the Security Challenges‖, Department of Computer Science and Engineering, Jain University Bangalore, India, IEEE, 2015.

[2] Internet of Things (IoT)― http//internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT.

[3] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, ―Security of the Internet of Things perspectives and challenges‖, Wireless Networks, 2014, vol. 20, no. 8, pp. 2481–2501, Springer 2014.

[4] Rwan Mahmoud, Tasneem Yousuf, Fadi Aloul, Imran Zualkernan, ―Internet of Things (IoT) Security Current Status, Challenges and Prospective Measures‖, Department of Computer Science & Engineering, American University of Sharjah, UAE, IEEE 2015.

[5] S. S. Basu, S. Tripathy and A. R. Chowdhury, "Design challenges and security issues in the Internet of Things," 2015 IEEE Region 10 Symposium, Ahmedabad, 2015, pp. 90-93.

[6] Lan Li, "Study on security architecture in the Internet of Things," Proceedings of 2012 International Conference on Measurement, Information and Control, Harbin, China, 2012, pp. 374-377.

[7] M. Mohsin, Z. Anwar, G. Husari, E. Al-Shaer and M. A. Rahman, "IoTSAT A formal framework for security analysis of the internet of things (IoT)," 2016 IEEE Conference on Communications and Network Security (CNS), Philadelphia, PA, 2016, pp. 180-188.

[8] B. F. Zahra and B. Abdelhamid, "Risk analysis in Internet of Things using EBIOS," 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, 2017, pp. 1-7.

[9] P. A. Wortman, F. Tehranipoor, N. Karimian and J. A. Chandy, "Proposing a modeling framework for minimizing security vulnerabilities in IoT systems in the healthcare domain," 2017 IEEE EMBS International Conference on Biomedical & Health Informatics (BHI), Orlando, FL, 2017, pp. 185-188.

[10] M. Leo, F. Battisti, M. Carli, and A. Neri, "A federated architecture approach for Internet of Things security" in Euro Med Telco Conference (EMTC), 1-5, 2014.

[11] Gurpreet Singh Matharu, Priyanka Upadhyay, Lalita Chaudhary,‖The Internet of Things Challenges & Security Issues‖, IEEE,2014.

[12] https//krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive- internet-outage/.

[13] http//www.zdnet.com/article/5-nightmarish-attacks-that-show-the-risks-of-iot-security/.

[14] https//f5.com/labs/articles/threat-intelligence/ddos/the-hunt-for-iot-the-rise-of-thingbots.

[15] https//www.gartner.com/newsroom/id/3291817.

[16] Kai Zhao1, Lina Ge1, ―A Survey on the Internet of Things Security‖, School of information science and engineering,Guangxi University for nationalitiesGuangxi, China, IEEE, 2013.

[17] Weizhe Zhang,Baosheng Qu, ―Security Architecture of the Internet of Things Oriented to Perceptual Layer‖ International Journal on Computer, Consumer and Control (IJ3C), Vol. 2, No.2(2013).

[18] Andrea Zanella,Senior Member, IEEE, Nicola Bui, Angelo Castellani,Lorenzo Vangelista,Senior Member, IEEE, and Michele Zorzi, Fellow, IEEE ―Internet of Things for Smart Cities‖ IEEE INTERNET OF THINGS JOURNAL, VOL. 1, NO. 1, FEBRUARY 2014.

[19] W. Z. Khan, H. M. Zangoti, M. Y. Aalsalem, M. Zahid and Q. Arshad, "Mobile RFID in Internet of Things Security attacks, privacy risks, and countermeasures," 2016 International Conference on Radar, Antenna, Microwave, Electronics, and Telecommunications (ICRAMET), Jakarta, 2016, pp. 36-41.

[20] Luigi Atzori , Antonio Iera , Giacomo Morabito, The Internet of Things A survey, Computer Networks The International Journal of Computer and Telecommunications Networking, v.54 n.15, p.2787-2805, October, Elsevier, 2010.

[21] Leloglu, E., A Review of Security Concerns in Internet of Things. Journal of Computer and Communications, 5, 121-136, 2017.

[22] Brian Russell, Cesare Garlati, David Lingenfelter, "Security Guidance for Early Adopters of the Internet of Things (IoT)", CSA Mobile Working Group, Apr. 2015.

[23] Senthilkumar Mathi, Lavanya Dharuman, Prevention of Desynchronization Attack in 4G LTE Networks Using Double Authentication Scheme, Procedia Computer Science, Volume 89, 2016, Pages 170-179.

[24] https//www.owasp.org.

[25] I. Kotenko, I. Saenko, F. Skorik and S. Bushuev, "Neural network approach to forecast the state of the Internet of Things elements," 2015 XVIII International Conference on Soft Computing and Measurements (SCM), St. Petersburg, 2015, pp. 133-135.

[26] R. Madeira and L. Nunes, "A machine learning approach for indirect human presence detection using IOT devices," 2016 Eleventh International Conference on Digital Information Management (ICDIM), Porto, 2016, pp. 145-150.

[27] J. Cañedo and A. Skjellum, "Using machine learning to secure IoT systems," 2016, 14th Annual Conference on Privacy, Security and Trust (PST), Auckland, 2016, pp. 219-222.

Minimizing Power Loss Through Network Reconfiguration using the Particle Swarm Optimization Algorithm

[1]Wei-Tzer Huang, [2]Tsai-Hsiang Chen, [3]Jhih-Siang Yang, [4]Kuo-Lung Lian, [5]Hong-Ting Chen, [6]Yung-Ruei Chang, [7]Yih-Der Lee, [8]Yuan-Hsiang Ho

[1,5]Department of Industrial Education and Technology, National Changhua University of Education, Taiwan

[2,3,4]Department of Electrical Engineering, National Taiwan University of Science and Technology, Taiwan

[6,7,8]The Institute of Nuclear Energy Research, Taiwan

E-mail: [1]vichuang@cc.ncue.edu.tw, [2]thchen@mail.ntust.edu.tw, [3]m10307106@mail.ntust.edu.tw, [4]ryanlian@mail.ntust.edu.tw, [5]edchen1991@gmail.com, [6]raymond@iner.gov.tw, [7]ydlee@iner.gov.tw, 8twingo_ho@iner.gov.tw

ABSTRACT

This study aims to minimize power loss through network reconfiguration in traditional distribution networks and microgrids. To address this problem, an algorithm composed of an objective function and operation constraints is proposed. Network connection matrices based on graph theory and the backward/forward sweep method is used to analyze power flow. A minimizing power loss approach is developed for network reconfiguration, and the particle swarm optimization algorithm is adopted to solve this optimal combination problem. The proposed approach is tested on the IEEE 33-bus test system and the first outdoor microgrid test bed established by the Institute of Nuclear Energy Research in Taiwan. Simulation results demonstrate that the proposed approach can be applied in network reconfiguration to minimize power loss.

Index Terms—Microgrid, Network Reconfiguration, PSO, Connection Matrices, Power Loss.

I. INTRODUCTION

The function of traditional distribution networks is to distribute electrical power to customers because voltage level in such networks is relatively lower and their total length is longer compared with transmission networks. Thus, reducing power loss in distribution networks is vital. At present, many distribution energy resources (DERs) are connected to distribution networks. Distribution networks have become active networks called microgrids. Microgrids consist of DERs and loads. DERs include renewable and nonrenewable generation units, as well as storage devices, such as photovoltaic systems, wind turbines, fuel cells, microturbines, diesel engines, battery banks, and super capacitors, among other. [1]–[2]. Microgrids can be operated under grid-tied and islanding modes through a static switch at the common coupling point between the main power grid and the microgrid. In the grid-tied operation mode, the microgrid may act as a load or source at any time in terms of the main power grid. The islanding operation mode must be operated autonomously based on the power balance principle to maintain constant voltage and frequency. Numerous renewable energy units are used in microgrids. Thus, CO2 emissions are reduced and global warming is prevented. Constructing microgrids in industrial parks, campuses, shopping malls, off-shore islands, and remote districts is worthwhile because of the aforementioned advantages.

Planning, designing, operating, and controlling microgrids are more complex compared with traditional distribution systems. Consequently, an energy management system (EMS) is essential in the system operation stage in microgrids. To increase operating efficiency, the network reconfiguration approach, which is one of the functions in EMS, has been adopted to minimize power loss and improve voltage quality. A. Merlin and H. Back [3]used the spanning tree structure to model a distribution system. The obtained solution results were independent from the initial status of the switches; however, their algorithm was very time-consuming. S. Civanlar et al. [4]proposed the branch-exchange method to minimize the number of switching operations; however, this approach is not systematic and can only reduce power loss. Y. J. Jeon et al. [5] presented the simulated annealing algorithm for network reconfiguration; this algorithm was easy to code but required considerable computation time in large-scale systems. B. Venkatesh and R. Ranjan[6] proposed an approach that used a fuzzy adaptation of evolutionary programming as a solution technique; however, as a system grew large, this method became increasingly complex.H. Hamdoui et al. [7] used the ant colony approach algorithm to identify the optimal combination of feeders with different parameters for a new topology design. This method is highly efficient and convergence definitely occurs; however, the length of time required to achieve convergence remains uncertain.

In the present study, a population-based stochastic optimization technique that adopts the particle swarm optimization (PSO) algorithm is used to search for the optimal network reconfiguration problem. This paper is divided into four sections. Section 1 presents the introduction. Section 2 reviews network reconfiguration algorithms and describes the network reconfiguration problem and its formulation. Section 3 demonstrates and discusses the simulation results.

Section 4 concludes the paper.

II. PROBLEM FORMULATION

A. Description of the Network

Most distribution networks exhibit a radial configuration from the distribution substation to the customers. Sectionalizing switches and tie switches are installed in these systems to consider normal and abnormal operations. Under normal conditions, the sectionalizing switches are typically closed and the tie switches are generally open. Nevertheless, the network can be changed by performing switching actions for the best network topology to increase system performance. This process is called reconfiguration. Through network reconfiguration, power loss is reduced, load distribution becomes uniform, and overloading is avoided. System reliability is enhanced after a fault occurs.

A combinatorial problem arises because of switching actions. Therefore, when the number of switches is high, the possibility of reconfiguration increases. The most common approaches to solve this problem in network reconfiguration can be classified as follows:

1. Mathematical optimization methods,
2. Heuristic methods, and
3. Artificial intelligence methods.

These methods have advantages and disadvantages. Based on literature reviews, these techniques can effectively address network reconfiguration problems. Solving a network reconfiguration problem involves two components: (1) the objective function and the system operating constraints and (2) the power flow algorithm. The common objective function is power loss minimization, and the constraints are the upper and lower limits of bus voltages, the ampere capacity of the conductor, and feasible network topology. The power flow algorithms must suit the characteristics of distribution networks with high X/R ratio, short distance between two connected buses, and unbalanced load distributions and system structure.

B. Objective Function

The objective function used in this study minimizes power loss. This objective function can be expressed as

$$\min f = \sum_{i=1}^{L} \left| I_j \right|^2 R_j \, , \tag{1}$$

which is subject to

$$P_{i+1} = P_i - r_i I_i^2 - P_{Li+1} \, , \tag{2}$$

$$Q_{i+1} - Q_i - x_i I_i^2 - Q_{Li+1} \, , \tag{3}$$

$$V_{Li} \leq V_i \leq V_{Ui} \, , \tag{4}$$

$$g \in G \, . \tag{5}$$

In (1), L represents the number of lines and Ij denotes the current of the jth line. Meanwhile, in (2) and (3), Pi and Qi denote the real and reactive power flow out of bus i, respectively; riand xi are the resistance and reactance between bus iand i+1; Li represents the line current between bus i and i+1; Vi, VUi, and Vlide note the voltage at bus i and its upper and lower limits, respectively; g is the network topology; and G represents the sets of radial topologies, which cannot be closed-loop and islanding topologies.

C. Power Flow Algorithm

Graph theory and the backward/forward sweep method [8]–[9] were applied in the proposed power flow algorithm. Graph theory is a systematic approach to build incidence matrices that correspond to network topologies. The incidence matrices used in the proposed algorithm is the A matrix, which is the element–bus incidence matrix, and the K matrix, which is branch–path incidence matrix. Based on these matrices, the bus-injection to branch-current (BIBC) matrix and the branch-current to bus-voltage (BCBV) matrix can be established according to various system structures. Furthermore, BIBC and BCBV matrices are adopted in the power flow algorithm. The power flow solution procedure is described as follows.

Step 1 : Build the A matrix. The K matrix can be derived using (6). Establish the BIBC matrix using (7), as follows:

$$K=[A^{-1}]^{t}, \qquad (6)$$

$$[BIBC]--K. \qquad (7)$$

Step 2 : Transpose the BIBC matrix and add the primitive line impedance into the corresponding non-zero element position to derive the BCBV matrix.

Step 3 : Compute the equivalent bus injection current at each bus connected to the source or load using (8) as follows:

$$I_i^k=(\frac{P_i+Q_i}{V_i^k})^{*}. \qquad (8)$$

Step 4 : Calculate the voltage derivation of each bus using (9):

$$[\Delta V^k]=[BIBC][BCBV][I^k]. \qquad (9)$$

Step 5 : Update the bus voltage using (10), where V_{no_load} is the no-load voltage at each bus, that is,

$$[V^{k+1}]=[V_{no\_load}][\Delta V^k]. \qquad (10)$$

Step 6 : Check whether convergence is achieved using (9). If convergence is achieved, then proceed to step 3; otherwise, end the solution procedure. ε is the maximum toleration, that is,

$$max_i(\left|I_i^{k+1}\right| \quad \left|I_i^k\right|)>\varepsilon. \qquad (11)$$

D. PSO Algorithm

(5P)SO was introduced by J. Kennedy and R.C. Eberhart [10]-[11] in 1995. This algorithm is a population-based optimal search technique attributed to the social behavior of certain animals, such as fish schooling or bird flocking. PSO simulates the population behavior that combines the cognition-only model and the social-only model, as shown in (12) and (13), respectively. The cognition-only model searches for the individual best solutions as the local best (pbest) and changes particle position and velocity to move in a multi-dimensional space until the position does not change or the computational limits are reached. In the social-only model, the pbest and global best (gbest) are compared to update the gbest and change particle position and velocity. The combination of pbest and gbest in PSO allows the particle to adjust rapidly and correctly, which results in fast convergence using (14)–(16).

$$V_n^{k+1} = V_n^k + c_1 \times rand_1 \times (pbest_n^k - s_n^k), \tag{12}$$

$$V_n^{k+1} = V_n^k + c_2 \times rand_2 \times (gbest^k - s_n^k), \tag{13}$$

$$\begin{aligned} V_n^{k+1} &= w \times V_n^k + c_1 \times rand_1 \times (pbest_n^k - s_n^k) \\ &\quad + c_2 \times rand_2 \times (gbest^k - s_n^k) \end{aligned}, \tag{14}$$

$$s_n^{k+1} = s_n^k + v_n^{k+1}, \tag{15}$$

$$w = w_{\max} - (w_{\max} - w_{\min}) \times \frac{k}{k_{\max}}, \tag{16}$$

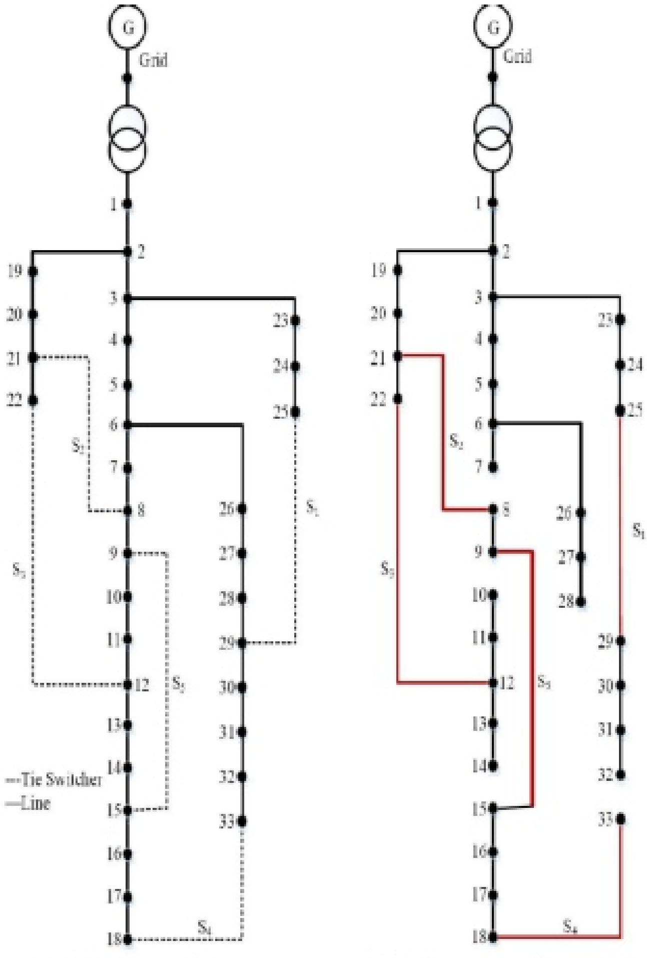
where k_{max} is the maximum iteration, n is the particle number, V_n^k is the velocity of particle n at the k^{th} iteration, S^k_n is the k^{th} position of particle n, c_1 and c_2 are learning factors, $rand_1$ and $rand_2$ are random numbers between 0 and 1, pbest $^k_n$is the best value of particle n at the k^{th} iteration, and $gbest^k$ is the global best value at the k^{th} iteration. w, w_{max}, and w_{minare} acceleration coefficients, maximum weighting values, and minimum weighting values, respectively. In this study, the related parameters of PSO are set to n = 500, w_{max} = 0.9, w_{min} = 0.2, c1 = 2, and c2 = 2. Moreover, the maximum iteration number is 200.

III. NUMERICAL RESULTS

In this section, the IEEE 33-bus test system and the microgrid of the Institute of Nuclear Energy Research (INER) in Taiwan were used as sample systems to verify the effectiveness of the proposed approach. The IEEE 33-bus test system is a traditional distribution system. It is a three-phase balance passive network that is only connected with loads. The INER microgrid is an active network with both DERs and loads. The simulation results are discussed in the following sections.

A. IEEE 33-Bus Test System

Figure 1(a) shows the IEEE 33-bus test system with five tie switchers and 32 sectionalizing switchers. The simulation result of the optimal network topology that uses the proposed approach for network reconfiguration is illustrated in Fig. 1(b). In the figure, five tie switchers are closed and five sectionalizing switchers between buses 7 and 8, 9 and 10, 14 and 15, 29 and 30, and 32 and 33 are opened. The convergence characteristics of the proposed method are shown in Fig. 2, the power loss from initial value (144.75 kW) to the globaloptimum (140.74kW) at the 24*th*iteration.Figure 3 indicates the simulation result of the bus voltage profile. The lowest bus voltage was 0.9131 p.u. at bus 18 before reconfiguration and 0.9413 p.u. at bus 32 after reconfiguration. Thus, the voltage profile before reconfiguration was better than that after reconfiguration. In addition, the simulation results of power loss before and after reconfiguration shown in Fig. 4 indicated that the power loss in each line section varied because the line flow was changed and the total power loss was 202.68 kW and 140.74 kW, respectively. Evidently, power loss was reduced after reconfiguration. Based on these numerical results, the proposed network reconfiguration algorithm effectively improved voltage profile, reduced power loss, and increased operation efficiency under normal operating conditions.



(a)Before reconfiguration (b)After reconfiguration

Fig. 1 IEEE 33-bus test system

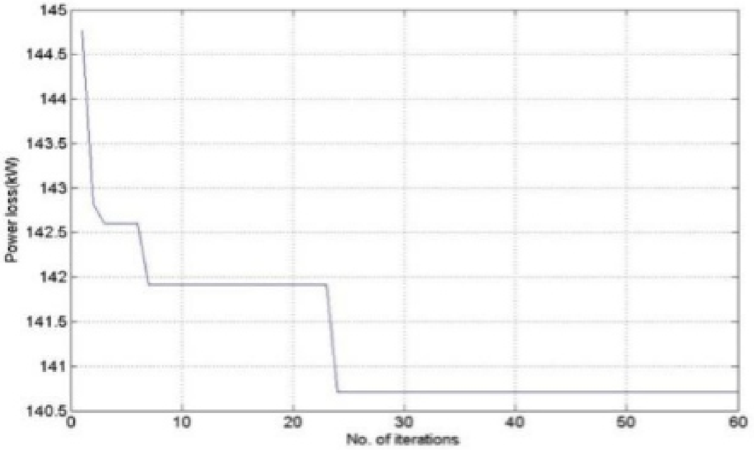


Fig. 2 Convergence characteristics of proposed methodof the IEEE 33-bus test system

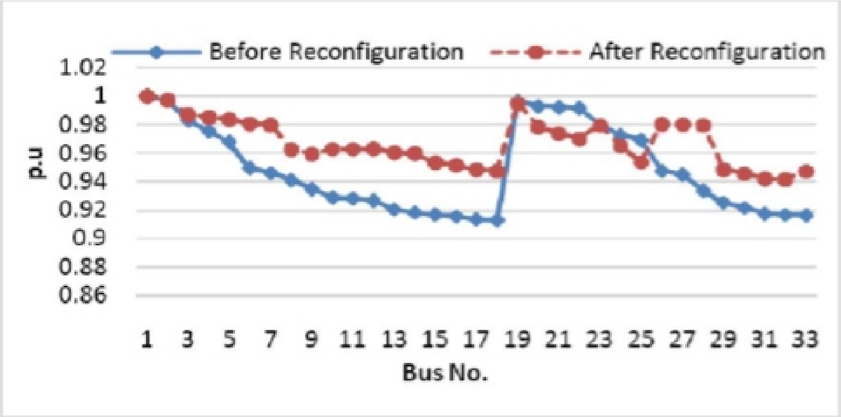


Fig. 3 Simulation result of the bus voltage of the IEEE 33-bus test system

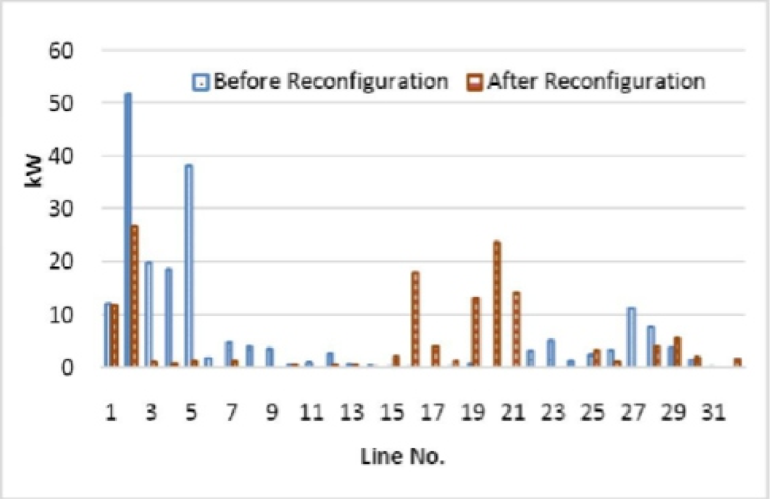


Fig. 4 Simulation result of the power loss of the IEEE 33-bus test system

B. INER Microgrid

The first outdoor microgrid test bed was developed by INER in Taiwan. This system consists of three zones with DERs and loads and includes a tie switcher and 11 sectionalizing switchers, as shown in Fig. 5. For example, zone 1 comprises 21 units of 1.5 kW high concentrator photovoltaic, 1 unit of 65 kW microturbine, a 60 kWh battery bank, and a lumped load in an office building (Building 048). The bus and line data of the INER microgrid for simulation are provided in Tables 1 and 2 in the Appendix. Although this is a sample network topology, the solution can be derived via a brute force search. Our proposed algorithm is a systematic approach that can be applied in a complex network topology. Thus, the effectiveness of the proposed approach can be verified using this sample system by comparing the results of the proposed approach with that of the brute force search method.

The simulation result indicated that the tie switcher was closed and a sectionalizing switcher between buses 3 and 7 was opened. This outcome is the same as that in the brute force search method. The convergence characteristics of the proposed method are shown in Fig. 6, the power loss reduced to the globaloptimum at the 18*th*iteration.Figure 7 depicts the simulation result of the bus voltage profile. The lowest bus voltage was 0.9745 p.u. at bus 10 before reconfiguration and 0.9774 p.u. at bus 12 after reconfiguration. Similarly, the voltage profile was improved after reconfiguration. Figure8 demonstrates that the simulation result of power loss has changed after reconfiguration. The total power loss was 2.18 kW before reconfiguration, which was reduced to 1.65 kW after reconfiguration. Based on the numerical results, the proposed algorithm was proven to be a feasible approach to improve voltage quality, reduce power loss, and increase efficiency under normal operating conditions.

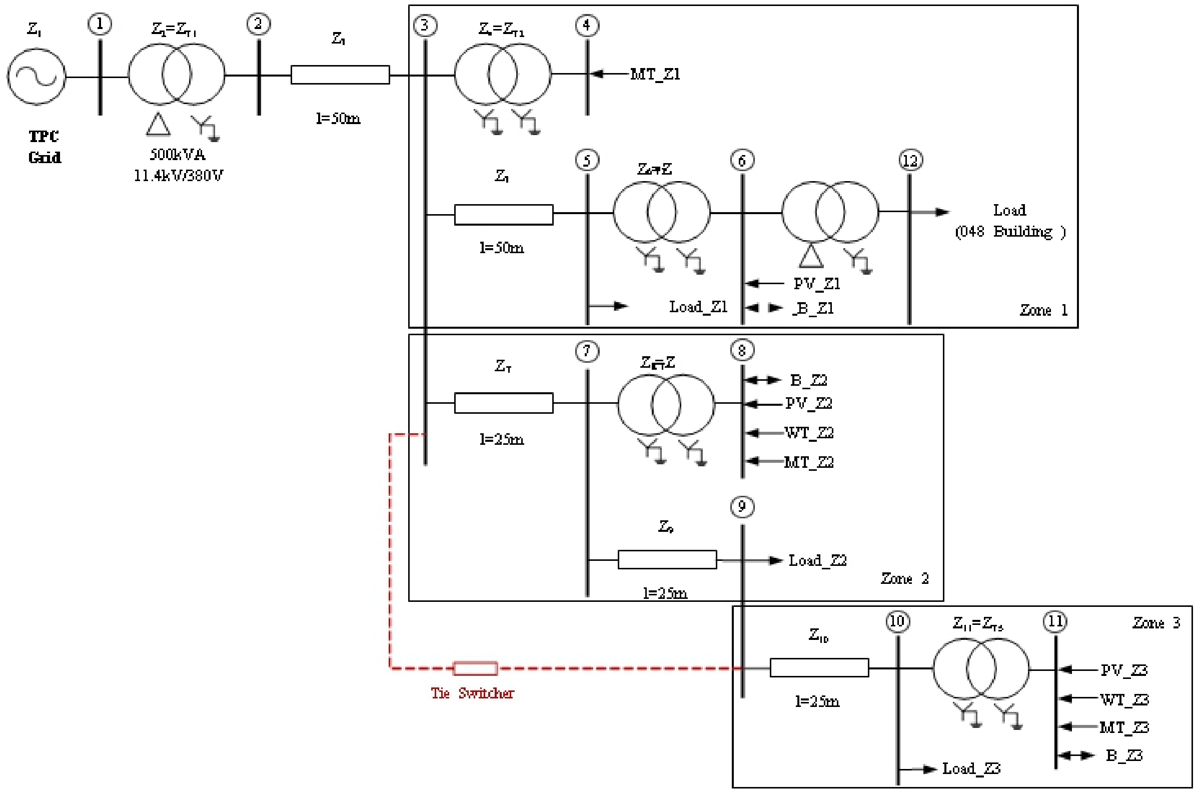


Fig. 5 Single line diagram of the INER microgrid

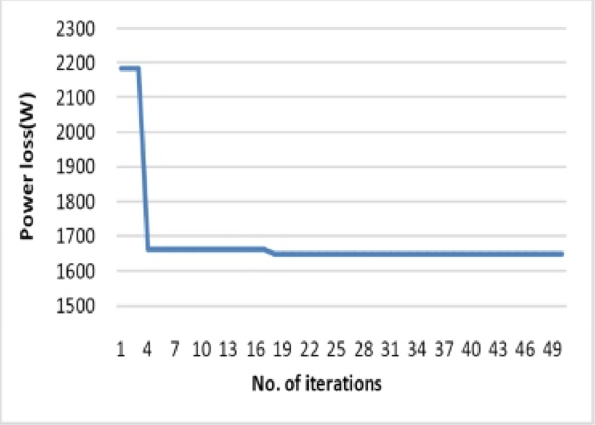


Fig. 6 Convergence characteristics of proposed method of the INER microgrid

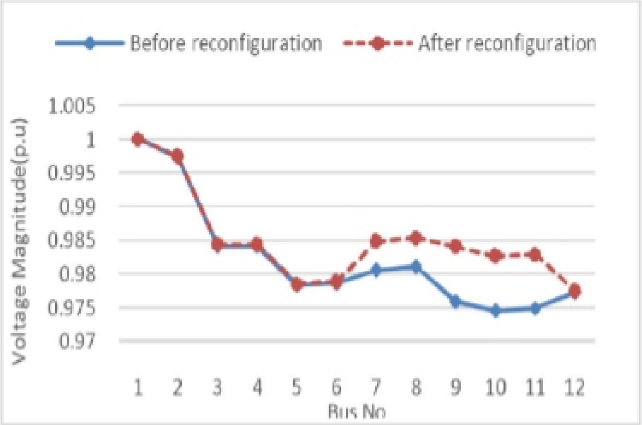


Fig. 7 Simulation result of the bus voltage of the INER microgrid

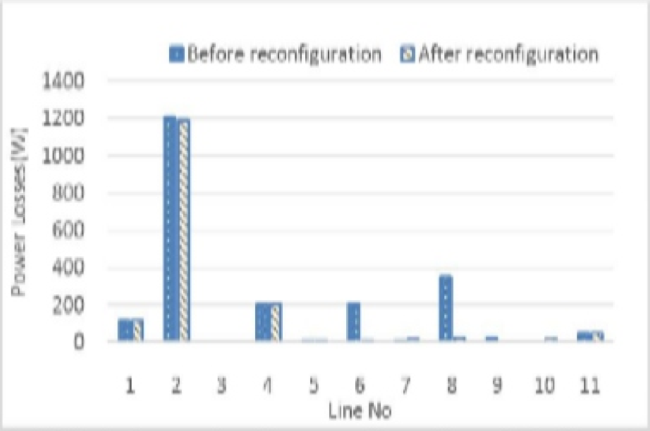


Fig. 8 Simulation result of the power loss of the INER microgrid

CONCLUSION

A network reconfiguration algorithm that applies a graph theory-based power flow solution technique has been developed in this study. PSO exhibits self-learning capability to obtain the most optimal solution, and the graph theory-based power flow algorithm can easily establish network topology using incidence matrices according to different system structures. The IEEE 33-bus system and the INER microgrid have been used as sample systems to verify the effectiveness of the proposed approach. The numerical results demonstrate that this approach can improve voltage profile, reduce total power loss, and increase efficiency under normal operating conditions. The developed algorithm can be applied in traditional distribution networks with or without DERs and microgrids to improve system operation performance.

REFERENCES

[1] R.H.Lasseter, "MicroGrids," IEEE Power and Energy Magazine, Volume 5, issue4, pp. 78-94, July-Aug. 2007.

[2] K. A. Nigim and W. J. Lee, "Micro Grid Integration Opportunities and Challenges," IEEE Power Engineering Society General Meeting, pp. 1-6, 24-28 June 2007.

[3] A. Merlin and H. Back, "Search for a minimal-loss operating spanning tree configuration in an urban power distribution system," proc. 5th power system computation Conf. (PSCC) Cambridge UK., pp. 1-18, 1975.

[4] S.Civanlar. J.J.Grainger, H. Yin, and S.S.H.Lee, "distribution reconfiguration for loss reduction," IEEE Transactions on Power Delivery, pp.1217-1223, 1988.

[5] Y. J. Jeon, J. C. Kim, J. O. Kim, J. R. Shin, and K. Y. Lee, "An efficient simulated annealing algorithm for network reconfiguration in large-scale distribution systems," IEEE Transactions on Power Delivery, vol. 17, no. 4, pp.1070-1078, Oct. 2002.

[6] B. Venkatesh and R. Ranjan, "Optimal radial distribution system reconfiguration using fuzzy adaptation of evolutionary programming," International Journal of Electrical Power & Energy Systems, vol. 25, no. 10, pp. 775-780, 2003.

[7] H. Hamdoui, S. Hadjeri, and A. Zeblah, "A new constructive method for electric power system reconfiguration using ant colony," Leonardo Electronic Journal of Practices and Techniques, no. 12, p.49-60, January-June 2008.

[8] J. H. Teng, "A network-topology based three: phase loadflow for distribution systems," Proceedings of NationalScience Council ROC (A), 2000. vol. 24, no. 4, pp.259-264.

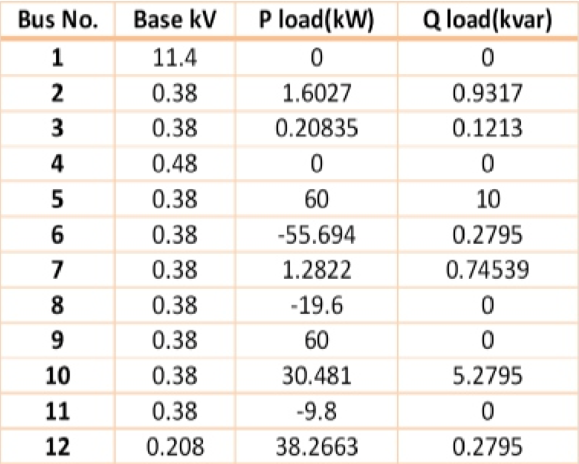
[9] T. H. Chen and N. C. Yang, "Three-phase power-flowby direct ZBR method for unbalanced radial distributionsystems," IET Generation, Transmission & Distribution,vol. 3, no. 10, pp. 903-910, March2009.

[10] J. Kennedy and R. C. Eberhart, "Particle swarm optimization," in: Proc. IEEE Int. Conf. on Neural Networks, Perth, Australia, vol. 4, pp. 1942-1948, 1995.

[11] R. C. Eberhart and J. Kennedy, "A new optimizer using particle swarm theory," in: Proc. IEEE Int. Symposium on Micro Machine and Human Science, Nagoya, Japan, pp. 39-43, 1995.

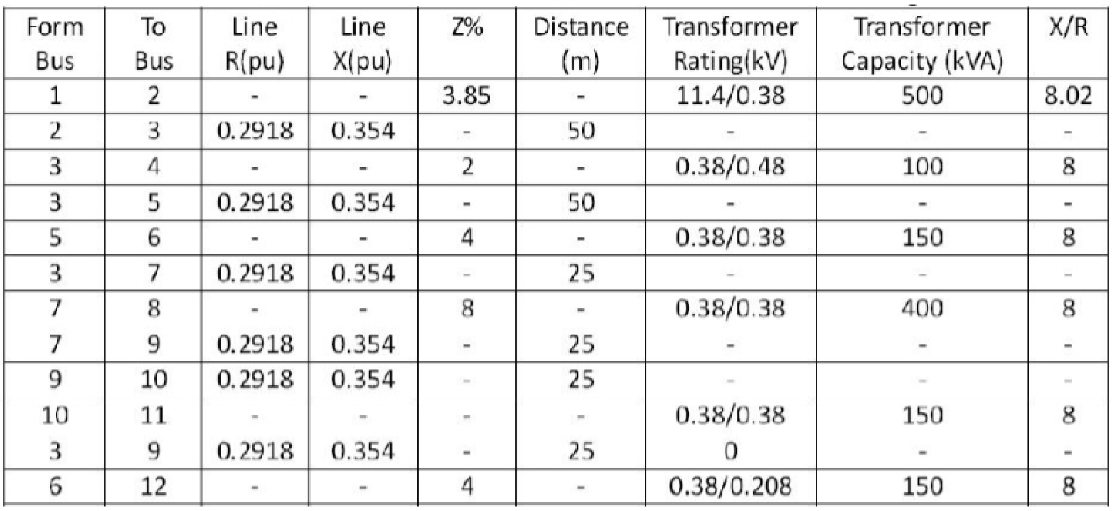
APPENDIX

Table 1 Bus data of the INER microgrid



Bus No.	Base kV	P load(kW)	Q load(kvar)
1	11.4	0	0
2	0.38	1.6027	0.9317
3	0.38	0.20835	0.1213
4	0.48	0	0
5	0.38	60	10
6	0.38	-55.694	0.2795
7	0.38	1.2822	0.74539
8	0.38	-19.6	0
9	0.38	60	0
10	0.38	30.481	5.2795
11	0.38	-9.8	0
12	0.208	38.2663	0.2795

Table 2 Line data of of the INER microgrid



Form Bus	To Bus	Line R(pu)	Line X(pu)	Z%	Distance (m)	Transformer Rating(kV)	Transformer Capacity (kVA)	X/R
1	2	-	-	3.85	-	11.4/0.38	500	8.02
2	3	0.2918	0.354	-	50	-	-	-
3	4	-	-	2	-	0.38/0.48	100	8
3	5	0.2918	0.354	-	50	-	-	-
5	6	-	-	4	-	0.38/0.38	150	8
3	7	0.2918	0.354	-	25	-	-	-
7	8	-	-	8	-	0.38/0.38	400	8
7	9	0.2918	0.354	-	25	-	-	-
9	10	0.2918	0.354	-	25	-	-	-
10	11	-	-	-	-	0.38/0.38	150	8
3	9	0.2918	0.354	-	25	0	-	-
6	12	-	-	4	-	0.38/0.208	150	8

Network Failures and Root Cause Analysis: An Approach using Graph Databases

[1] A. Vijay Kumar, [2] G. Anjan Babu

[1,2]Department of Computer Science,
S V University, Tirupati, India

ABSTRACT

Detecting the origin of a problem in network failures plays an important role to troubleshoot in order to function accurately. The structure of the network itself creates an ambiguity due to the non-sequential functionality of it. One of the optimal sources which tackle's the network related issues are Graph Databases. Root Cause Analysis is one of the application areas of Graph Databases as its data model which itself persuade its structure in the form of network. Though the portion of the network which was damaged is negligible when compare to its size, the impact on the network is unimaginable sometimes. Due to the flexibility to deal with network issues major focus was given to Neo4j Graph Database and its specific query language Cypher. This paper presents the salient features of Neo4j Graph Database make it possible to identify the Root Cause in the network with proper executions and outputs.

Keywords—Graph Database; Flexibility; Troubleshoot; Route Cause

I. INTRODUCTION

The Reduction of the biggest portion of the problem into small is the main objective of the proposed work. Neo4j Graph Database [1] along with its specific query language Cypher is used to tackle this task. The actual communication process in the network is carried out from the source from where the transformation of data will be started. Data will be transferred to destination from router to router. In the process of transformation of data from source to destination there is a chance of failure to receive data at destination. So many reasons to the malfunction in receipt of data at destination exist. Some include router failures, link failures, etc. This paper focuses on router failures or break downs leading to percolation problem in the communication there by it just fetches the information of failure router reducing the problem finding time.

II. GRAPH DATABASE

Graph Database [2] is one of the prominent NoSQL databases which use the graph properties like nodes and edges to handle the data. The term NoSQL [3] indicates other than SQL databases there are some designed especially to tackle the issues of SQL databases and it is a mechanism for storage and retrieval of data that is modeled in means other than the tabular relations used in relational databases [4].

Even traditional databases are present to handle lot of advancements are taken place in the database field. As the data advanced from structured to unstructured the technology too advanced from traditional to Graph Databases. Even there are more NoSQL databases exist the following few advantages will become sufficient statements to say whether the job of finding root causes dealt accurately by Graph Databases or not.

- White-board friendly nature gives ability to represent natural nature of networks.
- Schema-friendly nature gives ability to accommodate new changes at any stage.
- The querying technique used by Cypher “traversing” provides the facility to reach the failure node very fast.
- Minutes to milliseconds performance.

Both nodes and edges can have properties in Graph Database. Properties are the way to store information about each entity. Unlike relational databases Graph databases allows storing any type of data without any constraints on it. There are thousands of companies using this Graph Database as a medium to handle data like Facebook; uses the concept of features Graph Search, Google uses the Knowledge Graph, and Twitter uses graphs to recommend people to follow [5].

III. NEO4J

Neo4j is a Graph Database which is sponsored by the company Neo Technology [6]. It is a high performance scalable graph database. There are multiple Graph Databases [7] present out of all these Neo4j is best suitable for the application areas which involves networks.

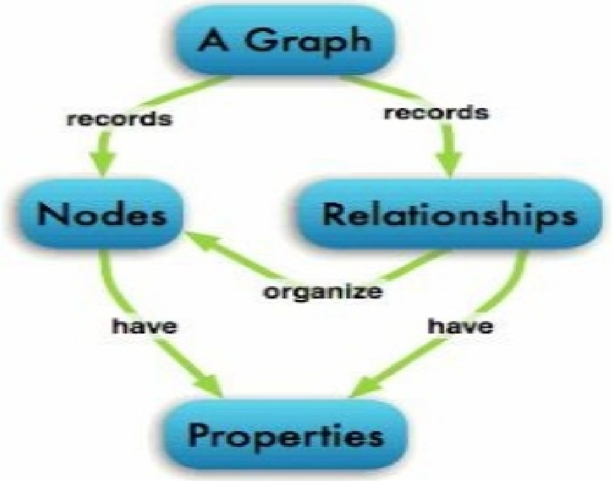


Fig 1. Data Modeling In Neo4j Graph Database

The above image clearly explains the data model used by Neo4j Graph Database [8].

A. Cypher Query Language

One of the significant assets of the Neo4j graph database invention today is its magnificent query language, called Cypher. Cypher is a declarative, pattern-matching query language that makes graph database management systems explicable and workable for any database user. People with little technical knowledge can also operate this. Commands which are used for creation of network and for finding the route cause are listed below [9]

I) CREATE

Creating Nodes:

The writing clause CREATE is used to create a node in Neo4j Graph Database. We can create a single node or multiple nodes at a time as shown below.

Single node:

The following syntax is used for creating single node.

CREATE (node: label {properties})

Properties of the node or relationship should be included within flower braces { } and node creation should be done within normal braces ( ).

Multiple Nodes:

Multiple nodes in Neo4j Graph Database will be created as shown below.

```
CREATE (node1: label {properties}),
  (node2: label {properties})….
  ……………………………
  (node N : label {properties})
```

The above syntax is followed here for creating the database of multiple routers.

Creating Relationships:

The same CREATE clause is used to create relationship between two nodes. But for establishing such relationship between nodes first the nodes have to be loaded into the database using MATCH command. Once the nodes are loaded then relationship between them can be established as shown below.

```
MATCH (a: p1), (b: p2)
WHERE a.name=” person1” AND b.name=” person2”
CREATE (a)-[r: RELTYPE] -> (b)
RETURN r
```

II) MATCH

MATCH is a reading clause which is used as a mechanism for getting data from Neo4j Graph Database. MATCH clause gets the known data and search for unknown data in the database. It specifies the pattern for which the cypher query needs to search in the database. It gives the starting point in the pattern from that point traversing will be started until it found the desired node which meets the conditions mentioned in WHERE clause.

The syntax of the MATCH clause is shown below:

```
MATCH (node: label)
```

WHERE constraints RETURN node

The above syntax is used for finding the failed router in the database.

III) WHERE

WHERE is not a clause instead it is a part of MATCH clause which adds constraints to the pattern described in the MATCH clause. The sample query which designates the important of WHERE is shown below.

```
MATCH (n)

WHERE n.age<18 RETURN n
```

The above query returns those people who are having age less than 18 years.

IV) RETURN

It is a general clause which tells the user to define which parts of the pattern desired to get as output. The sample query which defines the usage of RETURN clause is shown below.

```
MATCH (a {properties})-[r: KNOWS] -> (b)
RETURN r
```

The above query returns the relationship exist between node ‘a’ and node ‘b’.

IV. METHODOLOGY

The communication in the network passes through various intermediate routers, the failure of single router obstructs the communication passing through it. Since the data was fragmented in the network due to capacity limitations of the link, it will be transmitted through various routers as shown below [10].

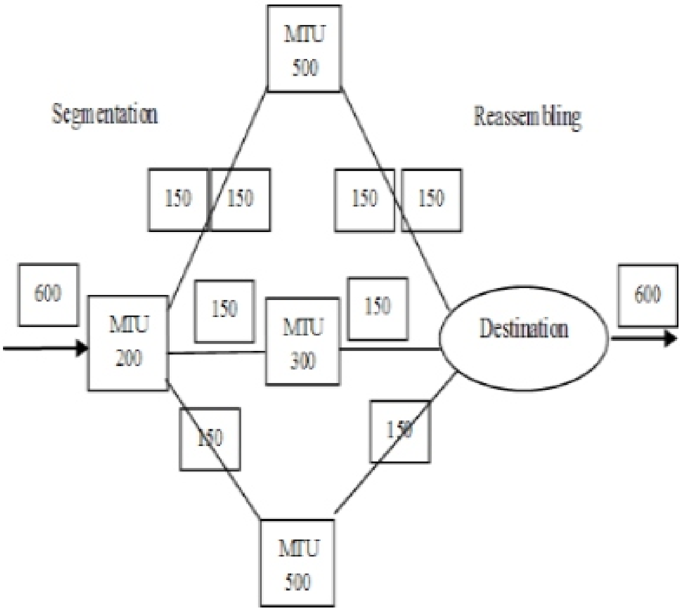


Fig 2. Fragment and Reassemble of Packets in Network.

Once packets are fragmented, reassembling must be done at destination only because of following two reasons:

- Different networks might have different MTU (Maximum Transfer Unit) sizes in that root to destination.
- In the network all the fragments may not follow the same root.

Therefore data or packet transferred through every root was vital in communication process in the network. This is the main reason why the failure of single router breaks the total communication process.

Each router in the network was modeled as a node in the Graph Database and links from router to router are represented as relationships. The white-board friendly nature of Neo4j made it easy to represent entire network as nodes and relationships connected them. In the Neo4j database; information pertains to the router was stored in the form of properties to node. The status of the router which is functioning properly will be indicated with the property “connected“. The status of any router will be changed to the property “disconnected” automatically whenever the specific router fails to working due to any reason. The technique used by Neo4j to query such information from the database is “traversing”.

The execution of cypher query starts from the node with label "router" and traverses node by node for checking whose status property was "disconnected". Once it founds the node it will return it along with all its properties to troubleshoot the specific router instead of checking all the routers in the network.

V. TEST DATA

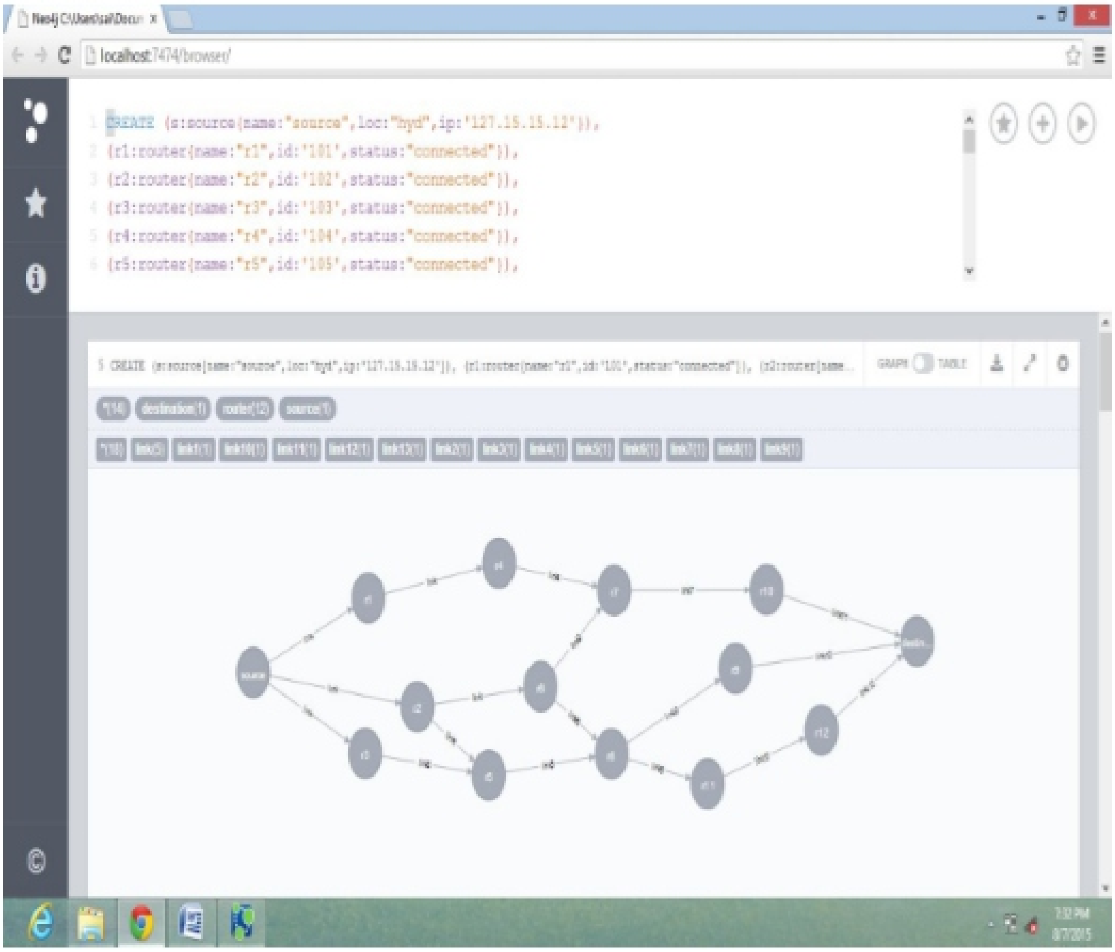
The test data of 12 routers have taken with one source and destination which formed as a small network. Information about all these routers in the network and their connections was stored in the Neo4j Database. The following table represents all the routers and their connections.

TABLE I. ROUTERS AND THEIR LINKED ONES

Router	Linked To
R1	Source, R4
R2	Source, R5,R6
R3	Source, R5
R4	R7
R5	R8
R6	R7,R8
R7	R10
R8	R9,R11
R9	Destination
R10	Destination
R11	R12
R12	Destination
R1	Source, R4

The following query used to create a network in Neo4j Graph Database with 14 nodes and 17 Relationships.

```
CREATE
(s:source{name:"source",loc:"hyd",ip:'127.15.15.12'}),
(r1:router{name:"r1",id:'101',status:"connected"}),
(r2:router{name:"r2",id:'102',status:"connected"}),
(r3:router{name:"r3",id:'103',status:"connected"}),
(r4:router{name:"r4",id:'104',status:"connected"}),
3(r5: router {name:"r5", id:'105', status:"connected"}),
(r6: router {name:"r6", id:'106', status:"disconnected"}),
(r7: router {name:"r7", id:'107', status:"connected"}),
(r8: router {name:"r8", id:'108', status:"connected"}),
(r9: router {name:"r9", id:'109', status:"connected"}),
(r10: router {name:"r10", id:'110', status:"connected"}),
(r11: router {name:"r11", id:'111', status:"connected"}),
(r12: router {name:"r12", id:'112',
status:"connected"}),
 (d:destination{name:"destination",loc:"america",ip:'2
 45.115.152.75'}),
(s)- [: link] -> (r1),
(s)- [: link] -> (r2),
(s)- [: link] -> (r3),
(r1)- [: link] -> (r4),
(r2)- [: link] -> (r6),
(r2)- [:link1] -> (r5),
(r3) - [:link2] -> (r5),
(r6)- [:link3] -> (r7),
(r4)- [:link4] -> (r7),
(r5)- [:link5] -> (r8),
(r6)- [:link6] -> (r8),
(r7)- [:link7] -> (r10),
(r8)- [:link8] -> (r11),
(r8)- [:link9] -> (r9),
(r11)- [:link10] -> (r12),
(r10)- [:link11] -> (d),
(r12)- [:link12] -> (d),
(r9)- [:link13] -> (d)
RETURN s,d,r1,r2,r3,r4,r5,r6,r7,r8,r9,r10,r11,r12
```



```
CREATE (s:source{name:"source",loc:"hyd",ip:'127.15.15.12'}),
(r1:router{name:"r1",id:'101',status:"connected"}),
(r2:router{name:"r2",id:'102',status:"connected"}),
(r3:router{name:"r3",id:'103',status:"connected"}),
(r4:router{name:"r4",id:'104',status:"connected"}),
(r5:router{name:"r5",id:'105',status:"connected"}),
```

```
$ CREATE (s:source{name:"source",loc:"hyd",ip:"127.15.15.12"}), (r1:router{name:"r1",id:'101',status:"connected"}), (r2:router{name...
```

Fig 3. Output of the Created network in Neo4j Graph Database.

Each node in the database is having the following properties:

Name: specific name assigned to router as R1, R2, etc. These names are displayed on the nodes in the created Neo4j Graph Database.

Id: each Router is having unique id. Since every router is having unique id troubleshooting can be done very quickly.

Status: indicates whether the router is functioning properly or not.

The output of the above query is the database which was represented in the form of network structure as shown below. The following Figures shows both query and network in the Neo4j.

Each node will be represented as one table along with its labels and properties. The above graph was represented in the form of table as shown below.

TABLE II. TABLE FORMAT OF ABOVE GRAPH DATABASE

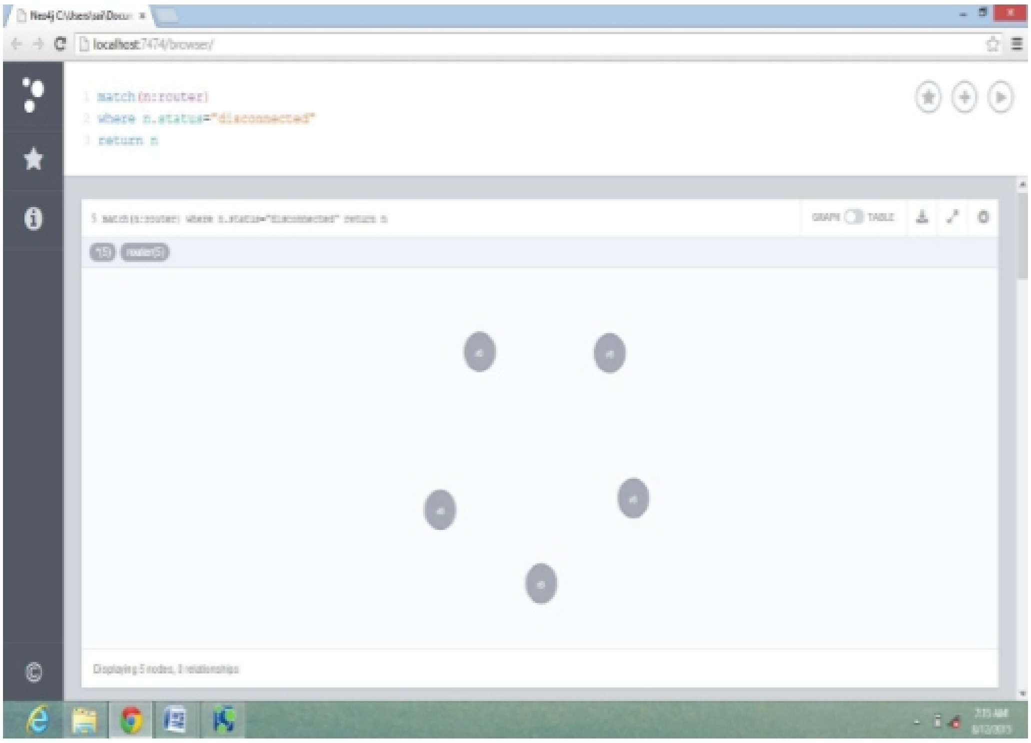
SNo	Name	ID	Status
1	R1	101	Connected
2	R2	102	Connected
3	R3	103	Connected
4	R4	104	Connected
5	R5	105	Connected
6	R6	106	Disconnected
7	R7	107	Connected
8	R8	108	Connected
9	R9	109	Connected
10	R10	110	Connected
11	R11	111	Connected
12	R12	112	Connected

Fig 5. Output Showing The Failed Routers R6, R8, R5.

Case 3: Five Routers Failure

The following Figure 6 depicts the output of 5 failure routers.

Due to the ease of representation [12] using Neo4j Graph Database both the searching time and troubleshooting time are reduced exponentially.



```
match(n:router)
where n.status="disconnected"
return n
```

```
$ match(n:router) where n.status="disconnected" return n
```

Displaying 5 nodes, 0 relationships

Fig 6. Output Showing The Failed Routers R6, R9, R8, R5

CONCLUSIONS

Since the practical proofs presented above clearly depicts the information of failed routers, Neo4j Graph Database along with its specific query language gives accurate results regarding root cause analysis. Different variations of the output in different cases which are presented in previous sections are sufficient to say that Neo4j Graph Database is the suitable and optimal source to deal root causes in network failures.

FUTURE WORK

So many network issues are there to be solved like shortest path problem, counting the number of hops from source to destination, etc. Using the path finding queries through cypher it will become handy to deal any network related issue. Since Neo4j Graph Database supports JSON and CSV file formats this work is extended to solve few more network related issues in future by getting the sample data from real world scenarios. Importing such supported file formats will provide the facility to view and analyze the real world data.

Some kinds of network failures have been studied in which heterogeneously connected networks are vulnerable to targeted attack at hubs and also at edges linking them together. The methods proposed in the present paper will also be used effectively in those situations, since it is possible to assign properties to both the routers and the edges, this will be helpful in finding the break downs of the router or the edge there by robustness can be achieved.

REFERENCES

[1] Pallavi Madan, Anuj Saxena, "Review: Graph Databases" IJARCSSE, volume 4, issue 5 may 2014.

[2] Darshana Shimpi, Sangitha Chaudhari, "An Overview Of Graph Databases", International Conference in Recent Trends in Information Technology and Computer Science (ICRTITCS-2012).

[3] http://nosql-database.org/

[4] Chad Vicknai, Michael Macias, Zhendong Zhao, Xiaofei Nan, Yixin Chen and Dawn Wilkins, "A Comparison of a Graph Database and a Relational Database", ACMSE '10, April 15-17, 2010, Oxford, MS, USA.

[5] Ian Robinson, Jim Webber & Emil Eifrem O'reilly Complements of Neo Technology "Graph Databases".

[6] www.neotechnology.com.

[7] Robert McColl, David Ediger, Jason Poovey, Dan Campbell David A.Bader, "A Performance Evaluation of Open Source Graph Databases", published to ACM, Februrary 16, 2014 Orlando, Florida, USA.

[8]Justin J.Miller, "Graph Database Applications and Concepts with Neo4j", Proceedings of the Southern Association for Information Systems Conference, Atlanta, GA, USA March 23rd-24th, 2013.

[9] http://neo4j.com/docs/stable/cypher-query-lang.html.

[10] http://www.linktionary.com/f/fragmentation.html.

[11] Neo4j. Home. http://neo4j.org, 2012.

[12] www.it-ebooks.ingo/ Learning Neo4j.

Intelligent Platform Integrating Social Networking Applications

[1] Saad. B. Alotaibi, [2] Mohamed- Foued. Sriti, [3] Amer. S. Alharthi

KACST, IMAM University, KACST

Email: [1]sbalotaibi@kacst.edu.sa , [2]sritia@gmail.com , [3]aharthi@kacst.edu.sa

ABSTRACT

The popularity of the social networking applications increases day after day. These applications propose to the users disparate services, that's what drives the users to deal with an important number of these applications. This situation makes difficult to the users to check the updates in their social network and to maintain their social relationship with other users. In this context, we propose SNAI (Social Networking Application Integration) platform for unifying access to different social networking applications and build Ontology using a semantic web for represent data and relationship.

Keywords: SNAI, Ontology, SNAs, Semantic

I. INTRODUCTION

The social networks is represented by different processes of communication and connection between people which can lead to create social relationships between them. The social network structure it is depend on three major attributes: User, Relationship, and Network [1].The social network applications have become a part of life for the most people. Recently, social network applications have abounded, and users are owning at least one account if different applications.

With the large number of social network applications, the user cannot manage and review updates of all his accounts. As a result, there will be some messages aren't read or are read but aren't responded. In addition, the user will take a lot of time and effort to access on all accounts and review all updates. On the other hand, in social network applications the government organizations cannot monitoring all messages between users for any reasons such as security reasons.

Therefore, in this paper we proposed a solution for this problem. The solution is a build platform from scratch for integrate all social network applications in one application. This platform help users to manage different social networks applications accounts using a single access point. In addition, the platform has multi functions and different applications. We build the platform to be easily extensible by adding new functionalities and we prove this by developing two applications based on this platform, the first application is a social network relationship representation, the second application is a text analyzer and user behavior detection.

II. RELATED WORK

Existing social platforms are designed for day-to-day activities. That is, the functionalities provided by these systems are centered on daily contacts activities and are not able to provide statistics on the different exchanges between the users an its contacts that shows the evolution extent of their relationships. Even if we suppose that social applications provide such analysis, users cannot take a direct benefit from them since they are not interoperable and did not provide a unified view of the provided analysis [2] [3].

The most available platform focused on integration some of social network applications in one application to see all updates of all social network applications, some of platforms focused on integration of social network application accounts in one account to reduce using the computer CPU in order to reduce update requests from the server [4].

In addition, some researchers focused on integration of social network applications to unify the friends, as an example save the important friends in the favorite list [5]. Finally, all the projects that we have seen, are focusing on a specific function. In other word, after they integrate some of social network applications, they platform provide one function, for example, reduce the update request, load the important friends, send message from one account and so on.

On the other side, our platform able to integrate with any new social network application and add new features such as relationships representation between friends and text analysis or any needed features.

III. SNAI PLATFORM

SNAI platform is a several systems under one name. The main idea of SNAI platform is an integration of many social network applications in one application. After the integration process, the user can access to all social network accounts by single access point, then he can browse all updates in one page (SNAI Wall) see (figure1) the SNAI wall arrange events of social network applications based on event time. In addition to integrate of SNAs the platform it contains many subsystems such as analysis of social relationships between users and show the relation weakness or strength with other users. Moreover, our platform has subsystem to analysis of texts that exchange between users. This platform is characterized by the ability to install an additional new subsystem. Also, our platform provide a high level of security such as encrypt the login information.

Figure 1: SANI Wall

To integrate the social network application, we need API keys of SNAI platform to use it in authenticate our platform for accounting purposes. In addition to API keys we need user access token for each SNAs for authorize SNAI platform to access the user data, the following diagram describe how to get user keys (cf. figure2).

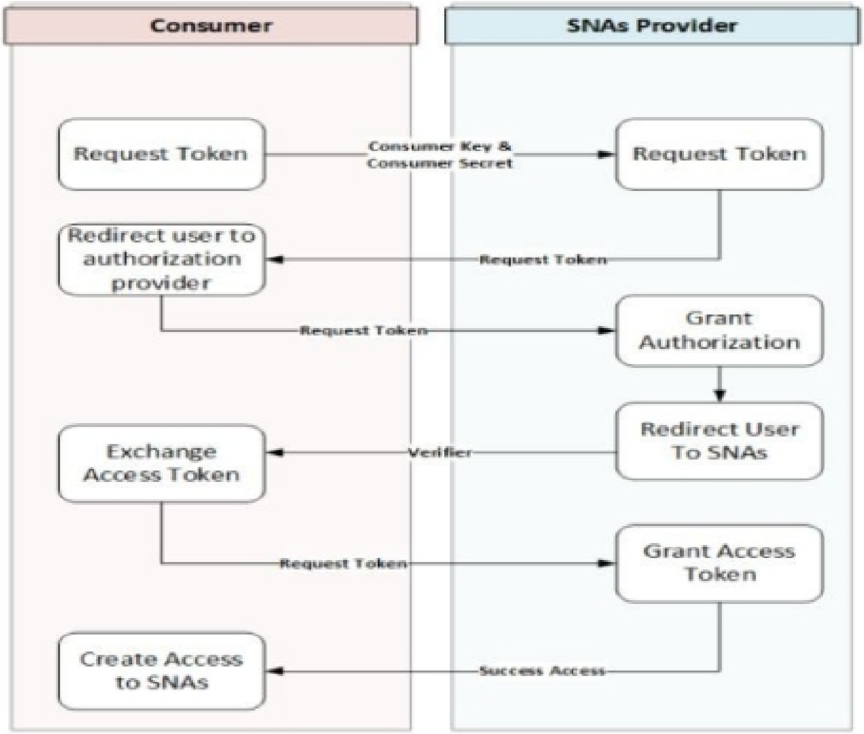


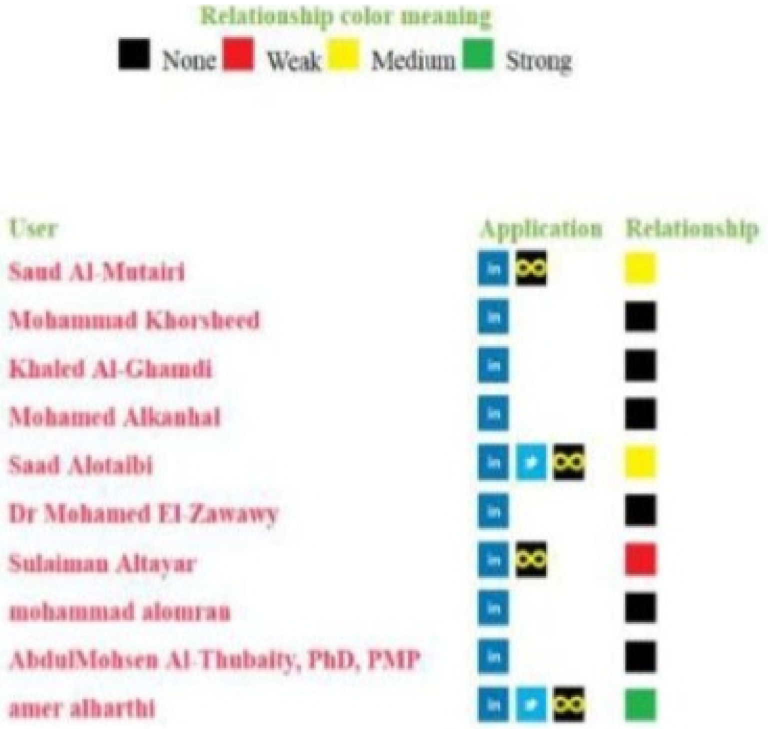
Figure 2: user access token

IV. HELPFUL HINTS

A. RELATIONSHIP REPRESENTION

The SANI platform save the users data in ontology for represent the relationship between the users. This ontology has several elements including message, date of message, sender and receiver. The ontology methodology is save all the daily date when the user browse SNAI account. We develop algorithm to extract and analysis the data from our ontology. To identify the relationship between the user with his friends the algorithm calculate the number of connections (messages, comments, etc.) for each friend, the following figure show the relationship result (cf. figure 3).

After we get the relationship strength (none, weak, medium and strong), we need to determine type of relationship (Positive / Negative). In next section (text analysis), we will explain how to get the type of relationship.



Relationship color meaning

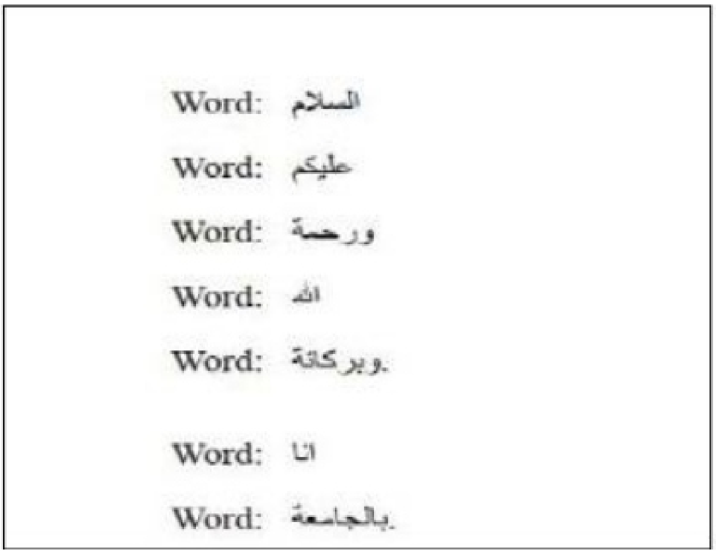
⬛ None 🟥 Weak 🟨 Medium 🟩 Strong

User	Application	Relationship
Saud Al-Mutairi	in ∞	🟨
Mohammad Khorsheed	in	⬛
Khaled Al-Ghamdi	in	⬛
Mohamed Alkanhal	in	⬛
Saad Alotaibi	in 🐦 ∞	🟨
Dr Mohamed El-Zawawy	in	⬛
Sulaiman Altayar	in ∞	🟥
mohammad alomran	in	⬛
AbdulMohsen Al-Thubaity, PhD, PMP	in	⬛
amer alharthi	in 🐦 ∞	🟩

Figure 3: Relationships Result

B. TEXT ANALYSIS

After extracting the data from ontology, we analyze the text on three steps. First step, we convert the sentences into words to make a more accurate analysis (cf. Figure 4).



Word: السلام

Word: عليكم

Word: ورحمة

Word: الله

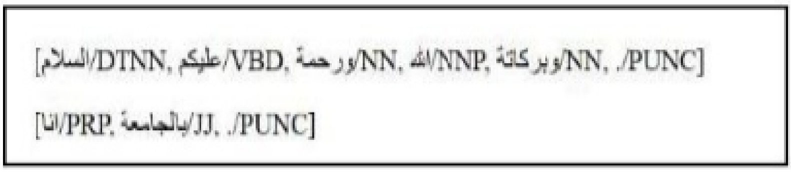
Word: وبركاته.

Word: انا

Word: بالجامعة.

Figure 4: Sentences converter

The second step, the algorithm remove prefix and suffix of the word, as a result we obtain on root of word. Third step, we use the Stanford tagger[6] to identify the word type such as Verbs, Adjectives or Nouns (cf. figure 5), that will determine type of relationship based on positive/negative words using SNAI dataset. The SNAI dataset contain most of the positive and negative words.



[السلام/DTNN, عليكم/VBD, ورحمة/NN, الله/NNP, وبركاته/NN, ./PUNC]

[انا/PRP, بالجامعة/JJ, ./PUNC]

Figure 5: Word tag

CONCLUSIONS AND FUTURE WORK

In SNAI platform, the social network applications will be integrated in one application that make it easy to capture the distributed social data, to reconcile objects (contact, community, media, etc.), and to summarize the social network activities (by performing preliminary analysis and providing statics on contacts activities). The SNAI help the user to manage all social network accounts by one account (SNAI account). In addition, the platform provide multi functions and different subsystems depends on our needs. Also, the SNAI infrastructure allow us easily to add new function of new subsystem. Finally, the SNAI platform saving the data of social network applications in the ontology to represent data and relationship.

In the future work we will develop SNAI platform for mobile phone (android and Apple IOS).

REFERENCES

[1]. A. M. a. B. Wellman, "Social Network Analysis: An Introduction1," Department of Sociology, University of Toronto , Canada, 2009.

[2]. T. R. M. C. a. V. A. Fabrício Benevenuto, "Characterizing User Behavior in Online Social Networks," ACM, Chicago, Illinois, USA, 2009 .

[3]. Y. W. a. J. V. Jie Zhang, "SocConnect: Apersonalized soical network aggregator and recommender," Elsevier Ltd, Singapore, 2012.

[4]. A. K. Hamid Mcheicka, "Collaborate Social Network Services via Connectors," in The 3rd International Conference on Ambient Systems, Networks and Technologies , Canada , 2012.

[5]. J. Z. a. J. V. Yuan Wang1, "SocConnect: Intelligent Social Networks Aggregator," Department of Computer Science, University of Saskatchewan, Canada School of Computer Engineering, Nanyang Technological University, Singapore, 2009.

[6]. K. Toutanova, "Stanford University Tagger," 20 4 2011. [Online].Available: http://nlp.stanford.edu /software/tagger.shtml.

Energy Aware Localization in Wireles Sensor Network using Lusa

[1] Prangya Paramita Panda, [2] Sibani Senapati

[1]Computer science & Engineering Department

[2]Electronics & communications Engineering Department

E-mail: [1]paramita.prangya1@gmail.com, [2]kunisenapati@gmail.com

ABSTRACT

The technique of finding physical co-ordinates of a node is known as localization Importance of localization arises from the need to tag the sensed data and associate events with their location of occurrence. Location information of a sensor node can be obtained by using GPS. But, installing GPS in every node is not a feasible solution. This is because: (i)sensor nodes are deployed in a very large number. Installing GPS at every node will increase the cost as well as size, (ii) GPS consume power, which will effect the network lifetime. Moreover, location cannot be pre-programmed as it is un- known where nodes will be deployed during their operational phase.In this thesis, we have made an attempt to address localization in static sensor networks. For static network we have proposed distributed range based localization techniques called (i) Localization using a single anchor node (LUSA), this technique is proposed for grid environment. In LUSA, we have identified three types of node: anchor, special an unknown node. For every anchor node there exists two special node and they are placed perpendicular to the anchor node. Localization in LUSA is achieved by a single anchor node and two special nodes. Localization occurs in two steps. First special nodes are localized and then the unknown nodes. We have compared LUSA with a closely related localization technique called Multi-duolateration(MDL). It is observed that the localization error and localization time is lesser in LUSA. This not only reduces the localization time but also the dependency.

Key words- Multi-Duolatertion(MDL), LUSA, beacon node ,Settled node.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) has become an emerging area of interest among the academia and industry in the last one decade [1,2,3,4]. It consists of a large number of densely deployment nodes which are tiny, low power, in-expensive, multi-functional and have limited computational and communication capabilities. These nodes interact with their environment, sense the parameters of the interest such as temperature, light, sound, humidity, and pressure; and report it to the sink node/base station. Deployment of WSN may vary from a controlled indoor environment to a remote and inaccessible area. Therefore, a sensor node is configured with necessary extra components for on-board limited processing ability, communication, and storage capabilities.

1.1 Key Issue:

In Wireless Sensor Networks Some of the important issues in WSNs are stated below :

(I) Energy Efficiency: Sensor nodes have limited battery capacity. This puts a constraint for other applications and on the lifetime of sensor node. Major sources of battery drainage include: (i) continuous sensing, (ii) transmission and reception modes of radio. Therefore, to increase the lifetime in unattended environments, efficient algorithms should be developed at each layer of WSN in concern with the less energy utilization. This includes techniques of data compression, data fusion (removal of data redundancy), rotation of cluster heads, and adaptive mechanisms for radio operations [5].

(ii) Localization : For robust WSN, localization of nodes is one of the most important issue. Information sensed by a sensor node becomes useful only when its geographical location is tagged. Geographical routing is possible only after the localization, and other issues like spatial querying and load balancing can also be achieved [6].

1.2 Motivation

Data gathered by a sensor node is usually reported to the sink for necessary action. For initiating a prompt action the sink must be aware of the location information of the reporting node. For example, assume that fire has occurred in some part of the forest and a near by sensor report this information to the sink. For quick response, the reporting sensor should include its location along with other information. Tagging of location stamp along with the sensed information is possible only when the reporting node is localized. This signifies the importance of localizing a node prior to its data collection process. A few applications indicating the importance of localization in WSNs is listed below:

(I) Sensors gather vital security related parameters such as radio communication, vigorous movements in an surveillance area, and report these to the back-end security system(a sink node). A prompt action by security personnel is possible only if location information is provided with the sensed information.

(ii) On some occasions, some nodes may die due to the battery drainage or by physical forces. In such cases, new nodes to be injected or battery replacements can be achieved efficiently by adopting geographic routing rather than physical routing schemes .Geographic routing eases task of locating a faulty node as compared to physical routing.

(iii) Location information is also used to divide the WSN into different clusters to facilitate collaborative processing and hierarchical routing. For each cluster, one node is taken as cluster head which remains responsible for cluster interconnectivity and state maintenance. Sensor networks is like a distributed database for users to query the physical world for useful information. With localization, efficient spatial querying by a sink or a gate way node is responded only by the intended sensor node.

(iv) Location based routing saves significant energy by eliminating the need for route discover and improve caching behaviour for applications where requests are location dependent. Determining the quality of coverage of all active sensors using their position.

1.3 Problem statement

Sensor nodes are low cost devices. Use of GPS to obtain location information will increase their cost. An alternative to the use of GPS is to obtain location information through localization algorithms. Use of localization algorithms mandate the deployment of a few location aware node. The remaining nodes are localized with the help of these location aware nodes. The objective of this paper includes: (i) Localization using lesser number of location-aware nodes.(ii) Develop a localization algorithm with no extra hardware cost.(iii) Reduce the localization error, and localization time

II. LOCALISATION USING SINGLE ANCHOR NODE [LUSA]:

Localization of nodes in a sensor network is essential for the following two reasons: (i) to know the location of a node reporting the occurrence of an event, and (ii) to initiate a prompt action whenever necessary. Different localization techniques have been proposed in the literature. Most of these techniques use three anchor nodes for localization of an unknown node. Increasing the number of anchor nodes will increase the overall cost of WSN. This is because GPS enabled nodes need frequent battery replacements or a battery of large capacity. Furthermore, GPS does not work well in indoors and dense areas/forests .Localization techniques also differ from environment to environment. In this chapter, we proposed a localization technique for grid environment. Sensor nodes are deployed in a grid pattern and localization can be achieved using a single location aware or anchor node.

2.1 Proposed Technique

In this section, we proposed a distributed range based localization algorithm for a grid environment. Since, a single anchor node is used for localization, we call this technique as localization using single anchor node (LUSA). We made the following assumptions:

(a) Sensors are deployed in a grid pattern as shown in Figure (a).

(b) We identify three types of node: (i) Beacon node: A node which can locate its own position, and is usually equipped with GPS, (ii) Special node: Nodes which are perpendicular to the beacon node, and can determine their co-ordinates with respect to beacon node. For every beacon node there exist two Special nodes, (iii) Unknown node: Nodes which are un- aware of their location.

They use localization algorithm to determine their position. Special nodes are treated as unknown nodes.

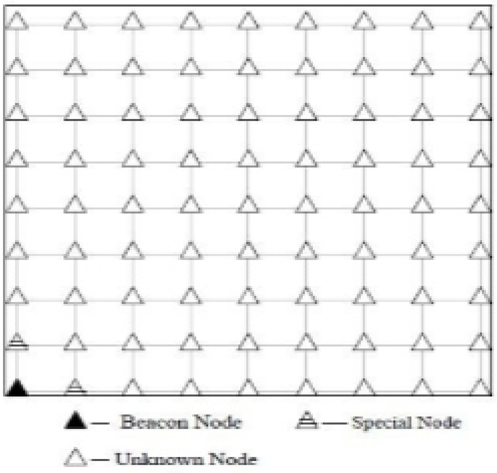
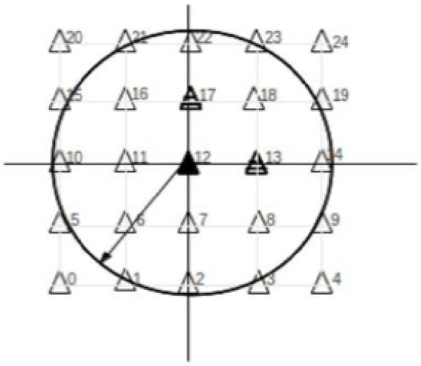
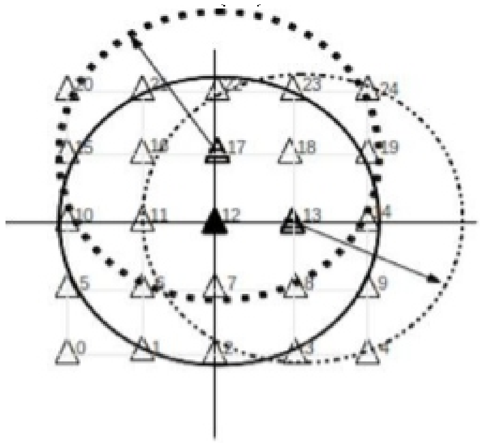


Figure (1): Deployment of Beacon node, Special node and Unknown node in a grid

For localization, the beacon node initially broadcast its location information. Special nodes compute their distance from the beacon node using RSSI and determine their co-ordinates with respect to the beacon node. After computing their location information, Special nodes also act as beacon node. Unknown nodes use trilateration mechanism to compute their location information .Scheme using Figure-(2.a), (2.b). Let node 12 in the figure is a beacon node, node 13 and 17 are Special nodes, and the remaining nodes are unknown nodes. Initially, node 12 broad-cast its position. This is received by the special nodes 13 and 17 along with other unknown odes within the transmission range of node 12 as shown in Figure-(2.a). Nodes 13and 17 calculate their distance with respect to node 12, and localize themselves. At this stage all the nodes within the transmission range of node 12 has the position estimate of beacon node 12. In next stage, node 13 and 17 act as beacon nodes and broadcast the estimated position, as shown in Figure-(2.b), which is received by nodes 7, 8, 11, 14, 18,22, and 23. These nodes localize themselves using trilateration[7,11] . As more and more nodes gets localized, they act as beacon nodes. Above process continues until the whole network is localized. Figure-(3) shows the progress of localization in the proposed scheme in a 9x9grid environment. Nodes encircled with same numerical value are likely to get localized at the same time instant.



(2.a)



(2.b)

Figure (2.a) , (2.b): Localization using LUSA

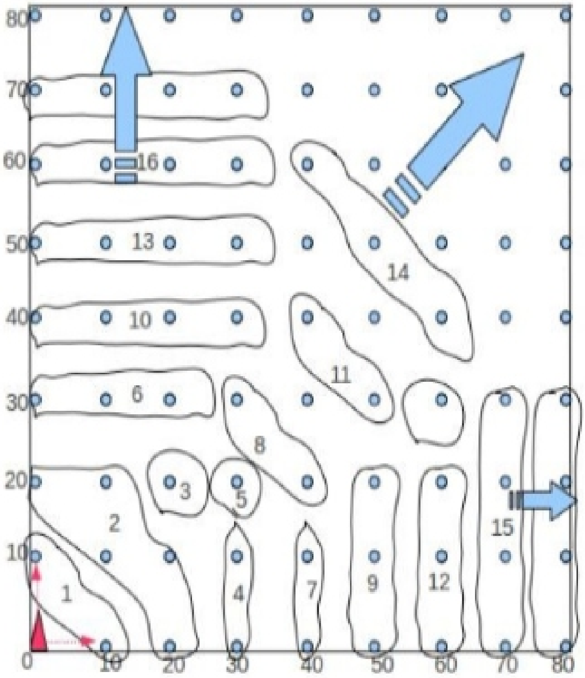


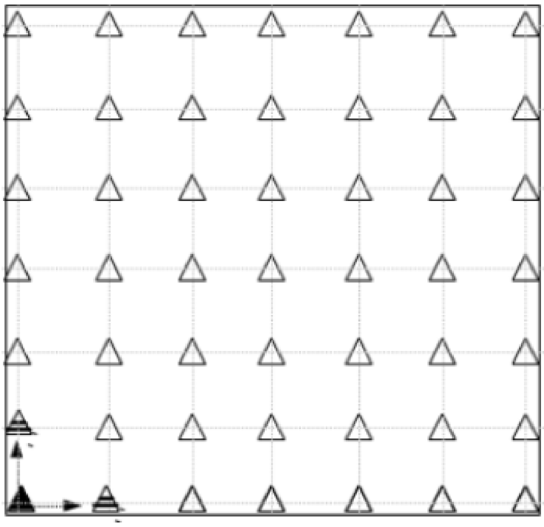
Figure (3): Localization pattern

2.2 Simulation Results:

We have simulated the proposed scheme using Castalia simulator that runs on top of C- Omnet++. Transmitting power of nodes is considered to be -5 dBm (0.316 mW) so as to limit the communication range to 30 meters, and the path loss coefficient (η) to be 2:4. A grid network of size 9 x9 is considered for simulation. Metrics of interest are: (i) Localization time; and (ii) Localization error - which is computed as described below.

Where θ is estimated position, θ_i is actual position, N is the total number of sensors in the Network and R is number of beacon nodes. We have considered the following two scenarios:

$$Error = \frac{\sum_{i=1}^{N-R} |\widehat{\theta_i} - \theta i|}{N-R}$$



Figure(4):Beacon node at the corner of grid

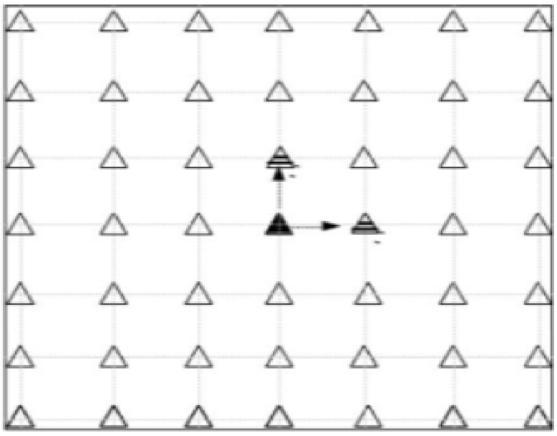
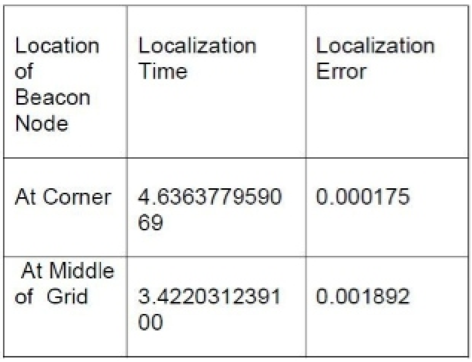


Figure (5):Beacon node at the middle of grid

Solar cells are the basic components of photovoltaic panels. Most are made from silicon even though other materials are also used. Solar cells take advantage of the photoelectric effect: the ability of some semiconductors to convert electromagnetic radiation The time for localization and the average localization error in the above two scenarios is shown in Table-III. It is observed from the Table - III, that localization error when the beacon node is at the corner of grid is lower in comparison to placing at the center of the grid.

Table II.I :Evaluation of proposed algorithm, placing the beacon node at two different places within the network.



Location of Beacon Node	Localization Time	Localization Error
At Corner	4.636377959069	0.000175
At Middle of Grid	3.422031239100	0.001892

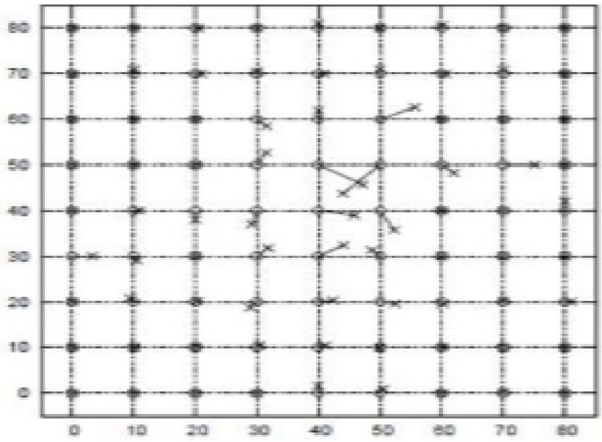


Figure (6.a)

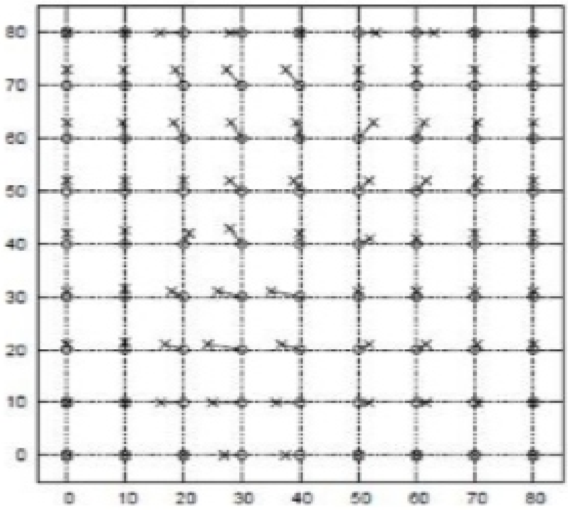


Figure (6.b)

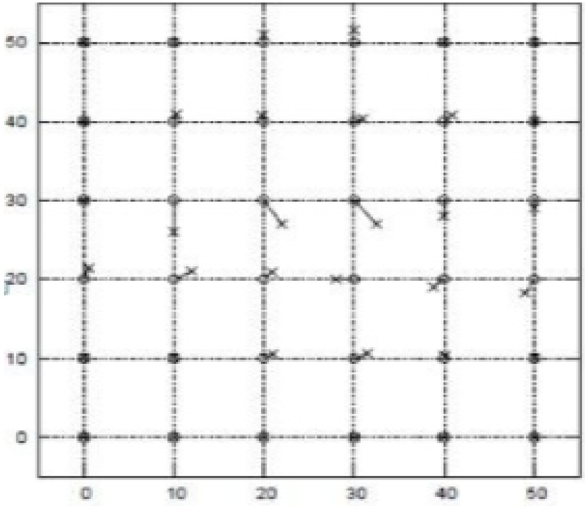
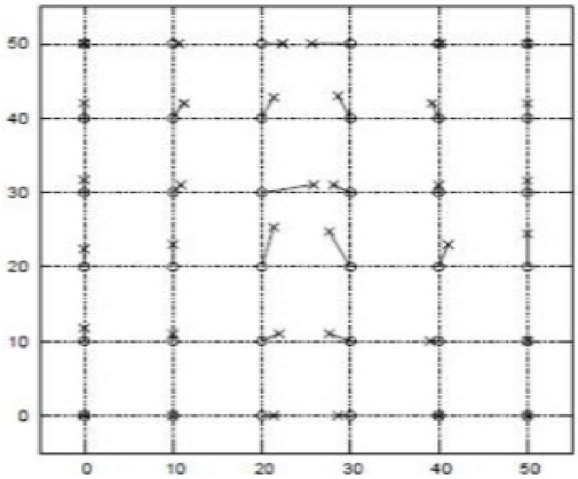
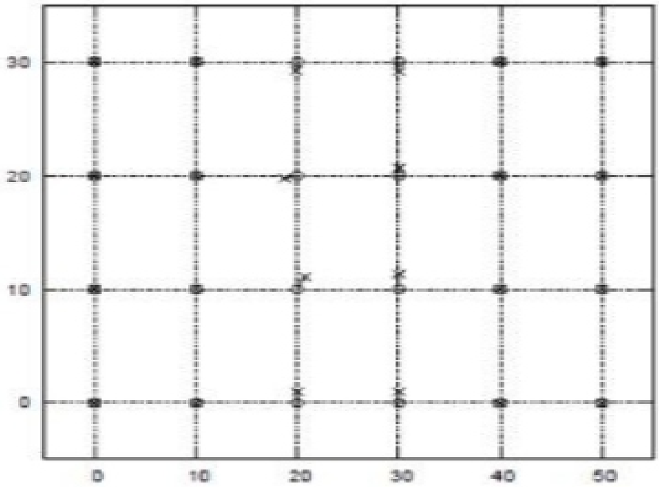


Figure (6.c)



Figure(6.d)



Figure(6.e)

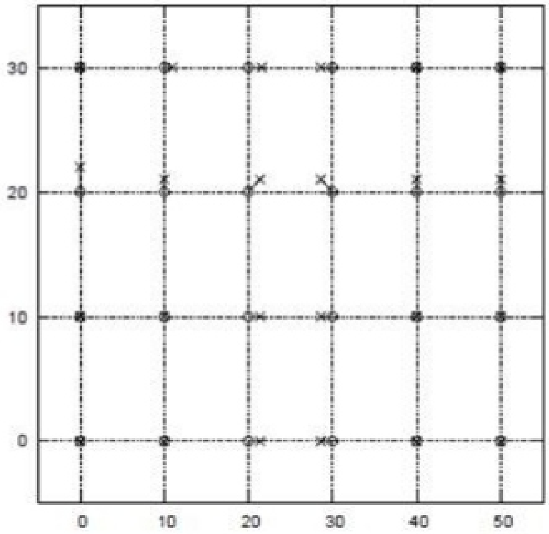


Figure (6.f)

Figure(6): Distribution of localization error without interference in LUSA and MDL

Next, we have compared LUSA with Multi- duolateration (MDL). This is because MDL closely resembles with LUSA. MDL is proposed for a grid environment. It works using internal division. First, it localizes the edge nodes and then the remaining surface nodes. In MDL, four beacon nodes are placedat the four corners of the grid. For comparison with MDL, we also placed four beacon nodes at the four corners of the grid in LUSA. Metrics considered for comparison are localization time and localization error. a two scenarios:(i)without interference, and (ii) with interference; and the following grid sizes: (i) Square grid of size:9x9, and 6 x6, and (ii) Rectangular grid of size: 6 x4, for comparison.

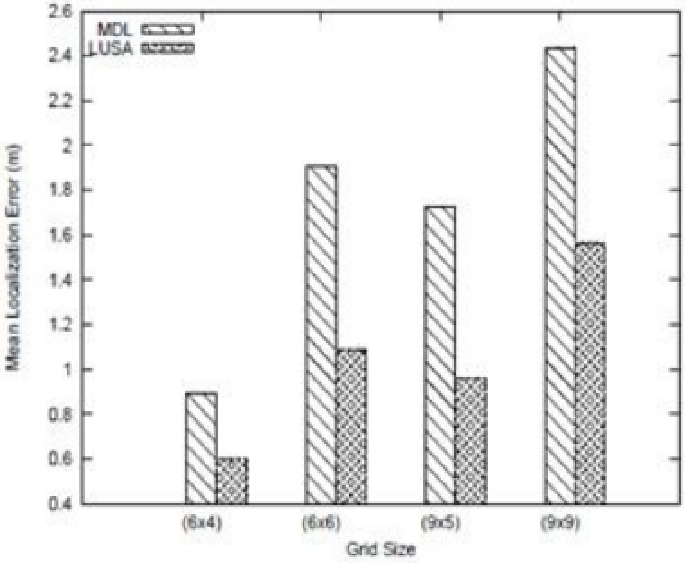


Figure (7.a)

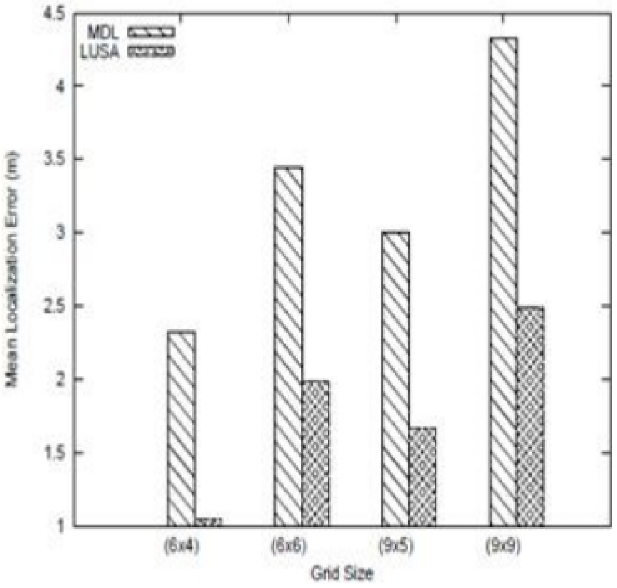


Figure (7.b)

Figure 7: Mean localization error (meters) in various grid: (a) Without interference (b)With interference.

2.3 Localization Error

The geographical distribution of error without interference in LUSA and MDL for different grid size is shown in Figure - 3.6. Distribution of error in LUSA is shown in Figure 6(a),.6(c), 6(e) and MDL in Figure-6(b), 6(d), 6(f) for grid size of 9x9, 6x6, and 6x4 respectively. In each figure dot '.' represents actual position of node and symbol 'x' represents corresponding estimated position. The line joining '.' and 'x' represents the magnitude of error. From Figure-.7, it is observed that LUSA has lower localization error than MDL. Higher localization error in MDL is attributed to the localization of surface nodes. Each surface node localize itself on the basis of four nearest edge nodes (left, right, above, below) using internal division. Localization of each surface node is independent of other surface nodes and depends solely on the edge nodes. Therefore, if any of the edge node do not get its exact location, it affects the location estimation of all surface nodes making use of that edge node for location estimation. We have shown the mean localization error in the corresponding grids for LUSA and MDL in Figure-7.

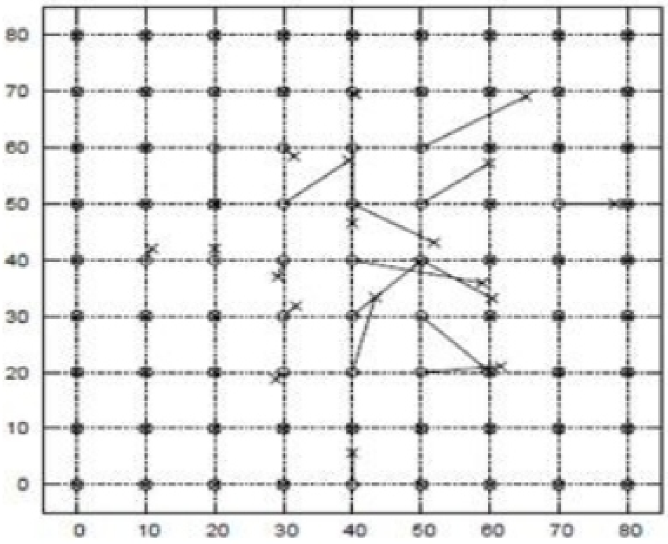


Figure (8.a)

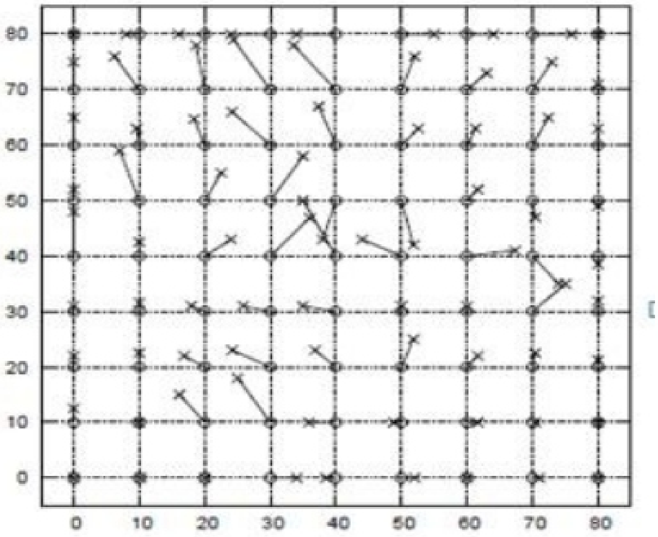


Figure (8.b)

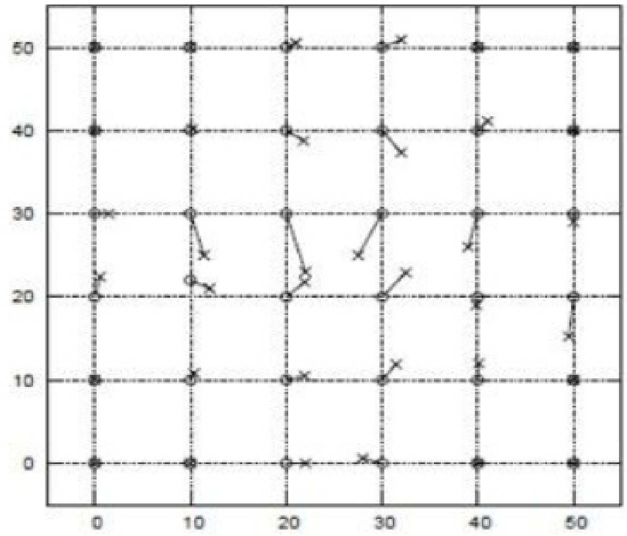
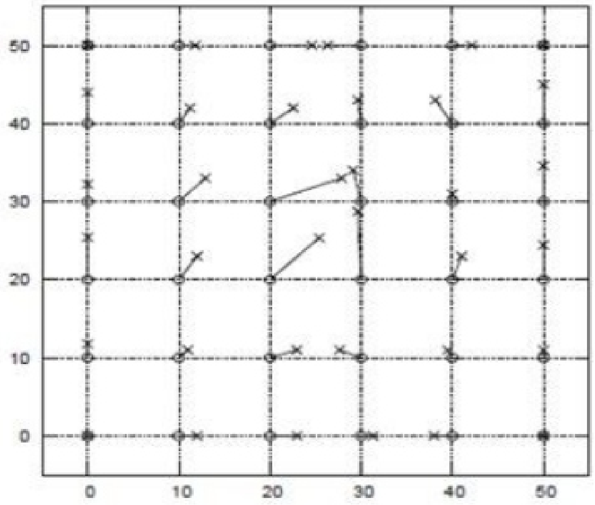
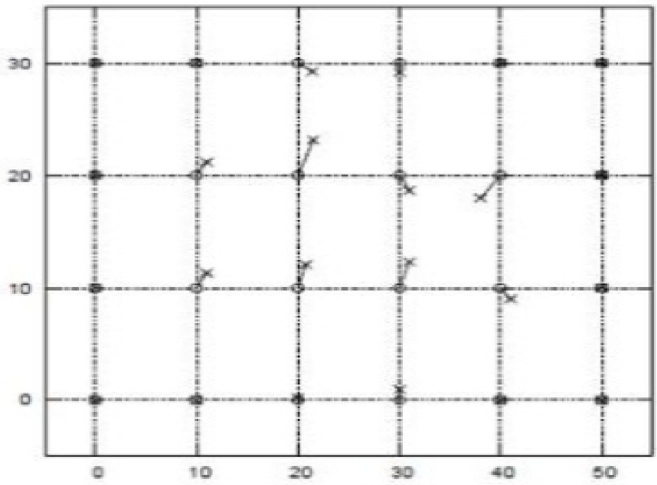


Figure (8.c)



Figure(8.d)



Figure(8.e)

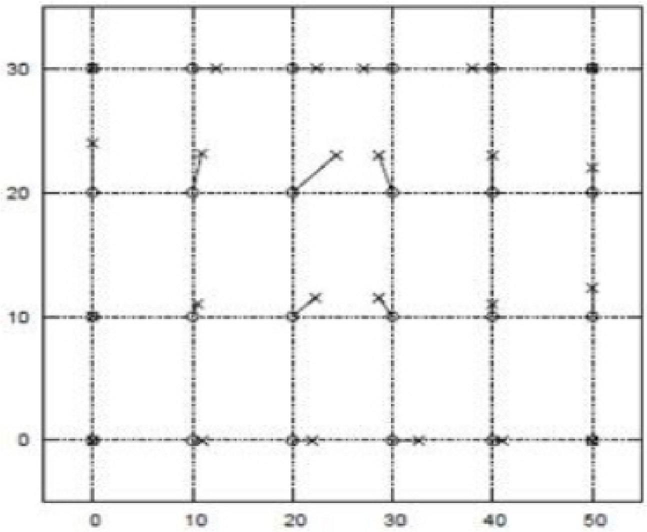


Figure (8.f)

Figure 8: Distribution of localization error with interference in LUSA and MDL

Next, we consider the effect of interference on location estimation. Effect of interference in LUSA and MDL is shown in Figure-8 where Figures-8(a), 8(c), 8(e) corresponds to LUSA and Figures8(b), 8(d), 8(f) corresponds to MDL in a grid size of 9x9, 6x6, and 6x4 respectively. Effect of interference on the localization error in grid of different size is shown in Figure-7(b). It is observed that MDL is heavily affected in the presence of interference as compared to LUSA.

2.4 Localization Time

Localization time of LUSA and MDL for different grid size is shown in Figure-(9). Higher localization time in MDL is attributed to the localization of surface nodes. In MDL localization proceed in two stages: (i) First, it localizes the edge nodes, and (ii) Next, it localizes the remaining surface nodes. In the second stage, each surface node select a reference edge node based on shortest path. This contributes to higher localization time. Whereas, in LUSA, localization of node's proceeds simultaneously and does not put any constraint on the selection of reference nodes9.

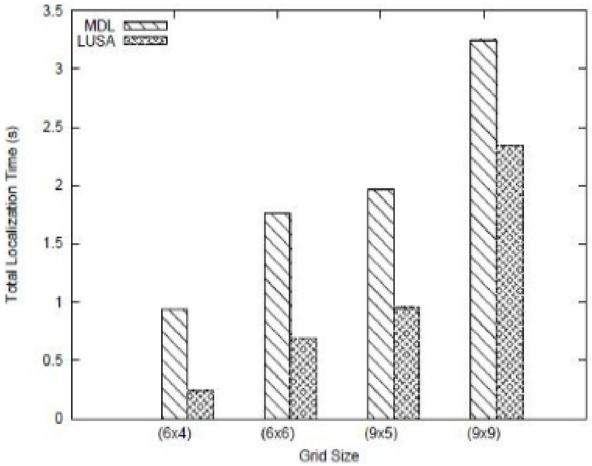


Fig (9): Localization Time

III. CONCLUSION

Localization in wireless sensor networks have received increasing attention over the last one decade. It not only provides the geographical position of a sensor node but also fills the requisite for geographic routing, spatial querying, and data dissemination. With the continuous research in localization of sensor networks, a number of effective algorithms have been proposed, but the stability has not yet reached. This is because of the storage, battery, processor) and the harsh deployment environments. Currently, none of the localization techniques is able to full-fill all these constraints. Most existing localization algorithms for static WSNs were designed to work with at least three anchor nodes except in those cases where directional antenna is used. Usage of antenna not only increases the cost, but also the size of node as well as complexity of the algorithm. As the of anchor nodes required in a network increases, overall cost of the network also increases. In addition, energy drainage of the network increases, but the localization time of the whole network decreases. Further, anchor nodes installed with GPS do not work well everywhere. Therefore, at present we are in the need of a novel technology that will solve problems: (i) reduce the number of required anchor nodes, (ii localize sensor nodes in areas where GPS do not work well, (iii) minimize the localization error.

Localization Using a Single Anchor Node: First, we proposed a technique for localization ,in a grid environment using a single anchor node. It is a distributed, range based technique. In technique ,we classify the nodes into three types. They are: (i) anchor node, (ii) special node and (iii) unknown node. Special nodes localize themselves with respect to anchor node localize with the help of anchor node and special node. We have compared the proposed scheme with a contemporary scheme called Multi-duolateration (MDL) We have observed that the localization time and localization error is smaller in the proposed scheme.

Localization problem in WSNs is not yet fully solved. There are several issues in localization which need further attention. Some of these are(I) Localization accuracy is mostly affected by the ranging techniques used. Each ranging technique in turn is severely affected by the wireless channel behavior in different environments. Therefore, for accurate localization, issues like signal fading, multipath, additive noise etc needs to be addressed. (ii)Error in distance measurement between nodes need to be handled with proper calibration because most of localization algorithms depend on the pair-wise distance.(iii) Not enough work has been drawn on the localization of mobile WSNs. Owing to more battery drainage in mobile networks, a predictive approach for localization can estimate the node location with less number of anchors required.(iv) Localization technique for mobile WSNs needs to be tested in various mobility models .This ensures that each new proposed technique operate properly in real time networks. (v) Furthermore, localization of WSN in certain specific environments like under-water environments has not been explored much.

REFERANCES

[1] I, E., Gu, Y., Bozdag, D.: Mobility-based communication in wireless sensornetworks. Communications Magazine, IEEE 44(7), 56–62 (2006).

[2] B. Zhang and F. Yu. LSWD: Localization Scheme For Wireless Sensor Networks Using Directional Antenna. IEEE Transactions on Consumer Electronics, Nov. 2010.

[3] L. Butty_an, D. Gessner, A. Hessler, and P. Langendoerfer. Application of Wireless Sensor Networks in Critical Infrastructure Protection: Challenges and Design Options. IEEE Wireless Communications, 17(5):44 - 49, 2010.

[4] J. Zheng and A. Jamalipour. Wireless Sensor Networks A Networking Perspective, chapter 13: Sensor Network Standards, pages 407-431. John Wiley and Sons,first edition, 2009.

[5] S. Meguerdichian, S. Slijepcevic, V. Karayan, and M. Potkonjak. "Localized algorithms wireless ad-hoc networks: location discovery and sensor exposure." In ACM Int'l Symp.on Mobile Ad Hoc Networking and Computing (MobiHOC), pp 106–116, 2001.

[6] B. Krishnamachari. Networking Wireless Sensors, chapter 4: Time Synchronization, pages 57-68. Cambridge University, first edition, 2005.

[7] F. Koushanfar, M. Potkonjak, and A. Sangiovanni- Vincentell. Fault Tolerance Techniques for Wireless Ad hoc Sensor Networks. In Proceedings of IEEE Sensors, volume 2, pages 1491-1496,2002.

[8] Y. Liu and Z. Yang. Location, Localization, and Localizability, chapter 7: Localization forMobile Networks, pages 97-109. Springer,first edition, 2011.

[9] R. Nagpal, H. Shrobe, and J. Bachrach. Organizing a Global Coordinate System from Local Information on an Ad hoc Sensor Network. In Proceedings of the 2nd International Workshop on Information Processing in Sensor Networks, ISPN 03, Palo Alto, California, April, 2003.

[10] X. Li, H. Shi, and Y. Shang. A Partial-Range-Aware Localization Algorithm for Ad-hoc Wireless Networks. In Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks, LCN '04, pages 77-83, 16-18 Nov. 2004.

[11] Y. Wang, X. Wang, D. Wang, and D. P. Agrawal. Range- Free Localization Using Expected Hop Progress In Wireless Sensor Networks. IEEE Transactions on Parallel and Distributed Systems, 20(10):1540-1552, Oct. 2009.

[12] S. Simic and S. S. Sastry. Distributed Localization in Wireless Ad-hoc Networks. TechnicalReport UCB/ERL M02/26, EECS Department, University of California, Berkeley, 2002.

[13] J.-P. Sheu, J.- M.Li, and C.-S. Hsu. A Distributed Location Estimating Algorithm for Wireless Sensor Networks. In IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, volume 1 of SUTC '06, pages 21-225, 5-7 June 2006.

[14] J.-P. Sheu, P.-C. Chen, and C.-S. Hsu .A Distributed Localization Scheme for Wireless Sennsor Networks with Improved Grid-Scan and Vector-Based Refinement .IEEE Transactions onMobile Computing, 7(9).

[15] Y. Shang, W. Ruml, Y. Zhang, and M. P. J. Fromherz. Localization From Mere Connectivity .In Proceedings of the 4th ACM international symposium on Mobile Ad-hoc networking and computing, (Mobi Hoc '03), pages 20{212, New York, NY, USA, 13 June 2003. ACM..

[16] T. He, C. Huang, B. Blum, J. Stankovic, and T. Abdelzaher. Range Free Localization Schemesin Large Scale Sensor Networks. In Proceedings of the 9th annual International Conference onMobile Computing and Networking, MobiCom '03, pages 81-95, 14-19 Sep. 2003.

[17] H. Lee, Y. Kim, and H. Chong. Grouping Multi- Duolateration Localization Using PartialSpace Information For Indoor Wireless Sensor Networks. IEEE Transactions on ConsumerElectronics, 55(4):1950-1958, 2009.

[18] S. Zhu and Z. Ding.Distributed Cooperative Localization of Wireless Sensor Networks with Convex Hull Constraint. IEEE Transactions on Wireless Communications, 10(7):2150-2161, 2011.

[19] H. M. Khan, S. Olariu, and M. Eltoweissy. Efficient Single-Anchor Localization In Sensor Networks. In Proceedings Of The Second IEEE Workshop On Dependability and Security in Sensor Networks and Systems, DSSNS '06, pages 35-43, 24-28 April 2006.

[20] P. N Pathirana, N. Bulusu, A. V Savkin, and S. Jha. Node Localization Using Mobile Robotsin Delay-Tolerant Sensor Networks.IEEE transactions on Mobile Computing, 4(3):285-296,May-June 2005.

[21] K.-F. Ssu.-H. Ou, and H. C. Jiau. Localization with Mobile Anchor Points in Wireless SensorNetworks.IEEE transactions on Vehicular Technology, 54(3):1187-1197, May 2005.

[22] Hofmann-Wellenhof, B., Lichtenegger, H., Collins, J.: Global Positioning System:Theory and Practice, 4th edn. Springer, Heidelberg (1997).

[23] Munir, S.A., Ren, B., Jiao, W., Wang, B., Xie, D., Ma, J.: Mobile wireless sensornetwork: Architecture and enabling technologies for ubiquitous computing. In:International Conference on Advanced Information Networking and ApplicationsWorkshops, vol. 2, pp. 113–120 (2007).

[24] H. Rashid, A. K. Turuk, \Distributed Binary Node Localization Estimation Approach", International Journal of Sensor Networks (Inderscience),Springer72(1) 2013.

[25] Amundson, I., Koutsoukos, X., Sallai, J.: Mobile sensor localization and navigationusing RF doppler shifts. In1st ACM International: Workshop on Mobile EntityLocalization and Tracking in GPS-less Environments, MELT (2008).

[26] S.Slijepcevic and M.Potkonjak. Power efficient organization of wireless sensor networks.In IEEE Int'l Conf. on Communications (ICC), pp 472–476, 2001.

[27] H. Rashid, A. K. Turuk, \Localization of Wireless Sensor Networks Using a Single Anchor Node", Wireless Personal communications (Springer), 72(2), 2013.

[28] R. R. Roy. Reference Point Group Mobility. In Handbook of Mobile Ad Hoc Networks forMobility Models, pages 637-670. Springer US, 2011.

[29] C. Schindelhauer. Mobility in Wireless Networks. In Proceedings of the 32nd Annual Conferenceon Current Trends in Theory and Practice of Computer Science, SOFSEM '06, pages 100-116,Berlin, Heidelberg, 2006. Springer-Verlag.

[30] E. M. Royer, P. Michael Melliar-Smithy, and L. E. Moser. An Analysis of the Optimum NodeDensity for Ad hoc Mobile Networks. In IEEE International conference on Communications,ICC, volume 3, pages 857-861, 2001.

Instructions for Authors

Essentials for Publishing in this Journal

1 Submitted articles should not have been previously published or be currently under consideration for publication elsewhere.

2 Conference papers may only be submitted if the paper has been completely re-written (taken to mean more than 50%) and the author has cleared any necessary permission with the copyright owner if it has been previously copyrighted.

3 All our articles are refereed through a double-blind process.

4 All authors must declare they have read and agreed to the content of the submitted article and must sign a declaration correspond to the originality of the article.

Submission Process

All articles for this journal must be submitted using our online submissions system. http://enrichedpub.com/ . Please use the Submit Your Article link in the Author Service area.

-

Manuscript Guidelines

The instructions to authors about the article preparation for publication in the Manuscripts are submitted online, through the e-Ur (Electronic editing) system, developed by **Enriched Publications Pvt. Ltd**. The article should contain the abstract with keywords, introduction, body, conclusion, references and the summary in English language (without heading and subheading enumeration). The article length should not exceed 16 pages of A4 paper format.

Title

The title should be informative. It is in both Journal's and author's best interest to use terms suitable. For indexing and word search. If there are no such terms in the title, the author is strongly advised to add a subtitle. The title should be given in English as well. The titles precede the abstract and the summary in an appropriate language.

Letterhead Title

The letterhead title is given at a top of each page for easier identification of article copies in an Electronic form in particular. It contains the author's surname and first name initial .article title, journal title and collation (year, volume, and issue, first and last page). The journal and article titles can be given in a shortened form.

Author's Name

Full name(s) of author(s) should be used. It is advisable to give the middle initial. Names are given in their original form.

Contact Details

The postal address or the e-mail address of the author (usually of the first one if there are more Authors) is given in the footnote at the bottom of the first page.

Type of Articles

Classification of articles is a duty of the editorial staff and is of special importance. Referees and the members of the editorial staff, or section editors, can propose a category, but the editor-in-chief has the sole responsibility for their classification. Journal articles are classified as follows:

Scientific articles:

1. Original scientific paper (giving the previously unpublished results of the author's own research based on management methods).

2. Survey paper (giving an original, detailed and critical view of a research problem or an area to which the author has made a contribution visible through his self-citation);

3. Short or preliminary communication (original management paper of full format but of a smaller extent or of a preliminary character);

4. Scientific critique or forum (discussion on a particular scientific topic, based exclusively on management argumentation) and commentaries. Exceptionally, in particular areas, a scientific paper in the Journal can be in a form of a monograph or a critical edition of scientific data (historical, archival, lexicographic, bibliographic, data survey, etc.) which were unknown or hardly accessible for scientific research.

Professional articles:

1. Professional paper (contribution offering experience useful for improvement of professional practice but not necessarily based on scientific methods);
2. Informative contribution (editorial, commentary, etc.);
3. Review (of a book, software, case study, scientific event, etc.)

Language

The article should be in English. The grammar and style of the article should be of good quality. The systematized text should be without abbreviations (except standard ones). All measurements must be in SI units. The sequence of formulae is denoted in Arabic numerals in parentheses on the right-hand side.

Abstract and Summary

An abstract is a concise informative presentation of the article content for fast and accurate Evaluation of its relevance. It is both in the Editorial Office's and the author's best interest for an abstract to contain terms often used for indexing and article search. The abstract describes the purpose of the study and the methods, outlines the findings and state the conclusions. A 100- to 250-Word abstract should be placed between the title and the keywords with the body text to follow. Besides an abstract are advised to have a summary in English, at the end of the article, after the Reference list. The summary should be structured and long up to 1/10 of the article length (it is more extensive than the abstract).

Keywords

Keywords are terms or phrases showing adequately the article content for indexing and search purposes. They should be allocated heaving in mind widely accepted international sources (index, dictionary or thesaurus), such as the Web of Science keyword list for science in general. The higher their usage frequency is the better. Up to 10 keywords immediately follow the abstract and the summary, in respective languages.

Acknowledgements

The name and the number of the project or programmed within which the article was realized is given in a separate note at the bottom of the first page together with the name of the institution which financially supported the project or programmed.

Tables and Illustrations

All the captions should be in the original language as well as in English, together with the texts in illustrations if possible. Tables are typed in the same style as the text and are denoted by numerals at the top. Photographs and drawings, placed appropriately in the text, should be clear, precise and suitable for reproduction. Drawings should be created in Word or Corel.

Citation in the Text

Citation in the text must be uniform. When citing references in the text, use the reference number set in square brackets from the Reference list at the end of the article.

Footnotes

Footnotes are given at the bottom of the page with the text they refer to. They can contain less relevant details, additional explanations or used sources (e.g. scientific material, manuals). They cannot replace the cited literature.
The article should be accompanied with a cover letter with the information about the author(s): surname, middle initial, first name, and citizen personal number, rank, title, e-mail address, and affiliation address, home address including municipality, phone number in the office and at home (or a mobile phone number). The cover letter should state the type of the article and tell which illustrations are original and which are not.

<u>Address of the Editorial Office:</u>

Enriched Publications Pvt. Ltd.
S-9,IInd FLOOR, MLU POCKET,
MANISH ABHINAV PLAZA-II, ABOVE FEDERAL BANK,
PLOT NO-5, SECTOR -5, DWARKA, NEW DELHI, INDIA-110075,
PHONE: - + (91)-(11)-45525005