ISSN Application No. 21722

Advanced Journal in Wireless and Mobile Communication

Volume No. 11

Issue No. 2

May - August 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

ISSN Application No. 21722

Advanced Journal in Wireless and Mobile Communication

Aims and Scope

Advanced Journal in Wireless and Mobile communication welcomes the original research papers, review papers, experimental investigations, surveys and notes in all areas relating to software engineering and its applications. The following list of sample-topics is by no means to be understood as restricting contributions to the topics mentioned:

•LTE
•4G
•5G
•Ultra wide band communications
•Nnovel mobile applications
•Mobile communications and networking
•Energy-efficient communication networks
•Molecular communications

ISSN Application No. 21722

Advanced Journal in Wireless and Mobile Communication

ISSN Application No. 21722

Advanced Journal in Wireless and Mobile Communication

(Volume No. 8, Issue No. 2, May - August 2020)

Contents

ISSN Application No. 21722

Security Control based on Blockchain in the WSN Network

[1]Dhoha Al-Mubayedh, [2]Mashael Al-Khalis, [3]Ghadeer Al-Azman, [4]Rachid Zagrouba

[1,3]Department of Computer Science, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia

[2]Department of Computer Information Systems, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia

[4]College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia

E-mail: [1]2150001651@iau.edu.sa, [2]2150001151@iau.edu.sa, [3]2150006115@iau.edu.sa, [4]rmzagrouba@iau.edu.sa

ABSTRACT

Wireless Sensor Networks (WSN) are one of the main components of the Internet of Things (IoT) paves the way for a world where the devices become interconnected in order to collect information and to automate some tasks. Hence, this vision requires control mechanism to preserve the security of data. The classical security solutions in WSN/IoT have some limitation due to the constrained capability of the devices. In addition to WSN devices limitations, the usual use of these networks depends on central operands to manage the security of increasing number of connectors to the network. Therefore, this paper studied the security control in WSN/IoT with the decentralized blockchain based solution. Mainly, this paper provided a comprehensive background with a literature review on several papers that have security solutions for WSN network based on blockchain technology. Moreover, this paper compared the reviewed solutions with certain criteria which are the efficiency, tamperproof, trustiness, confidentiality, authentication and some unique features provided by the reviewed solutions. Eventually with the deep analysis in the comparison, it appeared that a solution based on the blockchain for managing the access of the IoT has achieve most of the criteria. Thus, the paper chooses this solution and planned to find a possible enhancement on it for future work.

Keywords— Blockchain, WSN, IoT, Security, Network;

I. INTRODUCTION

With the rapid demands of internet and the feasibilities to connect things and build smart things, simple communications are no longer satisfied, people started to occupy the advance internet connection with automatic sensing, connecting and monitoring. These operations supported by what is called wireless sensor network (WSN), which have the ability to interconnect thousands of sensor nodes. WSN is the main component involved in the evolution of the Internet of Things (IoT) [1][2]. IoT as a model closely relevant to the human beings actions, which represent the major actor to make our entities smart. Such network can provide a verity of services because of its ability to interconnect a verity of smart things to interact and cooperate with each other, such as mobile phones, digital cameras and even in industrial

monitoring. It can enable users to produce data that can be recovered regardless of their location [3]. Basically, WSN provide to IoT ecosystems, the communication services for interconnected nodes or devices. It obtains the data from the targeted nodes in a distributed network, through a wireless communication to offer greater support for the upper layer system. Thus, such networks needs an efficient and applicable security mechanism with reliable trust between sensors or nodes [1]. Such routine and smart networks pose higher attention to intruders. Classical Security solutions in WSN/IoT may have limitations because of its use of sensors that lack sufficient power, large storage. in addition to the relay on central operand on the network for the transactions. To solve such problem the area of blockchain has been integrated with WSN and IoT ecosystems.

Recently, blockchain concept as a decentralized infrastructure has becomes an emerged research area in its integration with WSN or IoT. Two main benefits of blockchain systems are the ability of tamper proofing and the de-centering. It allows for secure storage of records, where users can share it with a high confirmation of information without the need for central authority [1].

This paper provides reviews of the existing proposed infrastructures of blockchain-based secure transactions integrated with both WSN and IoT, and provide a comparison and analysis on the reviewed works based on specific criteria that target the security on them.

Organization: this paper is organized as follow: section I introduce the area of WSN and IoT with blockchain. Section II provides a background describes the needed knowledge for this topic, section III will list the reviewed solutions, section IV provides a comparison based on the selected criteria and the analysis results will be mentioned in section V. Eventually the paper will conclude in section VI.

II. BACKGROUND

A. Transaction:

Is a data that represents any operations users claim to carry out. Also, it means sending data between two ormore nodes. One of a denoted formula of the transaction is "t= (from, to, value, sig)". From is the public key of the sender, to is the receiver public key, the value is the content needs to be transaction and the digital signature is a sig[1].

B. Block:

briefly block is a container of transactions. It contains a group of transactions plus, data, timestamp and hash value of the prior block [4].

C. Blockchain:

Blockchain is a ―distributed ledger system re- emerged as an underlying technology of peer-to-peer electronic cash system in 2008‖ [5]. Nowadays blockchain became a trend because of its potential applications under various areas such as smart contract, crypto-currency, the transaction of non-currency asset and IoT. The blockchain consists of several blocks each block contains the Id of the current block, the ID of the previous block and multiple transactions. The blockchain has a robust character of immutability since the ID of the previous block in each block makes a chain of continuous blocks ends at the first block [6]. The ID of each block contains the hash value of whole transactions of the block which then inclusive into the successive blocks of the chain. So, when an attacker wants to alter one transaction on the block, the attack the must change all the successive blocks of the chain which something is infeasible. There are three types of blockchain shown in Figure (1) below [5]:

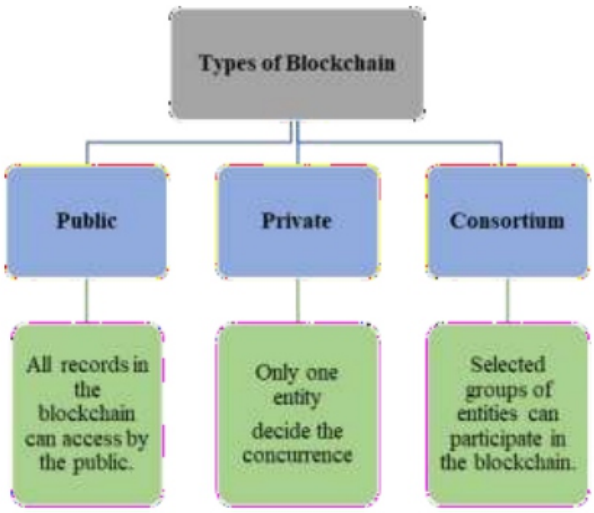

Figure 1: Blockchain types

D. Internet of things (IoT):

IoT is a new technology where devices are smart, have a capacity of computations and memorization, autonomous, and can exchange information between each other without involvement of human. IoT makes objects recognizable, intelligence and can notify information about themselves and can access aggregated information by other things [1]. One of the most benefits of the IoT that it is Facilitated the life since, it allows people and things can connect with anything and anyone at anytime and anyplace, using any path, any network, and any services [6]. Nowadays applications of IoT is huge it covers all areas everyday life of human life. Commonly, all IoT applications are under three main domains. First domain is the society, this domain covers all activities associated with improving or developing the society, cities, and people. For example, smart cities, smart homes and telecommunication which are all applications depend on the IoT. Second environment domain, which is all activities regard developing, monitoring and protecting natural resources such as, Smart Water Recycling, Disaster Alerting. Third

industry domain, all Activities regarding any transactions either financial or commercial between any entities such as Supply Chain Management Automotive and Industrial Control [7].

E. Wireless sensor network (WSN):

It is a set of nodes that interact with each other. As well,, it is a group of clusters that have limited capacity, and each cluster is managed by a non-limited capacity node called Personal Area Network Coordinator (CPAN). Also, it is a grid of dispersed sensors that work to sense the status of the surrounding and gather data at a central location called base station (BS) or sink [5]. It uses for several applications such as measuring the sound, temperature, and pollution. Nowadays it is popularly used at the IoT to gather data and manage several environments [8].

It has several advantages which are [9]:

- There is no need for fixed infrastructure to set up the network.
- The WSN can use in non-reachable places. For example, at deep forests, the sea, and the mountains.
- Flexible if there is a need to add an extra workstation.
- The price of the implementation is inexpensive.
- The access to the WSN can be through centralized monitoring.

A well It has several disadvantages which are [9]:

- It avoids a large number of wiring.
- It is vulnerable to several attacks since it is less secure. For example, the hacker can hack the access point and gather all information.
- It has a lower speed than the wired network.
- It can configure in a more complicated way than a wired network.
- It can be easily troubled by what it surrounds such as, microwave and large distances.

III. LITERATURE REVIEW

L. Feng et al [1], they integrated the decentralized distributed block chain with WSN as a mean to provide an authenticated transactions and secure storage system. In this approach Figure (2), each node has a signature and public key (his ID), those two used to authenticate the node and its transactions to the blockchain system. The infrastructure composed of three main operations which are, encrypted transaction, consensus validation, and distributed storage. The main parts in the blockchain ecosystem are consensus validation and distributed storage. The blockchain ecosystem separated in such a way that some nodes used for validation and others for storage. This model used a consensus algorithm called

Hierarchical Byzantine Fault Tolerant (HBFT) which is based on a private blockchain. To guarantee the confidentiality of the transmitted information the model proposed an algorithm called block-based WSN encryption BCE-WSN which consist of four procedures: Key-pair generation using an anonymous way in each node in the WSN, Encryption using asymmetric encryption, Signature to ensure the integrity of data, Verification before passing information to the blockchain system. This model provided good scalability, shorter delay and increased throughput with greater number of nodes.in addition to higher attack resistance and secure storage for the transmitted sensor data. The paper will refer to this schema with the Blockchain-based Collection Storage Platform (BCSP) in the comparison and analysis section.

Figure 2: Distributed blockchain with WSN for authenticated transactions and secure storage system

A. Moinet, et al [2], proposed a security model called Blockchain Authentication and Trust Model (BATM), that use PKI for a secure decentralized storage for cryptographic keys beside the trust data, to guarantee their integrity and validity in WSN. This achieved by using the blockchain as a database to store the public keys, peer information and digital signatures. Providing a mutual validation of information gained by each party in the network about the other nodes in the network. For BATM authentication, it used similar idea to Pretty Good Privacy (PGP) with PKI. Where the public master key is used to identify the nodes and services, and this key is used to generate the secondary keys that used for encryption and digital signature. Those keys are hold by node's credential payload. This payload will deliver it by the node at the authentication. The keys are renewable using validity timeout, to reduce possible attacks on it. When a node for the first time requested to connect to the network, the node will issue a Credential Payload (CP) to all nodes in the network. When authenticated network node adds this CP in valid block, the authentication request will be granted. BATM uses six different types of payloads:

Minor Approval (MP), Network Node (NN) and Available Services (AP) payloads, CP, Renew, Revoke, Blame and Ban payloads. Blame and Ban are mainly used for BATM trust management model. In this trust model, they used what is called Human-like knowledge-based trust (HKT) that depends on the reputation level. The trust level will be based on the payloads that the node used, and this level will be used to control network's node actions. There will be a trust evaluation if the node can perform the action correctly. To prevent malicious valid payloads, they put specific rules for the submitted payloads in the blockchain. The paper will refer to this model with the Blockchain Authentication and Trust Model (BATM) in the comparison and analysis section.

Mohamed el al. [8], proposed a new security mechanism based on the blockchain which called BCTrust. The concept of this mechanism that when one device is authenticated in one of the WSN clusters it will be trustful and accepted by all other clusters. The blockchain role is to ensures that the stored information is preserved from any modification and obtainable to all participated nodes. If any device wants to make a transaction with the blockchain, it will be done through CPANs of the network. For example, if the device "a1" belongs to "A" CPAN and it wants to communicate with the blockchain, it will authenticate by ―A‖ CPAN and then ―A‖ will send the transaction ―A: a1_ok" to the blockchain which means, that ―a1‖ is trustful and ―A‖ has a symmetric key with the ―a1‖ device for secure communication. This transaction will store in a new block validated by all participating CPANs. So, when next time ―a1‖ wants to associate with ―B‖ CPAN.‖ B‖ will check if ―a1‖ was authenticated previously or not. If it was authenticated, ―B‖ will request ―A‖ to send the symmetric key ―a1‖ through the asymmetric channel. After the transaction between ―a1‖ and ―B‖ it will be added in the blockchain ―B: a1_ok‖ with ―A: a1_ok‖ in order if a1 wants to make any transaction with any other CPANs the CPAN will take from the nearest CPAN the symmetric key with a1. The symmetric communication between CPANs and devices includes the key and initialization vector (IV). The benefit of this mechanism that in a secure association of the device it needs two exchanged messages without a need to demand a key derivation process. Also, The approach process operations and exchange messages between either, blockchain and CPAN, or between two CPANs. That is helpful since CPAN and blockchain devices have unlimited capacities and do not consume energy and do not pose any problem of storage or processing capacity. it provides a decentralized authentication system and overall view of the network. The paper will refer to this mechanism by Blockchain Trust (BCTrust) in the comparison and analysis section.

Yongfeng et al. [6] proposed decentralized blockchain-based security management model. This model considers the authentication of IoT devices problem since usually IoT depends on a trusted third party for identity authentication. As well it considers the transactions between the IoT and the problem of the

remote cloud that usually needs a strong security mechanism to prevent data modification. Also, it needs to guarantee timely and effective data. Thus, the authors proposed using a platform depends on the blockchain in order and set strong security policies on it which prevent needing to a third party for authentication and guarantee data integrity and security since it adopts a strong cryptography algorithm. As well, it is adding distributed storage models on IoT that depends on blockchain and device ledger to analyze the production and application of the IoT devices. Also, it makes all the IoT devices software upgrades management, privacy management based on blockchain. The most benefit of this model that it achieves the security management control without the existence of a trusted third party. The paper will refer to this model with the Blockcahin- based Security Management Model (BSMM) in the comparison and analysis section. In a paper was done by Z. Huang. et al. [10], claimed that the centralized infrastructure that uses an intermediate third party does not provide enough trust in IoT data exchange. Therefore, the paper provided deep analysis of the trust requirements of the IoT data exchange. Mainly, the paper divided the trust requirements to three categories: trusted trading, trusted data access and trusted privacy preserve. Then, it proposes a decentralized solution based on the blockchain to meet such trust requirements. Also, the paper developed a prototype using Ethereum blockchain and smart contracts that handles the management function. Basically, the solution of this paper has utilized the feature that the data is not tampered and completely transparent. The paper described the architecture of the solution in four layers which are data layer, network layer, management layer and interaction layer. The data has been divided into two parts in the data layer which are the IoT data and data exchange that stored in the blockchain containing the record of the whole data exchange process. While the network layer contains the core of the architecture where the blockchain network can guarantee IoT data exchange in a reliable, transparent and tamper-resistant environment. Additionally, the management layer in the platform is mainly responsible for managing and controlling user permissions and security. Lastly, the interaction layer allows the data exchange parties to interact and communicate with each other whether in web-based or mobile-based interactions. The prototype of the paper showed that the blockchain network makes the transaction recorded in an auditable, transparent and immutable way. The paper will refer to this solution with the data trusted exchange based on blockchain (DTEB) solution.

Another paper was done by O. Novo. [11], proposed a fully decentralized solution based on the blockchain for managing the access of the IoT in a scalable manner. The architecture of the solution contains six components with new and different functions which are WSN, managers, agent node, smart contract, blockchain network and management hubs. Basically, the architecture defines a new node which is the management hub that connects the blockchain with the IoT devices since the majority of IoT devices is not able to store the blockchain due to the capability constrained in term of CPU, memory, and battery. IoT devices in the WSN can be managed with considering the scalability and capability of IoT with the help of the management hubs.

Another component that gives an advantage of the solution is the smart contract which has the feature that it is unique and cannot be deleted. The smart contract defines the operation that is allowed in the access management system. Hence, the access policy of this solution brings some advantages as the mobility where every administrative domain can manage the IoT devices freely while the access control policies are still enforced by the blockchain. Also, the accessibility and concurrency where the access control policies are available at any time and can be managed concurrently. Additionally, the lightweight where the solution has the advantage that the IoT devices do not need any modification to be adopted with this system. Lastly, the transparency of this solution where the system preserves the location privacy of IoT devices and the resources accessibility. Furthermore, the paper studied the solution by evaluating it in realistic IoT scenarios with a proof of concept implementation. Eventually, the results show that access management technology based on blockchain can be used in specific scalable IoT scenarios. The paper will refer to this solution with the access management based on blockchain (AMB) solution. Figure (3) below shows the architecture of this solution.

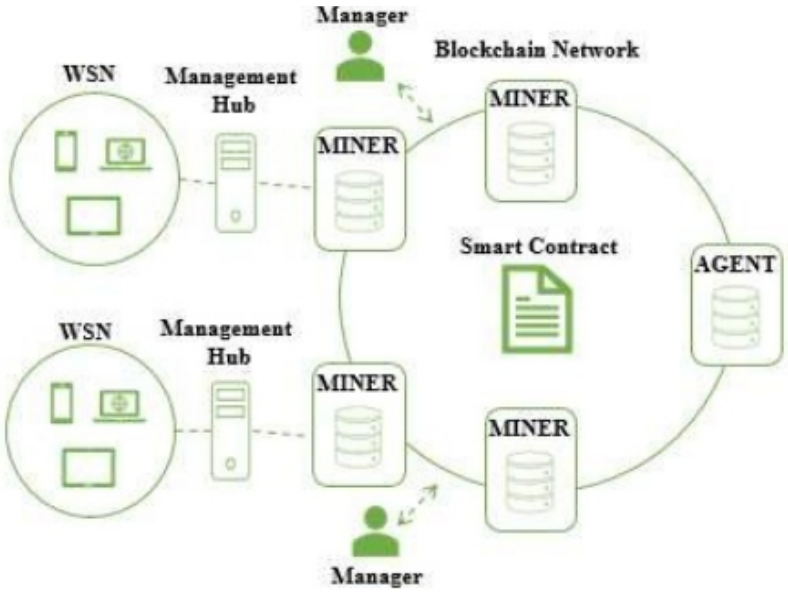

Figure 3: The architecture of the access management blockchain solution

IV. COMPARITION AND ANALYSIS

In this section, a comparison was done between the reviewed solutions as in Table (1) with six criteria which are defined as follow; first is the efficiency criteria wither the solution has proven its efficiency in term of time consumption where it has a higher throughput in less delay. Secondly, tamper proof criteria which guarantee that the data cannot be tampered or modified to preserve the data integrity. Thirdly, trustiness criteria show the trust level of the node in IoT and wither the transaction is trusted by the parties. The fourth is the confidentiality which means the protection of data and information from the non- authorized discloser [12]. The fifth is the Authentication which means the validation of user identity [13]. Lastly, the additional unique feature which means what is the additional feature that the solution provides that did not exist in other solutions.

	Efficiency	Tamperproof	Trustless	Confidentiality	Authentication	A unique feature of the proposed solution
BCSP [1]	✓	✓	•	✓	✓	•
BATM [2]	•	•	✓	•	✓	•
BCTrust [3]	✓	✓	•	✓	✓	✓
BSMM [4]	✓	✓	•	✓	✓	•
DTEB [10]	•	✓	✓	✓	•	✓
AMB [11]	✓	✓	•	✓	✓	✓

✓ - exists, •- not motioned on the paper

Table 1: Comparison between the reviewed solutions

E. Efficiency

In BCSP, the efficiency of it depends on two indicators, which are the system throughput and system delay, showed that their blockchain-based storage structure has a shorter delay with a higher throughput than the centralized server mode. While BSMM it is efficient because, it is fast and does not consume time, energy, power and storage related to the uses of the blockchain and CPANs. Also, because it uses Elliptic Curve Digital Signature Algorithm (ECDSA) which provides and guarantee fast and robust transactions. Furthermore, BSMM solution has high efficiency in key distribution processing without needing to the third party depend on blockchain. Whereas AMB, has proven the effectiveness of its design in some specific IoT scenarios; when WSN are connected to multiple management hubs. Management Hub is the node that connects the blockchain with the IoT devices. But in the case of a single management hub, this solution does not have a better performance that IoT the optimized centralized IoT systems [14].

It is noticeable that most solutions that provide efficiency on WSN and IoT depends on blockchain only or efficiency in a specific scenario such as AMB, while BCTrust solution depends on three components to provide better efficiency.

F. Tamperproof

BCSP it uses distributed ledger to record devices hashes of software and firmware, so any tampering in the transactions can be detected by its users easily. Also, in BCSP they use signatures techniques using the ID of the sender node as a public key to transfer the sender's transactions to a cipher text and then send it to the receiver. This is to prevent faking attempts to provide data integrity.

Whereas in BCSP, it has high tamperproof since it uses permissioned one mechanism which means only the truthful CPANs will have the writing permissions on the blockchain using public/private keys. As well, related to the consensus mechanism the stored data cannot be modified. While BSMM solution, it depends on blockchain features that prevent altering the data from unauthorized people. As well, it uses access control and policies that prevent unauthorized people to manipulate the data.

Whereas DTEB ensures that the data on the blockchain cannot be tampered and can be audited according to time order. Also, the transaction records are immutable. While AMB, has studied and provide a security analysis to provide satisfying level of security, in AMB the communication between the devices is done through DTLS which prevents the tampering.

Because of the inherent feature of tamper proof in blockchain mechanisms, it appeared that all the reviewed mechanisms offer this feature, however they differ in the used keys that provide such feature and controlled parties. However, there is a noticeable disadvantage in BCSP, since it depends in node's ID to sign the data which can be spoofed by attacker. Whereas, AMB provides an additional mechanism to prevent tampering.

G. Trustiness

In BATM, proposed a trust management based on reputation level of each network node. In this model it did not needed a trust center to control actions on the network. They build the trust based on the payloads in the blockchain. They used payloads as a behavioral indication of each network node over time. Based on this observation, they ensure that a network node cannot trick others through tampering data or impersonating someone else. The trust here referred to by the trust evaluation which is based on probability level whether an action can be done correctly be network node. While solution DTEM, combine the time stamp and the details of the transaction in the process of trading and storing which makes it trusted by many parties. However, the trust level of the nodes in the IoT had not been evaluated on this solution [15]. BATM is better because it evaluated that is trustful while, BTEB is not evaluated right now.

H. Confidentiality

BCSP used BCE-WSN encryption algorithm that firstly it provides key pair generation in anonymous way for each sensor node with node's ID as the public key. Secondly, encrypt using asymmetric encryption algorithm with a private key for each node, the cipher text generated by from the encryption function is transmitted on all sensor nodes in the network. While BCTrust, it uses two cryptography mechanisms in the symmetric secure communication between the devices and CPAN nodes which are the symmetric key and IV. Also, the transaction between the CPANs and the blockchain or between

two CPANs done through encrypted transaction using public and private keys. As well, it uses ECDSA that increases the confidentiality. Whereas BSMM, mentioned that the current use algorithm depends on ID-key algorithm to the data cryptography. But the platform is flexible to adapt any strong cryptography algorithms. While, in solution DTEB the involved parties in sending the transactions use only a public address without personal information which preserves the privacy. Also, it uses the asymmetric encryption on the user's private information to make it secure with the private and the public key as the only identifier of transaction subject. Whereas solution AMB prevents eavesdropping since the communication between the devices is done through DTLS.

It appeared that the best confidentiality at solutions BCTrust and DTEB since DTEB uses cryptographic keys, IV and ECDSA algorithm to prevent data disclosure. While, [10] uses additional feature which is DTLS to prevent eavesdropping.

I. Authentication

BCSP, uses HBFT private blockchain. Users cannot enter to the blockchain-based storage unless they are authenticated. In this infrastructure network's nodes and transactions are authenticated using the empowered node's ID as a public key and his signature. Since the public key is public in the network all the nodes in the network can verify the authenticity of the transmitted data through it. Whereas BATM, uses similar ideas to PGP and PKI for authentication. The cryptographic authentication data will be stored in a valid block of this blockchain- based secure storage. When a node for the first time requested to join to the network, the node will release a Credential Payload (CP) to all nodes in the network, and the authentication request will be granted when authenticated network node adds this CP in valid block. The used keys here will renewable to reduce attacks such as guessing key attacks. While BCTrust, the authentication is done through checking if the device information is stored in the blockchain before or not. If the device is recognizable in the blockchain, the secret key will be used to do the transaction between the device and the node. If the device is new, the association process should apply. Whereas BSMM, it uses identity authentication mechanism between any IoT devices or between IoT and cloud Based on blockchain. While in AMB the authentication is not needed since any IoT device is able to connect to any management hub directly to access the blockchain. So, it is observed that all solutions authenticate the devices by reviewing the blockchain since all mechanisms depends on storing credential data in the blockchain.

J. Unique feature of the proposed solution

Some of the solutions have a unique feature to simplify the usage of blockchain or to enhance the security. In BCTrust, when one device is authenticated by one CPANs, it will be trustful by all other

CPANs of the same network. Also, in DTEB, has the transparency feature for recording the transactions. As well, in AMB it has the transparency feature, but it uses it to hides the IoT devices location and how the resources are being accessed. However, AMB has a downside where it did not provide the specification and expression of access control policies [16].

V. RESULTS AND FINDINGS

Based on the above analysis, it appeared that BCTrust and AMB achieve the majority of the criteria in a higher level except the trustiness was not mentioned in these solutions. But, AMB has an extra security feature that make it stronger than BCTrust which is transparency feature. So, as future work this paper will work to find possible enhancement for the AMB.

VI. CONCLUSION AND FUTURE WORK

Internet of Things (IoT) becomes one of the fundamental parts of our life, a huge number of devices are connected and communicated to each other. Wireless Sensor Networks (WSN) is one of the major components of the success of the IoT. Thus, it is important to improve the security of them to prevent any damages. The blockchain is a great solution to most of IOT and WSN problems. Therefore, this paper aimed to find the best solution for utilizing the blockchain to enhance both the IoT and WSN by reviewing several solutions and compare them based on different criteria. The criteria are efficiency, tamperproof, trustiness, confidentiality, authentication, and additional unique feature. The paper founds that BCTrust and AMB are highly meeting all the criteria unless trustiness. As well, it founds that AMB is better than BCTrust regarding the extra security feature which is transparency that helps to hide the device location to prevent possible attacks. As a future work, this paper aims to enhance AMB by providing a clear specification and expression of the access control policies included in the solution. Also, try to find possible enhancement of the authentication mechanism on it.

REFERENCES

[1] L. Feng, H. Zhang, L. Lou and Y. Chen, "A Blockchain- Based Collocation Storage Architecture for Data Security Process Platform of WSN," 2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design ((CSCWD)), Nanjing, 2018, pp. 75-80.

[2] A. Moinet, B. Darties, and J.-L. Baril, —Blockchain based trust & authentication for decentralized sensor networks,‖ arXiv preprint arXiv: 1706.01730, 2017.I. S. Jacobs and C. P. Bean, —Fine particles, thin films and exchange anisotropy,‖ in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[3] B. Hammi et al, "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT," Computers & Security, vol. 78, pp. 126-142, 2018.

[4] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, —An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,‖ 2017 IEEE International Congress on Big Data (BigData Congress), 2017.

[5] N.Islam, —Towards a Secure and Energy Efficient Wireless Sensor Network using Blockchain and a Novel Clustering Approach‖. Master's Thesis, Dalhousie University, Halifax, NS, Canada, July 2018

[6] Y. Qian, Y. Jiang, J. Chen, Y. Zhang, J. Song, M. Zhou, and M. Pustišek, ―Towards decentralized IoT security enhancement: A blockchain approach,‖ Computers & Electrical Engineering, vol. 72, pp. 266–273, 2018.

[7] R. Porkodi and V. Bhuvaneswari, ―The Internet of Things (IoT) Applications and Communication Enabling Technology Standards: An Overview,‖ 2014 International Conference on Intelligent Computing Applications, 2014.

[8] M. T. Hammi, P. Bellot, and A. Serhrouchni, ―BCTrust: A decentralized authentication blockchain-based mechanism,‖ 2018 IEEE Wireless Communications and Networking Conference (WCNC), 2018.

[9] P.Tiwari, V. Saxena, R.Mishra, D.Bhavsar, ―Wireless Sensor Networks: Introduction, Advantages, Applications and Research Challenges,‖ HCTL Open International Journal of Technology Innovations and Research (IJTIR),2015

[10] Z. Huang, X. Su, Y. Zhang, C. Shi, H. Zhang, and L. Xie, ―A decentralized solution for IoT data trusted exchange based-on blockchain,‖ 2017 3rd IEEE International Conference on Computer and Communications (ICCC), 2017. Available: https://ieeexplore.ieee.org/document/8322729

[11] O. Novo, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT," in IEEE Internet of Things Journal, vol. 5, no. 2, pp. 1184-1195, April 2018. Available: https://ieeexplore.ieee.org/document/8306880

[12] N. Lal, S.Prasad, M.Farik,‖A Review Of Authentication Methods,‖ International journal of scientific & technology research, vol.5, no.11 2016,

[13] S. Majumder, S. Chakraborty, and S. Das, ―A New Advanced User Authentication and Confidentiality Security Service,‖ International Journal of Computer Applications, vol. 93, no. 11, pp. 4–11, 2014.

[14] O. Novo, ―Scalable Access Management in IoT using Blockchain: a Performance Evaluation,‖ IEEE Internet of Things Journal, pp. 1–1, 2018. Available: https://ieeexplore.ieee.org/document/8525343

[15] J. Qi, Z. Wang, B. Xu, M. Wu, Z. Gao, and Y. Sun, ―QoS- Driven Adaptive Trust Service Coordination in the Industrial Internet of Things,‖ Sensors, vol. 18, no. 8, p. 2449, 2018.

[16] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, ―Harnessing the power of blockchain technology to solve IoT security & privacy issues,‖ Proceedings of the Second International Conference on Internet of things, Data and Cloud Computing - ICC 17, 2017.

ISSN Application No. 21722

Multicasting Ad- Hoc Network based on Genetic Algorithm Approach

Bassam Mohammed Elzaghmouri
JPU, Jordon
E-mail: el_zaghmouri@yahoo.com

A B S T R A C T

Throughout this dissertation, a new approach for multicasting in Ad-hoc networks was developed. This approach is based on two schemes; firstly, a sub-optimal spanning tree of key nodes was built, secondly, the genetic algorithm was used to find this spanning tree. Actually, finding the optimal spanning tree of dominating or key nodes causes NP-was very hard, therefore, several heuristic approaches have been introduced in order to find a sub-optimal one. On the other hand, genetic algorithm is designed of individuals each represents distinguishable tree, and could provide means to tackle this problem by searching for a structure of a suitable spanning tree that can be optimized in order to meet the performance indexes related to the multicast problem. Our model was compared with simple flooding, the results showed the ability of our model to reduce broadcast storm problem while simple flooding causes broadcast storm problem with high probability, and reachability factor of our model is very close to the simple flooding. On the other hand, the complexity of our model is not high compared with the minimum spanning tree technique.

Keywords- Multicast, Ad-Hoc Optimized, Neural Network.

I. INTRODUCTION

Nowadays, mobile network has received much attention since it is an attractive computing environment [4].

A mobile ad hoc network (MANET) consists of an independent system mobile hosts (any host can be a router) created on the fly and connected by wireless links in the absence of a fixed wired infrastructure, of these models together constitute a communication network formed as a model of an arbitrary communication graph. In MANET, some nodes in the network are predicted to help in the routing of packets, all hosts can be moved freely without any limitations through the network, where each node can communicate directly with the other neighbor node within the range of transmission, in other words, both servers and clients are mobile. Generally, successful routing protocols provide devices to send packets to destination nodes with dynamic topologies. [5]

Other definitions described mobile ad hoc network as mobile devices that were set up to be short life network available for communication needs of the moment without any infrastructure, or wired network, (base stations) or centralized administration (mobile switching centers). [1] [4]

Wireless networks consist of wireless nodes that are distributed over a geographical area. These nodes have the capability to perform processing as well as communicating together by means of MANET. With the coordination among these nodes, the networks between each others will satisfy complex tasks in urban environments and in terrain with abnormal structure. However, as a result of limited transmission ranges, providing connectivity they need to be cooperated among all nodes in MANET [17].

MANET has some special properties that can be distinguished from other networks, in fact many papers address this issue for instance, MANET is decentralized and self-organizing network that has the ability to form a communication network without depending on any backbone network or fixed infrastructure Hekmat, [4].

Since the Mobility in MANET is very wide, lifetime of the node neighborhood is limited; moreover, the topology information is varying at any time [9].

The best representation of MANET is expressed by using unit graphs; this model is widely used, where two nodes A and B are neighbors with transmission radius R for all nodes, if the distance between them is at most R. Each node is provided with a radio transmitter and receiver used for communication with other nodes [3].

Now, if we want to send a message (data) to all nodes in the network, each node can be act as a relay station until the message is routed to all nodes. In other word, ad-hoc network allows multi-hop communication among nodes if needed [6].

There are currently two forms of mobile wireless networks. The first form is known as the infrastructure networks consist of two parts: a wired (fixed) part and a wireless part. The wired part is typically a hierarchy of wide area and local area wired networks, used as the backbone network. The wired backbone is connected to special switching nodes called base stations. The mobile host within this network is connected to the nearest base station that is within its communication radius. A base station uses the wired network to be connected to other base stations, hence, it is the wired part. Wireless network in this case is called a single –hop network. The second form is mobile wireless networks and are known as the Infrastructure less networks they doesn't depend on the existence of base stations or network infrastructure. Instead, they are consisted only of a collection of devices (computer, laptop, and palmtop) equipped with wireless communication and networking capability that act as both a host and a router. Such devices can communicate with another node that is immediately within radio hop range or

one that is outside their radio range in multi-hop scenario. This type of the network is called an (ad hoc network). Ad hoc network has the ability to be self-organizing and adaptive. Mobile ad hoc network is referred in the literature as MANET [9].

Cellular network is a single hop model in comparison with MANET [30]. Cellular networks depend on backbone network and fixed base stations in order to create connection between two mobile nodes, In MANET no backbone network or base station exist, and the topology of the network is not fixed and it dynamically changes in an unpredictable manner because of the free movement of the nodes.

II. RELATED WORK

Many algorithms introduced the multicasting and broadcasting in mobile ad-hoc network and tried to find optimal solution with different criteria, among them are: Simple flooding (SF) that was described by Ho et al., Jetcheva, Hu, Maltz, and Johnson [13][14], JungHwan, Kien and Prabhakara [3], On Demand Multicast Routing protocol, ODMRP was described by Yu et al. [6], ODMRP is a mesh-based multicast protocol in which a collection (mesh) of nodes forwarding multicast packets is created between the senders and receivers, Zone-Based Multicast Routing Protocol which was described by Chang et al. also depend on mesh idea but it is trying to overcome the disadvantage of ODMRP [5].

QoS Multicast Routing was Based on Bandwidth Estimation in Mobile Ad Hoc Networks and proposed a cross-layer framework to support QoS multicasting. And enhanced the IEEE 802.11 MAC layer to estimate the available bandwidth at each node.

Gui and Mohapatra, Overlayed multicast protocol and built a virtual mesh spanning to all member nodes of a multicast group [10]. It employed standard unicast routing and forwarding to fulfill multicast functionality.

Baburaj and Vasudevan, attempted to propose a new PSObased On Demand Multicast Routing Protocol (PSO-ODMRP), which improved the performance in the routing messages.[7]

Baburaj and Vasudevan. prepossessed a new genetic algorithm based on Multicast Ad-hoc On demand Distance Vector Protocol for MANETs (GA- MAODV), which improves the packet delivery ratio of the routing messages [8].Threshold Based Schemes were proposed by Ni et al, Peng and Lu, William and Camp, Qayyum,Viennot and Laouit, Sason and Kevin, William and Dinesh. [15]The operation of each one of broadcasting protocols can be described as (Simple Probabilistic Based Broadcasting (SPBB), Counter Based Scheme (CBB), Distance Based Broadcasting Technique (DBB), Location Based Broadcasting (LBB)).

On the other hand some researchers like Zhou and Singh, Content based multicast (CBM). [36]There are other methods depend on Topology such as Neighbor knowledge technique and Spanning Tree Broadcasting Technique(STB).Neighbor knowledge technique was proposed by Ho et al, Lim and Kim, Lauer and Al-Tabbakh, and divided into more categories like Self Pruning (SP), Scalable Broadcast (SBA), Dominant Pruning (DP), Multipoint Relay (MPR), Location Based Broadcasting (LBB) [9].

MATERIALS AND METHODS

A basic overview of the new model is shown in Figure 1.1

Figure 1.1

Network configuration is the input of the model and the multicast tree is its output, the Genetic algorithm model (GAM) gets network configuration that is formed as graph and applies GA on it. And then produces multicast tree that determines the track of multicasting process.

In Network configuration stage, the topology of the network is determined by determining number of nodes, and their radiuses, then according to the number of nodes and their radiuses the topology of the network (position of nodes) will be determined randomly, actually this way doesn't depend on any factor and it is the simplest way to create a network. Other ways depend on specifying the position of each node; indeed it's not easy to determine the position for each node especially in big network (not practical). After that, multicast group is defined by choosing a group from the network.

Genetic Algorithm model stage consists of three parts: genetic algorithm operations, encoding and decoding, and finally performance evaluation.

The Final stage is producing proposed multicast tree. Figure 1.2 illustrates the Genetic Algorithm Model in more details.

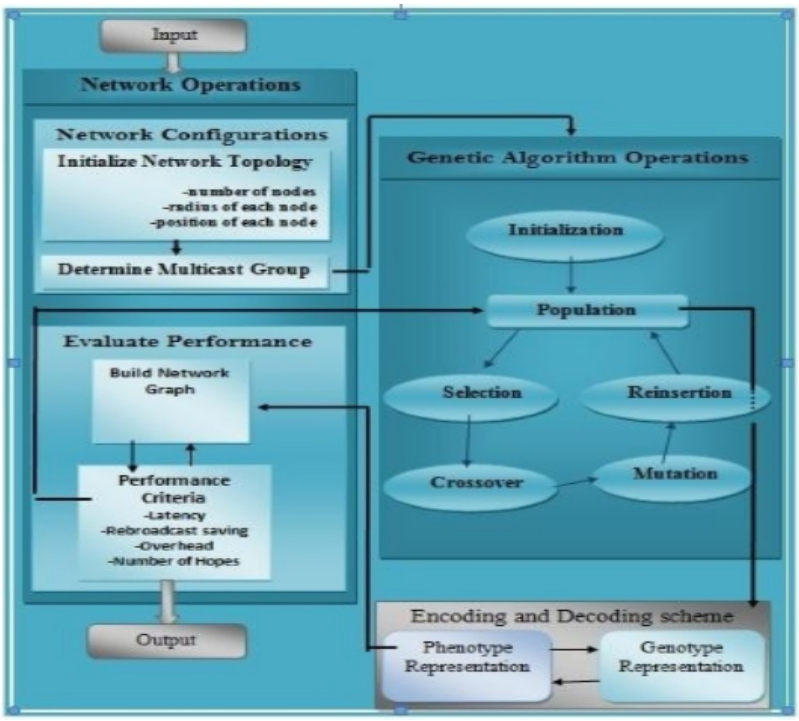

Figure 1.2

Genetic algorithm operations (cycle) contain five steps: Initialization of population, Selection, Crossover, Mutation and Reinsertion.

Initialization of population depends on random algorithm, where individuals (trees) are built randomly from graph network Figure 1.3 shows Genetic algorithm operations cycle.

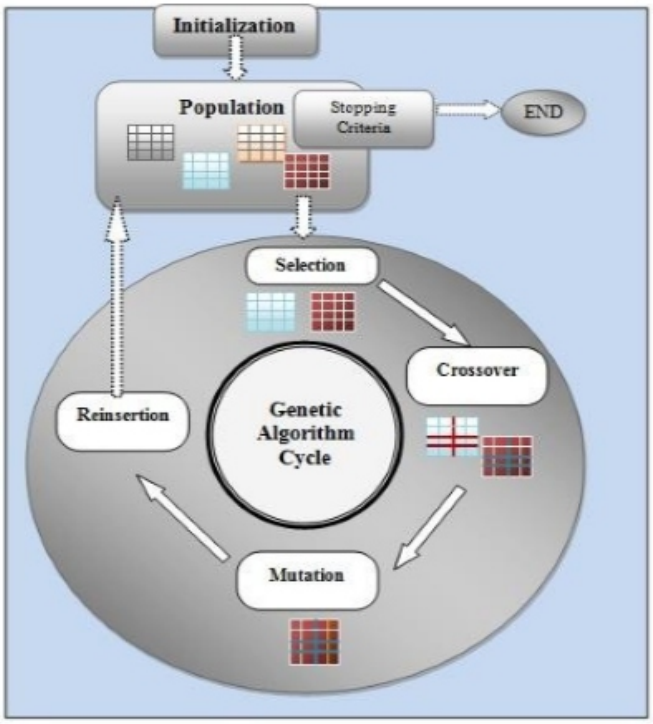

Figure 1.3

As we see from Figure 1.3 the first step in genetic algorithm cycle is Initialization, after creating first population from initialization, the crossover, mutation and reinsertion steps are repeated until reaching to stop criteria, more details about genetic algorithm cycle.

Multicasting Tree and genetic model

In our analysis, source tree (phenotype) is represented as a matrix in genotype, we used matrix representation with minimum gap between genotypic and phenotypic space.

The Operations of GAM

GAM operations consist of six parts, starting from selecting then encoding processes then crossover then mutation then reinsertion and finally termination.

GA over other techniques:

Many algorithms are proposed to optimize Multicasting process in ad-hoc network, but why we chose GA? Firstly, we try to find optima-spanning tree that is very close to the optimal-spanning tree, and of course cause NP complete problem, most statistical solutions cannot reach a good solution because they fill down in local minimum point and they cannot realize that the reason for that is that most statistical methods depend on some values (dependency) and this sometime leads to a bad judgment, while there is no full dependency in GA we put fitness function to evaluate individuals, but also choosing individuals randomly is the best way to avoid local minimum problem.

On the other hand, some solutions in AI is not attractive for optimization or searching like Artificial Neural Network (ANN), as we know, ANN usually uses machine for learning and also Fuzzy logic to consider a reasoning system and not a suitable solution for optimizing.

Complexity of GAM and SF:

Complexity of our model depends on many things such as the population size and number of generations, and we can change the value of parameters according to the problem: we need a good fast solution over the time, so we cannot give our model a specific value or an equation for complexity even if we fix all parameters, GA works randomly and we cannot give any equation for a random process, but we can evaluate it from the experimental results, that means that there is no specific O-notation for our model.

SF is considered a very simple technique and depends on just forwarding the message to other nodes, so in the worst case O (n).

III. RESULT AND DISCUSSION

There are many metrics were used to evaluate the performance of multicasting techniques considered in this Paper also there are many environmental parameters that may affect the performance. Parameters setting of technique are other important input for the techniques that may affect the performance. GAM has parameters to be specified, these parameters are population size, number of generations and mutation ratio, The effect of the number of nodes on the redundancy and the number of hops. A comparative study has been done between the approaches of interest: Simple Flooding (SF) and our proposed model (GAM),The result of GAM is so close to the result of simple flooding, since simple flooding is not heuristic approaches, The redundancy of Simple Flooding is very high, because it is not concerned about it, we noted that simple flooding is lower than GAM by a small value, the reason of this is because GAM tries to compromise among different performance metrics, simple flooding is not interested of how many intermediates will be used, while GAM tries to minimize the number of intermediates, therefore, in these cases; our model has lower number of intermediates than simple flooding, we noted that simple flooding is lower than GAM, the reason of this is because GAM depends on many things such as the population size and number of generations, SF is considered a very simple technique and depends on just forwarding the message to other nodes.

IV. CONCLUSION

The problem of Multicasting in mobile networks is tackled, as mentioned, protocols that were developed to improve multicasting process in MANET varied,but unfortunately most of them neglected some important factors such as redundancy which is considered as a main reason for broadcast storm problem, multicasting algorithms started from the simplest technique 'simple flooding' and ended with the most complex technique 'spanning tree'. Simple Flooding techniques caused the broadcast storm problem. The Minimum Spanning Tree approach is NP hard complete. Other heuristics methods, such as Counter Based Scheme, are not reliable and guaranteed.

A new approach solved the problem of multicasting in MANET by using the genetic algorithm methodology. The object of using GA-based is to construct a reliable and fast multicasting tree in MANET.

REFERENCES

[1] Elaiwat, S. Ammar, A. Venkatraman, S. and Alazab, M. (2010). Applying Genetic Algorithm for Optimizing Broadcasting Process in Ad-hoc Network. the Second International Joint Journal Conference in Computer, Electronics and Electrical, CEE 2010.

[2] Elaiwat, S. Ammar, A. Venkatraman, S. and Alazab, M. (2010). GOM: New Genetic Optimizing Model for Broadcasting Tree in MANET. 2010 2nd International Conference on Computer Technology and Development, ICCTD.

[3] Elaiwat, S. and Belal, M. (2010). An evolutionary creative design approach for optimising the broadcasting trees in MANET. International Journal of Design Engineering 3(1): 97-114.

[4] Alcalá-Fdez, J. Alcalá, R. et al. (2009). Learning the membership function contexts for mining fuzzy association rules by using genetic algorithms. Fuzzy Sets and Systems. 905-921.

[5] Chang, T. Wen, J. et al (2009). An efficient zone-based multicast routing protocol for ad hoc network. WSEAS TRANSACTIONS on COMMUNICATIONS 8. 1135- 1144.

[6] Yu, Y. Zhou, Y. et al. (2009). The effect of multiple tree construction process on ODMRP over mobile ad hoc networks. IEEE.

[7] Baburaj, E. and Vasudevan, V. (2008)b. An intelligent mesh based multicast routing algorithm for MANETs using particle swarm optimization. IJCSNS 8(5): 214.

[8] Baburaj, E. and Vasudevan, V. (2008)a. An Intelligent Multicast Ad-hoc On demand Distance Vector Protocol for MANETs. Journal of Networks 3(6): 62.

[9] Al-Tabbakh, S.M., Amer, F.A., Belal, M.A. and Sakr, E.M. (2007) A proposed distributed heuristic protocol for broadcasting in mobile ad hoc network, Egyptian Computer Science Journal, May, Vol. 29, No. 2.

[10] Gui, C. and Mohapatra, P. (2007). Overlay multicast for MANETs using dynamic virtual mesh. Wireless Networks 13. 77-91.

[11] Harvey, R. and Gargano, M. (2006). Minimal Edge- Ordered Spanning Trees Using a Self-Adapting Genetic Algorithm With Multiple Genomic Representations. Proceedings of Student/Faculty Research Day, CSIS, Pace University.

[12] Hekmat, R. (2006). Ad-Hoc Network: Fundament Properties and Network Topologies . Delft University of Technology, book, published by Springer.

[13] Kicinger, R. Arciszewski, T. and Jong, K (2005). Evolutionary Computation and Structural Design: a Survey of the State of the Art. Computers & Structures. (23-24).

[14] Xiong, Y. Golden, B. and Wasil, E. (2005). A One- Parameter Genetic Algorithm for the Minimum Labeling Spanning Tree Problem. IEEE Transactions on Evolutionary Computation, 9 (1). 55-60.

[15] Abraham, A. (2005). Evolutionary Computation. Handbook of Measuring System Design, edited by Peter H. Sydenham and Richard Thorn.

[16] Althaus, E., Funke, S., Har-Peled, S., K . nemann, J., Ramos, EA. and Skutella, M. (2004). Approximating k-hop minimum-spanning trees. Elsevier B.V Journal.

[17] Stojmenovic, I. and Wu, J. (2004). Broadcasting and Activity-Scheduling in Ad Hoc Networks. IEEE Press.

[18] Chen, X. and Wu ,J.(2003). Multicasting techniques in mobile ad hoc networks. CRC Press, Inc.

[19] Hornby G. S. (2003). Generative representations for evolutionary design automation. Ph.D. Dissertation, Department of Computer Science, Brandeis University, Waltham, MA, USA.

[20] Lipman, J. Boustead, P. Chicharo, J. Judge, J. (2003). Optimised Flooding Algorithms for Ad-Hoc Networks. Proceedings of the 2nd Workshop on the Internet, Telecommunications and Signal Processing (WITSP'03), Coolangatta, Gold Coast, Australia.

[21] Lou, W. and Wu, J. (2003). On Reducing Broadcast Redundancy in Ad HocWireless Networks. Proceedings of the 36th Hawaii International Conference on System Sciences.

[22] William, B. and Dinesh, M. (2003). Predictive Modeling of network Wide broadcasting protocols for mobile ad hoc networks. IEEE Transactions on Mobile Computing, TMC.

[23] Wu, Bang. and Chao, K. (2003). Spanning Trees and Optimization Problems. Book, CRC PRESS Boca Raton London New York Washington, D.C.

[24] Chen, X. Nocetti, F. Gonzalez, J. and Stojmenovic, I (2002). Connectivity Based k-hop Clustering in Wireless Networks. Proceedings of the 35th Hawaii International Conference on System Sciences.

[25] Sason, Y. and Kevin, D. (2002). Probabilistic broadcast for flooding in wireless mobile ad hoc networks. Technical Report IC/2002 54.

[26] William, B. and Camp, T. (2002). Comparison of broadcasting techniques for mobile ad hoc networks. In Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC).

ISSN Application No. 21722

Intruder Itinerary Prediction Techniques using Wireless Sensor Networks: A Survey

[1] Khelifa Benahmed, [2] Tariq Benahmed
[1,2]Dept of Mathematics and informatics, Tahri Mohammed University, Bechar, Algeria
E-mail: [1]benahmed_khelifa@yahoo.fr, [2]tarikben3@gmail.com

ABSTRACT

In recent years, almost all the countries are facing threats from terrorists and intruders from their border areas, challenging the internal security of the country in those areas, despite the existence of advanced defense systems, attacks and intrusions still occur. Defense systems tried to stop ongoing attacks and detect occurred attacks. However, often the damage caused by an attack is catastrophic. Intruder itinerary prediction is an important capability and difficult task that can help us to make a one step ahead prediction against possible serious intruders, and automatically responding to attacks in a timely manner. Our research presents a survey of existing intruder itinerary prediction using WSNs techniques.

Keywords - Intruder, Attack, Itinerary Prediction, Wireless Sensor Networks.

I. INTRODUCTION

The continuous evolution in wireless sensor network technology make it possible to implement the wireless sensor networks (WSNs) in a variety of scenarios, one of this scenarios is the intruder localization, each position given by a sensor is used to reach an important technology for ensuring safety of countries especially critical areas which is the intruder trajectory prediction.

The trajectory, which is a moving path of an object, can be described as a series of line segments [1], predicting the itinerary (trajectory) of a moving object has become a necessary job, a lot of research has addressed to the intruder tracking, monitoring and surveillance using WSN, but a few of them have dealt with the itinerary prediction. The purpose of this paper is to introduce, summarize and compare some of the trajectory prediction techniques currently used. Among this techniques we will talk about Hidden Markov Model (HMM), Bayesian network, Kalman filter, Artificial Neural Networks and linear regression.

II.RELATED WORK

Approaches to the trajectory prediction problem largely depend on the underlying assumptions about the motion of the agent or object of interest. In [2] authors present a Bayesian framework that estimates both the intended goal destination and future trajectory of a mobile agent moving among multiple static obstacles, Pierre et al [3] proposed a method to predict the trajectory of o moving objects in a robotic environment in real-time where the position, velocity, and acceleration are estimated by several neural

networks. In [4] an approach was presented to predict future motion of a moving object based on its past movements, the proposed approach exploits the similarities of short-term movement behaviors by modeling a trajectory as concatenation of short segments.

Wesley et al [5] presents a hybrid method for predicting human mobility on the basis of Hidden Markov Models (HMMs), the proposed approach clusters location histories according to their characteristics, and latter trains an HMM for each cluster. JaeHwei et al [6] proposed a novel approach to estimate the real-time moving trajectory of an object. The object's position is obtained from the image data of a charge coupled device camera, while a state estimator predicts the linear and angular velocities of the moving object. To overcome the uncertainties and noises residing in the input data, a Kalman filter and neural networks are utilized cooperatively. In [7] authors present a series of techniques for predicting a future path of an object moving on a road network, they propose a novel method for predicting a future path of an object in an efficient way by analyzing past trajectories whose changing pattern is similar to that of a current trajectory of a query object. We next present the most used prediction methods.

III. PROBLEM DESCRIPTION

In this paper we study the techniques proposed by the researchers to solve the problem of predicting the future trajectory of an intruder.

Predicting is making claims about something that will happen, often based on information from past and from current state. Trajectory prediction can be divided into two parts: the first which is detection and localization of the target through its evolution inside an area of interest using WSN. The positions of the target will be employed to get the appropriate prediction model and as a result the right trajectory. The second part is the prediction model, many techniques are available but a few of them have been tested, therefore we will see in this paper the most useful models, each technique has its characteristicsits advantages and inconvenient. In the following section we will describe in detail each technique which are presented in Fig.1.

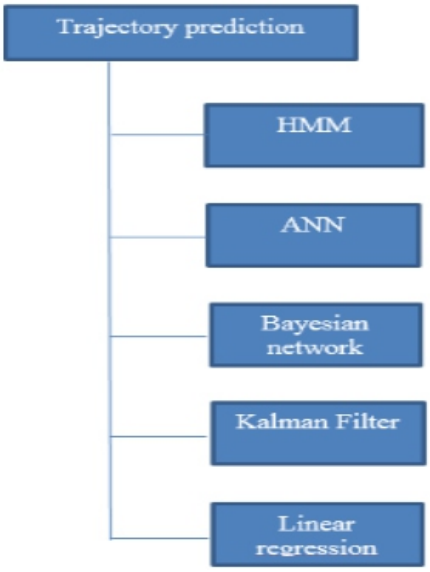

Fig.1. prediction models

IV. TAXONOMY OF TRAJECTORY PREDICTION TECHNIQUES

Intruder trajectory prediction has received Considerable attention in recent years and the solutions can be mainly classified into five schemes:

A. Hidden Markov Model

Hidden Markov Models (HMMs) are a well-known approach for the analysis of sequential data, in which the sequences are assumed to be generated by a Markov process with unobserved (i.e., hidden) states [4]. HMM is a statistical model used to describe the Markov process with unknown parameters. It is often used to look for some changing patterns in a period of time and analysis a system. The state which we hope to predict is hidden in the appearance, and is not what we observed.

a) HMM elements

(1) The hidden states S = { S1 , S2 ,..., SN }, which meet the Markov property, where N indicates the number of hidden states as shown in Fig. 2.

(2) The observed states O = { O1 , O2 ,..., OM }, associated with hidden states in the model, which can be obtained by direct observation (the number of observed states is not necessarily equal to the number of hidden states), where M is denoted as the number of observable states.

(3) The initial state probability matrix π represents hidden state probability matrix when in the initial timestamp t = 1. For example, when t = 1, P (S1) = π1 , P (S2) = π2 and P (S3) = π3 , initial state probability matrix π =[π1 , π2 , π3].

(4) The transition probability matrix A of hidden states, describes the transition probability between hidden states in HMM, where aij = P(Sj | Si), 1 ≤ I , j ≤ N , indicates that in timestamp t+1, the probability of state S j is aij , in the condition of state Si in times tamp t.

(5) The Confusion Matrix B of observed states, describes the transition probability between the hidden states and observed states in HMM, where bij = P (Oi | Sj) (1 ≤ i ≤ M ,1 ≤ j ≤ N) represents what the probability of observed state Oi is in the condition of hidden state Sj in times tamp t.

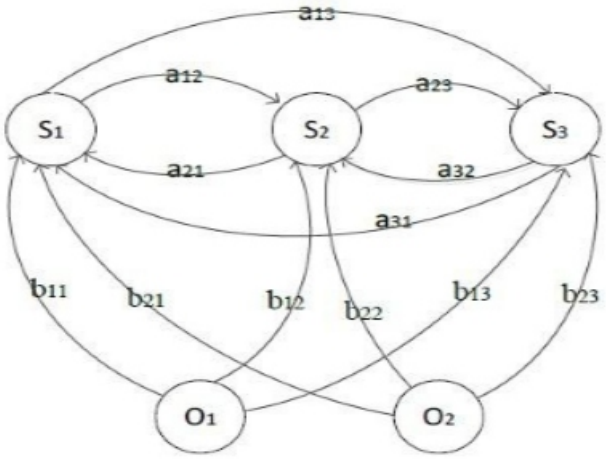

Fig. 2. Example of an HMM.

b) HMM basic problems

Learning, decoding, evaluation [8]

Learning: determines the parameters of the model. Can be solved by the Baum-Welch algorithm.

Decoding: determines the most probable state sequence. Can be solved by Viterbi algorithm.

Evaluation: computes the probability of the observation sequence. Can be solved by Forward-Backward algorithm.

Forward-Backward algorithms:

The Forward value ($\alpha t(i)$) is the probability of the partial observation sequence, o1 , o2 ,…, ot until time t and given state si at time t. One can solve for $\alpha t(i)$ inductively as follows:

1. Initialization:

$\alpha 1(I) = \pi i\, bi\,(o1), 1 \leq i \geq N$

2. Induction:

$\alpha\, t+1 = [\ N\ \alpha t(i)\, aij\ ]\, bj\,(ot+1), 1 \leq i \geq\ T+1, 1 \leq j \geq N .$

3. Termination:

$p(o \mid \lambda) =\ \ N \alpha T(i) .$

The backward value $\beta t(i)$ is the probability of the partial observation sequence from t+1 to the last time, T, given the state si at time t and the HMM λ . By using induction, $\beta t(i)$ is found as follows:

1. Initialization: $\beta T(i) = 1, 1 \leq i \geq N .$

2. Induction: $\beta\, t\ =\ \ N\ \ aij\, bj(ot)\, \beta t+1\,(j)\ \ , t\ = T-1, T-2, \ldots, 1, 1 \leq i \geq N .$

The backward variable is not used to find the probability $p(o \mid \lambda)$. Later, it will be shown how the backward as well as the forward calculation are used extensively to help one solve the second as well as the third fundamental problem of HMMs.

Viterbi Algorithm:

The complete procedure for finding the best state sequence, which is done via the array ψt(j) , can now be stated as follows:

1. Initialization:

$$\delta 1(i) = \pi i\, bi(o1),\ 1 \le i \ge N, \psi 1 = 0 .$$

2. Recursion:

$$\delta t(j) = max\ 1 \le i \ge N\ [\delta t-1(i)\ aij\ ]\ bj(ot)\ , 2 \le t \ge T,\ 1 \le j \ge N .$$

$$\psi t(j) = arg\ max\ 1 \le i \ge N\ [\delta t-1(i)\ aij\ ], 2 \le t \ge T\ ,\ 1 \le j \ge N .$$

3. Termination:

$$p* = max\ 1 \le i \ge N\ [\delta T(i)\ ].$$

$$p*T = arg\ max\ 1 \le i \ge N\ [\delta T(i)\ ] .$$

4. Path (state sequence) backtracking:

$$p*T = \psi\, t+1\ (p*t+1)\ , t = T-1, T-2, \ldots, 1$$

Baum-Welch algorithm:

To be able to re-estimate the model parameters, using the Baum-Welch method, one should start with defining ξt(i,j) , the probability of being in state si at time t, and state sj at time t+1, given the model and the observations sequence. In other words the variable can be defined using the forward and backward variables as follows:

$$\xi(i,j) = \frac{\alpha t(i)\ aij\ bj\ (\ Ot+1\ )\ \beta t+1\ (j)}{p(\ O \mid \lambda\ )}$$

$$= \frac{\alpha t(i)\ aij\ bj\ (\ Ot+1\ )\ \beta t+1\ (j)}{\sum_{i=1}^{N} \sum_{j=1}^{N} \alpha t(i)\ aij\ bj(\ Ot+1\ )\ \beta t+1(j)}$$

By using these interpretations, a method for the re- estimation of the model parameters Π,A,B for the HMM is as follows:

$$\pi i = \gamma 1(i) \qquad (1)$$

One should see that last equation can be interpreted as the frequency in state s i at time t=1. The next equation should be interpreted as the expected number of transitions from state si to sj divided by the number of transitions from state si .

$$\dot{\alpha} j = \frac{\sum_{t=1}^{T-1} \xi t\ i,j}{\sum_{t=1}^{T-1} \gamma\ t\ i} \qquad (2)$$

And finally, next can be seen as the expected number of times in state s j and observing the symbol νk , divided by the expected number of times in state sj .

$$b_j(v_k) = \frac{\sum_{t=1}^{T-1} \gamma_{tj}}{\sum_{t=1}^{T-1} \gamma_{tj}} \quad (3)$$

c) HMM as predictor

The objective of predicting is to estimate the probability of hidden state Si,t at time t, given the condition that observable state Ok,t is obtained at the same time, i.e., Pr(Si,t | Ok,t) . The challenge is to determine the hidden parameters from the observable parameters. There are three parameters, which represent the overall HMM model λ (λ={A,B,Π}): [9]

1. Transition matrix (A)
2. Observation emission matrix (B),
3. Initial probability matrix (π) of a HMM.

d) Prediction steps

The prediction steps change from a case to another it depends on what we want to predict positions, prices,...etc. However there are three basic steps that does not change, the first one is the model construction using Baum-Welch algorithm, the second step is to find the most probable current state using the Viterbi algorithm, the third step is computing the likelihood of the sequence using forward algorithm.

B. Artificial Neural Networks

Work on artificial neural network has been motivated right from its inception by the recognition that the human brain computes in an entirely different way from the conventional digital computer. The brain is a highly complex, nonlinear, and parallel computer (information-processing system). It has the capability to organize its structural constituent, known as neurons, so as to perform certain computations (e.g., pattern recognition, perception, and motor control) many times faster than the fastest digital computer in existence today [10].

ANN is a mathematical model or computational model based on biological neural networks. It consists of an interconnected group of artificial neurons, and processes information using a connectionist approach to computation. An artificial neuron is a simple unit that computes a linear, weighted sum with an additional output function. Perhaps, the greatest advantage of ANNs is their ability to be used as an arbitrary function approximation mechanism that 'learns' from observed data [11].

The most important neural network type is the Multi- Layer Perceptron (MLP) with strict feed-forward architecture of three layers. The connections between inputs and outputs are typically made via one or

more hidden layers of neurons or nodes. The input layer is defined to assume the values of the input vector and does not perform any additional computation, the hidden layer of neurons or nodes is fully connected to the input and output layers and usually uses the sigmoid function as output function.[11]

ANN techniques are successfully applied in various fields such as pattern recognition, control systems and signal processing,...etc [8].

A simple neural network can be represented as shown in Fig.3.

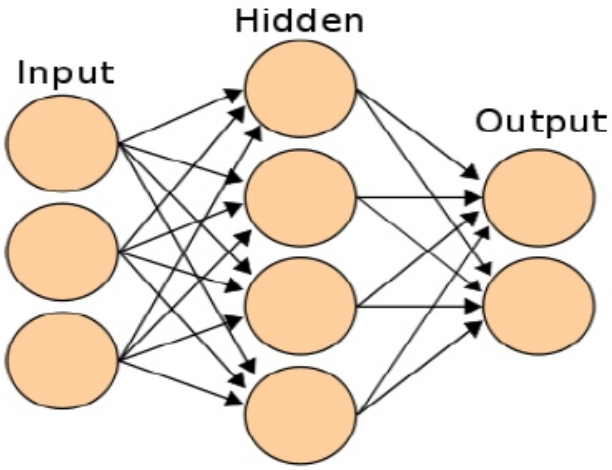

Fig. 3. A simple neural network

The only known values in the diagram are the inputs. Artificial Neural Networks (ANNs) are most often chosen for its ability to generalize results from unseen data, especially for dynamic systems on real time basis. ANNs are parallel computational models comprised of densely interconnected adaptive processing units. ANNs can identify and learn correlated patterns between input data sets and corresponding actual target values. ANNs are networks of highly interconnected neural computing elements that have the ability to respond to input stimuli and to learn to adapt to the environment. ANN includes two working phases, the phase of learning and that of recall. During the learning phase, known data sets are commonly used as a training signal in input and output layers. The recall phase is perfumed by one pass using the weight obtained in the learning phase. [12]

ANN model has equation formula (1) where nj is the j neuron from output layer of neural network, ni is the i neuron from input layer of neural network, wij is the weight between i neuron from input layer and j neuron from output layer (weight score between 1 and +1), bj is the j bias (Bias score is -1 or +1), and wj is the j bias weight.

$$nj = ni\ wij + bj\ wj \quad (4)$$

Artificial Neural Network (ANN) model is adaptable model and often used to compare each prediction possibility. These are important things to consider in designing ANN model for prediction:

1. The number of input neurons: This number is determined based on the database.

2. The number of hidden layer: The number of hidden layer neuron depends on the number of inputs and property data.

3. The number of hidden neurons: A commonly used technique in determining the number of hidden neurons is calculated experimentally.

4. The number of output neurons: Generally, ANN application and research for predictions use one neuron output.

5. Activation Function: Activation functions are used to determine the output of processed neurons.

a) ANN training

Training on Artificial Neural Network (ANN) includes an iterative process of the input data so the appropriate network and can be used for prediction. The purpose of training is to minimize the error, which indicates that the ANN model is in conformity with the input, in general the back propagation algorithm is used.[13]

C. Bayesian Network

Bayesian network is used as a powerful tool to help managers decide in uncertain situations. Bayesian networks can consider a set of relationships between variables and the confrontation uncertainty in expert systems .The basis of Bayesian network structure is the Bayes rule that can be expressed as follows: [14]

$$p(A|B) = p(A \Lambda B)/p(B) \quad (5)$$

Bayesian networks is a formalization of the human way of reasoning using propositional logic in combination with uncertain events. The definition of a Bayesian network given by Jensen [14] is: A Bayesian network consists of the following:

- A set of variables and a set of directed edges between variables.
- Each variable has a finite set of mutually exclusive states.

- The variables together with the directed edges form a directed acyclic graph. (A directed graph is acyclic if there is no directed path A1 ! . . . ! An s.t. A 1 = A n .)
- To each variable A with parents B1, . . . ,Bn, there is attached the potential table P(A|B1, . . . ,Bn).

A Bayesian predictor uses the conditional likelihood of actions represented by variables applying the Bayesian formula on a Bayesian network model. A Bayesian network is a directed acyclic graph of nodes representing random variables (Xi) and arcs representing dependencies between the variables. In case there is an arc from X1 to X2 then node X1 is a parent of node X2. Each variable takes values from a finite set and specific probabilities for those values. To calculate the joint probability distribution the following chain rule is used: [15].

$$p\,X\,1\,,\,.\,.\,.\,.\,,\,X\,n = n\,(\,X\,i\,|\text{parents}(\,X\,i\,)\qquad(6)$$

a) BN advantages

A Bayesian Network fills a role very similar to other Machine Learning algorithms such as an Artificial Neural Network (ANN), Decision Tree, or Support Vector Machine (SVM). However, a Bayesian Network has several unique advantages over some of the other Machine Learning algorithms. [15]

First, a Bayesian Network handles missing values very well.

Second, a Bayesian Network can be queried.

b) Kalman Filter

In 1960, R.E. Kalman published an article entitled "A new Approach to Linear Filtering and Prediction Problems". His research leads him to describe a process that will be known as the Kalman filter.

The Kalman filter is a set of mathematical equations that allows a better estimation of the future state of a system despite the inaccuracy of measurements and modeling.[16]. The filter is very powerful because it supports the estimations of past, present, and even future states, and it can do so even when the precise nature of the modeled system is unknown.

- **Dynamic system model**

Kalman filters are based on discrete linear dynamic systems. They are often modeled on a Markov chain with linear operators and Gaussian noise. At each time increment(discrete), this linear operator is applied to the current state to get the new state with some noise. The Kalman filter is similar to a Hidden Markov model(HMM) with one main difference. A Hidden Markov model can represent any arbitrary

distribution for the next value whereas in the Kalman filter it is Gaussian. The Kalman filter assumes that the state at time k evolves from the state at time (k-1) according to: [16]

$$Xk = Fk\ Xk - 1 + wk \qquad (7)$$

where :

Fk is the state transition model wk is the process noise.

This equation is called the dynamic (plant) equation or the system equation.

- **The algorithm**

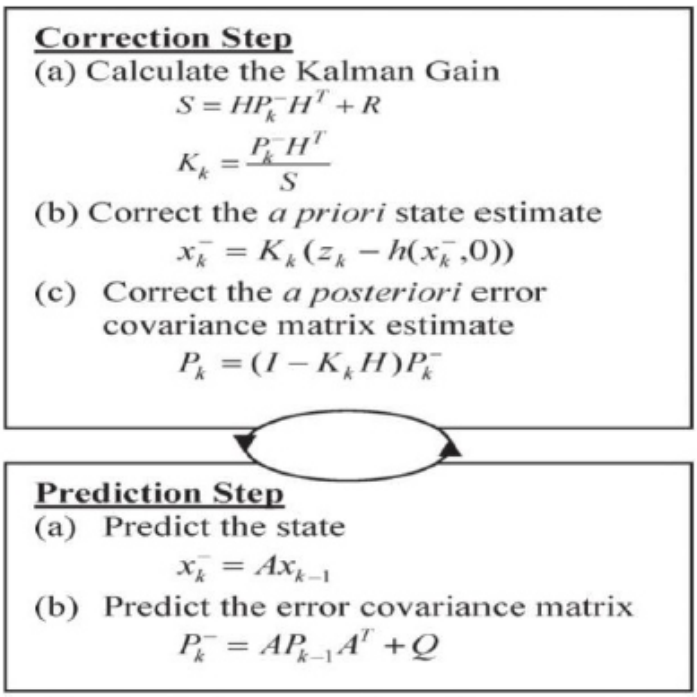

Fig.4. Kalman filter

The Kalman filter uses the previous estimated state and the current measurement to calculate the estimate of the current state. This means that it doesn't need historical values like a batch estimator and hence it is a recursive estimator. The state is represented by two variables: Xk , which is the state estimate given observations till time k and Pk , which is the estimated error covariance matrix or in simple words the a measure of the estimated accuracy of the state estimate. There are two stages in the Kalman filter algorithm namely: [17]

1. Prediction
2. Correction

The KF estimates a process by using a form of a feedback control loop. The filter estimates the process state at some time and then obtains feedback in the form of (noisy) measurements, and then, it repeats (see Fig. 4). In Fig. 4, the following notation holds:

x state estimate

z measurement data

A Jacobian of the system model with respect to state H Jacobian of the measurement model

Q process-noise covariance

R measurement-noise covariance K Kalman gain

P estimated error covariance σ p prediction noise

σ m measurement noise

As such, the equations for the KF fall into two groups: the "prediction step" and the "correction step." The prediction step equations are responsible for projecting forward (in time) the current state and error-covariance estimates to obtain the a priori estimates for the next time step. The correction step equations are responsible for the feedback, i.e., for incorporating a new measurement into the a priori estimate to obtain an improved a posteriori estimate.

D. Linear regression

Linear regression is a model that predicts a relationship of direct proportionality between the dependent variable (plotted on the vertical or Y axis) and the predictor variables (plotted on the X axis) that produces a straight line.[18]

Linear regression was the first type of regression analysis to be studied rigorously, and has been used extensively in practical applications. This is due to the fact that regression models which linearly depend on their parameters are easier to fit than non-linear regression models. In statistics, a linear model uses a linear function f(x) to represent the relationship between a dependent random variable Y and a k-dimensional vector of predictor variables x. When we have a sample (xi,yi) of n observations, in most cases it is not possible to find a linear function f(x) of the k- dimensional input vector x for which Equation yi=f(xi) holds for all i (1, . . . , n). So this inequality is modeled through a so called error i which is an unobserved random variable that adds noise to the linear relationship between the dependent variable and regressors. [18]

V. COMPARATIVE STUDY

The aim of this study was to present the most useful prediction tools and finally to compare between them.

In order to evaluate the prediction tools, the Table 1 bellow sums up a comparison between the techniques explained above, each one of them have its operating principle, its characteristics (features), its advantages and disadvantages.

prediction techniques	Operating principle	Features	Advantages	Disadvantages
HMM	• Set of states • probability of occurrence of a state depends only on the previous state • forward-backward algorithms • Baum-welsh algorithm • Viterbi algorithm	• Hidden states • Analysis sequential data • Three parameters ($\lambda=\{A,B,\Pi\}$	• Efficient learning algorithms • Strong statistical foundation • Wide variety of applications	• cannot express dependencies between hidden states • HMMs often have a large number of unstructured parameters.
ANN	• group of artificial neurons • ANN basically sums the signal from its inputs multiplying them with the correspondent weights. • if the result exceeds the threshold the neuron fires and a signal is transmitted at the output by a transfer function	• ANN is nonlinear model • ANN is non-parametric model. • robust performance in dealing with noisy or incomplete input patterns • made up of computing elements • analyze quickly complex patterns with a high degree of accuracy	• high fault tolerance • ability to detect all possible interactions between predictor variables • an ANN can be used successfully as tools for short term prediction and forecasting	• An ANN is not a universal tool of solving problems, a methodology for choosing, training and verifying an ANN doesn't exists. • ANN requires excessive training times
BN	• Bayes rule • set of variables • set of directed edges between variables • use the conditional likelihood of actions represented by variables • applying the Bayesian formula on a Bayesian network model	• directed acyclic graph of nodes representing random variables and arcs representing dependencies between the variables	• Missing data entries can be handled successfully. • can perform several types of reasoning	• computational difficulty of exploring a previously unknown network • Calculate the probability of any branch of the network, all branches must be calculated.
Kalman filter	• based on discrete linear dynamic systems • two stages: prediction & correction • Uses the previous estimated state and the current measurement to calculate the estimate of the current state. • estimates a process by using a form of a	• set of mathematical equations • estimate the future state of a system despite the inaccuracy of measurements and modeling • supports the estimations of past, present, and even future state	• provides the optimal estimate of the states of a stochastic dynamical system • Its recursive structure allows its real-time execution without storing observations or past estimates • KF is able to take into account quantities that are	• Some systems are hardly modelable •Imprecise/incorrect knowledge of the state dynamics and measurement models
	feedback control loop		partially or completely neglected in other techniques	

Linear regression	• predicts a relationship of direct proportionality between the dependent variable and the predictor variables	• linear function • predicting the value of a dependent variable from an independent variable	• more simple	• Linear regression is limited to predicting numeric output. • A lack of explanation about what has been learned can be a problem.

TABLE 1. TECHNIQUES COMPARISON

VI. CONCLUSION

In this paper, we have presented five most used prediction techniques especially in trajectory prediction, and a simple comparison between them based on their operating principle, their features, advantages and disadvantages. In addition to the studied prediction models there are two other methods available: Statistical analysis like Autoregressive Moving Average (ARMA) model and Support Vector Machine (SVM).

REFERENCES

[1] Yiwen S, Kyung T K, Jong C P, and Hee Y Y," Object Tracking based on the Prediction of Trajectory in Wireless Sensor Networks", 2013 IEEE International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing.

[2] Graeme B, Robert F, " Bayesian Intention Inference for Trajectory Prediction with an Unknown Goal Destination", IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), Hamburg, Germany, 2015.

[3] Pierre P, Hong Le-H, Clement M, " Trajectory prediction for moving objects using Artificial neural networks ", IEEE Transactions on Industrial Electronics, vol. 42, no. 2, April 1995.

[4] Sang-W K, Jung-I W, Jong-D K, Miyoung S, Junghoon L, and Hanil K, " Path Prediction of Moving Objects on Road Networks Through Analyzing Past Trajectories ", Springer- Verlag Berlin Heidelberg 2007, Part I, LNAI 4692, pp. 379– 389, 2007.

[5] Wesley M, Ruben R, Bruno M, "Predicting Future Locations with Hidden Markov Models", ACM journal, Pittsburgh, USA., 2012.

[6] JaeHwei P, JaeMu Y and JangMyung L," Trajectory estimation of a moving object using Kalman filter and Kohonen networks", Cambridge University Press, Robotica (2007) volume 25, pp. 567–574, 2007.

[7] Hoyoung J, Qing L, Heng Tao S, Xiaofang Z," A Hybrid Prediction Model for Moving Objects", in proceeding of IEEE 24th International Conference on Data Engineering, pp. 70-79 ,2008.

[8] L. R. Rabiner, " A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition " Proceedings of the IEEE, vol. 77, pp. 257-286, 1989.

[9] Afrah R.S, " Comparative Study of Artificial Neural Networks and Hidden Markov Model for Financial Time Series Prediction ", the international journal of engineering and information technology (IJEIT), vol. 1, no. 2, 2015.

[10] S. Haykin, " Neural Networks", A Comprehensive Foundation, New York, Macmillan Publishing., 1994.

[11] Y. Bengio, Y. LeCun, C. Nohl, and C. Burges, "A NN/HMM Hybrid for On-Line Handwriting Recognition, " Neural Computation, vol. 7, pp. 1289-1303, 1995.

[12] Hening Titi C, Chastine F, Altea S," Network Traffic Anomaly Prediction Using Artificial Neural Network", Engineering International Conference (EIC), AIP Conference Proceedings, 2016.

[13] M. H. Eng, Y. Li, Q. G. Wang, and T. H. Lee, " Forecast Forex with Artificial Neural Network Using Fundamental Data, " 2009, pp. 279-282.

[14] F. V. Jensen, "An Introduction to Bayesian Networks", UCL Press, 1996.

[15] F. V. Jensen, " Bayesian Networks and Decision Graphs", Springer, 2001.

[16] C. Hilde, T. Moore, and M. Smith, " Multiple Model Kalman Filtering for GPS and Low-Cost INS Integration.", Nottingham, U.K.: Inst. Eng., Surveying Space Geodesy, Univ. Nottingham, 2004.

[17] Cesar B and Yuichi M, "Improving Estimation of Vehicle's Trajectory Using the Latest Global Positioning System With Kalman Filtering", IEEE Transactions On Instrumentation And Measurement, vol. 60, no. 12, December 2011.

[18] M. Ghasemi Hamed, D. Gianazza, M. Serrurier, N. D, "Statistical prediction of aircraft trajectory: regression methods vs point-mass model", ATM 2013, 10th USA/Europe Air Tra_c Management Research and Development Seminar, Chicago, 2013.

ISSN Application No. 21722

Wireless Sensor Network based Healthcare Monitoring System

[1] D. B. Karhale, [2] S. B. Thorat, [3] Tazeen Khan
[1]School of Computational Sciences, SRTMU, Nanded, Maharashtra, India
[2]Institute of Technology & Management, SRTMU, Nanded, Maharashtra, India
[3]TIBCO Software, Chandivali, Powai, Mumbai - 400072
E-mail: [1]deepa_karhale@yahoo.com, [2]suryakant_thorat@yahoo.com

ABSTRACT

The healthcare monitoring systems have emerged as one of the most vital systems and became technology oriented from the past decade. Humans are facing a problem of unexpected death due to various diseases which are because of lack of medical care to the patients at right time. Technology plays the major role in healthcare system, not only for recording parameters through sensor devices but also in communicating, recording and displaying the measured parameter. It is very important to monitor various medical parameters and post operational data. The main objective of this paper is to transmitting the patient"s health monitoring parameters through wireless communication. These input data are uploaded in cloud server and transmitted to the computer for doctor"s reference. The healthcare system is setup using Raspberry Pi, web technology and Cloud.

Keywords - CLOUD, Raspberry Pi, WHO, PMS, ECG.

I. INTRODUCTION

Health is one of the global challenges for humanity. According to the constitution of World Health Organization (WHO) the uppermost possible standard of health is a fundamental right for an individual. Healthy individuals also diminish pressure on the already overwhelmed hospitals, clinics, and medical professionals and reduce workload on the public safety networks, charities, and governmental (or non-governmental) organizations. To keep individuals healthy an effective and readily accessible modern healthcare system is a prerequisite [1]. A modernized healthcare system should provide better healthcare services to people at any time and from anywhere in an economic and patient friendly manner. Currently,[2] the healthcare system is undergoing a cultural shift from a traditional approach to a modernized patient centered approach. In the traditional approach the healthcare professionals plays the major role. They need to visit the patients for necessary diagnosis and advising. There are two basic problems associated with this approach. Firstly, the healthcare professionals must be on site of the patient all the time and secondly, the patient remains admitted in a hospital, wired to bedside biomedical instruments, for a period of time. In order to solve these two problems, [3] the patient oriented approach has been conceived. In this method the patients are equipped with knowledge and information to play a more active part in disease diagnosis, and prevention. The key element of this second approach is a reliable and readily available Patient Monitoring System (PMS). The essential for a real time recording

and notification of vital signs of a patient is of prime importance for an effective PMS. By summarizing the advantages of modern bio instrumentation, computers, and telecommunication technologies a modern PMS should acquire, record, display, and transmit the physiological data from the patient body to a remote location at same time.

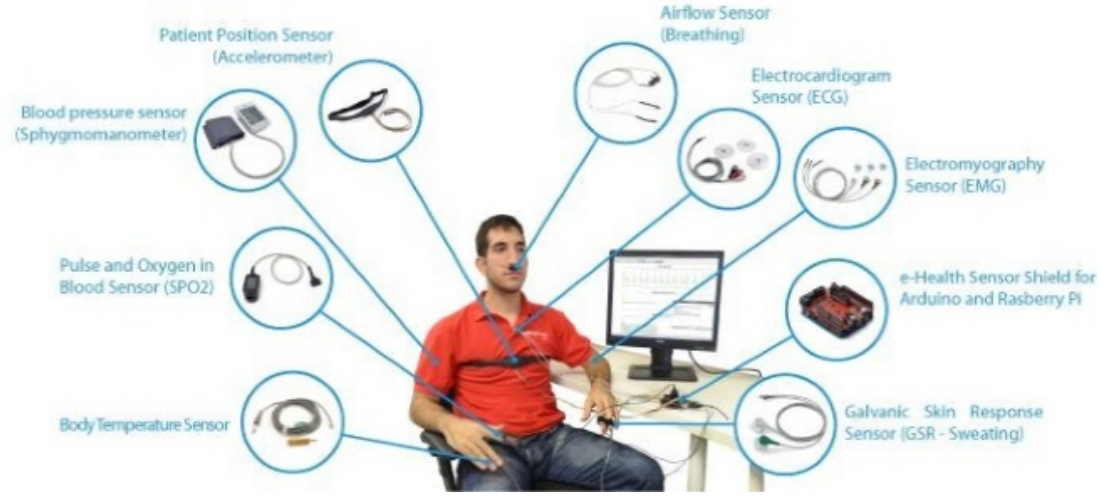

Figure 1: Application of Different types of sensors on human body externally [5]

For more efficient, timely, and emergency medical care, the PMS must also be equipped with an alarm system. In order to alert the patient as well as the health care service providers, the PMS should not only monitor and analyze the serious patient‟s data but it should also send alarming messages in case the monitored data when goes outside their normal ranges. Hence, an active database system must be associated with the PMS. Most of the proposed PMS are centralized in a sense that all patient‟s data are stored in a single server, by using necessary firmware and software, the server can be connected to an open communication network via TCP/IP protocol. Thus a patient can be monitored from a remote location. Existing and widespread mobile phone networks can assist in this regard. Recently, [4] mobile networks are considered critical for solving future global health challenges. With the global market penetration of the mobile phones the mobile healthcare system is a matured idea now. By use of the mobile phone, healthcare system can be made available for people, who are living in remote areas without much access to other types of communications. Even a simple mobile phone can become a powerful healthcare tool now. Text messages and phone calls can quickly deliver real-time and critical information of a patient to a remote location. Thus the patients, living in remote areas, can reduce needless back-and-forth travel to the far located healthcare centers. Figure 1 shows application of different types of sensors on human body externally[5].

II.LITERATURE REVIEW

S. J. Jung and W. Y. Chung studied the Flexible and scalable patient‟s health monitoring system in 6LoWPAN. The main advantage of this enabling factor is the combination of some technologies and communications solution. The results of Internet of Things (IoT) are synergetic activities gathered in various fields of knowledge like telecommunications, informatics and electronics.

K. S. Shin and M. J. Mao Kaiver studied a cell phone based health monitoring system with self-analysis which incorporates IoT [6], a new paradigm that uses smart objects which are not only capable of collecting the information from the environment and interacting with the physical world, but also to be interconnected with each other through internet to exchange data as well as information.

Gennaro tartarisco and Tabilo Paniclo had studied a maintaining sensing coverage and connectivity in large sensor networks which mainly includes the information about how to build or develop a new computational technology based on clinical decision support systems, information processing, wireless communication and also data mining kept in a new premises in the field of personal health care.

Cristina Elena Turcua studied Health care applications; a solution based on the Internet of Things (IoT) survey which aims to present detailed information about how radio frequency identification, multi-agent and Internet of Things (IoT) technologies can be used to develop and improve people‟s access to quality and health care services and to optimize the health care process.

Gubbi, Jayavardhana, Buyya, Rajkumar, Marusic, Slaven, Palaniswami, Marimuth studied the Internet of Things (IoT): A vision, architectural elements, and future direction which propose on demand positioning and tracking system. It is based on Global Positioning enabled devices and suitable for large environments. Smart phones between two terminals are used for making initial communication. The initial communication is performed by synchronization phase.

J.L. Kalju developed a system, which is capable of measuring different physiological parameters and are used to design a system for heart rate reconstruction for rate adaptive pacing.

Loren Schwiebert, Sandeep K.S. Gupta and Jennifer Weinmann studied the strength of smart sensors which are developed from the combination of sensing materials along with combined circuitry for other biomedical applications.

Gentili G.B proposed a simple microwave technique to monitor the cardiac activity. This technique is dependent on changes in modulation envelope of amplitude modulated waves passing through the body. It explained the use of wireless micro sensor networks for medical monitoring and environmental sensing.

Reza S.Dilmaghani (2016) in their study found the design of Wi-Fi sensor network that is capable of monitoring patient‟s chronic diseases at their home itself via a remote monitoring system. So emerging of wireless sensor technology with individual test like only blood pressure, heart rate, temperature etc. can be measured however this research project enable all this parameter together to be measured under single system, and also thus all can be worn by patient and processed data is send to internet through internet of things (IOT) [7].

III. PROPOSED SYSTEM

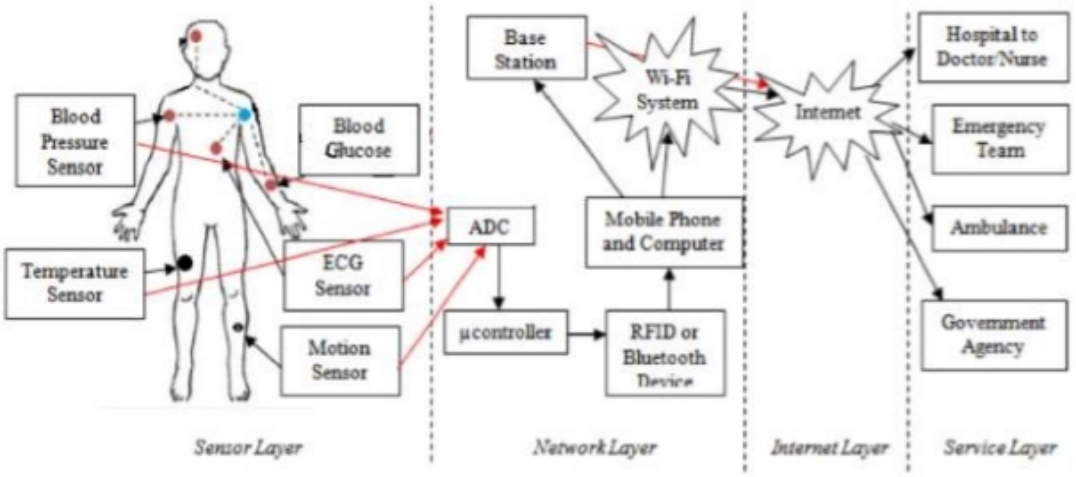

Figure 2: Proposed Wireless Sensor Network Based Health Monitoring System

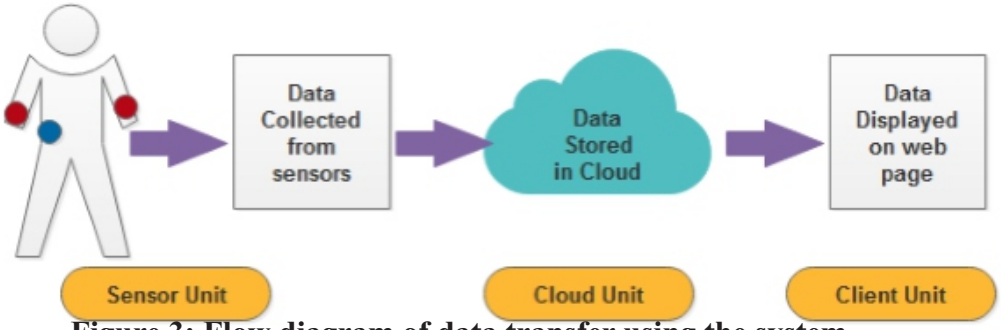

Figure 3: Flow diagram of data transfer using the system

Figure 4 is a Proposed Wireless Sensor Network Based Health Monitoring System

Figure 3 shows the Flow diagram of data transfer using the system. Different types of sensors applied on human body and collected data from sensors that data will be stored on cloud and the data will be displayed on web page for client uses or doctor‟s uses.

Figure 5 represents Wireless Sensor Network‟s Cloud Server Architecture WSN (wireless sensor networks) based real- time health monitoring system comprises association between micro controller and actuator to procure faithful estimation, real-time monitoring and evaluating the cases condition & eventually grows the strength of this technology in healthcare. Proposed framework contains ECG sensor, Blood Pressure sensor, temperature sensor, Motion sensor and Blood Glucose sensor. The combination of micro controller with the smarts sensors offers advantages like as incorporated precision analog capabilities, small power consumption and easy for designing GUI's(Graphical user interface). It consists of the sensors which are attached to human body, Microcontroller, Analog to digital converter (ADC), wireless devices like as Bluetooth, RFID, Mobile Phones, Wi-Fi system, Internet devices and patient is monitored by doctors/nurses, hospitals, emergency team, Ambulance, Government Agencies, etc. which provides the facility to the patients for their health monitoring. The sensors continuously collect the real- time information from the patient's body to get the patient details. In case of any emergency, these wireless devices can distantly report the physical condition of the patient to his doctors and/or relatives. In such condition the doctors and hospitals can respond with emergency medical services such as ambulance or provide the necessary actions to the relatives to help the patients. These real-time signals generated from these sensors are in analog form making it necessary to be converted into digital form for which ADC is used. These digitalized signal form the ADC are forwarded to RFID/Bluetooth device through microcontrollers. RFID/B1uetooth devices wirelessly transmits these signal to the mobile phone for the transmission of data through internet to the specific destination. The internet either uses the base station or internet for the transmission purpose.

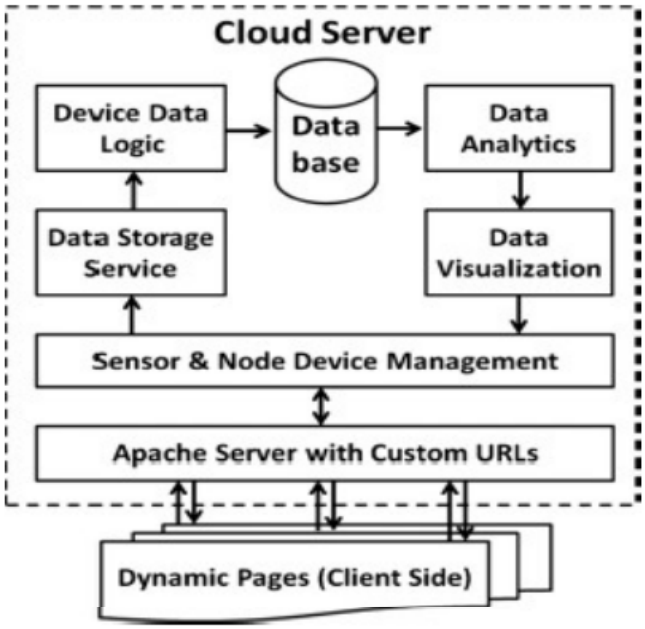

Figure 6 : Wireless Sensor Network's Cloud Server Architecture

IV. EXPERIMENT AND RESULTS

Figure 5 is of ECG sensor connection. An electrocardiogram (ECG) is an examination which measures the electrical activity of your heart to show whether or not it is functioning normally. An ECG can tell a wealth of information about cardiac regulation, as well insights into pathological circumstances.

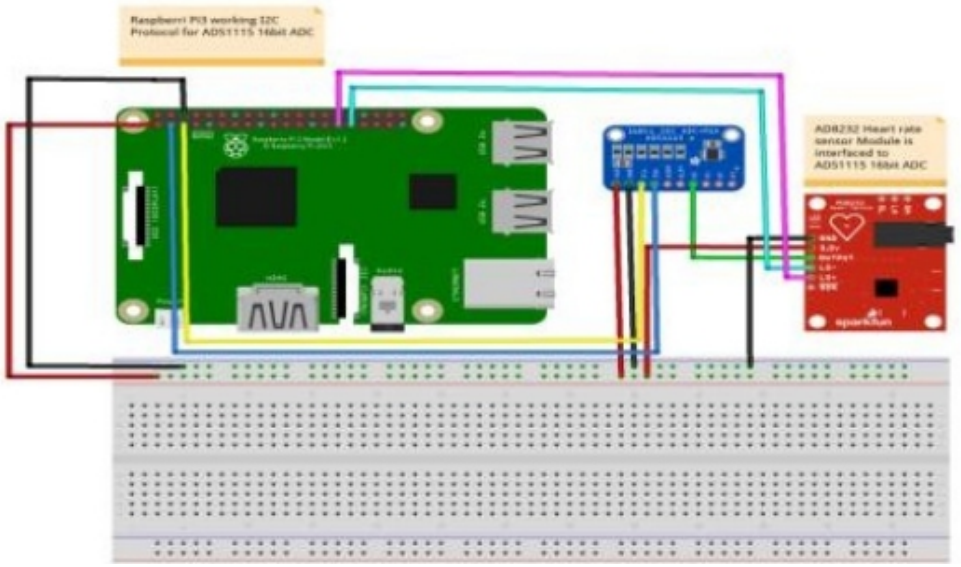

Figure 7 :ECG Sensor Connection on Bread Board

Figure 8 : Snippet of ECG

Figure 6 is a snippet of ECG. An electrocardiogram can be a useful way to find out whether your high blood pressure has caused any damage to your heart or blood vessels.

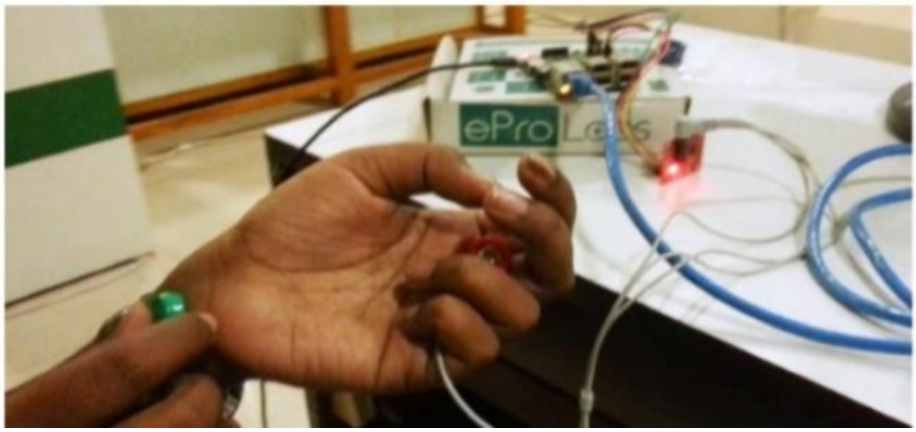

Figure 9: Sensor attachment on Hand

Figure 7 is a representation of sensor attachment on hand. The AD8232 is an integrated signal conditioning block for ECG and other bio potential measurement applications. It is designed to extract, amplify, and filter small bio potential signals in the presence of noisy conditions, such as those created by motion or remote electrode placement. The AD8232 Heart Rate Monitor breaks out nine connections from the IC that you can solder pins, wires, or other connectors to. SDN, LO+, LO-, OUTPUT, 3.3V, GND provide essential pins for operating this monitor with development board. Also provided on this board are RA (Right Arm), LA (Left Arm), and RL (Right Leg) pins to attach and use your own custom sensors. Additionally, there is an LED indicator light that will pulsate to the rhythm of a heartbeat. The ECG signal comes from the ECG circuit AD8232 is microcontroller compatible and maximum amplitude is 3.3V which is not safe for the microphone input of the PC audio. Typically the maximum amplitude of a microphone can be 1V. So, voltage divider circuit is introduced to reduce the amplitude of the ECG signal from 3.3V to 1 volt [8]. The figure 8 shows the waveforms generated by ECG through raspberry pi using web server, this can be viewed on web page. It is useful to both patient and doctor to know ECG values.

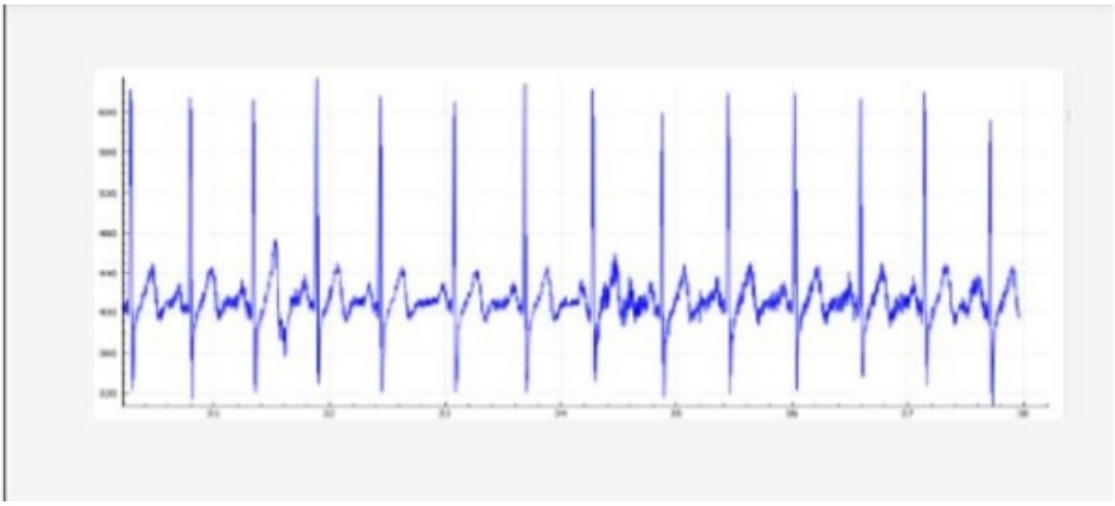

Figure 10 : Generated Waveforms (ECG)

V. CONCLUSION

This paper emphasizess on a real-time healthcare monitoring system using WSN(wireless sensor network) which are more valuable for elder patients and patients having chronic diseases. In this paper has proposed a remote ECG monitoring system. The deployment of the proposed system is done using a prototype developed using Raspberry Pi. Web programing is used to capture the heart-rate sensor data from AD8232 module through 16-bits ADC ADS1115 and publish the data to the web server, the results & outputs are shown and discussed in the experiment and results section of this paper. The End- user in this case a doctor or any medical technician can visualize the data from any internet enabled device Appropriate medications are recommended based on the diagnosis of the provided set of symptoms. The system sends an alert message to the caretakers and doctors in case of any abnormality through WBA (Wireless Body Area Network)The system enables the clinical experts to optimize the usage of available medical resources and minimize the costs in monitoring the patients. In the future, we will focus on improving wearing sensor experience by using softer materials and enabling controlled sharing of information among the doctors, the patient, and the patients‟ family through social networking paradigm.

FUTURE WORK

This work can be extended by developing software modules to detect any ECG pattern and in case of any heath condition should be able to send E-mail or SMS notification or any web based notification to the doctor to make the system automated and for time critical early detection of critical patients.

ACKNOWLEDGMENT

I would like to thank Dr. S. B. Thorat for guidance and support. I will forever remain grateful for constant support and guidance extended by him, for the completion of paper. I am also thankful to Dr. Pritam Patil for his help during the literature search process.

REFERENCES

[1] R.M.Madhumathi, Dr.A.Jagadeesan, S.Kaushik "Healthcare Monitoring System Using Body Sensor Network", International Conference On Engineering Innovations And Solutions (ICEIS-2016), E-ISSN : 2348 – 8549.

[2] Darwish A, and Hassanien AE 2012, „Wearable and Implantable Wireless Sensor Network Solutionsfor Healthcare Monitoring Sensors", 12: 12375-12376.

[3] Ahmed Harbouche, Mohammed Erradi and Abdellatif Kobbane2013, „A Flexible Wireless Body Sensor Network System for Health Monitoring", International Journal of Digital Content Technology and its Applications, vol. 3, no. 3,pp. 185–193.

[4] Fen Miao and Xiuli Miao 2012, „Mobile Healthcare System: Body Sensor Network Based MHealth System for Healthcare Application", E-Health Telecommunication Systems and Networks, 2012, 1,12-18.

[5] https://www.cookinghacks.com/documentation/tutorials/eh ealth-biometric-sensor-platform-arduino-raspberry-pi medical.

[6] Dr.A.Sabanayagam, G.Anish Girija," DESIGN AND MODELING OF MOBILE HEALTH MONITORING SYSTEM", International Journal of Innovations in Scientific and Engineering Research (IJISER),vol4,no 2,pp.63- 65,2017.

[7] C.Senthamilarasi, J.Jansi Rani, B.Vidhya , H.Aritha, "A SMART PATIENT HEALTH MONITORING SYSTEM USING IOT" , International Journal of Pure and Applied Mathematics, Volume 119 No. 16 2018, 59-70, ISSN: 1314-3395 (on-line version) url: http://www.acadpubl.eu/hub/ Special Issue.

[8] Ayaskanta Mishra, Akanksha Kumari, Pooja Sajit, Pranjal Pandey, "REMOTE WEB BASED ECG MONITORING USING MQTT PROTOCOL FOR IOT IN HEALTHCARE", Scientific Journal of Impact Factor (SJIF): 5.71, International Journal of Advance Engineering and Research Development, Volume 5, Issue 04, April - 2018, e-ISSN (O): 2348-4470, p-ISSN (P): 2348-6406.

ISSN Application No. 21722

A Survey in Wireless Sensor Network based on Time Synchronization

[1] RAVI KUMAR, [2] RAJENDER KUMAR

[1,2]Department of Electronics and Communication Engineering, National Institute of Technology, Kurukshetra, India

E-mail: [1]ravikumarakola@gmail.com, [2]rkumar.kkr@gmail.com

A B S T R A C T

Wireless sensor networks is the region in which small devices are spread. Time synchronization plays an important role in the sensor networks. Over the period of time wireless sensor networks has come out to be the most important research field for the scholar. Time synchronization aims to synchronizing the time of different sensor node to the root node to operate them without delay. The main factor that influence the synchronization is send time TS, receive time TR, propagation time TP, temperature change and clock design due to imperfection of quartz crystal. The paper explain different techniques, topology and synchronization algorithms to syncing the child nodes to the root node. The motive of writing this paper is to study different technique, topology and approaches to secure time synchronization and create new synchronization technique and compare the new one to the previous technique and get the better synchronization in the wireless sensor network.

Keywords - Time Synchronization, Root Node, Spanning Tree, Children Find Packets, Broadcast.

I. INTRODUCTION

Sensor network has emerged as a prominent research area in the recent time and it is widely used in the data acquisition, home automation, industrial automation, health monitoring application. In many application involve a large number of sensor and due to imperfection in quartz crystal, temperature, humidity, pressure, and different environment condition the clock run at different frequency and due to which the clock drift arises[1, 3]. The applications of Sensor network requires that the time should be synchronized in the network. TDMA radio scheduling, message ordering, environmental monitoring, mobile object (target) tracking, and data fusioning are some example of its applications. Let the application of mobile object tracking, in which the sensor network is deployed is an area of interest of the monitor passing objects. To detect the object the sub-node detect the position and location of the object and send these information to the main node but the actual location and position of the object is different from the received one, so to avoid this time shift between the real one and the received one we need the proper synchronization of the sensor nodes [2]. This time shift occurs in the sensor network because of send time, settling time and receive time of the sensor nodes. For synchronization of sensor nodes of the network GPS technique is not useful because sensor nodes are very small in size and low energy consumption devices and GPS technique is costly [3]. Conventional techniques that have used in wired network is not suitable in wireless sensor network. Because those technique are frequently used in

internet and very typical to implement and has energy efficiency problem. Sensors are design to confront in the raucous environment and condition. Deployment of extra sensors in the network is only for reduce the redundancy occur in the network because of node failure. Generally node failure happens because of power draining of sensor as we know sensors are very low power device so the life span of the sensors mostly depend on the battery power of the sensor. We use life time of sensor network only at the time of performance evaluation of sensor network and it depend on the total life time of the sensor network not on the single device and total life time of the network is the average life time of all sensor node[4, 7].

This paper propound a novel time synchronization scheme for wireless sensor networks. First it create the spanning tree of all the sensor nodes and then this tree is further divided in sub-tree and then we synchronized these sub-tree with the help of two algorithms and compare the performance reference broadcast synchronization (RBS) in the network. Then we found that the proposed algorithms scheme performance is better than the RBS approach [3, 5, 7]. In the remaining paper we describe synchronization technique, network model, and performance evaluation, and final section gives the conclusion.

II.NETWORK MODEL

Let us assume there are N sensor nodes present in an area A, and each sensor node is triggered by its own clock and has its own notion of time. To synchronize all the sensor node with each other we need a common time scale and common notion of time. First we take a node as the reference node or “root node” and then take the clock of it as a reference to others. This reference or root node will act like a gateway between the external world and the network and will synchronize it to the real world [5]. Then we synchronize the other node to the “root node”, i.e., adjust the clock of other node to the root node. Fig. 1 gives the brief idea of sensor network. In Fig. 1, the circle denotes the area A of the sensor nodes and the red point on the middle of the circle represents the root node. The all other node are directly synchronize with its immediate neighbor and each node in the area A has its own identifier. Link between the sensor nodes is bidirectional to generate the spanning tree and this spanning tree includes all the sensor nodes of the area A and this synchronization technique is mostly spanning tree based.

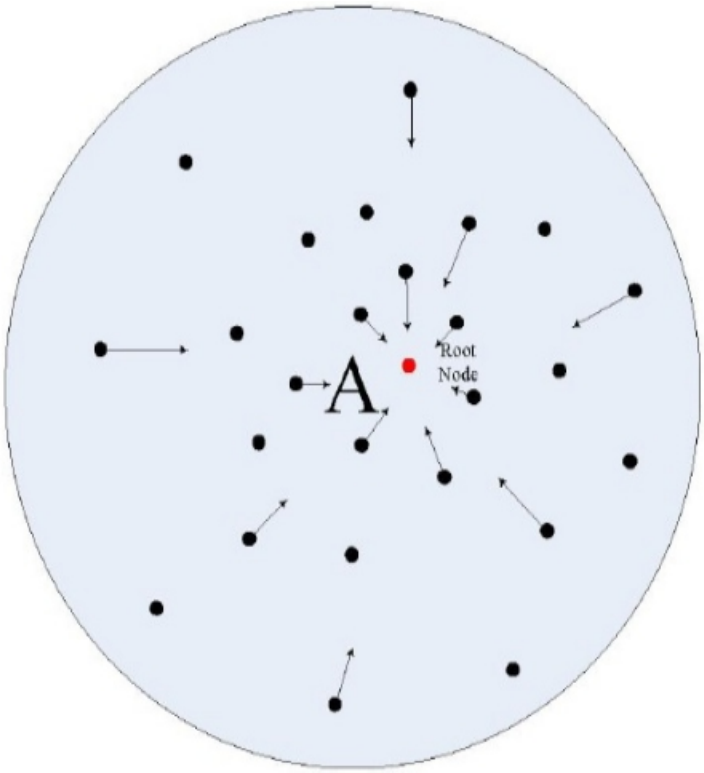

Figure 1. The working model of a Wireless Sensor Network.

III. PROPOUND SYNCHRONIZATION TECHNIQUES

A. The Generation of Spanning Tree

Initially the parent node will enter in to the spanning tree and it will assign as level 0, it has its own identifier and level. After this the root node will search its sub node by transmitting the identifier by child-finding packets. The sub node has its level 1, which is higher than its parent nodes level. Then all the sub node will act like parent node and they transmit there identifier and children find packet to the neighbour and entered in to the spanning tree. This process will keep on moving until the last node of the sensor networks enter in to the spanning tree.

At last we observed that the node that entered in to the spanning tree may encounter the second time children find packet and identifier, and in that case the node will reject those packets. Fig. 2, shows the formation of spanning tree and at last Fig. 3 show the creation of spanning tree.

In Fig. 2 node 0 is the parent node and arrow sign denote the “children find packets (CFP)”. Here the node 6 start transmitting the packets and the identifier and then root node 0 will receive the packet and reject it because node 0 has already entered in to the spanning tree process. This is the packet neglecting process. Fig. 3 will have four level and our synchronization method is based on it.

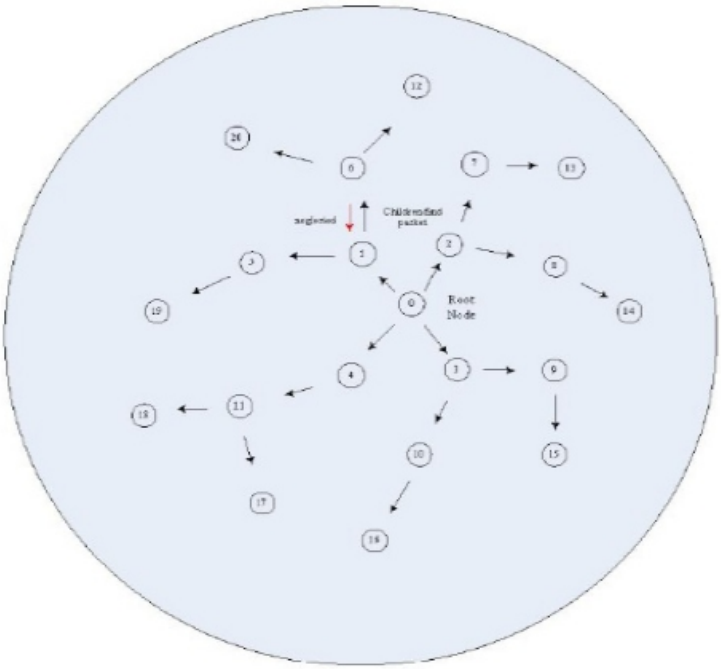

Figure 2. Spanning Tree Formation Process.

B. Techniques used for Synchronisation

Synchronization schemes motive is to adjust the clock frequency of all the node at the reference frequency or the root node clock frequency [3, 7]. There are different technique which are used for synchronization the sensor nodes of the network.

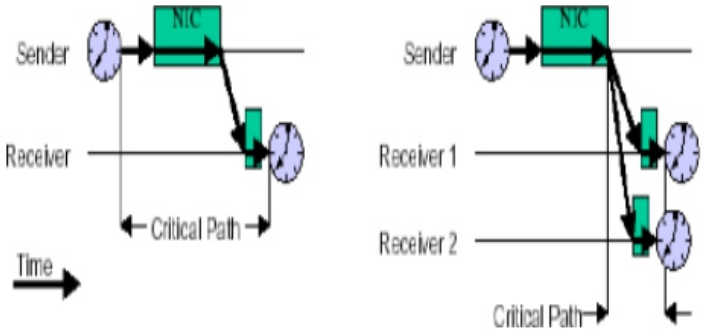

Figure 3. Analysis of conventional time synchronization and Reference Broadcast Synchronization.

1) Conventional Time Synchronization

In conventional time synchronization, network node send the message signal to the receiver, with its current identifier and local time like network time protocol (NTP). Then the receiver adjusts its local clock accordingly to the received one. This technique works only if delay time between the sender and receiver is less. If delay is large, receiver will use that time to synchronize the network and will consider that the node will reply instantaneously and calculate the round trip time [5].

2) Reference Broadcast Synchronization (RBS) The sensor nodes repeatedly send beacon messages to their neighbours using the network's physical-layer broadcast during RBS scheme and beneficially for comparing their clocks, it uses the message's arrival time as a point of reference. Here the message has got no clear timestamp, and also it is not important when it is sent.

The accuracy of RBS is generally calculated by the amount of Time taken by the reference node or time to process it [7]. In Fig. 3, it clearly denote the sender and receiver has drift time which can be calculated by the synchronization algorithms.

C. Propound Synchronization Algorithms

It first define a node and it's all sub-nodes in the spanning tree as a sub-tree and then divide sub-tree from the spanning tree. The sub-tree are identified by its parent node or root node, root node has level 0 and sub tree has level 1 which is one higher than root node's level [3, 8].

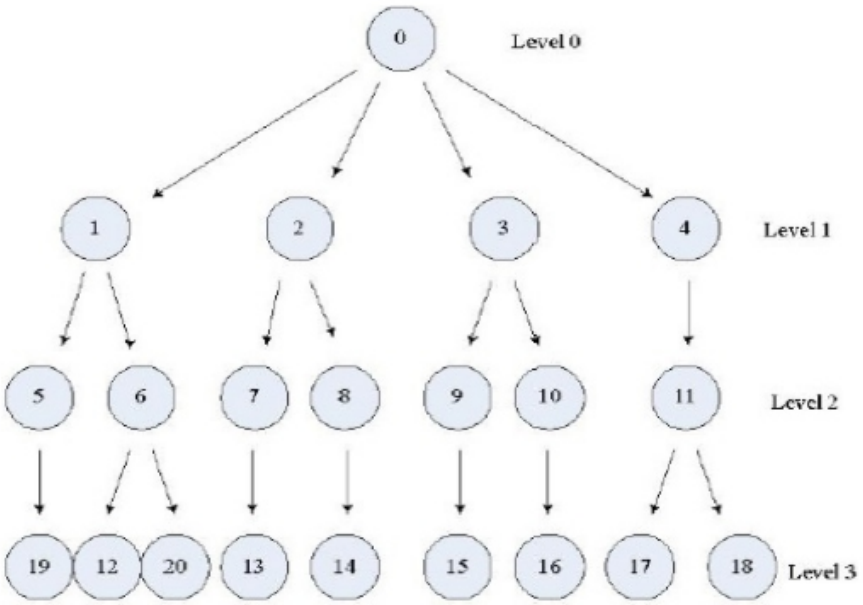

Figure 4. Spanning tree creation.

In sub-tree our goal is to synchronize the parent node to the chid node. And every child node act as a parent node to its child node when it entered in to the spanning tree. And this synchronization method will go on until all the node is synchronizing to the root node. To synchronize the child nodes with the root node we use two algorithms which are as under below.

1) Bi-Directional Message Exchange Algorithm

As shown in Fig. 5, the bidirectional message exchange process each child node, and send the message at time T0 to the father node. And then father node receive the clock sync message at T1. At the same time

the root node send back reply message containing T0 and T1, and child node get reply from the root node at time T2. So we have

$$T_1 = T_O + \alpha + \beta \quad (1)$$

$$T_2 = T_1 - \alpha + \beta \quad (2)$$

Where α denotes the relative time shift between child node and parent node and the propagation delay is denoted by β for the clock modifying message. Let the clock drift be constant between two nodes for a small period of time of a single bidirectional message and the propagation delay is also constant. Therefore from equation (1) and (2) we get,

$$\alpha = \frac{(T_1 - T_o) - (T_2 - T_1)}{2} \quad (3)$$

$$\beta = \frac{(T_1 - T_o) + (T_2 - T_1)}{2} \quad (4)$$

Hence the child node has the knowledge of propagation delay and clock drift and then the local clock is synchronized to the father node.

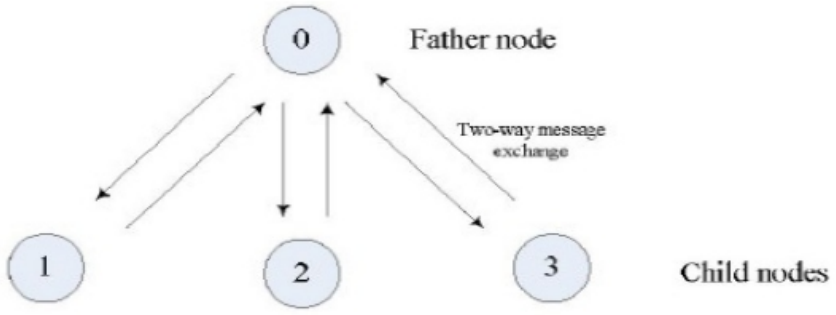

Figure 5. Bidirectional message exchange algorithms

The sub-tree synchronization will be achieved if all the child nodes have synchronized with the father node.

2) Broadcasting based Improved Algorithms

In initial phase, bi-directional message exchange technique between child and father node is used and then synchronize the child node to the parent node.

In second phase father node will transmit clock adjusting message to all children node including the sync child node. When child node receive message signal then it try to exchange with the other one and calculate the clock drift, if father node is synchronized with all the other node, then sub tree synchronization is achieved [2, 4].

So we can say that the improved algorithms are easy and have fewer messages to achieve the synchronization and is energy efficient. More energy will be saved if the node count increases.

IV. PERFORMANCE APPRAISAL

The performance of the network may be appraised by the calculation of synchronization error and synchronization delay.

A. Delay in Synchronization

There is two important factors in Total synchronization delay. One is time of creating spanning tree i.e T_{tree} and other one is time of synchronization T_{sync}

$$\text{Delay} = T_{syn} + T_{tree} \qquad (5)$$

The Fig. 6 compare the synchronization delay in between the RBS and tree based scheme we find that delay in our scheme is reduce. And as the number of node will increase the delay time will decrease.

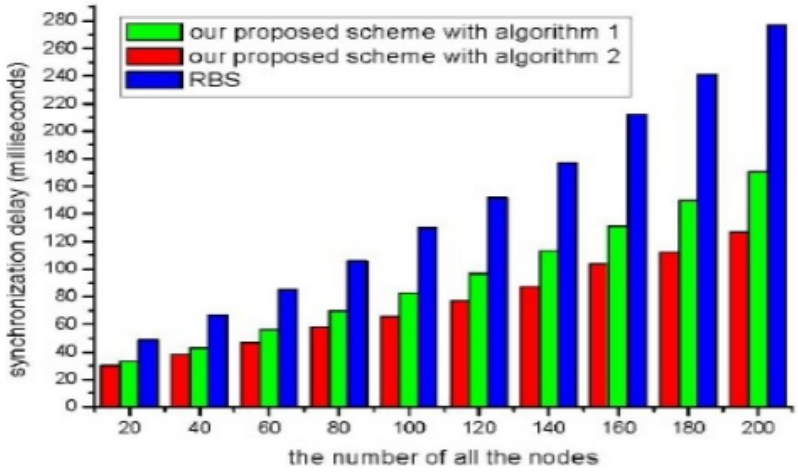

Figure 6. Synchronization delay v/s the number of all the nodes for our proposed scheme.

B. Error in Synchronization

Second phase is always accompanied by synchronization error. For different node, the synchronization error is different. So to calculate the synchronization error, individual error is considered for single node. Afterwards the whole problem is discussed for the entire network [6].

In entire network we will discuss the error as the average synchronization error and we see that the error in the proposed scheme is much lesser than that of RBS [8].

V. CONCLUSION

The proposed time synchronization scheme is very simple and easy to understand. By creating the spanning tree we divide the whole network in small sub tree and connect all the nodes to each other and

to synchronize the entire network we propose two algorithms. The performance of second algorithms is much better than that of first one. In case of both synchronization delay and synchronization error the performance of the proposed scheme is much better than reference broadcast synchronization.

REFERENCES

[1] Meng Zhou, and Jie Wu, "Cascading sensor network clock synchronization scheme," Member IEEE, Xuesong LIU 2011.

[2] Prakash Ranganathan, Kendall Nygard, "Time synchronization in wireless sensor network: a survey," International Journal of ubicomp, vol. 1, no. 2, April 2010.

[3] Sami M. Lasassmeh, and James M. Conrad "Time synchronization in wireless sensor network: a survey," IEEE 2010.

[4] Heng Wang, Lun Shao, Min Li, and Ping Wang, "Estimation of frequency offset for time synchronization With Immediate Clock Adjustment In Multi-Hope Wireless Sensor Network," IEEE Internet of things journal, vol. 4, no. 6, December 2017.

[5] Zhehan Ding, N. Yamauchi, "An Improvement of Energy Efficient multi-hop time synchronization algorithms in wireless sensor network," IEEE 2010.

[6] Liming He and Geng-Sheng (G.S.) Kuo "A novel time synchronization in wireless sensor network," IEEE 2006.

[7] Vehbi C. Gungor, Bin Lu, and Gerhard P. Hancke "opportunity and challenges of wireless sensor network in small grid" IEEE Transactions on Industrial Electronics, vol.57, no. 10, October 2010.

[8] Shushant Jain, and Yogesh Sharma "Optimal performance reference broadcast synchronization for time synchronization in wireless sensor network," International Conference on Computer, Communication and Electrical Technology – ICCCET 2011, 18th & 19th March, 2011.

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.

Address of the Editorial Office:

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

Note