Self Organizing Secure WSN for IOT Implementation

Surbhi Gehi[1], Roshan Jain[2]
[1]Student, M.tech (Digital Communication), Rajasthan College of Engineering for Women,
Jaipur, India
Surbhigehi011@gmail.com

[2]Assistamt Professor, Rajasthan College of Engineering for Women,
Jaipur, India
Roshan_vjain@rediffmail.com

Abstract: As wireless sensor networks are gaining widespread acceptance & popularity the need for making the secure & easily deployable is emerging as major challenge. This work is aimed at development of a self organizing wireless sensor network which employs tree hierarchy & provides high level of security using the most advanced cryptography & key sharing technique MATLAB is employed to demonstrate. Automatic node initialization tree based node organization employment of wireless node machine address in private key generation & use of natural randomizers to enhance security. Also communication between nodes that node to node or node to base /master over TCP/IP is demonstrated. A master node or base node which is the tree root handless all node initialization addition & deletion in conjunction with random key generation server. Also the base node facilitated generation of separate private keys for every node under it. Thus a highly secure hierarchical WSN is presented for IOT implementation.

Keywords: *Image Self organizing secure WSN, IOT Implementation, Self organizing WSN for IOT Implementation, Wireless Sensor Network.*

*****

I. Introduction

Today, the dream of smart grid, smart home, smart network and also smart city have come true with the implementation of the concept of Internet of Things (IOT). Internet of Things has the capability to couple the sensors and the entire infrastructure through the communications and information technology. In this regard, Wireless Sensor Networks have revolutionized the IOT industry by building a reliable and efficient communication system. Wireless Sensor Networks feature easy and flexible implementation of the devices. With the rapid growing technology of sensors, Wireless Sensor Networks play a key role for implementing Internet of Things.Today, our life is surrounded by a large number of sensors. One could not even imagine life without these sensors. Starting from smart phones, to automatic open gates then going underground of the soil, sensors are fitted everywhere for taking input data and processing the result accordingly. It has become the part and parcel of everyone's life. The internet of things (IOTs) is the massive deployment of trillions of low cost wireless internet protocol (IP)- based sensor nodes to identify and monitor every object, or things, around us. Also, because of its huge market, internet of things has been adopted by several governments all over the world, and this came to be known as the third wave of information technology after internet and mobile communication network. It is already seen that Internet of Things has made a firm grip in the field of security, intelligence, library so on. In the near future, a standard practical protocol stack of the giant network might be constructed which will include everything and have the capacity to change the world dramatically.

II. Literature review

In this paper, we propose an efficient self-organization protocol named ETSP for sensor networks of IOTs. ETSP saves more energy and has a longer network lifetime by constructing a tree-based network quickly. We use the weight of nodes, including residual energy, hop, number of child nodes and distance between the nodes, to determine whether the node can be a sink node. Thus the depth of tree is optimized by using ETSP. During the process of data transmission, the network topology changes dynamically. Each sink node will be dynamically reselected due to the energy consumption of sink nodes is faster than other nodes. The simulation results show that ETSP is able to build reliable tree-based networks, reduces the energy consumption and prolongs the lifetime of sensor networks. [1]

The Internet of Things (IOT) is revolutionizing and extending existing fundamental research areas into new dimensions by integrating the concept of intelligence or smartness. The new domains, including intelligent transportation systems, smart cities, smart homes, smart industries, autonomous vehicle, smart healthcare are but a few examples of this revolution. Some other prominent IOT application domains include automated security devices such as alarms and surveillance systems, automated grids used in industrial metering, vehicular telemetric as support for navigation and fleet management, remote maintenance as in vending machine control and industrial automation, and manufacturing control as in production chain monitoring. The integration of IOT in almost every aspect of human lives is due to the focus of inventions towards a greener and smarter world for sustainability reasons. [2]

The proposed system message authentication enhances security with light weight hash function at the receiver node; the default hash tree balances security and provides independent packet verification with 160bit signature and authenticates every packet by using 2AMD-160 algorithm. The proposed scheme ensures that markle tree is more efficient then chain based hash. The performance evaluation result shows that the proposed scheme is effective and scalable. [3]

The Internet of Things (IOT) is intended for ubiquitous connectivity among different entities or "things". While its purpose is to provide effective and efficient solutions, security of the devices and network is a challenging issue. The number of devices connected along with the ad-hoc nature of the system further exacerbates the situation. Therefore, security and privacy has emerged as a significant challenge for the IOT. In this paper, we aim to provide a thorough survey related to the privacy and security challenges of the IOT. This document addresses these challenges from the perspective of technologies and architecture used. This work focuses also in IOT intrinsic vulnerabilities as well as the security challenges of various layers based on the security principles of data confidentiality, integrity and availability. This survey analyzes articles published for the IOT at the time and relates it to the security conjuncture of the field and its projection to the future. [4]

IOT is an ideal emerging technology for the evolution of machine-to-machine communication. In this paper, various routing protocols such as Depth-First Forwarding (DFF), Multipath Loss and Low powered network Routing protocols (MRPL), Energy Efficient Probabilistic Routing Algorithm (EEPR), Congestion Avoidance Multipath Routing Protocol (CA-RPL), Movement-Aided Energy Balance (MAEB) and Least Path Interference Beaconing (LIBP) are been compared for the parameters average delivery ratio, average end-toend delay and energy consumption. We observed that Multipath RPL protocols (MRPL) produced better result than other routing protocols. [5]

GSTEB outperforms many protocols LEACH, PEGASIS, TREEPSI and TBC.Because GSTEB is a self-organized protocol which only consumes a small amount of energy in each round to change the topography for the purpose of balancing the energy consumption. Transmitting delay is short because all the leaf nodes can transmit data in the same timeslot. When the data collected by sensors cannot be fused, GSTEB does a tremendous job by introducing a simple approach to balancing the network load. Though it's difficult to balance the load on each node and even GSTEB needs BS to compute the topography which leads to an increase in energy wastage and longer delay are acceptable when it is compared with the energy consumption and the time delay for data transmitting. [6]

In this paper, we propose an efficient self organization pro-tool for sensor networks of IOTs. ETSP saves more energy and has a longer network lifetime by constructing a tree-based network fast. We use the weight of nodes and including residual energy, number of child nodes and distance between the nodes, to determine whether the node can be a sink node. Thus the depth of tree is optimized by using ETSP during the process of data transmission, the network topology changes. Each sink node will be dynamically reselected due to the energy consumption of sink nodes is faster than others. The simulation results show that ETSP is able to build reliable tree-based networks, reduces the energy consumption. [7]

The proposed system with network topology based on an efficient self-organization protocol. ETSP saves the energy and it has a longer lifetime of network by constructing a treebased network with short timing. By using the nodes weight, the residual energy of nodes, hop, number of child nodes and distance between the two nodes we determine the Best sink node. The network topology changes dynamically in the process of data transmission. Each sink node can dynamically reselected the nodes according to energy consumption of that node. In future we shows simulation results for ETSP which is build the reliable topology of tree-based networks which can reduces energy consumption and also Maximize the lifetime of Network. [8]

Routing in wireless sensor networks differs from conventional routing in fixed networks in various ways. There is no infrastructure and also routing protocols have to meet strict energy saving requirements. Researchers have used many techniques and devised many energy efficient routing protocols to address the energy constrained nature of nodes in WSN. One such energy efficient routing protocol devised for WSN is STEB (Self-organized Tree Based Energy Balance (STEB) Routing Protocol) protocol. In STEB, the main idea lies behind the construction of routing tree to transmit the data collected from sensor nodes to base station using a process where, for each round, BS assigns a root node and broadcasts this selection to all sensor nodes. Subsequently, each node selects its parent by considering only itself and its neighbors' information. Thus making STEB is considered to be a dynamic protocol but the problem with STEB is the energy consumption is more than required due to excessive broadcast of data. In future there is a possibility that the existing STEB protocol can be enhanced by incorporating the concept of clustering in it for longer lifetime and better performance of network. [9]

Bluetooth devices are becoming more popular as modern technology is transferring data onto wireless mediums for access flexibility and user mobility. Specifically, Bluetooth is one of the technologies that is capable enough to provide the last-meter connectivity. However, the inefficient inter-piconet communication in the scatter net topology has led to the overall inefficiency of the Bluetooth communications. This inefficiency is mainly contributed to the delay and control overhead in the inter-piconet scheduling policy. It is analyzed, that existing routing protocols construct a route that is based on a master and relay nodes that increases the number of hops. Furthermore, the existing protocols perform route optimization, but route optimization is based only on the RSP. Therefore, the existing protocols do not reduce an optimum number of hops motivates towards the development of a new routing protocol that would reduce the number of hops and repair weak link that ultimately improve the overall system performance. The proposed LMRO protocol finds the best shortest route between a source and a destination. Analytically, the LMRO has reduced the hop count and successfully repaired damaged link between a source and a destination. Empirically, through simulation, the performance of the proposed LMRO protocol is compared against the performance of the RRDR, LARP, and SFBN protocols based on several performance metrics. It was found that the LMRO protocol has outperformed all four protocols in terms of hop count, message overhead, delay, and throughput. Interestingly, the LMRO's throughput has improved in the range of 30% - 40%, and this was achieved by reducing hop count in the inter-piconet routing. [10]

The performance analysis (Residual energy, Dead Nodes) of Self-Organized Tree-Based Energy Balance Routing Protocol (STEB) for WSN is done by using MA TLAB. From the simulation results, it is observed that STEB outperforms LEACH in terms of rounds and remaining energy. This work can be further extended by incorporating security algorithm in STEB to prevent network attacks and also to enhance the performance of the network. [11]

III. METHODOLOGY

3.1 Random Key Generation Process

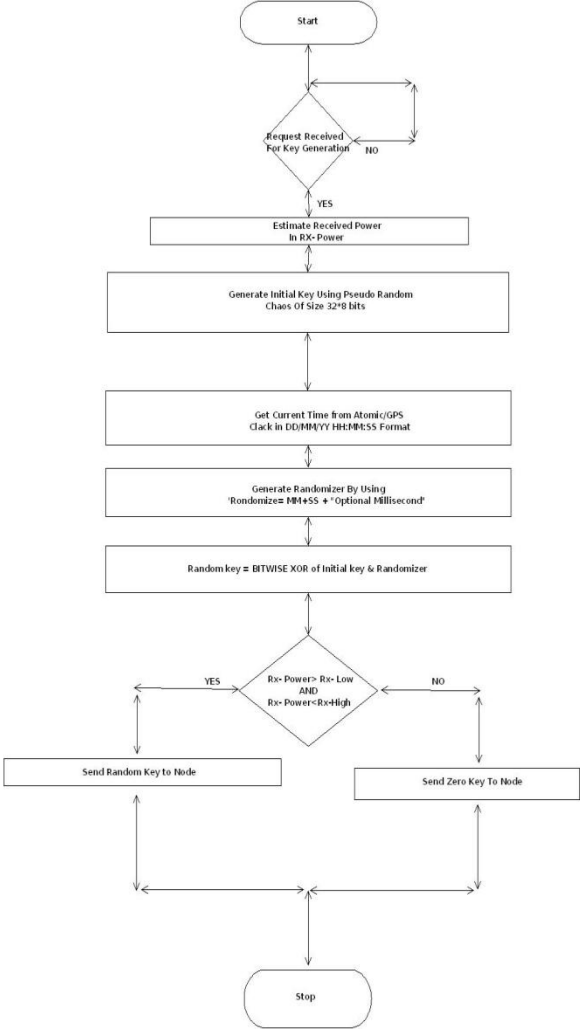

Start
Request Received For Key Generation
NO
YES
Estimate Received Power In RX- Power
Generate Initial Key Using Pseudo Random Chaos Of Size 32*8 bits
Get Current Time from Atomic/GPS Clack in DD/MM/YY HH:MM:SS Format
Generate Randomizer By Using 'Rondomize= MM+SS + *Optional Millisecond'
Random key = BITWISE XOR of Initial key & Randomizer
Rx- Power> Rx- Low AND Rx- Power<Rx-High
YES
NO
Send Random Key to Node
Send Zero Key To Node
Stop

Fig 3.1 Random Key Generation Process

Random key generator is grater key randomly in the fixed particular time period. If it receive request for random key generation then it generates random key. And if the receiver power is less or node is at large distance from the receiver then it generate random key.

3.2 VLMKG Encryption and Decryption

Mixed cipher alphabets differ from standard alphabets in that one or both sequences are mixed sequences. A mixed sequence is any sequence not in normal alphabetical order. The two main types of mixed sequences are systematically mixed and random mixed sequences. a. b. systematically mixed sequences are produced by an orderly process based on easily remembered keywords, phrases, or simple rules. There are a number of mixed sequence types, which will be explained in this section. Their advantage is that the keys can be easily memorized and reconstructed for use when needed. Their disadvantage is that the orderliness in construction can be used by the opposing cryptanalyst to aid in their recovery. Random mixed sequences are not based on any orderly generation process. They can be produced by various means ranging from pulling the 26 letters out of a hat to complex machine generation. Their advantage is that their structure offers no help to the opposing cryptanalyst. Their disadvantage is that the keys cannot be memorized easily or produced from simple directions as systematically mixed sequences can. They must be printed out in full and supplied to every user.

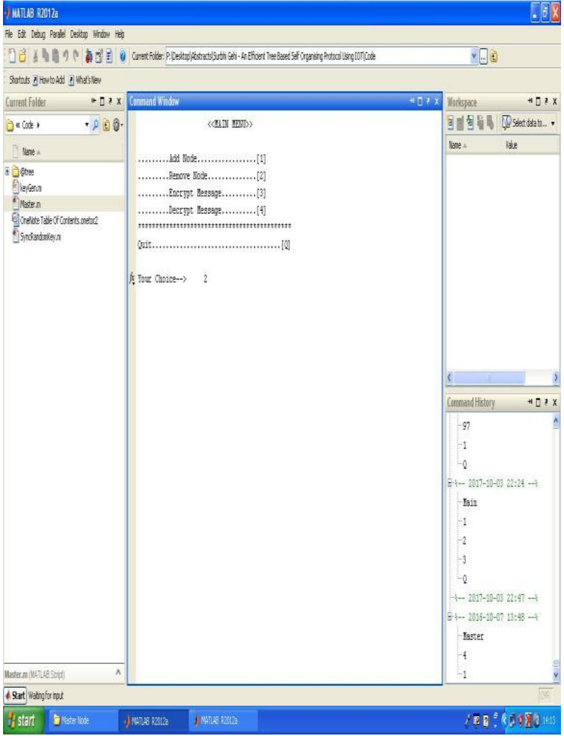
3.3 Process of Mixed Key Generation

In this process of mixed key generation 1st we generate n as input that is number of bytes. For convert it into byte we multiply it to 8. Then create zero multi of size nx1.There we initialize randomizer 3.9999998. Then we convert ind =2. Then we convert input into the binary. And we initialize input into the binary. And we initialize to 0, unsigned 8-bit integer. And initialize key to zero multi of size4 n/8X1. And we convert this data in to binary using key (ind1)=(ind1) + binary X(ind2- ind1)-2 power (ind2-1.)If equations value less than one then one then value is Return.

IV. RESULT

5.1 Master Node Results:

In this process 1st we run the main code and a loading window will be shown. After the loading process a main menu bar will be open in this menu window some options are available for choosing the user here user choose option for add node, Remove node, encrypt and decrypt message. At the 1st time we select maximum 4 nodes. After selecting node the master node is connected to the key server then the key server generate a random key this random key generate by the key server For each selected node. and by using this key we are encrypt message and decrypt message. After a particular pre set time the new key is generated automatically.



```
                <<MAIN MENU>>

.........Add Node................[1]
.........Remove Node.............[2]
.........Encrypt Message.........[3]
.........Decrypt Message.........[4]
********************************************
Quit.................................[Q]

Your Choice-->    2
```

```
97
1
Q
%-- 2017-10-03 22:24 --%
Main
1
2
3
Q
%-- 2017-10-03 22:47 --%
%-- 2016-10-07 13:48 --%
Master
4
1
```

Fig 5.1

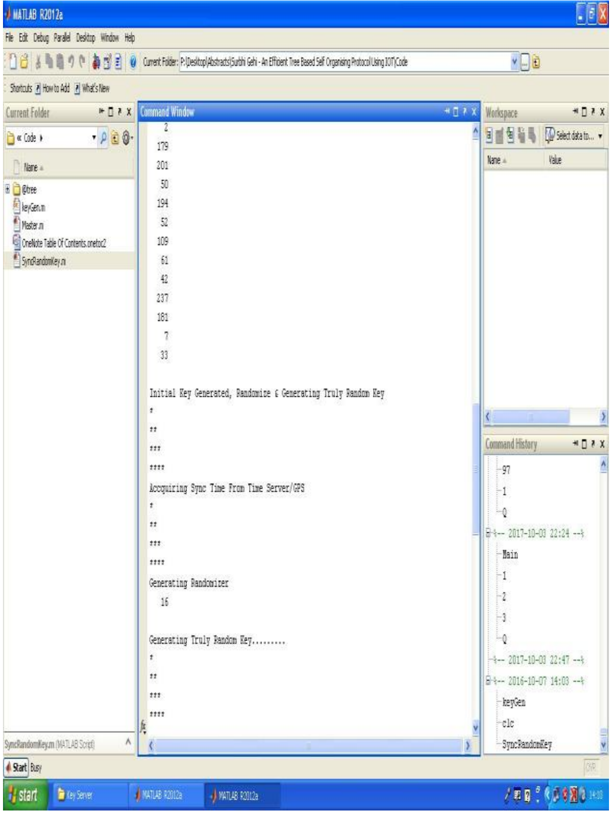
In this window we can see there is menu options that are choosen by the user.these four options are given below.

1. Add Node
2. Remove Node.
3. Encrypt Message.
4. Decrypt Message.
5. **2 Key Server Results:**

The key server is work when we select the number of node then the master node is connecting to the key server then the key server is generates the random key for each selected nodes here 8 node is available for selection and at 1st we select only 4 node maximum. And after a particular pre set time the key server is again generate a new random key for the each selected nodes automatically.

The window which is shown in figure 5.2 show that the random key is generated and the time is taken by GPS. After a particular time period this true random key is rejected automatically.

And after the process of random key generation this random key is send to the master node automatically.



```
     2
   179
   201
    50
   194
    52
   109
    61
    42
   237
   181
     7
    33


Initial Key Generated, Randomize & Generating Truly Random Key
#
##
###
####
Acquiring Sync Time From Time Server/GPS
#
##
###
####
Generating Randomizer
    16


Generating Truly Random Key.........
#
##
###
####
```

Fig 5.2

V. CONCLUSION AND FUTURE SCOPE

Conclusion

A highly secure structured & hierarchical self organizing wireless sensor network is demonstrated in this proposed work. As the demand for IOT devices is increasing manifolds large scale WSN deployment is anticipated also for the coming challenges are security concerns of environmental/user data over wireless medium & reduction of human effort in deployments & maintenance of large scale wireless sensor networks. Thus work demonstrated development of a master node/base node or controller node which acts as the root of the tee hierarchy allow for initialization addition & deletion of other wireless nodes beneath it.Also the master node facilities generation of truly random key using separate key generation server. MATLAB is used to depict & demonstrate the proposed WSN architecture network tree hierarchy is achieved by the use of tree toolbox & TCP/IP communication between nodes. Master controller & random key generation is also demonstrated using the TCP/IP socket functionality. As shown by the results above the proposed WSN exhibits tree topology central handling of node initialization addition/ deletion & provide high level security by using truly random keys based on natural event/ phenomena & usage of machine address of wireless nodes to customize private key for individual nodes providing tightly governed communication environment along with hierarchical setup.

Future Scope

As demonstrated above a highly secure self organizing wireless sensor network with stringent security measure have been developed & simulate but as widespread dominance of WSN‘s future IOT deployment is inevitable in WSN A IOT domain is underway the proposed technique should also improve with emerging technological trends. The most sought of improvements in this context is introduction of self healing techniques, failure prediction health monitoring of WSN’s. also there is emerging requirement of self aware WSN’s which are aware of connectivity option & provide foil safe redundancy in communication of important/urgent events via multitude of connectivity options available.

References

[1.] Xize Liu, Lin Feng∗, Yu Zhou, Kaiyu Zheng “An Efficient Tree-based Self-Organizing Protocol for Internet of Things” IEEE 2016.

[2.] Kirshna Kumar , Sushil Kumar , Omprakash Kaiwartya , Yue Cao , ID , Jaime Lloret ID and Nauman Aslam “Cross-Layer Energy Optimization for IoT Environments: Technical Advances and Opportunitie” MDPI 2017

[3.] Mallikarjunaswamy, Latha Yadav, Dr. Keshava Prasanna “Markle Tree Based Authentication Protocol for Lifetime Enhancement in Wireless Sensor” Int. J. Advanced Networking and Applications 2017.

[4.] Diego Mendez , Ioannis Papapanagiotou , Baijian Yang “Internet of Things: Survey on Security and Privacy” IJETT 2017.

[5.] Vidya Rao , Vallabh Mahale , G G Sivasankari , Venugopal “Wireless Routing Protocols for Internet-of-Things (IoT)-A Survey” IJLEMR 2017.

[6.] Devarshi Dang, Gagan Dhawan “Survey on Tree Based Energy Balanced Routing Protocols in WSNs” International Journal of Recent Research Aspects 2017.

[7.] Miss. Rohini Korulkar & Prof. Dr. Sonkamble Sulochana “An Efficient Tree-based Self-Organizing Protocol for Internet of Things” IJIR 2017.

[8.] Arti Mandlik,Ms. Bharti Patil “AN EFFICIENT DATA TRANSMISSION USING TREE-BASED SELF-ORGANIZING PROTOCOL” IJAREM 2017.

[9.] Er. Zahid Farooq , Nidhi Sharma “A Review of Energy Efficient Routing Protocols in WSN” IJESC 2016.

[10.] Sheikh Tahir Bakhsh “A Self-organizing Location and Mobility- Aware Route Optimization Protocol for Bluetooth Wireless” IJACSA 2016.

[11.] Dasari Raja, P.Samundiswary “Performance Analysis of Self-organized Tree Based Energy Balance (STEB) Routing Protocol for WSN” IEEE 2015.