ISSN 2277-3061
Volume 16 Number 4
International Journal of Computers & Technology

ZONE BASED SECURED ENERGY EFFICIENT MECHANISM IN WIRELESS SENSOR NETWORKS FOR EFFICIENT COMMUNICATION

Pankaj Kumar [1], Ramanjeet Singh [2]
[1] Research Scholar, Department of Electronics Communication & Engineering, LCET, Katani Kalan
pankaj.1123@gmail.com
[2] Assistant Professor, Department of Electronics Communication & Engineering, LCET, Katani Kalan
raman.lcet@gmail.com

ABSTRACT

Wireless sensor network has revolutionized the way computing and software services are delivered to the clients on demand. Wireless sensor network is very important to the mankind. It consist of number of sensor called nodes and a base station. Nodes collect data and send to the base station. There are number of nodes which send data at a time. So, number of problems are occurred. Usually the WSNs are automated, that is they work without the human intervention. In such cases it becomes very crucial that the network must have the capability of self-healing security mechanism to handle with all the types of attacks. Without the use of security mechanism, the data can be altered or hacked by some intruder in the network. The nodes are connected with each other without a wired connection through the base stations, they are highly prone to the hacking attacks. WSNs are used to sense various environmental or other parameters which can be used to predict natural hazards, climatic changes or other types of data analysis. During the periods when the WSN nodes are in working condition, they need secure cryptographic keys for secure propagation of the sensitive information. The present research is focused on the design of energy efficient security mechanism for improved reliability in sensor based environment. The RSA encryption algorithm has used for encryption purposes.

Keywords

WSN, Security, RSA, Cluster

INTRODUCTION

A Wireless Sensor Network or WSN is supposed to be made up of a large number of sensors and at least one base station. The sensors are autonomous small devices with several constraints like the battery power, computation capacity, communication range and memory [1]. They also are supplied with transceivers to gather information from its environment and pass it on up to a certain base station, where the measured parameters can be stored and available for the end user. In most cases, the sensors forming these networks are deployed randomly and left unattended to and are expected to perform their mission properly and efficiently. As a result of this random deployment, the WSN has usually varying degrees of node density along its area. Sensor networks are also energy constrained since the individual sensors, which the network is formed with, are extremely energy-constrained as well. The communication devices on these sensors are small and have limited power and range. Both the probably difference of node density among some regions of the network and the energy constraint of the sensor nodes cause nodes slowly die making the network less dense [2]. A real and appropriate solution for this problem is to implement routing protocols that perform efficiently and utilizing the less amount of energy as possible for the communication among nodes.

A wireless sensor network is a technology that emerges as a consequence of the evolution of network technology along with microelectronics and micromechanical devices. It is a new concept, a view towards the future, a clear consequence of the new steps forward in the communications field [3]. In few words a wireless sensor network, is a network that could contain from a couple to many small nodes with sensors attached and communications capabilities to transmit and receive information.

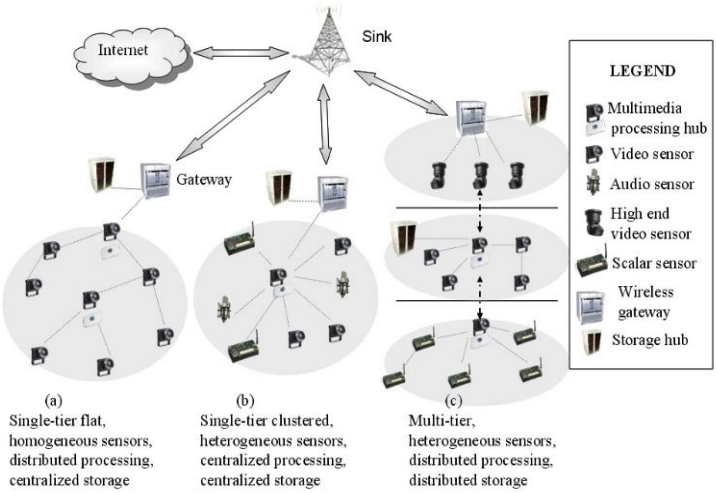

Figure 1. Wireless Sensor Network

In order to counter the threats stemming from these vulnerabilities, well- known mechanisms can be employed, including code authentication, message encryption and authentication, and tamper proofing [4]. However, the specific constraints of sensor networks may be prohibitive to lifting them to a security level as high as traditional computer systems [5][6]. Instead, we must explore solutions that exploit inherent characteristics of sensor networks, such as the large number of nodes, redundant deployment, and sensory input, to provide adequate security guarantees. We concentrate on a type of attack on wireless sensor networks, which is both specific to and relevant in this domain.

Djamila Bendouda et al. (2015) proposed an effective new method for Fault Management with RPL protocol (MFM-RPL) in WSN. Their work is the first effort for fault and failure management using the RPL protocol with mobile nodes. They used the Contiki operating system and COOJA simulator. The performance of MFM-RPL algorithm is evaluated for different network settings, in terms of, the control traffic, latency, energy consumption and PDR (%).

Dahane Amine et al. (2015) states that the main concern of clustering approaches for mobile Wireless Sensor Networks (WSNs) is to prolong the battery life of the individual sensors and the network lifetime. The goals of the proposed algorithm are: detecting common routing problems and attacks in clustered WSNs, based on behavior level.

Nonhlanhla Ntuli et al. (2016) proposed security architecture for smart water management systems, the architecture leverages existing security solutions and design patterns. Water scarcity and water stress issues have become clear threat to the global population. This makes water management a critical aspect to ensure sustainable water.

Rashmi Mahidhar et al. (2016) proposed Dynamic Multilevel Priority (DMP) Packet Scheduling Scheme with the Bit Rate classification. The threshold value check mechanism is also proposed to prevent the deadlock situation. To provide security they have implemented the RC6 security algorithm.

Pooja Nandu et al. (2015) states that the wireless reprogramming in (WSN) is the process of inseminating new code or correlated commands to sensor nodes. It enables sensor nodes to self-reprogram so adapting them to unravelling milieu's Applications include geophysical/habitat monitoring, controlling disaster, battlefield information, collection and monitoring, security surveillance and home entry systems.

Swapna Naik et al. (2015) discusses that the wireless Sensor Networks (WSNs) can be used to monitor environments, and therefore have broad range of interesting applications. The applications which may use WSN can be of sensitive nature and therefore might require enhanced secured environment. As sensors are used to monitor sensitive areas therefore Security and energy efficiency is essential consideration when designing wireless sensor networks (WSNs). The Sensor nodes get their power from batteries. Since the sensor nodes are deployed in harsh environment they cannot be recharged.

Parmar Amish et al. (2016) has surveyed unique characteristics like limited bandwidth, limited battery power and dynamic topology makes Wireless sensor network (WSN) vulnerable to many kinds of attacks. Therefore, interest in research of security in WSN has been increasing since last several years. Infrastructure less and self-governing nature of WSN is challenging issue in terms of security.

Shital Patil et al. (2016) finds that wireless Sensor Networks (WSN) has wide applications in data gathering and data transmission via wireless networks. Due to the weaknesses in the WSN, the sensor nodes are vulnerable to most of the security threats. Denial-of-Service (DoS) attack is most popular attack on these sensor nodes. Some attack prevention techniques must be used against DoS attacks. There are different techniques to prevent DoS attack in wireless sensor network.

S.Sangeetha Mariammal et al. (2015) researches that the wireless Sensor Networks (WSNs) is spatially distributed in sensor nodes without relay. A Mobile Data Investor, M-Investor is used to gather the data from sensor node and upload the data into data sink. When one M-Investor is moving, gathers the data from each and every node of entire network and upload the data into data sink. Also, it raises distance/time constraints. The proposed system uses multiple M-Investors that are formed by portioning a network into a number of small sub networks.

RESEARCH METHODOLOGY

• All the nodes in the WSN network are homogeneous and base station is located outside the network area.

• The clusters in the network are created with the help of centralized approach.

• Base station will send its location to all the sensor nodes by advertising the "HELLO" message

• The sensor nodes will receive the message from the base station and will send the acknowledgement with their location coordinates, remaining energy and number of neighbors to the base station.

• On receiving the messages, the base station will form the clusters and will advertise the Cluster Head and Member nodes of that cluster to all the nodes.

• The Base Station will calculate the threshold (mean) distance of all the nodes and will divide them into 2 zones: far zone and near zone.

• The cluster head in the far zone will chose the cluster head in the near zone (next relay node) according to the minimum distance from its current location.

• Key Generation table is used to store the keys generated by each of the nodes. The nodes which are dead or they are found to be malicious or intruders are not allowed to store their keys in the table.

• The trust identification is established by scanning the behavior of each of the node. If the node keeps on changing its key again and again, it is found to be intruder or has been hacked by someone else.

• Node 1 will send its request to the node 2 for data transmission.

• Node2 will send the acknowledgement on receiving the request.

• On receiving the acknowledgement, Node 1 will generate its key and will encrypt the key using RSA algorithm before sending it to the node 2.

• The node 2 will decrypt the received key using blowfish from node 1 and will verify the key from the key generation table.

• If the values are matched, then data transmission will take place, else the node is marked as malicious and is not allowed to transmit any type of data in the network.

RSA ALGORITHM

RSA algorithm is designed by Ron Rivest, Adi Shamir, and Leonard Adleman at MIT in1978. It can be broadly classified into three steps; a) key generation, b) encryption, and c) decryption. RSA has two keys; public key and private key. Both keys are used for encryption and decryption purpose. Sender encrypts the message using receiver's public key and when the message gets transmit to receiver, then receiver can decrypt it using his own private key. It uses two prime numbers and to generate private key and public key. For small values of the designing of key in the encryption process becomes too weak and one could be able to decrypt the data using random probability theory. On the other hand, if large value of and are selected, it consumes more time and its performance degrades. Hence, RSA is slower than other symmetric algorithms.

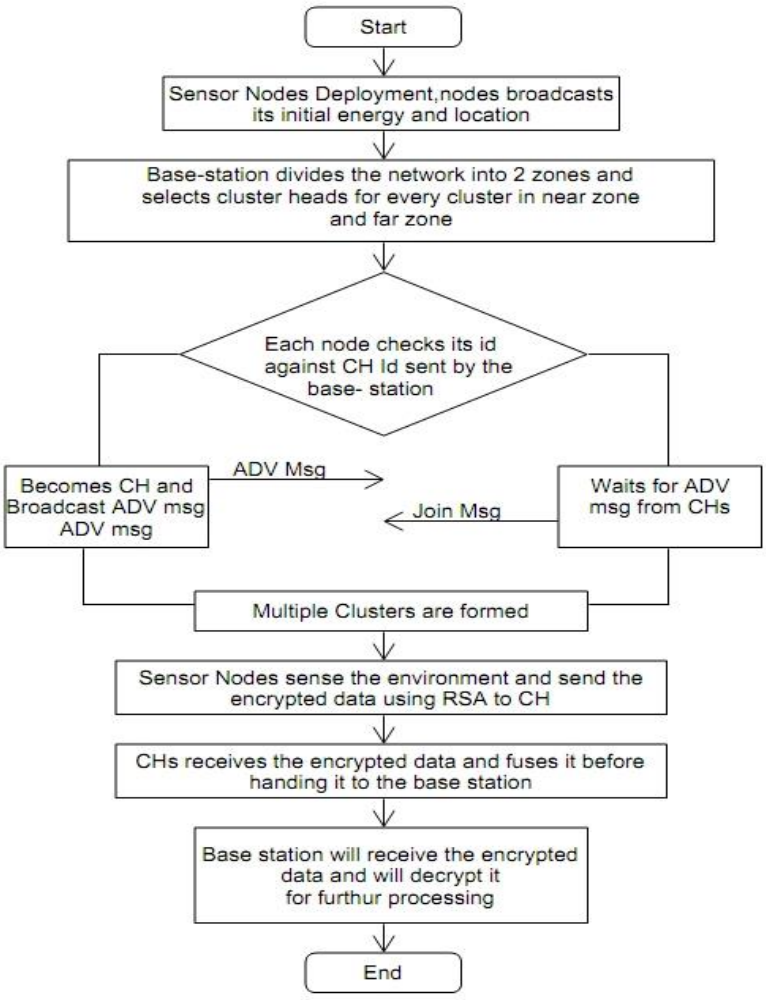

Figure 2. Flow Chart of Proposed Work

RESULTS AND DISCUSSIONS

As already discussed, security based energy efficient WSN deployment is not an easy task due to large number of parameters, i.e., energy parameters and cluster head selection then their data transmission procedure. This section presents the simulation results of the work done and the proposed approach. The proposed approach has been implemented in MATLAB.

Table 1. Network Parameters

PARAMETER	VALUE
SIMULATION TIME	5000 rounds
Number of Nodes	50
Network Grid	150m * 150m
Initial Energy	.5 Joules
Packet Size	4000 bits
$E_{electrical}$	50 nJ/bits
E_{amp}	.0013 pJ/bit/m^4
E_{fs}	10 pJ/bit/m^2

Table 1 shows the network parameters that are used for evaluating the results. The parameters considered during simulation have their own significance for the better performance of the network.

Table 2. Network Lifetime

Initial Energy	FND	MND	LND
.5	2470	2508	2632
.25	1239	1253	1316
.1	497	505	527

Table 2 shows that the network lifetime for the different levels of energy for multiple experiments. The first node dead, middle node dead and last node dead are evaluated in the Matlab envrionment. The first node Dead is different in the both cases. The above mentioned table is created using the different energy parameters and it gives the different values of dead nodes.

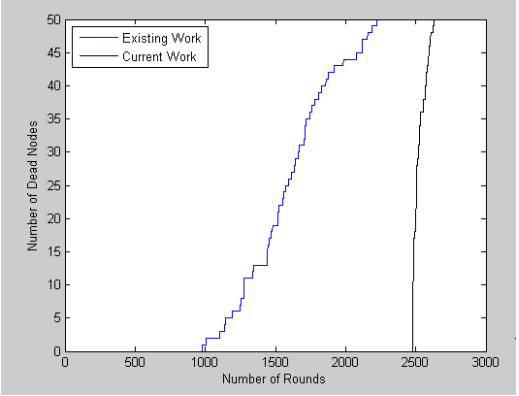

Figure 3. Comparison b/w Dead Nodes of Current Work and Existing Work

Fig 3 shows the dead node comparison between the existing work and current work. It shows the dead nodes of the network i.e. when whole network is dead. It shows the network lifetime has been increased. The network lifetime of current work is better than the existing work. The current work has extended the lifetime up to 2632 rounds as it is clear from the graph. Fig 4 represents the graph between the alive nodes and number of rounds. Alive nodes means number of nodes participating in the network. In the above fig number of nodes of proposed work are alive for the more number of rounds than the existing work.

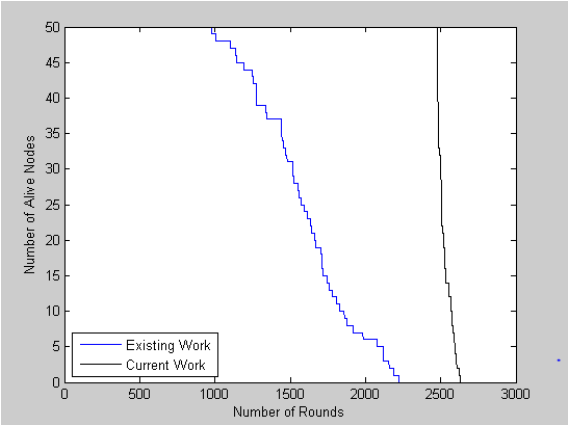

Figure 4. Comparison b/w Alive Nodes of Current Work and Existing Work

The figure 5 explains the average remaining energy of the entire network for 100 nodes. The average remaining energy starts at .5 Joules for all the nodes and it keeps on decreasing as the number of rounds are increasing and it becomes zero at approximately 2600 rounds.

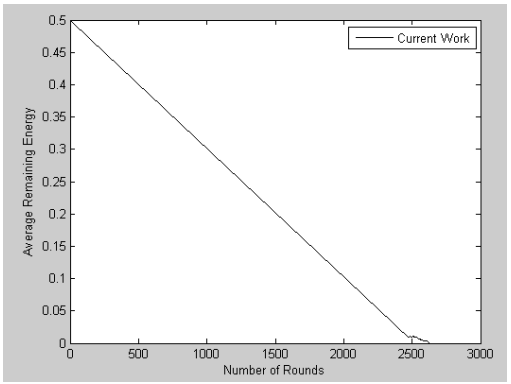

Figure 5. Average Remaining Energy of current Work

CONCLUSION

The lower cost and easier installation of the WSNs than the wired counterpart pushes industry and academia to pay more attention to this promising technology. The security of WSNs is one of the key issues of smart cities. Applications of WSNs include maintaining environmental homeostasis, controlling industrial processes, monitoring health conditions, and detecting abnormalities in the region of interest. Rigid relationship based key algorithm has been used as a reference to compare the performance of each of the clustering methods. It was found that the proposed algorithm gives a much-improved network lifetime as compared to existing work. In this research work, a new encrypted mechanism of communication using RSA has been presented. By analyzing the results and graph, it is clear that the overall lifetime of the complete network has been improved. Due to the potential deployment in uncontrolled and harsh environments and due to the complex architecture, wireless sensor networks are and will be prone to a variety of malfunctioning. In future work, there is a need to calculate the detection accuracy for the nodes in the Wireless Sensor Network where detection accuracy depicts the ratio of the number of faulty sensors detected to the total number of faulty sensors in the network.

REFERENCES

[1] D. Bendouda, L. Mokdad and H. Haffaf, "Method For Fault Management With RPL Protocol In WSNs," *ELSEVIER,* p. 395 – 402 , 2015.

[2] A. Dahane , Berrached Nasr Eddine and L. Abdelhamid, "A Distributed and Safe Weighted Clustering Algorithm for Mobile Wireless Sensor Networks," *ELSEVIER,* pp. 641-646, 2015.

[3] N. Ntuli and Adnan Abu-Mahfouz, "A Simple Security Architecture for Smart Water Management System," *ELSEVIER,* p. 1164 – 1169, 2016.

[4] R. Mahidhar and A. Raut, "A Survey On Scheduling Schemes With Security In Wireless Sensor Networks," *ELSEVIER,* p. 756 – 762, 2016.

[5] N. Shekokar and P. Nandu, "An Enhanced Authentication Mechanism to Secure Re- Programming in WSN," *ELSEVIER,* pp. 397-406, 2015.

[6] S. Naik and N. Shekokar, "Conservation of energy in wireless sensor network by preventing denial of sleep attack," *ELSEVIER,* p. 370 – 379, 2015.

[7] P. Amish and V. Vaghela, "Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV protocol," *ELSEVIER,* p. 700 – 707, 2016.

[8] S. Patil and S. Chaudhari, "DoS attack prevention technique in Wireless Sensor Networks," *ELSEVIER,* p. 715 – 721, 2016.

[9] S. Mariammal and J.Gayathri, "Ensuring higher security for gathering and economically distributing the data in social wireless sensor," *ELSEVIER,* p. 408 – 416, 2015 .

[10] C. Baskar, Balasubramaniyan C and Manivannan D, "Establishment of Light Weight Cryptography for Resource Constraint Environment using FPGA," *ELSEVIER,* p. 165 – 171, 2016.

[11] S. M. Sajjad, S. H. Bouk and M. Yousaf, "Neighbor Node Trust Based Intrusion Detection System for WSN," *ELSEVIER,* p. 183 – 188, 2015.

[12] S. K. Shankar, A. S. Tomar and G. K. Tak, "Secure Medical Data Transmission by using ECC with Mutual Authentication in WSNs," *ELSEVIER,* p. 455 – 461, 2015.

[13] S. Uke and R. Thool, "UML Based Modeling for Data Aggregation in Secured Wireless Sensor Network," *ELSEVIER,* p. 706 – 713, 2016.

[14] J. Wu, K. Ota, . M. Dong and C. Li , "A Hierarchical Security Framework for Defending against Sophisticated Attacks on Wireless Sensor Networks in Smart Cities," *IEEE,* pp. 1-9, 2015.

[15] T. Park and H. Shi, "Extending the Lifetime of Barrier Coverage by Adding Sensors to a Bottleneck Region," *IEEE,* pp. 537-342, 2015.

[16] A. Faquih, . P. Kadam and Zia Saquib, "Cryptographic Techniques for Wireless Sensor Networks: A Survey," *IEEE,* 2015.

[17] Anita Daniel. D and Emalda Roslin. S , "A Review on Existing Security Frameworks with Efficient Energy Preservation Techniques in Wireless Sensor Networks," *IEEE,* pp. 658-662, 2015.

[18] H. Zhao, . C. Hu, R. Zheng and B. Lv, "Study on the Coverage of Adaptive Wireless Sensor," *IEEE,* pp. 1312-1317, 2015.