International Journal of Pure and Applied Mathematics
Volume 117 No. 21 2017, 21-28
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

DETECTION OF NODE REPLICATION ATTACKS IN WIRELESS SENSOR NETWORKS

Miss. M. Sri Sakthi Nishalya[1] , Miss. Madhumitha R[2], Mrs.L.Sujihelen[3]

1. UG Scholar, Department of Computer Science and Engineering, Sathyabama University.

2. UG Scholar, Department of Computer Science and Engineering, Sathyabama University.

3. Assistant Professor, Department of Computer science and Engineering, Sathyabama University.

ABSTRACT

Wireless sensor networks (WSN) are made out of various minimal efforts, low-control sensor hubs. It is used for communication at short separation through remote connections. These sensors are profoundly conveyed to gather and transmit information of the physical world to one or two couples of goals called sinks. Due to this type of open spending in wide condition, makes the networks vulnerable to a variety of physical attacks. The wireless communication technology also acquires various types of security threats. With little exertion, the attacker may catch investigations hubs and repeat them. These copies at various areas in the system may corrupt the network data or disconnect significant parts of the network. Once the hub is caught and gathers keys, etc. The assaults can reinvent it, and duplicate the hub, keeping in mind the end goal is to eavesdrop the transmitted messages. The proposed system is used to detect the replicated node in distributed sensor networks.

KEYWORDS: Wireless Sensor Networks, Key Pre- distribution schemes, Random graphs,

1.INTRODUCTION

Sensor nodes are nodes which perform operations like processing, gathering information, and communicating with other connected node. Fig.1 represents the block diagram of a sensor node. The principle segments of sensor hubs are miniaturized scaled controller, handset, outer memory and more than one sensor. A controller performs tasks and controls the functionality of other components. Mostly microcontrollers are used in embedded system. Transceiver makes use of radio band frequencies and consumes power. External memory is used for storage feature and suitable for chips. Sensor nodes collect data from the environment in which they are deployed, the analog signal is continuously digitized with the help of analog to digital converter.

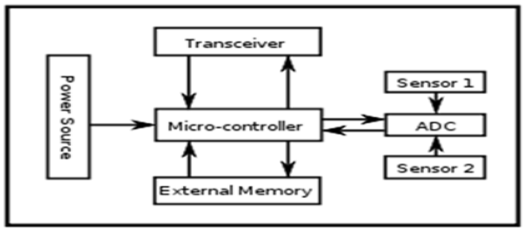

Fig. 1 Overview of WSN

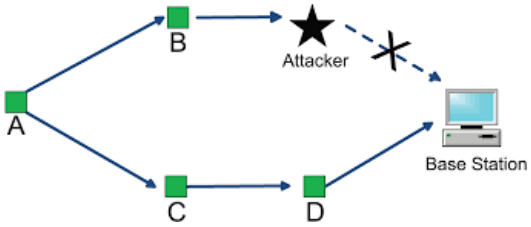

Fig. 2 Sensor Nodes with Attacker

Fig. 2 explains how the attacker destroys the communication between a sensor node and the base station. The cryptographic secrets of nodes and deploys itself in the network and produces duplicate nodes, which in turn is distributed all over the network. These duplicated nodes will bring down the performance of the network or the

whole network may crash. This is called as Node Replication Attack, which is very harmful attack and also injurious to functions like resource allocation, etc.

2.RELATED WORKS

L. Sujihelen [1] has given the detailed study about wireless sensor networks. The two types 1. Static WSN 2.Mobile WSN are explained and different types of schemes Centralized and Distributed, with all with each unique factor like communication overhead and storage overhead. J. Anthoniraj [2] has grouped various protocols into two main types of approach –Centralized and Distributed approach and types of protocols e.g. Set protocol, LM protocol, RM protocol, etc. This proposed work has a disadvantage that it mainly concentrates on stationary wireless sensor networks, and also only for detection of clone attack.

G. Raja [3] has proposed the features about detecting node replication attacks only using the single hop methods and a selection algorithm to detect replica nodes. This protocol is only used for portable sensor systems. Two primary calculations XED and EDD were proposed and it consists of four major processes. Node deployment, execute offline step, find next hop and candidate hop, localized detection. M.H. Ansari [4] has explained all the procedures for the detection of replica nodes. The protocols like UTLSC, MTLSD and SPRT have a higher recognition rate and low false caution rate. The paper gives us a detailed advantages and disadvantages of methods like UTLSC, MTLSD and SPRT. It only gives the best methods of protocol.

Haafizah Rameeza Shaukat [5] has proposed the technique single hop detection. This protocol uses location claim as a parameter to detect duplicate nodes. Since it is a mobile sensor network each node updates with a various location claim and node ID for the base station, which in turn consumes more time to check all the information provided by the base stations. L.S. Sindhuja [6] has proposed technique used is a single hop detection along with the clonal selection algorithm in order to select the base station according to the location claim to detect replica. The paper deals with clonal algorithm in order to detect replica which takes more time and uses more parameters to select the base station

Miss. Raisa M. Mulla [7] has proposed techniques for detecting clone assaults in both versatile and stationary remote sensor systems. It only gives the classification of different attacks and based on the report of the experimental analysis, the protocol to be used is found. Neenu George [8] and T.K. Parani Detection of Node Clones in Wireless Sensor utilizing Detection Protocols in 2014. Two novel hub clone discovery conventions were proposed 1. Distributed Hash table (DHT), completely decentralized key based reserving and checking framework. 2.Randomly Directed Exploration (RDE). When compared DHT, RDE has higher detection probability less memory storage consumption and low communication cost. Mainly concentrates on mobile sensor networks and only two techniques will give maximum and efficient result.

Avnet Kaur [9] Detection of Clone Attacks in Wireless Sensor Networks: A Survey in 2014. It is a survey of clone attacks and various forms of security attacks like HELLO FLOOD, Sink hole, Worm hole, Sybil attack etc. Only clone attacks are detected using protocols. Other security attacks are only defined.Mindaugas Blonzelis [10] Both the active and passive intersection of graphs are discussed, the Lemma theorem is also proved This technique mainly concentrates on the clustering activity, only in the case of clustering co-efficient this technique can be used.

G. Keerthana [11] in 2016 Sinkhole attacks uses swarm intelligence techniques, among those techniques Ant colonization algorithm was used, and then they proposed Particle swarm technique in Wireless Sensor Network using Enhanced Particle Swarm Optimization Technique This protocol mainly covers the detection of sink hole attacks. It consumes more time to detect the node.

3. PROPOSED System

In order to overcome the disadvantages of the existing system, we have enhanced the scheme Eschaneur-Gligor along scheme with additional features called q-composite key pre-distribution. This algorithm comprises of 3 major steps:

1. q-Composite key pre-distribution
2. Clonal Selection Algorithm.
3. Eschenaur-Gligor scheme

3.1 Q-COMPOSITE KEY PRE-DISTRIBUTION

In our scheme, key pre-distribution consists of three phases, namely key pre-distribution, shared-key discovery, and path- key establishment. This scheme consists of five steps: 1.Genration of pool key from the range of (e.g., 2^{17}-2^{20} keys) to form a ring like structure in order to arrange. 2. The key pre-distribution phase ensures that only small number of keys must be shared every hub has a set of two keys which are used in communication process, only when the pair-wise keys are matched communication between any two nodes or any network takes place. The keys are:

- Private key
- Public key

In every hub, the public keys are same and only the private key makes the hub unique. The pair-wise match is made by the communication of both public key and private key as follows

$$P\ (K_1,K_2)$$

Where

K_1 - public key.

K_2 - private key.

P- Pool or the pair of both public and private keys.

The keys are used for matching purpose,so that only two pre-registered nodes could communicate. These keys are already pre-designed and ordered so that communication happens fluently without any physical barriers or disturbance in the system.

3.2 CLONE SELECTION ALGORITHM

The Clone Algorithm can be listed as follows:

Step 1: Generate a set of antibodies (generally created in a random manner) which are the current candidate solutions of a problem.

Step 2: Calculate the affinity values of each candidate solutions.

Step 3: Sort the antibodies starting from the lowest affinity. Lowest affinity means that a better matching between antibody and antigen.

Step 4: Clone the better matching antibodies more with some predefined ratio.

Step 5: Mutate the antibodies with some predefined ratio. This ratio is obtained in a way that better matching clones mutated less and weakly matching clones mutated much more in order to reach the optimal solution.

Step 6: Calculate the new affinity values of each antibody.

Step 7: Repeat Steps 3 through 6 while the minimum error criterion is not met.

This Clone Selection Algorithm is used to select the witness node or Base Station more efficiently not only depending by the location but also according to the energy-level of each node

3.3 ESCHANAEUR-GLIGOR SCHEME

Eschanaeur – Gligor key pre conveyance plot under the state of halfway perceivability with i.i.d, on-off connections between the sets of hubs. This circumstance was displayed as the crossing point of two arbitrary charts, in particular an irregular key diagram and ER Diagram. With n hubs in the system, the Eschanaeur - Gligor plot with key rings of size K drawn from the pool P particular keys (K<P) offers ascend to the irregular key chart K(n, θ) where θ=(K,P) . Let qs(θ) signify the likelihood that a connection does not exist between two hubs K(n, θ). The correspondence between two hubs relates to ER Diagram chart G with connection likelihood

4. SIMULATION RESULTS

Grouping of nodes takes place according to their key value, grouping is the first step in any detection protocol. Grouping restricts the number of nodes that could actually take part in communication with high and consistent energy-level for the transfer of messages. The blue concentric circles in fig.3 indicates grouping of nodes. The blue small circles are the sink nodes selected by applying Clone Selection Algorithm.

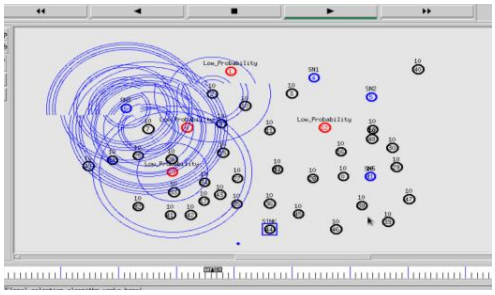

Fig.3 Grouping of nodes with sink nodes

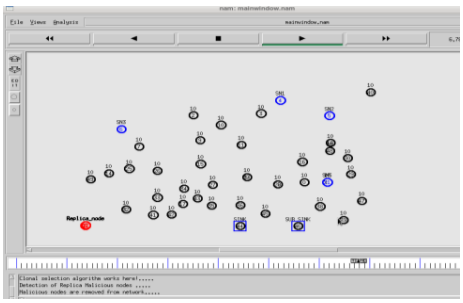

Fig.4 Sink nodes have detected the replica nodes

In fig 4, by the use of Eschenauer-Gligor scheme, and Q- composite key pre-distribution scheme, the sink nodes have detected the replica nodes and the duplicate nodes are highlighted red in colour.

4.1 DETECTION RATIO

Thus using the scheme proposed, the disadvantages of the existing system are overcome, and the result is shown as a comparative graph between the existing and proposed system. This graph(fig.5) shows that we have achieved our objective i.e., to detect the replica nodes within lesser span of time. The speed of this scheme is mainly attained by the Eschenauer- Gligor scheme.

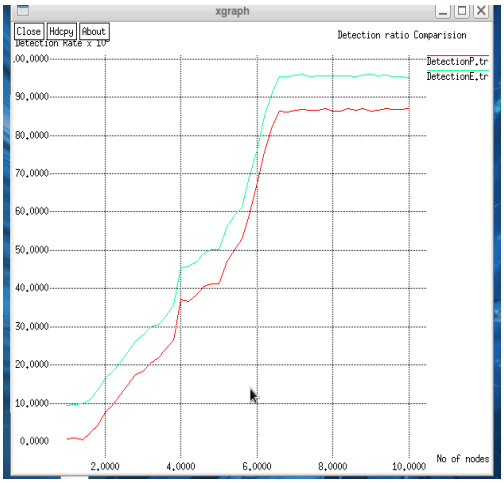

Fig.5 Detection Ratio

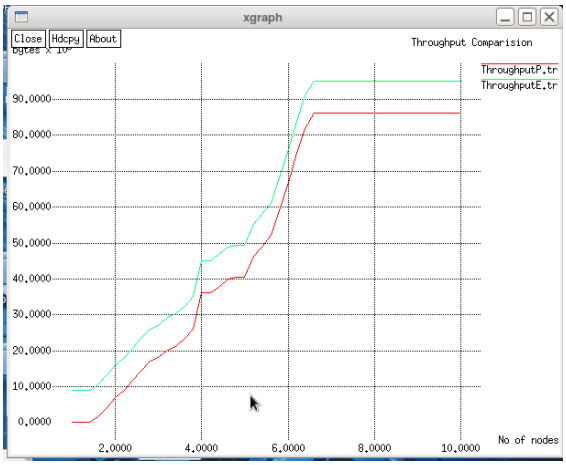

Fig.6 Throughput

4.2 THROUGHPUT

Throughput is the most rate of creation or the greatest rate at which something can be handled. At the point when utilized as a part of the setting of correspondence systems. Thus, the below graph(Fig.6) shows how the proposed scheme has proved its efficiency over the existing scheme.

4.3 PACKET RATIO

The ratio between received packets and over the packets also defined as the ratio of the number of delivered data packet to the destination (fig.7). The formula illustrates the level of delivered data to the destination.

$$\sum number\ of \frac{packetsreceive}{numberof\ packets\ sent}$$

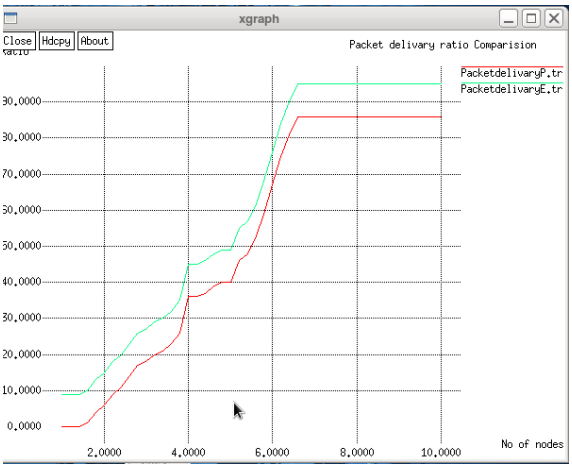

Fig.7 Packet Ratio

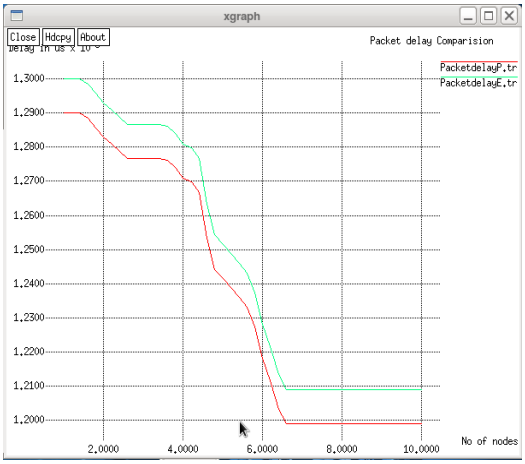

Fig.8 Message Delay

4.4 MESSAGE DELAY RATIO

The messages sent are converted into packets and there is a acknowledgement done between each packet while receiving, in the ratio of 1:1 is message delay ratio. The delay between each message is shown in the form of graph in this project(Fig.8).

5.CONCLUSION

In versatile WSN, hub replication assault is an essential one. The different reproduction recognition techniques are data traded based identification, hub meeting based location, and the portability based discovery. Of all the above mentioned three copy recognition techniques, the suggested study focuses on the versatility helped based location strategy.. The planned study upgrades the SHD strategy utilizing Clonal Selection calculation of AIS to enhance the recognition proportion through the choice of the good eyewitness hub. The suggested CSSHD strategy is utilized as a part of a completely appropriated environment where correspondence happens among single jump neighbors, exceedingly solid against hub plot and effective in securing against different copy hubs. The test is directed utilizing the ns-2 test system. The proposed technique is being great throughput, little above head and less untrue caution rate.

6.REFERENCES

1. L. Sujihelen and C.Jayakumar "**Detecting Node Replication Attacks in Wireless Sensor Networks: Survey**" Indian Journal of Science and Technology, July 2015.

2. J.Anthoniraj and T.Abdul Razak **"Clone Attack Detection Protocols in Wireless Sensor Networks"** International Journal of Computer Applications (0975 – 8887) Volume 98– No.5, July 2014

3. G.Raja, Dr.A.Rajesh "**Efficient Detection of Node Replication Attacks in Mobile Sensor Networks**" International Journal of Innovative Research in Computer And Communication Engineering,Vol. 2, Issue 2, February 2014.

4. M.H Ansari, V. TabatabaVakily **"Classification and Analysis of clone attack detection procedures in mobile wireless sensor networks**" International Journal of Scientific and Research Publications, Volume 2, Issue 11, November 2012.

5. Haafizah Rameeza Shaukat "**Node Replication Attacks in Mobile Wireless Sensor Network: A Survey**". International Journal of Distributed Sensor Networks,Volume 2014, Article ID 402541, 15 pages

6. L.S. Sindhuja and G. Padmavathi "**Replica Node Detections Using Enhanced Single Hop Detection with Clonal Selection Algorithms in Mobile Wireless Sensor Networks**" Journal of Computer Networks and Communications Volume 2016, Article ID 1620343, 13 pages

7. Miss. Raisa M. Mulla, Mrs. P.P. Belagali and Mr. Shivraj A. Patil "**Detection of Clone Attacks in Wireless Sensor Networks on the basis of Classification and Experimental Analysis"** International Conference on Computing,Communication,and Energy Systems ,Jan 2016.

8. G. Raja, Dr. A. Rajesh "**Efficient Detection of Node Replication Attacks in Mobile Sensor Networks"** International Journal of Innovative Research in Computer and Communication Engineering *(An ISO 3297: 2007 Certified Organization)* Vol. 2, Issue 2, February 2019.

9. Mohammad Hasan Ansari, Vahid Tabataba Vakili "**Performance analysis and classification of Clone attack detection procedures in mobile wireless sensor Networks"** International Journal of Computer Applications (0975 - 8887) Volume 71 - No. 21, June 2013.

10. Mindaugas Blonzelis **"Degree and Clustering Coefficient in Sparse Random Intersection Graphs**"

11. V. Manjula and C. Chellapan **The Replication Attacks in Wireless Sensor Networks Analysis and Defenses** Department of CSE, Anna University, Chennai, India.