X-EDD: A Hybrid Algorithm to Detect the Clone Attacks in Mobile Wireless Sensor Networks

Sandhya S, Vaishali Roy, Vinitha B, Dr. C. Geetha

Abstract: In wireless sensor networks, detection of duplicate nodes is done in many different ways. There are a number of nodes present which can be easily compromised by an adversary. There are many algorithms available in static sensor networks to detect the clones. The aim of our proposed algorithm is to find the clones in mobile sensor networks. The proposed algorithm divides the network into many clusters thus detecting the duplicate nodes easily. The network is divided into clusters whose radius is set by a random number. Every node entering the cluster then sends beacon to its neighbors. In case the node wants to move to other location, it sends its credentials like new location and the cluster ID to its neighbors in current as well as destination cluster. Now the cluster head detects the clones by verifying the node's distance travelled, speed of travelling and possibility of moving to a new location.

Index Terms: Clone Nodes, Cluster Head, Distance, Registration, Speed, sensor networks, Velocity

———————— ◆ ————————

1 INTRODUCTION

Wireless sensor network is an environment which consists of large number of spatially distributed sensor nodes that communicates wirelessly with each other. A sensor node, sometimes known as a mote, is a node present in a sensor network which is capable of performing some processing and gathering sensory information, communicating with other connected nodes in the network. In many WSN applications, the sensor nodes are said to be battery driven and are at times placed in some remote areas. So it is very difficult to recharge or change the batteries. Because the sensor nodes are depending on batteries extending the network lifetime is a critical issue. So in designing a good WSN, the main requirement should be energy efficient. The modern sensor networks are bi-directional also enabling control of sensing activity. The traditional network does not depend on deployment but sensor networks depend on dense deployment and all the nodes in the network are in co-ordination to carry out their tasks. Previously sensor networks consisted of less number of sensor nodes that were connected to a central processing station. However, nowadays, in the real time environment it focuses more on wireless, distributed, sensing nodes. [4].

The main characteristics of WSNs are battery-operated nodes, short range wireless communication, mobility of nodes, no/limited central manager, requirements: small size, large number, tether-less, and low cost, constrained by energy, computation, and communication. Additional characteristics are small size which implies small battery, low cost & energy implies low power CPU, radio with minimum bandwidth and range. It is said that the wireless sensor network has almost 43 constraints when compared to a traditional computer network. There are basically two types of networks in WSNs namely, static networks and dynamic networks where static networks are used as a result of its main feature, that is security. With the help of static network, the communication is possible only between nodes within its cluster or shorter coverage range. Hence duplicate nodes can be automatically and easily detected. So the detection protocols formulated for static sensor networks, all depends upon its self location claim, its ID and other non-important credentials which can be shared. It uses centralized detection, where after each location claims received by every node are then forwarded to the base station, which is present in every network. Ultimately, it is the responsibility of the base station, to detect the clone with the help of the data provided by the nodes present in that network. In case of dynamic network, communication or transfer of data is done with the help of routing information. That is, if required data can be transferred to other nodes of a network if required. This is most probably used in need of a wide use of communication. Usually dynamic networks are used, and it faces a lot of issues due to security. Generally, the detection protocol in dynamic network follows witness finding strategy where the witness node which is basically the base station (BS) finds the duplicate node in the network. Sometimes certain parameters are misread hence resulting in false positives and negatives. This problem is easily resolved with the help of sequential probability test [5], which helps the BS to decide accurately about the genuineness of the node under test. However, this protocol relies mainly on the BS which may incur the problem of single-point failure. Also, fast energy depletion in nodes surrounding the BS may occur. It also

Sandhya S, Vaishali Roy, Vinitha B are doing III Year CSE in R.M.K. Engineering College.
Mail Id: ssandhyarmk@gmail.com
Dr. C. Geetha is working as Associate Professor in the CSE Department of R.M.K. Engineering College.
Mail Id: cga.cse@rmkec.ac.in

suffers from storage overhead. The topology of the WSNs varies from a simple star network to an advanced multi-hop wireless mesh network and can be a combination of a number of types of networks. The propagation technique between the hops of the network can be routing or flooding.[10] Generally, sensor nodes are found to be useful in applications like area monitoring, military applications, health care monitoring, environmental sensing, air pollution monitoring, forest fire and landslide detection, water quality monitoring , data logging , structural health monitoring etc . To perform critical operations sensor networks could be deployed in a region which is known as hostile region. In that case, certain security constraints or requirements are applied to the respective node. The most important requirement would be the data confidentiality which plays a major role in the field of military where the data should be kept confidential. Sometimes nodes tend to get easily compromised by an adversary. This process is done by cloning the original node by copying all its credentials to the duplicate node and at last deploying it in the network. Thus the whole network will be taken under the control of the adversary gradually, thereby making the network vulnerable to a large class of insidious attacks, if left undetected. For detecting the duplicate nodes, detection algorithms are available in which the most popularly known is the witness finding strategy [9].Other detection algorithms include Sequential probability test [8]. Detection of duplicate nodes in the sensor network is a challenging problem hence only few algorithms have been proposed so far. In this paper, we have proposed an algorithm which helps in detection of duplicate node in a mobile sensor network.

2 RELATED WORKS

There are basically two differentiation on the basis of which the detection algorithm [3] is classified, namely the centralized and localized detection.

2.1 Centralized Detection

It is the most straightforward schemes. This method involves sending of data from each table (details of their neighbor node and their location) of each and every node present in the network cluster [2] to the base station. With the provided data, the base station then looks out for the replicated node which may be present in that specific cluster. If the search for the duplicate node becomes successful, then the base station can provoke the clone node by flooding the network with authenticated revocation message. But this approach faces many drawbacks starting with the base station. If the adversary tends to compromise the base station, then this protocol ends up being useless. Furthermore, the node nearest in its position to the base station may even attract the adversaries to replicate it. Finally, many networks do not have the luxury of a powerful base station, making a distributed solution a necessity.

2.2 Localized Detection

Localized detection is almost similar to the centralized detection. But instead of using a base station for detecting the duplicate node, in localized detection technique all the neighbor nodes present in the cluster plays a major role in finding the replica node. But the role played by each node isn't uniform. Hence that forms a major disadvantage for the localized detection, resulting in most people opting centralized detection.

2.3 Multicast

There are two main schemes in multicasting [7], namely, randomized and line-selected multicast. The first scheme, called randomized-multicast, distributes location claims to a randomly-selected set of nodes in the network. With an appropriate choice of parameters, they show that the birthday paradox ensures that a collision occurs with high probability, thereby creating witness nodes. The second protocol, called line-selected multicast, takes advantage of the routing topology of the network to select witness nodes. They show that line-selected multicast is more efficient that randomized-multicast in terms of communication and storage requirements.

Most of detection algorithms are mostly based upon 'witness finding strategy', 'velocity exceeding strategy' and other performance meters. The velocity exceeding strategy follows the concept of the travelling with the same velocity in the given network. Hence the node with the abnormal velocity is considered as the replica. Secondly, the witness finding strategy involves in selecting a node in the sensor network as the witness node, which contains all the details about the nodes present in that network. Hence, when a replica node is present in the network, it is easily identified with the help of information stored by it. The other parameters consider the performance level of the node in terms of speed, security, efficiency.

2.4 XED

The need of development of XED algorithm [11] is motivated by the observation that, if a sensor node meets another sensor node at an earlier time in the network and also exchanges a random number at that time. And when these nodes meet each other again, you can ascertain whether this is the node which met before by requesting the random number to it. In XED algorithm, we assume that the replicas cannot collude with each other in the network but this assumption will be removed in the next solution. In addition to this, all of the exchanged messages between the nodes in the network should be signed unless specifically noted. The XED scheme is mainly consisted of two steps [6] such as offline step and an online step. The offline step is executed before sensor node deployment in the network while online step is executed by each node in the network after deployment. One of the major disadvantages of this algorithm is that the effectiveness are fully depended on assumption that the replicated nodes would not collaborate with each other in the network. Hence to solve this drawback, EDD method is used.

2.5 EDD

In EDD algorithm the communication between nodes is based on certain conditions, like the maximum number of times that a node encounters with another node and this should be limited with high probability in fixed period of time in the network. Whilst the second condition is the minimum number of times the node encounters the replicas with the same ID in the network should be larger than a threshold in the same period of time. So that it has the ability to identify the replicas. Also that it overcomes drawback of XED [6][12] that replicas can collude with each other in EDD.

In addition to this, unless specifically noted all the exchanged messages between nodes should be signed. Mainly EDD algorithm is consist of two steps such as an offline step and an online step. The offline step is performed before sensor node deployment. On the other side, in the online step will be executed by each node after each move. Then each node checks whether the encountered node is a blacklisted node, hence at last preventing further communication with the node. After its detection, the node sometimes sends a beacon to the other neighbors about the new updation in the blacklisted node array, which in turn serves as a warning for the replica. Though, this method resolves the problem faced in XED method, it isn't that efficient in the detection process.

2.6 RED

This method, RED [1] , known as the randomized, efficient and distributed algorithm was found to be efficient in terms of communication , storage costs and detection accuracy of line selected multicasting. This algorithm involves the concept of witness node, which is responsible for detecting the clones in the network. RED executes at fixed intervals of time, and in each time period, witness nodes are selected as a function of a random seed broadcast by the base station. Because of the randomized nature of choosing witness nodes, the adversary is unable to identify and compromise these witness nodes ahead of time. While the costs of RED are lower than that of line-selected multicast per time period, the overall costs are higher, since RED repeats itself periodically.

3 PROPOSED METHOD

The proposed method in this paper is an advanced and hybrid version of both EDD and XED algorithm of detection of duplicate nodes along with time constraints.

3.1 System Architecture

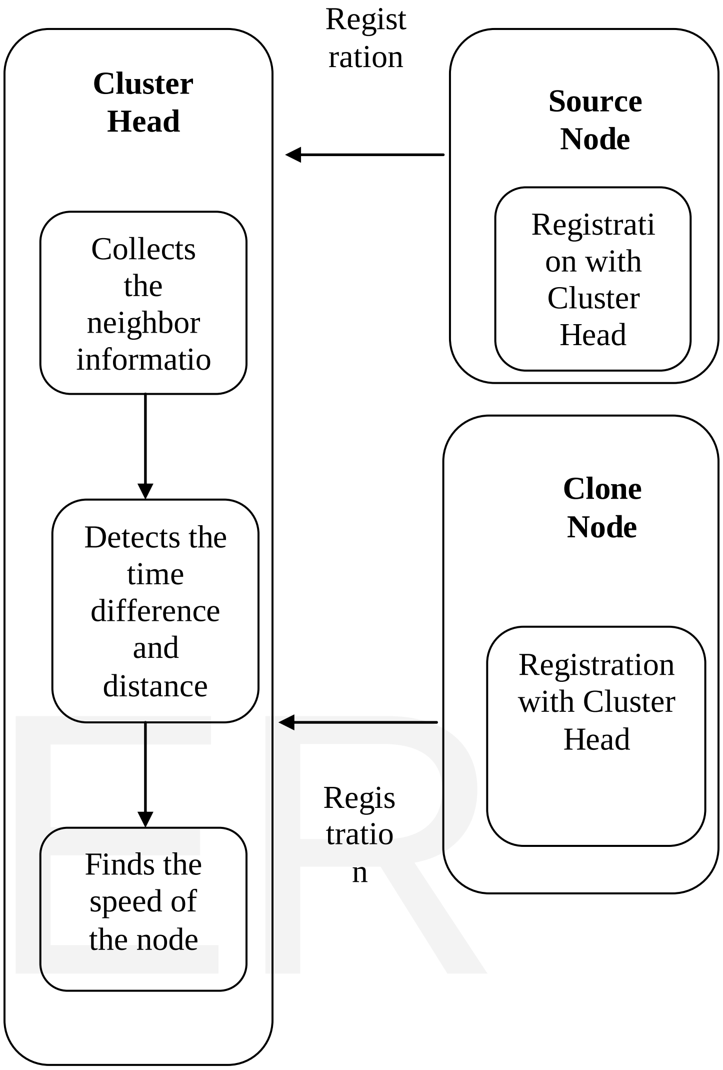
Regist
ration
Cluster Head
Source Node
Registrati on with Cluster Head
Collects the neighbor informatio
Clone Node
Detects the time difference and distance
Registration with Cluster Head
Regis tratio n
Finds the speed of the node

Figure 1. System Architecture

The Figure 1 shows the system architecture. Each node either it is original or clone register itself to the associated cluster head. Cluster head collects the registered credentials of the nodes within the cluster area and maintains it. Every time when a new node is registering to a cluster head by moving to from one cluster to another, head will collects the details like the time of the registering process, previous cluster head ID and location. It forwards this information to the previous cluster head. Now the previous cluster head will calculate the distance travelled by the node, by finding the timing of relieving from the previous cluster, from the time travelled, it finds the speed of the node. The speed calculated is compared with actual speed of the node and finds the possibility of moving to the new position. If everything is valid then the new cluster head will register the node. Otherwise it reports that the new node is a fake node.

3.2 Algorithm

Aim: To divide the network into many clusters thus increasing the probability of finding the duplicate nodes in the network.

1. Divide the network into clusters by using a radius which is calculated from the random number generated from rand() function.

$$\text{Rand}() \rightarrow \text{Random Number}$$

$$\textit{Radius} = (\textit{Random number} \div 100)$$

2. The nodes within the cluster can exchange the message between them as they are direct neighbors. For example, consider CH as the cluster head of that particular cluster. A node N1 belonging to that cluster sends a beacon to the CH with the following details.

$$\text{CH} \xleftarrow{\text{Encrypted}} < \text{id}, \text{Loc}, \text{Pkey}, \text{Starttime}, \textit{Status} >$$

Where,

id – the individual node's unique id

Loc – refers to the location of the node in the cluster

Pkey – Public key of the respective node

Starttime – The time when it started travelling to reach the present cluster.

3. Every node is maintaining a neighbor information table which consists of information about the neighbors within the cluster.

4. The cluster head will have collectively all the information from all neighbors.

5. In addition head is having the information about the nodes moved from this cluster.

6. When a node wants to move from this cluster to another cluster, it send a intimation message to cluster head and move.

7. After it reaches the new location, it starts the registration process with the new cluster head.

$$CH_{new} \xleftarrow{Encrypted} < id, loc, Pkey, Starttime_{new}, Status >$$

8. New registration information is emanated to all the cluster heads and updating happens in all head tables.

Given Table 1 is an example of the table maintained by the new cluster head.

TABLE 1 CLUSTER HEAD TABLE

ID	LOC	Pkey	Starttime	Status
U1	(10,20)	455	17:52	Present
U2	(25,100)	238	19:09	Present
U3	(32,15)	863	21:01	Absent

The status of each node can either be present or absent. If the value for id U1 is updated as present in new cluster head table, then the value of status in the old cluster head table will be updated as absent.

9. Now the source cluster head will find the time difference and the distance travelled.

$$Time\ difference\ T = StartTime_{new} - StartTime$$

$$Distance = T \div S$$

Where,
T – Time difference
S – is the speed or velocity of the node in the cluster.

10. From these statistics it checks the speed of the mobile node and its possibility to travel in the calculated speed.

11. If the speed is ok then the new registration is done by authenticated node. Otherwise it is clone node.

Let us consider a node U1. Using the random function, a random number is generated and radius is calculated from the designated formula. In that particular radius, many clusters are formed and each cluster is assigned a cluster head which contains a table containing all the details about the nodes. When a node enters a cluster, it sends a beacon with the necessary details to that cluster head. The status of that node is updated as 'Present'. If that node U1, now wants to move to another cluster, it sends an intimation message to the cluster head and moves. After reaching the new cluster, the previously done similar registration process is done. To check if it's a valid node, some constraints are calculated from the details provided by the node to the new cluster head. Before that, the head checks the id with the ids of the previously termed clone nodes. If the node id isn't present, node verification and validation is done. The needed constraints are calculated and cross checked with the values maintained by the old cluster head. If the values doesn't match, it is termed as a duplicate node.

4 RESULTS AND DISCUSSIONS

Considering an area 500 x 500 m , a minimum of 100 nodes are deployed in the network. In the Figure 2 the nodes are deployed in a way that each of the node belongs to a unique cluster. Each of the clusters is assigned a cluster head. Each node is assigned an ID. Each node knows its own location. The nodes are assigned with a public key and a private key. For example, the node ‘a’ is assigned with Puba and Pria as its public and private key respectively.

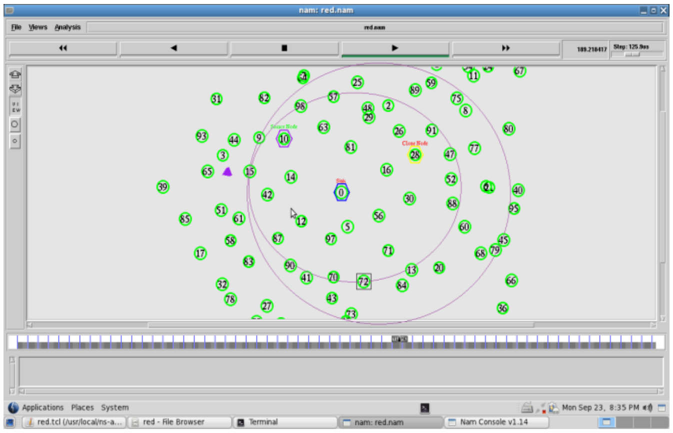

Figure 2.. Deployment of Sensor Nodes

The following graph shows the data taken from the execution of the algorithm for the factors detection rate and space occupancy. The graph in Figure 3 shows the detection rate in various iterations. The algorithm is executed for approximately 50 iterations and the corresponding detection rate is taken. The x-axis denotes the ‘detection rate’ and the y axis denotes the ‘number of iterations performed’. Initially, the detection rate is too low as the ‘previously detected clone node id’ column would be empty in the table. But as the number of iterations increases, the detection rate increases proportionally and drastically high when compared to EDD method. Soon after a particular extent, all the duplicate nodes will be detected and also the energy level of the cluster heads decreases than a threshold value. The detection rate is compared for both existing EDD and the proposed X-EDD algorithms. Our proposed method, X-EDD is found to be more efficient than EDD.

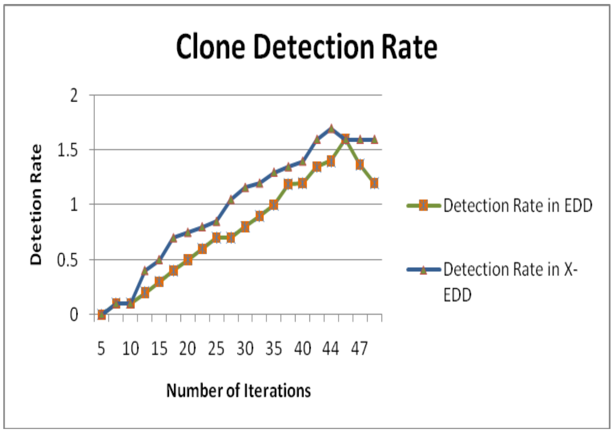

Figure 3. Iteration Vs Detection Rate

As per the algorithm’s time space trade-off, the algorithms space occupancy is little bit more because the messages are transmitted between the nodes as well as between the cluster heads. The space requirement comparison for both existing and proposed algorithms is show in Figure 4.

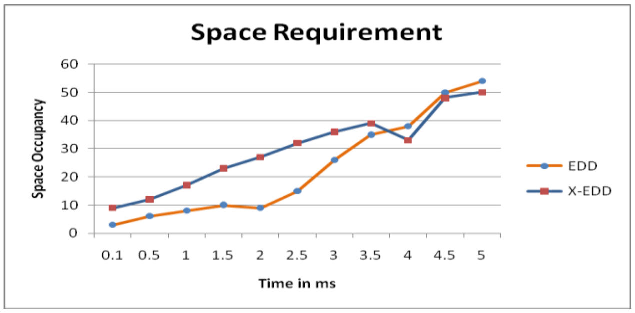

Figure 4. Time Vs Space Occupancy

5 CONCLUSION

It is very essential that the sensor nodes are effectively protected from the adversaries and to safeguard all its credentials. Hence it is understood that the level of security, efficiency, error rate should be accurately perfect. Hence, in this paper X-EDD, features of both XED and EDD algorithm were implemented and analyzed. The algorithm of our proposed method is found to be resolving the disadvantages of the previously available algorithms. By combining the concept of velocity exceeding strategy, the algorithm is found to be really efficient after introducing these along with the other two algorithms. The detection protocol discussed above can be used in many applications like military surveillance, environment monitoring, object tracking, patient health monitoring etc., By detecting node replication attacks, a large number of insidious attacks inside the network could be greatly resisted.

REFERENCES

[1] S. Angelin Vidhya ,"Detecting Node Replication Attacks in Mobile Sensor Networks ", International Journal of Communication and Computer Technologies Volume 02 – No.12 .

[2] Bryan Parno, Adrian Perrig ,Virgil Gligor ,University of Maryland , "Distributed Detection of Node Replication Attacks in Sensor Networks".

[3] C. Geetha, M.Ramakarishnan , Extended-Randomized, Efficient, Distributed: A Dynamic Detection Of Clone Attacks In Static Wireless Sensor Networks”, Journal of Computer Science, Vol 10 Issue 10 2014, pg 1900-1907.

[4] Gowrishankar.S , T.G.Basavaraju , Manjaiah D.H , Subir Kumar Sarkar , Proceedings of the World Congress on Engineering 2008 Vol I WCE 2008, July 2 - 4, 2008, London, U.K.,"Issues in Wireless Sensor Networks "

[5] Jun-Won Ho, Matthew Wright, and Sajal K. Das Department of Computer Science and Engineering, University of Texas at Arlington ,"Fast Detection of Node Replication Attacks in Mobile Sensor Networks"

[6] Manisha R, R.V Patil , "Detection of Node Replication Attack Using XED and EDD algorithms in Wireless Sensor Networks" Volume 7 • Number 1 Sept 2015 - March 2016 pp.50-58 in IJCSC

[7] Narasimha Shashidhar , Chadi Kari , and Rakesh Verma ,J. Sens. Actuator Netw. 2015, 4, 378-409; doi:10.3390/jsan4040378 , "The Efficacy of Epidemic Algorithms on Detecting Node Replicas in Wireless Sensor Networks".

[8] D.Prabhakaran,D.Gowthami, D.Suresh Babu ,"Detection of Node Replication Attacks in Mobile Sensor Networks" , International Journal of Electronics and Computer Science Engineering.

[9] Pooja Chaturvedi, Shyam S. Gupta Computer Department, Pune University Pune, India , International Journal of Computer Science and Information Technologies, Vol. 5 (6) , 2014, 7922-7926, "Detection of Node Replication Attacks in Mobile Sensor Networks Using Localized Algorithms".

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

[11] S.Silambarasi, Dr. G. J. Joyce Mary, "Effective and efficient detection of node replication attacks in mobile sensor networks" IJCN Special Issue - Data Management and Network Control in Wireless Networks (SICN) Singaporean Journal of Scientific Research(SJSR) Vol 6.No.3 2014 Pp.199-207

[12] Snehal R. Rane, Sachin D. Babar , Department of Information Technology, Sinhgad Institute of technology, University of Pune, "Detection of Node Replication Attack in Wireless Mobile Sensor Network Using Paillier" Volume 3 Issue 7 July 2014: Page 4.