ISSN (Online): 2319-8753
ISSN(Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 4, Special Issue 5, April 2015*

International Conference On Emerging Trends in Engineering and Technology (ICETET'15)

On 13th & 14th March 2015

Organized by

Pandian Saraswathi Yadav Engineering College, Arasanoor, Sivagangai, Tamilnadu, India

Dynamic Node Clone Detection Approach in Wireless Sensor Network

T. Tabitha Sharon[1], P.Balamanikandan[2]

P.G. Student, Department of CSE, Raja College of Engineering& Technology, Veerapanjan, Madurai, Tamil Nadu,India[1]

Assistant Professor, Department of CSE, Raja College of Engineering & Technology, Veerapanjan, Madurai, Tamil Nadu,India[2]

ABSTRACT: Sensor nodes that are placed in hostile environment are easily captured and compromised by any adversary entering into the network. The adversary creates multiple numbers of identical duplicates and adds it to network to reprove the network's performance. This type of attacks in wireless sensor network are called cloning attacks. Considering a static network in the existing system, two protocols have been used for clone detection namely, Distributed Hash Table (DHT) and Randomly Directed Exploration (RDE). The major problem in existing system is the communication overhead due to the 'witness-finding strategy'. Proposed work is implemented in the dynamic sensor network, where the clone detection is more effective and efficient using eXtremely Efficient Detection (XED) protocol. It provides a satisfactory level of security and storage consumption compared to the existing work. It also shows that the proposed work excels in efficient clone detection without any communication overhead.

KEYWORDS: Cloning attack, Distributed Hash Table, Randomly Directed Exploration, Extremely Efficient Detection, Communication overhead.

I. INTRODUCTION

A wireless sensor network is a collection of sensor nodes that will the physical conditions of the environments like sound, pressure, temperature etc. and pass the sensed data to a base station in a regular time intervals. The sensor nodes are made of low cost hardware components, small memory capacity with less computation compatibility. The sensors are also resource and battery life constrained, that are left unattended after deployment. Since these nodes lack in tamper resistant hardware, nodes are open to physical attacks. A serious physical attack is the sensor node cloning.

An adversary can enter into the network without anybody's notice, capture and compromise the sensor node deployed in the network. From the extracted details like identity, location, secret keys and credentials, the adversary will create identical duplicates in multiples and deploy those duplicates into the network, hence increasing the adversary's territory and reproving the sensor network's performance. In the critical conditions the adversary can gain control over the entire network leading to network failure.

The duplicate nodes can be detected through the clone detection methods. The nodes in the network communicate with one another by sending a location claim. Any nodes that receive 2 different location claims with same id and different location is said to be clones. Since the location of all the nodes remain unchanged after deployment in the case of static network.

In the previous study, considering the static wireless sensor network, there are 2 novel clone detection protocols implemented namely, Distributed Hash Table (DHT) and Randomly Directed Exploration (RDE). DHT is a distributed, checking and caching system. Though DHT provided high level of security the communication cost is comparatively high. This protocol is not suitable for the sensor networks that are sensitive to energy consumption. RDE protocol reduces the communication overhead by subsequently using the probabilistic directed technique to maintain a line property throughout the network transmission to detect the adversary. The above protocol provides reasonably communication cost and satisfactory level of detection probability.

ISSN (Online): 2319-8753
ISSN(Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 4, Special Issue 5, April 2015*

International Conference On Emerging Trends in Engineering and Technology (ICETET'15)

On 13th & 14th March 2015

Organized by

Pandian Saraswathi Yadav Engineering College, Arasanoor, Sivagangai, Tamilnadu, India

The proposed work is based on the dynamic wireless sensor network. The above protocols will not satisfy the requirements. Since these protocols are based on 'witness-finding strategy', it is little complicated in dynamic network. A new protocol named eXtremely Efficient detection (XED) is implemented that will be efficiently detect clones in the dynamic environment along with the automatic updation of time and location of each and every nodes.

The rest of the paper is partitioned as follows. First, the previous methods of clone detections are discussed in section II. Then, the clone analysis techniques implemented in this paper is elaborated in section III. Then, the XED protocols implementation and algorithms are explained in section IV. Next, the protocols are supported by the simulation results with a brief discussion in section V. Finally, the paper work is concluded in section VII.

II. RELATED WORK

In the paper [1], a novel distributed protocol is proposed for detecting duplicate nodes. By selecting the witnesses of the nodes randomly, that is located within a limited geographical area. This approach is known as Localised Mulicast (LM). There are 2 divergent approaches Single Deterministic Cell (SDC) and Parallel-Multiple Probablistic Cell (P-MPC). This approach provides resilience against the clone attacks.

In the paper [7], Random key Pre-distribution Scheme is implemented, where security of network is improved by pre-distributing keys. Even-though the adversary can capture the key. An algorithm is proposed to detect the presence of clones by looking how frequently the keys are used to authenticate in the network. Form the usage statistics, the clones are detected.

In the paper [3], SET Scheme is implemented, where the SET operations of exclusive subsets of the one-hop neighbours is done to detect the clones. SET employs a tree based structure to prepare non- overlapping subsets. Finally implements randomization to make subset and tree structure unpredictable by the adversary. Clones are detected if the intersection of subsets is non-empty.

In the paper [5], a new self-healing protocol named Randomized, Efficient and Distributed (RED) protocol is implemented for clone detection. Each node will broadcast a random value to all other nodes, while communication each node sends digital signal with the ID and location claim, since nodes cannot lie to the base station about the location of the nodes. Each time the node is verified with random value to assure it as a trusted node.

In the paper [6], Efficient and Effective Detection (EED) is a distributed protocol in which clones are detected by noting the number of times node 'A' encountering node 'B' in a particular time interval within area of range with rate of probability. It is implemented in offline and online to nodes to efficiently and effectively detect the clones.

III.CLONE DETECTION ANALYSIS

The sensor network consists of countable number of sensor nodes with a unique ID. Each and every node will communicate with its neighbor periodically with a message. One sensor node cannot be in 2 different places since it is a static network, witness-finding strategy helps clone detection. But in the case of mobile sensor network, the nodes can be in different positions at different period of times. The above schemes cannot be implemented directly in this mobile wireless sensor networks. Some modification has to be made to protocols, to make it adaptable to the dynamic network. Witness-finding strategy can be made flexible to dynamic network by adding a timestamp along with the each node's location claim. Also accuracy in time synchronization in the network is important feature in the dynamic sensor network.

The proposed protocol is based on the challenge -- and – response strategy. It is a localized detection algorithm. In this strategy each node can communicate with only one-hop neighbour, thus tremendously reducing the communication overhead. XED protocol provides efficient and effective clone detection by finding the clones with high degree of detection accuracy.

This approach also helps to reduce revocation message transfer by avoiding flooding of broadcast messages. The sensor nodes will move in a random path in the network and each node is aware of its current location in the network. All the nodes will move in a particular speed and reach the random destination position, then remains static for a random time and then it will start its movement again randomly in the network. Each node has a key for itself for communicating with the neighbours in the network.

ISSN (Online): 2319-8753
ISSN(Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 5, April 2015

International Conference On Emerging Trends in Engineering and Technology (ICETET'15)

On 13th & 14th March 2015

Organized by

Pandian Saraswathi Yadav Engineering College, Arasanoor, Sivagangai, Tamilnadu, India

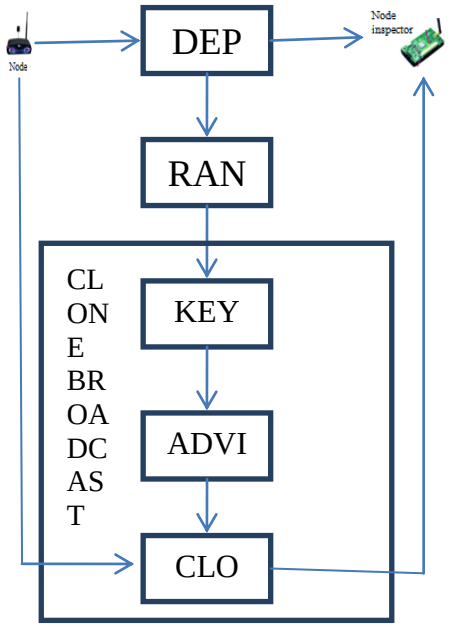


Figure 1: Architecture diagram of XED protocol.

Node deployment is the pre-work of the network formation. Each sensor sends the location claim to the all other nodes in the network for authenticating its details. Once communication is authenticated, nodes send the sensed data to the destination node. Initially each node shares a random number with each of its neighbours along with the key. This random number is checked in all the next meeting of the networks.

Nodes that communicate with the other nodes using the random number, clones can be detected if a node tries to communicate with a random number that doesn't match the trusted number. In this cases independent messages transferred to neighbours and size of the messages is

$$t= (1+kx)/(k+x) \qquad \text{.....(1)}$$

where k is the random k is the random number, and x is the distance between the two clone nodes. Then, if there are two cloned node identification, is

$$z=1+(1+2kx^2)/(k+2x)(k+x) \qquad \text{.....(2)}$$

This equation will implement to all witness nodes and separates the random numbers that will obtain by the

$$z_1 = 1+k(1-(1-k))^2 \qquad \text{.....(3)}$$

The probability is calculated P that is continues one. In this equation, there is a line divided by x point in k+1 segments and P is determined by the ratio of the segment length over the line length. Based on this, it is assumed that all point coordinate points are independent.

ISSN (Online): 2319-8753
ISSN(Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 4, Special Issue 5, April 2015*

International Conference On Emerging Trends in Engineering and Technology (ICETET'15)

On 13th & 14th March 2015

Organized by

Pandian Saraswathi Yadav Engineering College, Arasanoor, Sivagangai, Tamilnadu, India

IV. XED PROTOCOL IMPLEMENTATION

The basic concept behind this XED protocol is that, if a sensor node x meets another sensor node y initially in the network, node x will send a random number r to node y. when x and y meet again, x will request for the random number to y. If the random number matches, it will make sure that it is the trusted node that is communicated before. This random number is only for the x and y nodes. Each and every node communicating in the network will have to shares a random number at the first meet, so that those nodes can authenticate with that number in the future meetings.

Since being a mobile sensor network, the each and every node has to update the location information and the distance to the neighbour nodes in a regular time intervals. All the messages sent from one node to another have to be signed along with key before sending to another node.

The XED protocol is executed in 2 modes, namely offline and online mode. Online detection step refers to that sensor are verified before the deployment in the network. Offline mode refers to process of clone detection after the sensor nodes are deployed in the network.
This process is the effective implementation in extremely efficient detection (XED) method, but node movement is the primary factor of this network, so the movement distance is also implemented with the random key value. The following algorithm effectively implements this protocol.

Algorithm: Random_Number_Generation (RNx) : generates a random number for second meet neighbour nodes with distance

Output: Null, if two nodes transfer messages at initial time; Otherwise, it is the ID and random value that receives the messages in the network.

1. No ← N (listen || R)
2. If No € (next node, x) then { has transferred data}
    a. Analyse (R value) { implement key}
    b. If it is same then go to step 3
    c. Else return Null.
3. For q=1 to all nodes do
    a. If No € neighbour list then
    b. Inspect R value to neighbours
    c. Broadcast to all neighbours
    d. Repeat this process to all nodes
4. Verify the key value to the No node
5. Reconstruct the Neighbour list.

V. RESULTS AND DISCUSSION

The implementation works have been done over a dynamic wireless environment. This work is implemented both in simulation and model based environment. The first work is an initial network with a random graph model and starting with n nodes (n is limited and up to 10) that are placed in a wireless environment.

Initial location claim messages are sent per node in this model is in the following figure. In this graph network's load for nodes of X_p= 0.4 are exactly the node that is same parameters to other nodes. The graph is plotted with message transfer with random number evaluation time with different nodes with clone nodes.

The average size of neighbor nodes table and the witness number is identified in this graph which clearly indicates that the performance evaluation is considering by the network scenarios and the detection protocol implements the scalability of nodes that effectively detects the clone nodes with random number.

ISSN (Online): 2319-8753
ISSN(Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

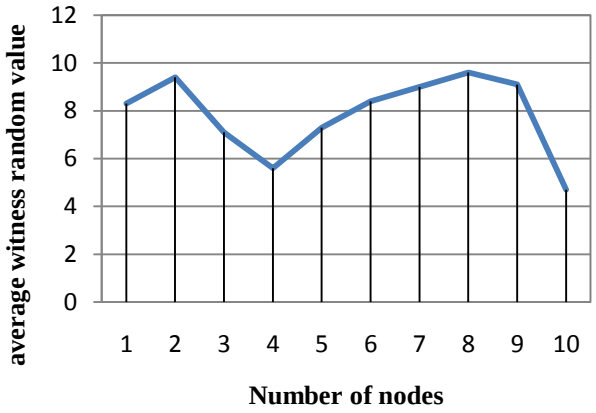
An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 5, April 2015

International Conference On Emerging Trends in Engineering and Technology (ICETET'15)

On 13th & 14th March 2015

Organized by

Pandian Saraswathi Yadav Engineering College, Arasanoor, Sivagangai, Tamilnadu, India



VI.CONCLUSION

The sensor nodes in wireless sensor networks are open to clone attacks. This paper focused the clone attack detection through few novel clone detection protocols. The two former algorithms holds good for clone detection in a static wireless sensor network whereas they these protocols cannot be directly implemented in the dynamic sensor network. These protocols had communication overhead problem since they are implemented based on witness-finding strategy. The eXtremely Efficient Detection protocol is proposed that be efficiently and effectively detecting the clone nodes and also tremendously reducing the communication overhead condition. The simulation result shows that this protocol outperforms the previously proposed method.

REFERENCES

[1].Bo Zhu, Sanjeev Setia, 'Efficient Distributed Detection of Node Replication Attacks in Sensor Networks' Computer Security Applications Conference, 2007.

[2].S.Dhanalakshmi1,S.Kaliraj2,Dr.J.Vellingiri3,'Efficient and Effective Detection of Node Replication Attacks in Mobile Sensor Networks', IJERD, Volume 8, Issue 10 (October 2013), PP. 26-31.

[3]. Heesook Choi, Sencun Zhu, Thomas F. La Porta 'SET: Detecting node clones in Sensor Networks', 2007.

[4].Kai Xing, Fang Liu, Xiuzhen Cheng David H.C. Du, 'Real-time Detection of Clone Attacks in Wireless Sensor Networks',Distributed Computing Systems, 2008.

[5]. Murali Pulivarthi1, Shafiulilah Shaik2, M Lakshmi Bai3, 'Detection of Clone attacks in Wireless Sensor Networks Using RED (Randomized, efficient, and distributed) Protocol', IJERD, Volume 4, Issue 7 (November 2012), PP. 30-44.

[6]. Raju M, Selvan M, 'An Approach in Detection of Replication Node in Wireless Sensor Networks: A Survey', Raju M et al, /IJCSIT, Vol. 5 (1) , 2014, 192-196.

[7].Richard Brooks, P. Y. Govindaraju, Matthew Pirretti, N. Vijaykrishnan, ,and Mahmut T. andemir, ,'On the Detection of Clones in Sensor Networks Using Random Key Predistribution', IEEE TRANSACTIONS VOL. 37, NO. 6, NOVEMBER 2007.

[8].Tamara Bonaci, Phillip Lee, Linda Bushnell, Radha Poovendran , 'Distributed Clone Detection in Wireless Sensor Networks: An Optimization Approach' 2011 IEEE International Symposium.

[9]. Zhijun li, and Guang gong, 'On the node clone detection in wireless sensor networks', IEEE / ACM TRANSACTIONS ON NETWORKING, VOL. 21, NO. 6, December 2013.