Automated Method of Clone Nodes Detection in Wireless Sensor Networks

Dr. Z. Faizal khan,
Department of Computer and Network Engineering,
College of Engineering, Shaqra University,
Al Dawadmi, Kingdom of Saudi Arabia
Email: faizalkhan@su.edu.sa

Dr. Syed Usama Quadri,
Department of Computer and Network Engineering,
College of Engineering, Shaqra University,
Al Dawadmi, Kingdom of Saudi Arabia
Email: usyed@su.edu.sa

Abstract: A computer network is a collection of computers and other hardware components interconnected by communication channels that allow sharing of resources and information. Wireless sensor network refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. In this paper, a new automated algorithms for detecting clone nodes in sensor networks has been proposed. One of the serious physical attacks faced by the wireless sensor network is node clone attack. In this paper, two node clone detection protocols are introduced through XED (eXtremely efficient Detection) and EDD (Efficient distributed Detection to detect node clones. The former can resist node replication attacks in a localized fashion to detect node clones. The later one is can identify replicas with high detection accuracy. The simulation results for the spatial distribution of witness nodes and for detecting clone nodes are done using NS2 and obtained randomly directed exploration is the best one having accurate detection of clone nodes.

Keywords: EDD, Networking, Replication, Sensor nodes, Wireless network, XED.

I. INTRODUCTION

A group of sensor nodes work collaboratively to perform a common application. In many WSN applications, the sensor nodes are battery driven and they are often very difficult to recharge or change the batteries. Prolonging network lifetimes a critical issue. Sensors often have long period between transmissions. This mechanism allows to identify replicas that are formed in the mobile sensor network. These replicas are formed due to the node replication attack in which an adversary compromises one node, fabricate many replicas having the same identity (ID) from the captured node, and place them back into strategic positions in the network. The replicas can easily launch insider attacks, without easily being detected.

To detect the node replicas, two localized algorithms, eXtremely Efficient Detection (XED) and Efficient Distributed Detection (EDD) are used. Each node shares a different secret key with all its neighbors when it communicates for the first time. When a node receives a message it asks for the random key and verifies it. If the key matches it receives the message. If key does not match the sender node is clone node. In the EDD algorithm, when a node receives a message it asks for the last communicated location. If the location matches it receives the message. If location differs, the sender node is clone node. If any node informs next position where it going to move and if it doesn’t move to that position means it is considered as malicious node and maintained by the neighbors. If misbehavior length is reached to given limit means, then it is also considered a clone node.

II. RELATED WORKS

There are many works corresponds to this area wireless sensor network. When a sensor node attempts to join the network it must broadcast a signed location claim to its neighbours. Most of the existing distributed detection protocols adopt the witness-finding strategy to detect the replicas. When there are replicas in the network, the witnesses, according to the received location claims, have possibility to find a node ID with two distant locations, which implies that the node ID is being used by replicas. Afterward, the detected replicas are excluded using network-wide revocation. In this process after identifying the replicas, a message is used to revoke the replicas, possibly issued by the witness that detects the replicas, is usually flooded throughout the network. Time synchronization is needed by almost all detection algorithms which is still a challenging task to synchronize the time of nodes in the network.RM and LSM were proposed to determine the witnesses randomly. The difference between RM and LSM is that the witness nodes that find the conflicting location in the former are primarily affected by the number of witness nodes and the ones in the latter are primarily affected by the forwarding traces of location claims. Main challenges of existing system, used only for static sensor network and are not useful if nodes have mobility, false witnesses.

Yao-Tung tsou et al explains about Localized Algorithms for Detection of Node Replication Attacks in Mobile Sensor Networks. It deals with the challenging problem of node replication detection. Although defending against node replication attacks demands immediate attention, compared to the extensive exploration on the defense against node replication attacks in static networks, only a few solutions in mobile networks have been presented. Moreover, the most of the existing schemes in static networks rely on the witness-finding strategy, which cannot be applied to mobile networks, the velocity-exceeding strategy used in existing schemes in mobile networks incurs efficiency and security problems. Therefore, based on our devised challenge and response and encounter-number approaches, localized algorithms are proposed to resist node replication attacks in mobile sensor networks.

Marwan krunz et al described Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes. Compromised-node and denial-of-service are two attacks in wireless sensor networks. In data delivery mechanisms black holes are formed by these attacks. Classic multipath routing approaches are vulnerable to such attacks. So once the adversary acquires the routing algorithm, it can compute the same routes known to the source, hence making all information sent over these routes vulnerable to its attacks. The routes taken by the “shares” of different packets change over time. So even if the routing algorithm becomes known to the adversary, the adversary still cannot pinpoint the routes traversed by each packet. The generated routes are also highly dispersive and energy efficient, making them quite capable of circumventing black holes.

Adrian perrig et al explains about Random Key Pre-distribution Schemes for Sensor Networks Key establishment is a challenging problem because asymmetric key cryptosystems are unsuitable for use in resource constrained sensor nodes, and also because the nodes could be compromised by an adversary. There are three new mechanisms for key establishment using the framework of pre-distributing a random set of keys to each node. First, in the q-composite keys scheme, trade off the unlikeliness of a large-scale network attack in order to significantly strengthen random key pre-distribution’s strength against smaller-scale attacks. Second, in the multipath-reinforcement scheme, it shows how to strengthen the security between any two nodes by leveraging the security of other links. Finally, the random-pair wise keys scheme, which perfectly preserves the secrecy of the rest of the network when any node is captured, and also enables node-to-node authentication.

Vamsi paruchuri et al described Key Distribution in Mobile Heterogeneous Sensor Networks.There are two key pre-distribution based scheme for heterogeneous networks that consist of nodes which are stationary as well as highly mobile. The existing schemes make use of only one key pool to establish links between the stationary and the mobile nodes. This restricts the mobility of nodes to one specific network. If the same key pool is used in multiple networks, the compromise of keys in one network would lead to compromise of keys in all the networks. Two different solutions are described in this problem. The first approach uses a separate disjoint key pool to establish links between the stationary and mobile nodes of the network. In the second approach, have to take a large key pool and segment it into smaller key pools. Each of these segments acts as the key pool for different stationary sensor networks. The aggregate key pool can have some segments which can be used for future deployments.

III. PROPOSED SYSTEM

To detect the node replicas in mobile sensor networks, two localized algorithms, XED (eXtremely efficient Detection) and EDD (Efficient distributed Detection) are proposed. The techniques developed in our solutions, challenge-and-response and encounter-number, are fundamentally different from the others. XED and EDD can resist node replication attacks in a localized fashion. Each node in the localized algorithm can communicate with only its one-hop neighbors. This characteristic is helpful in reducing the communication overhead significantly and enhancing the resilience against node compromise. The XED and EDD algorithms can identify replicas with high detection accuracy. Notably, the storage, communication, and computation overheads of EDD are all only O (1). The revocation of the replicas can be performed by each node without flooding the entire network with the revocation messages. The time of nodes in the network does not need to be synchronized.

IV. PROPOSED ARCHITECTURE

Proposed architecture represents the way of clone detection in mobile sensor networks. If any node communicates with another node means, first, it shares the random number, secret key and last location. This architecture contains buffer and its used to store the information of the nodes. Buffer L contains all the previous location communicated with other nodes. Communication arrow includes all type of checking by XED (eXtremely efficient Detection) and EDD (Efficient distributed Detection) algorithms. Buffer K contains all keys sent and received from other nodes. Buffer C contains all clone node detected by that node. If any node moves from one position to another position means it should inform to all of its neighbor nodes. Buffer Mc contains count of malicious behavior for each and every node.

V. MODULE DESCRIPTION

Each node created by assigning some name and range. Here node is indicated with a small circle filled with some color and its coverage is shown by a big circle, it's based on given range. Now the node should be moved inside the given network. Once you moving your node automatically that particular nodes x-axis and y-axis changes accordingly. And a random port number is assigned to each node. The architecture of the proposed system is shown in figure 1.

After the network formulation each and every node shares a different secret key with all its neighbors. So, the sharing keys between two nodes won't be same. While any node which is going to move from its current region, it must forward the region where it going to move in next 'n' seconds. Now all of its neighbors calculate the position which they received, will come under their communication range or not. If it lies in communication range means the sender node will be neighbor, otherwise the sender node will be removed from the neighbor list.

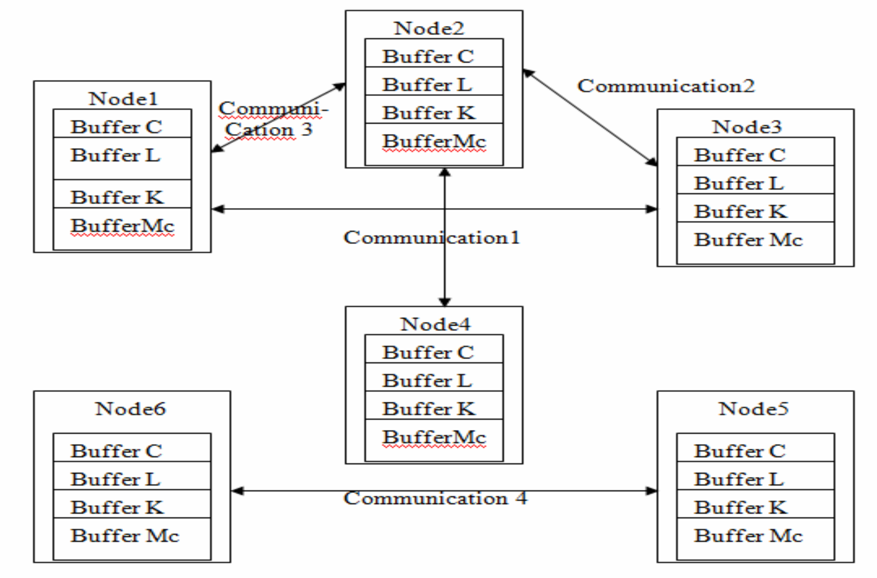


Figure 1 Proposed Architecture

During the detection phase, if any node receives a data, first it checks the buffer (contains clones detected by this node) whether the sender node present in the buffer or not. If the sender is clone node means it will drop the communication, else it checks the buffer (maintained by all nodes independently) whether the sender node is already communicated or not. If it is already communicated means, first it asks for last location details of both the node and after that asks for random number. And these two details were maintained by all nodes independently.

Once receiver receives the keys, it will check whether the sender keys matches or not. If the key matches means then the sender is not malicious node. If any of key doesn't matches means then the sender node is clone node. So it adds the sender name to buffer (contains all clones detected by this node) which is maintained by all nodes locally. And if any node misbehaves in moving, i.e, if it will informs next position where it going to move and if it doesn't move to that position means its misbehavior is considered and maintained by the neighbors. If misbehavior length is reached to given limit means, then also that node is considered a clone node and added to buffer. The proposed algorithm for detecting clone nodes is as follows.

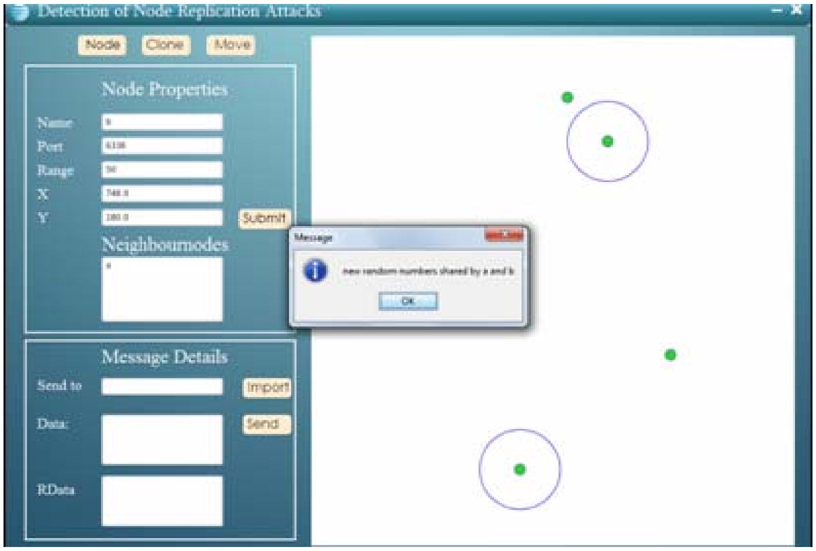
Input: Communication between two nodes.
Output: Detecting clone node.
Step1: Node creation.
Step2: Random number is shared by node a and b while first time communication.
Step3: secret key is shared by the corresponding node.
Step4: Key information is stored in the buffer K.
Step5: Compromising request send from node c to node b.
Step6: Compromising request is accepted by node b.
Step7: Node b become a clone node.
Step8: Clone node details are stored in the buffer C.

VI. IMPLIMENTATION

This work has been implemented by using XED (eXtremely efficient Detection) and EDD (Efficient Distributed Detection) algorithm in a java environment. Java platform allows software developers to write program code in other languages than the Java programming language which still runs on the Java virtual machine. The Java platform is usually associated with the Java virtual machine and the Java core libraries. Java manages the memory allocation and de-allocation for creating new objects. The program does not have direct access to the memory. The so-called garbage collector automatically deletes objects to which no active pointer exists.

VII. RESULT AND DISCUSSION

The solutions for static networks provide a detection algorithm that "can detect the replicas" without mentioning "when the network owner should apply the detection algorithm." The drawback is that the network owner has to be aware of the existence of the replicas. Afterward, the network owner resorts to the detection algorithms to identify the replicas. In contrast, our proposed algorithms automatically detect the replica anytime and anywhere. In the algorithms adopting the witness-finding strategy, the spatial distribution of witness nodes is usually an evaluation metric of the underlying detection algorithms. Ideally, it is uniformly distributed over the sensing region. Nevertheless, this evaluation metric is specific for the algorithms adopting the wit-ness-finding strategy due to the need of witness nodes in their methods, and is not required in our proposed algorithms. The results obtained for our proposed algorithm is shown in figure



Detection of Node Replication Attacks

Node Properties
Name: b
Port: 6138
Range: 50
X: 748.0
Y: 180.0
Neighbournodes: a

Message Details
Send to:
Data:
RData

Message
new random numbers shared by a and b

Fig.2 Information sharing

VIII. CONCLUSIONS

In this paper, two replica detection algorithms for mobile sensor networks, XED and EDD, are proposed. Although XED is not resilient against collusive replicas, its detection framework, challenge-and-response, is considered novel as compared with the existing algorithms. Notably, with the novel encounter-number detection approach, which is fundamentally different from those used in the existing algorithms, EDD not only achieves balance among storage, computation, and communication overheads, which are all O(1), but also possesses unique characteristics, including network-wide time synchronization avoidance and network-wide revocation avoidance, in the detection of node replication attacks.

REFERENCES

[1]. M. Conti, R. Di Pietro, L. V. Mancini, and A. Mei, "A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks," in Proc. ACM Int. Symp. Mobile AdHoc Networking and Computing (MobiHoc), Montreal, Canada, 2007, pp. 80–89.

[2]. M. Conti, R. D. Pietro, and A. Spognardi, "Wireless sensor replica detection in mobile environment," in Proc. Int. Conf. Distributed Computing and Networking (ICDCN), Hong Kong, China, 2012, pp.249–264.

[3]. R. Sathish, D. Rajesh Kumar, "Proficient Algorithms for Replication Attack Detection in Wireless Sensor Networks," 2013 IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology (ICECCN 2013)

[4].J. Ho, M. Wright, and S. K. Das, "Fast detection of replica node attacks in mobile sensor networks using sequential analysis," in Proc. IEEE Int. Conf. Computer Communications (INFOCOM), Brazil, 2009, pp.773–1781.

[5]. Zhijun Li, Guang Gong, "On the Node Clone Detection in Wireless Sensor Networks", IEEE/ACM transactions on networking, vol. 21, no. 6, december 2013.

[6]. Sinthiya, S.Abirami, "In Mobile Sensor Networks Localized Algorithms for Detection of Node Replication Attacks", International Journal of Research Studies in Computer Science and Engineering (IJRSCSE) Volume 1, Issue 1, May 2014, PP 65-69

[7]. B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node repli- cation attacks in sensor networks," in Proc. IEEE Symp. Security and Privacy (S&P), Oakland, CA, USA, 2005, pp. 49–63.

[8]. Jun-Won Ho, Matthew Wright, Sajal K. Das, "Fast Detection of Mobile Replica Node Attacks in Wireless Sensor Networks Using Sequential Hypothesis Testing," IEEE transactions on mobile computing, vol. 10, no. 6, june 2011

[9]. B. Zhu, S. Setia, S. Jajodia, S. Roy, and L. Wang, "Localized multicast: Efficient and distributed replica detection in large-scale sensor networks," IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 913–926, Jul. 2010.

[10]. M. Zhang, V. Khanapure, S. Chen, and X. Xiao, "Memory efficient protocols for detecting node replication attacks in wireless sensor networks," in Proc. IEEE Int. Conf. Network Protocols (ICNP), Princeton, NJ, USA, 2009, pp. 284–293.

[11] R. Brooks, P. Y. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M.T. Kandemir, "On the detection of clones in sensor networks using random key predistribution," IEEE Trans. Syst., Man, Cybern. C, Applicat. Rev., vol. 37, no. 6, pp. 1246–1258, Nov. 2007.

[12]. Sidhhi Raut , Vrunda Bhusari," Efficient and Effective Algorithm Detection of Node Replication Attacks in Mobile Sensor Networks," International Journal 2 Volume 4, Issue 2, February 2014

[13]. Kwantae Cho, Minho Jo, Taekyoung Kwon, Hsiao-Hwa Chen, Dong Hoon Lee, "Classification and Experimental Analysis for Clone Detection Approaches in Wireless Sensor Networks" IEEE systems journal, vol. 7, no. 1, march 2013

[14] Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie, "Random-walk based approach to detect clone attacks in wireless sensor networks," IEEE J.Sel. Areas Commun., vol. 28, no. 5, pp. 677–691, Jun. 2010

AUTHORS PROFILE

Dr. Z. Faizal Khan, is working as an Assistant Professor in the Department of Computer and Network Engineering, College of Engineering Dawadmi, Shaqra University, Kingdom of Saudi Arabia. His areas of interest include Medical image processing, Soft computing, Pattern Recognition and Wireless Sensor Networks.

Dr. Syed Usama Quadri is working as Head, Department of Computer and Network Engineering, College of Engineering Dawadmi, Shaqra University, Kingdom of Saudi Arabia. His areas of interest include Software Engineering, Computer Networks and Wireless Sensor Networks.

.