Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 02, February-2016

Mobility Assisted Distributed Solution for Node Replication Attacks in Mobile Sensor Networks

Hehma Gayatri. R
ECE department
MVIT Puducherry, India

Priyadharshini. M
ECE department
MVIT Puducherry, India

Brindha. B
ECE department
MVIT Puducherry, India

***Abstract*— In wireless sensor networks one of the greatest challenging problem is node replication detection. In static sensor networks , the witness finding strategy was used in node replication detection, in which a subset of nodes named witness nodes was used . But however in mobile sensor networks due to the motion of the nodes , its location varies and the witness finding strategy fails. And hence in mobile sensor networks, the velocity exceeding strategy was used. Yet practically there could be some errors in node speed measurement resulting in false positives and false negatives. In order to avoid such false judgments the velocity exceeding strategy has been dropped. Later on several algorithms were proposed to detect node clone attacks in mobile network but however they were prone to node compromise issues and affecting effective detection. Hence localized detection algorithms like eXtremely Efficient Detection (XED) and Efficient Distributed Detection (EDD) were proposed. The random number exchange technique used in XED fails as a smart attacker can crack out the random number being exchanged. And in case of EDD algorithm it leads to storage overhead problem as each node needs to maintain a list. To avoid routing and other problems, we make use of mobility property of the node in the algorithm UTLSE (Unary Time Location Storage and Exchange) and MTLSD (Multi-Time Location Storage and Diffusion) in which time location exchange occurs only when two witness nodes encounters each other. Using network simulator 2 (ns2) analysis of the proposed algorithm is made and the replication attacks will be avoided.**

***Keywords*— Replica, XED, EDD, UTLSE, MTLSD.**

I. INTRODUCTION

Wireless sensor networks (WSNs) are generally deployed in the unnoticed environments for some missions, like enemy surveillance and environment monitoring. The unnoticed nature and the lack of tamper-resistant hardware will make WSN to be vulnerable to various insider attacks, and threatens the operation of WSNs. Replication attack is one of the insider threats in the network. The attacker captures one or more sensor nodes, interferes with them and gets the credential materials, such as the identity and keys, then clones some nodes as replica nodes, and clandestinely inserts these replicas in the network. This allows a situation where the adversary or the hacker can compromise one sensor node, fabricate many replicas having the same ID from the captured node, and place these replicas back into the positions we need in the network for further malicious activities in the network. This is a so-called *node replication attack*. Subsequently, the attacker may launch a variety of subtle attacks, such as selecting forwarding, data injection, routing loop, or even topology partition

II. RELATED WORK

A. Centralised approach

The schemes in [3–6] assume a central base station to conduct the detection. Choi et al. [3] proposed to detect the replicated nodes by set. The network is divided into disjoint sub regions. A header node is listed to report the member list to the base station in each sub region. The reports from the entire header nodes are computed by set .The intersection of two sets are checked; any nonempty intersection implies that the existence of the replica sensor node. Brooks et al. [4] gave a centralized scheme to detect replication attacks by using random key pre distribution. Every sensor node should report the key usage to the base node. If the usage of some key exceeds the threshold, then the sensor node was identified to be cynical. Ho et al. [5] presented a SPRT method for node replica detection in mobile sensor networks, where the base station checks whether the speed of the mobile sensor nodes exceeds the threshold value. Based on a signal processing technique, compressed sensing, Yu et al. [6] proposed CSI to detect replication attacks.

B. Localized approach

To detect the node replicas in mobile sensor networks, two localized algorithms, XED and EDD, are made. The techniques developed in our solutions, challenge-and-response and encounter-number, are basically different from others.

1.) *XED:* The idea behind XED is motivated by the observation that, if a sensor node u meets another sensor node v at an earlier time and sends a random number to v at that time, then, when u and v meet again, node u can ascertain whether this is the node met before by requesting the random number. If node u receives the same random number exchanged before then it can conclude that it was the original node v it met before. But if it receives any random number inconsistent to the one exchanged before then it identifies it as the replica of node v.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 02, February-2016

2.) *Disadvantages of XED:* The effectiveness of XED, regrettably, heavily relies on the assumption that there is no collusion of replicas with each other. When replicas can communicate with each other, the replica can share the newest received random numbers with the other neighbouring replicas in the network, thus degrading the detection capability because two or more replicas are able to reply with the correct random number to encounter genuine nodes accordingly.

3.) *EDD:* The idea behind EDD is due to the following observations given below. The maximum number of times, the node encounters a specific node, should be limited with a very high probability during a fixed period of time, while the minimum number of times, that encounters the replicas with same ID, should be larger than a threshold during the same period of time. According to these observations, if the nodes can discriminate between these two cases, it has the ability to find the replicas. Different from XED, EDD makes assumption that the replicas can overlap or collude with each other. In addition, unless we specifically note that the exchanged messages should be signed.

4.) Distributed Detection Approaches: In distributed approaches, the replication attacks detection is made by reporting the location claim messages to randomly chosen witness nodes in the network. Differences of the location claims indicate the detection of replication attacks. For further improvement in the detection probability, UTLSE and MTLSD algorithms are being used. In this work, we seek to detect and defend the replication attacks with some small communication, computation, and memory overheads than previous works. We propose a pairwise key scheme, location-binding for forcing the attacker to insert the replica nodes to the vicinity of the compromised node. Then, the neighbour nodes around the replica sensor nodes are made the first possible witnesses to detect the replication attacks.

III. Proposed Method

A. *Unary-Time-Location Storage and Exchange (UTLSE)*

In this protocol each node in the network is initialized with unique tracking set, which means every node is a witness of each node in that tracking set. When a node meets a new neighbour who is a member of that node's tracking set, it will asks the neighbour for its time-location claim to it. Also if the tracking set of the node and the neighbour is not disjoint and the ID of the neighbour is smaller than the node, it sends all the stored time-location claims of each common tracked node to its neighbour. If any witness node receives two contradictory time-location claims for the same node ID, it will detect the existence of a replica and can take appropriate actions to nullify the node's credentials. Once the replica is identified in the network, then the replica will either be destroyed or else the transmission between those networks are avoided.

B. *Multi-Time-Location Storage & Diffusion (MTLSD)*

To show that loop hole exists in UTLSE protocol we consider the situation. Suppose two legitimate nodes *a* and *b* both are witnesses of a compromised node *x*. At time t_1, node *a* rendezvous one replica of node *x* positioned at l_1. At time t_2, node *b* encounters another replica of node say *x* positioned at l_2. $<t_1, l_1>$ and $<t_2, l_2>$ are contradictory. However before node *a* encountering node *b*, they separately meet another replica x_I which is the replica of node *x* of which location is same and given as l_3. Then both of them replace l_1 and l_2 with l_3. Thus node a (or node b) regards node *x* as a legitimate or reliable node. Though the explained situation does not always occur, it reduces the detection probability to some extent. So MTLSD was made by making some modifications in UTLSE to minimize the loss made due to loop hole. In MTLSD a queue called FIFO queue of length three is maintained to store the corresponding time location claims for each node in the tracking set. Considering node *a* meets node *b* and if their tracking set is not disjoint, then both node *a* and *b* send a request messages to each other. Receiving these messages which are different from they have stored, the received time location claims are inserted into the corresponding queue at the right position. But like UTLSE the detection process is done only to the node with smaller ID.

IV. Performance Analysis

Two metrics are used in order to figure out the efficiency of the two protocols UTLSE and MTLSD.

A. *Communication Overhead*

Communication overhead refers to the average number of messages sent by a sensor node while propagating the location claims. According to the calculations made by the authors the communication overhead is O (N) where N is the total number of nodes in the sensor network

B. *Storage Overhead*

Storage overhead is the average number of the location claims stored in a sensor node. Hence each node in the network tracks nodes, and for each tracked node, only one queue (with fixed length) is maintained and the storage overhead of every node is O for storing the corresponding location claims. Detection probability and Detection time are two the performance evaluation indices of UTLSE and MTLSD protocols. From observation the detection probability was high for MTLSD compared to UTLSE .But detection time was less for MTLSD compared to UTLSE.

C. *Area Vs Detection Time*

From the figure1 it is evident that as the area of observation increases, with fixed number of nodes the detection time increases as the communication distance between the nodes increases as the area increases. But however the detection time of MTLSD is less compared to other existing techniques because of the use of an FIFO queue which can detect more than one replica simultaneously.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 02, February-2016

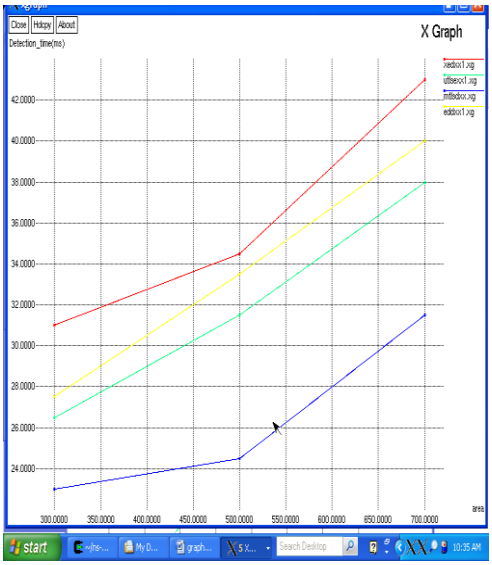

Figure1: Area Vs Detection Time

D. Number of nodes Vs Detection Time

From the graph it is evident that as the number of nodes within a particular area of fixed size increases the detection time increases. But however the detection time of the proposed techniques (UTLSE and MTLSD) were found to be less when compared to the existing techniques (XED and EDD). Here UTLSE and MTLSD will detect the replica at a at the earlier time than XED and EDD. Also the performance of the proposed technique is efficient as shown in figure2.

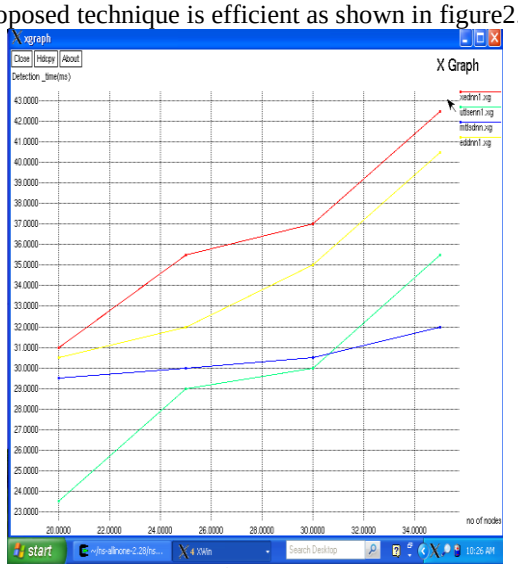

Figure2: Number of nodes Vs Detection Time

V. CONCLUSION

Because of the mobility-assisted property the protocols (UTLSE and MTLSD) do not rely on any specific routing protocol in the network, which makes them suitable for various mobile settings and the added advantage is the fast and accurate detection. Also the MTLSD proposed technique uses FIFO queue inorder to store the time location claims which is more advantageous than XED and EDD algorithms. In future this can be extended by applying it in real time applications.

REFERENCES

[1] Chia-Mu Yu, Yao-Tung Tsou, Chun-Shien Lu *and Sy-Yen Kuo"* Localized Algorithms for Detection of Node Replication Attacks in Mobile Sensor Networks ", *IEEE Transactions on Information Forensics and Security*, VOL. 8, NO. 5, MAY 2013.

[2] *Abu Saleh Md. Tayeen , A.F.M. Sultanul Kabir , Razib Hayat Khan "*Mobility Assisted Solutions for Well-known Attacks in Mobile Wireless Sensor Network "*(IJCSIS) International Journal of Computer Science and Information Security*, Vol. 9, No. 5, May 2011.

[3] C. Bettstetter, H. Hartenstein, and X. P. Costa, "Stochastic properties of the random waypoint mobility model," *Wireless Netw., vol. 10, no.* 5, pp. 555–567, 2004.

[4] G. Cormode and S. Muthukrishnan, "An improved data stream summar the count-min sketch and its applications," *J. Algorithms, vol.*55, no. 1, pp. 56–75, 2005.

[5] M. Conti, R.Di Pietro, L. V. Mancini, andA.Mei, "Arandomized, efficient,and distributed protocol for the detection of node replication attacks in wireless sensor networks," in *Proc. ACMInt. Symp. Mobile Ad Hoc Networking and Computing (MobiHoc), Montreal, Canada, 2007*,pp. 80–89.

[6] M. Conti, R. D. Pietro, L. V. Mancini, and A. Mei, "Distributed detection of clone attacks in wireless sensor networks," *IEEE Trans. Depend. Secure Comput., vol. 8, no. 5, pp. 685–698, Sep./Oct. 2012.*

[7] 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.

[8] H. Choi, S. Zhu, and T. F. La Porta, "SET: Detecting node clones in sensor networks," in *Proc. Int. ICST Conf. Security and Privacy in Communication Networks (Securecomm), Nice, France,* 2007, pp.341–350.

[9] R. Groenevelt, P. Nain, and G. Koole, "The message delay inmobile ad hoc networks," *Performance Evaluation, vol. 62, no. 1, pp. 210–228,* 2005.

[10] Y.-C. Hu, A. Perrig, and D. Johnson, "Packet leashes: A defense against wormhole attacks in wireless networks," in *Proc. IEEE Int.Conf. Computer Communications (INFOCOM), 2003, pp. 1976–1986.*

[11] 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.*1773–1781.