International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682
Vol.2, No.10, October 2013 DOI:10.15693/ijaist/2013.v2i10.23-26

A Survey of Dynamic Detection of Node Replication Attack in Wireless Sensor Network

Dr.M.BalaGanesh[1]
Associate Professor /Department of CSE
Anna University, Chennai, India

S.NithyaDhevi[2]
PG Scholor /Department of CSE
Anna University, Chennai, India

[1] Asso. Professor, Dept of CSE/Sembodai Rukmani Varatharajan Engineering college
[2] PG Scholar of Sembodai Rukmani Varatharajan Engineering college

***Abstract* - A survey of MANET plays an major role in data communications. The node can be formed automatically without any centralised infrastructure, even though the nodes are formed automatically the replication of data to the node's are unavoidable. In single point attack that brings the whole network down and corrupted. An adversary can easily attack analyse the clone of unshielded sensor nodes and create replicas and insert them in the network. This gives the adversary to create on a large class of several insidious attack like disrupting communication, subverting, data aggregation, eavesdropping, deny of services, clone it etc..To overcome this situation in this paper present new protocols for securing and preventing algorithm for the replicated node and implement the distributed approach in dynamic nature.**

Index terms: EDD, CLONING ATTACK, LSM, XED

I.INTRODUCTION

Generally, wireless sensor node consists of millions of a small number of low cost node which may be in either static or dynamic in nature. In wireless sensor network inhibits in unsupervised fashion. This function indicates even if any node can be added or part of the node may be disappearing due to adversary, current network automatically continue their work in the network without any corruption.

In a mobile sensor networks, User can able to detect or find the node replication attack in the network environment. In existing systems, they use centralised approach i.e the centralised approach is one of the major defect because single point failure attack in the centralised network. From that effect, the whole sensor network would be corrupted. To overcome this situation in this paper use distributed approach, in dynamic nature is implemented. Generally, adversary creates one or more nodes similar to our original node for the purpose of injecting false data, reassemble the node id and its location for replication/cloning attack. From this scheme of false injected data, the node can easily communicate with other nodes for sharing the information in illegal manner. Time synchronisation is important inorder to provide sharing information service to another node in the network. To rectify the environment, implement two algorithms as XED and LED are proposed.

Node Replication attack

Now a days one of the challenging problem is node cloning attack. In node replication attack an adversary compromise and capture all other node in the neighbourhood region due to poor security imbalance. After that, adversary changes all its location, and their corresponding id's. Adversary may also introduce replicas of source node and employ arbitrary attack on the nodes to extract their information. Mostly, hackers deploy them in the network to launch a variety of inside attackers. By the way of proposal algorithm reduce percentage of node capturing.

Mostly replication attack deals with black hole attack, it intimate a wormhole attack and inject false data into the node. Once the node is captured by the attackers, it reprogram and replicate the node in large number of clones. Thus the cloned node attack the other node is referred as cloning attack. An adversary may replicate captured sensors and deploy them in the network to launch a tremendous amount of inside attackers.

In existing system mainly affects due to black hole attack, because black holes intrude the incoming or outgoing traffic is silently destroyed without any prior information from the source node. From the attack data may be corrupted or incomplete to reach the destination.

II.RELATED WORK

Generally, Sensor deployment in two ways using broadcasting devices such as Unmanned Aerial Vehicles(UAVs)[3].First, one is before sensor deployment (offline)and another one is after sensor deployment in the network(online). In before sensor deployment ,it split the sensing region into cells. Each cell claims its own location and capture forward and backward location. In lower communication cost,

RED protocol [4] adopt the concept of witness finding to analyse node capacity.

In the network ,two nodes are interacted in LSM[11] via double ruling. Memory usage of intermediate node in LSM is very large using bloom filter to reduce the usage of memory. Another technique in LSM in random walk technique is utilised. Unfortunately, from the above characteristic are used only for static sensor network, but proposed method exhibits the characteristic in dynamic manner, if nodes have mobility nature.

Yu.et.al [2] propose the dynamic pattern to detect the collision replicas. But in this,storage are linearly dependent on the network size and is not scalable. Based on the double ruling a suite of memory-efficient detection algorithms is introduced. The idea is to guarantee the intersection of traces in LSM that is double ruling and to reduce the memory usage of intermediate nodes in LSM via the Bloom filter. In addition, to better distribute the responsibility of witness node selection, the random walk technique is utilized in LSM.Some algorithms exploit other characteristics like social fingerprint, pre distributed keys,and random clustering to detection the replica.

Ho.et.al [10] propose a centralised detection algorithm using SPRT (Sequential Probability Ratio Test). Intuitvely, by having each node send the address and location of encountered or captured node, the base station can verify if there is a encountered node appearing in any different location with a velocity preceding. If such a node exists ,it is likely to be a said replicates. The major advantages of SPRT is to analyse the hypotheses value. If the hypotheses are set to NULL alternate hypothesis use “the node is not a replica” or replica node generates respectively.

Local information exchange algorithm is a general detection technique are proposed one node encounters the another node they exchange the information including ID, time, location, hash values and signature in assumption way .One way hash chain is used to preload the node.

In our existing system using two methods such as witness finding and another one is velocity finding. In velocity finding technique, a source node find its neighbourhood node nearer to the destination node. Then only source node enquiry about the destination if any replica attackers present inside. If the node may be replicated ,it do the following activities such as eavesdrop, reprogram it. From this witness finding technique ,energy and communication cost will be high due to occurrence of communication. Next, discuss about velocity finding, depends upon time synchronisation if the node replicated definitely it requires only amount of time.

2.1 Protocols used:

Moreover the protocols provide so many defection mechanisms. Thus far, protocols for finding the node replication attack in the wireless sensor network have relied on a trusted base station to provide local detection. In Centralised protocols have a single point failure; some of the local protocol never detects the replicated nodes in the distributed manner in distributed network. Our algorithm rectifies this defect and provides more effective and efficient in terms of the communication and storage overheads.

2.2 Analysis Result:

In existing system use stimulator to show the result. In below figure shows the exhausted node replication in different manner using existing protocols LSM and RED. The red circle indicates

Before Detection After Detection

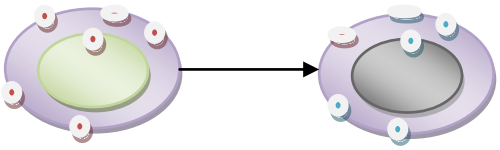

Figure 1.Clone Detection In Node Network

the cloned nodes in the network and the blue circles indicates free from replicated nodes by using existing algorithms and protocols like LSM,RED.

III PROPOSED SYSTEM

The contribution of our work is distributed in threefold. First, analyse the cloned node replicas in mobile sensor networks. Second, we show that the known solution describe for this problem without meet all user requirements. Third, we propose two localized algorithms, such as XED and EDD. These algorithm encounter challenge-and-response, encounter-number problem.

These problem are fundamentally different from the others. XED and EDD can resist node replication attacks in a localized and unsupervised fashion. Generally compared to our existing algorithm, which needs only that corresponding node perform the task without the guidance of base station. In our proposed system use the localized algorithm is a generalised type of distributed algorithm.

Each node in the localized algorithm can communicate with only its one-hop neighbours. This characteristic is helpful in reducing the communication overhead significantly and enhancing the resilience against node compromise. 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.

Proposed Methods:

1)XED (eXtermely Efficient Detection)

The idea behind XED is observed by two steps. First, one is offline step and other is online step.

Offline step: Initialise the blacklist B(u) is to be empty. Cryptographic function is denoted as h(.) . Let us consider two array such as $Lr^{(u)}$ and $Ls^{(u)}$ with size of the length n. Using these arrays to check the random numbers legimate are not.

Online step: In this step, u encounter the node v for the first time, u randomly generates and computes the cryptographic function. If it is first check, v is in the black list $B^{(u)}$.Then, we consider that node v is replicates. If not, proceed the following procedures.

i)Exchange the random numbers between the $Lr^{(v)}[u]$ and $Lr^{(u)}[v]$

ii)Verify the random number u sent to v last time. In this step unfortunately, replicas share the new version of random numbers with neighbouring nodes.

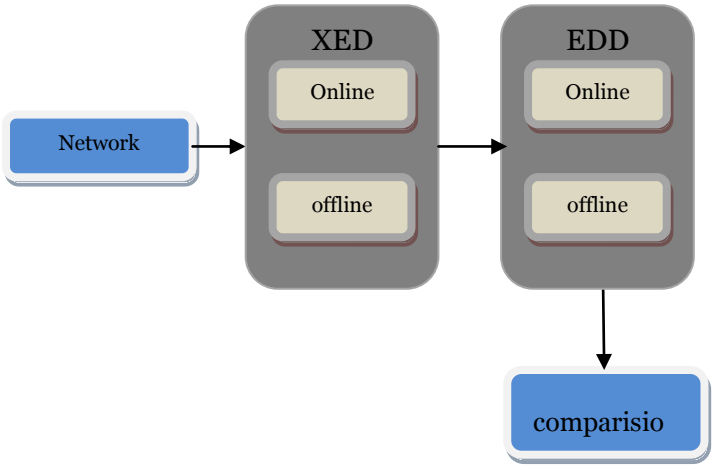

Figure.1 Block Diagram For Detection Algorithm

From these random numbers generate more random numbers for multiple nodes in the hostile environment. This problem is solved by using EDD algorithm in next section

2)EDD(Efficient Distributed Detection)

The idea behind EDD is observed by two steps. First, one is offline step and other is online step.

In offline step - Mainly performed in before sensor deployment .The goal of offline to calculate the parameter of each node, threshold, and length of the time interval. The calculating threshold is used for discrimination between the legimate node and the genuine node. In next step i.e is **online step** performed in after sensor deployment in each node at each move. Each node checks its own between its neighbouring node for its corresponding threshold .Finally analyse the number of encounters occur on each node.

IV PERFORMANCE EVALUATION

We discuss performance in this paper in five different manner:

- Detection Accuracy:
  In the detection algorithm, accuracy is used to represent using false positive rate and false negative rate. Falsely positive rate determines genuine node as a replica and falsely negative rate determines replica as a genuine node.
- Detection time:
  According to average time, how much required to compute the node detection in the network.
- Storage overhead:
  Generally record storage may be different depends upon its algorithm. Storage overhead in terms of the capacity of each node to store the record. Each record containing node ID, signature, and its location. Records are stored in terms of number of bits.
- Computation overhead:
  Each node requires minimum number of operation to be executed as per move.
- Conveyance overhead:
  Conveyance overhead detects number of records needs for each node to be transmitted. In case overhead measured in terms of bits But did not consider this bit value for further estimation.

V CONTRIBUTION

In Proposed system expose the following contribution in this paper related to node replica.

- *Localised Detection*:
  Without , the intervention of source station find the detection node in a random manner fashion.

- *Network Wide Revocation Avoidance:*
  Each node sent the revocation message to neighbourhood without disturbing the entire network.

- *Efficiency and effectiveness:*
  It provides detection accuracy and reduce the communication overhead.

- Time synchronisation:
  Each node does not consider about time synchronised.

VI CONCLUSION

In this paper, our proposed scheme is highly to detect find the node replication attack in the network in the way of dynamic manner and existing system provide more importance to static manner. To overcome the existing static manner in the way of using two exclusive algorithm are introduced for detection of node replication attack in the wireless sensor networks, XED and EDD are proposed. In XED, examines the randomised number in the node and EDD analyses the threshold and its parameter depend upon its location and avoid synchronisation in wireless sensor networks. Finally our methods are more effective and efficient in terms of malicious data replication attack ,communication overhead and traffic level data security.

VII REFERENCE

[1] 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.

[2] 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.

[3] 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.

[4]D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," Mobile Comput., pp. 153–181, 1996.

[5] T. Karagiannis, J. L. Boudec, and M. Vojnovic, "Power law and exponential decay of inter contact times between mobile devices," in Proc. ACM Int. Conf. Mobile Computing and Networking (MobiCom), Montreal, Canada, 2007, pp. 183–194.

[6] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: Analysis and defenses," in Proc. Int. Conf. Information Processing in Sensor Networks (IPSN), Berkeley, CA, USA, 2004, pp. 259–268.

[7] R. Sarkar, X. Zhu, and J. Gao, "Double rulings for information brokerage in sensor networks," *IEEE/ACM Trans. Netw.*, vol. 17, no. 6, pp. 1902–1915, Dec. 2009.

[8] K. Xing and X. Cheng, "From time domain to space domain: Detecting replica attacks in mobile ad hoc networks," in Proc. IEEE Int. Conf. Computer Communications (INFOCOM), SanDiego,CA, USA, 2010, pp. 1–9.

[9] K. Xing, F. Liu, X. Cheng, and D. Du, "Real time detection of clone attack in wireless sensor networks," in Proc. IEEE Int. Conf. Distributed Computing Systems (ICDCS), Beijing, China, 2008, pp. 3–10.

[10] C.-M. Yu, C.-S. Lu, and S.-Y. Kuo, "Efficient and distributed detection of node replication attacks in mobile sensor networks," in Proc. IEEE Vehicular Technology Conf. Fall (VTC-Fall), Anchorage, AK, USA, 2009, pp. 1–5.

[11] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," in Proc. IEEE Int. Conf. Computer Communications (INFOCOM), Hong Kong, China, 2004, pp. 2446–2457.

[12] 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

Mr.M.Balaganesh completed his Master Degree from Anna University, Chennai, India. Currently working Associate Professor in Sembodai Rukmani varatharajan Engineering college, Anna University Chennai, India.His research interest includes image processing,Network Security,Network Security and Networks and fuzzy logic.

S.Nithyadhevi received the **B.E.** degree in computer science engineering from the J.J College of Engineering, Trichy, Anna University, Chennai, India, in 2011.Currently doing **M.E.** in Computer Science Engineering in Sembodai Rukmani varatharajan Engineering college, Anna University chennai, India. Her research interest includes network security, forensic communication ,Neural Networks and fuzzy logic, and Data Mining.