International Journal of Computer Sciences
April'2017 Issue
ISSN Number: 4142 3453

A Novel Technique for Detecting Clone Nodes in Wireless Sensor Network

Yadala Mounika[1] , M.Malyadri[2]

[1]M.Tech (CSE),PG Scholar ,Department of Computer Science & Engineering, Rao & Naidu Engineering college, ongole,AP.

[2]Associate Professor , Department of Computer Science & Engineering, Rao & Naidu Engineering college, ongole,AP.

Abstract- Wireless Sensor Networks (WSNs) are often deployed in hostile environments where an adversary can physically capture some of the nodes, first can reprogram, and then, can replicate them in a large number of clones, easily taking control over the network. A wireless sensor network is a collection of nodes organized in to a cooperative network. This network is prone to various attacks due to poor security .A few distributed solutions to address this fundamental problem have been recently proposed.Wireless sensor networks are vulnerable to the node clone, and several distributed protocols have been proposed to detect this attack. However, they require too strong assumptions to be practical for large-scale, randomly deployed sensor networks. In this paper, we propose two novel node clone detection protocols with different tradeoffs on network conditions and performance. The first one is based on a distributed hash table (DHT), by which a fully decentralized, key-based caching and checking system is constructed to catch cloned nodes effectively. The protocol performance on efficient storage consumption and high security level is theoretically deducted through a probability model, and the resulting equations, with necessary adjustments for real application, are supported by the simulations. Although the DHT-based protocol incurs similar communication cost as previous approaches, it may be considered a little high for some scenarios. To address this concern, our second distributed detection protocol, Our second distributed detection protocol named randomly directed exploration, presents good communication performance for dense sensor networks by a probabilistic directed forwarding technique along with random initial direction and border determination. The simulation results uphold the protocol design and show its efficiency on communication overhead and satisfactory detection probability.

Keywords: Clone node, Distributed detection, Node replication, Wireless Sensor Network, Witness nodes

1. INTRODUCTION

Nowadays WSN are invaded in most of the areas of our daily life. Typically a WSN consist of large number of spatially distributed autonomous sensor node, with ability to sense environment, doing computation of sensed data and providing wireless communication. All the nodes in WSN collaborate to accomplish a common task, for example, earth sensing, military surveillance, health care monitoring . Here in this network sensor nodes collect data within their sensing environment and send this data to the sink node. These types of networks are generally heedless because sensor nodes are unattended and deployed in a hostile environment; hence there is a high chance of various attacks on sensor nodes. Normally WSNs are employed for some critical application, so one of the primary concerns of this type of system should be considered as its security. Generally sensor nodes are not equipped with any tamper resistant hardware. So it is easy for an attacker to capture and compromise a sensor node. In node clone attack an attacker captures a sensor node; retrieve the information about the node and produces copies of the captured node. And also all the cloned node will be having the same ID of the captured node. Clone nodes are treated as statutory nodes and hence it will be difficult to detect them. Once the clone nodes acquire the trust of other sensor nodes, they can perform various attacks on these sensor networks. For example they may provide false sensor reading, drop packet while communication, spy for confidential information and leak it to an adversary. In order to overcome these difficulties it could be efficient to identify the replicas in a static WSN In node clone attack also called as node replication attack, an attacker will physically capture a node from its deployed location. Then the attacker will access the it's memory, communication and processing unit of the captured node, and they also steals the relevant information including its secret key, identity and intrusion detection characteristics. After that by using the stolen information attacker will generate a number of clones having the same ID of the captured nodes, and deploy them back into the network. These clones operate under the control of the attacker. Also clones will then try to behave like a legitimate node, and participate in the process of communication using the stolen keying materials. The aim of an attacker in node clone attack is to control the network activities by using clones. With the help of clones, an attacker can launch a variety of insider attacks likes selective forwarding, wormhole, hello flooding and false data injection. An attacker can perform all of the above mentioned attacks only by compromising a single node from the network. Therefore, node clone attack is considered as one of the most serious threats in WSN. After creating replicas it is a great challenge to differentiate between the statutory node and its clones. Since, clones execute the same network protocols and they use the same keying materials as that of a original node, they pass in all authentication and verification process during transmission [8]. Most of the schemes discussing in the literature recommends for the identification of existence of clones in the network. These schemes mostly use the parameters such as unique set of neighboring nodes, position etc., to differentiate a clone from its original node.

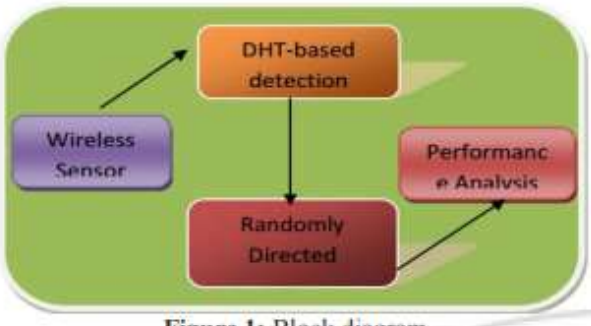

Figure 1: Block diagram

II. LITERATURER SURVEY

Approaches for detecting clone node in static WSNs are broadly categorized into centralized and distributed techniques [7]. In Centralized scheme [1] each node sends a list of its neighbors and their location claim to the base station, and the base station checks whether there exist same node ID with different location information. If such nodes exist, it could be revoked from the network by flooding an authenticated revocation message. In distributed method [1] one or more nodes are responsible for to identify the replica. These nodes are called witness node. When a new node joins in the network its ID and location information is send to witness node, and witness node check for clones. Preliminary approaches to detect clone node in distributed environment are, Node to Network broadcasting (N2NB) [1] and Deterministic multicast (DM) [1]. In Node ToNetwork Broadcasting every node in the network uses an authenticated broadcast message to flood the network with its location information. Each node stores the location information for its neighbors. If it receives a conflicting claim, it revokes the offending node. In this method the total communication cost for each node should be very high. In Deterministic multicast a nodes location claim is shared with a limited subset of deterministically [1] chosen witness nodes. Since deterministic, the attacker can also determine the witness nodes. Also it cannot afford a large number of witness nodes. Other distributed detection techniques are,

Randomized multicast (RM) In Randomized multicast [1] each of the node's neighbors probabilistically forwards the location claim to a randomly selected set of witness nodes. If any witness node receives two different location claims for the same node ID, it can revoke the replicated node. The birthday paradox[9] ensures that two conflicting claims have a high probability of sharing a common witness node. Its drawbacks are higher communication cost and lower detection probability. Randomized multicast improves the resiliency of the deterministic multicast by randomizing the witnesses for a given node, so that the adversary cannot anticipate their identities.

Line Selected Multicast (LSM)

Line Selected Multicast uses the routing topologies to detect and to identify the clones in sensor network. It is an improved version of RM. In addition to the witness nodes of RM, LSM checks all the intermediate node within the path for clone nodes. Here all intermediate nodes from a node to a destination node will also store location claims as a line. When location claim is transferred, any node on the path verifies the signature of the claim and checks for the conflict, by using the location information stored in its buffer. If there is a conflict, it revokes offending node from the network. Otherwise store the claim and forwards to next node. Here a node on the line-crossing point will detect a conflict, if conflicting location claim line crosses the node. So LSM has lower communication cost and better detection level as compared to Randomized Multicast.

Memory Efficient multicast using Bloom filters and cell forwarding (BC-MEM) Memory Efficient Multicast using Bloom filters and cell forwarding (BC-MEM) [2] is introduced to overcome the memory overhead problem occurred in LSM. In this protocol, the deployment area is divided into virtual cells. In each cell, an anchor point is assigned for every node in the network. The node close to the anchor point is called anchor node. The location claim is forwarded to the anchor point of the next cell where the line segment interacts. The claim is then forwarded from one anchor node to another until it reaches at the last cell. The anchor nodes in the intermediate cells are watchers and the anchor nodes in the first and last cells are witnesses. Here the location claim is only transmitted through the watcher nodes, and the witness nodes store the claim message. Watcher node uses bloom filter [2] for storing claim message in memory, so it takes lesser memory than LSM. This protocol also avoids the cross over problem [1] in LSM.

Localized Multicast There are two variants of localized multicast [3] are introduced: Single Deterministic Cell (SDC) [3] and Parallel Multiple Probabilistic Cells (P-MPC) [3]. In these two protocols witness nodes are selected from a geographically limited region of node, called cell. By using a deterministic function each node ID should be mapped to one or more cells. To increase the resilience and security of the scheme randomization is using within the cells. In SDC, each cell is mapped into a single destination cell by using a geographical hash function. Each node in the destination cell independently decides whether to store the claim. On reception of different location claims with the same ID, destination cell can detect the presence of clones. In the P-MPC scheme, the location claim is mapped and forwarded to multiple deterministic Cells with various probabilities [3]

III. EXISTING SYSTEM

In this section introducing a cost effective method for detecting clone nodes in wireless sensor network (CEMDCN) by combining merits of RDB-R [6] and the RED [5] protocol. So in the proposed method which uses neighboring information of node to find out the replica, i.e. when a node is replicated, the original node and replicated node has different set of neighbors. Neighboring node IDs are presented with a constant size using a Bloom filter. The Bloom filter output (BFO) is used as a proof of identification. Here the witness nodes are selected pseudo-randomly by using a pseudo-rand() function. Pseudo-rand function select same set of witness node in one run of the protocol, and it takes different set of witness in different run of the protocol. So it highly improves the detection level of this protocol.

IV. PROPOSED WORK

Wireless sensor networks (WSNs) have gained a great deal of attention in the past decade due to their wide range of application areas and formidable design challenges. In general, wireless sensor networks consist of hundreds and thousands oflow-cost, resource-constrained, distributed sensors nodes, which usually scatter in the surveillance area randomly, working without attendance. If the operation environment is hostile, security mechanisms against adversaries should be taken into consideration. Among many

physical attacks to sensor networks, the node clone is a serious and dangerous one. Because of production expense limitation, sensor nodes are generally short of tamper - resistance hardware components; thus, an adversary can capture a few nodes, extract code and all secret credentials, and use those materials to clone many nodes out of off-the-shelf sensor hardware. Those cloned nodes that seem legitimate can freely join the sensor network and then significantly enlarge the adversary's capacities to manipulate the network maliciously.

.

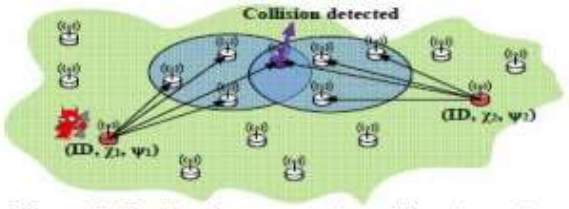

Figure 2: Graphical representation of the witness-based clone detection methods: a captured node and its clone

V METHODOLOGY

We consider a WSN consisting of N wireless sensors, randomly deployed over a monitoring area. All sensors are assumed to be limited in communication and computation power as well as in battery life. On average, every sensor is able to directly communicate with d other sensors, referred to as neighbors. Prior to deployment, every sensor is assigned a key pair (PK, SK). The key PK represents the node's public key. It is known to all the other network nodes and it is used as the node's unique identifier (ID). The key SK represents the node's secret key. We assume every sensor is able to determine its position using secure localization mechanisms
[9].

a) Adversarial Model We consider a time-persistent adversary, e.g., an adversary who operates over an extended period of time. The adversary compromises a set of network nodes and extracts their information, such as sensed data, the states of the network protocols and the assigned cryptographic secrets. Using the extracted data, the adversary then fabricates exact functional copies of captured nodes (clones) and deploys the clones back into the network. Every captured node is assumed to be cloned at least once.

b) Detection of Clone Attacks For sensor u, its fingerprint is computed from the code words collected from its neighborhood N(u). As stated in Section 3, sensors are stationary after deployment. A legitimate sensor u belongs to a "fixed" neighborhood, whose social characteristics can be encoded into u's fingerprint. Therefore, each sensor is required to "sign" with its fingerprint FPu whenever it generates a new message to send to the base station. The message transmission should be in the following format2: u → BS : {IDu, FPu, content} Assume X is the superimposed s-disjunction code to generated the social codeword for each sensor, which can be represented by an M × N matrix. According to Algorithm 1, the length of a fingerprint is log2(M). Even with M = 100, 000, a fingerprint takes no more than 2 bytes to be included in a message. Hence, our detection algorithm imposes a very slight message overhead for protecting a sensor network against clone attacks. In our consideration, a cloned sensor may use an arbitrary fingerprint (e.g. the fingerprint of the original sensor), or compute a new fingerprint that is consistent with its new residency. Hence, detecting clone attacks should be conducted in two aspects:

VI. RESULT AND DISCUSSIONS

The problems associated with the dht are it incurs more communication cost because of the chord overlay network and thus it is sensitive to energy and storage consumption. To overcome these problems a new node clone detection protocol introduced namely randomly directed exploration. Here the each node only needs to know and buffer a neighbor list having all neighbors ID and locations. During detection round each node constructs claiming message with signed version of neighbor list and then deliver message to others which will compares with its own neighbor list to detect node clone. If there exists any node clone, one witness node successfully catches the clone and notifies the entire network by broadcasting. The efficient way to achieve randomly directed exploration needs some mechanisms and routing protocols. First the claiming message needs to provide maximum hop limit and it is sent to random neighbors. Then the further message transmission will maintain a line and this transmission line property enables a message to go through a network as fast as possible[6]. The communication cost of this protocol is low and it is limited by the border determination mechanism. And the assumption made here is that each node knows about its neighbors location.

Detection round: Initially the node clone detection round is activated by the initiator. At the right mentioned action time, each node creates its own neighbor list (ID of neighbor and location). Then that node act as an observer for all its neighbors and starts to generate claiming messages. The claiming message involves node ID, location and its neighbor list[6].

Algorithm 1:

rde-processmessage Mα:

An intermediate node processes a message

1: verify the signature of Mα

2: compare its own neighbor-list with the neighbor-list in Mα 3: if found clone then 4: broadcast the evidence;

5: ttl<=ttl-1

6: if ttl ≤ 0 then

7: discard Mα

8: else

9: next node<=get next node (Mα) {See Algorithm 4}

10: if next node =NIL then

11: discard Mα

12: else

13: forward Mα to next node[6]

The intermediated nodes will change the value of ttl during transmission. In each time, the node transmits message to a random neighbor. When an intermediate node β receives a claiming message Mα, it launches rde-process message Mα. During the processing the node clone is detected by comparing the neighbor list of node which acts as inspector β with neighbor list in the message. If clone detected then the witness node β will broadcast an evidence message M evidence= (Mα,Mβ) to notify the whole network such that the cloned nodes are removed from the network[6]. Node decreases the message's ttl by 1 and discards the message if ttl reaches zero during routing; otherwise it will query Algorithm 4 to determine the next node receiving the message.

Algorithm 2:

get next node (Mα):

To determine the next node that receives the message

1: determine ideal angle, target zone, and priority zone

2: if no neighbors within the target zone then

3: return NIL 4: if no neighbors within the priority zone then 5: next node<= the node closest to ideal angle

6: else

7: next node<= a probabilistic node in the priority zone, with respect to its probability proportional to angle distance from priority zone border

8: return next node[6].

A. Deterministic directed transmission: The ideal direction can be calculated when node receives a claiming message from previous node and the next destination node should be closest to the ideal direction for the best effect of line transmission. Network border determination: The communication cost is reduced by taking network shape into consideration. Due to physical constrains in many sensor network applications, there exist outside borders. The claiming message can be directly discarded when reaching some border in the network. To determine a target zone then no neighbor is found in this zone, target range is used along with ideal direction, the current node will conclude that the message has reached a border, and thus throw it away. B. Probabilistic directed transmission: priority range along with the ideal direction is used to specify a priority zone, in which the next node will be selected. The deterministic directed candidate within the target zone will be selected as the next node when no nodes are located in that zone,. If there are several nodes in the priority zone, their selection probabilities are proportional to their angle distances to priority zone border. As a result, to reduce detection probability dramatically the adversary may remove some nodes in strategic locations Claiming messages transmissions from a cloned node's neighbors are highly correlated, which affects the protocol communication and

V.CONCLUSION

Wireless sensor network is an emerging area which has wide applications. Hence the security in wireless sensor network is of great concern. Node replication attacks are an important attack against a wireless sensor network in which an adversary compromises a sensor node and creates copies of that node and deploying it in strategic areas. Various methods have been developed in order to detect the node replication attacks. Low priced and energy efficient detection of node replica in WSN introduced RDB-R detection scheme and it is a low cost and efficient solution of replica detection in wireless sensor network. But RDB-R protocol has problems in terms of its memory overhead and detection level. To overcome these difficulties a CEMDCN protocol is introduced. Implementation result shows that the proposed method reduces the memory and communication overhead and also improves the detection level of RDB-R detection scheme. And this protocol is best suited for resource constraint sensor application. Because it uses neighbouring information instead of location information for detecting replica, so it avoids use of GPS and reduce sensor node cost. So this scheme is a cost effective mechanism for detecting clone nodes in wireless sensor network.

REFERENCE

[1] Bryan Parno, Adrian Perrig, Virgil Gligor ,"Distributed detection of node replication attacks in sensor networks" in Proceeding of the IEEE Symposium on Security and Privacy,(IEEE S and P`05),pp49-63, May 2005.

[2] Ming Zhang, Vishal Khanapure, Shigang Chen, Xuelian Xiao, "Memory efficient protocols for detecting node replication attacks in wireless sensor networks", in Proceedings of the 17th IEEE International Conference on Network Protocols (ICNP'09), pp 284-293, Princeton, NJ,USA, October 2009.

[3] Bio Zhu, Sanjeev Setia, Sushil Jajodia, Sankar das Roy and Lingyu Wang, "Localized multicast: efficient and distributed replica detection in large scale sensor networks", IEEE Transactions on Mobile Computing, Vo1. 9, No. 7, pp 913-926, 2010.

[4] Yingpei Zeng, Jiannong Cao, Shigeng Zhang,Shanqing Gao and Li Xie ,Random walk based approach to detect clone attacks in wireless sensor networks, IEEE Journal on selected areas in Communications, Vol. 28, No.5, pp 677-691, 2010.

[5] M. Conti, R. Di Pietro, L. Mancini, and A. Mei, A Distributed detection of clone attacks in wireless sensor networks, IEEE Transactions on Dependable and Secure Computing, vol. 8, no. 5, pp. 685698, 2011.

[6] Kwantae Cho, Byung-Gil Lee, and Dong Hoon Lee, "Low Priced and Energy Efficient Detection of Replicas for Wireless Sensor Networks", IEEE Transactions on dependable and secure computing, Vol. 11, NO. 5, September/October 2014.

[7] S. S. Koshy and M. Sajitha, "Zone based node replica detection in wireless sensor network using trust", International Journal of Computer Trends and Technology, vol. 4, no. 7, pp. 2316-2320, 2013

[8] Wazir Zada Khan, Mohammed Y. Aalsalem, Mohammed

Naufal Bin Mohammed Saad, and Yang Xiang, "Detection and Mitigation of Node Replication Attacks in Wireless Sensor Networks: A Survey", International Journal of Distributed Sensor Networks, March 2013.

[9] https://en.wikipedia.org/wiki/Birthday_problem

[10] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in Proc. IEEE Symp. Security Privacy, 2005, pp. 49–63.

[11] H. Balakrishnan, M. F. Kaashoek, D. Karger, R. Morris, and I. Stoica, "Looking up data in P2P systems," Commun. ACM, vol. 46, no. 2, pp. 43–48, 2003.

[12] Y. Zhang,W. Liu,W. Lou, andY. Fang, "Locationbased compromise tolerant security mechanisms for wireless sensor networks," IEEE J. Sel. Areas Commun., vol. 24, no. 2, pp. 247–260, Feb. 2006.

[13] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient security mechanisms for large-scale distributed sensor networks," in Proc. 10th ACM CCS, Washington, DC, 2003, pp. 62–72.

[14] R. Anderson, H. Chan, and A. Perrig, "Key infection: Smart trust for smart dust," in Proc. 12th IEEE ICNP, 2004, pp. 206–215.

[15] M. Conti, R. D. 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. 8thACMMobiHoc,Montreal, QC, Canada, 2007, pp. 80–89.

[16] B. Zhu, V. G. K. Addada, S. Setia, S. Jajodia, and S. Roy, "Efficient distributed detection of node replication attacks in sensor networks," in Proc. 23rd ACSAC, 2007, pp. 257–267.

[17] H. Choi, S. Zhu, and T. F. La Porta, "SET: Detecting node clones in sensor networks," in Proc. 3rd SecureComm, 2007, pp. 341–350.

[18] 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.s, Man, Cybern. C, Appl. Rev., vol. 37, no. 6, pp. 1246–1258, Nov. 2007.

[19] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in Proc. 9th ACM Conf. Comput. Commun. Security, Washington, DC, 2002, pp. 41–47.

[20] A. Shamir, "Identity-based cryptosystems and signature schemes," in Proc. CRYPTO, 1984, LNCS 196, pp. 47–53. [21] R. Poovendran, C. Wang, and S. Roy, Secure Localization and Time Synchronization for Wireless Sensor and Ad Hoc Networks. New York: SpringerVerlag, 2007. [22] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Commun. Mag., vol. 40, no. 8, pp. 102–114, Aug. 2002.

[23] S. Ratnasamy, P. Francis, M. Handley, R. Karp, and S. Schenker, "A scalable content-addressable network," in Proc. SIGCOMM, San Diego, CA, 2001, pp. 161– 172.

[24] I. Stoica, R.Morris, D. Liben-Nowell, D. R. Karger,M. F.Kaashoek, F. Dabek, and H. Balakrishnan, "Chord: A scalable peer-to-peer lookup protocol for internet applications," IEEE/ACM Trans. Netw., vol. 11, no. 1, pp. 17–32, Feb. 2003.

[25] A. I. T. Rowstron and P. Druschel, "Pastry: Scalable, decentralized object location, and routing for largescale peer-to-peer systems," in Proc. IFIP/ACM Int. Conf. Distrib. Syst. Platforms Heidelberg, 2001, pp. 329–350.

[26] A. Varga and R. Hornig, "An overview of the OMNeT++ simulation environment," in Proc. 1st Int. Conf. Simulation Tools Tech. Commun., Netw. Syst. Workshops, Marseille, France, 2008, pp. 1–10.

[27] A. Awad, C. Sommer, R. German, and F. Dressler, "Virtual cord protocol (VCP): A flexible DHT-like routing service for sensor networks," in Proc. 5th IEEE MASS, 2008, pp. 133–142. [19] R. Diestel, Graph Theory, 3rd ed. New York: Springer, 2006.

[28] H. Chan and A. Perrig, "Security and privacy in sensor networks," Computer, vol. 36, no. 10, pp. 103–105, 2003. [29] X. Wu, G. Chen, and S. K. Das, "On the energy hole problem of nonuniform node distribution in wireless sensor networks," in the Proc. of IEEE International Conference on Mobile Adhoc and Sensor Systems, 2006, pp180–187.