EFFICIENT DISTRIBUTED DETECTION OF NODE REPLICATION ATTACKS IN MOBILE SENSOR NETWORKS

Balaji.N[1], Anitha.M[2]

[1]*Department of Computer & Communication Engineering M.A.M College of Engineering, Tamilnadu, India*
[2]*Department of Information &Technology Engineering M.A.M College of Engineering, Tamilnadu, India*

Abstract

Wireless Sensor Network (WSN) technology uses many nodes in a network for transformation of data. Detecting and monitor of the node is very difficult in distributed network and form a node replication attacks in a mobile sensor network .To detect the node replication attacks in mobile sensor networks using two localized algorithms, XED and EDD. Our proposed algorithm can resist node replication attacks in a localized fashion. Note that, the Nodes only need to do a distributed algorithm, task without the intervention of the base station. The techniques developed in our solutions are to challenge and response and encounter number, are fundamentally different from the others. Moreover, while most of the existing schemes in static networks rely on the witness finding strategy is cannot be applied to mobile sensor networks, the velocity exceeding strategy used in existing schemes in mobile networks incurs efficiency and more no security problems. Therefore, based on our node replication challenge and response to encounter number approaches in localized algorithms are proposed to resist node replication attacks in mobile sensor networks. The advantage of our proposed algorithm include 1) Localized detection; 2) Efficiency and effectiveness; 3) Network-wide synchronization avoidance; 4) Network-wide revocation avoidance Performance comparisons with known methods are provided to demonstrate the efficiency of our proposed algorithms.

Keywords: *Mobile Sensor Network, Attack, node replication attack, static and mobile WSN.*

----------***----------

1. INTRODUCTION

Recent researches Wireless communication and portable computers with two or more mobile nodes already issued a temporary network without the use of network infrastructure or centralized management of the sensor mobile network you can create . That led to a new concept [1]. Source and destination mobile node to communicate with each other, if not within the scope of the data packets to the mobile parts [2], which is between the relaying transmissions through other mobile hosts in the mobile host is not allowed to do. Here, in no special infrastructure such as military and rescue affairs in various fields, many applications developed for mobile networks are expected to be required. A sensor node, the node captured from the same identity (ID) number of copies of the lead, and malicious activities, and strategic levels of the network makes the replicas. This is a so -called node replication attacks. Each node in a sensor network is free to move freely in any direction. Cellular system is rather a master -slave relationship.

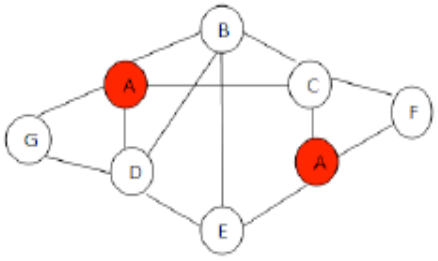

Fig.1 Node Replication Attack

This temporary access to data networks is less than that of conventional fixed networks. Hope is not a viable solution for the owner of the original data, the data items that went into the mobile area. A voting mechanism, using neighbors ' can reach consensus on a legal point [3].Unfortunately, when you reach a distributed fashion innovation, disjoint parts distribution network response time to discover the identity of the node .At least when nodes to replicate two hops from each other, the local approach can detect the replicated node in a network. When reproducing at least two hops away from each other at the ends, you can find a local approach with the tip of a network.

1.1Wormhole Attack

In wormhole attack, a malicious node adversary receives packets at one location in the network and tunnels them to another location in the network, then that packets are resent into the network, this tunnel between two colluding attackers is called wormhole.

1.2 Black Hole Attack

This attack will flood of demand -based protocol to say it all. In this attack, the attack will create a very narrow path in response to a node receives a route request. The real answer is that a malicious node will start from the front edge of the answer, and then created a false path. [5] Malicious communication between nodes can be added to the device itself, it is the ability to move between them for misbehavior. Interfere will carry the node with proper operation of the network routing protocol and the number of attacks mounted.

1.3 Routing Table Overflow

In the case of overflow routing table, routing table overflow, the causes are not nodes. Novel routes to avoid the creation or implementation of the protocol were enough to overwhelm the need to create routes. Proactive routing algorithms, routing information before it needs to be found. It only needs to find a way to process the reaction becomes mandatory. Toxic poisoning routing node

1.4 Node Routing Poisoning

The node routing network nodes compromised. Other authorized end up sending the actual routing of packets to send updates or updates of any change [6]. Routing table poisoning will provided caused by sub-optimal routing. Traffic congestion in the network [7], or access the network set up in a few areas. This invention uses the pseudo- demand routing the attack can launch the attack. So before the request packet is received by the legal way to receive and reject those packets that the nodes

1.5Rushing Attack

On-demand routing protocol which use duplicate during the route innovation process are vulnerable to this attack. An attacker which receives a route request packet from the initiate node flood the packet rapidly throughput the network before further nodes which also receive the same route request packet can respond. Nodes that receive the lawful route request packet previously received through the attacker and hence discard those packets.

1.6 Identification of Problem

Sensor networks, which are composed of a number of sensor nodes with limited resources, have been demonstrated to be useful in applications, such as environment monitoring [8] and object tracking [9]. As sensor networks could be deployed in a hostile region to perform critical missions, the sensor networks are unattended and the sensor nodes normally are not equipped with tamper-resistant hardware [7]. This allows a situation where the adversary can compromise one sensor node, fabricate many replicas having the same identity (ID) from the captured node, and place these replicas back into strategic positions in the network for further malicious activities. This is also-called node replication attack. Since the credentials of replicas are all clones of the captured nodes, the replicas can be considered as legitimate members of the network, making detection difficult. From the security point of view, the node replication attack is extremely harmful to networks because replicas, having keys, can easily launch insider attacks, without easily being detected.

2. RELATED WORKS

The first detection of node replication attacks solutions relies on a centralized base station WORKS. In this solution, each node is a base station (BS), its neighbors and sends a list of suggested places [3] .the “Close" to each other, the two lists are sent to the nodes that do not result in the entry clone detection. Then, BS becomes clones. This solution has several drawbacks in the presence of a single point of failure BS, and communication costs are high due to the large number of messages. Also, BS so close to the edges of their operational life is shorter than the other nodes to route messages. Finding other solutions remains local. For example, a voting mechanism for a particular node [10] is used in a near -term adoption. These kinds of node will the same location, the false detection problem, if you cannot find. Node replication attacks described finding the solution to a naive point of distribution network broadcast. . The solution for the network was flooded by comparing the location information. Each node in a network containing information about the location neighbor found a tip of the nozzle is in a position corresponding to the position that enjoys a location claim; this will result in clone detection. The WSN nodes and the number of iteration, the N flooded However, this process is very energy consuming. Sybil attack, a node will be deleted from the ends of a number of stolen identities says. Identity theft is on the chip and clone attacks that are based on the reference; however, angles two attacks [11] are available. They are effectively addressed RSSI or authentication mechanism based on a fixed key knowledge. They are efficiently addressed mechanism for RSSI or with authentication Based on the knowledge of a fixed key set for efficient detection of clone attacks is actually an open issue.

To the best of our knowledge the first non naïve, globally-aware and distributed node-replication detection solution was recently proposed [12]. In particular, two distributed detection protocols with emergent properties were proposed. The first one, the Randomized Multicast (RM) [13], distributes node location information to randomly-selected nodes. The second one, the Line-Selected Multicast (LSM), uses the routing topology of the network to detect replication. In the RM, when

a node broadcasts its location, each of its neighbours sends a digitally signed copy of the location claim to a set of randomly selected nodes. Assuming there is a replicated node, if every neighbour randomly selects O (√n) destinations, then exploiting the birthday paradox. There is a non negligible probability at least one node will receive a pair of non coherent location claims. The node that detects the existence of another node in two different locations within the same time-frame will be called witness.

The RM protocol implies high communication costs: Each neighbour has to send O (√n) messages. To solve this problem the authors propose using the LSM protocol [14]. The LSM protocol behaviour is similar to that of RM but introduces a minor modification that implies a noticeable improvement in terms of detection probability. Node replication is eventually detected by the node (called witness) on the intersection of two paths that originate from different network positions by the same node ID [15], [16], In fact, during a check the same node y0 is present with two non-coherent locations; the Witness will trigger a revocation protocol for node y0.

3. PROPOSED SYSTEM

To detect the replicas node in mobile sensor networks using two algorithms, XED and EDD, are proposed. The proposed techniques developed a solutions for a replica attack, challenge-and-response and encounter-number, are fundamentally different from the others. The proposed algorithm can resist node replication attacks in a localized fashion. Compared to the distributed algorithm, nodes perform the task without the intervention of the base station. The localized algorithm is a particular type of distributed algorithm. 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 algorithm can identify replicas with high detection accuracy. 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.

3.1 Target Localization Problem

Such as environmental monitoring and multi- sensor target tracking sensor network applications, plays a key role. Wireless sensor networks based on techniques developed in places like the tip of a sensor based on the location information in routing decisions need to shout . Beacon nodes to use some special nodes to be considered in their own places of ethics / prediction methods, innovation, and more than location. These algorithms work in two steps. The first step: Non lighthouse beacon nodes to nodes that receive messages from the radio signals. The message includes a reference to the location of the beacon node. Second Step will provide non lighthouse beacon and non- beacon nodes, for example, the distance between the nodes, perform some specific measurements. And the arrival time difference between the received signal strength measurements in terms of the messages. Without protection, an attacker can easily spoil and normal operation of the sensor nodes for location estimation of sensor networks to be carried out. In different places, running in the wrong place can offer tips to prevent an attack beacon packets. Also, an attacker manipulating and lying about the location of a lighthouse or beacon signals may be compromised to distribute malicious location references. Beacon signals. In one case, the non- beacon nodes to determine their locations wrong. From the point of view of security and connection dimensions of the problem has been studied intensely in recent years. The most common problem with a sensor area of security issues in the sensitive area of a circular disk model assumes that it is cantered. At one point he is said to be in the sensing area.

4. DETECTON TECHNIQUE OVER MOBILE SENSOR NETWORK

In this paper, a defense mechanism against replication attacks is proposed in mobile sensor networks .In this technique; multiple paths are established between source and destination for data transmission using XED and EDD for optimization. In the elected routes, the nodes with highest trust value, residual bandwidth and residual energy are elected as active nodes by using ant agents. Every active node monitors its neighbor nodes within its transmission region and collects the trust of all monitored node. The active nodes adaptively change as per the trust thresholds.

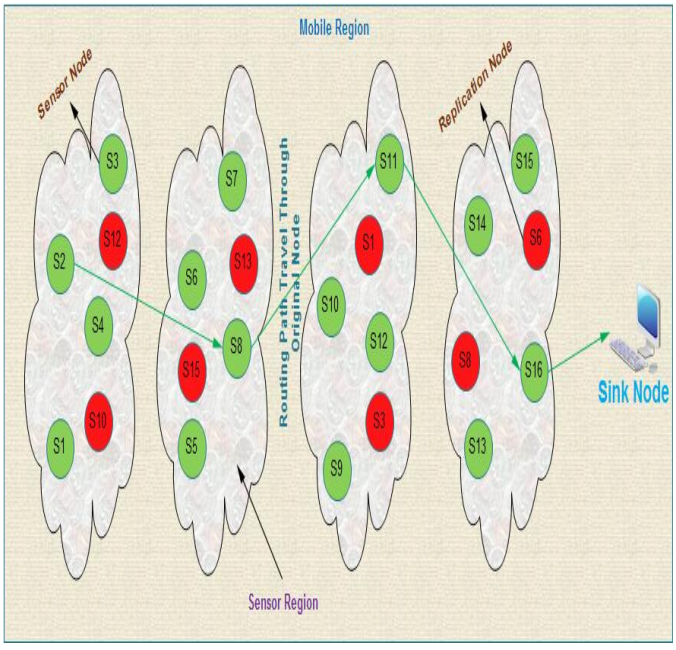

Fig.2 Architecture of mobile sensor network

4.1 Detection System

In this paper detection -based security scheme provided for mobile sensor network. Although mobile sensor network is less computation and communication skills, as they continue to permit the detection of anomalies in network nodes with specific characteristics of the neighborhood information. We show that the properties as key enablers to be used in large-scale sensor networks security. In many attacks against mobile sensor networks, initially as a legitimate node within the network it has to do with the attack. Near the edges of a simple dynamic statistical model of the received packet power levels and lower risk by monitoring the arrival of a sensor capable of detecting intruder detection built in conjunction with the protocol to create nose in the networking nodes. We show that such characteristics can be exploited as key enablers for given that the security to large scale sensor networks. In many attacks against Mobile sensor networks, initially attacker is to make itself as a legitimate node within the network. To create a sensor nose capable of detecting an intruder a simple dynamic statistical model of the adjacent nodes is built in conjunction with a low complication detection algorithm by monitoring received packet power levels and arrival rates

4.2 Node Deployment

Each node requests our node deployment to the base station at the time of deployment. After requesting, Node details are verified and save accordingly. Details include Node-Id, IP-Address and Port Number. Base station captures the node position and also save the node current position. Base station updates node position as per the node movement. Base station monitors the entire network and updates its position as per the movement.

4.3Execute Offline Step

In this module execute our proposed algorithm's Offline steps. Our algorithm generates the secret key and saves accordingly. The current node maintains other node's given secret key at the time of meet past interaction. Current node maintains the block list also. The block list consist of replicated node details are stored.

4.4 Find Next Hop and Candidate Hop

Based on sensor node's geographic position and source node's (Main system) geographic position prepare the neighbor list to avoid opposite direction nodes. Neighbor list consist of current coverage's all the node. Prepare next hop and candidate list based on the neighbor list. Next hop is selected from neighbor list based on the source node nearby hop balanced node is add candidate list. The candidate list is used when current next hop is any problem (For example at the time of replication detection next hop is any problem furthermore candidate list is considerable.) the next priority is given to candidate hop. If more than one candidate is available the higher priority is goes to nearby source node position.

4.5 Localized Detection

After getting next hop name, execute our proposed algorithm's online steps. In that algorithm first check next hop is source node or not, if yes object will directly forward to source node. Otherwise check current node meet already the next hop or not, if yes request the secret key given during previous interaction. Current hop check the received secret key is matching to previously given. If yes, then current node made communication to next hop and replace the existing secret key in next hop otherwise it is replicated node. The current next hop name is added to the current sensor nodes block list.

4.6 Eliminate Replicated Hop

In localized detection find any replicated node to eliminate current hop and select another next hop from candidate list. Again execute our proposed algorithm. This process is made up to get original hop

5. PERFORMANCE METRICS

The performance is evaluated according to the following metrics for node reapplication attack in mobile sensor network. This can evaluate a dictions performance in easy manner

Table1: Detection Mechanisms for performance overheads

Schemes	Communication cost	Memory
Deterministic Multicast	O(g ln g√n / d)	O(g)
Randomized Multicast	O(n2)	O(√n)
Line-Selected Multicast (LSM)	O(n√n)	O(√n)
RED	O($r\sqrt{n}$)	O(r)
XED	O(1)	
EDD & SDD	O(1) /O(n)	O(n) /O(ξ)
Node –to – Network (Broadcast),	O(n2)	O(d)
Where, n – No. of nodes in the network d – Degree of neigh boring nodes g - no. of witness nodes ξ– Distinct IDs from set of nodes as monitor set r- Communication radius		

6. MATHEMATICAL MODEL

Step 1*:* Let us consider in WSN with node, witness node set &neighbour.
Where,
x = Number of nodes in the network
p = probability a neighbour replicates location information
z = Number of witness nodes
Step2: Probability of selected witness node is

(1-z) (1)

Step3: The attack is detected is equal to the probability that at least one neighbour of each clone sends the claim to the same witnesses.

(1-(1-z) ^x)^2 (2)

Step4: The evaluation of protocol is done based on energy consumption, memory overhead, detection probability by using below equation

(O (p .z .x) (3)

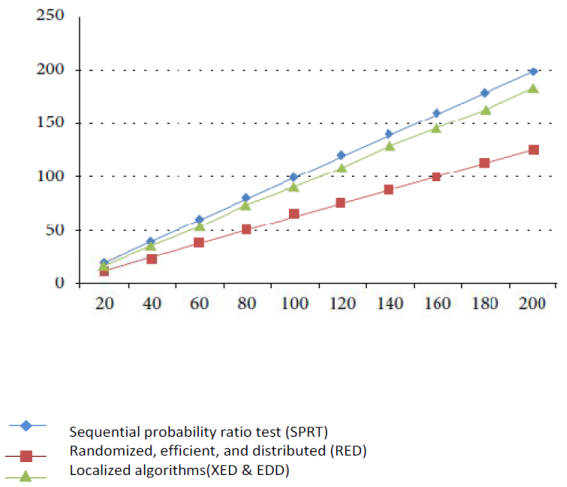

Chart -1. Comparison of protocols

7. CONCLUSIONS

The 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, but also possesses unique characteristics, including network-wide time synchronization avoidance and network-wide revocation avoidance, in the detection of node replication attacks. This method improves the security aspect of wireless sensor networks mainly in unattended environment and improves the real time data acquisition systems in future.

REFERENCES

[1] 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.

[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] 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.

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

[5] 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.

[6] C.-M. Yu, C.-S. Lu and S.-Y. Kuo, *"Mobile sensor network resilient against node replication attacks,"* in Proc. IEEE Conf. Sensor, Mesh, and Ad Hoc Communications and Networks (SECON), California, USA, 2008, pp. 597–599, (poster).

[7] 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.

[8] 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.

[9] 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.

[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. A. Johnson and D. W. Wichern, *Applied Multivariate Statistical Analysis*. Englewood Cliffs, NJ, USA: Prentice-Hall, 2007.

[12] 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.

[13] M. Luk, G. Mezzour, A. Perrig, and V. Gligor, *"MiniSec: A securesensor network communication architecture,"* in *Proc. Int. Conf. Information Processing in Sensor Networks (IPSN)*, Cambridge,MA, USA, 2007.

[14] Liu and P. Ning, "*TinyECC: A configurable library for elliptic curvecryptography in wireless sensor networks,"* in *Proc. Int. Conf. Information Processing in Sensor Networks (IPSN)*, Missouri, USA, 2008, pp.245–256.

[15] D. J. Malan, M. Welsh, and M. D. Smith, *"Implementing public-key infrastructure for sensor networks," ACM Trans. Sensor Network*, vol. 4, no. 4, pp. 1–23, 2008

[16] 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

BIOGRAPHIES

N.BALAJI received B.E.-Computer science Engineering (2012) from j.j. college of engineering and Technology, Trichy ,Tamil Nadu, India under Anna University and M.E. in Computer and Communication Engineering (2014) from Anna University, M.A.M College Of Engineering, Trichy, India. Her current research area is Wireless Sensor Network Security.

Ms.M.Anitha is an Assistant Professor in the Department of information technology at M.A.M College Of Engineering, Trichy, India. She received his B.E. in computer Sciences and Engineering from A.R.J College of Engineering & Technology, Mannargudi. Anna University Tamil Nadu, India. In 2011 and She received his M.Tech in Advanced Computing from SASTRA University Tamil Nadu, India in 2013.