ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

IJIRSET

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)

On 21st& 22nd March Organized by

K.L.N. College of Engineering, Madurai, Tamil Nadu, India

Efficient and Effective Detection of Node Replication Attacks in Mobile Sensor Networks

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

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

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

Abstract-wireless sensor networking (WSN) techniques consists of spatially distributed autonomous sensor node to monitor node replication detection .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 in wireless communication and the smallness of computers have led to a new concept called the mobile sensor network .where two or more mobile Nodes can generate a temporary network without the use of any already presented network infrastructure or centralized administration [1]. If the source and the destination mobile node are not within the communication range of each other, data packets are forwarded to the destination mobile host by relaying the transmission through other mobile hosts which exist between the two mobile regions [2].

Here no special infrastructure is needed, in various fields such as military and rescue affairs, many applications are expected to be developed for mobile networks. One sensor node, fabricates many replicas having the same identity (ID) from the captured node, and places these replicas back into strategic positions in the network for further malicious activities. This is a so-called node replication attack.Each Node in a sensor network is free to move independently in any direction. In contrast to the Cellular System there is no master slave relationship.

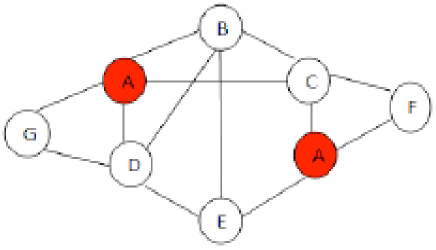

Fig.1 Node Replication Attack

If a network is a partitioned into two networks due to the migrations of mobile region in one of the partitions cannot access data items held by mobile region in one of the partitions cannot access data items held by mobile region in the other [3]. Thus data accessibility in ad hoc networks is lower than that in conventional fixed networks. A possible and hopeful solution is the replication of data items at mobile region that are not the owner of the original data. Since mobile region generally have poor resources, it is usually not possible for them to have replicas of all data items in the network the central base station can be avoid, by tip to the police rely on neighbors Detection. A voting mechanism, using neighbors' can reach consensus on a legal Node [3]. Unfortunately, while achieving a shared innovation Fashion, the method to detect distributed Replication node in the disjoint parts can be identified in Network [4]. At least when nodes to replicate two hops from each other, the local approach can detect the replicated node in a network.

A. Wormhole 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.

B.Black hole Attack

In this attack an attacker hears the request for routes in a flooding based protocol. In this attack the attacker receives the request for a route to the destination node, which creates a reply consisting of an extremely short route. If the malicious reply reaches the initiate node before the reply from the real node, a false route gets created [5]. Once the malicious device able to insert itself between the communicating nodes, it is capable to do misbehavior action between them.There are many attacks which can be mounted on the routing protocols and interrupt the proper operation of the network. Brief descriptions of such attacks are specified below.

C.Routing Table overflow

In case of routing table overflow, the attacker establishes routes to nonexistent nodes. The goal is to create enough routes to avoid novel routes from being created or to overwhelm the protocol implementation. In proactive routing algorithms, it is necessary to discover routing information even before it is needed. In the reactive algorithms it is compulsory to find a route only when it is needed.

D.Node routing poisoning

In node routing poisoning will the compromised of nodes in the network. Which send fabricated routing updates or modify genuine route updates packets sent to other approved node [6], [7]. Routing table poisoning might result in sub-optimal routing. Congestion in portion of the network, or even construct a few parts of the network inaccessible.

E.Rushing 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.

F.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.

II.RELATED WORKS

One of the first solutions for the detection of node replication attacks relies on a centralized base station. In this solution, each node sends a list of its neighbours and their claimed locations to a Base Station (BS) [3].The entry in two lists sent by nodes that are not "close" to each other will result in clone detection. Then, the BS revokes the clones. This solution has several drawbacks, such as the presence of a single point of failure in BS, and high communication costs due to the large number of messages. Further, nodes close to the BS will be required to route far more messages than other nodes, hence shortening their operational life.

Other solutions rely on local detection. For example, in a voting mechanism is used within a neighbourhood to agree on the time period of a given node [10]. However, applying this kind ofmethod to the problem of replica detection, if this fails to detect cloneswithin the same neighbourhood. As described a naive distributed solution for detecting the node replication attacks in Node-To-Network Broadcasting. With this solution each nodefloods the network with a message containing its location information and compares the received location information with that of its neighbours. If a neighbour *y1*of node *y0*receives a location claim thatthe same node *y0*is in a position not coherent with the position of *y0* detected by *y1*, this will result in the detection of a clone. However, this method is very energy consuming since it requires *n* flooding as per iteration, where*n* is the number of nodes in the WSN.

In the Sybil attack, a node claims multiple existing identitiesstolen from corrupted nodes. Note that both the Sybil andthe clone attacks are based on identity theft, however the two attacksare orthogonal [11]. Theyare efficiently addressed mechanism for RSSI or with authenticationBased 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 protocolswith 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 networkto detect replication. In the RM, when a node broadcasts its location, each of its neighbours sends a digitallysigned copy of the location claim to a set of randomly selectednodes. Assuming there is a replicated node, if every neighbourrandomly selects O ($\sqrt{n}$) destinations, then exploiting the birthday paradox. There is a non negligible probability at least onenode will receive a pair of non coherent location claims. The node that detects the existence of another node in two different locationswithin the same time-frame will be called *witness*.

The RM protocolimplies high communication costs: Each neighbour has to send$O$ ($\sqrt{n}$) messages. To solve this problem the authors propose usingthe LSM protocol [14]. The LSM protocol behaviour is similar to that ofRM but introduces a minor modification that implies a noticeableimprovement in terms of detection probability.

In the LSM protocol, when a node announces its location, everyneighbour locally checks the signature of the claim and then itforwards this location claim with probability p. If the neighbourforwards the claim, it randomly selects a fixed number $g \geq 1$ ofdestination nodes and sends the signed claim to all the destinationnodes [15],[16]. In order for a location claim to travel from source to destinationnode, it must pass through several intermediate nodes by defining a claim message path. Moreover, every node that routes their claim message will check the signature, store the message, andcheck for coherence with the other location [17]. The claims will receive withinthe same iteration of the detection protocol.

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 [18], [19],. In fact, during a checkthe same node *y0*is present with two non-coherent locations; theWitness will trigger a revocation protocol for node *y0*.

III. PROPOSED SYSTEM

To detect the node replicas in mobile sensor networks using two localized algorithms, XED and EDD, are proposed. The proposed techniques developed in our solutions, challenge-and-response and encounter-number, are fundamentally different from the others. The proposed algorithm can resist node replicationattacks 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.

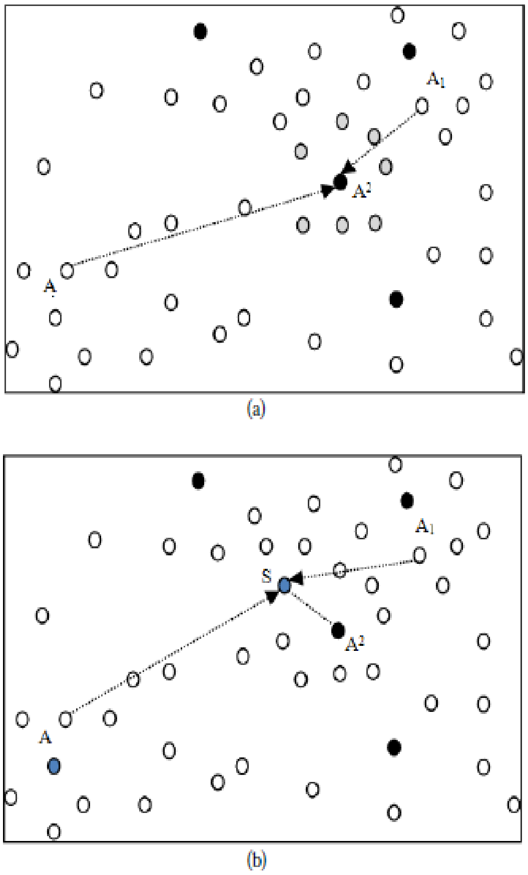

Fig 3(a) Existing Approach (b) Proposed Approach

A. Target localization problem

Sensor play a vital role in many sensor network applications, such as environmental monitoring and target tracking. Fundamental techniques developed for wireless sensor networks also requires a sensor location information, suchas routing protocols that make routing decisions based on node locations. Location discovery/estimation protocols, alsocalled localization protocols, use some special nodes called beacon nodes which are assumed to known their own locations. These protocols work in two steps. First step: Non beacon nodes receive radio signals called reference messages from the beacon nodes. A reference message includes the location of the beacon node. Second step: The non beacon nodes make certain measurements, for example distance between the beacon and non beacon nodes. The measurements are based on features of the reference messages like received signal strength indicator and time difference of arrival. Without protection, an attacker may easily mislead the location estimation in sensor nodes and the normal operation will carried out in sensor networks. An attacker may provide incorrect location references by replaying the beacon packets intercepted in different locations. Also, an attacker may compromise a beacon mode and distribute malicious location references by lying about the location or manipulating the beacon signals. In either case, non beacon nodes will determine their locations incorrectly. From the point of view of coverage and connectivity, the dimension problem has been intensely studied in recent years . The most commonly used problem in coverage problems is the disk model, which assumes that sensing region for a sensor is a circular region centred it. A point is said to be sensing region.

IV.DETECTONTECHNIQUE OVER MOBILE SENSOR NETWORK

A.Overview

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.

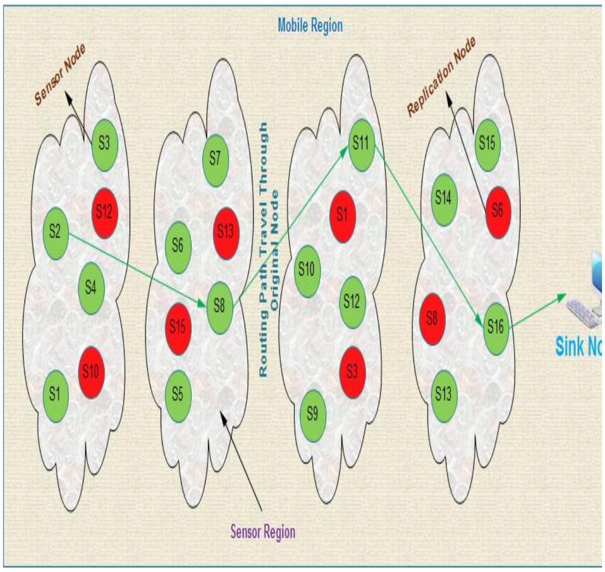

Fig.2 Architecture of mobile sensor network

B.Detection System

In this paper a detection based security scheme is provided for Mobile Sensor network .AlthoughMobile Sensor network has low computation and communication capacity, they specific properties such as their constant neighborhood information that permit for detection of anomalies 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

C.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.

D.Execute 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.

E.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.

F.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.

G.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.

V.PERFORMANCE METRICS

The performance is evaluated according to the following metrics:

Table1**:** Detection Mechanisms for performance overheads

Schemes	**Communication cost**	**Memory**
Deterministic Multicast	$O(g \ln g\sqrt{n} / d)$	$O(g)$
Randomized Multicast	O(n2)	$O(\sqrt{n})$
Line-Selected Multicast (LSM)	$O(n\sqrt{n})$	$O(\sqrt{n})$
RED	$O(r \sqrt{n})$	$O(r)$
XED	O(1)	
EDD & SDD	O(1) /O(n)	$O(n)$ /$O(\xi)$
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		

VI.MATHEMATICAL MODEL

*Step 1:*Consider WSN with nodes with witness node set nneighbour.

Where,
n = Number of nodes in the network
p = probability a neighbour replicates location information
g = Number of witness nodes

*Step2:*Probability of selecting witness node

$$(1-g) \tag{1}$$

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

$$(1-(1-g)^{n})^{2} \tag{2}$$

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

$$(O (p .g .n) \tag{3}$$

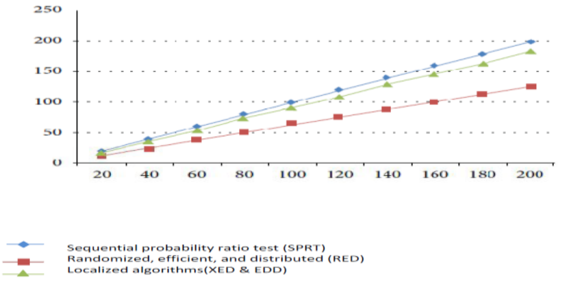

Fig 4.Comparison of protocols

ACKNOWLEDGMENT

I would like to thank Ms.M.Anithafor helpful discussions about this work.

CONCLUSION

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-numberdetection 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.DiPietro, 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 StatisticalAnalysis*. Englewood Cliffs, NJ, USA: Prentice-Hall, 2007.

[12] T. Karagiannis, J. L. Boudec, and M. Vojnovic, *"Power law and exponentialdecay 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.

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

[18] S. M. Ross, *Introduction to Probability Models*. New York, NY,USA: Academic, 2006.

[19] Sharma and R. Mazumdar, *"Scaling laws for capacity and delay in wireless ad hoc networks with random mobility,"* in *Proc. IEEE Int.Conf. Communications (ICC)*, Paris, France, 2004, pp. 3869–3873.