AN ENHANCED DETECTION OF MASKED REPLICATION ATTACK IN WIRELESS SENSOR NETWORKS

Somesh Pal[1] , K. Vinay Kumar[2]

[1]PG Scholar, [2]Associate Professor, Dept. of CSE,

National Institute of Technology Karnataka, Surathkal, Karnataka, (India)

ABSTRACT

Wireless sensor nodes are very tiny battery powered and lack of hardware support for tamper resistance. They are often deployed in unattended environments, so the sensor nodes are vulnerable to various kinds of attacks. An adversary can easily enter into the network, deploys different types of malicious activities into the network. Firstly, adversary captures random node into the network and extracts the credentials from that node and launch many insider attacks within the network. Node replication attack is one of the most dangerous threats through which an adversary creates many clones and extracts secret contents of the captured node. The replicas are then placed by an adversary at a certain position. A special case of node replication attack which is more harmful when the neighbors of a clone node are compromised, so the detection process of node replication attack is unable to detect the malicious clone node as it gets sheltered by its neighbors. There exists a detection process of this attack which basically monitors the neighbors of the clone node that it is misbehaving, but this solution cant solves the problem when the clone node sends the fake location claim to its neighbors or when monitor node misbehaves or compromised. This paper presents the complete solution for misbehaving of the claimer node and monitor node to make the detection process at global level.

I. INTRODUCTION

Sensor networks contains a number of sensor nodes which are very tiny battery powered, useful in several applications, like environment monitoring and object tracking etc. Unattended nature of this networks and nodes are not equipped with tamper-resistant hardware leverage the adversary to [1] captures and compromises the sensor node, fabricate many replicas of that node and extracts the credentials from that node and launch many insider attacks within the network.

A special case of node replication attack called masked replication attack is more injurious form of node replication attack. In this attack, reporter nodes are compromised so it either forwards fake ID to the witness node or not forward any traffic. There is a mask created by the neighbor nodes and clone node gets sheltered inside it. The detection process of masked replication attack is based on watchdog mechanism such that there is a monitor node which monitors the behavior of the reporter nodes. The monitor node checks the packet alteration by reporter nodes by watching the network traffic. Monitor node sets a time quantum t in such a way that monitor node will wait t unit time after getting the location claim from claimer node, after timeout it triggers an alarm and sends the misbehavior of the reporter node to the witness node. In that way, monitor node reduces the misbehaving rate of the reporter node.

According to the problem in masked replication attack, detection scheme should be designed when any node may be compromised in WSN network. We can apply the compromised node detection algorithm proposed by [2] It has two parts, firstly in the initialization phase nodes communicates with neighbors. Finally, packet arrival time checks by its neighbor. If it's out of the range send alert to the base station. Based on the transmission time-buffer base station decides the compromised node. For secure communication between each node in claimer reporter-witness based framework, Threshold cryptography for sharing message and Chinese Remainder Theorem for verification of route and authentication [3]. But such type of computationally intensive algorithm is infeasible for the tiny devices. Key pre distribution scheme is the best solution for secret communication in WSN. So for encrypting data between communicating sensor nodes shared secret keys are required.

There are several pre distribution scheme have been proposed for secret communication between the nodes.[5] launched the q-composite key pre-distribution. Pair wise keys will be set up between the nodes if at least q no of common keys shared between them. [5] proposes SPINS architecture where each node in the network will share their secret key with base station. Two sensor nodes use the base station as a third party to establish the secret key between them. [6] proposes a scheme where a group of n node for computing a common key. This scheme mainly focuses on communication costs.

II. RELATED WORK

B.Parno et al. [4] have introduced two distributed algorithms for the detection of clone nodes in wireless sensor networks. The first protocol is called Randomized Multicast (RM) which distributes location claims to a randomly selected set of witness nodes. The Birthday Paradox predicts that a collision will occur with high probability if the adversary attempts to replicate a node. Their second protocol, Line- Selected Multicast (LSM), exploits the routing topology of the network to select witnesses for a nodes location and utilizes geometric probability to detect replicated nodes. In RM, each node broadcasts a location claim to its one-hop neighbors. Then each neighbor selects randomly witness nodes within its communication range and forwards the location claim with a probability to the nodes closest to chosen locations by using geographic routing. At least one witness node is likely to receive conflicting location claims according to Birthday Paradox when replicated nodes exist in the network. In LSM the main objective is to reduce the communication costs and increase the probability of detection. Besides storing location claims in randomly selected witness nodes, the intermediate nodes for forwarding location claims can also be witness nodes. This seems like randomly drawing a line across the network and the intersection of two lines becomes the evidence node of receiving conflicting location claims.

The preliminary version of this paper presents the first distributed detection algorithm for mobile networks based on a simple challenge-and-response strategy. Nevertheless, its detection effectiveness is vulnerable to the collusive replicas. Thus, Yu et al. propose exploitation of the mobility pattern to detect the collusive replicas. Unfortunately, their storage requirement is linearly dependent on the network size and is not scalable. Ho et al. [10] propose a centralized detection algorithm for mobile sensor networks using Sequential Probability Ratio Test (SPRT). Intuitively, by having each node send the location of each encountered node, the base station can check if there is a node appearing at two distant locations with a velocity exceeding the predefined limit. If such a node exists, it is very likely to be a replica. Nevertheless, practically there could be some errors in the node speed measurement, leading to either false positives or false negatives. To avoid the above false judgment, the method in [10] checks whether the estimated speed of a specific node can conclude that is a replica with the aid of SPRT. Essentially, SPRT is a specific sequential hypothesis test with null and alternative hypotheses. The purpose of SPRT is to determine which hypothesis should be accepted with the consideration of a sequence of observations. In the case of replica detection, null and alternative hypotheses correspond to the node is not a replica and the node is a replica, respectively. The BS using SPRT continuously receives a stream of the estimated speeds of a specific node. Based on the decision principle of SPRT, the BS can make an accurate decision on whether the node under consideration is a replica even though some of the measured speeds are erroneous. The effectiveness of the method in [10], however, relies on the involvement of the base station, easily incurring the problems of single-point failure and fast energy depletion of the sensor nodes around the base station.

Conti et al. [1] have proposed a Randomized, Efficient, and Distributed protocol called RED for the detection of node replication attack. It is executed at fixed intervals of time and consists in two steps. In first step a random value, rand, is shared between all the nodes through Base station. The second step is called Detection phase. In the Detection phase each node broadcasts its claim (ID and location) to its neighboring nodes. Each neighbor node that hears a claim sends (with probability p) this claim to a set of pseudo-randomly selected network locations (g). The pseudo random function takes as an input: ID, random number. Every node in the path (from claiming node to the witness destination) forwards the message to its neighbor nearest to the destination. Hence the replicated nodes will be detected in each detection phase.

III. DRAWBACKS OF EXISTING SOLUTION

In this attack, reporter nodes are compromised so it either forwards fake ID to the witness node or not forward any traffic. There is a mask created by the neighbor nodes and clone node gets sheltered inside it. The detection process of masked replication attack is based on watchdog mechanism such that there is a monitor node which monitors the behavior of the reporter nodes. The main mechanism of monitor node is to watch the network traffic between reporter node and witness node. The monitor node checks the packet alteration by reporter nodes by watching the traffic. Monitor node sets a time quantum t in such a way that monitor node will wait t unit time after getting the location claim from claimer node, after timeout it triggers an alarm and sends the misbehavior of the reporter node to the witness node. In that way, monitor node reduces the misbehaving rate of the reporter node. In the existing detection process it is assumed that monitor node is not compromised. If monitor node misbehaves, it is necessary to extend the idea of detection of reporter's misbehavior. Secondly, claimer nodes collaborate with reporter nodes and alter their location or claimer node forwards the location claim by fake ID's then monitor node cannot detect the alteration of the location because it only monitors the compromised reporter node.

In the previous solution of masked replication attack we have considered that the monitor node which works as a watchdog for hearing the misbehavior of reporter node is not compromised. In that case, detection process fails for the misbehaving of the monitors.

The three major drawbacks of the existing detection process is as follows:

- In case of Colluding adversaries can provide multiple authenticated ids to compromised node.
- Claimer can send fake location ID to Compromised Reporter.
- When monitor node misbehaves.

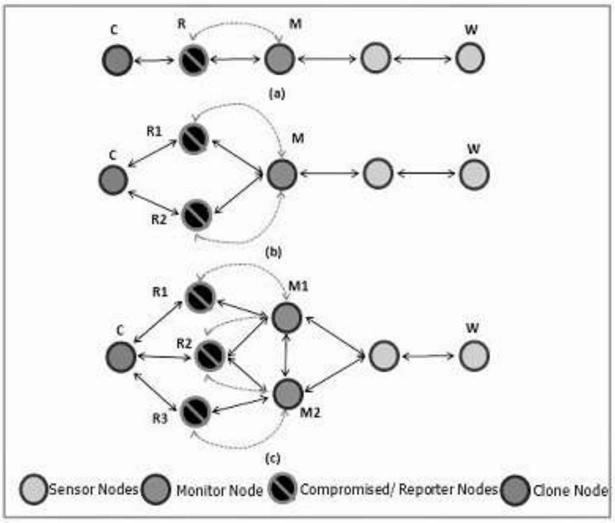

Fig 1: Existing MRA Detection Technique

IV. ENHANCED DETECTION TECHNIQUE

To solve the problem of the existing solution, Firstly, in the claimer reporter witness based framework detection of compromised node algorithm [2] will be applied to the network. So, Initially it will filter out the compromised node with high probability. New node will be added if it is authenticated and not compromised. For secure communication between the each sensor node Random pre distribution scheme is the solution where shared secret keys generated for secret sharing of the messages between the nodes. So, it prevents eavesdropping and colluding attacks. Watchdog is the monitoring technique to detect nodes misbehavior. In this technique every node in the network overhears the communication of neighboring nodes [9]. Suppose sensor node A intends to send message to C which is not in its communication range. Firstly, it will send to node B then B forwards to C. Let Sa be a set of sensor nodes that overhear the communication from A to B and Sb be a set of sensor nodes that overhear the communication from B to C. We can select watchdogs of B, common between the sets Sa and Sb. It is clear that nodes which belonged to the common region is able to capture both messages and trace malicious node by watching the incoming and outgoing packets. The proposed solution is that, several nodes in the network acts as a watchdog for claimer-reporter witness framework which will detect the error code while communicating. It will check that the claimer node changes the location ID or not. For the monitor node, watchdog checks whether it is working as per its behavior and by tracing the incoming and outgoing packets checks any content of the message modified or not.

An enhanced RED protocol TKRED [10] is used which is nothing but a pseudo-random function that runs on each node taking current time as seed. In phase 1 intermediate seed is concatenation(XOR) of current time and claimer ID. Then the seed, claimer-ID as arguments of pseudo-random functions. Pseudo-random function decreases computational and the communication costs. As system changes key at certain interval of time and time is here the security key so even if attacker gets one key, after certain time no longer key will be used. Instead of using rand as argument of pseudo-random function used in RED protocol, we are using seed here for finding witness locations.

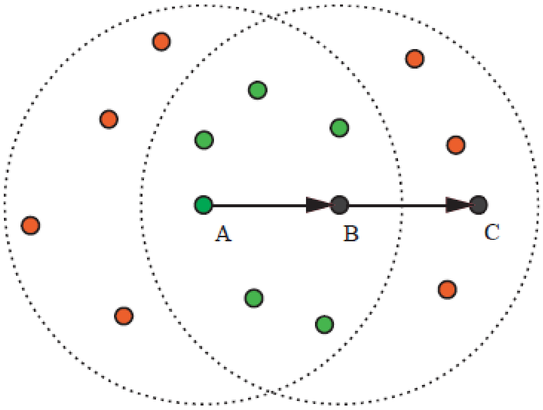

Fig.2 Embed Watchdog Mechanism

V. ALGORITHM

nodeid = Node id of the Network.

nodeloc = location of the Node.

prkey = Private Key of the Node.

pubkey = Public Key of the Node.

nodetime = Current Time of a Node.

5.1 Algorithm for Claim Broadcasting

```
1. locclaim <== ( nodeid, isClaim(), nodeloc, nodetime )
2. claimsigned <== ( locclaim, prkey(H(locclaim)) )
3. bm <== ( neighborOf(nodeid : ( nodeid, neighborOf(nodeid, claimsigned ))
```

5.2 Algorithm for Receiving Message m

```
1. if(isClaim(m)) then (Probability: p)
2. ( nodeid, neighborOf(nodeid), claimsigned ) <== m
3. (locclaim, signature) -->   claimsigned
4. if bad signature then discard m
5. else if incoherent location claim then
6. (nodeid, nodeloc, nodetime, claimsigned) <== locclaim
7. end if
8. seed <== time(0) || IDclaimer
9. locations <== pseudo rand(seed; IDclaimer; g)
10. //otherwise forward the claim
11. for all i locations do
12. a ==>  (nodeid, i, isFwdClaim, claimsigned)
13. end for all
14. else if isFwdClaim(m) then
15. ( nodeid, neighborOf(nodeid), claimsigned) <== m
16. (locclaim, signature) <== claimsigned
```

```
if bad signature(signedclaim) then discard m
else
(nodeid, nodeloc, nodetime, claimsigned) <== locclaim
if detectClone(memory, nodeloc , nodetime ) then
trigger revocation procedure for nodeid
else
store fwdClaim in memory
end if
end if
end if
```

5.3 Algorithm for Monitor Node

```
if isClaim(m) then
Run Recieve message Procedure
else if isFwdClaim(m) then
LookUp List Neighbours (nodeid )
else
trigger masked attack procedure for nodeid
end if
```

It is assumed that the routing will deliver a message sent to a network location to the node closest to this location that the routing protocol will not fail that message forwarding is not affected by dropping or wormhole attacks (for these kinds of attacks a some solutions can be found to test the protocols, we assume that the adversary has introduced two nodes with the same ID in the network. Clearly, if the adversary introduces more replicas, the task of detecting the attack is actually easier.

The set of witness nodes is selected using the Pseudorandom function. This function takes in input the ID of the node, that is the first argument of the claim message, the current rand value, and the number g of locations that have to be generated. Using a pseudo-random function guarantees that, given a claim, the witnesses for this claim are unambiguously determined for a given protocol iteration. Time synchronization is used by nodes to discern between various iterations. Each node signs its claim message with its private key before sending it. The nodes that forward the signed claim towards destination are not required to add any signature or to store any message. For each received claim, the potential witness node: Verifies the received signature. checks for the freshness of message. Indeed, it could be just a reply of an old message. This check is performed verifying the coherence between the time inserted in the message by the claiming node and the current time.

VI. SIMULATION AND DISCUSSION

In designing a protocol for the detection of masked replication attacks, a major issue lies in the selection of witnesses. An adversary is able to subvert the nodes and the attack goes undetected if an adversary gains the knowledge of future witnesses before the detection protocol executes. Through simulation results it is justified that our proposed protocol SRRED is both ID and area oblivious. This is because proposed enhanced technique neither provides any information on the ID of the sensors that will be the witnesses of the clone attack nor it selects an area with high density of witnesses. Rather, in this proposed technique, the IDs of the witness are selected randomly among all the nodes throughout the network.

With the help of the ns-2 network simulator we simulate the proposed mobile replica detection scheme in a mobile sensor network. In our simulation, 200 mobile sensor nodes are placed within a square area of 250 m x 250 m. We use the Random Waypoint Mobility (RWM) model to determine mobile sensor node movement patterns. The trace file is also used to send the request packets to all the nodes in the network. Using this RWM the nodes moves for 0.05ms. In the RWM model, each node moves to a randomly chosen location with a randomly selected speed between a predefined minimum and maximum speed. After reaching that location, it stays there for a predefined pause time. After the pause time, it then randomly chooses and moves to another location.

All simulations were performed for 1,000 simulation seconds. We fixed a pause time of 20 simulation seconds and a minimum moving speed of 1.0 m/s of each node. Each node uses IEEE 802.11 as the medium access control protocol in which the transmission ranges is 50 m initially the nodes are deployed in the hostile environment after deploying the nodes the base station send the coverage region to all the nodes in the network. Then the nodes gather the data and send to the base station if any of the node get drops the data or it sent the false data then the functionality of replica nodes takes place. Using the hypothesis testing method the replica nodes are detected. If null hypothesis is accepted then the replica nodes are detected and revoked from the network.

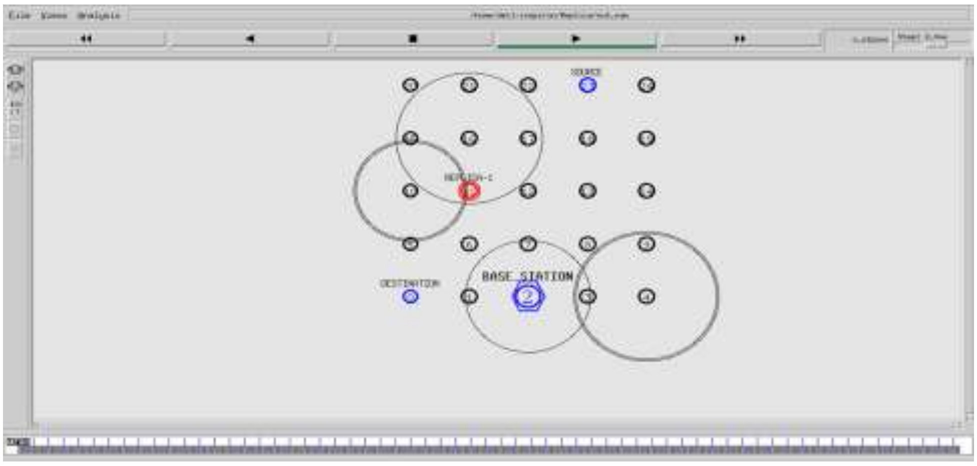

Fig.3 Random No. Sent by Base Station

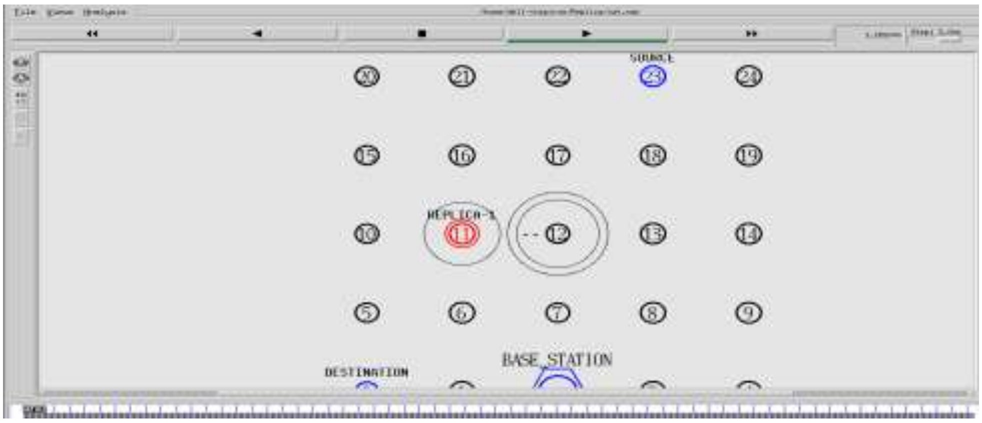

Fig.4 Detection of Replica Node

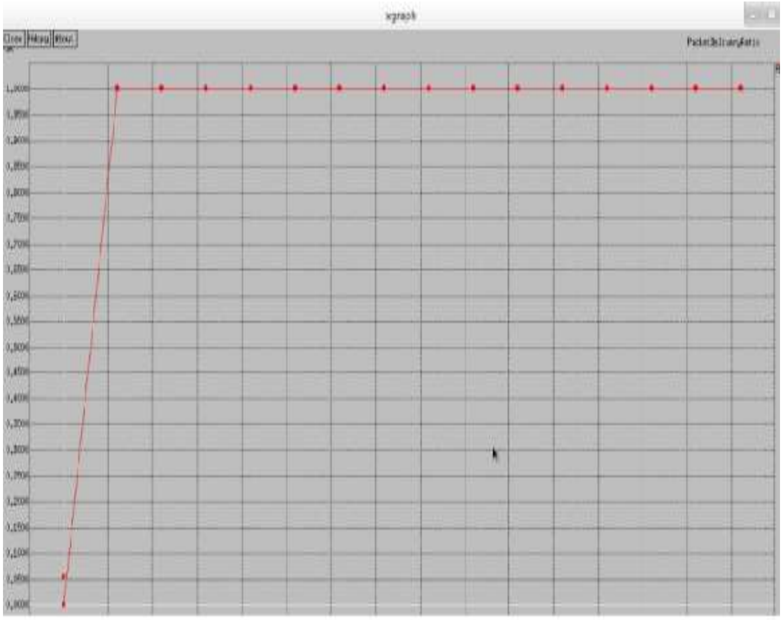

Fig.5 Detection Ratio

VII. CONCLUSION

In this paper, we presented an enhancement of the existing detection protocol of masked replication attack by exploiting the mechanism of Temporal Key based RED protocol for securing the network from clones and replicas and justified its resiliency to a smart adversary through stunning examples and simulations. We have deployed several Watchdog node as per its range over the whole network deployed. We have also introduced a mechanism for detecting and countering masked replication attack which RED and LSM are unable to thwart. Analyzing the security of the proposed protocol, it is concluded that it is more robust, efficient and highly resilient against masked replication attack. The addition of time as the seed of a pseudo random function and elimination of the base station requirement will not only build greater security against clones but also the communication and computation overhead is also reduced deliberately. Probability of misbehaving monitor node is very less.

REFERENCES

[1] M. Conti and R. D. Peoto, A Randomized Efficient and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks, In Proceedings of the 8th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc) , 2007.

[2] M.Y. ; Saad M.N.M. Khan, W.Z. ; Aalsalem. Detection of masked replication attack in wireless sensor networks, Information Systems and Technologies (CISTI), 2013 8th Iberian Conference on IEEE CONFERENCE PUBLICATIONS, pages 1-6, 2013.

[3] Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker, Mitigating Routing Misbehavior in Mobile and Ad Hoc Networks, In Proc. of International Conference on Mobile Computing and Networking (Mobicom), 2000, pp. 255-265.

[4] B. Parno, A. Perrig and V. Gligor., Distributed detection of node replication attacks in sensor networks, In Proceedings of the IEEE Symposium on Security and Privacy (SP), 2005.

[5] A. J. Menezes, S. A. Vanstone and P. C. V. Orschot. Handbook of Applied Cryptography, CRC Press, Inc., 1996.

[6] Zhu B, Setia S ,Jajodia S ,Roy S, Wang L. Localized multicast: efficient and distributed replica detection in large-scale sensor networks . IEEE Transactions on Mobile Computing 2010; 9(July) :91326.

[7] 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 Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, vol. 37, no. 6, pp. 1246- 1258, 2007.

[8] K. Xing, F. Liu, X. Cheng, D. H.C. Du, Real-Time Detection of Clone Attacks in Wireless Sensor Networks, In Proceedings of the 28th International Conference on Distributed Computing Systems (ICDCS), pages: 3-10, 2008.

[9] Wen Tao Zhu, Jianying Zhou, Robert H. Deng, Feng Bao,Detecting Node Replication Attacks in Wireless Sensor Networks: A Survey, Journal of Network and Computer Applications, 2012.

[10] Wazir Zada Khan, Mohamad Naufal Mohamad Saad and Mohammed Y Aalsalem, Scrutinizing Well-known Countermeasures against Clone Node Attack in Mobile Wireless Sensor Networks, International Journal of Grid and Utility Computing (IJGUC), 2012.

[11] A. Seshadri, A. Perrig, L. van Doorn, and P. Khosla, SWATT: Software based attestation for embedded devices, IEEE Symposium on Security Privacy, pp. 272282. 2004.