IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 3, June-July, 2013
ISSN: 2320 - 8791
www.ijreat.org

Mobile Replica Node Detection & Rejection In WSN Using SPRT

Sneha Mohan[1], Rinsa E A[2]

[1,2]**Electronics and Communication Department, MG University, Muvattupuzha, Kerala, India**

Abstract

Sensor network deployment is becoming more common place in environmental, business and military applications; security of these networks emerges as a critical concern. Without proper security, it is impossible to completely trust the results reported from sensor networks deployed outside of controlled environments. The replica nodes are controlled by the adversary, but have keying materials that allow them to behave like authorized participants in the network. Protocols for secure sensor network communication would allow replica nodes to create pair wise shared keys with other nodes and the base station, thereby enabling the nodes to encrypt, decrypt and authenticate all of their communications as if they were the original captured node. Sequential Probability Ratio Test (SPRT) uses the fact that an uncompromised mobile node should never move at speed in excess of the system-configured maximum speed. The main attack against the SPRT based scheme is when the replica nodes fails to provide signed location and time information for speed measurement. This is overcome by employing a quarantine defense technique to bloc non complaint nodes. Through quarantine analysis, the amount of time during a given time slot, that the replicas can affect the network is very limited. Black hole detection technique can be implemented, thereby enabling the effective detection of static and mobile replica nodes.

Keywords-sequential probability ratio test, replica nodes, black hole detection,quarantine defense scheme

1. Introduction

Wireless sensor networks are becoming increasingly popular in many spheres of life. Their development was originally motivated by military applications such as battle surveillance. Wireless Sensor Network (WSN) deploys a large number of small nodes in Ad-Hoc manner that can sense environmental changes and report them to other nodes over flexible network architecture. Securing data from sensor nodes is the most crucial task in any process. Due to the unattended nature of wireless sensor networks, adversary can attack the sensor nodes and can cause damages to the network. False data injection, signal jamming, privacy violation, physical attacks, and affecting the network protocol are the possible damages. A particularly dangerous attack is the replica node attack [1] in which the adversary takes the secret keying materials from a compromised node, generates a large number of attacker controlled replicas that share the compromised node's keying materials and ID, and spreads these replicas throughout the network. With a single captured node, the adversary can create as many replica nodes as needed. The time and effort needed to inject replica nodes into the network is far less than the effort to capture and compromise the equivalent number of original nodes. The replica nodes are controlled by the adversary but have keying materials that allow them to seem like authorized participants in the network. Hardware based techniques to mitigate them are easy to break. The paper introduces a software method with probability information to resist replica node attacks to the largest possible extent. Velocity information can be of much use to identify replica nodes. Base station performs sequential probability ratio test to revoke any node with false identity from the network. Quarantine defense can be used to limit attack strategies.

A solution to stop replica node attacks is to prevent the adversary from extracting secret key materials from mobile nodes by equipping them with tamper-resistant hardware. But it can make the node significantly harder and more time-consuming to extract keying materials from captured nodes. The main drawback is that it is applicable only for a small number of nodes. Several software-based replica node detection schemes have been proposed for static sensor networks [2]. The scheme mentions Sequential Monte Carlo Localization method that exploits mobility to improve accuracy and precision of localization. This approach does not require additional hardware on the nodes and works even when the movement of seeds and nodes is uncontrollable. Location awareness is important for wireless sensor networks since many applications such as environment monitoring, vehicle tracking and mapping depend on knowing the locations of sensor nodes.

A novel mobile replica detection scheme based on the Sequential Probability Ratio Test[1] was proposed. An uncompromised mobile node should never move at speeds in excess of the system configured maximum speed. As a result, a benign mobile sensor node's measured speed will appear to be at most the system-configured maximum speed. On the contrary, replica nodes will appear to move much faster than benign nodes and thus their measured speeds will likely be over the system-configured maximum speed because they need to be at two different places at once. It is likely that at least two nodes with the same identity are present in the network. By leveraging this intuition, SPRT is performed on every mobile node using a null hypothesis that the mobile node has not been replicated and an alternate hypothesis that it has been replicated. In using the SPRT, the occurrence of a speed that falls short of or exceeds the system-configured maximum speed will lead to acceptance of the null and alternate hypotheses, respectively. Once the alternate hypothesis is accepted, the replica nodes will be revoked from the network.

2 Network Assumptions

For the purpose of analysis, a two dimensional mobile sensor network is considered wherein the nodes roam freely throughout the network. To perform SPRT, the following assumptions are considered:

1. Every mobile sensor node's movement is physically limited by the system-configured maximum speed, Vmax.
2. All direct communication links between sensor nodes are bidirectional.
3. Every mobile sensor node is capable of obtaining its location information and also verifying the locations of its neighboring nodes.
4. Clocks of all nodes are loosely synchronized.
5. All the nodes in the mobile sensor network communicate with a base station.
6. Base station may be static or mobile; the nodes can communicate reliably to the base station on a regular basis.

The communication model used here is common in the current generation of sensor networks. Secure localization and synchronization protocols are implemented in the network.

2.1 REPLICA DETECTION USING SPRT

SPRT is a statistical decision making process which is considered as a one dimensional random walk with lower and upper limits[3]. Before the walk starts, null and alternate hypotheses are defined in such a way that the null hypotheses associated with the lower limit while the alternate one is associated with the upper limit. A random walk starts from a point between two limits and moves toward the lower or upper limit in accordance with each observation. If the walk reaches (or exceeds) the lower or upper limit, it terminates and the null or alternate hypothesis is selected, respectively. A benign mobile sensor node should never move faster than the system configured maximum speed, Vmax. As a result, a benign mobile sensor node's measured speed will appear to be atmost Vmax. The lower and upper limits can be configured to be associated with speeds less than and in excess of Vmax, respectively. Whenever a mobile sensor node moves to a new location, each of its neighbors ask for a signed claim containing its location and time information and decides probabilistically whether to forward the received claim to the base station. The base station computes the speed from every two consecutive claims of a mobile node and performs the SPRT by considering speed as an observed sample. Each time the mobile node's speed exceeds Vmax, it will expedite the random walk to hit or cross the upper limit and thus lead to the base station accepting the alternate (respectively, null) hypothesis that the mobile node has been (respectively, not been) replicated. Once the base station decides that a mobile node has been replicated, it revokes the replica nodes from the network.

2.2 CLAIM GENERATION AND FORWARDING

Each time a mobile sensor node u moves to a new location, it first discovers its location Lu and then discovers its set of neighboring nodes, N(u). Every neighboring node $v \in$ N (u) asks node u for an authenticated location claim by sending its current time T to node u. Upon receiving T, node u checks whether T is valid or not. If

$$T^1 - T \Big| > \delta + \varepsilon$$

Where T' is the claim receipt time at u,

δ is the estimated transmission delay of claim

$\in$ is the maximum error in time synchronization, C_u=u‖ L_u‖ T‖ Sig_u is the location claim generated and is sent to v, where sig_u is the signature over

the tuple (u,L_u, T) generated using node u's private key. If u denies the claim requests or if its claim contains invalid time information or fails to authenticate, then u will be removed from N (v). Also, if u claims a location L_u such that the distance between L_u and L_v is larger than the assumed signal range of v, then it will be removed from N(v). Once the above filtering process is passed, each neighbor v of node u forwards u's claim to the base station with probability p.

2. 3 DETECTION AND REVOCATION

Upon receiving a location claim from node u, the base station verifies the authenticity of the claim with the public key of u and discards the claim if it is not authentic. Let the authentic claims from node u be C_u^1 , C_u^2,…. The base station extracts location information L_u^i and time information T_i from claimC_u^i. Let d_i denote the Euclidean distance from location L_u^i at time T_i to L_u^{i+1} at T_{i+1}. Let O_i denote the measured speed at time T_{i+1}, where i =1, 2… can be calculated from time and distance information.

On the basis of the log-probability ratio,L_n, the SPRT for H_0 against H_1 is given as follows:

L_n <= l_n(β'/(1-α')) :

accept H0 and terminate the test. (1)

L_n >= l_n ((1-β')/α') :

accept H1 and terminate the test. (2)

l_n (β'/(1-α')) < L_n((1-β')/α') :

continue the test process. (3)

If a mobile node u is judged as benign, the base station restarts the SPRT with newly arrived claims from u. If, however, u is determined to be replicated, the base station terminates the SPRT on u and revokes all nodes with identity u from the network.

3 Quarantine Defense Technique

A malicious node u may attempt to forge a claim, either by sending a claim with incorrect data or by sending a claim with a bad signature. However, all of u's neighbors will check the validity of u's identity, reported location, reported time, and the signature over these values using node u's public key. Alternatively, node u can simply ignore the claim $\Pi\|$requests. In our scheme, if u's benign neighbor does not receive a claim despite sending a claim request, it will remove u from its neighboring set and will not communicate with u. Similarly, an attacker will not gain much benefit from having multiple replicas of a single node form a group that always moves together and stays close enough so that all replicas can claim the same location. This is because these nodes would essentially have the same set of neighbors.

An interesting variant of this attack, however, is to keep replicas close to each other so that the perceived velocity between their location claims is less than Vmax. To do this, an attacker coordinates a set of replicas to respond with correct claims only to those claims requests that make it appear as a single node never moving faster than Vmax. The attacker can have some replicas grouped closely together for this purpose; replicas that are further away must ignore claim requests or respond with false claims to avoid detection.

Since the replicas do not provide valid claims that would make the observed speed exceed Vmax, they can trick the base station into accepting null hypothesis that they are not replicas. To stop this attack, the base station checks whether each node responds with correct claims to all incoming claim requests.

Specifically, each time a malicious node u ignores a claim request from a benign neighbor node v or responds with false claims; v generates a denial of claim request notification message, (DCN) and sends it to the base station. Upon receiving the DCN message from v, the base station first checks the authenticity of the DCN and rejects it if it is invalid. Assume that the entire time domain is divided into time slots. The base station maintains a DCN counter for each node such that it initializes each counter to 0 and then resets it to 0 at the beginning of each time slot. Each time the base station receives a DCN message on u from v, it increases the DCN counter for u. If the DCN counter for u exceeds a predefined threshold during a time slot, it is highly likely that u has discarded a substantial fraction of claim requests during the time slot and is likely to be a replica node.

In this case, the base station will temporarily quarantine u from the network by disregarding all messages from u and broadcasting the quarantine information to all nodes. Upon receiving this quarantine message, all nodes will stop communicating with u except for exchanging claim request and response messages. If the DCN counter

for u does not exceed threshold during the quarantine period, the base station will release the quarantine that it imposed on u after the expiry of the quarantine period and broadcast the release information. Otherwise, it will extend the quarantine period by one time slot. The quarantine period needs to long enough to ensure that the replica nodes would. To trick the base station into putting benign nodes into the quarantine, the attacker could send many fake DCN messages.

Specifically, if the base station receives more than fake DCN messages on the benign node v, then v will be quarantined even though it responds correctly to all incoming claim requests. To discourage this type of attack, each node is restricted from sending more than one DCN from a node during a time slot; it will accept only one DCN from the node and discard the others. Hence, the attacker needs more than ρ compromised nodes per time slot to force a benign node to be quarantined, thus suppressing him from mounting a fake DCN attack.

The base station can further detect replica node by black hole detection technique. If the replica node moves away from the coverage area of the network, it can remain undetected. In this scenario the replica node can again make damages to the sensor network.

3.1 Black Hole Detection Technique

The base station drops control packets at the routing level, usually using a routing protocol to implement the filtering on wireless sensor nodes. The uncompromised benign nodes can be configured to silently discard packets addressed to forbidden host. But the replica nodes often dynamically respond quickly to the distributed packets. Thus the base station can detect the replica node and reject the node from the network. Once the replica node is detected the base station will send the message to all other nodes in the network and thus the nodes will stop communication from the replica node. And finally the replica node fails to obtain any kind of information from the network. The most common form of black hole is simply an IP address that specifies a host machine that is not running or an address to which no host has been assigned. Even though TCP/IP provides means of communicating the delivery failure back to the sender via ICMP , traffic destined for such addresses is often just dropped. Note that a dead address will be undetectable only to protocols that are both connectionless and unreliable (e.g., UDP). Connection-oriented or reliable protocols such as Transmission Control Protocol (TCP) will either fail to connect to a dead address or will fail to receive expected acknowledgements.

4 Simulation Study

We simulated the proposed mobile replica detection scheme in a mobile sensor network with the help of the ns-2 network simulator. In our simulation, 50 mobile sensor nodes were placed. Random Waypoint Mobility (RWM) model was used to determine mobile sensor node movement patterns. Threshold and packet size were set to 100 and 250. Bandwidth of the channel was 2MHz and the data rate was 2Mbps.

4.1 Simulation Results

The Quality Of Service parameters were analyzed. For any wireless network the QOS parameter is analyzed to study the efficiency of the network. The QOS parameters are communication ooverheads, packet loss and end to end delay. Overhead involves sending various control and signaling data required to achieve the reliable transmission of the desired data

Fig 1 End To End Delay

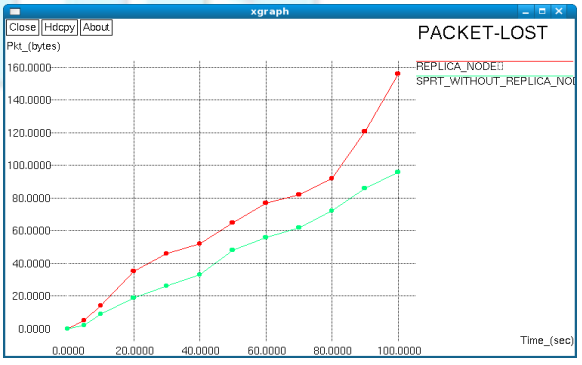

Fig 2 packet loss packet size versus time

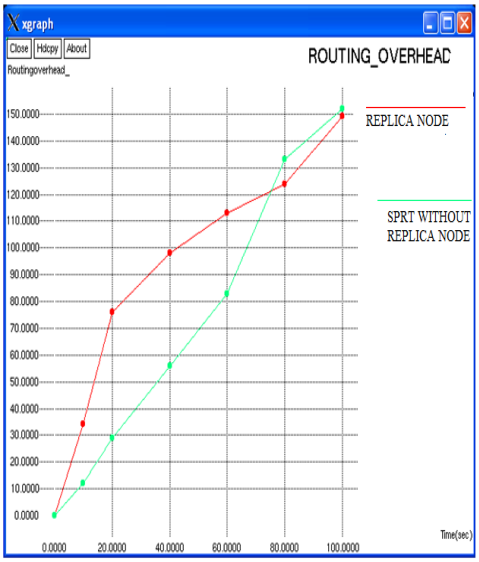

Fig 3 routing overhead , routing overhead versus time

5 CONCLUSION

In potentially hostile environments, the security of unattended mobile nodes is extremely critical. The attacker may be able to capture and compromise mobile nodes, and then use them to inject fake data, disrupt network operations, and eavesdrop on network communications. A particularly dangerous attack is the replica node attack in which the adversary takes the secret keying materials from a compromised node, generates a large number of attacker-controlled replicas that share the compromised node's keying materials and ID, and then spreads these replicas throughout the network. This project provides a novel mobile replica detection scheme based on the Sequential Probability Ratio Test .The fact that an uncompromised mobile node should never move at speeds in excess of the system-configured maximum speed. As a result, a benign mobile sensor node's measured speed will nearly always be less than the system-configured maximum speed. SPRT is performed on every mobile node using a null hypothesis that the mobile node has not be replicated and an alternate hypothesis that it has been replicated. Through quarantine analysis it is shown that the amount of time, during a given time slot, that the replicas can impact the network is very limited.

Further if the replica node moves away from the coverage area of the network, it can remain undetected. In that scenario, the base station drops control packets at the routing level, usually using a routing protocol to implement the filtering on wireless sensor nodes. The uncompromised benign nodes can be configured to silently discard packets addressed to forbidden host. But the replica nodes often dynamically respond quickly to the distributed packets. Thus the base station can detect the replica node and reject the node from the network. Once the replica node is detected the base station will send the message to all other nodes in the network and thus the nodes will stop communication from the replica node

REFERENCES

[1] Jun-Won Ho, Matthew Wright, and Sajal K. Das, "Fast Detection of Mobile Replica Node Attacks in Wireless Sensor Networks Using Sequential Hypothesis Testing",IEEE transactions on mobile computing, vol. 10, no. 6, June 2011.

[2] L. Hu and D. Evans, "Localization for Mobile Sensor Networks," Proc. ACM MobiCom, pp. 45-57, Sept. 2004.

[3] J. Jung, V. Paxon, A.W. Berger, and H. Balakrishnan, "Fast Port scan Detection Using Sequential Hypothesis Testing," Proc. IEEE Symp. Security and Privacy, pp. 211-225, May 2004.

[4] K. Dantu, M. Rahimi, H. Shah, S. Babel, A. Dhariwal, and G.S. Sukhatme, "Robomote: Enabling Mobility in Sensor Networks," Proc. Fourth IEEE Int'l Symp. Information Processing in Sensor Networks (IPSN), pp. 404-409, Apr. 2005.

[5] S. Capkun and J.P. Hubaux, "Secure Positioning in Wireless Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 221- 232, Feb. 2006.