Fast Detection of Node Replication Attacks in Mobile Sensor Networks

Jun-Won Ho, Matthew Wright, and Sajal K. Das
Department of Computer Science and Engineering, University of Texas at Arlington
{ho, mwright, das}@cse.uta.edu

I. Introduction

Advances in robotics have made it possible to develop a variety of new architectures for autonomous wireless networks of sensors. Mobile nodes, essentially small robots with sensing, wireless communications, and movement capabilities, are useful for tasks such as static sensor deployment, adaptive sampling, network repair, and event detection [1]. These advanced sensor network architectures could be used for a variety of applications including intruder detection, border monitoring, and military patrols. In these kinds of hostile or potentially hostile environments, the security of unattended mobile nodes is critical. The attacker may be able to capture and compromise mobile nodes, and then he can use them to inject fake data, disrupt network operations, and eavesdrop on network communications.

In this scenario, a particularly dangerous attack is the *replica 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 node's keying materials and ID, and then spreads these replicas throughout the network. With a single captured node, the adversary can create as many replica nodes as he has the hardware to generate.

Software-based replica node detection schemes have been proposed for static sensor networks [2]. The primary method used by these schemes is to have nodes report *location claims* that identify their position and attempt to detect conflicting reports that signal one node in multiple locations. However, since this approach requires fixed node locations, it cannot be used when nodes are expected to move. Thus, our challenge is to design an effective, fast, and robust replica detection scheme specifically for mobile sensor networks.

In this paper, we propose a novel mobile replica detection scheme based on the *Sequential Probability Ratio Test* (SPRT) [3]. We use the fact that an uncompromised mobile node should never move at speeds in excess of the system-configured maximum speed. In practice, an uncompromised mobile node's measured speed can exceed the system-configured maximum speed due to the error in speed measurement. However, the likelihood of this case will be very low as long as we employ a speed measurement system with low error rate. Accordingly, if we observe that a mobile node's measured speed is over the system-configured maximum speed, it is then highly likely that at least two nodes with the same identity are present in the network. By leveraging this intuition, we perform the SPRT 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. Once the alternate hypothesis is accepted, the replica nodes will be revoked from the network.

II. Mobile Replica Detection Using Sequential Probability Ratio Test

We assume that every mobile sensor node is able to obtain its location information and verify the locations of its neighboring nodes. Furthermore, we assume that the clocks of all nodes are loosely synchronized with a maximum error of ϵ. Our proposed protocol proceeds in two phases.

1) Claim Generation and Forwarding: Each time a mobile sensor node u moves to a new location, it first discovers its location L_u and then discovers a set of neighboring nodes $N(u)$. Every neighboring node $v \in N(u)$ asks for an authenticated *location claim* from node u by sending its current time T to node u. Upon receiving T, node u checks whether T is valid or not. If $|T' - T| > \delta + \epsilon$, where T' is the claim receipt time at u and δ is the estimated transmission delay of claim, then node u will ignore the request. Otherwise, u generates location claim $C_u = \{u||L_u||T||Sig_u\}$ and sends it to a neighboring node v, where Sig_u is the signature generated by node u's private key. If u denies the claim request or if its claim 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_v and L_u 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) Detection and Revocation: Upon receiving a location claim, the base station verifies the authenticity of the claim with the public key of node u and discards the claim if it is not authentic. We denote the authentic claims from node u by $C_u^1, C_u^2, \ldots,$. The base station extracts location information L_u^i and time information T_i from claim C_u^i. Let d_i denote the Euclidean distance from location L_u^{i-1} at time T_{i-1} to L_u^i at T_i. Let o_i denote the measured speed at time T_i, where $i = 1, 2, \ldots,$. In other words, o_i is represented as:

$$o_i = \frac{d_i}{|T_i - T_{i-1}|}$$

Let V_{max} be a system-configured maximum speed of a mobile node and S_i be denote a Bernoulli random variable that is defined as:

$$S_i = \begin{cases} 0 & \text{if } o_i \leq V_{max} \\ 1 & \text{if } o_i > V_{max} \end{cases}$$

The success probability λ of Bernoulli distribution is defined as $\Pr(S_i = 1) = 1 - \Pr(S_i = 0) = \lambda$.

Now, we present how SPRT is performed to make a decision about node u from the n observed samples, where a measured speed of u is treated as a sample. Let us define H_0 as the null hypothesis that node u has not been replicated and H_1 as the alternate hypothesis that node u has been replicated. We then define L_n as the log-probability ratio on n samples, given as:

$$L_n = \ln \frac{\Pr(S_1, \ldots, S_n | H_1)}{\Pr(S_1, \ldots, S_n | H_0)}$$

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

- $L_n \leq \ln \frac{\beta'}{1-\alpha'}$: accept H_0 and terminate the test;
- $L_n \geq \ln \frac{1-\beta'}{\alpha'}$: accept H_1 and terminate the test;
- $\ln \frac{\beta'}{1-\alpha'} < L_n < \ln \frac{1-\beta'}{\alpha'}$: continue the test process with another observation,

where α' and β' are the user-configured false positive and false negative rates, respectively.

If a mobile node u is judged as benign node, 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.

III. Security Analysis

An interesting attack approach is to keep replicas close to each other so that the perceived velocity between their location claims is less than V_{max}. To do this, an attacker coordinates a set of replicas to respond with correct claims only to those claim requests that make it appear as a single node never moving faster than V_{max}. Since a set of replicas selectively respond to the claim requests that help prevent them from being detected and discard the others or respond with false claims to them, they can trick the base station into accepting H_0, the hypothesis that they are not replicas. Thus, a straightforward defense strategy against the above attack is to have the base station check whether each node responds with correct claims to all incoming claim requests. The base station will temporarily *quarantine* nodes, which deny incoming claim requests, from the network. The base station will then release the quarantined nodes if they conform to the claim requests during the quarantine period. This quarantine defence strategy will greatly put limit on the amount of time for which a set of replicas can avoid detection when they follow a strategy of responding only to selected claims.

IV. Simulation Results

We used the ns-2 simulator to evaluate the proposed scheme. In this simulation, we adopted an random attacker model in which a compromised node and its replica randomly move in the network. We set the system-configured false positive and false negative rates both to 0.01 and and varied V_{max} by 20 m/s in the range from 20 m/s to 100 m/s. Moreover, we set the speed error rate γ to the values of 0.01, 0.1, and 0.2.

Simulation results show that the replica nodes were detected with at least probability of 0.99, and benign nodes were misidentified as replicas with at most probability of 0.01 at all speed error rates and mobility rates. The average number of claims to detect replica reaches its maximum of 8.86 when $V_{max} = 20$ m/s and $\gamma = 0.1$. This demonstrates that SPRT achieves fast replica detection at all mobility rates.

References

[1] K. Dantu, M. Rahimi, H. Shah, S. Babel, A. Dhariwal, and G. S. Sukhatme. Robomote: enabling mobility in sensor networks In *IEEE IPSN*, 2005.

[2] B. Parno, A. Perrig, and V.D. Gligor. Distributed detection of node replication attacks in sensor networks. In *IEEE Symposium on Security and Privacy*, May 2005.

[3] A. Wald. Sequential Analysis. *Dover Publications*, 2004.