Fast Detection of replica node attack in wireless Sensor network

Shirish Kapase S.[1] *Jagdish Bodke V.*[2] *Sunny Gaikwad K.*[3] *Sadashiv Shinde P.*[4] *Avinash Gavhane D.*[5]

Prof. Mohit Dighe
(Project Guide)

[1] Computer Department, Shri Chhatrapati Shivaji College of Engineering Rahuri Factory, Ahmednagar, India
[2] Computer Department, Shri Chhatrapati Shivaji College of Engineering Rahuri Factory, Ahmednagar, India
[3] Computer Department, Shri Chhatrapati Shivaji College of Engineering Rahuri Factory, Ahmednagar, India
[4] Computer Department, Shri Chhatrapati Shivaji College of Engineering Rahuri Factory, Ahmednagar, India
[5] Computer Department, Shri Chhatrapati Shivaji College of Engineering Rahuri Factory, Ahmednagar, India

(Department of Computer Engineering)
Shri Chhatrapati Shivaji College of Engineering

***Abstract*— Sensor networks are subject to a number of insidious attacks, including replication attacks, denial-of-message attacks, wormhole and Sybil attacks. Our work investigates innovative algorithms for preventing and/or detecting these attacks. While considering Wireless Sensor Network, there are different kinds of attacks can be taken under consideration. Majorly, attacks are nothing but attempts to stole the credentials of existing network and try to leave harm to the system. An attack happens due to lack of supervision. Intent of protecting our system from these kinds of attacks can be achieved using prevention and detection techniques. At any instant of time for providing identity of nodes, pair wise key and group wise key are being generated. With the help of these techniques, it is possible to detect an attack on the system. Replica attack is an underlined concept in the security of wireless sensor networks. We employ mobile nodes as patrollers to detect replicas distributed in different zones in a network. We also perform security analysis to discuss the defense strategies against the possible attacks on the proposed detection protocol. Moreover, With the help of comparison of communication cost and detection probability we show the advantages of the proposed protocol by using some existing methods.**

***Index Terms*— Wireless Sensor Network (WSN), Sequential Probability Ratio Test (SPRT), Sequential Hypothesis Test(SHT).**

I. INTRODUCTION

In real world, tasks such as static sensor deployment, adaptive sampling, network repair, and event detection, Mobile nodes with sensing, wireless communications, & movement capabilities are useful. In variety of applications like intruder detection, border monitoring, and military patrols these advanced sensor network architectures could be used. In potentially hostile environments, the security of un-attended mobile nodes is extremely critical. The attacker can easily acquires the credentials of mobile nodes and compromise with them, and then use them to release fake data, disturb network operations, and tries to interrupt on network communications. In which the adversary can acquire node generate the duplicate copy of original node (Replica) and attacks can be made.

Thus these types of attacks must be a hazardous and compromise over the network. This leads to the network disruptions over the network. Using that acquired node the adversary takes the secret keying information from a compromised node, produces a large number of attacker-controlled replicas that share the compromised node’s keying information and ID, and then spreads these replicas throughout the network. An adversary can create as many replica nodes as he/she has the hardware to generate, with a single acquired node.

The replica nodes are controlled by the adversary, but have keying information that allows them to appear like authorized participant nodes 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, by enabling the nodes to encrypt, decrypt, and authenticate all of their communications as if they were the original captured node. Cluster formation, localization, and data aggregation are some common network protocols, undermine by more aggressive attackers. Through these methods, an adversary with a large number of replica nodes can easily defeat the mission of the deployed network.

Our system aim is to provide a straightforward solution to stop replica node attacks, Fast communication between Different Nodes and provides security while their interaction on the basis of different Algorithm.

We also evaluate the performance of our scheme via simulation study using .NET simulator. In particular, we consider two types of replicas for performance evaluation: mobile and static. In case of mobile replicas, we investigate how replica mobility affects the detection capability of our scheme. In case of static (immobile) replicas, the attacker keeps his replica nodes close together and immobile to lessen the chance of speed-based detection. An exploration of the static replica case is useful since this case represents the worst case for detection, and thus we can see how our scheme works in the worst case. The simulation results of both cases show that this scheme very quickly detects mobile replicas with low false positive and negative rates.

The rest of this paper is organized as follows: In section I, we review the Related Work in this area. In Section II, we review System Architecture of the project; then, in Section III, we provide our system's working; Section IV presents Advantages of system; in section V, some real life applications of our system are given; section VI is of limitations of system; section VII is Expected results in which we predicts the expected results; finally, conclusions and possible future work to our research are presented in Section VIII.

The robotics made it possible to develop a variety of new architectures for autonomous wireless networks of sensors. Enabling the nodes to encrypt, decrypt, and authenticate all of their communications as if they were the original captured node. We propose a novel mobile replica detection scheme based on the Sequential hypothesis Test (SHT).Sensor network architectures could be used for a variety of applications including intruder detection, border monitoring, and military patrols. In potentially hostile environments, the security of unattended mobile nodes is extremely critical. It will first describe the detection accuracy of our proposed scheme and then present attack scenarios to break this scheme and a defense strategy

II .RELATED WORK

In this section, first stating the threat model and the network considerations for our proposed system and then elaborate the attacker models used to evaluate our approach.

The existing detection schemes can be classified as centralized Approaches and distributed approaches.

Centralized Detection Approaches- The schemes in assume a central base station to conduct the detection. Cholet al. [3] proposed to detect the replica nodes by set. The network is divided into disjoint sub regions. A header node is enumerated to report the member list to the base station in each sub region. The reports from the entire header nodes are computed by set.The intersection of two sets are checked; any nonempty intersection implies the existence of the replica sensor node. Brooks et al. [4] proposed a centralized scheme to detect replication attacks by using random key redistribution. Every sensor node should report the usage of its keys. If the usage of some key exceeded the threshold, then the sensor node was identified to be suspicious. Ho et al. presented a SPRT method for replica detection in mobile sensor networks, in which the base station checks whether the speeds of the mobile sensor nodes exceed the threshold. Based on a state-of-the-art signal processing technique, compressed sensing, Yu et al. proposed CSI to detect replication attacks.

Distributed Detection Approaches- In distributed approaches, the replication attacks detection is conducted by reporting the location claim messages to randomly chosen witness nodes in the network. Paradoxes of the location claims indicate the detection of replication attacks. To further improve the detection probability, Conti et al. proposed RED scheme, in which a random seed was shared and upgraded in the network. The same random seed and the same pseudo random function result in the same witness node chosen by replica nodes and the compromised node.

RELATED WORK

INPUT

Input: location information L and time information T

OUTPUT

Output: accept the hypothesis H0 or H1

5.1.2 PROCESS

```
Initialization: n = 0, Wn = 0
cur loc = L
cur time = T
if n > 0 then
compute T0(n) and T1(n)
compute speed o from cur loc and prev loc, cur time and prev time
if o > Vmax then
Wn = Wn + 1
end if
if Wn >= T1(n)then
accept the hypothesis H1 and terminate the test
end if
if Wn <= T0(n)then
initialize and Wn to 0 and accept the hypothesis H0
return;
end if
end if
n = n + 1
prevloc = curloc
prevtime = curtime
```

COMPLEXITY

We now analyze the time complexity of the Sequential Probability ratio test.

$O(n^2 \log n)$.

III .TEMPLATE MATCHING ALGORITHM

Working of algorithm is shown in *Fig. 2.*

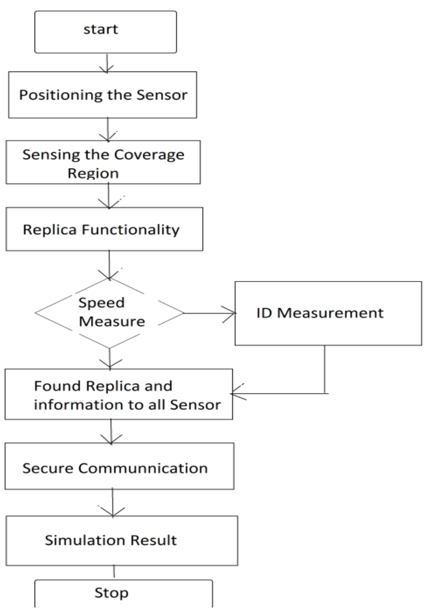

Fig.2. Algorithm Flowchart

This section presents the details of our technique to detect replica node attacks in mobile sensor networks. Defining "random trip", a generic mobility model for independent mobiles that contains as special cases: the random waypoint on convex or non convex domains, random walk with reflection or wrapping, city section, space graph and other models. A sensor node is regarded as being replicated in static sensor network, if it is placed in more than one location. Propose a mobile replica detection scheme by leveraging this intuition. The scheme is based on the Sequential Probability Ratio Test which is a statistical decision process. The SPRT can be thought of as one dimensional random walk with the lower and upper limits. 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. The lower and upper limits can be configured to be associated with speeds less than and in excess of Vmax, respectively. To apply the SPRT to the mobile replica detection problem as follows: Each time a mobile sensor node moves to a new location, each of its neighbors asks 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. Fig. Detection of attacker nodes I also assume that the base station is a trusted entity. This is a reasonable assumption in mobile sensor networks, because the network operator collects all sensor data and can typically control the nodes' operation through the base station. Thus, the basic mission of the sensor network is already completely undermined if the base station is compromised. Each time mobile node's speed exceeds (respectively, remains below) V max, it will expedite the random walk to hit or cross the upper (respectively, lower) 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.

IV. System Architecture

We define a mobile replica node u0 as a node having the same ID and secret keying materials as a mobile node u. An adversary creates replica node u0 as follows: He first compromises node u and extracts all secret keying materials from it. Then, he prepares a new node u0, sets the ID of u0 to the same as u, and loads u's secret keying materials into u0. There may be multiple replicas of u, e.g., u0 1; u0 2; . . . , and there may be multiple compromised and replicated nodes. Our goal is to detect the fact that both u and u0 (or u01; u02; . .)Operate as separate entities with the same identity and keys

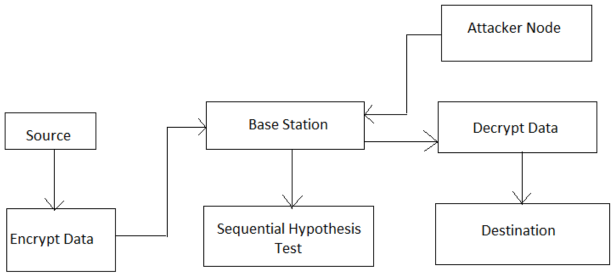

Fig.3. Architecture of Replica Detection System

Module Description

Every sensor node gets secret keying materials for generating digital signatures before deployment. We will use an identity-based public key scheme. It has been demonstrated that public key operations can be efficiently implemented in static sensor devices; most replica detection schemes in static sensor networks employ identity-based public key signatures. Mobile sensor devices are generally more powerful than static ones in terms of battery power, due to the fact that the mobile sensor node consumes a lot of energy to move. Additionally, for public key operations the energy consumption due to movement is known to be substantially larger.

Neighbor Node

A two-dimensional mobile sensor network considered by this module where sensor nodes freely move throughout the network. It means that every mobile sensor node has physically limited movement by the system-configured maximum speed, Vmax. This communication model is common in the current generation of sensor networks. Every mobile sensor node is able to obtain its distance information. And it also assumes that the nodes in the mobile sensor network communicate with a base station. On the basis of distance and range of network sensor node can detect the neighbor node**.**

DATA COMMUNICATION

For each instance of time a mobile sensor node moves to a new location, so its in dynamic in nature and first discovers its set of neighboring nodes, time and location can considers both randomly generated. All direct communication links between sensor nodes are bidirectional. The data was to send one node to another node for normal data communication to communicate at particular node it will send encryption and decrypted format using cryptography algorithm (RSA). Normal data communication to send one time to the destination but the Attack data communication is send multiple time in same data in different location and different speed**.**

ATTACKER MODELS

This section presents the details using SHT (Sequential Hypothesis Testing), this technique is used for detection of replica node attacks in mobile sensor networks. Speed denote a Bernoulli random variable defined as, S = { 0; if oi _ V_{max}; 1; if oi > V_{max}: } The problem of deciding whether it had been replicated or not can be formulated as a hypothesis testing problem with Null and Alternate hypotheses respectively. Null hypothesis mean V_{max} speed controlled by system configuration, Alternative hypothesis mean V_{max} speed Increased over the system configuration. If the base station receive alternative hypothesis that node was identified attack Node then the base station.

DETECTION MODULE

Each time a mobile sensor node moves to a new location, each of its neighbors asks 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.

SECURITY

In this section, we will first describe the detection accuracy of our proposed scheme and then present attack scenarios to break this scheme and a defence strategy we propose to limit these attacks. We will show that the attacker's gain is substantially limited by the defence strategy at the end.

PERFORMANCE

Now analyze the performance of our scheme in terms of computation, communication, and storage overheads.

COMMUNICATION OVERHEAD

We first describe how many observations on an average are required for the base station to make a decision that whether a node has been replicated or not. Then, we will present the communication overhead of our scheme.

COMPUTATION AND STORAGE OVERHEAD

To define computation and claim storage overhead as the average number of public key signing and verification operations per node and the average number of claims that needs to be stored by a node, respectively. Each time a mobile node receives B claim requests on an average at a location, it needs to perform B signature generation operations. Similarly, each time a mobile node sends B claim requests on an average at a location, it needs to verify up to B signatures. In order to perform the SPRT, the base station stores location claims whereas the sensor nodes do not need to keep its own or other nodes' claims. Thus, we only need to compute the number of claims that are stored by the base station. A sample is obtained from two consecutive location claims of node U, in case of SPRT. During an overflow, the node could stop the protocol, or drop packets to free memory. To understand what type of impact this scenario might have on the detection capability of the protocol itself it is very important. To summarize the above considerations with the general requirement that the overhead generated by the protocol should be small, that it should be sustainable by the WSN as a whole, and almost evenly shared among the nodes. every node that forwards a position claim should also perform signature verification and store the forwarded messages. As analyzed,in every line-segment includes O(√n) nodes and every node stores O(√n) location claims. It must be pointed out that this memory requirement could be impractical in real networks with thousands of nodes.

V .SYSTEM WORKING

A. Working of system:

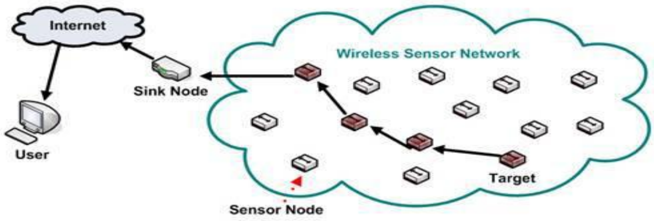

Fig.4.Working of replica node detection system

To apply the SPRT to the mobile replica detection problem as follows: Each time a mobile sensor node moves to a new location, each of its neighbors asks 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.

I also assume that the base station is a trusted entity. This is a reasonable assumption in mobile sensor networks, because the network operator collects all sensor data and can typically control the nodes' operation through the base station. Thus, the basic mission of the sensor network is already completely undermined if the base station is compromised.Each time mobile node's speed exceeds (respectively, remains below) V max, it will expedite the random walk to hit or cross the upper (respectively, lower) 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.

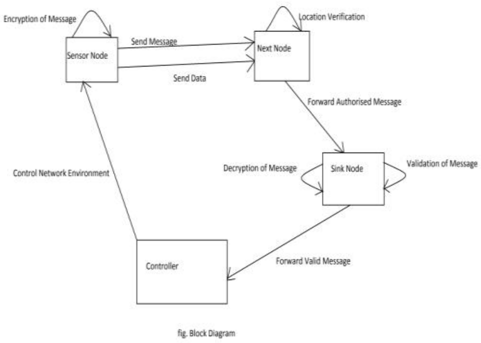

Fig.4. Block of replica node detection system

We are concerned with the design of protocols for WSNs used to close the loop between plants and controllers, see Fig. 9.1. The nodes connected to the plants take state information and transmit it to the sink via a multi-hop WSN.

The controllers are attached to the sink of the network. The sink must receive packets from the nodes of the plants with a desired probability of success and within a latency constraint demanded by the controllers so that the control decision can be correctly taken. We assume that the communication network must be energy efficient to guarantee a long network lifetime.

VI. Actual Results

In this section, This project is to propose a fast and secure effective mobile replica node detection scheme using the Sequential Hypothesis Test to detect replica node attacks in mobile sensor networks. To the best of our knowledge, this is the first work to reduces the problem of replica node attacks in mobile sensor networks.

We show analytically and through simulation experiments that our system detects mobile replicas in an efficient and robust manner at the cost of reasonable overheads.

ANALYSIS

Test Id	Test Case Description	Input	Output	Expected Output	Result
TC 1	Create Network	Enter No of Nodes	Display Sensor Node	Display Sensor Node	Pass
TC 2	Sensing Range	Enter radius to Sensor Node	Display Sensing Range	Display Sensing Range	Fail
TC 3	Mobility	Assigning Mobility to Node	Display Movement of sensor Node	Display Movement of sensor Node	Pass
TC 4	Pause Time	Enter Pause Time to Node	Node have to pause for given time	Node have to pause for given time	Pass
TC 5	Massaging	Sensor node send massage to neighbor node	Display node and their message	Display node and their message	Pass
TC 6	Communication	Each node communicate with neighbor node	Display Communication of node	Display Communication node	Pass
TC 7	Authentication	Sender node send message to receiver node	Receiver node forward message to controller	Receiver node forward message to controller	Pass
TC 8	Validation	Sensor Node Send Message to Controller	Controller checks accepting valid messages	Controller checks accepting valid messages	Pass
TC 9	Attack	Entering attack	Display attack	Display attack	Pass

		node	node	node	
TC 10	Detecting replica node	Replica node sends message	Nodes are detecting replica node	Nodes are detecting replica node	Pass
TC 11	Detecting replica node	Replica node send message to sink node	Sink node detects replica node	Sink node detects replica node	Fail

VII. CONCLUSION

In this paper, we have implemented a replica detection scheme on the basis of SPRT for mobile sensor networks. Analytical demonstration about the limitations of attacker strategies to shuffle the detection technique is done. In particular, the limitations of a group attack strategy in which the attacker controls the movements of a group of replicas is discussed and presented quantitative analysis of the limit on the amount of time for which a group of replicas can avoid detection and quarantine. In this work, I propose a fast and effective mobile replica node detection scheme using the Sequential Probability Ratio Test.

VIII. REFERENCES

[1] J.-Y.L. Boudec and M. Vojnovi_c, “Perfect Simulation and Stationary of a Class of Mobility Models,” Proc. IEEE INFOCOM, pp. 2743-2754, Mar. 2005.

[2] 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.

[3] M. Conti, R.D. Pietro, L.V. Mancini, and A. Mei, “A Randomized,Efficient, and Distributed Protocol for the Detection of NodeReplication Attacks in Wireless Sensor Networks,” Proc. ACM MobiHoc, pp. 80-89, Sept. 2007.

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

[5] J. Ho, M. Wright, and S.K. Das, “Fast Detection of Replica Node Attacks in Mobile Sensor Networks Using Sequential Analysis,” Proc. IEEE INFOCOM, pp. 1773-1781, Apr. 2009.

[6] J. Ho, D. Liu, M. Wright, and S.K. Das, “Distributed Detection of Replicas with Deployment Knowledge in Wireless Sensor Networks,” Ad Hoc Networks, vol. 7, no. 8, pp. 1476-1488, Nov. 2009.

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

[8] J. Jung, V. Paxon, A.W. Berger, and H. Balakrishnan, “Fast Portscan Detection Using Sequential Hypothesis Testing,” Proc. IEEE Symp. Security and Privacy, pp. 211-225, May 2004.

[9] A. Liu and P. Ning, “TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks,” Proc. Seventh IEEE Int’l Symp. Information Processing in Sensor Networks (IPSN), pp. 245-256, Apr. 2008.

[10] S. PalChaudhuri, J.-Y.L. Boudec, and M. Vojnovi_c, “Perfect Simulations for Random Trip Mobility Models,” Proc. 38th Ann.Simulation Symp., Apr. 2005.

AUTHORS

Shirish Kapase S.
Computer Department,
Shri Chattrapati Shivaji College of Engineering
Rahuri Factory, Ahmednagar, India
shirishkapase@outlook.com

Jagdish Bodke V.
Computer Department,
Shri Chattrapati Shivaji College of Engineering
Rahuri Factory, Ahmednagar, India
jagdishbodke220@gmail.com

Sunny Gaikwad K.
Computer Department,
Shri Chattrapati Shivaji College of Engineering
Rahuri Factory, Ahmednagar, India
sunnygaikwad65@gmail.com

Sadashiv Shinde P.
Computer Department,
Shri Chattrapati Shivaji College of Engineering
Rahuri Factory, Ahmednagar, India
sada.shinde83@gmail.com

Avinash Gavhane D.
Computer Department,
Shri Chattrapati Shivaji College of Engineering
Rahuri Factory, Ahmednagar, India
avinashgavhane@gmail.com

Prof. Dighe M.S. (Guide)
H.O.D of Computer Department,
Shri Chattrapati Shivaji College of Engineering
Rahuri Factory, Ahmednagar, India