# FAST DETECTION OF REPLICA NODE IN MOBILE SENSOR NETWORK

**Abhishek Anand[1], Venu Gopal[2], Nilesh Keni[3] ,Nilesh Madke[4]**

*[1] Abhishek A,Student of B.E, Dept. of computer Engineering,ISBM SOT,University of Pune,Pune,India.*
*[2]Venu G,Student of B.E, Dept. of computer Engineering,ISBM SOT,University of Pune,Pune,India.*
*[3] Nilesh Keni,Student of B.E, Dept. of computer Engineering,ISBM SOT,University of Pune,Pune,India*
*[4]Nilesh Madke,A.Prof of B.E, Dept. of computer Engineering,ISBM SOT,University of Pune,Pune,India.*

---

**Abstract -** *Due to* unattended nature of wireless sensor networks leads to mobile replica node attack. An adversary can capture and compromise sensor nodes, make replicas of them, and then mount a variety of attacks with these replicas. These replica node attacks are dangerous because they allow the attacker to leverage the compromise of a few nodes to exert control over much of the network. Previous works on replica detection rely on fixed sensor locations and hence do not work in mobile sensor networks. The proposed work is a fast and effective mobile replica node detection scheme using the Sequential Probability Ratio Test.

***Key Words***: Wireless Sensor Network (WSN), Mobile Sensor Network, Static Sensor Network, Mobile Sensor node, Probability Ratio Test (SPRT).

## 1.INTRODUCTION

Security researchers have long recognized that wireless Sensor networks, with low-resource nodes that are typically left unattended and meant to be self-organizing, are potentially vulnerable to a wide range of attacks. Cryptographic protocols can prevent some attacks, such as by authenticating packets at each hop to ensure that they originate from legitimate nodes[1]. However, an attacker can still physically capture sensor nodes, extract their cryptographic keying material, and modify their code to behave maliciously. He can also remotely compromise nodes by injecting malicious code via the exploit of certain types of software vulnerabilities With a small subset of nodes compromised through either approach, the attacker can launch a number of damaging attacks.

To overcome these drawbacks, we propose a Distributed detection scheme to identify and block mobile Malicious nodes by leveraging the Sequential Probability Ratio Test (SPRT). Our scheme is designed to quickly detect and revoke mobile malicious nodes in a fully distributed manner We leverage the intuition that immobile sensor nodes appear to be present around their neighbor nodes and communicate with them regularly. We describe how we embed this intuition into the SPRT so that neighbors can detect and block nodes that are silent unusually often.

## 2.NETWORK MODEL

We investigate attacks and defenses in a static (immobile) sensor network in which sensor nodes are fixed to their locations after deployment. We also assume bidirectional communication links, such that any pair of nodes that can communicate can both send and receive from each other. Moreover, we assume that sensor nodes are deployed in an automated manner[3]. In an automated deployment, an aircraft or mobile robot randomly scatters many sensor nodes over the field.

Finally, we assume that the system is using some form of trace back or local misbehavior detection. Although not necessary for our scheme to detect

mobile nodes, the attacker does not need to use mobile nodes if a scheme like this is not in place to block static malicious nodes.

### 3.ATTACKER MODELS

However, we place some limits on the ability of the adversary to compromise nodes. We note that if the adversary can compromise major fraction nodes of the network, he will not need nor benefit much from the deployment of replicas. To amplify his effectiveness, the adversary can also launch a replica node attack, which is the subject of our Investigation. We assume that the adversary can produce many replica nodes and that they will be accepted as a legitimate part of the network. We also assume that the Attacker attempts to employ as many replicas of one or more compromised sensor nodes in the network as will be effective for his attacks. The attacker can allow his replica nodes to randomly move or he could move his replica nodes in different patterns in an attempt to frustrate our proposed scheme.

### 4. MOBILE REPLICA DETECTION USING SEQUENTIAL PROBABILITY RATIO TEST

This section presents the details of our technique to detect replica node attacks in mobile sensor networks. In static sensor networks, a sensor node is regarded as being replicated if it is placed in more than one location. If nodes are moving around in network, however, this technique does not work, because a benign mobile node would be treated as a replica due to its continuous change in location Fortunately, mobility provides us with a clue to help resolve the mobile replica detection problem [2].

We propose a mobile replica detection scheme by leveraging this intuition. Our scheme is based on the Sequential Probability Ratio Test which is a statistical decision process.[3] Hence, we must use some other technique to detect replica nodes in mobile sensor networks. Fortunately, mobility provides us with a clue to help resolve the mobile replica detection problem.

### 5.Literature Survey

In this we will discuss about the existing system and their drawbacks and proposed system its advantages.

### 5.1 Static Sensor Network.(Existing System)[1]:

"Static sensor network is a set of sensors which are stable at on place and sense the conditions activities[1]."

In static sensor network all sensor nodes are at x position an having x difference between them[1]. They can pass message to the controller by communicate with each other.

### 5.2 Attacks in static Sensor network[1]:

For Intruder it's easy to find the location of Sensor.Create replica node(duplicate node) sends fake messages. -Intruder uses more bandwidth. Due to this attack on sensor network easy to attack and disturb the sensor network.It leads to breaking the security of the sensor network.

Unsecure Communication[2]: -Receiver node checks the location of sender and communicates with other neighbor nodes. -More chances of fake messages as true due to x distance. Controller gets busy in reading fake messages.

### 5.3 Mobile Sensor Network[2]:

"Mobile Sensor Network is network which has sensor nodes with dynamic location".

In mobile Sensor network sensor nodes are having dynamic location. Node difference between two nodes is not fixed. Each node is having system assigned speed for its dynamic movement. Due to this dynamic location it's not easy to intruder to attack on sensornetwork.

### 5.4 Attack in Mobile sensor Network[3]:

It's not easy to intruder to attack on Mobile sensor network due to the dynamic location of the sensor node, because intruder not able to catch the location speed of the moving sensor node. So there are rare chances of attack on Mobile sensor Network. Secure Communication In mobile sensor network if Intruder tries to attack on network then it will be detected in Location Verification process.Also if he sends the fake messages they also detected by using different technique.

-If intruder tries to send fake messages then it will be detected in Location Verification process. -If fake message get detected then it is dropped.

### 5.5 Detection using sequential analysis[4]:

Due to the unattended nature of wireless sensornetworks, an adversary can capture and compromise sensor nodes, generate replicas of those nodes, and mount a variety of attacks with the replicas he injects into the network. These attacks are dangerous because they allow the attacker to leverage the compromise of a few nodes to exert control over much of the network.

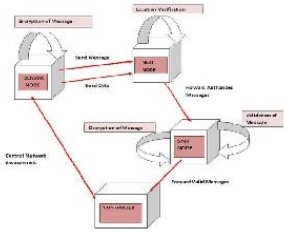
### 5.6 Sequential Hypothesis Testing Based Approach[5]:

In wireless sensor networks, replica node attacks are very dangerous because the attacker can compromise a single node and generate as many replicas of the compromised node as he wants, and then exploit these replicas to disrupt the normal operations of sensor networks. Several schemes have been proposed to detect replica node attacks in sensor networks. The evaluation results demonstrate that it accomplishes robust replica cluster detection capability[5].

### 5.7 Probability Ratio Testing[4]:

In wireless sensor networks(WSN), there are many nodes and they are unattended so an adversary can easily capture and compromise the sensor nodes and take secret key from the nodes then make many replicas(duplicate) of them. To avoid this node compromised attack we use sequential probability ratio testing (SPRT). In[4] literature several compromised node detection works well in static sensor networks and they do not work well in mobile sensor networks. Using SPRT we detect the compromised node in mobile sensor networks. This paper show analytically and through ns2 simulation experiments that the scheme detects duplicate node in an efficient and robust manner[4].

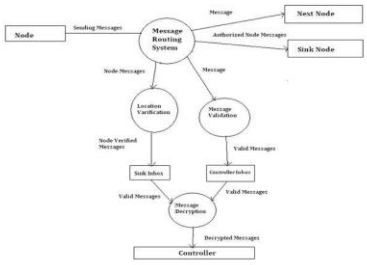
## 6. SYSTEM DESIGN



## 7 Analysis Model

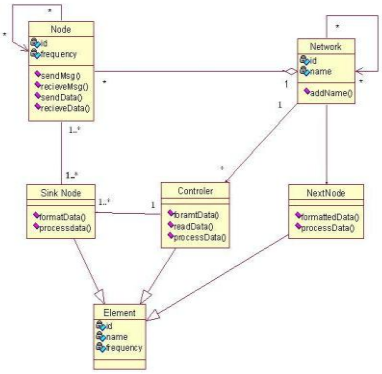
### 7.1 DATA FLOW DIAGRAM

DFD Level-0

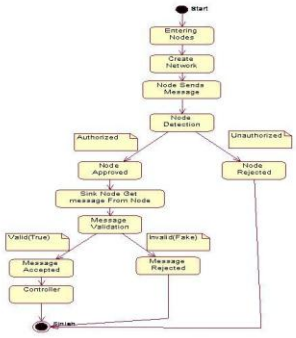


DFD Level 1

### 7.2 Class Diagram




### 7.3 State Transition Diagram




## 8.RELATED WORKS

We first describe a number of research works on static node compromise detection in wireless sensor networks. Software attestation based schemes have been proposed to detect the subverted software modules of sensor nodes. Specifically, the base station checks whether the flash image codes have been maliciously altered by performing attestation randomly chosen portions of image codes.

In a sensor node's flash image codes are attested by its neighbors. However, all these schemes

require each sensor to be periodically attested and thus incur a large overhead in terms of communication and computation. Our static node compromise detection scheme does not require periodic attestation but one-time attestations against untrustworthy zones. Proposed information theoretic frameworks for trust evaluation.

## 9.CONCLUSION AND FUTUREWORK

We have proposed a replication detection scheme for mobile sensor networks based on the SPRT. We have analytically demonstrated the limitations of attacker strategies to evade our detection technique. In particular, we first showed the limitations of a group attack strategy in which the attacker controls the movements of a group of replicas. We presented quantitative analysis of the limit on the amount of time for which a group of replicas can avoid detection and quarantine. We also modeled the interaction between the detector and the adversary as a repeated game and found Nash equilibrium.We Performed simulations of the scheme under a random Movement attack strategy in which the attacker lets replicas randomly move in the network and under a static placement attack strategy in which he keeps his replicas from moving to best evade detection. The results of these simulations show that our scheme quickly detects mobile replicas with a small number of location claims against either strategy and also apply data structure algorithm for effective communication.

## ACKNOWLEDGEMENT

Our thanks to first and foremost I offer my sincerest gratitude to my college ISB&M SOT, and my department of computer engineering which has provided the support and equipment. Which I have needed to complete my work. I extend my heartfelt gratitude to my guide, Mr NILESH MADKE, who has supported me throughout our research with their patience and knowledge

## 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 Node Replication 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: Enabling 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.