Energy Efficient Mobile Replica Detection in Wireless Sensor Network based on Modified Sequential Probability Ratio Test

Snehal Y. Kulkarni[†] and Nalini A. Mhetre[††],

Smt. Kashibai Navale College of Engineering, Pune , University of Pune, India

Summary-
In wireless sensor network, an attacker can capture sensor nodes and can compromise sensor nodes. Then would create duplicate nodes and built up various attacks using duplicate nodes, inserts into the network. This is happened because of unattended nature of wireless sensor network. These attacks helps attacker to control few more nodes to have control over the network. There are many node replication detection methods which have been used to secure from attacks in the sensor network where nodes are static. These methods are dependent on fixed location of sensors and hence do not works for sensor network where nodes are mobile. In wireless sensor network where sensor node are moving i.e. mobile, for node replication detection proposed system is used where attacks are detected quickly. In Modified Sequential Probability Ratio Test (MSPRT) method basic idea is used that mobile node never have more speed than system speed. Nodes undergoes the signature test, communication range test and packet sent test at node communication level so that system can detect node replication in effective and robust manner.

Keywords
Mobile sensor network, security, sequential analysis, replicated mobile node.

1. Introduction

The *wireless sensor network* is a collection of nodes organized into a cooperative network. Each node consists of processing capability may contain multiple types of memory, have a RF transceiver, have a power source, and accommodate various sensors and actuators. In wireless sensor network if sensor nodes are at fixed location, it called as *static wireless sensor network* and sensor nodes are *static nodes*. If sensor nodes are moving, it is called as *mobile sensor network* and sensor nodes are *mobile nodes*. Mobile nodes are small robots which are having capacity of sensing, wireless communication, and movement. Robomote is a robot that functions as a single mobile node in a mobile sensor network. It is hardware and software design. Mobile nodes are useful for application such that sensor deployment, adaptive sampling, network repair and event detection [2]. The security of mobile nodes is serious. The attacker is able to obtain and extract information of mobile node, and attacker uses this information to introduce false data, disturb network operations, and have control over network communication. In this situation attacker takes secret information from compromised node and creates greater number of attacker –controlled replica nodes which share the node's secret information and identity. The attacker spreads these replicas over entire network. With the help of single affected node, the attacker creates many replica nodes.

The requirement for mobile node is that node has software and key information to communicate in the network. The attacker – controlled nodes have secret information that allow them to appear like authorized element or member of the network. Procedures for secure sensor network communication would allow replica nodes to create shared keys with other nodes and the base station, enabling the nodes to encrypt, decrypt, and authenticate their communications as they were the collected from captured node. The attacker can use this insider position in many ways. For example attacker can monitor network traffic as per his requirement. Also he could jam genuine signals from authorized nodes or inserts fake data to corrupt the sensors' monitoring operation. A more destructive attacker could use common network protocols, including cluster information, localization and data aggregation, which cause continuous disruption to network operation. Through these methods attacker who is having large number of replica nodes can easily beat the main purpose of the deployed network. Hardware solution is tamper resistant which easy to implement but it is time consuming method.

For static sensor network, many different node replication attack detection schemes are used. The primary method used by these schemes is to have node creates report of location claims which identifies its position and attempt to detect conflicting reports that signal one node in multiple locations. This approach requires fixed node location. Thus main challenge is to design a scheme which traces replicated mobile nodes in effective and robust manner for mobile sensor network [4][5]. In [1] algorithm is proposed used to identify the replica node in mobile sensor network. The given algorithm uses concept of sequential analysis. Sequential analysis is different from classical analysis in which sample size is not fixed. The number of samples is treated as a random variable in the sequential analysis. This feature makes the test reach a decision much earlier than the classical hypothesis testing. In [1] samples of

Manuscript received August 5, 2014
Manuscript revised August 20, 2014

location claim for each node are sent to base station due to which average no. of claims required to detect a node as replica are more.
In the proposed MSPRT system basic concept which used is that an original mobile node is moving at speed less than the system maximum speed. At node communication level, signature test, communication range test and packet sent test are performed to find malicious nodes. The non-malicious nodes are considered for further testing. If mobile node's speed is greater than maximum speed, it is possible that at least two nodes with same identity are present in the network. The sequential analysis using probability ratio test on every mobile node using null hypothesis that mobile node has not been duplicated and an alternate hypothesis that it has duplicated nodes is performed. With the help of probability and hypothesis replicated node is detected. The proposed system detects which traces replicated mobile nodes with zero false positives and negatives. This is because the probability ratio test with sequential analysis is proven to be the best mechanism in terms of number of observations to reach a decision among all sequential and non – sequential decision processes.

2. Preliminaries

In this section, problem statement, assumptions for proposed system, basic requirements of the proposed scheme are described.

2.1 Problem Statement:

Here, problem of detecting mobile node replication attack is tackled. If mobile node is *x* then its replica node is *x*'. Mobile node *x*' having secret information and identity same as mobile node x. An attacker creates replica node *x*' as follows: He first captures the node and extracts all secret information from it. Then he prepares new node *x*', sets identity same node *x* and loads secret information of node *x* into node *x*'. There may be multiple captured and duplicated nodes.
Main goal is to detect node *x* and *x*' (or its multiple replicas) as separate entities with same identity and keys.

2.2 Network Assumptions:

Consider a two-dimensional *mobile sensor network* where sensor nodes freely travel in the entire network. Also assume that every mobile sensor node's movement is physically limited by the system's maximum speed. Also assume that all direct communication links between sensor nodes are bidirectional. It is assume that every mobile node is having capability of finding its location and also validating the locations of its neighboring nodes. It is also assume that the mobile nodes in the network communicate with a base station. The base station is static as long as the nodes have a way to communicate reliably to the base station on a regular basis.

2.3. Adversary Model :

It is assumed that an attacker may have full control over set of sensor nodes and enabling him to build up various kinds of attacks. For example, he can introduce false data into network and disturb control protocol. Moreover he can launch denial of service attacks by squeezing the signals from authorized nodes. Also assumed that attacker try to use as many duplicated nodes of original nodes in the network as will be effective for his attack. Also it is assumed that an original and replica node (or nodes) follows the Random Waypoint Mobility (RWM) model when they are moving in the network. Note that attacker could move his duplicated nodes in different patterns to discourage the scheme.

2.4 Robomote: Enabling Mobility

This is hardware design of the mobile sensor node. The robomote is designed to be compatible with the popular mote/tinyos platform. The robomote (Fig. 1and Fig. 2) consists of an Atmel 8535 microcontroller. This is an 8-bit AVR RISC MCU with 8k bytes of In-system programmable flash along with 512 bytes of EEPROM and 512 bytes of Internal SRAM. The microcontroller also incorporates various desirable features like programmable sleep modes and reprogramming capability. It has two motors, compass for heading and IR sensors. Each of these is described in further detail below. The robomote is complete with the addition of a mote. The mote is used as the master. All basic functionality of the robomote is exported to the mote via modular interfaces [2].

2.5 Mobility Model:

Several mobility models have been used to evaluate performance of methods which are used for detection of node replication attacks in wireless sensor network. Usually the Random Waypoint Mobility (RWM) is used. The Random waypoint model is a random-based mobility model. The mobility model is designed to describe the movement pattern of mobile nodes, and how their location. Mobility models are used for simulation purposes when new network protocols are evaluated. In the Random Waypoint Mobility model, each node moves to location which chosen randomly with speed. The speed is randomly selected with the help of a predefined minimum and maximum speed. Once reached to location, node stays at location for predefined pause time. Once pause time is

completed, it then randomly chooses another and moved to that location. The process of random movement is continuous for simulation period. When the Random Waypoint Mobility model is used in simulation, it takes some time for the probability distribution of the movement of nodes to converge to a steady state distribution after the start of simulation. Furthermore, the convergence time is changed in accordance with the parameters of the mobility model and the performance of the network varies with the convergence time. Thus, it is hard to find a steady-state distribution in the RWM model.

To resolve this problem, the Random Trip Mobility (RTM) model is proposed as a generic framework for finding the steady-state distribution of any mobility model based on random movement. It is believed that the performance of the scheme will be more accurately evaluated under a mobility model with a steady-state distribution; accordingly, Random Waypoint Mobility model with steady-state distribution obtained from Random Trip Mobility model will be used. In proposed system Random Waypoint Mobility model is used with steady – state distribution provided by the Random Trip Mobility (RTM) model [6][7].

3. Mathematical Model:

Consider simple application of faulty sensor detection. The fact to be considered is the faulty sensor devices likely generate more inaccurate sensory data than non-faulty ones.

Let,
di = data produced by sensor S
Yi = Bernoulli Random Variable, which written as

$$Yi = \begin{cases} 0, & \text{if di is accurate} \\ 1, & \text{if di is inaccurate} \end{cases} \quad \text{----------[1]}$$

The success probability σ of Bernoulli random variable is defined as ,

$\sigma = Pr(Yi = 1) = 1 - Pr(Yi = 0)$ ---------- **[2]**

If $\sigma \leq \sigma'$ then sensor S is not faulty
If $\sigma > \sigma'$ then sensor S is faulty.
Where σ' = preset threshold.

This can be formulated as a hypothesis testing problem.
Let,
H0 = null hypothesis
H1 = alternate hypothesis
Then,
If $\sigma \leq \sigma'$ → H0
If $\sigma > \sigma'$ → H1 ---------- **[3]**

In this problem an appropriate sampling strategy to be devised in order to prevent hypothesis testing form leading to a wrong decision.

Thus reformulation of equation [3] is
If $\sigma \leq \sigma 0$ → H0
If $\sigma > \sigma 1$ → H1 ---------- **[4]**
Such that $\sigma 0 < \sigma 1$

Let's denote

H0 = Null hypothesis i.e. S is non-faulty
H1= Alternate hypothesis i.e. S is faulty
n = observed samples

Log probability ratio on n samples

$$Ln = \ln \frac{Pr[Y1,\ldots,Yn \mid H1]}{Pr[Y1,\ldots,Yn \mid Ho]} \quad \text{--------- [5]}$$

Assume that conditional on the hypothesis is Hj, the random variables Yi | Hj , i=1,2,…… are independent and identically distributed then

$$Ln = \ln \frac{\prod_{i=1}^{n} Pr[Yi \mid H1]}{\prod_{i=1}^{n} Pr[Yi \mid H0]} \quad \text{---------- [6]}$$

This can be written as

$$Ln = \sum_{i=1}^{n} \ln \frac{Pr[Yi \mid H1]}{Pr[Yi \mid H0]} \quad \text{------ [7]}$$

Let,
ω_n = no. of times that Yi =1 in the n samples
Equation [7] can be rewrite as

$$Ln = \omega n \ln \frac{\sigma 1}{\sigma 0} + (n - \omega n) \ln \frac{1-\sigma 1}{1-\sigma 0} \quad \text{----- [8]}$$

Where , $\sigma 0 = Pr[Ri = 1 \mid H0]$
$\sigma 1 = Pr[Ri = 1 \mid H1]$

Equation [8] is used to detect faulty sensor device in the network.

Finally, it is to needed to compute how many samples are required on the average for each node to decide whether sensor devices are defective or not.

Since *n* is varied with types of sample, it is treated as a random variable i.e.
n = no. of samples which are tested to find S is defective or not.
count = no. of samples which gives S is defective.
Thus

$$\text{Avg. number of samples} = \frac{n}{count} \quad \text{---------- [9]}$$

Avg. samples gives efficiency of dissertation work.

4. System Architecture of MSPRT:

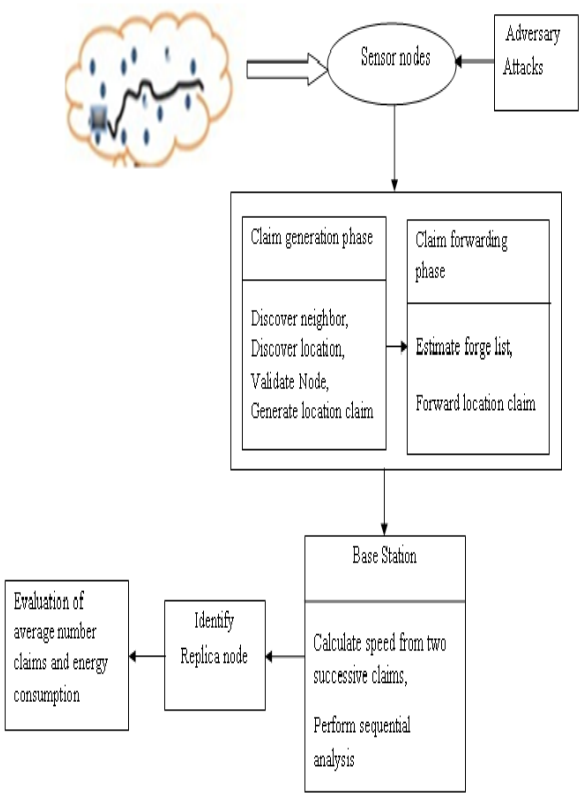


Fig. 1 Architecture of MSPRT

4.1. Claim Generation phase

In Claim Generation phase, each time a sensor node moves to new location and it discovers its location. Then discovers its neighboring node which belongs set of neighboring nodes. Node communication starts with broadcasting HELLO message to neighboring nodes. Every neighboring node asks for location claim by sending current time T to node.

Now node is validated by signature test i.e. neighboring node checks communication signature of node. Node generates signature for communication. This is generated by using node ID, location of node (L), time sent by neighboring node (T).

Also neighboring nodes perform communication range test on node i.e. neighboring nodes check range of node by considering number of hops required for communication. And the last neighboring nodes check number of packets sent by node during communication. If the node is not validated through these tests, it has been discarded from communication and considered as malicious node.

The validated node generates location claim (C) which is combination of location of node (L), ID of node, time sent by neighboring node (T) and signature generated by node. This location claim is sent to neighboring node.

4.2. Claim Forwarding Phase

This phase estimates forge node list based on the signature test, communication test and packets sent test. The neighboring node sends location claims of those nodes that are not available in forge list. The neighboring node forwards location claim (C) to base station at time T_i, and other neighboring nodes forwards location of node at time T_{i+1}, T_{i+2},.. and so on.

4.3. Sequential Probability Ratio Test (SPRT)

Base station receives location claim from neighboring nodes. Base station considers only authenticate location claims for identification of replica node. Authenticate location claims for node is C_1, C_2, C_3, and so on. Base station extracts location information L_i and time information T_i from location claim C_i. Also calculates distance from L_i at time T_i and L_{i+1} at time T_{i+1}, which further defines measured speed (v) as

$$v_i = di / (| T_{i+1} - T_i|)$$

Sequential Probability ratio test which was defined by mathematician *A. Wald* is performed on measured speed by considering different samples of location claim for one node.

The Bernoulli random variable defined as,

$$S_i = \begin{cases} 0, \text{ if } v_i \le V_{max} \\ 1, \text{ if } v_i > V_{max} \end{cases}$$

Where V_{max} = maximum system-configured speed.

This in turns used to define Null hypothesis (H0) and Alternate hypothesis (H1). Where Null hypothesis (H0) indicates that node has not been replicated and alternate hypothesis (H1) indicates that node has been replicated.

These hypotheses used in sequential analysis (which is also called as sequential hypothesis testing) to identify replica node in the network. These hypotheses are calculated from 'n' number of samples for each node which to tested. From these hypotheses log –probability (Ln) has been calculated. This log-probability is tested and then replica node is detected.

The success probability *p* is defined as

$$Pr (S_i = 1) = 1 - Pr (S_i = 0) = p$$

Here define,

H_0 = null hypothesis = hypothesis that node *x* has not been replicated.

H_1 = alternate hypothesis = hypothesis that node *x* has been replicated.

L_n = log probability ratio on *n* samples.

$L_n = ln \{(P(S_1, S_2, S_n | H_1) / (P(S_1, S_2, S_n | H_0)\}$

If Si is independent and identically distributed then L_n as follows,

$$L_n = \sum_{t=1}^{n} \left(ln \frac{P(Si|H1)}{P(Si|H0)} \right)$$

Consider, Ωn = number of times that $S_i = 1$ in the *n* samples

Then, $L_n = \{ \Omega_n \, l_n \, (p_1 / p_0) + (n - \Omega_n) \, l_n \, ([1-p_1] / [1-p_0])$

Where, $p_0 = P(S_i = 1 | H_0)$, $p_1 = P(S_i = 1 | H_1)$

On the basis of log probability ratio L_n, the probability ratio test using sequential analysis for H_0 against H_1 is as follows,

- $L_n \leq l_n \{ b' / (1 - a') \}$: choose H_0 and end the test
- $L_n \geq l_n \{ (1 - b') / a' \}$: choose H_1 and end the test
- $l_n \{ b' / (1 - a') \} < L_n < l_n \{ (1 - b') / a' \}$: continue the test with other observation.

If node *x* is evaluated as trusted node, the base station starts the probability ratio examination using sequential analysis with recently arrived claims from *x*. If, *x* is determined to be replicated, the base station terminates the probability ratio examination on *x* and invalidates all nodes with identity *x* from the network.

5. Simulation Results

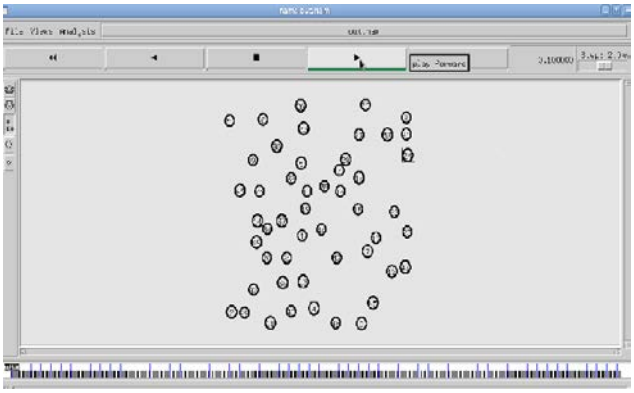


Fig 2. Route Request

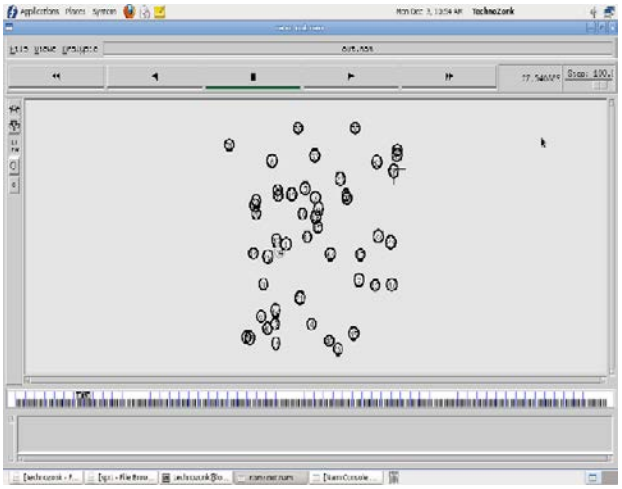


Fig 3. Route Reply

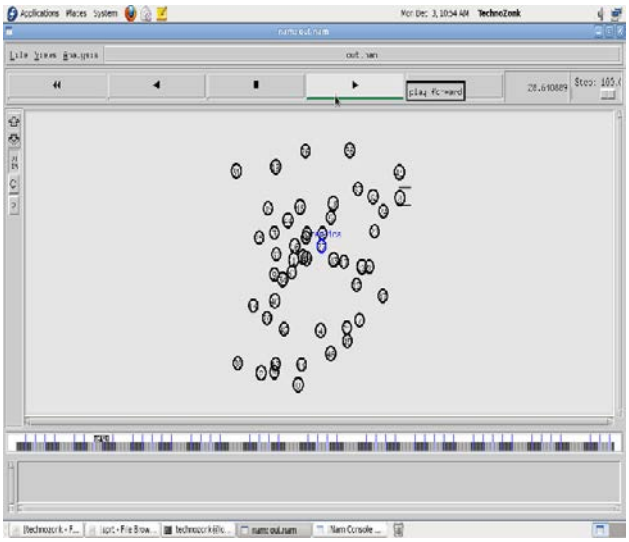


Fig 4: Replicated Mobile Node

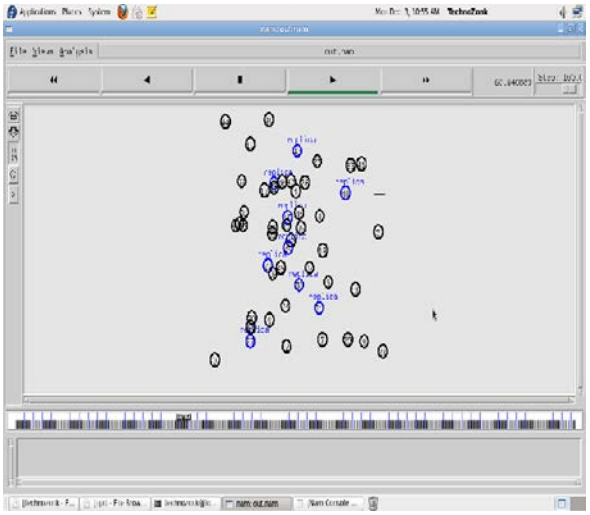
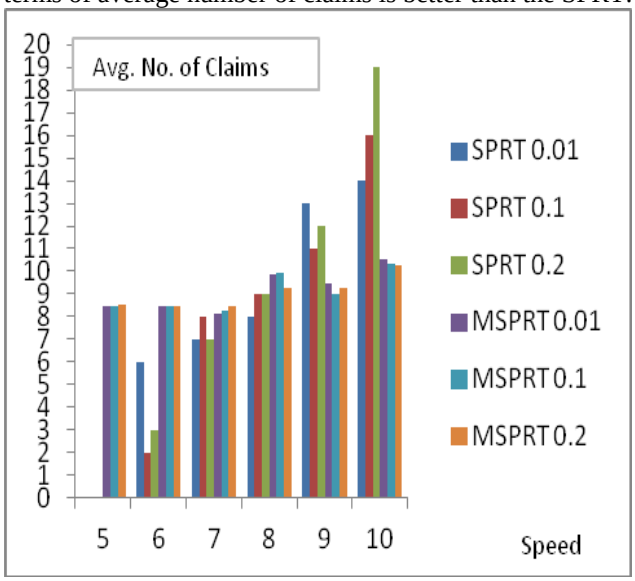


Fig 5: Replicated Mobile Nodes

6. Results

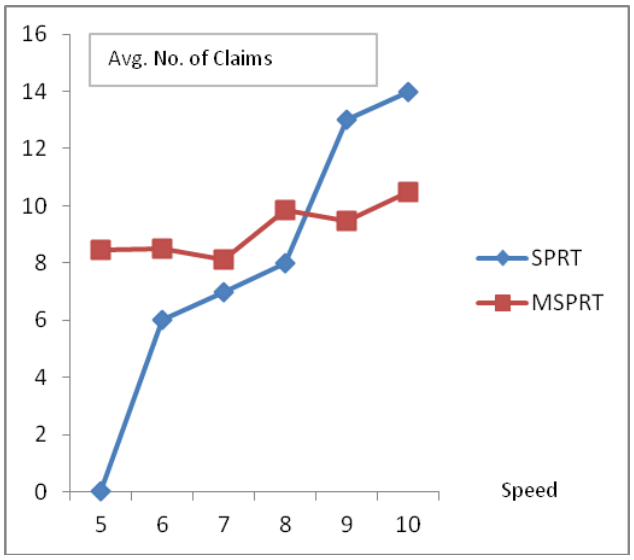
G. 1: Average number of claims Vs Mobility Speed of node for SPRT and MSPRT.

In graph G. 1 it is clear that the performance of MSPRT in terms of average number of claims is better than the SPRT.

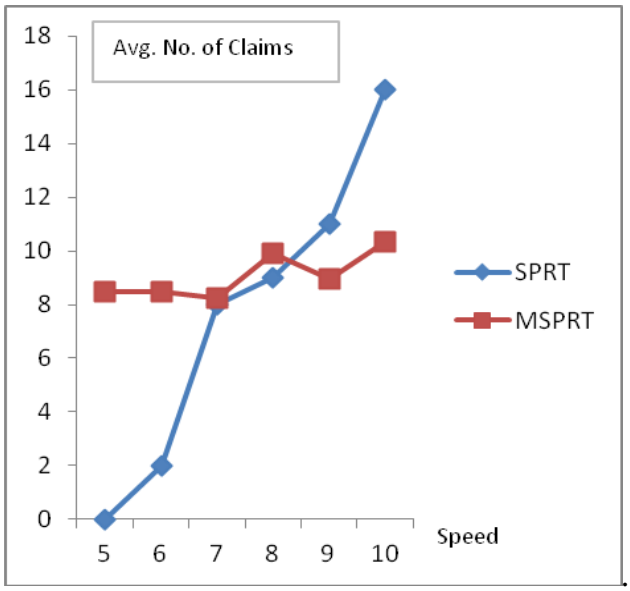


G. 1: Average number of claims Vs Mobility Speed of node for SPRT and MSPRT.

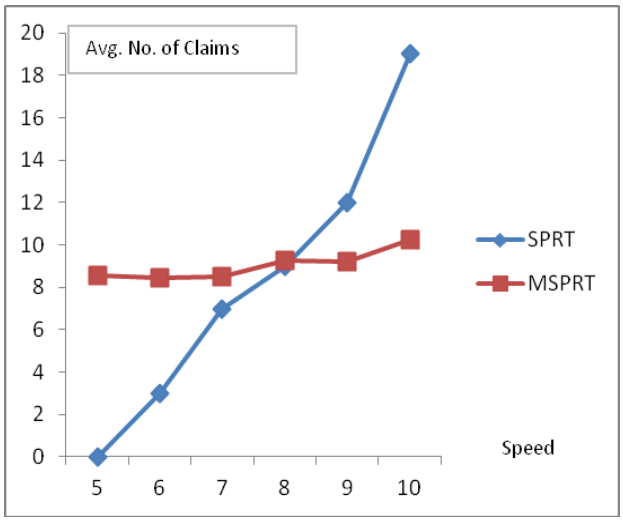
G.2: Average number of claims Vs Mobility Speed of node for SPRT and MSPRT for speed error rate 0.01m/s



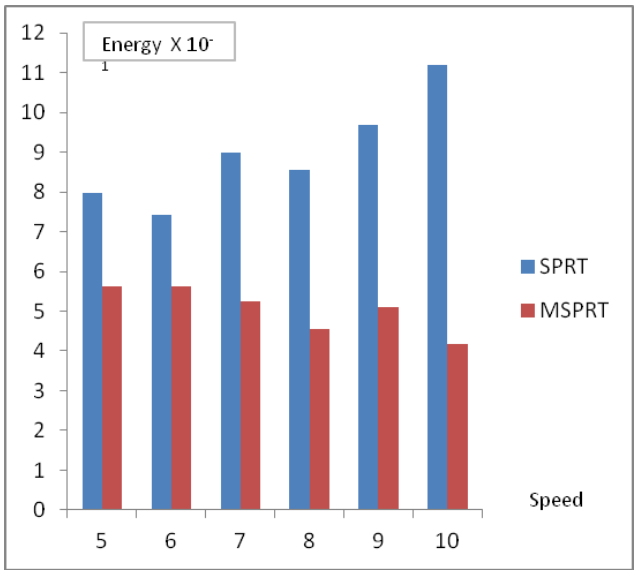
G. 2: Average number of claims Vs Mobility Speed of node for SPRT and MSPRT for error speed rate 0.01m/s



G.3: Average number of claims Vs Mobility Speed of node for SPRT and MSPRT for error speed rate 0.1m/s



G.4: Average number of claims Vs Mobility Speed of node for SPRT and MSPRT for error speed rate 0.2m/s



G.5: Energy Consumption Vs Mobility Speed of node for SPRT and MSPRT

7. Conclusion

The proposed system is centralized approach in which base station is centralized entity. The basic idea used in proposed scheme is that a mobile node never has velocity greater than the maximum velocity of system built up. Using this idea, probability ratio test with sequential analysis is performed to detect mobile node replication attack. Before performing sequential probability ratio test at base station, sensor nodes undergoes signature test, communication range test and packet sent test. The proposed scheme discovers node replication attack with less number of location claims. This centralized approach is efficient than deployment knowledge because deployment knowledge is not suitable for mobile sensor network, since location changes time to time in mobile wireless sensor network. The performance of the scheme is good as compared to the other approaches. The proposed scheme detects the attack faster. The proposed system can detect node replication attack in effective and robust manner.

References

[1] Jun-Won Ho, Matthew Wright, Sajal K. Das, " Fast Detection of Mobile Replica Node Attacks in Wireless Sensor Networks using Sequential Hypothesis Testing" , IEEE Transaction on Mobile Computing Vol 10 No. 6 June 2011, Pg no. 767 – 782

[2] 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

[3] 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.

[4] 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.

[5] B. Parno, A. Perrig, and V.D. Gligor, "Distributed Detection of Node Replication Attacks in Sensor Networks," Proc. IEEE Symp. Security and Privacy, pp. 49-63, May 2005.

[6] 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.

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

[8] D. Boneh and M.K. Franklin. Identity-Based Encryption from the Weil Pairing. In *Advances in Cryptology CRYPTO*, 2001.

Kulkarni Snehal was born in Nasik, India, in 1982. She received the Bachelor in Computer Engineering degree from the University of Pune, Pune in 2004 and the Master in Computer Network degree from the University of Pune, (pursuing). Her research interests include Computer Networking, Computer Graphics, and Data Structure

Nalini Mhetre is working as Assistant Professor in Sinhgad Technical Education Society's Smt. Kashibai Navale College of Engineering, Pune having experience of 12 years. She received the Bachelor in Computer Science and Engineering. She also received Masters in Computer Science and Engineering and Information Technology from University of Pune. Her research interests include Data Structure, Computer Network, Software Testing, Object Oriented Modeling and Design.