ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 1, Issue 10, December 2012

Detection of Mobile Replica Node Attacks in Mobile Sensor Networks Using Speed Measurement Testing

T.Nidharshini, V.Janani

***Abstract*— Wireless sensor networks contains large number of sensor nodes they are deployed in hostile environment so there is no security. An adversary may capture and compromise the sensor node and make replicas of them. The replica nodes are also called duplicate nodes. These replica node attacks are dangerous which leads to eaves dropping in network communication. Replica node detection scheme work well in fixed sensor network and do not work well in mobile sensor network. To detect these replica node attacks, Sequential Probability Ratio Testing (SPRT) that is speed measurement testing method is used. The proposed system shows the problem of sensor node failure. If a sensor node fails because of energy depletion we need to choose alternative sensor for that particular region. Then energy threshold for each sensor will be fixed, if it reaches that threshold it will inform the base station about the death. The base station should route another near-by energy-efficient sensor node to collect sensed data from that particular failed region. This paper show analytically and through ns2 simulation experiments that the scheme detects replica node in an efficient and robust manner.**

***Index Terms*— Replica detection, mobile sensor nodes, SPRT, compromised node.**

I. INTRODUCTION

In wireless sensor networks, sensor nodes are deployed in unattended environment and there is no security. An attacker can easily capture and compromise sensor node [13] and make replicas of them. The replicas nodes are duplicate nodes which are created by an adversary make many replica nodes all having same ID and these replica nodes are controlled by an adversary. Then these fake data are injected into a network which may cause eaves dropping in network communication. The fake data disrupt the network operations in network communication. Several replica node detection schemes have been proposed to defend against in static sensor network and they do not work well in mobile sensor networks where sensors are expected to move.

To detect replica node in mobile sensor network, the proposed system use a new technique called Sequential Probability Ratio Testing (SPRT) [7]. The uncompromised mobile node should never move at the speed in excess of system configured maximum speed. The compromised mobile node measured speeds will be maximum then the system configured speed because two or more nodes with the same identity are present in the network. If the system decides that a node has been replicated based on a single observation, the nodes moving faster than the system configuration speed many false positive errors occurred in speed measurement. If the system decides that a node is benign based on the single observation, the node moving less than the system configuration speed now the high false negative rates occurred. To minimize these false positive and false negative rates, SPRT a hypothesis testing method is used. That can make decisions quickly and accurately.

SPRT is performed on every mobile node using null hypothesis the mobile node has not been replicated and in alternate hypothesis that it has been replicated. Once the alternate hypothesis is accepted the replica nodes will be revoked from the network.

II. NETWORK ENVIRONMENT

The network model diagram for detection of mobile replica node attacks in wireless sensor networks using speed measurement testing is shown in figure1. In order to evaluate the performance of the proposed method, initially the sensor nodes are deployed in hostile environment. After deployment, the base station of each cluster node senses the coverage region. An adversary can capture and compromise sensor node and make replicas [1] of them. These replica node attacks are dangerous attacks because they cause eaves dropping in network communication and disrupt the network operation. To find the mobile replica node the proposed system uses a new technique called Sequential Probability Ratio Testing (SPRT).

In SPRT there are two measurements, speed measurement and ID measurement. 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 as long as, a speed measurement system with a low error rate. On the other hand, replica nodes are in two or more places at the same time.

Manuscript received December 20, 2012.
***T.Nidharshini**, Department of Computer Science and Engineering, Adhiyamaan College of Engineering, Hosur, India.*
***V.Janani**, Department of Computer Science and Engineering, Adhiyamaan College of Engineering, Hosur, India.*

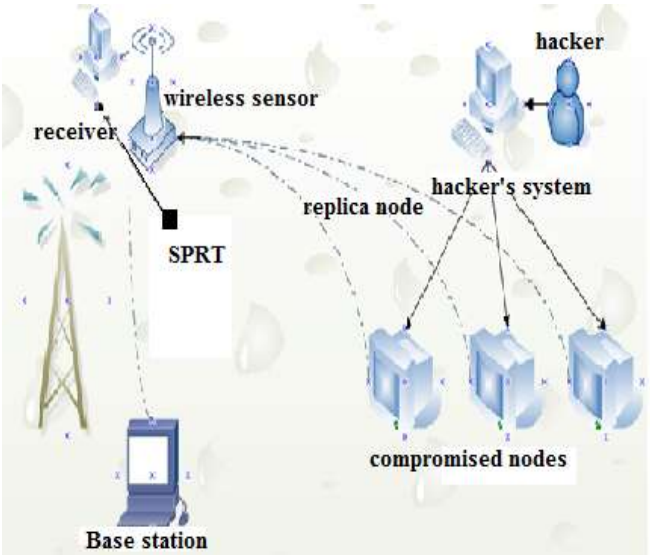

Figure 1: Network model

This makes it appear as if the replicated node is moving much faster than any of the benign nodes, and thus the replica nodes measured speeds will often be over the system-configured maximum speed. Accordingly 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 [4]. Using this speed measurement if replica node is found then the sensor node will send that information to all sensors in network; else another measurement called ID measurement is used.

To minimize these false positives and false negatives, the SPRT, a hypothesis testing [4] method that can make decisions quickly and accurately. 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. In using the SPRT, the occurrence of a speed that is less than or exceeds the system-configured maximum speed will lead to acceptance of the null or alternate hypotheses, respectively. Once the alternate hypothesis is accepted, the replica nodes will be revoked from the network. After finding the replica node it should be revoked from the network and then the secure communication takes place. Using NS2 simulator the performance and efficiency of mobile replica in wireless sensor network using speed measurement is detected.

III. DETECTION OF REPLICA NODE

Replica node attack is a dangerous because they allow the attacker to leverage the compromise of few nodes to exert control over much of network. In static sensor networks replica node detection scheme works well, because the nodes are static so it is possible to detect the additional node which has the same sensor node ID. In mobile sensor networks it is difficult to detect which node is replica because all the nodes are dynamic.

In replica node attack, an adversary may capture the node and take the data into his own sensor. Then he deploys those sensors in to the network for various malicious activities. Replica node attack is a dangerous one since all the replica are having legitimate keys which makes the replica to be an benign node since there is no difference between the benign node and replica in terms of their authentication it is difficult to detect replica. Once the node is compromised the information get leaked adversary may inject false data on the node or modifying the data which is passed between the nodes. So finding the replica node is an important one for protecting the network from various attacks. Protection of sensor networks can be done in two ways: both centralized [3] and distributed approaches are needed and also needed for static sensor networks and wireless sensor networks.

IV. SEQUENTIAL PROBABILITY RATIO TESTING

We propose a fast and effective replica node detection schema using the sequential probability ratio test. The sensor node is compare it to a predefine threshold, if it is more than threshold value, we decide the sensor node has a captured nodes. This simple approach achievers efficient node captures detection capability as long as a threshold value is properly configured. However, it is not easy to configure a proper a threshold value to detect captured nodes. If we set threshold to a high value it is likely that captured nodes bypass the detection. On the contrary if we set threshold to a low value, it is likely that benign nodes can be detected as a captured nodes. We use a scheme for distributed detection of mobile malicious node attacks in mobile sensor networks. The key idea of this scheme is to apply sequential hypothesis testing to discover nodes that are silent for unusually many time periods such nodes are likely to be moving and block them from communicating.

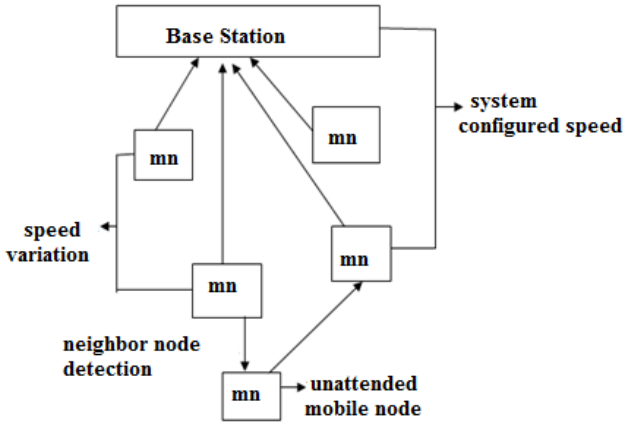

Figure 2: detecting neighbour node

By performing all detection and blocking locally, we keep energy consumption overhead to a minimum and keep the cost of false positive slow after physically capturing and compromising a few sensor nodes attacker can generate many replica node with the same ID and secret keying materials as a compromised nodes and mount a variety of attacks with replica nodes randomized and line selected multicast schemes were proposed to detect replicas in wireless sensor networks. In the randomized multicast scheme [11] every node is required to multicast a single location claim to randomly chosen witness nodes that receives two conflicting location claims for a node

concludes that the node has been replicated and initiates a process to revoke the node.

The line selected multicast [11] scheme reduces the communication overhead of the randomized multicast scheme by having claim relaying node participate in the replica detection and revocation process. 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 as long as we employ a speed measurement system with a low error rate. On the other hand, replica nodes are in two or more places at the same time. This makes it appear as if the replicated node is moving much faster than any of the benign nodes, and thus the replica nodes' measured speeds will often be over the system-configured maximum speed.

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 shown in figure 2. However, if the system decides that a node has been replicated based on a single observation of a node moving faster than it should, we might get many false positives because of errors in speed measurement. Raising the speed threshold or other simple ways of compensating can lead to high false negative rates. To minimize these false positives and false negatives, we apply the SPRT, a hypothesis testing method that can make decisions quickly and accurately.

We perform the SPRT [6] 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 is less than or exceeds the system-configured maximum speed will lead to acceptance of the null or alternate hypotheses, respectively. Once the alternate hypothesis is accepted, the replica nodes will be revoked from the network.

A. *Advantage of SPRT*

If the replicated node is moving much faster than any of the benign nodes, and thus the replica nodes' measured speeds will often be over the system-configured maximum speed. 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. To minimize these false positives and false negatives, we apply the SPRT, a hypothesis testing [6] method that can make decisions quickly and accurately. 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. In using the SPRT, the occurrence of a speed that is less than or exceeds the system-configured maximum speed will lead to acceptance of the null or alternate hypotheses, respectively. Once the alternate hypothesis is accepted, the replica nodes will be revoked from the network. We find that the main attack against the SPRT based scheme is when replica nodes fail to provide signed location and time information for speed measurement.

V. EXISTING SYSTEM

The Existed schemes rely only on fixed sensor locations in static sensor networks. A particularly dangerous attack is the replica node attack, in which the adversary takes the secret keying materials from a compromised node. The adversary can 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. For detecting replica node attacks is due to randomized and line selected multicast schemes [11] to detect replicas in static wireless sensor networks. Also a scheme to enhance the line-selected multicast scheme in terms of replica detection probability, as well as storage and computation overheads by using trusted random values. A fingerprint-based replica node detection scheme. In this scheme, nodes report fingerprints, which identify a set of their neighbors, to the base station. The base station performs replica detection by using the property that fingerprints of replicas conflict each other. To detect mobile replicas by leveraging the intuition that the number of mobile nodes encountered by mobile replicas in a time interval is more than the number encountered by a benign mobile node.

VI. LIMITATIONS

In potentially hostile environments, the security of unattended mobile nodes is extremely critical. The replica nodes are controlled by the adversary, but have keying materials that allow them to seem like authorized participants in the network. The adversary can then leverage this insider position in many ways. The adversary can simply monitor a significant fraction of the network traffic that would pass through these nodes. Alternately, the adversary could jam legitimate signals from benign nodes or inject falsified data to corrupt the sensors monitoring operation. The main strength of is that it detects mobile replicas in fully distributed manner, while our scheme relies on the base station for mobile replica detection.

VII. PROPOSED SYSTEM

To design an effective, fast, and robust replica detection scheme specifically for mobile sensor networks. For the effective scheme a novel mobile replica detection scheme based on the Sequential Probability Ratio Test (SPRT)[7] .By using the fact that an uncompromised mobile node should never move at speeds in excess of the system-configured maximum speed. Also through quarantine analysis that the amount of time, during a given time slot, that the replicas can impact the network is very limited.

A. *Advantages*

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. Although tamper-resistant hardware can make it significantly harder and more time-consuming to extract keying materials from captured nodes, it may still be possible to bypass tamper

resistance for a small number of nodes given enough time and attacker expertise. The primary method used by these schemes is to have nodes report location claims that identify their positions and for other nodes to attempt to detect conflicting reports that signal one node in multiple locations. This is the first work to tackle the problem of replica node attacks in mobile sensor networks. An uncompromised mobile node should never move at speeds in excess of the system-configured maximum speed.

VIII. SIMULATION

With the help of the ns-2 network simulator we simulate the proposed mobile replica detection scheme in a mobile sensor network. In front end object oriented tool command language (OTcl) and in back end C language is used. In our simulation, 200 mobile sensor nodes are placed within a square area of 250 m x 250 m and the mesh topology is created. We use the Random Waypoint Mobility (RWM) model to determine mobile sensor node movement patterns. The trace file is also used to send the request packets to all the nodes in the network. Using this RWM the nodes moves for 0.05ms. In the RWM model, each node moves to a randomly chosen location with a randomly selected speed between a predefined minimum and maximum speed. After reaching that location, it stays there for a predefined pause time. After the pause time, it then randomly chooses and moves to another location.

This random movement process is repeated throughout the simulation period. We use code from to generate RWM-based movement's model with a steady-state distribution. All simulations were performed for 1,000 simulation seconds. We fixed a pause time of 20 simulation seconds and a minimum moving speed of 1.0 m/s of each node. Each node uses IEEE 802.11 as the medium access control protocol in which the transmission ranges is 50 m. initially the nodes are deployed in the hostile environment after deploying the nodes the base station send the coverage region to all the nodes in the network. Then the nodes gather the data and send to the base station if any of the node get drops the data or it sent the false data then the functionality of replica nodes takes place. Using the hypothesis testing method the replica nodes are detected. Using drop, throughput and packet delivery we can show the comparative graph. The NAM window displays the network animated output.

A. Simulation results

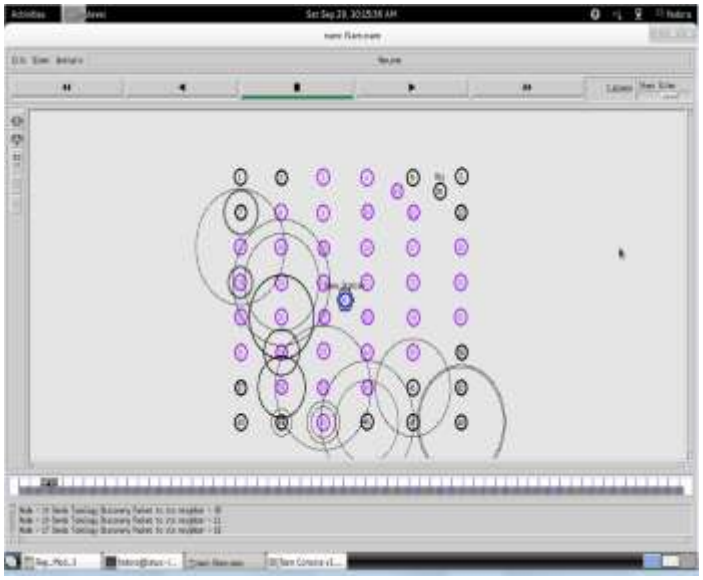

Figure 3: route request and reply

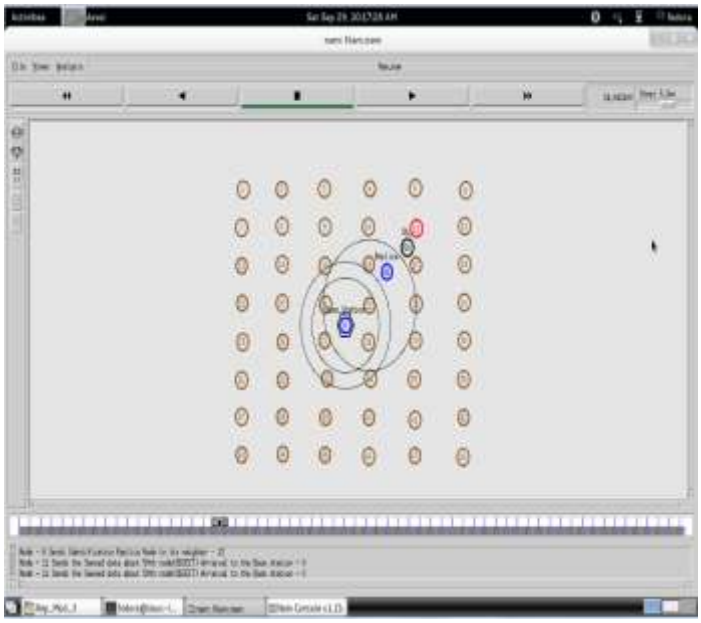

Figure 4: replica node detection

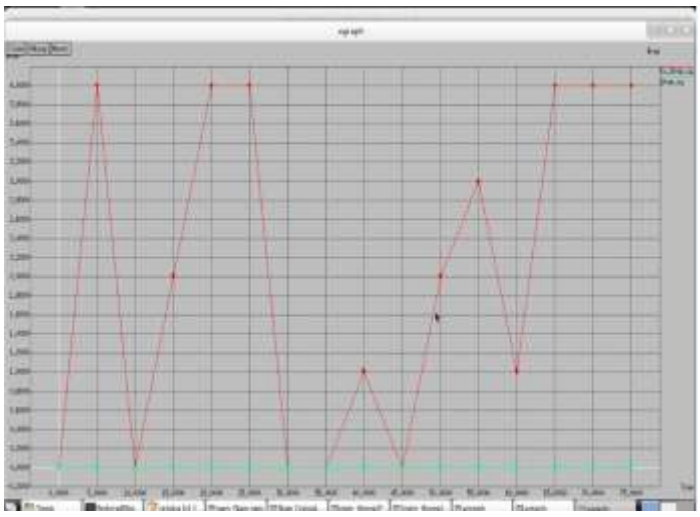

Figure 5: packet drop

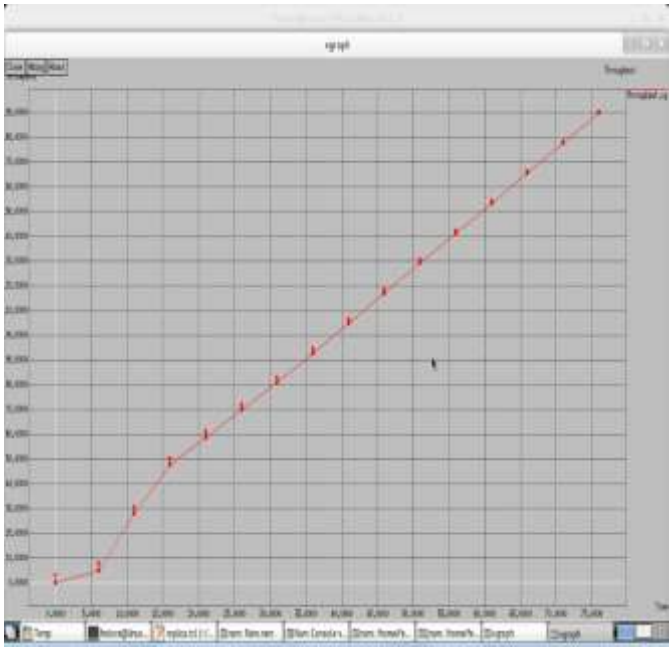

Figure 6: throughput

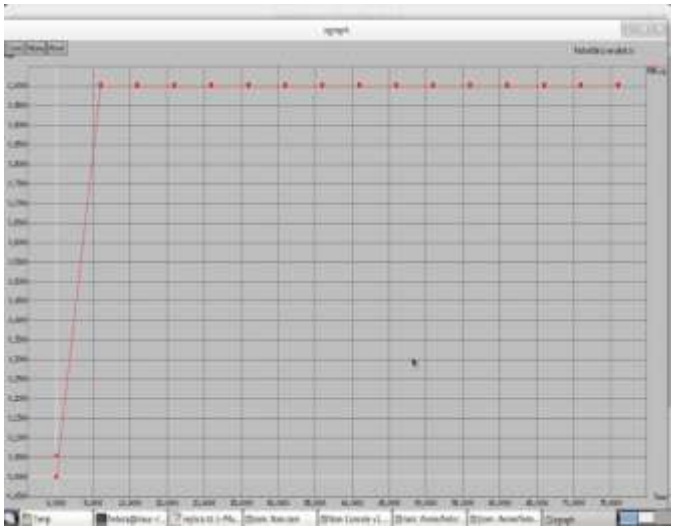

Figure 7: packet delivery

IX. CONCLUSION

The paper concludes detection of mobile replica node attacks in mobile sensor networks using speed measurement testing. Several replica node detection schemes have been proposed in the literature to defend against such attacks in static sensor networks. However, these schemes rely on static sensor locations and hence do not work in mobile sensor networks, where sensors are expected to move. In this work, a fast and effective mobile replica node detection scheme using the Sequential hypothesis testing. SPRT is a proposed technique to solve the problem of replica node attacks in mobile sensor networks.

ACKNOWLEDGMENT

Our thanks to the experts who have contributed for the development of detection of mobile replica node attacks in mobile sensor networks using speed measurement testing and its simulated solution.

REFERENCES

[1] **Ambiritha M.A, Gomathi V** "Efficient Node Replica Detection In Wireless Sensor Networks"2008.

[2] **Chakib Bekara and Maryline Laurent-Maknavicius** "Defending Against Nodes Replication Attacks on Wireless Sensor Networks"2010.

[3] **Dr.Chellappan..CandManjula.V**,"Replication Attack Mitigations for Static and Mobile Wireless sensor networks"1999.

[4] **Divakarmn, rajutumkur.C.K** asst professor "Detection of Mobile Replica Node Attacks in Wireless Sensor Networks Using Sequential Hypothesis Testing"2005.

[5] **jun-won ho**, "Distributed Detection Of Replicas With Deployment Knowledge In Wireless Sensor Networks"2007.

[6] **Jun-Won Ho,"**Sequential Hypothesis Testing Based Approach for Replica Cluster Detection in Wireless Sensor Networks"2010.

[7] Jun-Won Ho, Matthew Wright "Fast Detection of Mobile Replica Node Attacks in Sensor Networks Using Sequential Hypothesis Testing" *IEEE 2011*.

[8] **Liang-Min Wang, and Yang Shi** "Patrol Detection for Replica Attacks on Wireless Sensor Networks"2011.

[9] **Ming Zhang Vishal Khanapure Shigang Chen Xuelian Xiao** "Memory Efficient Protocols for Detecting Node Replication Attacks in Wireless Sensor Networks" Department of Computer & Information Science & Engineering, University of Florida.

[10] **Pavithraa.S,Balakrishnan.**C "Fake Data Termination in Wireless Sensor Networks" International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-1, Issue-2, June 2012

[11] **Ram Prabha.V and Latha.P**"An Overview of Replica Node Detection in Wireless Sensor Networks" International Conference on Recent Trends in Computational Methods, Communication and Controls (ICON3C 2012) Proceedings published in International Journal of Computer Applications® (IJCA).

[12**] Sajal K. Das a, Jun-Won Ho** "A synopsis on node compromise detection in wireless sensor networks using sequential analysis" (Invited Review Article) a Center for Research in Wireless Mobility and Networking (CReWMaN), Department of Computer Science and Engineering, University of Texas at Arlington, Arlington, TX 76019-0015, USA Department of Information Security, Seoul Women's University, 621 Hwarangro, Nowon-Gu, Seoul, South Korea.

[13] **Xiaojiang** "Detection of Compromised Sensor Nodes in Heterogeneous Sensor Networks" Department of Computer Science North Dakota State University Fargo, ND 58105, USA

T.Nidharshini received her B.E degree in Computer Science Engineering from Anna University Coimbatore in 2011 and is currently doing her M.E degree in Adhiyamaan College of Engineering. She can be reached at tnidharshini@gmail.com.

V.Janani received her B.E degree in Computer Science Engineering from Periyar University in 2003 and M.E degree in Computer Science Engineering from Anna University Chennai in 2008 and currently working as Assistant Professor in Adhiyamaan College of Engineering. She can be reached at vajjiram.janani@gmail.com.