Journal of Computer Applications ISSN: 0974 – 1925,
Volume-5, Issue EICA2012-5, February 10, 2012

An Efficient Monitoring Scheme for Malicious Node Detection in Wireless Sensor Networks

Aiswarya S
II MECS, Hindusthan College of Engineering and Technology, Coimbatore, India
E-mail:aisvarya.be@gmail.com

Mohanarathinam A
Assistant Professor, Dept of ECE, Hindusthan College of Engineering and Technology, Coimbatore, India
E-mail:mohanarathinam@gmail.com

Abstract - Security plays an major role in the ability to deploy and access trustworthy information from a wireless sensor network. Local monitoring schemes have proved to be effective mechanisms for security in Wireless sensor networks. Designing an efficient scheme integrated with good monitoring capability and also secure against various kinds of attacks is the need of the hour. Better performance is achieved at the cost of security concerns as a result an adversary might be able to determine which nodes to attack, so as to control or compromise a part or whole of the sensor network. Hence, we need to insert some security constraints into the monitoring schemes. This work analyses the performance of self monitoring scheme based on algorithmic approach and a more reliable approach which is efficient in terms of various network performance parameters compared to self monitoring scheme and secure employing location monitoring is proposed.

Keywords: *Self monitoring, location monitoring.*

I. INTRODUCTION

One of fundamental goals for Wireless Sensor Networks (WSNs) is to collect information from the physical world. Although a number of proposals have been reported security in WSNs, provisioning security remains critical and challenging task. WSNs have attracted much attention due to its great potential to be used in various applications. Comparing to existing infrastructure – based networks, wireless sensor networks can virtually work in any environment, especially those where wired connections are not possible. Unlike conventional networks supporting mostly point-to-point or point-to-multipoint data forwarding, WSNs are often deployed to sense, process and disseminate information of targeted physical environments.

Wireless security is just an aspect of computer security. All organizations with any number of members or employees are particularly vulnerable to security breachescaused by rogue access points. If an employee (trusted entity) in a location brings in an easily available wireless router, the entire network can be exposed to anyone withinrange of the signals. If an employee adds a wireless interface to a networked computer via an open USB port, thevery same riskmay be spread for the respective network. However, for any of these entities concepts are available to protect the computer and the network. Such protection must be applied to all levels of communication, to all entities networked and to all functions used and data processed.

There were relatively few dangers when wireless technology was first introduced, as the effort to maintain the communication was high and the effort to intrude is always higher. The variety of risks to users of wireless technology have increased as the service has become

more popular and the technology more commonly available. Today there are a great number of security risks associated with the current wireless protocols and encryption methods, as carelessness and ignorance exists at the user and corporate IT level. Cracking methods have become much more sophisticated and innovative with wireless.

II. MONITORING SCHEMES IN WSN

A. Anamoly Detection Mechanisms

Wireless sensor networks is composed of wireless sensor nodes which deploy in the environment without any network topology, it can support stars and peer to peer models, the nodes can join or quit freely. Since the features of self-organization, self-management, data centric in WSN, it has broad application prospects in environmental monitoring, intelligent monitoring, data collection, security, military and so on. But limited by the energy, the computing resource, the changeful topology and the multiple-hop data transmission, WSN faces a variety of special attacks such as data interception, Sybil attacks, wormhole attacks and selective forwarding attacks except traditional attacks. From analysis of the solution to this issue, we found that combining the WSN nodes monitoring and compromised node detecting together is an effective way.

By monitoring each node, we can know the physical information, energy status and behavior of data communication, which can grasp the living condition of the node to help the sink node to balance the network load, extending the living time of the nodes and the network. What's more, by statistically analyzing node communication behavior we can effectively detect compromised nodes in the network, while the attack action is launched by those nodes.

The general problem of detecting interesting changes from the normal observed behavior in sensor measurements is known as *anomaly detection*. An anomaly can be caused by an unusual change in the phenomena (e.g., water temperature or nutrient concentration), or by faulty sensors: that cause incorrect measurements, or even by malicious events such as security attacks in sensor networks . Important challenges for the management of sensor networks in complex environments such as the GBR are the detection, inference, reporting and correcting of anomalies. Centralized solutions to anomaly detection, which involve collection of all data from sensors to a centralised node for processing, can be communication intensive and thus very energy inefficient. An alternative approach for anomaly detection in sensor networks is to use in-network processing in order to prolong the lifetime of the resource constrained wireless sensor networks. Our research into distributed anomaly detection in wireless sensor networks addresses the above challenges in order to provide a reliable, energy efficient and self-correcting wireless sensor network for use in small to large scale deployments.

B. Local Monitoring

Local monitoring is the one of the powerful technique for improving the security in multi hop Wireless Sensor Network (WSN).Although it is a good technique for security purpose in WSN but it has a major drawback that it is costly in terms of energy consumption which makes overhead for the energy constrained system such as WSN. In WSN environment, the

scarce power resources are typically addressed through sleep- wake scheduling of nodes but sleep-wake technique is vulnerable even to simple attacks. In WSNs, local monitoring is a promising security mechanism as an effective complement for cryptographic mechanisms. Existing local monitoring schemes assume the existence of sufficient nodes to carry out the monitoring function. Such a requirement is often practically difficult when we consider minimizing the number of monitoring nodes selected for a large scale WSN.

Local monitoring exploits the convenience of overhearing due to the broadcast nature in wireless communication and dense deployment of large-scale systems. On the other hand, local monitoring also incurs extra energy cost since it requires monitoring nodes to keep active and oversee network behaviours. Hence, to employ as few nodes as possible is highly desirable

C. Self Monitoring

The development of small wireless sensors and smart-phones, which include various sound, video, motion and location sensors have facilitated new pervasive applications. These include health-care, monitoring and control in buildings, environmental monitoring and even tracking wildlife movement. These pervasive systems are expected to perform in urban as well as inaccessible rural environments, with different resources, and requirements may change dynamically requiring flexible adaptation. Some applications such as health-care may be life-critical so recovery from faults and errors is important. Wireless sensor networks (WSNs) are a fundamental aspect of pervasive systems for supporting context aware adaptation. Accuracy of sensing readings is vital to the correct functioning of the system in many applications. The deployment of the sensing devices vary from a small set of sensor nodes for a body network to hundreds or even thousands of nodes, forming a complex collaborative network structures for environmental sensing. In general, self monitoring is also named as ubiquitous computing, connected computing devices in the environment. Namely, self monitoring is a convergence of wireless technologies and the Internet. With the rapid development of wireless technologies and electronics devices, wireless sensor networks which consist of sensing, data processing, and communication components have been attracting technology for self monitoring because of the miniaturization, low-cost, and low-power. By analyzing traffic flows, monitoring nodes are able to detect malicious behaviours, such as delaying, dropping, modifying, or fabricating packets, etc. To meet the requirements, we sometimes require multiple nodes to conduct monitoring. In the local monitoring scheme [1], a number of nodes are employed for watching the specific area in the network. These monitoring nodes are normal nodes and can perform basic operations of communication and sensing in addition to monitoring In the edge self monitoring scheme two distributed algorithms are employed for secure transmission of packets from the source to destination.[4].

III. MONITORING NODE SELECTION PROCESS

A secure and most common method adopted for network security is location monitoring. Here each node proves its reliability based on its location information may be in various forms which determine the performance competence of each location monitoring scheme. Location disclosure is an attack that targets the privacy requirements of an ad hoc network. Through the use of traffic analysis techniques or with simpler probing and monitoring

approaches, an attacker is able to discover the location of a node, or even the structure of the entire network. Monitoring individual locations poses privacy threats to the monitored nodes, because an adversary could abuse the location information gathered by the node to infer personal sensitive information. In an ordinary location monitoring system the sensor nodes report the individual location information to the monitoring node. Thus such schemes pose a major privacy threat. To tackle such a privacy threat, the concept of group location information, that is, a collection of location data relating to a group or category of nodes from which individual identities have been removed has been suggested as an effective approach to preserve location privacy.

This paper proposes a secure and efficient location monitoring system for wireless sensor networks to provide monitoring services. Our paper uses a concept, where a person can be identified among a group of persons. In this paper, each sensor node is categorised into its sensing area into a group area. Each sensor node reports only group location information, which is in a form of a group area, along with the member nodes residing in it. Thus the group location information of a particular coverage area is to be collected by a secondary monitoring node which also acts as a broadcast node and that information is forwarded to the master monitoring node. This node is the administrator node equipped with every details of the network, including the location information both individual and group. On verification of the above location claim sent by a node the master monitoring node categorises a node to be reliable or not. Thus based on the decision taken on the reliability of anode based on its group location claim the node is accepted to proceed broadcast or rejected immediately as it is identified as a malicious node.

IV. PROBLEM DEFINITION

Monitoring schemes are mainly focusing on either minimizing the time taken for monitoring or minimizing the number of monitoring nodes in order to make the monitoring scheme energy efficient. Either performance or security concerns are concentrated or either of the one is achieved at the cost of other. In this work performance analysis parameters like energy consumption, packet delivery ratio and delay of general self monitoring scheme based on Local Maximal Element algorithm and Local Dual Feasible algorithm is done in order to compare the performance of our scheme with that of the existing self monitoring scheme[1] and verify the efficiency of our work.

Many location monitoring mechanisms mostly focus on individual location claims, ie a nodes location claim inferred from its XY coordinates, number of hops from source to destination or Euclidean distance from source to destination. Thus such schemes pose a major privacy threat because individual nodes can be easily compromised by adversarial nodes. To tackle such a privacy threat, the concept of group location information, that is, a collection of location data relating to a group or category of nodes from which individual identities have been removed has been suggested as an effective approach to a more secure and efficient location claim mechanism.

V. RESULTS AND DISCUSSION

The Simulation is carried out in NS2 under LINUX platform for comparing the protocols based on different parameters as shown in table 1.

A. Simulation Parameters

Packet delivery ratio
The ratio of the number of packets received and the number of packets expected to receive.

Energy consumption
The difference between the initial energy set to the node and energy remaining after the transmission is taken as the energy consumed for the transmission.

Delay
The time interval between the arrival of the first packet and the next one divided by the total number of packets sent.

B. Location Claim Parameters

The entire network area is subdivided into groups and nodes within the group are identified by the following location claim parameters:

Member id: It is the individual identification of the member node assigned by the network administrator.

Member count: This is an integer assigned to a node within a group in order to distinguish a node from other nodes in the same group.

Group area: This is the value of the group to which the node is presently belonging.

Simulation Time	100s
Topology Size	1000m x 1200m
Number Of Nodes	11-40
MAC Type	MAC 802.11
Radio Propagation Model	Two Ray Model
Maximum Transmission Range	40m
Pause Time	0s
Max Speed	4m/s to 40m/s
Initial Energy	100J
Transmit Power	1.0W
Receive Power	0.5W
Traffic Type	CBR
Packet size	512 bytes
Antenna	Omni directional

C. Simulation Results

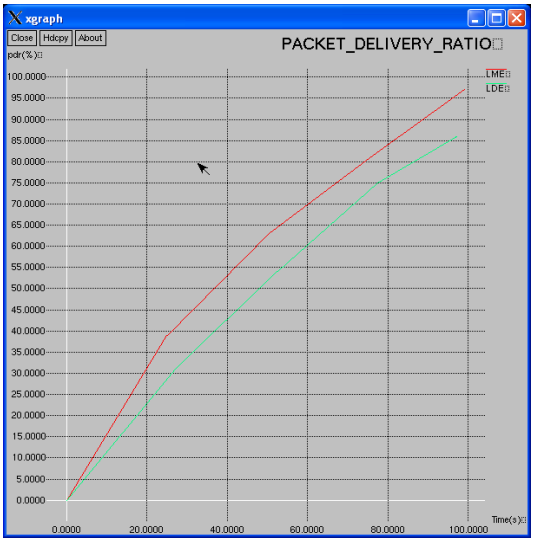

Figure 1: Packet Delivery Ratio vs Time Taken

The Figure 1 shows that *the* packet delivery ratio increases with time for both LME and LDF which is a desirable feature.From the above result we infer that as LME is an optimal selection method it proves a better packet delivery ratio when compared with LDF method.

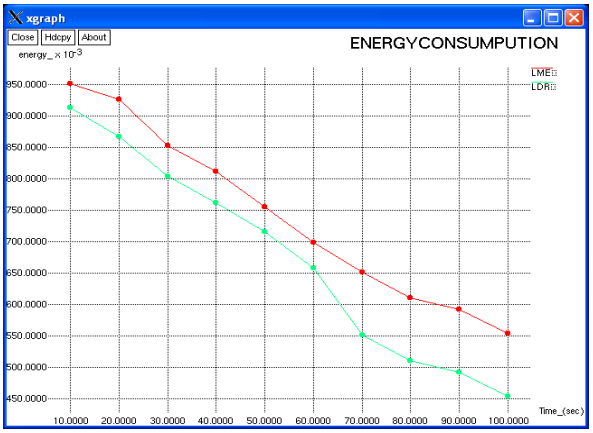

Figure 2: Energy Consumption Vs Time Taken

The Figure 2 shows the plots of energy consumption on Y-axis and time on X-axis. This result also proves the optimality of LME method over the LDF method.

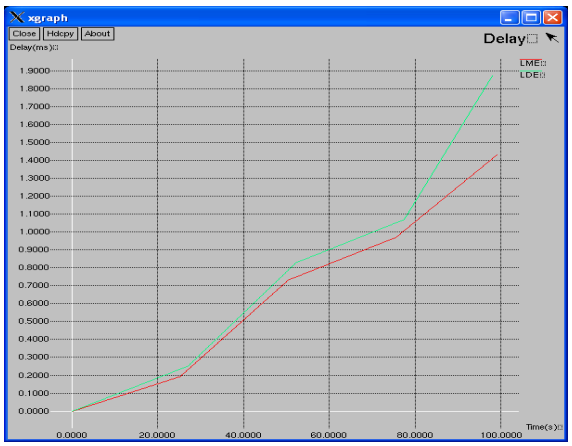

Figure 3: Delay Vs Time Taken

The Figure 3 shows the delay on Y-axis and time taken on X-axis. The random selection method ie, LDF shows an increased delay compared with the LME. Now let us see the simulation results of our scheme.

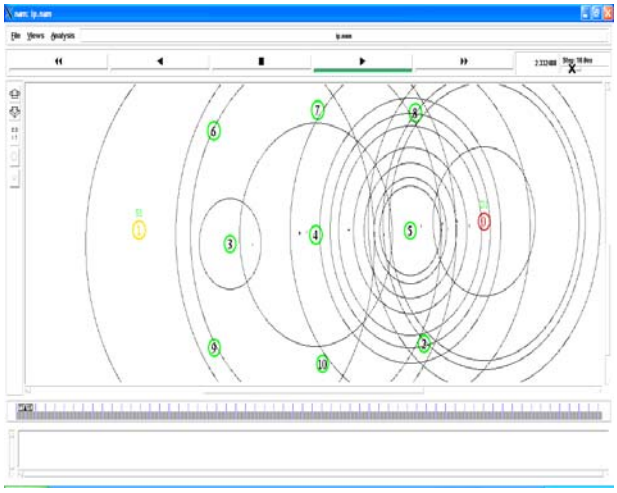

Figure 4: Location Claim &Packet Transmission via Path 1.

The Figure 4 shows the network configuration consisting of 11 nodes. Node 1 acts as the source node as well as the secondary monitoring node which verifies the location claim sent by other sensor nodes in the network. Node 0 acts as the destination node. On successful verification of the location claim sent by the nodes in path 1 packet transmission is done successfully via path 1 as no malicious node is currently identified.

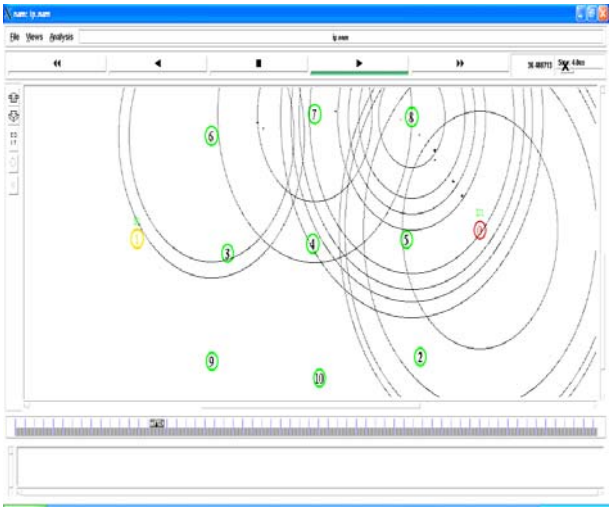

Figure 5: Location claim & packet transmission via path 2.

The Figure 5 shows a similar case like figure 1. All arguments for figure 1 holds true for this case also but here the location claim approval is done for nodes in path 2.

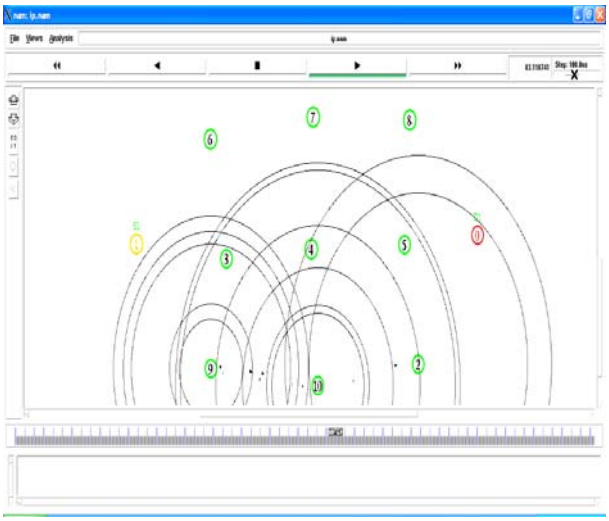

Figure 6: Location Claim Sent by Nodes in Path 3

Figure 6 shows the location claim information sent to the source cum secondary monitoring node for approval and for the enabling of packet transmission.

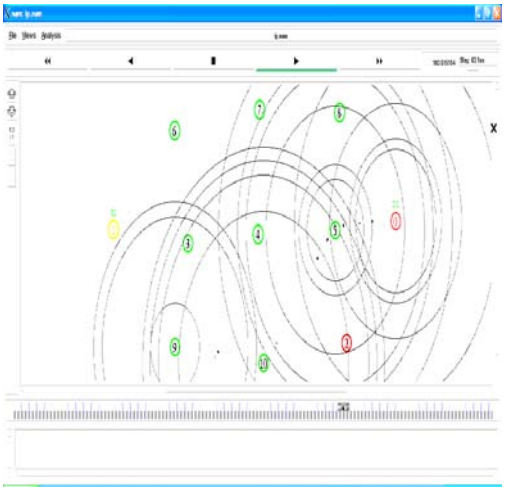

Figure 7: Malicious Node Detection and Alternate Routing

The Figure 7 shows the malicious node detection process. Here node 2 has been identified as the malicious node because it has proved to have sent a false location claim. A malicious node is treated as equally as a compromised node. On receiving this false claim node 1 verifies it with the stored location information. On any disapproval with the above will need immediate action for preserving the security constraints of the network. Thus node 2 is proved to be malicious and rejected out of the transmission path. Equally important is the need for alternate routing for preventing the disruption of packet transmission. Thus packets are rerouted via node 5 which has already proved its reliability through is successful location claim.

VI. CONCLUSION

In this work malicious node detection simulation has been done successfully using the location claim information for wireless sensor networks. We see this process to be an immediate response to an adversarial attack or a mischievous node behavior. Alternate routing via a secure path has also been achieved which stands to be a good argument for the efficiency of this method.

VII.FUTUREWORK

The future work will be to incorporate certain constraints of scaling so that this method is suitable for a wide variety of applications. Also here in this work only a single group area is considered. The primary master monitoring node is to be incorporated which will also act as the administrator node so that this scheme will be much more efficient due to the incorporation of two levels of security. Equally important is to preserve the network performance parameters. A detail analysis of various network performance parameters like energy consumption, packet delivery ratio etc is to be done to avoid performance degradation and improve the optimality of this scheme.

VIII. ACKNOWLEDGMENT

We wish to thank our college management and head of our department for their kind support and continuous encouragement in perusing this work.

REFERENCES

1. C.Hsin and M. Liu, “Self-Monitoring of Wireless Sensor Networks, ”Elsevier Computer Comm., vol. 29, pp. 462-476, 2006 .
2. I.Khalil, S. Bagchi, and N.B. Shroff, “SLAM: Sleep-Wake Aware Local Monitoring in Sensor Networks,” Proc. IEEE/IFIP Conf. Dependable Systems and Networks (DSN), 2007.
3. Khalil, S. Bagchi, and C. Nina-Rotaru, “DICAS: Detection, Diagnosis and Isolation of Control Attacks in Sensor Networks, ”Proc. IEEE First Int’l Conf. Security and Privacy for Emerging Areas in Comm. Networks(Secure Comm), 2005.
4. Edge Self-Monitoring for Wireless Sensor Networks. Dezun Dong, Student Member, IEEE Computer Society, XiangkeLiao, Yunhao Liu, Senior Member, IEEE Computer Society, Changxiang Shen, and Xinbing Wang, Member, IEEE Computer Society. (IEEE transactions on Parallel and distributed systems, VOL. 22, NO. 3, MARCH 2011.
5. N. Sastry, U. Shankar, and D. Wagner, “Secure verification of location claims,” in ACM Workshop on Wireless Security (ACM WiSe), 2003.
6. S.Vural and E. Ekici, “Analysis of Hop-Distance Relationship in Spatially Random Sensor Networks,” Proc. ACM MobiHoc, pp.320–331, May 2005.
7. S.Capkun and J.-P. Hubaux, “Secure positioning of wireless devices with application to sensor networks,” in Proc. IEEE INFOCOM, 2005.
8. Marc Greis’ Tutorial for the UCB/LBNL/VINT Network Simulator.
9. T. He, C. Huang, B. Blum, J. Stankovic, and T. Abdelzaher, “Range-free localization schemes for large scale sensor networks,” in Proc.Mobicom,2003.
10. L. Fang, W. Du, and P. Ning, “A beacon-less location discovery scheme for wireless sensor networks,” in *Proc. IEEE INFOCOM*,2005.
11. S. Capkun and J.-P. Hubaux, “Secure positioning of wireless devices with application to sensor networks,” in Proc. IEEE INFOCOM, 2005.
12. L. Lazos and R. Poovendran, “Serloc: secure range-independent localization for wireless sensor networks,” in *ACM* Workshop on Wireless Security (ACM WiSe), 2004.
13. M. Gruteser, G. Schelle, A. Jain, R. Han, and D. Grunwald, Privacy-aware location sensor networks,. In Proc. of Hot OS, 2003.

BIOGRAPHY

S.Aiswarya received Bachelor of Engineering degree from KLN college of Engineering and Technology, Anna University Chennai in the year 2009. She is currently doing her Master of Engineering at Hindustan College of Engineering & Technology, Anna University, Coimbatore.