IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834, p- ISSN: 2278-8735. Volume 5, Issue 1 (Jan. - Feb. 2013), PP 13-18
www.iosrjournals.org

Unearthing the Compromised Nodes and Restoring them in Wireless Sensor Network

Abhinaya.E.V[1]
Post Graduate Student Department of Electronics and Communication K.Ramakrishnan College Of Engineering,India

Abstract: *Sensor nodes are usually deployed in an open environment therefore they are subjected to various kinds of attacks like Worm Hole attack, Black Hole attack, False Data Injection attacks. Since the attackers can cause disruption and failure to the network, it's very important to detect these compromised nodes and revoke them before any major disruption occurs. Therefore, it's very important to safe guard the network from further disruption. For this purpose a method called Biased SPRT (Sequential Probability Ratio Test) is used by setting up some Threshold Value and Trust Aggregator in the network scenario for which the network is divided into number of Zones.*

Key terms *– Compromised Node, SPRT, B-SPRT, Trust Aggregator, Zones, False Positives, False Negatives.*

I. Introduction

Wireless Sensor Networks (WSNs) have emerged as a research areas with an overwhelming effect on practical application developments. They permit fine grain observation of the ambient environment at an economical cost much lower than currently possible. In hostile environments where human participation may be too dangerous sensor networks may provide a robust service. Sensor networks are designed to transmit data from an array of sensor nodes to a data repository on a server. The advances in the integration of micro-electro-mechanical system (MEMS), microprocessor and wireless communication technology have enabled the deployment of large-scale wireless sensor networks[1]. WSN has potential to design many new applications for handling emergency, military and disaster relief operations that requires real time information for efficient coordination and planning.sensors are devices that produce a measurable response to a change in a physical condition like temperature, humidity, pressure etc. WSNs may consist of many different types of sensors such as seismic, magnetic, thermal, visual, infrared, acoustic and radar, capable to monitor a wide variety of ambient conditions. Though each individual sensor may have severe resource constraint in terms of energy, memory, communication and computation capabilities; large number of them may collectively monitor the physical world, disseminate information upon critical environmental events and process the information on the fly.

The issues of network lifetime and data availability are extremely important in WSN due to their deployment in hostile environment. The system should provide fault tolerant energy efficient real-time communication as well as automatic and effective action in crisis situations. A typical sensor network operates in five phases which are planning phase, deployment phase, post-deployment phase, operation phase and post-operation phase.

a. In planning phase, a site survey is conducted to evaluate deployment environment and its conditions to select a suitable deployment mechanism.
b. In deployment phase, sensors are randomly deployed over a target region.
c. In post-deployment phase, the sensor networks operators need to identify or estimate the location of sensors to access coverage.
d. The operation phase involves the normal operation of monitoring tasks where sensors observe the environment and generate data.
e. The post-oeration phase involves shutting down and preserving the sensors for future operations or destroying the sensor network.

The sensor nodes consist of sensing, data processing and communicating components. They can be used for continuous sensing, event detection as well as identification, location sensing and control of actuators. The nodes are deployed either inside the phenomenon or very close to it and can operate unattended. They can use their processing abilities to locally carry out simple computations and transmit only required and partially processed data. They may be organized into clusters or collaborate together to complete a task that is issued by the users. In addition, positions of these nodes do not need to be predefined[1][2]. These allow their random deployment in inaccessible terrains or disaster relief operations. The WSN provides an intelligent platform to gather and analyze data without human intervention. As a result, WSN's have a wide range of applications such as military applications, to detect and track hostile objects in a battle field or in environmental research applications, to monitor a disaster as seismic tremor, a tornado or a flood or for industrial applications, to guide

and diagnose robots or machines in a factory or for educational applications, to monitor developmental childhood or to create a problem solving environment.

Main idea of this paper is to detect the compromised nodes using Sequential Hypothesis Testing (SPRT). Two scenarios are checked here. In first scenario, the whole network is divided randomly into some number of zones where software attestation is performed over the affected zone with maximum number of untrustworthy nodes which consumes more energy and provides more delay whereas in second scenario the whole scenario is divided into low trust samples and high trust samples where only high trust samples are used in transmission and reception. This is performed using Biased SPRT. Since only high trust samples are used the problem of compromising is restricted. Hence it provides better results than the previous scenario.

II. Model

A two-dimensional *static* sensor network is assumed in which sensor nodes do not change their locations after deployment since they are immobile. Their locations can be obtained by using some Secure Localization Schemes. We also assume that the link between all sensors is bidirectional as they can perform both transmission and reception. Let's assume an Adversary attacks a set of nodes in each Zone. However, we limit on his attack capability such that he does not compromise a majority of the nodes in each region. This is reasonable, since compromising a majority of sensor nodes in a region is far from optimal. This is mainly because his influence is limited to the region while he spends substantial time and effort to compromise many nodes. The same time and effort could instead be used to spread out compromised nodes over a wider area and cause greater disruption to the network.

III. Dectection And Revocation Of Compromised Nodes

Reputation-based trust management schemes do not stop compromised nodes from doing malicious activities in the network[2][3][4][5]. Also, existing schemes based on software attestation require each sensor to be periodically attested because it cannot be predicted when attacker compromises sensors. The periodic attestation of individual nodes will incur large overhead in terms of computation and communication[2]. To mitigate these limitations, we propose a zone-framed node compromise detection and revocation scheme. Our scheme facilitates node compromise detection and revocation by leveraging zone trust information. In the first scenario specifically, we divide the whole network into a number of zones randomly like Z1,Z2,Z3,.....For each zone a Trust Aggregator(TA) is assigned for a particular time slot. The Trust Aggregator is responsible for collecting the log information's from all the nodes available in that particular zone for that particular time slot. Once it fetches all the informations's then the Trust Aggregator sends the report to Base Station(BS). This way all the Trust Aggregator of different zones sends their report to Base Station. At Base Station, all reports from different zones are checked. Each reports contains some particular Trust Value(TV) which is checked in accordance to a Threshold Value(TV) set prior at Base Station. Once the Trust value is below the given Threshold Value, the corresponding node can participate in further transmissions and receptions. But, if the Trust Value of particular node is higher than the given Threshold Value, that particular node is said to be Compromised Node(CN) or Malicious Node(MN) or Untrustworthy Node(UN). This particular node is considered as affected. The Zone with maximum compromised nodes are said to be affected zone. The affected nodes in that particular zone can be restored by performing Software Attestation schemes. This Software Attestation Scheme checks for the subverted module and programs and restores them using SPRT. In this case, large delay is noticed as each node's log information has to be collected every time. Also, overhead and energy consumption is high.

In second scenario the whole network is considered into two set of samples: low trust samples and high trust samples where only high samples are considered to take part in the network transmission using Biased SPRT. Therefore, less delay and less energy is consumed compared to previous scenario.

IV. Protocol Description

A. Network Formation

A network is divided into a set of zones with Trust Values and untrustworthy zone is detected in accordance with the zone Trust Values. Once a zone is found to be affected or untrustworthy then software attestation is performed by the network operator over all the sensor nodes present in that particular zone. Since, the software attestation is performed over all the nodes including the Honest nodes/Trustworthy nodes along with compromised nodes, only in untrustworthy nodes it incurs less overhead. In our scheme, specifically SPRT method is used as this method depends on multiple evidences rather than single evidence. Also, its known fact that multiple evidences produces accurate result when compared to single evidence. Therefore this statistical method is chosen which contains two limits namely null hypothesis and alternate hypothesis. These two limits play major role in determining the correct results. When the Trust Value is less than the given Threshold Value, it is considered to be null hypothesis and it can be included in the upcoming process whereas when the Trust

Value is greater than the Threshold Value, it is considered as affected requiring revocation. The main advantage of using SPRT is that correct decision can be reached at very shorter time providing low false positives and false negatives.

The network operator assigns each node with unique ID and preloads each and every sensor node with shared secret keys to communicate with Base Station and pair-wise keys to communicate between themselves[6][11]. Zone area plays an important role in estimating the cost of the system. For example, if the zone size is small it would not be possible to place all the nodes within the zone without causing some disruptions. And if the zone is huge, the intra-communication between the nodes require multiple hops which increases the cost of the system[12][13]. Therefore, zone is taken in the form of square whose perimeter is P such that the diagonal is √2P equal to the communication range and the optimal zone size is √2P/2.

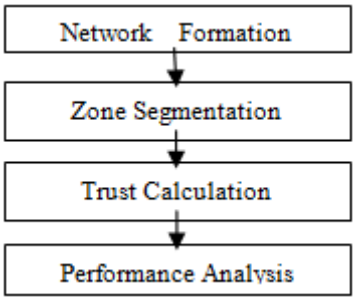

Fig. 1 Basic block diagram of 1st scenario using SPRT

The network operator assigns each node with unique ID and preloads each and every sensor node with shared secret keys to communicate with Base Station and pair-wise keys to communicate between themselves[6][11]. Zone area plays an important role in estimating the cost of the system. For example, if the zone size is small it would not be possible to place all the nodes within the zone without causing some disruptions. And if the zone is huge, the intra-communication between the nodes require multiple hops which increases the cost of the system[12][13]. Therefore, zone is taken in the form of square whose perimeter is P such that the diagonal is √2P equal to the communication range and the optimal zone size is √2P/2.

B. Trust Aggregator Setup and Trust Evaluation

The network considered here is static network which contains sensor node s with fixed location. The sensor node s discovers the ID's of its neighbouring nodes and establishes pairwise secret keys with them. The Trust Aggregator is selected(TA) in round robin manner using pseudorandom number. Each node acts TA in its given duty time slot and the starting time of each node is same providing same permutations. For each time slot Ti, one node act as Trust Aggregator by collecting the log information of all neighbouring nodes and also includes its own log information which are together called as Trust Reports. The more information is shared between the nodes, the more will be the trust level. Neighbouring nodes are represented using s .

TABLE 1
COMMON PARAMETERS ADOPTED IN THE SIMULATION

Parameters	**Values**
Simulation area	1000*1000m
Number of nodes	100
Transmission range	250m
Simulation duration	150ms
Mobility model	Random waypoint
Propagation	Two way ground

C. Detection and Revocation

Each TA sends its trust reports to the Base-Station along with fresh time stamp. Hence, here replay attacks can be avoided[7]. As already the BS is maintaining the list TA's neighbouring lists, it would be easier for the BS to detect most affected zone with maximum number of affected sensor nodes. For this purpose basic simple SPRT is used which contains both null hypothesis and alternate hypothesis[8]. When the Trust Value is less than Preset Threshold Value, it is considered as null hypothesis and these nodes are eligible to participate in further transmissions where as the nodes with alternate hypothesis are corrected using some available software attestation schemes. The whole network is divided into two sets of samples low trust samples and high trust samples. The sensor nodes with low trust values are not allowed to participate in the transmission and reception process in Biased-SPRT. Instead only high trust values are used exclusively. Since only high trust samples are taken into consideration the probability of false positive and false negative is lesser compared to the first scenario of simple SPRT. Also delay, throughput results are better than the first scenario.

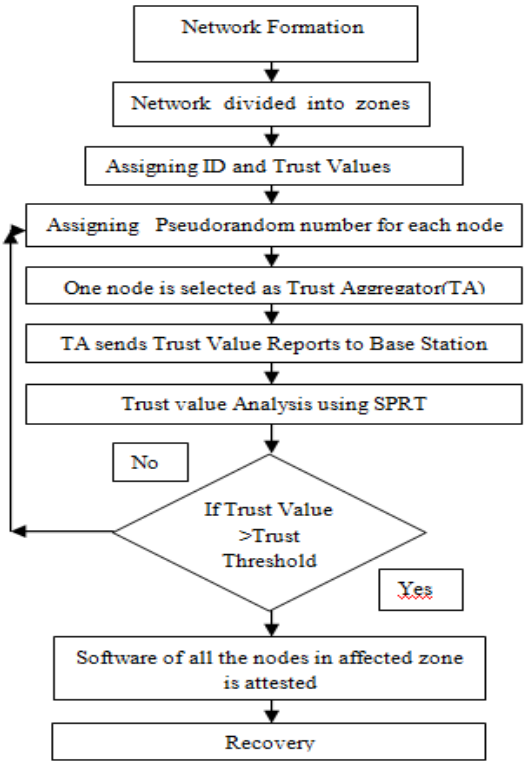

Fig. 2 Flow diagram of the 1st scenario using SPRT

V. Simulation Results

The network environment contains 100 nodes for simulation within a network area of 1000*1000m.The simulation time or simulation duration is 150ms and the propagation model chosen is a Two way ground model capable of both transmitting and receiving. The main three metrics used to evaluate the performance are *Number of reports, False positives, False negatives.* Number of reports is the zone trust reports sent by TA to the BS. False positive is the error probability that a trustworthy zone is impersonated as untrustworthy zone. False negative is the error probability that a untrustworthy zone is misidentified as trustworthy. Performance parameters like delay, throughput, energy consumption etc simulated using Network Simulator2(NS2) of version 2.26. The simulated graphs clearly shows that delay is lesser and throughput is also better in Biased-SPRT.

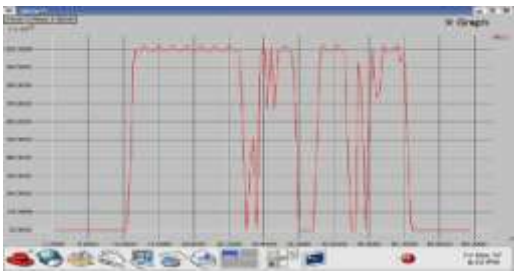

Fig. 3 False Positive

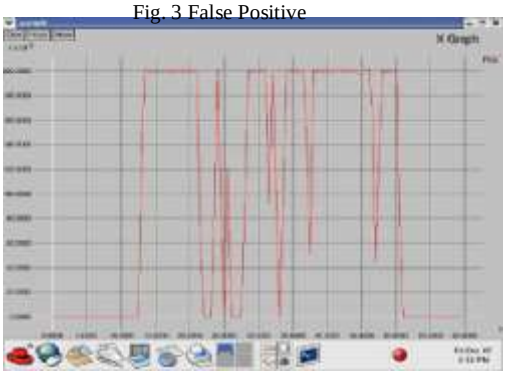

Fig. 4 False Negative

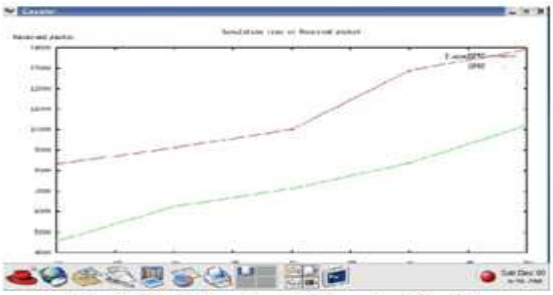

Fig. 5 Simulation time Vs Received Packet

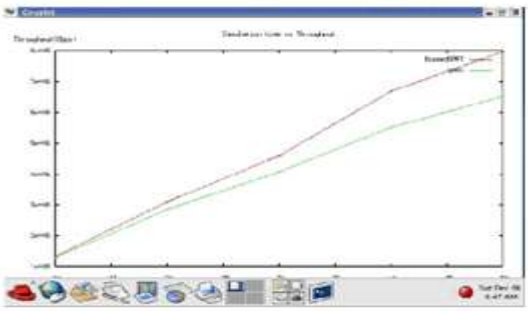

Fig.6 Simulation time Vs Throughput

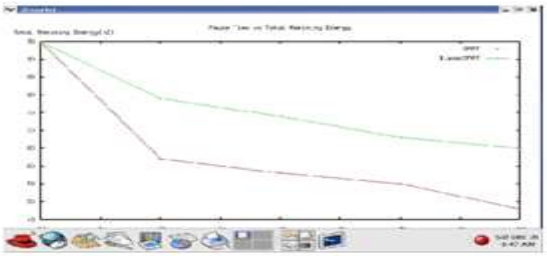

Fig. 7 Pause time Vs Total remaining energy

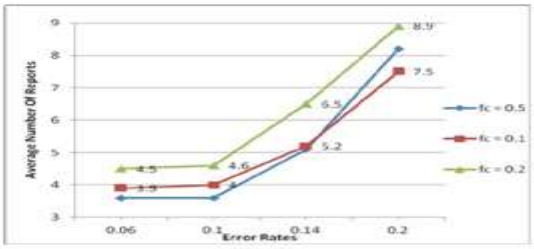

Fig.8 Average number of reports and Error rates (fc-fraction of compromised nodes)

VI. Conclusion And Future Enhancement

We infer that the Biased-SPRT requires fewer number of samples to arrive at a correct decision than the simple SPRT used in first scenario. The performance of Biased-SPRT is comparatively better than the result of first scenario. First scenario with Sequential Hypothesis Testing(SPRT) gives 78.6% of correct performance and second scenario with Biased-SPRT provides 83.4%. Future enhancement method will be Policy Enforcing Protocol first, policy implementation in the multi-tier networks is entirely distributed without relying on any central trusted choke points. Second, the trusted networks are self-organized. They can be established and managed spontaneously without requiring pre-deployed trusted entities or centralized management. Third, the multi-level trust enables flexible enforcement of complex policies, which can be defined across various interdependent protocols and enforced independently.

Acknowledgement

The authors would like to thank Dr.A.Varadarajan, Deputy Director of IGNOU, Chennai for his full cooperation for providing us with good faculties and thanks to all anonymous reviewers for their valuable suggestions and comments.

References

[1] S.Capkun and J.P. Hubaux. Secure positioning in wireless networks. *IEEE Journal on Selected Areas in Communications*, 24(2):221–232, February 2006.
[2] S.Ganeriwal and M. Srivastava. Reputation-based framework for high integrity sensor networks. In *ACM SASN*, October 2004.
[3] J. Ho, M. Wright, and S.K. Das. Fast Detection of Replica Node Attacks in Sensor Networks Using Sequential Analysis. In *IEEE INFOCOM,*April 2009.
[4] X. Hu, T. Park, and K. G. Shin. Attack-tolerant time-synchronization in wireless sensor networks. In *IEEE INFOCOM,* April 2008.
[5] J. Jung, V. Paxon, A.W. Berger, and H. Balakrishnan. Fast port scan detection using sequential hypothesis testing. In *IEEE S&P*, May 2004.
[6] Z. Li, W. Trappe, Y. Zhang, and B. Nath. Robust statistical methods for securing wireless localization in sensor networks. In *IEEE IPSN*, April2005.
[7] B. Parno, A. Perrig, and V.D. Gligor. Distributed detection of node replication attacks in sensor networks. In *IEEE S&P,* May 2005.
[8] Y. Sun, Z. Han, W. Yu, and K. Liu. A trust evaluation framework in distributed networks: vulnerability analysis and defense against attacks In *IEEE INFOCOM,* April 2006.
[9] A. Wald. Sequential analysis. *Dover Publications*, 2004.
[10] Y. Yang, X. Wang, S. Zhu, and G. Cao. Distributed software-basedattestation for node compromise detection in sensor networks. In *IEEE SRDS*, October 2007.
[11] W. Zhang, M. Tran, S. Zhu, and G. Cao. A random perturbation-based scheme for pairwise key establishment in sensor networks. In *ACM Mobihoc*, September 2007.
[12] M.G.Zapata, "Secure Adhoc On-Demand Distance Vector (SAODV) Routing", *IETF MANET* Mailing List, October 2001.
[13] Y.C.Hu, A.Perigg and D.B.Johnson, "Wormhole detection in wireless adhoc networks," Department of Computer Sciience, Rice University, June 2002.
[14] F.Ye, A.Chen, S.Lu and L.Zhang,"A scalable solution to minimum cost forwarding in large sensor networks", in *Tenth International Conference on Computer Communications and Networks*, 2001.