An Improved Intrusion Detection Syste`m (IIDS) using Enhanced Sequential Probability Ratio Test (eSPRT) Algorithm in Wireless Sensor Networks

Ram Pradeep Manohar,
Research Scholar, St.Peter's University, Chennai. ram_pradheep@yahoo.co.in

E.Baburaj,
*Professor, Narayanaguru College of Engineering, Manjalumoodu***.** alanchybabu@gmail.com

Abstract

Due to the improved technology and reduced costs, wireless sensor networks have gained much more preferences over wired networks in the past few decades. A wireless sensor network consists of sensor nodes which are placed in an area for communication and it forms a wireless network. WSN is accepted various critical applications; network security is of fundamental importance. The open medium and remote distribution of WSN make it exposed to various types of attacks. An identity based spoofing attacks are especially easy to launch and can cause significant damage to network performance. In this case, it is essential to develop efficient intrusion detection mechanisms to protect WSN from attacks. Even if the identity of a node can be verified through cryptographic authentication, the classical security approaches are not always desirable because of their overhead requirements. To avoid these overheads, some researches use spatial information, a physical property associated with each node, hard to falsify, and not reliant on cryptography, called received signal strength (RSS). This method proposed under the assumption that the sensors are non movable or static. Moreover in wireless sensor network the nodes are not always static and this formulates the problem with considerable false positive and negative rates. The RSS readings are not stable. To overcome the issue, in this paper we propose and extend our intrusion detection system with a powerful statistical tool called Sequential Probability Ratio Test, using the sensor node speed we can detect the spoofing node. If the sensor node speed is less than the system configuration speed than that node is take as a uncompromised node. If the node speed is greater than the system configuration speed that node is taken as a compromised node and the test has bounded false positive and false negative error rates. Compared to contemporary approaches, our proposed method demonstrates higher intrusion detection rates while does not greatly affect the network performances.

Index Terms—Wireless network security, Intrusion detection, Spoofing attack, Received signal strength,

Introduction

A wireless sensor network consists of 'n' number of sensor nodes which are placed in a finite area and it form a network. These nodes sense the sensitive data from the location and send the sensitive data to the base station. The base station will verify the data and then stored or uses for further needs. These networks may be very large systems contains of small sized, low power, low cost sensor devices that collect detailed information about the physical environment [1]. Due to the open nature of the wireless transmission medium, adversaries can monitor the data communications. Further, adversaries can easily purchase low cost wireless devices and use these to launch a variety of attacks. Among various types of attacks, identity based spoofing attacks are easy to launch and can cause significant damage to network performance. Spoofing attacks can further facilitate a variety of traffic injection attacks [2], [3], such as attacks on access control lists, access point (AP) attacks, and Denial of Service (DoS) attacks. Lot of studies for the possible of spoofing attacks can be found in various works [4], [5]. In a large-scale network, multiple attackers may pretense as the same identity and work together to launch malicious attacks such as network resource utilization attack and denial of service attack quickly. Therefore, the research industry needs to detect the presence of spoofing attacks and make the necessary steps to find the prevention mechanism in the wireless sensor network.

Most of the existing approaches address the solution for spoofing attacks by use of cryptographic schemes [6], [7]. However, the solutions of cryptographic schemes require reliable key sharingsn, management, and maintenance mechanisms. It is not always desirable to apply these cryptographic methods because of its infrastructural, computational, and management overhead. In addition, cryptographic methods are vulnerable to node compromise, which is a notable concern as most wireless nodes are easily accessible, allowing their memory to be easily scanned.

In a recent work [8], the authors propose to use received signal strength (RSS) based spatial correlation, a physical property associated with each wireless node that is difficult to falsify and not dependent on cryptography as the basis for detecting spoofing attacks. Since we are assumed with attackers who have different locations than legitimate wireless nodes, utilizing spatial information to address spoofing attacks has the unique power to identify the presence of these. An added advantage of using spatial correlation to detect spoofing attacks is that it will not require any additional cost or modification to the wireless devices themselves.

Software based intrusion detection schemes have been proposed for static sensor networks. The sensor nodes generate the location claims that identify their location and send it to the base station. In this paper we proposed intrusion detection scheme based on the sequential probability ratio test (SPRT) [9]. A benign node should not move at speeds in not exceeds the system configuration speed. The non compromised sensor node should be always nearly or less than the system design speed. That means the non compromised node should never move greater of threshold value. In wireless sensor networks the attacker (spoofing) nodes have same ID present in the network which moves greater than the threshold value, which is taken as a spoofing node.

In centralized detection approach the single base station will verify the full network operation and validates the data which are sending by the sensor nodes. The sequential probability ratio testing is come under centralized detection approach. SPRT is a hypothesis testing method and it contains "null hypothesis (H0)" and "alternate hypothesis" (H1). An non compromised node is taken as a null hypothesis and a compromised node is taken as an alternate hypothesis.

The rest of the paper is organized as follows. We place our work in the context of related work in Section 2. We provide our proposed system and describe the detection model in Section 3. We provide our result and discussions in Section 4. Finally we conclude our conclusion in Section 5.

Related work

Several studies have been proposed in this area where most of them are in intrusion detection mechanisms committed to ad hoc networks. As a result they are not concentrating wireless sensor networks because of its constraints and limitations. There are some researches trying to adapt the solutions to WSNs and propose new solutions. Before study the intrusion detection and avoidance in WSN, initially we describe some of the attacks and their impacts as below;

1. Sybil Attacks

In Sybil attacks the intruder presents itself as it as multiple nodes. This type of attack tries to degrade the usage and the efficiency of the distributed system. Sybil attack can be performed against distributed storage, routing, data aggregation, resource allocation, and misbehavior detection [10].

2. Wormhole Attack

Wormhole attack [11] is an attack in which the intruder node tunnels messages from one part of the network over a link to another part of the network. The simplest way of the wormhole attack is to induce two nodes that they are neighbors. This attack would be used in combination with selective forwarding and eavesdropping.

3. Acknowledgement Attack

Acknowledgement attack is an attack in wireless sensor network, some routing algorithms require link layer acknowledgements. A compromised node may use this by spoofing these acknowledgements, thus influential the sender that a weak link is strong [12].

4. Selective forwarding Attack

Selective forwarding attack a attacker node may not ready to forward every packet it gets, acting as black hole [13] or it can forward some packets to the wrong receiver and simply drop other packets.

5. Sinkhole Attacks

Sinkhole attack [14], the plan of the attacker is to attract all the traffic. Especially, in the case of a flooding based protocol the intruder node may listen to routes requests, and then response to the requesting node with messages containing a fake route with the shortest path to the requested destination.

6. HELLO flood Attacks

Hello flood attack is based on the use by many protocols of broadcast Hello messages to broadcast themselves in the network [15]. So an attacker with greater range of transmission may send many Hello messages to a large number of nodes in a large area of the network. These nodes are then converted that the attacker is their neighbor.

7. Spoofing Attacks

A wide survey of possible spoofing attacks can be found in [4]. In a large scale network, multiple adversaries may use as the same identity and work together to launch malicious attacks such as network resource utilization attack and denial of service attack (DoS). Therefore, it is necessary and important to detect the presence of spoofing attacks then find the mitigation methods.

The above attacks are having their own characteristics or nature in their functionally and impacts. Some of them are needed more functionality or process; some of them are need additional components etc. In addition some attacks make more impacts and some attacks make fewer impacts in the network operation. As a comparison with spoofing attack, it is easy to launch but its impacts on the network operation is more. This motivates us to select spoofing attack detection as our area of interest.

The traditional approach to prevent spoofing attacks is to use cryptographic based authentication [16]. In their study some protocols are used to find the spoofing detection which are centralized protocol and distributed protocol. In centralized protocol, apart from central base station present in the network all other nodes which are present in the networks may communicate with the single base station. If the base station fails the whole network gets failed but in distributed protocol each and every node act as a base station if any of the node gets failed the node will take care of network.

In centralized detection the single base station will verify the whole network operation and it validates the data which are sending by the sensor nodes. Luo et al. [17] have pointed out that infrastructure less ad hoc networks rarely have a real defense mechanism against most of the attacks, including both outsider and insider attacks such as compromised node attacks. They suggested a system design that is if one node is named trusted by certain number of its neighboring nodes, that particular node is trusted both locally and globally. However, the system uses a minimum number of trusted nodes it is not so applicable to sensor networks where the nodes are randomly spread out. In other words, it is possible that under certain conditions nodes cannot find the minimum number of neighboring nodes in order to be named trusted. One solution for location based anomaly detection in a group of nodes is suggested in [18]. Every node gets the localization information from the neighboring nodes and also computes the localization information itself and compares these two values. If the difference is small enough, that node decides there is no adversary around causing the localization problem in its location.

In our related work covers varies attacks and current solution on that attacks. In the case of spoofing attack and detection techniques are discussed. This paper addresses some of the security problems in wireless sensor network problem are discussed. The proposed framework is used detection and revocation of impersonating attack in the network.

Proposed work

1. Wireless Sensor Network (WSN) & Attackers

Wireless sensor network (WSN) refers to a communication system that consists of number of low cost, resource limited sensor nodes to sense important data related to environment and to transmit it to sink node. The WSN is in a hostile environment, where the administrator or human beings have no physical contact with the sensor nodes.

Attacks come in different types and directions. The attacks are conducted from the inside and the outside of the network. External attackers are attackers they are not legally part of the network. They could be part of another network which is linked to the target network using the same infrastructure or same communication technology. This node employs attacks without any authorization on the target network. This attackers may be an outside sensor node, which is not part of the network, but with passive eavesdropping capability. Internal attackers are compromised nodes which are authorized on the target network.

2. Access Architecture of WSN

The proposed technique use the three layer wireless sensor network structure as clustered sensor network, which includes base station layer, sink layer and sensor layer. The base station (BS) layer can act as an interface for WSNs to communicate with satellite. As illustrated in Fig. 1, BS, sink and sensor are the access points (AP) when users access the data in the WSN. Local users access the network directly. However, remote users need access the WSN through satellite.

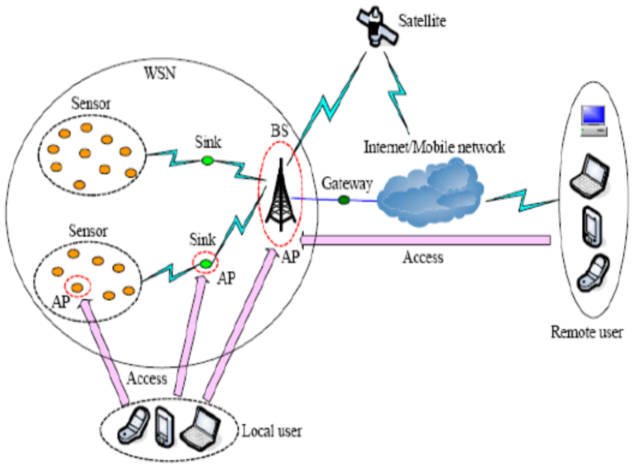

Fig 1: Access architecture of WSN

Two types of approaches exist to protect WSN, that is prevention based approaches such as access control and detection based approaches seems as intrusion detection. If access control and intrusion detection work separately then they may not produce higher security. So the scope of the paper is more concentration on intrusion detection.

Access Control

Access control is an important security service in Wireless sensor network, to prevent malicious nodes entry to the sensor network. On one hand, WSN must be able to authorize right users to the right access to the network. Meanwhile, WSN must organize data collected by sensors in such a way that an unauthorized entity (the adversary) cannot make arbitrary queries. This restricts the network access only to eligible users and sensor nodes, while queries from outsiders will not be answered or forwarded by nodes. The secure authentication protocols of the most current security access schemes have high expenses in computation, storage and communication. Therefore, WSNs need authentication protocol with low expenses.

Intrusion Detection

Intrusion detection developed to be used in traditional networks cannot be applied directly to WSNs, since they demand more resources that are not available in sensor networks. WSNs are typically application oriented, which means they are designed to have very specific characteristics according to the target application. The intrusion detection believe that the normal system behavior is different from the behavior of a attacked system. Normally the intrusion detection system contains three major steps or process monitoring, analyzing and responding.

Monitoring
Analysis
Response

Fig 2 : Architecture of IDS

Spoofing Attack Modeling

The nodes are captured by an adversary can compromise the sensor nodes functionality. These compromised nodes use the same ID and enters in the network. After the control of that node, the attacker can do the necessary changes and make the node to observe the information in the network, input malicious data and make attacks on the network. A node compromise attack often consists of three stages. The first stage is physically obtaining and compromising the sensors; the second stage is redistribute the compromised nodes to the sensor network; and the final stage is compromised sensors launching attacks. So the best intrusion detection system can covers all the three stages in the detection process.

Sequential Probability Ratio Test

In Classical Hypothesis Testing (CHT) the data collection is executed without analysis of the data. After all data are collected the analysis is done and conclusions are drawn. In Sequential Analysis every case is analyzed directly after being collected, the data collected up to that moment is compared with certain threshold values, incorporating the new information obtained from the freshly collected case. This approach allows a final decision can possibly be reached at a much earlier stage as it compared with Classical Hypothesis Testing. The advantages of Sequential Analysis are very simple. As data collection can be terminated after fewer cases and decisions taken earlier.

Proposed Scheme

The enhanced Sequential Probability Ratio Test (eSPRT) which is a statistical hypothesis testing. SPRT has been proven to be the best mechanism in terms of the average number of observations that are required to reach a decision among sequential and non sequential test processes. SPRT can be one dimensional random walk with lower and upper limits.

The null and alternate hypotheses are defined before the random walk starts, in such a way that the null one is related with the lower limit and the alternate one is related with the upper limit. A random walk starts from a point between two limits and moves toward the lower or upper limit in agreement with each observation. If the walk reaches or exceeds the lower or upper limit, it terminates and returns the null or alternate hypothesis.

We believe that SPRT is well suited for tackling the spoofing detection problem in the sense that we can construct a random walk with two limits in such a way that each walk is determined by the observed speed of a mobile node; the lower and upper limits are properly assigned to be associated with the less and excess of the maximum speed of the mobile node, respectively.

We apply SPRT to the mobile spoofing detection problem as follows. Each time a sensor node moves to a new location, each of its neighbors request for a signed claim containing its location and time information and decides probabilistically whether to forward the received claim to the base station. The base station computes the speed from every two consecutive claims of a sensor node and performs the SPRT by taking speed as an observed sample.

Each time maximum speed is exceeded by the mobile node, it will rush the random walk to strike or cross the upper limit and thus it decides that the base station accepting the alternate hypothesis that the mobile node has been spoofed.

On the other hand, each time the maximum speed of the sensor node is not reached, it will expedite the random walk to hit or cross the lower limit and thus lead to the base station accepting the null hypothesis that mobile node has not been spoofed.

Once the base station decides that a mobile node has been spoofed, it initiates revocation on the spoofing nodes. The false positive rate and false negative rate are minimized using SPRT a hypothesis testing method that can make decisions quickly and accurately. In null hypothesis the mobile nodes are not been spoofing but in alternate hypothesis the nodes get spoofed. If the alternate hypothesis is accepted the spoofed nodes are revoked from the network. The base station sends the coverage region to all the nodes. Then the sensor nodes gather the data and sent to base station, the base station verifies the data.

Using the sensor node speed we can detect the spoofing node. If the sensor node speed is less than the system configuration speed than that node is take as a non-compromised node. If the node speed is greater than the system configuration speed that node is taken as a compromised node and if the node is compromised in the particular location then the neighbor node will take care of that particular region and sense the data and finally secure communication takes place.

After deploying the nodes the base station sends the region request 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 spoofing nodes takes place.

Using the hypothesis testing method the spoofing nodes are detected. If null hypothesis is accepted then the spoofing nodes are detected and revoked from the network. A sensor node may be a malicious node or a normal node that generating alarms.

Algorithm process for enhanced SPRT:

```
Decelerations : n=0,wn=0
Inputs : Location information L and time information T
Outputs : Return hypothesis H0 or H1
curr_loc=L
curr_time=T
if n>0 then
    Compute T0(n) and T1(n) // Low and High Thresholds
    Compute speed S // using curr_loc and prev_loc, curr_time and prev_time
    if S>Vmax then
        wn=wn+1
    end if
    if wn>=T1(n) then
        Accepts the hypothesis H1 and terminate the test
    end if
    if wn<=T0(n) then
        initialize n and wn to 0
        Accepts the hypothesis H0
        return;
```

```
end if
end if
n=n+1
prev_loc=curr_loc
prev_time=curr_time
```

Performance analysis

The metrics to evaluate the performance of this scheme:

1. Number of Claims is the average number of claims required for the base station to decide whether a node has been spoofed or not.
2. False Positive is the error probability that a benign node is misidentified as a spoofing node.
3. False Negative is the error probability that a spoofing node is misidentified as a benign node.

Three metrics are defined to evaluate the performance of the proposed technique. The first metric is response time, which is the average detection cycles of correctly detected malicious nodes shows how fast malicious nodes can be detected. The Detection rate, which is the ratio of the number of detected malicious nodes and the number of total malicious nodes, indicates the effectiveness of our scheme. The misdetection ratio, which is the ratio of misdetected nodes to all detected nodes including correctly detected and misdetected nodes. Generally these misdetected nodes consist of two things:

1. The number of normal nodes being treated as malicious ones and
2. The number of malicious node being treated as normal nodes.

We have compared our proposed scheme Sequential Probability Ratio Test (SPRT) with Classical Hypothesis Test (CHT)

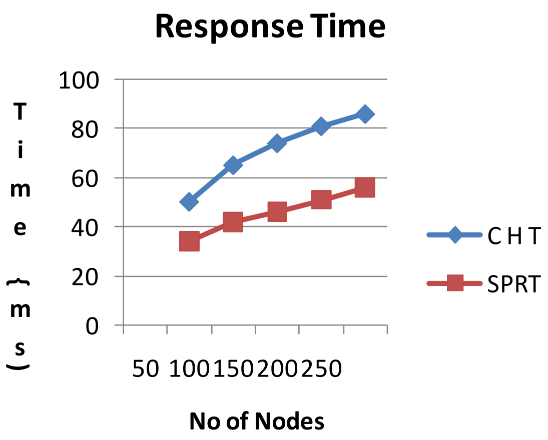

Fig 3 (a) Response Time Comparison

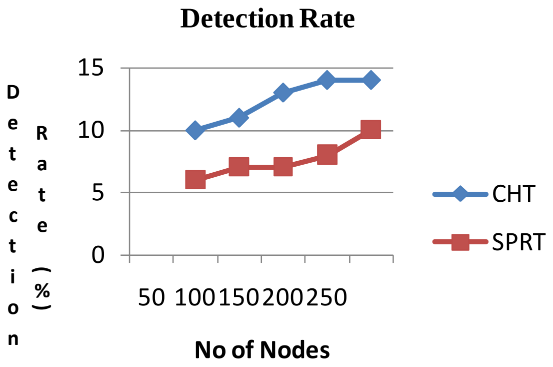

Fig 3 (b) Detection Rate Comparison

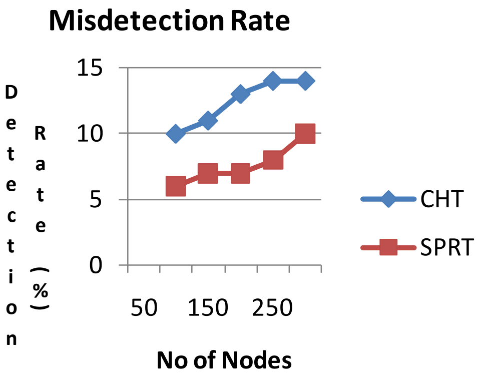

Fig 3 (c) Misdetection Rate Comparison

The above graphs 3 (a), (b) & (c) shows our proposed intrusion detection scheme, short response time, high detection rates are desired as well as a low misdetection ration.

Conclusion

The nature and characteristics of WSN, there is multiple changes for various types of attacks. An identity based spoofing attacks can cause significant damage to network performance. Even if the identity of a node can be verified through cryptographic authentication the classical security approaches are not always desirable because of their overhead requirements. To avoid these overheads, a physical property associated with each node, hard to falsify, and not reliant on cryptography, called received signal strength (RSS). This method proposed under the assumption that the sensors are non movable or static. Moreover in wireless sensor network the nodes are not always static. To overcome the issue, in this paper we propose and extend our intrusion detection system with a powerful statistical tool called Extended Sequential Probability Ratio Test (SPRT), using the sensor node speed the test can detect the spoofing node. The comparison studies states, our proposed method produced higher intrusion detection rates and does not greatly affect the network performances.

References

[1] L. Hu and D. Evans, “Localization for Mobile Sensor Networks,” Proc. ACM MobiCom, pp. 45-57, Sept. 2004.

[2] J. Bellardo and S. Savage, “802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions,” Proc. USENIX Security Symp., pp. 15-28, 2003.

[3] F. Ferreri, M. Bernaschi, and L. Valcamonici, “Access Points Vulnerabilities to Dos Attacks in 802.11 Networks,” Proc. IEEE Wireless Comm. and Networking Conf., 2004.

[4] D. Faria and D. Cheriton, “Detecting Identity-Based Attacks in Wireless Networks Using Signalprints,” Proc. ACM Workshop Wireless Security (WiSe), Sept. 2006.

[5] Q. Li and W. Trappe, “Relationship-Based Detection of Spoofing Related Anomalous Traffic in Ad Hoc Networks,” Proc. Ann. IEEE Comm. Soc. on IEEE and Sensor and Ad Hoc Comm. and Networks (SECON), 2006.

[6] B. Wu, J. Wu, E. Fernandez, and S. Magliveras, “Secure and Efficient Key Management in Mobile Ad Hoc Networks,” Proc. IEEE Int’l Parallel and Distributed Processing Symp. (IPDPS), 2005.

[7] A. Wool, “Lightweight Key Management for IEEE 802.11 Wireless Lans With Key Refresh and Host Revocation,” ACM/Springer Wireless Networks, vol. 11, no. 6, pp. 677-686, 2005.

[8] Jie Yang, Yingying (Jennifer) Chen, Jie Yang, “Detection and Localization of Multiple Spoofing Attackers in Wireless Networks”, IEEE Transaction on Parallel and Distributed System Vol. 24, No 1, January 2013.

[9] J. Jung, V. Paxon, A.W. Berger, and H. Balakrishnan, “Fast Portscan Detection Using Sequential Hypothesis Testing,” Proc.IEEE Symp. Security and Privacy, pp. 211-225, May 2004.

[10] J. Newsome. E.Shi, D. Song and A. Perrig, “The Sybil Attack in Sensor Networks, Analysis & Defends”, Proc. Of The Third International Symposium on Information Processing in Sensor Networks, ACM 2004, PP 259-268.

[11] Y.C.Hu, A. Perrig and D.B Johnson, “Wormhole Detection in Wireless Adhoc Networks”, Dept. of Computer Science, Rice University, Tech Rep. TR01-384, June 2002.

[12] Joglekar C.M.& Naoghare M.M. “Acknowledgement based Security for Manets Against DDOS attacks” OSR Journal of Electronics and Communication Engineering PP 18 – 23

[13] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao, “A survey of black hole attacks in wireless mobile ad hoc networks” Human-centric Computing and Information Sciences 2011, 1 : 4.

[14] Edith C. H. Ngai, Jiangchuan Liu,and Michael R. Lyu, “On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks “

[15] Akhil Dubey, Deepak Meena, Shaili Gaur, “ A Survey in Hello Flood Attack in Wireless Sensor Networks”, International Journal of Engineering Research & Technology Vol. 3 - Issue 1 (January - 2014)

[16] A. Wool, “Lightweight Key Management for IEEE 802.11 Wireless Lans With Key Refresh and Host Revocation,” ACM/Springer Wireless Networks, vol. 11, no. 6, pp. 677-686, 2005.

[17] Haiyun Luo, Petros Zerfos, Jiejun Kong, Songwu Lu, Lixia Zhang, “Self-securing Ad Hoc Wireless Networks,” IEEE ISCC (IEEE Symposium on Computers and Communications) 2002, Italy.

[18] W. Du, L. Fang, and P. Ning, “LAD: Localization Anomaly Detection for Wireless Sensor Networks,” the 19th International Parallel and Distributed Priocessing Symposium (IPDPS’05), April 3 – 8, 2005, Denver, Colorado, USA.