IDS in WSN Based on Spy Node & Trust based Scheme

Nidhi Kundu¹ Navneet Verma²
¹,²Department of Computer Science and Engineering
¹,²Geeta Engineering College Naultha, Panipat

Abstract— Wireless sensor networks (WSNs) are highly susceptible to security attacks at various levels due to resource constraints nature of sensor nodes. Since sensor nodes are resource constrained so we will put a mobile spy in WSN which will take data from every sensor node. Intrusion Detection Systems (IDSs) play an important role in detecting security attacks. Intrusion detection is a process of monitoring the events occurring in a computer system or network and analyzing them for signs of intrusions to have the security mechanisms of a network. Mostly IDS don’t show interaction among various layers of OSI Model. So these systems are not that much efficient.

Figure 1: WSN Design.

Keywords: Wireless Sensor Networks (WSNs), Intrusion Detection System (IDS)

I. INTRODUCTION

Typically, WSNs contain a large number of sensor nodes, which are densely and randomly deployed in the field under study as shown in figure 1. Each of these scattered sensor nodes has the capabilities to collect data and route data back to a collection point called a Sink. Data are forwarded to the Sink through a multihop wireless architecture as shown in figure 1. Once the collected data reach the sink, it has to route them to the task manager, where the appropriate decisions can be made. The sink may communicate with the task manager node via Internet or satellite. There are three types of reporting: event-driven, on-demand, and continuous monitoring. In the event-driven reporting, the sensor network is tailored to detect the occurrence of a pre-specified type of event within the sensor field. Once this event occurs, the reporting task is initiated and the related information is forwarded to the Sink. Thus communication is triggered by the event occurrence and only nodes within the event area become sources of communication. The most famous detection based applications are: fire, food detection and alarms. In the on-demand reporting, communication is initiated by the Sink, and sensor nodes send their data in response to an explicit request.
Researchers in WSNs are working on two broad categories of IDSs, that is, signature-based and anomaly-based IDSs.

A. Signature-Based Intrusion Detection Systems

Signature based IDS, also known as rule-based IDS, has predefined rules of different security attacks. When the network’s behaviour shows any deviation from the predefined rules, it is classified as an attack. Signature-based IDSs are well suited for known intrusions; however they cannot detect new security attacks or those attacks having no predefined rules. In this section, we present existing signature-based IDSs for WSNs. It is host based in which every node has IDS.

B. Anomaly-Based Intrusion Detection Systems

Anomaly based IDS monitors network activities and classifies them as either normal or malicious using heuristic approach. Most of anomaly-based IDSs identify intrusions using threshold values; that is, any activity below a threshold is normal, while any condition above a threshold is classified as an intrusion. The main advantage of anomaly-based IDS is its capability to detect new and unknown attacks; however sometimes it fails to detect even well-known security attacks.

C. Hybrid Intrusion Detection Systems

Hybrid IDSs are a combination of both anomaly-based and signature-based approaches. Hybrid mechanisms usually contain two detection modules; that is, one module is responsible of detecting well-known attacks using signatures, while the other is responsible for detecting and learning normal and malicious patterns or monitor network behavior deviation from normal profile.

D. Cross Layer Intrusion Detection Systems

Cross layer design is a relatively new security technique in which different parameters across OSI layers are exchanged for optimal solutions. Traditional IDS operates at a single layer of the OSI model and hence can monitor and detect intrusions at that particular layer. For example, network layer Intrusion Detection System can detect only routing attacks but cannot respond to MAC, physical, or transport layer anomalies. Cross layer IDSs have the capability to monitor and detect intrusions at multiple layers by communicating and exchanging parameters amongst different layers using cross layer interface. As we know, WSNs have many constraints in terms of computations, memory, and energy. Although cross layer IDS can detect many intrusions at different layers, this technique consumes more energy and computational resources by monitoring, analyzing, and exchanging multilayer parameters.

II. Overview of Security in Wireless Sensor Networks

WSNs are vulnerable to many types of security attacks due to open wireless medium, multihop decentralized communication, and deployment in hostile and physically unprotected areas. Security attacks against WSNs can be classified as active and passive. Passive attacks are silent in nature and are conducted to extract important information from the network. Passive attacks do not harm the network or network resources. Active attacks are used to misdirect, temper, or drop packets. The unique characteristics such as wireless medium, contention-based medium access, multihop nature, decentralized architecture, and random deployment of such networks make them more vulnerable to security attacks at various layers. Physical layer of WSN is responsible for radio and signals management. Radio jamming is one of the severe attacks against WSN. Another physical layer attack is battery exhaustion attack. In a WSN, battery power of sensor nodes plays an important role and determines the lifetime of the network. Keeping in view the power limitations of WSNs, it is highly desirable to design power efficient mechanisms for sustainable WSNs. Sensor nodes in sleep mode consume less energy as compared to active mode. In energy exhaustion attack, the attacker tries not to allow sensor nodes to switch to sleep mode. This can be done by sending unnecessary data or beacons to sensor nodes to keep them always busy. As WSNs are deployed in hostile environment, it is susceptible to many physical attacks such as node destruction, node replacement, node replication, battery replacement, or reprogramming of node with malicious code. However such attacks need to physically access the network. Most WSNs use contention based carrier sense multiple access with collision avoidance mechanism (CSMA/CA). This mechanism tries to avoid collision; however it adds more complications in the form of collision, hidden-node problem, MAC selfishness, and unfairness. Possible countermeasures against such kind of attacks are small frames and rate limitations. Network layer is responsible for appropriate route selection from source to destination. In WSN, the multihop route from source to destination is vulnerable to many active and passive attacks. Active attacks include packet dropping attacks, packet misdirecting attacks, rushing attack, Sybil attack, by zantine attack, routing table overflow attack, spoofed routing information, hello flood, and acknowledgement spoofing.

III. Related Search

We have analyzed that WSNs have special vulnerabilities that do not exist in wire-line networks. Therefore, our protocols can’t be simply transferred for wire-line networks to WSNs. Protocols must be designed with low computational power and low energy requirements in mind. In this paper it has been seen some of the protocols that are used, as well as some ways to determine where to check packets, including a new game theoretic approach in which it has been observed that by allowing the attack to have some utility, author is able to increase through energy saving for sufficiently large, resource constrained networks. In(1) author proposed while designing a security...
mechanism, we must consider the limited resources of WSNs. Anomaly-based IDSs are lightweight in nature; however they create more false alarms. Signature-based IDSs are suitable for relatively large-sized WSNs; however they have some overheads such as updating and inserting new signatures. Cross layer IDSs are usually not recommended for networks having resources limitations, as more energy and computation are required for exchanging multilayer parameters. In (2) author proposed the development of an Intrusion Detection Program (IDP) which could detect known attack patterns. An IDP does not eliminate the use of any preventive mechanism but it works as the last defensive mechanism in securing the system. Three variants of genetic programming techniques namely Linear Genetic Programming (LGP), Multi-Expression Programming (MEP) and Gene Expression Programming (GEP) were evaluated to design IDP. Several indices are used for comparisons and a detailed analysis of MEP technique is provided. Empirical results reveal that genetic programming technique could play a major role in developing IDP, which are light weight and accurate when compared to some of the conventional intrusion detection systems based on machine learning paradigms. In (3) author considered the problem of cooperative intrusion detection in wireless sensor networks where the nodes are equipped with local detector modules and have to identify the intruder in a distributed fashion. The detector modules issue suspicions about an intrusion in the sensor’s neighborhood. We formally define the problem of intrusion detection and identify necessary and sufficient conditions for its solvability. Based on these conditions we develop a generic algorithm for intrusion detection and present simulations and experiments which show the effectiveness of our approach. In (4) Many intrusion detection system (IDS) have been proposed by author to secure WSNs. But all these systems operate in a single layer of the OSI model, or do not consider the interaction and collaboration between these layers. Consequently these systems are mostly inefficient and would drain out the WSN. In this paper a new intrusion detection system based on cross layer interaction between the network, Mac and physical layers has been proposed. Indeed it addressed the problem of intrusion detection in a different way in which the concept of cross layer is widely used leading to the birth of a new type of IDS. The proposed is experimentally evaluated using the NS simulator to demonstrate its effectiveness in detecting different types of attacks at multiple layers of the OSI model. In (5) author have illustrated MAC address based intruder tracking system for cluster based wireless sensor networks. This proposed system implements base station based detection and thus is very energy-efficient for early detection and prevention of security threats and attacks. Early detection and prevention of the intruder by efficient security system can prevent many problems like slowing down of the network, sending of fake data, etc. By designing a security system in which the Base Station (BS) keeps track of the security of the Wireless network, high security can be ensured without any significant energy overheads on individual nodes and cluster heads. In (6) Sensors are used by author to sense the temperature, humidity, light, voltage etc in a particular area. Extended Kalman Filter (EKF) mechanism is proposed to filter the false data in sensor network. The false data can be acted by some event namely malicious, emergency event. Malicious event a reacted by intruders, and Emergency event are acted by some accident occurrence e.g. Fire. Intruders make the sensors to get the false reading therefore EKF mechanism is proposed. EKF monitors the behaviour of neighbours and predict their future states, each node aims at setting up normal range of the neighbor’s future transmitted aggregated values. Using different aggregation functions (average, sum, max, and min), theoretical threshold value is calculated. Combining Cumulative Summation (CUSUM) and Generalized Likelihood Ratio (GLR) detection sensitivity can be increased. Intrusion Detection Modules (IDM) and System Monitoring Modules (SMM) work together in order to provide intrusion detection capabilities for WSNs. EKF address various uncertainties in WSNs and create an effective local detection mechanism. In (7) an Advanced Intrusion Detection System has been proposed by author. It improves the detection rate and efficiency so that almost all the Intrusions can be detected. Also the systems applicable to small, medium as well as large sized networks. That means it gives a wide range of flexibility in detection of Intrusions compared to the other existing systems. Also the energy efficiency and the system life time is greatly improved. In (8) author presented in detail a secure routing protocol for WSN which is based on ant colonization technique. Hellopackets are used for surrounding neighbor’s discovery. This mechanism uses forward ants which collect and increment the reputation values along the path. Similarly, destination node uses backward ants which carry information and instruction from destination node about route security. The proposed mechanism uses two paths for data forwarding not only to overcome the problem of node failure but also to increase the efficiency of overall network. When compared to other routing protocols such as iACO and LEACH, our proposed routing scheme shows better performance in terms of end to end delay, routing overheads, and data forwarding efficiency. Furthermore, the proposed mechanisms show high data delivery rate in the presence of malicious nodes. In (9) author proposed a model to identify malicious node from real-world datasets within a non WSN. This model ensured the data integrity within LN and BS by deploying a detection engine within the MDC. In simulation, the results show that we can achieve ~95% of detection rates based on our measured causing the real data. In terms of the true alarm rate, the proposed algorithm outperforms. It has been noted that detection ratio has an impact on selecting the threshold value. Proposed algorithm results suggest that the finding optimum threshold can lead to more effective anomaly detection. In particular, these results confirm that the proposed algorithm can maintain acceptable anomaly detection accuracy while using just half of the input data.

IV. COMPARISON AND DISCUSSION

WSN suffers from various attacks by anomaly nodes. These nodes are stated as intruders which can alter the message passed to base station. As WSN is used in various applications like in emergency data transfer, military applications, surveillance etc. so requirement of accurate information is necessary, but if any intruder is active in the network and unidentified then false information can be transferred to head which may lead to dire consequences. So
it is necessary to detect these anomaly nodes. For this many problems are faced some of them which are considered in our work, after literature survey are: WSN is a resource constrained and energy constrained network. So there is always scarcity of resources and battery in sensor nodes so conventional IDS can’t be used for WSN. Many IDS presented by researchers are limited to only network layer due to which many types of attacks by intruders may go unidentified. So detection scheme should be such that it can analyze the anomaly node at each OSI layer so that attacking probability decreases or in other words cross layer detection scheme should be tried. Crossover detection has a problem of using different IDS at each layer which consumes more energy and resources too. So a generalize algorithm for almost all type of attacks should be proposed.

V. CONCLUSION

Taking security as main objective, we will propose an intrusion detection system based on Spy node dedicated for wireless detection system. In our proposal the problem is discussed in a way as sensor nodes are resource constrained so we will put a mobile spy in WSN which will take data from every sensor node. The establishment of WSN network can be done by three methods, out of which we will select unsupervised learning for WSN nodes distribution as it don’t require prior training. Detection mechanism has to be deployed on each node which consumes battery of node, rather than we will deploy this only on spy node as it will have the information of every sensor node. Trust based detection mechanism will be followed for intruder detection in spy node and results will be shown in form of false alarms in case of different attacks in network.

REFERENCE


