Intrusion Detection Systems in Wireless Sensor Networks

Vijay Kumar Mallarapu¹, K.V.D.Sagar²

¹Pursuing M.Tech(CS) from Nalanda Institute of Engineering & Technology, Siddharth Nagar, Sattenapalli, Guntur., Affiliated to JNTUK, Kakinada, A.P., India.

²Asst. Professor, Department of Computer Science Engineering, Nalanda Institute of Engineering & Technology, Siddharth Nagar, Sattenapalli, Guntur., Affiliated to JNTUK, Kakinada, A.P., India.

vijaymallarapu@gmail.com

Abstract— Wireless Sensor Networks (WSNs) are a new technology foreseen to be used increasingly in the near future due to their data acquisition and data processing abilities. Security for WSNs is an area that needs to be considered in order to protect the functionality of these networks, the data they convey and the location of their members. The security models & protocols used in wired and other networks are not suited to WSNs because of their severe resource constrictions. In this paper, we describe various threats to WSN and then examine existing approaches to identify these threats. Finally, we propose an intrusion detection mechanism based on these existing approaches to identifying threats.

Keywords— Wireless sensor network, Threats, Intrusion detection system.

1. Introduction

Wireless sensor networks (WSNs) have emerged as one of the hottest research areas in recent years. Numerous potential economically viable applications include environment monitoring, health monitoring, and military applications [1]. WSNs typically consist of small inexpensive devices deployed in open, unprotected, and unattended environments for long term operations to monitor and collect data. This data is subsequently reported back to a base station over a wireless link. A WSN is vulnerable to various attacks; hence security is an important factor in the design of WSNs. However, sensor nodes have limited memory, power, computational capability, and transmission range [1], so security needs to be implemented keeping in mind these limited resources. In general, security solutions for WSNs can be categorized into two main techniques; prevention based and detection based. Prevention techniques such as encryption and authentication are tricky for WSNs because of the limited resources and the use of a broadcast medium. Detection techniques identify the attacks based on the system’s behavior. WSNs can be categorized into two types based on the nodes’ capabilities [2]: a homogeneous network where every sensor node has same capability and a heterogeneous network where some of the nodes have greater capabilities (such as longer transmission range). This paper describes the security threats and various kinds of attacks on WSNs and describes the need for an intrusion detection system (IDS) in WSNs. We mention some existing approaches to implement IDS for a WSN. As the last step an intrusion detection approach is specified.

2. Security Threats and Attacks on Sensor Networks

Wireless networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Furthermore, wireless sensor networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected.

A. Passive Information Gathering

An intruder with an appropriately powerful receiver and well designed antenna can easily pick off the data stream. Interception of the messages containing the physical locations of sensor nodes allows an attacker to locate the nodes and destroy them. Besides the locations of sensor nodes, an adversary can observe the application specific content of messages including message IDs, timestamps and other fields. To minimize the threats of passive information gathering, strong encryption techniques needs to be used.
B. Subversion of a Node

A particular sensor might be captured, and information stored on it (such as the key) might be obtained by an adversary. If a node has been compromised then how to exclude that node, and that node only, from the sensor network is at issue.

C. False Node and malicious data

An intruder might add a node to the system that feeds false data or prevents the passage of true data. Such messages also consume the scarce energy resources of the nodes. This type of attack is called “sleep deprivation torture” in [3]. Insertion of malicious code is one of the most dangerous attacks that can occur. Malicious code injected in the network could spread to all nodes, potentially destroying the whole network, or even worse, taking over the network on behalf of an adversary. A seized sensor network can either send false observations about the environment to a legitimate user or send observations about the monitored area to a malicious user. By spoofing, altering, or replaying routing information, adversaries may be able to create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, increase end-to-end latency, etc. Strong authentication techniques can prevent an adversary from impersonating as a valid node in the sensor network.

D. The Sybil attack

In a Sybil attack [4], a single node presents multiple identities to other nodes in the network. They pose a significant threat to geographic routing protocols, where location aware routing requires nodes to exchange coordinate information with their neighbors to efficiently route geographically addressed packets. Authentication and encryption techniques can prevent an outsider to launch a Sybil attack on the sensor network. However, an insider cannot be prevented from participating in the network, but (s)he should only be able to do so using the identities of the nodes (s) he has compromised. Using globally shared keys allows an insider to masquerade as any (possibly even nonexistent) node. Public key cryptography can prevent such an insider attack, but it is too expensive to be used in the resource constrained sensor networks. One solution is to have every node share a unique symmetric key with a trusted base station. Two nodes can then use a Needham- Schroeder like protocol to verify each other’s identity and establish a shared key. A pair of neighboring nodes can use the resulting key to implement an authenticated, encrypted link between them. An example of a protocol which uses such a scheme is LEAP [5], which supports the establishment of four types of keys.

D. Sinkhole attacks

In a sinkhole attack, the adversary’s goal is to lure nearly all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the adversary at the center. Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes with respect to the routing algorithm. For instance, an adversary could spoof or replay an advertisement for an extremely high quality route to a base station. Due to either the real or imagined high quality route through the compromised node, it is likely each neighboring node of the adversary will forward packets destined for a base station through the adversary, and also propagate the attractiveness of the route to its neighbors. Effectively, the adversary creates a large “sphere of influence”, attracting all traffic destined for a base station from nodes several hops away from the compromised node.

E. Wormholes

In the wormhole attack [6], an adversary tunnels messages received in one part of the network over a low latency link and replays them in a different part. The simplest instance of this attack is a single node situated between two other nodes forwarding messages between the two of them. However, wormhole attacks more commonly involve two distant malicious nodes colluding to understate their distance from each other by relaying packets along an out-of-bound channel available only to the attacker. An adversary situated close to a base station may be able to completely disrupt routing by creating a well-placed wormhole. An adversary could convince nodes who would normally be multiple hops from a base station that they are only one or two hops away via the wormhole. This can create a sinkhole: since the adversary on the other side of the wormhole can artificially provide a high quality route to the base station, potentially all traffic in the surrounding area will be drawn through her if alternate routes are significantly less attractive.

3. Existing Intrusion Detection Approaches

Intrusion detection is a set of actions that discover, analyze, and report unauthorized and damaging activities. The goal is to detect violations of confidentiality & integrity, and reduced availability of resources. An IDS monitors the network and improves the user’s activity to detect intrusion. Generally, there are two major types of detection techniques: signature detection and anomaly
detection. Signature detection is based on creating a profile of known attack signatures, then an IDS implements signature detection by comparing current activity with each of the stored attack profiles. The system generates an alarm if a match is found. Unfortunately, signature based detection will fail to detect new types of attack. In contrast, anomaly detection creates normal profiles of system behavior. It compares the system’s normal profile(s) with the current activity. The main drawback of anomaly based technique is that it generates lots of false alarms. A new approach is specification based technique. This alternative combines the advantages of both signature based and anomaly based intrusion detection system by using manually developed specifications to describe the normal system behavior, thus, reducing the rate of false alarms. In [7], Y. Wang divides intrusion detection techniques into single-sensing detection and multi-sensing detection. In single-sensing detection, the intruder can be successfully detected by one sensor. While in multisensing detection, multiple collaborating sensors are used to detect the intrusion.

Several intrusion detection techniques have been proposed for use in ad hoc networks. However, many of these IDS solutions cannot be implemented in sensor networks because of the limited resources in the sensor nodes. In this section, we will describe some existing proposals for intrusion detection in WSNs.

F. Anomaly Intrusion Detection

V. Bhuse and A. Gupta in [8] describe a system for intrusion detection based on anomaly intrusion detection techniques in multiple layers detection system more robust. In their approach, they try to detect intrusion based on physical, link, network, and application layers. At the physical layer, the Received Signal Strength Indicator (RSSI) value is used to detect anomalies. During neighbor discovery, each node records the RSSI value received from its neighbor. Therefore, any node receiving a packet with an unexpected RSSI value will generate an alarm. However, this has a high positive false alarm rate because the RSSI value is affected by the background noise. At the link layer, if a time scheduling algorithm is used to allocate time slots to each node, and then if node A receives packets from node B when B is supposed to be sleep an alarm will be raised.

G. Distributed approach for detecting sink hole and false node attack

Krontiris, Tassos, and Felix in [9], proposed an IDS in each sensor node with two rules for detecting a sink hole and false node attack. They propose that if a node is sending messages, then its entire neighbor will monitor this node. The first rule is, if the node A sends a packet to node B, then the monitoring node stores the packet in its buffer and watches to see whether B forwards it or not. If B does not forward the packet, then a counter is incremented by one. When the failure count exceeds a threshold value, then an alarm will be raised. The second rule is: if the majority of the monitor nodes have raised an alert, then the target node is compromised.

H. Spontaneous watchdog

Roman, Zhou, and Lopez proposed a novel technique to monitor neighbors named “spontaneous watchdog” [10]. They utilize (1) a local agent that monitors local activities and the information exchanged each sensor and (2) a global agent that monitors the communication between neighbors. Their spontaneous watchdog technique relies on the broadcast nature of sensor networks. Their global agent works as a spontaneous watchdog. Initially, all active nodes will receive the packets because of the broadcast nature of the transmission. When a node receives a packet, then it will check if it is the destination of the packet. If it is not, then it will drop the packet. The node will also check whether the receiver is in its neighborhood. If so, then this node will act as a spontaneous watchdog and will verify how many nodes activated themselves as spontaneous watchdog.

4. Proposed Intrusion Detection Approach

In this section, we propose an intrusion detection system for wireless sensor network. Our intrusion detection system is a four layer architecture and uses the specification based detection technique. The following subsections describe our architecture and techniques in more detail.

Our network architecture is based on four layers. The bottom layer consists of all leaf level sensors that collect data from the environment. The second and third layers consist of monitor nodes; where the second layer monitors the communication pattern of leaf level sensors. Level 3 sensors monitor the behavior of level 2 sensors. The placement of level 3 sensors should be such that each can monitor the communication of two level 2 sensors. Finally, the top layer is the base station, usually operated by a human. Figure 1 illustrates how the sensor nodes are organized into a network. This approach requires a heterogeneous network with level 2 and level 3 sensors being more powerful than the leaves in terms of both transmission range and battery life.
All the leaf level sensors deployed in the network are divided into several groups. This network partition can be done using the delta grouping algorithm [11]. For each group we deploy one level 2 sensor to monitor the group. Level 2 and level 3 sensors implement the IDS solution. Each leaf level sensor sends data to a level 2 sensor. The level 2 sensor aggregates all the data and sends it to a level 3 sensor. Level 3 sensors monitor the level 2 sensor’s behavior. Each level 3 sensor must be placed within range of two level 2 sensors from where it can watch the communication of these two sensors. If an anomaly is detected by a level 2 sensor, it raises an alarm and sends it to level 3, where the alert is investigated and if it is valid, then an alarm with aggregated data is sent to the base station.

We have modified the intrusion detection algorithm proposed by Da Silva, et al. [12] and implemented in our level 2 and level 3 sensors. Due to their limited resources, we have not implemented any IDS in the leaf level sensors. Monitor nodes functionalities are divided into three phases. Phase 1 all the leaf level sensors collect information from their environments and report it to the level 2 sensors. In phase 2, rather than using the rules described in [12], we have used layer based attack detection in phase 2 to detect attacks as proposed in [8]. Phase 3 compares each report to the defined the threshold value to decide whether it should raise an alarm. Phase 3 is used to reduce the false alarm rate. Threshold values can be defined manually or adjusted based on the requirements of a particular WSN. Thus, our proposed architecture can detect most of the security threats by reducing the false positive alarms.

5. Conclusion

In this paper, we have presented the security threats and challenges in WSNs. We investigated several existing intrusion detection approaches to learn how they have implemented their intrusion detection. We proposed a hierarchical intrusion detection system based on a synthesis of the existing approaches. Future work will focus on implementing our proposed architecture on a simulator.

REFERENCES


AUTHORS PROFILE

Vijay Kumar Mallarapu, Pursuing M.Tech(CS) from Nalanda Institute of Engineering & Technology, Siddharth Nagar, Sattenapalli, Guntur Affiliated to JNTUK, Kakinada, A.P., India. My research Interests are computer networks and Mobile computing.

K.V.D Sagar, working as Asst.Professor, Department of Computer Science Engineering at Nalanda Institute of Engineering & Technology, Siddharth Nagar, Sattenapalli, Guntur Affiliated to JNTUK, Kakinada, A.P., India. My research Interests are Mobile Computing, Network Security and Mobile Networks. He is a Life member of MISTE.