Detection and Mitigation of Intrusion in Cluster Based Wireless Sensor Networks

Sivarajan. A¹ Arunbalaji. N²
¹Department of Communication and Networking ²Department of Electronics and Communication
¹,²P.B College of Engineering, Sriperumbuthur, India

Abstract— Intrusion Detection plays an important role in the area of security in WSN. Detection of any type of intruder is essential in case of WSN. WSN consumes a lot of energy to detect an intruder. In order to operate WSNs in a secure and energy efficient way, any kind of intrusions should be detected before attackers can harm the network (i.e., sensor nodes). Therefore, an Cluster Based IDS approach for energy efficient intrusion detection in WSN is proposed in this paper. First, a detailed information about WSN and IDS is defined. Secondly, Cluster based IDS is proposed for WSN. Finally, the survey is concluded by highlighting open research issues in the field.

Key words: intrusion detection, IDS, security, cluster, WSN

I. INTRODUCTION

Wireless sensor network (WSN) are spatially distributed autonomous sensors to monitor physical or environmental conditions such as pollution, earthquake, water quality, temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on[6].

The WSN is built of "nodes" from a few to several hundreds or even thousands, where each node is connected to one or several sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning “motes” of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.

Security attacks against WSNs are classified into two groups: Active and Passive attacks. In passive attacks, The attackers are monitoring and listening of the communication channel by unauthorized attackers are known as passive attack. The attacks against privacy is passive in nature. The main privacy problem is not that sensor networks enable the collection of information. In fact, much information from sensor networks could probably be collected through direct site surveillance. Passive attacks are Monitor and Eavesdropping, Traffic Analysis, Camouflage Adversaries. In Active attacks, The unauthorized attackers monitors, listens to and modifies the data stream in the communication channel are known as active attack. The Active attacks are Routing Attacks in Sensor Networks, Denial of Service Attacks, Node Subversion, Node Malfunction, Node outage, Physical Attacks, Message Corruption, False Node, Node Replication Attacks, Passive Information Gathering[3][7].

There are three main components is used to prevent, detect and react against security attacks in networks[1]:

1) Prevention: It is used to prevent any attack before it happens. Any proposed technique will have to defend against the targeted attack.
2) Detection: In any case the prevention step is failed to defend against the attack. At this time, the security solution would immediately switch into the ‘detection’ phase of the attack in progress and specifically identify the nodes that are being compromised.
3) Mitigation: Mitigate any attack after it happens by removing the affected nodes and securing the network.

Intrusion is an unauthorized activity in a network that is either achieved or actively. In a security system, if the first line of defense, “Intrusion Prevention,” does not prevent intrusions, then the second line of defense, “Intrusion Detection,” comes into play. It is the detection of any suspicious behavior in a network performed by the network members. The intrusion in WSN will be detected using the detection methodologies, whenever the prevention step failed to do the process at the detection technique is used to detect the intrusion in the wireless sensor networks. Finally, By removing the affected node in the network and securing remaining nodes in the network[5].

Intrusion Detection Systems (IDSs) provide some or all of the following information to the other supportive systems: identification of the intruder, location of the intruder, time of the intrusion, intrusion activity, intrusion type, layer where the intrusion occurs. This information would be very helpful in mitigating and remedying the result of attacks, since very specific information regarding the intruder is obtained. Therefore, intrusion detection systems are very important for network security. WSNs have unique characteristics such as limited power supply, low transmission bandwidth, small memory size and data storage. At the time intrusion prevention and detection...
performs their operation in WSN, it consumes high amount power from the network that is the major problem placed in it.

II. INTRUSION DETECTION SYSTEMS (IDSs)
An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. IDS come in a variety of “flavors” and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPS for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IDPS have become a necessary addition to the security infrastructure of nearly every organization[7].

IDPS typically record information related to observed events, notify security administrators of important observed events and produce reports. Many IDPS can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment (e.g. reconfiguring a firewall) or changing the attack's content. Alert Type: True Positive: : Attack – Alert, False Positive: : No attack – Alert, False Negative: : Attack - No Alert, True Negative: : No attack - No Alert. Classification of IDS is mention below.

A. Types Of Intruder: Intruders To A Network Can Be Classified Into Two Types:
1) External intruder: The unauthorized member implementing different types of attacks to reach the network.
2) Internal intruder: The authorized member of the network using different types of attacks to harm the network. The insider attacks can classified into two types of nodes:
   - Selfish node: Uses the network resources but does not cooperate, saving battery life for their own communications. It does not directly damage other nodes.
   - Malicious node: Aims at damaging other nodes by causing network DoS by partitioning, while saving battery life is not a priority.

The Intrusion Detection System can detect both external and internal intruder. The external intruders are easy to detect because they don’t have network id or proper keying materials to access the network information. But the internal intruders are harder to detect. Because the internal intruders have the necessary keying materials to manage any precautions taken by the authentication mechanisms.

B. Types Of Intrusion: Intrusions In A Network May Happen In Various Ways:
- Leakage: An undesirable information flow from the network.
- DoS: Blockage of the network resources to the other users.
- Malicious use: Deliberately harming the network resources.
- Attempted break-in: An attempt to have an unauthorized access to the network.
- Masquerade: An attacker uses a fake identity to gain unauthorized access to the network.
- Penetration: The acquisition of unauthorized access to the network.

IDS will detect the all kind of known and unknown attacks in the network by using different detection techniques. IDSs may provide partial detection solution to those attacks. But of course, all system administrators would like to have a perfect IDS that would able to detect all of the intrusions listed above [2].

C. Detection Techniques:
The detection techniques can be categorized into three groups that are: anomaly based detection, misuse based detection and specification based detection:
1) Anomaly Based Detection:
Anomaly based detection is the process of comparing definitions of what activity is considered normal against observed events to identify significant deviations. An IDS using anomaly based detection has profiles that represent the normal behavior of such things as users, hosts, network connections, or applications. The profiles are developed by monitoring the characteristics of typical over a period of time. The major benefit of Anomaly based detection technique is that they can be very useful for detecting unwanted traffic that is not specifically known. For instance, anomaly based IDS will detect that an Internet protocol packet is malformed. It does not detect that it is malformed in a specific way, but indicated that it is anomalous [4].

2) Misuse Based Detection:
Misuse based detection is looking for events or sets of events that match a predefined pattern of events that describe a known attack. The patterns are called signatures. Rule based system: encoding intrusion scenarios as a set of rules. The rules are, Interval rule, Retransmission rule, Integrity rule, Delay rule, Repetition rule, Radio transmission range, Jamming rule. Advantages: Very effective at detecting without generating an overwhelming number of false alarms. Disadvantages: Can only detect those attacks they know about therefore they must be constantly updated with signatures of new attacks. Many misuse detectors are designed to use tightly defined signatures that prevent them from detecting variants of common attacks[8].

3) Specification Based Detection:
Specification based intrusion detection techniques combine the advantages of both misuse and anomaly based detection techniques. Identified the main distinction among the anomaly based detection and misuse based detection as: “anomaly detection systems try to detect the effect of bad behavior but misuse detection systems try to recognize known bad behavior”. Specification based techniques are similar to anomaly detection in that they also detect attacks as deviations from a norm. However, instead of relying on machine learning technique, specification based approaches
are based on manually developed specifications that capture legitimate system behaviors. They avoid the high rate of false alarms caused by legitimate but unseen behavior in the anomaly detection approach. Their downside, however, is that development of detailed specifications can be time consuming. Thus, one has to trade off specification development effort for increased false negatives[9].

III. CLUSTER BASED IDS PROPOSED FOR WSNS

A. Clustering Based IDSs:

A hierarchical framework for intrusion detection as well as data processing is proposed. Throughout the experiments on the proposed framework, they stressed the significance of one-hop clustering. The authors believed that their hierarchical framework was useful for securing industrial applications of WSNs with regard to two lines of defense.

We proposed an isolation table to detect intrusions in hierarchical WSNs in an energy efficient way. Their proposal required two-levels of clustering. According to their experiment, their isolation table intrusion detection method could detect attacks effectively. The problem with this proposal is as follows: The authors claim that each level monitors the other level and report any anomalies to the base station. Since it is a hierarchical network, any alert generated by the lower level nodes must pass through the higher level nodes. In the case that the higher level node is the intruder, it will not allow the BS to be aware of its misbehavior by simply blocking the alert messages it receives from the lower level nodes.

An IDS based on clustering approach was proposed. Their proposal also ensured the security of the CHs. In their approach, members of a cluster monitor their CH in a time scheduled manner. In this way, energy for all cluster members is saved. On the contrary, cluster members are monitored by the CH, not by the contribution of cluster members. This also saves the energies of the cluster members. Through simulations, the authors showed that their proposed algorithm is much more efficient compared to other algorithms in the literature. The problem with this approach is its key management mechanism. It is a part of the IDS and helps IDS to establish pair wise keys among the nodes. The IDS uses these keys through the authentication of the messages. The key management assumes that the nodes are stationary (non-mobile) and the new nodes cannot be added after the pair wise keys are established. This constitutes a handicap for the model considering the fact that WSN may periodically require deployment of new nodes.

A hierarchical IDS model in which the network is divided into clusters and for each cluster, a CH is elected. They issued centralized routing, meaning that every packet of transmitted data will be forwarded to the CH and then to the base station. Their proposal included a method to place intrusion detectors in the CHs so that the entire network is covered with a minimum number of detectors. So that the energy of the network is increased.

A distributed cluster based anomaly detection algorithm was proposed. They minimized the communication overhead by clustering the sensor measurements and merging clusters before sending a description of the clusters to the other nodes. The authors implemented their proposed model in a real-world project. They demonstrated that their scheme achieves comparable accuracy when compared to centralized schemes with a significant reduction in communication over-head.

B. Intrusion Response (Mitigation):

When an attack is possible to occur, the IDS does not take preventive measures, since the prevention part is left to the Intrusion Prevention System (IPS). The IDS works in a reactive way compared to the proactive way of the IPS. Whenever the intrusion alert is generated by the IDS, the following action(s) would be taken according to the system specifications:

1) An audit record should be generated.
2) All the network members, the system administrator and the base station should be alerted about the intrusion. If possible, location and identity of the intruder should be provided in the alert message.
3) If it exists, a mitigation method should be induced in order to stop the intrusion. An automated corrective action should be generated through a collaborative action of the network members.

After detecting the malicious node in the network an alert message is send to the cluster head and the remaining...
unaffected nodes to secure the network by blocking the information flow to the affected node.

IV. FUTURE DIRECTIONS OF CLUSTER BASED IDS FOR WSN

Energy consumption of the IDSs is an important issue from a system design point of view. WSNs consume energy through sensing the surrounding phenomena, processing the sensed information and transmitting the resultant data. Therefore, the IDSs need to spend the least amount of energy as possible to spare enough energy for the crucial operations of the WSN. As a result of this low energy consumption requirement of WSNs, it is beneficial to use a hierarchical model for IDSs. This means that the network would be divided into clusters, each of which will have a CH. Accordingly, the energy consumption will be minimized by avoiding the need for all the nodes to send data to the BS. Besides, high energy consuming IDS algorithms would run only on the CHs which would save energy on the rest of the nodes and ultimately increase the total lifetime of the network.

In hierarchical, clustering based IDSs, clustering algorithms may consume considerable amount of the network’s energy through the formation of the clusters. After the clusters are formed and the CHs are elected, CHs may constitute a single point of failure and they have to be secured. Besides, if the CH is not a special node then the overhead of being a CH will diminish its resources very quickly. By comparing cluster based IDS we can able to develop more energy efficient IDS for Wireless sensor network to save more energy of the network. For the future research this is an excellent field to work on it.

For the researchers that are considering to simulate and compare the performances of the various IDS schemes. To simulate an attack against a WSN and evaluate the performance of an anomaly-based IDS. Authors simulate their scenario in ns-2 simulation environment[10], with AODV protocol. They provide 4 metrics (namely, true positives, true negatives, false positives, and false negatives) calculated by analyzing the packet delivery ratio while changing the pulse rate.

V. CONCLUSION

In this paper, an Cluster Based IDS approach for energy efficient intrusion detection in WSN is proposed. First, a detailed information about WSN and IDS is defined. Secondly, Cluster based IDS is proposed for WSN. Finally, the survey is concluded by highlighting open research issues in the field of more energy efficient intrusion detection in WSN.

VI. ACKNOWLEDGMENT

It is my greatest pleasure to present sincere thanks to Dr. S. SRINIVASAN, Head of the Department, Information Technology, P.B. College of Engineering and Mr. N.ARUNBALAJI, Assistant Professor, Department of Electronics and Communication Engineering, P.B. College of Engineering, for their constant support and encouragement for my academics and while writing this paper. I am also very thankful to all of my friends and my family members for their valuable presence in my life.

REFERENCES