ABSTRACT:

Wireless Sensor Networks (WSN) are one of the hottest areas over the past few years. Security is a major concern in WSN now a day. Intrusion detection represents one of such security aspects. Preventive mechanisms can be applied to protect WSNs against some types of attacks. In this paper, we carry out an extensive survey on intrusion detection system (IDS) exploring the resources available as of today. We also discuss the architecture of IDS in WSN based on their applications. We assume that this survey report can provide a platform for the researchers to develop their research work in contest of IDS in WSN.

KEYWORDS: WSN, IDS, Attacks.

1. INTRODUCTION:

Wireless sensor networks (WSN) have become increasingly one of the most promising and interesting areas over the past few years. The sensing technology combined with processing power and wireless communication makes it lucrative for being exploited in abundance in future. These networks may be very large systems comprised of small sized, low power, low-cost sensor devices that collect detailed information about the physical environment. Each device has one or more sensors, embedded processor(s), and low-power radio(s), and is normally battery operated. Examining each such single device individually, might appear to have small utility. The value of sensor networks however, lies in using and coordinating a vast number of such devices and allows the implementation of very large sensing tasks. In a usual scenario, these networks are deployed in areas of interest (such as inaccessible terrains or disaster sites) for fine grained monitoring in various classes of applications [1]. The flexibility and self-organization, fault tolerance, high sensing fidelity, low-cost, and rapid deployment characteristics of sensor networks create many new and exciting application areas for remote sensing. In the near future, this wide range of application areas will make sensor networks an integral part of life [2].

A WSN is composed of hundreds or even thousands of small, cheap sensors nodes which communicate with one another wirelessly. Sensor nodes typically do not have very much computational power, limiting the kinds of networking protocols and security mechanisms they can employ. Because WSNs are composed of so many nodes, which may be deployed in a hostile environment, replacing batteries is not feasible. Sensors nodes must therefore survive on the small amount of energy in the batteries they are deployed with (typically about 6 amp-hours [3]). This creates a need to conserve energy. Because of the wireless nature of WSNs, security is a fairly difficult issue.

The threats that damaged the security in WSN can be detected by the Intrusion detection systems (IDSs). An IDS attempt to identify computer system and network intrusions and misuse by gathering and analyzing data. The wireless IDS can monitor and analyze user and system activities, recognize patterns of known attacks, identify abnormal network activity. Thus it is desirable to have several sensor that monitors the attacks and let each sensor report to a base station to avoid losing an important event. In this paper we survey the need of security for WSN.

2. BACKGROUND OF IDS:

An intrusion-detection system (IDS) can be defined as the tools, methods, and resources to help identify, assess, and report unauthorized or unapproved network activity. Intrusion detection is typically a part of an overall protection system that is installed around a system or device and it is not a stand-alone protection measure [4]. The purpose of intrusion detection is to serve as an alarm mechanism for a computer system or a network. It provides information of unwanted or misbehaving elements and isolates those elements to deny them from the computer or network resources. It is possible to identify three main modules in an IDS: a Monitoring Module, controlling the collection of data, an Analysis Module deciding if the data collected indicate an intrusion or not, and a Response Module managing the response actions to the intrusion [Fig.1]. The first assumption is that user and program activities are observable. The second assumption, which is more important, is that normal and intrusive activities must have distinct behaviors, as intrusion detection must capture and analyze system activity to determine if the system is under attack. Depending on the detection techniques used, IDS can be classified into three main categories [5]: 1) signature or misuse based IDS, 2) anomaly based IDS, 3) specification based IDS, which it is a hybrid both of the
signature and the anomaly based IDS. The signature-based IDS uses pre-known attack scenarios (or signatures) and compare them with incoming packets traffic. There are several approaches in the signature detection, which they differ in representation and matching algorithm employed to detect the intrusion patterns. The detection approaches, such as expert system [6], pattern recognition [7], colored petri-nets [8], and state transition analysis [9] are grouped on the misuse.

**Fig. 1: IDS basic modules**

Meanwhile, the anomaly-based IDS attempts to detect activities that differ from the normal expected system behavior. This detection has several techniques, i.e.: statistics [10], neural networks [11], and other techniques such as immunology [10], data mining ([12], [13]), and Chi-square test utilization [14]. Moreover, a good taxonomy of wired IDSes was presented by Debar [15].

The specification-based IDS monitors current behavior of systems according to specifications that describe desired functionality for security-critical entities [16]. A mismatch between current behavior and the specifications will be reported as an attack.

Anomaly detection [Fig.2] bases its idea on statistical behavior modeling and anomaly detectors look for behavior that deviates from normal system use. A typical anomaly detection system takes in audit data for analysis. The audit data is transformed to a format statistically comparable to the profile of a user. The user’s profile is generated dynamically by the system (usually using a baseline rule laid by the system administrator) initially and subsequently updated based on the user’s usage. Thresholds are normally always associated to all the profiles [17]. If any comparison between the audit data and the user’s profile resulted in deviation crossing a threshold set, an alarm of intrusion is declared. This type of detection systems is well suited to detect unknown or previously not encountered attacks.

**Fig.2: Example of anomaly detection system**

The second type of model bases its detection upon a comparison of parameters of the user’s session and the user’s commands to a rule base of techniques used by attackers to penetrate a system. Known attack methods are what this model looks for in a user’s behavior. Since this model looks for patterns known to cause security problems, it is called a “misuse” detection model [Fig.3].

**Fig.3: Example of a misuse detection system**

It is obvious that the enemies, knowing that intrusion prevention and detection systems are in our networks, will attempt to develop and launch new types of attacks. In anticipation of these trends, IDS researchers are designing techniques for combining anomaly and misuse detection, and system architecture for distributed and coordinated intrusions.

3. INTRUSION DETECTION IN WSN:

In wireless network security threats are more challenging task than wired network. Here we will try to summarize all types of possible attack in WSN. We also focus the architecture of IDS in WSN in next section.

3.1 INTRUSION DETECTION IN A WSN ATTACK MODELS:

The routing attacks are classified into different categories. Many routing protocols for WSN are simple. So an attack is possible easily in this environment.

I. Sybil attacks

In Sybil attack the compromised node presents itself as it as multiple nodes. This type of attack tries to degrade the usage and the efficiency of the distributed algorithms that are used. Sybil attack can be performed
against distributed storage, routing, data aggregation, voting, fair resource allocation, and misbehavior detection [18].

II. Wormholes

Wormhole attack [19] is an attack in which the malicious node tunnels messages from one part of the network over a link, that doesn’t exist normally, to another part of the network. The simplest form of the wormhole attack is to convince two nodes that they are neighbors. This attack would likely be used in combination with selective forwarding or eavesdropping.

III. Acknowledgement

Some wireless sensor network routing algorithms require link layer acknowledgements. A compromised node may exploit this by spoofing these acknowledgements, thus convincing the sender that a weak link is strong or an dead sensor is alive.

IV. Selective forwarding

In this kind of attack a malicious node may refuse to forward every message it gets, acting as black hole or it can forward some messages to the wrong receiver and simply drop others.

V. Spoofed, altered, or replayed routing information

While sending the data, the information in transit may be altered, spoofed, replayed, or destroyed. Since sensor nodes usually have only short range transmission, an attacker with high processing power and larger communication range could attack several sensors simultaneously and modify the transmitted information.

VI. Sinkhole attacks

In the Sinkhole attack, the goal of the attacker is to attract all the traffic. Especially, in the case of a flooding based protocol the malicious node may listen to requests for routes, and then reply to the requesting node with messages containing a bogus route with the shortest path to the requested destination.

VII. HELLO flood attacks

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

3.2 Denial of Service (DoS)

This class of attacks is not concerned with the information that is transmitted. Rather, the goal of the attacker is to exhaust the resources of the networks and cause it not to function properly. Wood and Stankovic [20], [21] classify several forms of DoS attacks based on the layer that the attack uses. Some of them were already mentioned so we will not repeat them. At the physical layer the attacks take the form of jamming and tampering.

Jamming has to do with interfering with the radio frequencies nodes are using. Tampering refers to the the physical altering or even damaging of the nodes. An attacker can damage and replace a node, for example, by stealing or replacing information or cryptographic keys. At the link layer the attacker can generate collisions and exhaustion may be caused from protocols that attempt retransmission repeatedly, even when triggered by an unusual and suspicious collision. Additionally unfairness threats may occur when the attacker seeks to abuse a cooperative MAC-layer priority scheme. This threat may not result a total DoS, but it could downgrate the service which others experience.

4. IDS ARCHITECTURES:

IDS architectures are classified into two basic categories: host-based and network-based, depending on the data collection mechanism. Host-based IDS consult several type of log files (kernel, system, application ,etc.) and compare the logs against an internal database of common signatures for known attacks. Network-based IDS operate differently from host-based IDS. The design philosophy of a network based IDS is to scan network packets, auditing packet information, and logging any suspicious packets. Additionally, IDS architectures can further be classified based on the detection technique. Signature based IDS centers on finding an occurrence of predefined signatures or behavior that matches a previously known malicious action or indicates an intrusion. Anomaly-based IDS check for any behaviors that fall outside the predefined or accepted model of behavior. In [22], Brutch and Ko introduce another type of IDS. Their specification-based IDS defines a set of constraints that are indicative of a program’s or protocol’s correct operation.

5. IDS ARCHITECTURE FOR WIRELESS SENSOR NETWORKS:

1. Detection Objects

The constraint inherent to sensor networks, such as limited battery life, impose a cautious planning on how the detection tasks are performed. As in ad hoc networks, IDS agents must be located in every node. But in WSN to give better performance the architecture of the agents must be divided into two parts: local agents and global agents.

Local agents should monitor the local activities and the information sent and received by the sensor. This is only carried out when the sensor is active, and the sensor only manages its own communications. Thus, the overheads imposed on the sensor node are low.

Global agents should watch over the communications of their neighbors, and can also behave as watchdogs [23]. However, not all nodes can perform this operation at the same time, because this operation would require sensors to analyze the contents of all packets in their radio range. Therefore, only a certain subset of the nodes must watch over the network communications at a time.
Once any agent, global or local, discovers a possible breach of security in the network, it must create and send an alert to the user. The only way the user can be reachable is through the base station. Hence, all alerts must be sent to the base station.

Every agent and every node must store information about its surroundings in order to work properly. This information can be divided into two categories: knowledge about the security (an alert database that contains information about alerts and suspicious nodes), and knowledge about the environment (a list of the neighbors of the immediate neighbors of the node, which can be updated over the lifetime of the node using the received messages).

Every node has an internal alert database, which is used for storing the security information generated by the node agents. The format and size of that database is implementation dependant (i.e., depends on the protocols used in the sensor network).

II. Distributed and Cooperative

All nodes are running their own IDS, in WSN but the IDS cooperate in order to create a global intrusion detection mechanism.

III. Hierarchical

In hierarchical configurations, sensors are grouped into clusters. One of the members of the cluster behaves as server, or “cluster head (CH)” (which can be more powerful than the other nodes [25] or not [26]), with management and routing tasks.

In hierarchical architectures, global agents are activated in every cluster head, because the combination of all cluster heads covers (in most cases) the entire sensor network. Consequently, total network coverage is assured. This approach helps to preserve the overall energy of the system because cluster heads are either more powerful than other nodes or are rotated periodically.

These nodes are responsible for routing within the cluster and accept all the accusation messages from the other cluster members indicating something malicious. Additionally, the cluster-head nodes may also detect attacks against the other cluster-head nodes of the network, as they constitute the backbone of the routing infrastructure.

The base station (BS) is responsible for the formation of clusters, the election of CHs and the establishment of chains of node based on routing information (identifier, geographical position and energy reserve) sent by all nodes in the network.

All the network nodes will transmit collected data to their CH through the chain of neighboring nodes (N). Then CHs take the responsibility of transmitting received data directly to the base station (BS), or indirectly through the neighboring CHs. Fig-4 shows the organization of the network.

To overcome the complexities of clustering network, add more number of special powerful nodes in flat architectures, which is called as spontaneous watchdogs.

IV. Spontaneous Watchdogs

The spontaneous watchdog technique relies on the broadcast nature of sensor communications, and takes advantage of the high density of sensors being deployed in the field. For every packet circulating in the network, there are a set of nodes that are able to receive both that packet and the relayed packet by the next-hop, as shown in Fig. 5. Hence, all these nodes have a chance to activate their global agents in order to monitor those packets.

The process is as follows:

- Every active node will receive all packets sent inside its neighborhood, due to the broadcast nature of communications.
- The node will check if it is the destination of the packet. If not, it will not drop the packet instantly. Instead, it will check if the destination of the packet is in its neighborhood (thus it could receive any packet forwarded by the destination). This check can be done because all nodes store a list of neighbors for every node in its neighborhood.
- If true, the node can be a spontaneous watchdog. Consequently, it will calculate how many nodes in the network are in its same situation.
If the number of nodes that fulfill the requirements are \( n \), a single node will select itself as a global agent for this packet with a probability of \( 1/n \).

Due to the independence of the nodes’ behavior, the spontaneous watchdog technique does not assure that one and only one node will activate its global agent for every packet in the network.

6. IDS TECHNIQUES FOR WSN:
In this section, we present a survey of existing IDS research in the context of a WSN. WSN provides a relatively newer communication paradigm. Therefore, there are fewer works that address the construction of WSN IDS. It is necessary to integrate IDS approaches with corresponding applications because attacks targeted at different applications and services of WSN.
In this paper we summarize two important services of WSN, secure aggregation and secure localization.

6.1 SECURE AGGREGATION IN WSNs:
Aggregation has become one of the required operations for a WSN to save energy. One example of an aggregation tree is illustrated in Fig. 6. Nodes A, B, ..., N denote different sensor nodes in WSNs, respectively. \( f \) denotes an aggregation function (average, sum, maximum, minimum, count, etc.). If node \( I \) is compromised, it can send false reports to node \( J \). However, many existing schemes are designed without sufficient security in mind and cannot detect the above malicious behavior. Preventing this malicious behavior is the secure aggregation problem. Based on statistical estimation theory, Wagner [28] introduces a theoretical framework model and to analyze the resilient data aggregation problem. After concluding that commonly used aggregation functions are insecure, Wagner proposed using robust statistics for resilient aggregation. Finally, several general techniques, such as truncation (to place upper and lower bounds on an acceptable range of a sensor reading) and trimming (for instance, to ignore the highest 5 percent and the lowest 5 percent of sensor readings) are used to help improve the resilience of aggregation functions.

Many WSN applications require that sensor nodes have location information. Due to cost considerations, it is still not practical to equip every sensor node with a global positioning system (GPS) receiver. Therefore, many localization protocols have been proposed to help sensor nodes to estimate their locations. To utilize localization protocols, some special nodes, called beacon nodes, often are used. These beacon nodes are assumed to know their locations and transmit their locations to other non-beacon nodes through beacon packets.

Localization protocols may become vulnerable when a WSN is deployed in a hostile environment. For example, beacon nodes may be compromised, thus providing incorrect information to misleading location estimation at non-beacon nodes. Therefore, secure location discovery services are required to ensure the normal operation of a WSN.[29]

7. CONCLUSION:
The security of WSN is more vulnerable to real world situation. In this paper, we perform a survey on existing intrusion detection techniques in the context of WSN. We also focused on IDS architecture in WSN and try to summarize a secure method to some of the application of WSN. Since Intrusion prevention alone is not sufficient to achieve security in a network. An intrusion detection system aims to detect attacks on sensor nodes or intrusions into the networks.
Future work will involve the implementation and simulation of the architecture over a particular group of protocols in order to study the energy consumption and IDS performance in WSN.

8. REFERENCES:
4. A Survey on MANET Intrusion Detection: Satria Mandala, satriamandala@hotmail.com Faculty of Science & Technology Department of Informatics Engineering State Islamic University of Malang Jl. Gajayana 50 Malang, Indonesia, Md. Asri Ngadi Dr.asri@utm.my Faculty of Computer Science & Information System, Department of Computer System & Communication Universiti Teknologi Malaysia (UTM) Skudai - Johor, 81310, Malaysia.


16. Intrusion Detection in Wireless Ad-Hoc Networks: Foong Heng, Wei Heng, Weifoong@nus.edu.sg; Yin New Aye <yinnewaye@comp.nus.edu.sg> Ng Hian James nghianaj@comp.nus.edu.sg; CS4274 Introduction to Mobile Computing.


25. EYES European Research Project, IST-2001-34734. HTTP://EYES.EU.ORG.


