International Journal of Electronics Communication and Computer Engineering
Volume 3, Issue 6, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

A Study of Intrusion Detection Systems in Heterogeneous Wireless Sensor Networks

Naga Venkata Srinivas Kale
M.Tech.
Chaitanya Institute of Science and Technology, Kakinada

M. Vamsi Krishna
Head, Deptt. of CSE,
Chaitanya Institute Of Science and Technology, Kakinada

K. V. Ramana
Asst. Prof., Deptt. of CSE,
Chaitanya Institute Of Science and Technology, Kakinada

***Abstract* — Wireless sensor networks (WSNs) composed of smart sensors interconnected over wireless links are quickly becoming the technology of choice for monitoring and measuring geographically distributed physical, chemical, or biological phenomena in real time. These are deployed for monitoring in a range of critical domains for example health care, military, critical infrastructure. Wireless Sensor Networksare homogeneous or heterogeneous systems. The existing sensor fields communication will not be reduce a traffic issues to compare use of the single and multiple sensor fields. The heterogeneous is shrinking of the network nodes will not be supported to detect the intrusions.A Heterogeneous WSN is more complex as compared to homogeneous WSN and which consists of a number of sensor nodes of different types deployed in a particular area and which are collectively working together to achieve a particular aim. The aim may be any of the physical or environmental condition. For e.g. the wireless sensor network is mainly used in military applications such as in borders for finding out the infiltrations. It is also used in industrial process monitoring and control, machine health monitoring, environment and habitat monitoring, healthcare applications, home automation and traffic control. Wireless sensor networks are vulnerable to many attacks. This paper presents an overview of the intrusion detection in heterogeneous wireless sensor networks.**

***Keywords* — Heterogeneous WSN, Intruders, IDS, Sensors.**

I. INTRODUCTION

Wireless Sensor Networks (WSN)[1][2] are becoming increasinglypervasive in all aspects of environmental monitoring.Systems can be deployed in remote locations such as out inthe ocean, on a mountain, or deep down a mineshaft. Whilethis offers users flexible deployment options and access toa wealth of data, security is often over looked. As thesenetworks can cover large geographical areas, physical securityis often not a practical option, and the wireless transmissionof data leaves it vulnerable to interception, eavesdropping, modification, fabrication and/or blocking. This situation is untenable if the data has a significant commercial value, is safety critical, or part of a sensitive military application.

The heterogeneous approach [3] makes designing WSN systems easier and cheaper, it introduces new security concerns that have not been previously addressed by the literature. Sensors and sensor nodes typically have limited memory and processing capabilities, and also must strive to conserve power. Security protocols/algorithms are usually the opposite, requiring memory for key storage, processing overhead for encryption/authentication, and do not really consider power scarce applications. Heterogeneous WSNs on the other hand need to take into account varying security capabilities on sensor hardware, the intermediate nodes, and the end-user's system, regardless of the memory/processing capacity and power requirements. This is a fundamentally new and particularly difficult problem for WSN security to tackle. This paper presents an overview of intrusion detection in heterogeneous WSNs.

The last few years have seen a dramatic increase in the number of attacks, intrusion detection has become the mainstream of information assurance. While firewalls do provide some protection, they do not provide full protection and still need to be complimented by an intrusion detection system. The purpose of intrusion detection is to help computer systems prepare for and deal with attacks. Intrusion detection systems collect information from a variety of sources within computer systems and networks. For most systems, this information is then compared to predefined patterns of misuse to recognize attacks and vulnerabilities. However, there are new techniques of intrusion detection including the use of support vectors and neural network machines. These techniques, along with behavioral data forensics, create a database of normal user behavior and will alert the security officer if a deviation from that normal behavior occurs. In the majority of intrusion detection systems, however, both network and host- based intrusion detection systems combine to deal with attack detection and prevention from both inside and outside sources. Still, the intrusion detection system itself has an inherent risk attributed to it because of the absence of human intervention in some response scenarios.

II. NEED OF INTRUSION DETECTION SYSTEM FOR WIRELESS SENSOR NETWORKS

An intrusion [4][5] can be defined as a set of actions that attempt to compromise the integrity,confidentiality or availability of a resource.

Integrity: Assurance that the information is authentic and complete. Ensuring that information can be relied upon to be sufficiently accurate for its purpose. The term Integrity is used frequently when considering Information Security as it is represents one of the primary indicators of security (or lack of it). The integrity of data is not only whether the data is 'correct', but whether it can be trusted and relied upon. For example, making copies (say by e-mailing a file) of a sensitive document, threatens both confidentiality and the integrity of the information. Why? Because, by

International Journal of Electronics Communication and Computer Engineering
Volume 3, Issue 6, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

making one or more copies, the data is then at risk of change or modification.

Confidentiality: Assurance that information is shared only among authorized persons or organizations. Breaches of Confidentiality can occur when data is not handled in a manner adequate to safeguard the confidentiality of the information concerned. Such disclosure can take place by word of mouth, by printing, copying, e-mailing or creating documents and other data etc. The classification of the information should determine is confidentiality and hence the appropriate safeguards.

Availability: Assurance that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them.

An Intrusion Detection System(IDS)[4][5] is software and/ or hardware based system that monitors network traffic and monitors for suspicious activity and alerts the system. In some cases the IDS may also respond to anomalous or malicious traffic by taking action such as blocking the user or source IP address from accessing the network. Typical locations for an IDS is shown in figure 1.

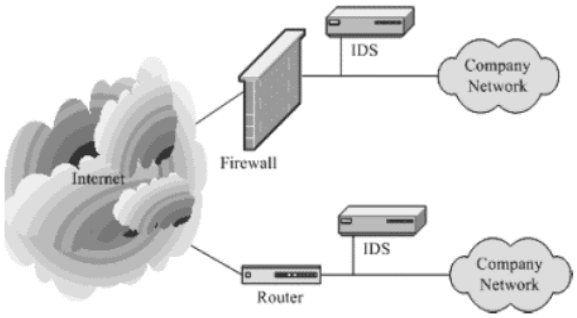

Fig.1. Intrusion Detection System

The following are the requirements for IDS in a wireless sensor network:

- IDS must be able to detect the anomalies with considerable accuracy.
- Detection and responses to anomalies must be within acceptable time period.
- It must be capable of isolating intruders successfully in WSNET.
- IDS must be lightweight consuming less energy (minimal computing and battery) to extend WSN life cycle.

III. Distributed Intrusion Detection System for Heterogeneous WSN

Intrusion detection load is divided among the sensor nodes, which may collaborate with each other to form a global intrusion detection mechanism. This architecture is more suitable for flat wireless sensor networks. A distributed Intrusion Detection System(dIDS)[6] can be defined as: "multiple Intrusion Detection Systems (IDS) [spread] over a large network, all of which communicate with each other, or with a central server that facilitates advanced network monitoring, incident analysis, and instant attack data."

A challenging research issue is the placement of the IDS modules in sensor networks in order to achieve efficient and effective intrusion detection. A number of placement strategies have been proposed. The following describe most important of them.

A. Promiscuous monitoring

A simple strategy would be to place IDS modules inevery sensor node as illustrated in figure 2 and to have each node operate in apromiscuous mode (always listening on the wireless interface). In this way, anymalicious packet can be easily detected. However, because of the high overheadassociated with this strategy, each participating node's ability to forward network traffic is severely reduced. Furthermore this IDS module placement strategy maylead to network traffic collisions and power consumption.

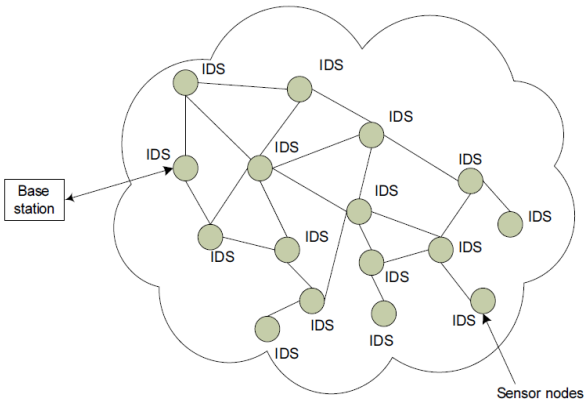

Fig.2. Distributed IDS architecture

B. A node monitors only the packets that pass through it

According to this placement strategy the IDS modules are also placed on every sensor node as illustrated in Figure 2, but only the packets that pass through each sensor node are used for the analysis. Thus, the IDS modules are placed on every sensor along the path from a source to a destination. This approach implies that each packet is analyzed multiple times leading to a waste of computational resources.

IV. Hierarchical Intrusion Detection System for Heterogeneous WSN

In hierarchical architectures [7], sensors are grouped into clusters. One of the member nodes is the" cluster head" and is responsible for management and routing tasks. The placement of IDS modules would position the IDS monitors in such a way that all the packets would be inspected only once, in order to address the resource constraints of the sensor networks. Thus, the IDS modules could be placed in selected sensor nodes (Figure 3) that would be able to cover all the paths from every source node to the base station. In order to achieve this, the sensor network may be divided into clusters with each cluster having a cluster head. This placement strategy implies that every member node of a cluster should forward its data packets to the cluster head which correspondingly

forwards them to the base station. However, this approach may lead to a high overhead since the member nodes do not select the shortest path, but instead have to forward their packets through the cluster head. This disadvantage may be limited if the hops between each member node and the cluster head are minimized.

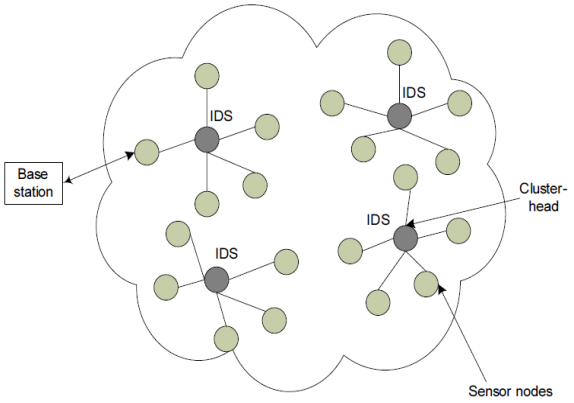

Fig.3. Cluster- based IDS architecture

Introduction to Genetic Algorithms

This is an introduction to genetic algorithm methods for optimization. Genetic algorithms were formally introduced in the United States in the 1970s by John Holland at University of Michigan. The continuing price/performance improvements of computational systems has made them attractive for some types of optimization. In particular, genetic algorithms work very well on mixed (continuous and discrete), combinatorial problems. They are less susceptible to getting 'stuck' at local optima than gradient search methods. But they tend to be computationally expensive. To use a genetic algorithm, you must represent a solution to your problem as a genome (or chromosome). The genetic algorithm then creates a population of solutions and applies genetic operators such as mutation and crossover to evolve the solutions in order to find the best one(s).This presentation outlines some of the basics of genetic algorithms. The three most important aspects of using genetic algorithms are: (1) definition of the objective function, (2) definition and implementation of the genetic representation, and (3) definition and implementation of the genetic operators. Once these three have been defined, the generic genetic algorithm should work fairly well. Beyond that you can try many different variations to improve performance, find multiple optima (species - if they exist), or parallelize the algorithms.

V. CONCLUSION

Wireless Sensor Networks (WSNs) are homogeneous or heterogeneous systems consist of many small devices, called sensor nodes. It is reliable to the shrinking of the network to detect a intrusions and overcome easily to reduce the traffic failures and increase reliability of the network .We are introducing a genetic algorithm for detecting the intrusions .In heterogeneous sensor network, a large number of inexpensive nodes perform sensing, while a few nodes having comparatively more energy perform other tasks such as data filtering, transport. This leads to there search on heterogeneous wireless sensor network (HWSNET) where different types of nodes are considered to prolong the life-time and reliability of the network.

Intrusion is a main security problem for WSNs. For this two intrusion detection architectures are used. In distributed architecture, all sensor nodes have almost the same communication capabilities and resource constraints and the information is routed sensor by sensor. This architecture is more suitable for flat wireless sensor networks. In hierarchical architectures, sensors are grouped into clusters. One of the member nodes is the “cluster head” and is responsible for management and routing tasks. This architecture has been proposed for multilayered wireless sensor network.

REFERENCES

[1] Kay Römer and Friedemann Mattern. The design space of wirelesssensor networks. IEEE Wireless Communications, 11(6):54–61,December 2004.

[2] Z. Li and G. Gong; A Survey on Security in Wireless Sensor Networks; Department of Electrical and ComputerEngineering, University of Waterloo, Canada.

[3] Kumar, D., Aseri, T.C. and Patel, R.B. (2009). Analysis On Deployment Cost And NetworkPerformance For Heterogeneous Wireless Sensor Networks, International Journal of Computerscience & Information Technology (IJCSIT). 1 (2): pp 109120.

[4] R. A. Kemmerer and G. Vigna; Intrusion Detection: A Brief History and Overview; 2002.

[5] K. Scarfone and P. Mell; Guide to Intrusion Detection and Prevention Systems (IDPS); NIST 800-94; Feb 2007.

[6] S. Selliah; Mobile Agent-Based Attack Resistant Architecture for Distributed Intrusion Detection System; MSc Thesis, College of Engineering and Mineral Resources at West Virginia University; 2001.

[7] Chen, R.-C., Hsieh, C.-F., Huang, Y.-F., (March 2010) , “An Isolation Intrusion Detection System for Hierarchical Wireless Sensor Network”. Journal of Networks.