An Implementation Approach for Intrusion Detection System in Wireless sensor Network

Ruchi Bhatnagar *, Dr. A.K. Srivastava+,Anupriya Sharma+

*Department of Information Technology,
IIMT Engineering College, Meerut.

+Principal, B.R.C.M. College of Engineering & Technology, Bhiwani (Haryana)

+Department of Computer Science,
IIMT Engineering College, Meerut.

ABSTRACT

The Intrusion Detection System (IDS) has become a critical component of wireless sensor networks security strategy. In this paper we have made an effort to document related issues and challenges of intrusion detection system for wireless sensor network and proposed a novel secure strategy for their implementation that can detect possible intrusion in the network, alerting user after intrusion had been detected and reconfigure the network if possible.

Keywords

Intrusion Detection System, Wireless Sensor Network, Connected Dominating Set

I. INTRODUCTION

A wireless sensor network is a network of simple sensing devices; which are capable of sensing some changes of incidents/parameters and communicating with other devices, over a specific geographic area for some specific purposes like target tracking, surveillance, environmental monitoring etc. Since sensor nodes are tightly constrained in processing ability, storage capacity and energy, routing and data aggregation in WSN are very challenging due to inherent characteristics. Therefore, sensor network need to become autonomous and exhibit responsiveness and adaptability to evolution changes in real time, without explicit user or administrator action. This need is even more imperative when it comes to security threats, so an attempt to apply the idea of implementation of an IDS that can detect a third party attempts of exploiting possible insecurities and warn for malicious attack in WSN makes a lot of sense.

In case of wireless sensor network, the communication among the sensors is done using wireless transceivers. 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, and detect policy violations for WSN. 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 explore the related issues and challenges for IDS in wireless sensor networks and a model for the implementation of IDS using concept of virtual backbone created by k-connected m dominating set of sensor nodes.

II. RELATED WORK

The constraints inherent to sensor networks, such as sparse resources, limited battery life, impose a cautious planning on how the detection tasks are performed. Previous study in this area focused on either distributed and cooperative and hierarchical architecture. In our paper, we used the concept of k-connected m-dominating set of sensor nodes proposed by Yiwei Wu & et all.[2] for implementing Intrusion Detection System, considering all related issues and challenges.

III. INTRUSION DETECTION SYSTEM : ISSUES

The Intrusion Detection System (IDS) has become a critical component of wireless sensor networks security strategy. However, deployment of intrusion detection brings with it a number of potential pitfalls, which can compromise security. Some of the issues related to ids in sensors network are:

A. It is not possible to have an active full-powered agent inside every node in a sensor network. Each node is totally independent, sending data and receiving control packets from a central system called Base Station, usually managed by a human user.

B. An IDS for sensor networks must send the alerts to the base station in order to warn the human user.

C. An IDS must be simple and highly specialized for reacting against specific sensor network threats and to the specific protocol used over the network.

D. Heavy traffic networks

- In these environments the high amount of traffic overloads the IDS sensor and intrusion traffic is missed.

E. Switched networks.

- In these environments an IDS needs to see the traffic on each switch segment. In switched networks there is no ideal location to connect n IDS – and switch SPAN ports can't keep up with all the traffic on the switch. Deploying IDS on each segment is cost prohibitive in many environments, thereby leaving segments unprotected.

F. Asymmetrical networks.

- In asymmetrically routed networks the traffic can traverse multiple paths before it reaches the n IDS and the n IDS will only see parts of the conversation (flow); thus missing an attack. An IDS needs to see a complete conversation (flow) in order to determine if an intrusion is present.

IV. Challenges of Intrusion Detection system

Basically the major challenge for employing any efficient security scheme in wireless sensor networks is created by the size of sensors, consequently the processing power, memory and type of tasks expected from the sensors. Intrusion detection systems look like a defense tool which every organization needs. However there are some challenges the organizations face while deploying an intrusion detection system in wireless sensor network. Some of them discussed below:

- IDS technology itself is undergoing a lot of enhancements. It is therefore very important for organizations to clearly define their expectations from the IDS implementation. IDS technology has not reached a level where it does not require human intervention. Of course today's IDS technology offers some automation like notifying the administrator in case of detection of a malicious activity, shunning the malicious connection for a configurable period of time, dynamically modifying a router's access control list in order to stop a malicious connection etc. But it is still very important to monitor the IDS logs regularly to stay on top of the occurrence of events. Monitoring the logs on a daily basis is required to analyze the kind of malicious activities detected by the IDS over a period of time. Today's IDS has not yet reached the level where it can give historical analysis of the intrusions detected over a period of time. This is still a manual activity. It is therefore important for an organization to have a well-defined Incident handling and response plan if an intrusion is detected and reported by the IDS. Also, the organization should have skilled security personnel to handle this kind of scenario.

- The success of an IDS implementation depends to a large extent on how it has been deployed. A lot of plan is required in the design as well as the implementation phase for deploying an IDS in WSN. In most cases, it is desirable to implement a hybrid solution of network based and host based IDS to benefit from both. In fact one technology complements the other. However, this decision can vary from one organization to another. A network based IDS is an immediate choice for many organizations because of its ability to monitor multiple systems and also the fact that it does not require a software to be loaded on a production system unlike host based IDS. Some organizations implement a hybrid solution. Organizations deploying host based IDS solution needs to keep in mind that the host based IDS software is processor and memory intensive. So it is very important to have sufficient available resources on a system before installing a host based sensor on it.

- It is important to take care of sensor to manager ratio. There is no thumb rule as such for calculating this ratio. To a large extent it depends upon how many different kinds of traffic is being monitored by each sensor and in what environment. Lot of organizations deploys a 10:1 ratio. Some organizations go for 20:1 and some others 15:1. It is very important to design the baseline policy before starting the IDS implementation and avoid false positives. A badly configured IDS sensor may send a lot of false positives to the console and even a 10:1 or even better sensor to console ratio can be inadequate.

- The IDS technology is still reactive rather than proactive. The IDS technology works on attack signatures. Attack signatures are attack patterns of previous attacks. The signature database needs to be updated whenever a different kind of attack is detected and the fix for the same is available. The frequency of signature update varies from vendor to vendor.

V. Network Model

In this paper, we are mainly focused in multi hop WSNs. The topology of a network is considered as Unit Disk Graph, denoted as G (V,E), where V is the node set and E is the edge set. For a graph G(V,E), a dominating set S of G is defined as subset of V such that each node in V / S is adjacent to at least one node in S. A connected dominating set of G i.e. C, a connected sub graph of G. The nodes in set C called dominators, and other are called dominatees. The following figure represented 2-connected 2-dominating set of Graph G.

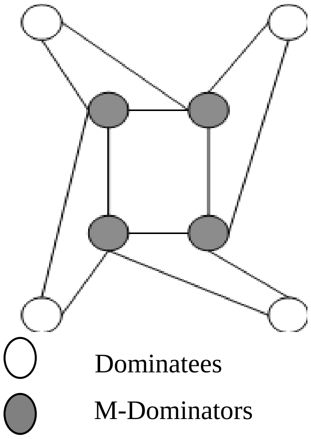

Figure: 2-connceted 2-dominating set

VI. PROPOSED APPROACH

The low energy constraint in WSN dictates the use of hierarchical model for implementation of IDS. Our model is different than the hierarchical approach as instead of dividing the network in to cluster we uses k connected m dominating set of sensor nodes that form a virtual backbone of few nodes to support routing flexibility and fault tolerance[2]. In this architecture considering the related issues and implementation challenges we first sort the all sensor nodes in non-increasing order of energy i.e. the nodes with more remaining energy added in to set C instead of less energy nodes. This process must be repeated till C is an m-dominating. The next step is to check C must be k-connected after the removal of redundant nodes with the optimization procedure [2]. Through this method the network which is considered as Unit disk Graph must be divided into k-connected m-dominating sets. As the figure represented the above graph must be in 2-connecting 2-dominating mode because each dominate neighbor has 2 neighbor dominators. In our proposed work the task of all m-dominating nodes is to discover any attack and threat that can affect the normal behavior of sensor nodes by analyzing actual status of a node, packet sent and received by node and measurement made to the environment. These m-dominating nodes of set C are k-connected thus report against the threat to the base station by sending an alarm. These K-connected neighbors' nodes which form the virtual backbone must be able to make a network in live condition if its m-1 dominators neighbor's are dead and it is still connected to base station by k-connection to report against the attack.

VII. INTRUSION DETECTION : DECISION MAKING TECHNIQUE

As every node of sensor network 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 data base that contain information about alerts and suspicious nodes), and the 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 received messages). In hierarchical IDS system, if an anomaly is detected a cooperated mechanism is initiated in order to take the decision of intrusion detection action while in our approach we used independent decision making system i.e. there are a no. of dominators node that have the task to perform the decision making functionality. They collect intrusion and anomalous activity evidences from other nodes and they make decision about network level intrusion. For an example if a node detects attack against the physical or logical safety i.e. they are being manipulated or not, must report to its any of dominator by raise an alarm, and this will take decision of intrusion by reporting to base station.

As sensor nodes can operate on their own, however for propagating information on misbehaving nodes a platform to enable collaboration for dissemination of such IDS data is needed. The scope of a dominating set based IDS deployed on a dense sensor area helpful in selection of nodes to monitor and increase the scalability and detection accuracy of the IDS. It will be highly fault tolerant as well as enhances the security by providing maximum area coverage using virtual backbone concept.

VIII. CONCLUSION

Although encryption and signed headers are intrusion prevention measures, vulnerabilities remain nonetheless. An ids further defenses the strength of a wireless sensor networks. In this paper we proposed an efficient scheme for IDS implementation which is more secure; provide efficient coverage and connectivity and minimizing routing overheads. In the future we test our proposed model with simulation with real experiments. As many of proposed security schemes are based on specific network models and lack of combined effort to take a common model to ensure security for each layer, in future though the security mechanisms become well-established for each individual layer, combining all the mechanisms together for making them work in collaboration with each other will incur a hard research challenge.

IX. REFERENCES

[1] Dai and J. Wu, On Constructing k-Connected k-dominating Set in Wireless Network, IEEE International Parallel & Distributed Processing Symposium, 2005.

[2] Y. Wu, F. Wang, T. Thai and Y. Li, “Constructing k-connected M-dominating sets in wireless sensor networks”, IEEE 2005.

[3] Y. Li, M.T. Thai, F. Wang, C.-W. Yi, P.-J. Wang and D.-Z. Du, On Greedy Construction of Connected Dominating Sets in Wireless Networks, Special issue of Wireless Communications and Mobile Computing (WCMC), vol. 5, no. 88, PP.927-932,2005.

[4] T D Garvey and Teresa F Lunt. Model based intrusion detection. In Proceedings of the 14th National Computer Security Conference, pages 372-385, October 1991.

[5] Yu-Xi Lim, Tim Schmoyer, John Levine, Henry L. Owen. Wireless Intrusion Detection and Response. Proceedings of the 2003 IEEE Workshop on Information Assurance

[6] Younis, M., Youssef, M., and Arisha, K., “Energy-aware routing in cluster-based sensor networks” Proc. 10th IEEE International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunications Systems, 1-16 Oct. 2002 pp. 129 – 136.

[7] Onat and A. Miri, “An intrusion detection system for wireless sensor networks,” in *Proceeding of the IEEE International Conferenceon Wireless and Mobile Computing, Networking and Communications*, vol. 3, Montreal, Canada, August 2005, pp. 53–259.

[8] Avancha, S, “A Holistic Approach to Secure Sensor Netis then compared with the works”, PhD Dissertition, University f Maryland, 2005.