Distributed Intrusion Detection System for Sensor Networks

Biswajit Panja and Sherif Rashad
Department of Computer Science
Morehead State University, Morehead, KY 40351
{b.panja, s.rashad}@morehead-st.edu

Abstract - **An intruder tries to disable the single point in a network, i.e. the central analyzer. If this is disabled, the entire network is without protection. Since the sensor nodes fail often, the use of a centralized analyzer is highly limited. Processing all the information at a single host implies a limit on the size of the network that can be monitored. Because of the limit of the central analyzer, it is difficult to keep up with the flow of information in large network like sensor. We have proposed distributed intrusion detection system for distribute sensor networks.**

I. INTRODUCTION

In today's world, information has gained an utmost importance. The failure to protect information could result in the loss of people, organizational resources and a great deal of time in attempting to recover it. Intrusion Detection Systems (IDS) help computer systems prepare for and deal with external and internal attacks. Information is collected from a variety of system and network sources, and that is then analyzed so that it adheres to the security required for the system. Vulnerability assessment technologies along with Intrusion Detection allow organizations to protect themselves against network security problems. An Intrusion Detection System (IDS) is a computer program that attempts to perform intrusion detection (ID). There are two well known methods to implement the same. They are misuse detection and anomaly detection. At times a combination of these techniques is used depending on the applications. It is preferred that the IDS perform its tasks in real time. IDs are usually classified as host-based or network-based. In Host-based systems, the decisions on information are obtained from a single host usually called as audit trails [3], while network-based systems obtain data by monitoring the traffic of information in the network to which the hosts are connected. Intrusion detection models in a distributed system can be distinguished as follows:

a. Misuse detection model [5]**:** A specific pattern of events within a network is analyzed to detect that the system has been misused. The sequence of events such as audit trails or systems logs on analysis will depict an unusual pattern. This pattern corresponds to exploitation of weak points within the system.

b. Anomaly detection model [5]**:** Changes in the patterns of behavior of the system is analyzed. Metrics obtained from the system's operation aids in building a model for this type of Intrusion. Events or observations that are intrusive in nature are flagged, if they have a significant deviation from the model used.

Motivation: Intrusion detection is one of the most important aspects in distributed sensor networks. Distributed sensor networks communicate among large numbers of sensor nodes; those are connected remotely or locally. Different types of intrusion are possible in sensor networks. Some of them are as follows:

1. Some sensor nodes from the group compromise the information.
2. Nodes from other groups which are not authorized to get information and join the group with false identification and access the messages.

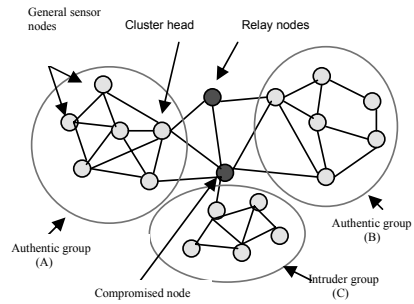

Figure 1. Motivational architecture

In figure 1 group A and B are authentic groups. Group C is nodes. The relay node can compromise and passes the information to unauthentic group. The above figure shows such relay nodes. So the relay node is intruder. Other sensor nodes can also be the intruder, if it passes information to other unauthentic group. The other intrusion possible is if unauthentic nodes of group C can join authentic group A or B by falsifying the identification.

General constraints in sensor networks

- *Hardware:* The hardware constraints for deployment of intrusion detection in sensor networks are memory, power, CPU, radio frequency channel. In modern distributed computers those parameters are not important.
- *Failure:* Sensor nodes fail frequently. The routing changes frequently.

T. Sobh (ed.), Innovations and Advanced Techniques in Computer and Information Sciences and Engineering, 117–122.

- *Size:* Size of the sensor network devices need to be considered. The nodes and network device need to be small, as sometime it needs to deploy it in secret locations.
- *Scalability:* Sensor nodes are deployed in multiple groups. The number of nodes in each group is large.

Existing intrusion detection systems [2]*:* Many of the existing network and host-based intrusion detection systems perform data collection and analysis centrally using a monolithic architecture (single layered). Audit trails or packets in a network are monitored and collected by a single host, and it is then analyzed by a single module using anomaly-based or rule-based detection techniques. In distributed applications, the patterns from the different distributed modules are collected and the data is sent to a central location where it is analyzed by a monolithic engine.

An intruder tries to disable the single point in a network, i.e. the central analyzer. If this is disabled, the entire network is without protection. Since the sensor nodes fail often, the use of a centralized analyzer is highly limited. Processing all the information at a single host implies a limit on the size of the network that can be monitored. Large numbers of sensor nodes are deployed. After that limit, the central analyzer becomes unable to keep up with the flow of information. Distributed data collection can also cause problems with excessive data traffic in the sensor network. It is difficult to add capabilities to the IDS. Changes and additions are usually done by editing a configuration file, adding an entry to a table or installing a new module. Analysis of network data can be flawed. Performing collection of network data in a host other than the one to which the data is destined can provide the attacker the possibility of performing Insertion and Evasion attacks. We have modified the existing distributed intrusion detection system. We will see if it can fit in distributed sensor network.

Problem Statement: Different types of intrusions are possible in sensor networks. There can be an active intruder and a passive intruder. Active intruders are nodes who come from outside to harm the network, and passive intruders are insider nodes which passes the authentic information to outsiders. Below we have analyzed different possible intrusion in sensor network.

Relay node as intruder: In figure 1 group A and B are authentic groups. Group C is not authentic. The cluster head of group A has the final information of the group. It passes the information to group B through relay nodes. The relay node can compromise and passes the information to the unauthentic group. The above figure shows such relay nodes. So the relay node is the intruder. Other sensor nodes can also be the intruder, if it passes information to other unauthentic group. The other intrusion possible if unauthentic nodes of group C can join authentic group A or B by falsifying the identification.

Cluster head node as intruder: Sensor network works in different clusters, each cluster has a cluster head. In figure 1, each cluster head will have the final data or final decision on behalf of the group. If cluster head passes the information to the unauthentic group C, then it is taken as the intruder.

General sensor nodes as intruder: General sensor nodes can also be intruder because of the following reasons:

1. It can misroute the information or data from its neighboring nodes.
2. Sensor nodes have very limited memory. Some sensor nodes can send unnecessary information to other nodes to make buffer overflow.
3. It can jam the network by not passing the information to other nodes.

Outsider senor nodes as intruder: If some sensor node can falsify the identity and join an authentic sensor group, then it is hard for the authentic group to distinguish between authentic and intruder sensor nodes. After joining a authentic group, that node can pass the information to the unauthentic group.

Constrains of sensor network which make intrusion probability high: Battery Power/Energy, Transmission Range, Memory (Program Storage and Working Memory), Unattended Operations, Ad hoc Networking, Limited Pre-Configuration, Channel error, Unreliable communications, Isolated subgroups, Unknown Recipients.

Intrusion because of less Battery Power/Energy: Sensor nodes having limited battery power. Intruder nodes can falsify the identity and replace the failed authentic node. Implementation of IDS also requires energy, so we need to balance it with the other functions done by the sensor network.

Intrusion because of Transmission Range: Low transmission range of sensor nodes can leads to loosing of information and the intruder nodes can take advantage of that.

Memory: Intrusion is possible by buffer overflow.

Intrusion because of Unattended Sensor node groups: The deployment of sensor network is very dynamic; sensor network can be deployed from aircraft. There can be unattended sensor group near intruder group, and managing module may not be aware of that. If some other sensor nodes send some authentic information this unattended group then the intruder sensor group can get that information.

Intrusion because of Ad hoc Networking: Sensor network is ad hoc in nature. Because of frequently changing position of nodes, intruder nodes get to falsify identification.

Channel error: Wireless sensor networks use radio frequency (RF) channel. This channel has very less capability because of its not physical channel. Intruder nodes can attack the channel and get the information.

Intrusion because of Unknown Recipients: Sensor network contains hundreds and thousands of sensor nodes. It is impossible to keep track of all sensor groups and all sensor nodes. Authentic information can be sent to intruder nodes by mistake.

Intrusion because of Unreliable communications: Communication can fail because of frequently sensor node failure. Intruder nodes can take advantage of this situation and act as authentic node to get the information.