Secure MANET using Two Head Cluster in Hierarchal Cooperative IDS

Zeba Ishaq
Pukyong National University

ABSTRACT
In modern era of technology wireless networks are widely used for data communication through out the world. Mobile Ad hoc Network (MANET) is one of the type in which each device works as an independent node and also as a router for forwarding data between nodes of the MANET.

MANET has no centralized or authorized body to protect the communication from intruders and considered as vulnerable to attacks due to its distributed nature and lack of infrastructure. Cluster based distributed and cooperative intrusion detection system (IDS) provides security to some extent. The header node in a cluster is a key component because if compromised the whole cluster will be destroyed. We propose a system that uses two heads per cluster with cooperative IDS mechanism. These head nodes not only cooperate for finding intrusion for cluster members but also protect each other against intrusion. In result more permenent cluster will appear which give birth to more consistent network connection. The performance metric of our work is based on how smoothly and securely the cluster operates when one header is compromised. The proposed system increases the detection rate and decreases the traffic and therefore offers the efficient utilization of power in mobile nodes.

General Terms
MANET security.

Keywords: IDS, MANET, Cluster, Header Node, Mobile node.

1. INTRODUCTION
Traditional wired wireless cellular mobile networks depend on existing infrastructure for managing their mobility. Mobile ad hoc networks have no infrastructure unlike traditional systems base stations and costly wires systems. Due to the absence of conscientious infrastructure, nodes must cooperate for data communication through the network. To carry out such communication the nodes must supposed to be friendly and is willing to relay data for others to get their ultimate destinations.

However, it is not necessary that forwarding nodes always be trustworthy for the communication. Assumption is not always true in reality. Most of the routing protocols only focus on providing efficient route discovery, maintenance functionality and pay little attention to routing security. Very few of them specify security measures from the very beginning.

The nature of MANET makes it very vulnerable to malicious attacks compared to traditional wired networks, because of wireless links, the low degree of physical security of the mobile nodes, a dynamic topology, a limited power supply and the absence of central management point [1].

There are a lot of attack prevention measures, such as encryption and authentication that can be used in MANET to minimize intrusions, but not eliminate them. Previous research reveals that no matter how many security techniques employed but still some weak point's lies in system for attackers. MANET IDSs, the second wall of defense to secure MANET, should have prevention mechanisms (authentication, encryption etc.) to guarantee an environment with high secure requirements. They should integrate with other MANET security measures to provide a high-survivability network.

However, today's Intrusion Detection Systems (IDSs) mainly focus on wired networks. Differences between MANET and wired networks make it difficult for researchers to apply the wired traditional IDS techniques to MANET. MANET does not have a fixed infrastructure. While most of wired IDSs, rely on real-time traffic parse, filter, format and analysis; monitor the traffic at switches, routers, and gateways. The lack of such traffic concentration points makes traditional wired IDSs inapt on MANET platforms.

A lot of research has been made in order to provide security to MANET and many Protocols has been developed. Other techniques such as IDS systems and clustering approach has also been adopted by researchers for strong security measure and also to improve the performance by considering limitations of the mobile nodes in the MANET. Various intrusion detection techniques has developed in the wired environment but due to quite big difference in architecture of MANET with wired networks, it's difficult to apply the same techniques as it is for MANET.

In our proposed solution, we use two head nodes with IDS agents in a cluster to provide better security. A MANET node typically has limited battery power and is not always efficient to make each MANET node the monitoring node for itself, especially when the threat level is low. We describe a cluster-based detection scheme where a cluster of neighboring MANET nodes can periodically, randomly and fairly elect two monitoring node for the entire neighborhood.

The remaining paper is composed as Section 2 of this paper presents the Related work In Section 3, we present Background

of IDS, IDS Architecture Problems in existing IDS architecture. Proposed Architecture and working mechanism are in Section 4, Result of detection rate in Section 5 and finally Section 6 presents our conclusions and future works.

2. RELATED WORK

In order to provide security to MANET in past researchers has performed their research in software as well as in hardware fields to make the mobile ad hoc network secure for use. MANET is useful in many fields to provide useful services. Zhang and Lee [1] proposed architecture based on distributed and cooperative nature of MANET nodes. Each node is responsible for itself, but neighboring nodes can help to investigate attacks collaboratively. Albers et. al. [2] proposed a distributed and collaborative architecture of IDS by using mobile agents. A local intrusion detection system (LIDS) with every node can be extended for global concern to find the intrusion more effectively.

To form clusters, distributed algorithms have been studied extensively [3, 4]. Most of these approaches have the drawback that the cluster head computation can be easily manipulated. Security policy adaptation reinforced through agents (SPARTA), an IDS based on mobile agents suggested by Krugel et. al. [5] and uses an event definition language (EDL) for the description of attacks.

3. IDS ARCHITECTURES AND PROBL-EMS

Major IDS architectures are threefold: standalone, distributed and collaborative, and hierarchical distributed and collaborative. The main features of these are described below.

- Standalone IDS: In this architecture, an IDS agent runs on each node endlessly and independently. It shows greater power consumption and performance degradation.
- Distributed and collaborative IDS: In this architecture, every node has an IDS agent that has the quality of distribution and cooperation, but has the drawback of the traffic overhead.
- Hierarchical distributed and collaborative IDS: It divides network into clusters. Each cluster has the head node with IDS agent that acts as a monitoring point for the whole cluster. It minimizes traffic overhead and also increases the detection rate. The main problem of this architecture is that the cluster head node may be compromised in the beginning of cluster life. Our proposed idea is to use two head nodes per cluster in order to guarantee the head node life.

4. PROPOSED SOLUTION

Based on the hierarchical distributed and collaborative IDS architecture, we propose to use two head nodes per cluster as shown in Fig. 1.

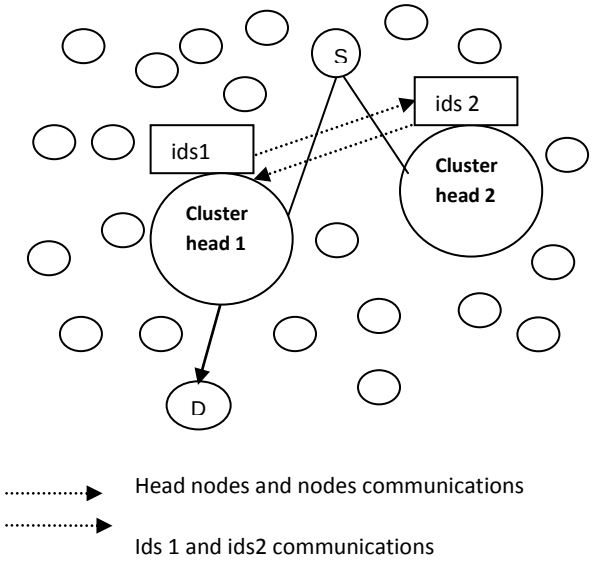

Fig 1: Cluster with Two Head Nodes in Hierarchical Cooperative IDS Architecture

We employ the following clustering algorithm and head node selection procedure.

4.1 Cluster Formation

First, select one of the nodes as initiator, which broadcasts a message to make a cluster. The information included as part of the message is memory size, CPU power, neighbor nodes list and battery power.

Obtaining information from the willing nodes, initiator node arranges all nodes in the table in a descending order of their energy value as shown in the Table 1. The initiator node selects the two head nodes for the first time with greater energy values and have direct link. After selection, initiator sends the table of information to the head nodes. Head nodes should broadcast the message which contains their addresses to all nodes in the cluster for the first time. The head nodes will work for a particular time period.

4.2 Head Nodes and IDS Agents Working Mechanism

Head nodes have IDS agents those are activated after their selection as the head node. Each IDS agent has a different database of attack signatures that increases detection rate, compared with standalone IDS architecture and also decreases traffic compared with distributed and collaborative IDS architecture. When some node inside and outside of the cluster sends a message to head node, they check it for any possible action. If it is a cluster joining message, they request necessary information from the node. On basis of this information, they accept or reject the node. In case of acceptance, they update the table of cluster making nodes as shown in Fig. 2. Otherwise, IDS agents of head nodes check the message for intrusion presence as shown in Fig. 3. After checking, head nodes send a message to each other for presence or absence of intrusion. If they do not get any message from each other, it is an alarming situation. It means that either of head nodes is under the attack. In this situation, the other head node reinitializes the process of selecting head nodes.

If trespassing data is found in a packet for specific destination, it discarded by either of them. Otherwise the first head node is responsible to sends data to the destination and saves the energy of second head node. After completing their turn without any abnormality, the first head reinitializes the process for the second turn.

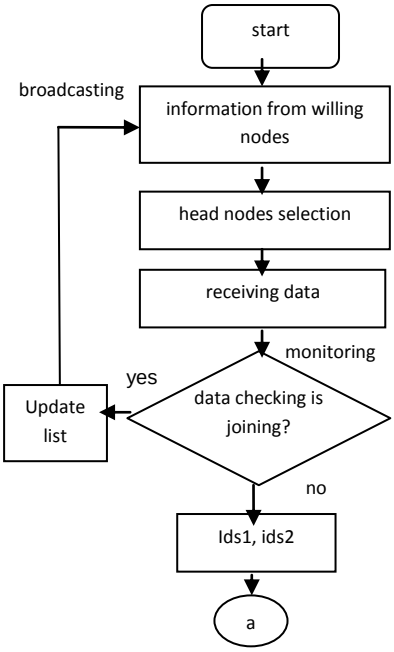

Fig 2: Clustering Algorithm (Part 1)

5. RESULTS OF DETECTION RATE

In case of one head node the detection is fairly less than the two head nodes in the cluster. Because the cluster with one head node has limited memory size for storing of database of attack signature, so the attack detection space is limited for IDS agent. But in case of two head nodes per cluster it becomes double than the previous one which increase the detection rate of the IDS agent automatically.

The results below are calculated with the help of C program.

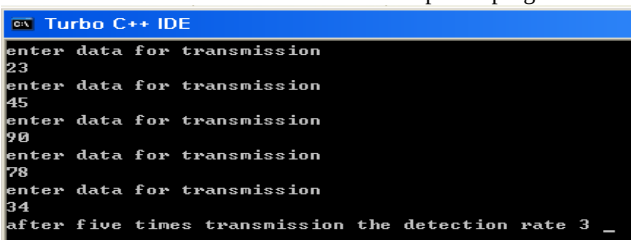

Fig 4: Results from one head cluster

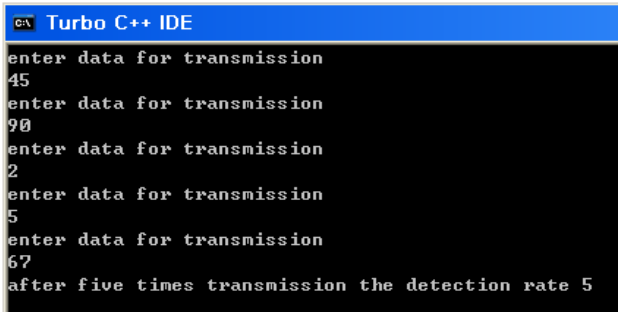

Fig 5: Results from two head cluster

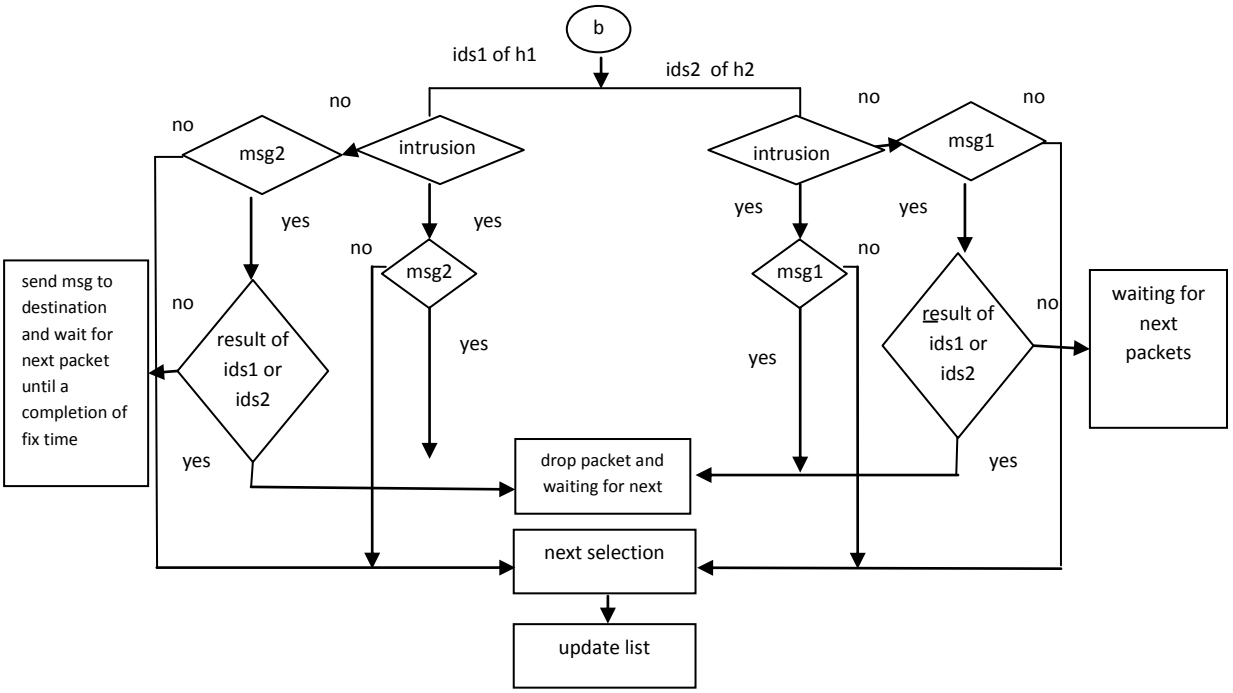

Fig 3: IDS Function and Working of Head Nodes (Part 2)

6. CONCLUSION AND FUTURE WORK

The IDS architecture using two head nodes per cluster gives greater security to MANET. Head nodes have IDS agent with different database of attack signature and using the misuse detection technique to find attacks more effectively. They support each other if one database doesn't contain the attack signature the other will find that. This increases the detection rate. The nodes in the cluster only communicate with cluster heads for their communications and in return cluster head will manage their activities in and out of the cluster and thus saves energies of member nodes of the cluster. In normal situation first head node will responsible for every activity and thus saves energy of the second head node. Two heads in cluster also provide security to each other by inspecting each other response and decrease the chance of destroying cluster in beginning which in turn increases stability of MANET networks.

In future IDS agent with database of attack signatures using misused detection technique can be replaced by the anomaly detection techniques to solve the problem of new attacks. Anomaly detection can find every diverse action not found in node profile of the activities. This will solve the problem of finding new attacks signature very easily. In future we can compare the energy consumption of nodes using IDS agents with different detection techniques to use the one batter in all aspects. We will implement this architecture by using NS2 simulator. It will include clustering algorithm and system having clusters with two head nodes.

7. REFERENCES

[1] Zhang Y, Lee W. Intrusion detection in wireless ad hoc networks. Proc. of 6th Ann. Int. Conf., (ACM MobiCom′00): Boston, MA, Aug 2000; 275-283.

[2] Albers P, Camp O, et,al.Security in ad hoc networks: a general ID architecture enhancing trust based approaches. Proc. of 1st Int: April 2002; 1-12.

[3] Vasudevan, Decleene B, Immerman N, et,al.Leader election algorithms for wireless ad hoc networks. In 3rd DARPA Information Survivability Conference and Exposition (DISCEX III): April 2003.

[4] Krishna P, Vaidya N H, et,al.A cluster-based approach for routing in dynamic networks.ACM SIGCOMM Computer Communication Review: 1997; 27, (2): 49-64.

[5] Krugel C, Toth T.Flexible, mobile agent based intrusion detection for dynamic networks. In European Wireless: 2002.