Intrusion Detection facilitation by routing protocols in Ad-Hoc Networks

Farooq Anjum and Prathima Agrawal
Telcordia Technologies Inc. Morristown NJ.

I. Introduction

Wireless multi-hop networks have come to be used in various facets of our life. A well-known example is their use by the army in battlefield scenarios. Recovery operations in cases of disasters such as hurricanes, floods, terrorist acts as witnessed by the WTC bombing etc are also facilitated very much on account of the use of ad hoc networks for communications amongst the personnel involved. This is because such situations render the existing infrastructure unusable. University campuses and conference settings also gain on account of these networks since they allow easy collaboration and efficient communication on the fly without the need for costly network infrastructure. Expectations are also high with respect to the use of these networks in places like hotels, airports etc. But a vital problem that must be solved in order to realize these applications of ad hoc networks is that concerning the security aspects of such networks. We believe that solving these problems combined with the widespread availability of devices such as PDAs, laptops, small fixtures on buildings and cellular phones will ensure that ad hoc networks will become an indispensable part of our life.

Protecting ad-hoc networks needs to be a multi-pronged strategy. In this paper we focus on the design of efficient intrusion detection mechanisms. Comparing the actual behavior of the system with the normal behavior of the system in the absence of any intrusions is normally the approach used for intrusion detection. A basic assumption here is that the normal and abnormal behaviors of the system can be characterized. The intrusion detection community has been concentrating mainly on wired networks. But techniques geared towards wireline networks would not suffice for an environment consisting of multihop wireless links because of the various differences such as lack of fixed infrastructure, mobility, the ease of listening to wireless transmissions, lack of clear separation between normal and abnormal behavior in ad hoc networks (for example a node might be sending out false updates since the routing protocol being used is slow to converge and not because the node is malicious) etc. In addition, conventional network approaches to network intrusion detection are normally based on the presence of common pinch points at which a small number of dedicated intrusion detection platforms can monitor all traffic. But this approach is not possible in ad-hoc networks on account of the absence of any such choke points[1][2].

The two main techniques used for intrusion detection are anomaly detection and misuse detection (signature detection). In order to realize these ID techniques the packets can be sniffed on each of the end-hosts. This is called as host intrusion detection (HID). It is also possible to sniff these packets on certain predetermined machines in the network. This is called as network intrusion detection (NID). HID systems are designed to monitor, detect and respond to user and system activity and attacks on a given host. While these systems are best suited to combat internal threats/file modifications and can collect and analyze data originating on a computer/processing system that hosts a certain service, they can get unwieldy. NID deals with information passing on the entire network between any pair of communicating hosts. While it is very good at detecting unauthorized outsider access, bandwidth theft, DOS, it is incapable of operating in encrypted networks and in high-speed networks. In addition, NID is effective when the network has certain chokepoints at which detection can be done. As is obvious the NID approach will not be effective in ad-hoc networks on account of absence of any choke points in such networks. As a result one might have to depend on having the intrusion detection mechanisms on all or some of the hosts in the system.

The objective of an intruder in any network is to have malicious packets delivered to the endpoint of interest resulting in harm to the endpoint. The intrusion detection system tries to detect the occurrence of these packets while in transit between the intruder (source of packets) and the endpoint of interest (destination of packets) so as to take proper corrective action. It is here that the routing protocols will have an effect on the intrusion detection capabilities of the network. Routing protocols determine the path taken by packets traversing between a source and destination node. And if individual hosts have to be able to determine intrusions based on attack signature recognition, it would be necessary for the packets in a given flow (at least all the packets that constitute the attack) to pass through a node that is part of the intrusion detection subsystem. But this would not always be possible for nodes other than the destination node on account of the fact that the packets might traverse different paths. Mobility would cause the path of packets to change and intruders can take advantage of this. In addition, in ad-hoc networks with many nodes there might be redundant paths between a given source-destination pair. The routing protocols might switch packets between these paths. Due to this it might be difficult to detect attacks knowing their signatures even when mobility is not allowed. Thus, as we see the intrusion detection subsystem would depend on the routing protocols and we hope to investigate this relationship in the current work.

Note that as a solution to the above problem one can argue for having all hosts in the ad-hoc network be part of the intrusion detection subsystem. Given known attack signatures, all attacks can be detected in such as case. But this would be inefficient and in many cases not possible on account of the resource constraints in such networks. So then given a routing protocol and a system with N nodes, how many of these should be part of the intrusion detection so that a given percentage of attacks can be detected. We attempt to answer this question for a very simple scenario in the next section.

II. PERFORMANCE ANALYSIS

We use the simulator ns2 and consider an ad-hoc network consisting of N number of static nodes where N varies from 10 to 90. Some of these nodes contain the attack signatures used by the intrusion detection logic and such nodes are said to constitute the *intrusion detection subsystem*. We assume that there is one intruder sending a sequence of consecutive packets constituting an attack to the destination. These packets are sent in a flow consisting of normal packets. Note that the intruder is considered to be the only source of packets in all the scenarios considered in this paper. Further, we assume that the nodes that are part of the intrusion detection subsystem know this sequence of packets that constitute the intrusion. The intrusion is considered detected if this subsequence of attack packets pass through any of the nodes that constitute the intrusion detection subsystem.

So given an ad-hoc network with N nodes and a given attack signature, we use 5 different topologies (each with N nodes) and consider a sequence of five consecutive packets as constituting the attack signature. For each topology we use 3 distinct trials with each trial containing a different sequence of 5 packets that constitute the attack. In each trial we consider the intrusion detected if *all the packets that constitute the attack pass through the same node*. For a given topology the possibility of detecting an intrusion is taken to be the average over three trials. Further, for a given number of N nodes the probability of detecting an intrusion is assumed to be the averaged value over the 5 different topologies. Thus, we determine the probability of detecting an intrusion for a given number N of nodes. This probability of detection is denoted as percentage of detection and is plotted on the y-axis.

We assume that the nodes that constitute the intrusion detection subsystem (IDS) are chosen randomly. We also assume that given a network with N nodes, a certain percentage of N are part of the IDS. Further, if a node Y is part of the IDS when the IDS contains x percent of the system nodes then the same node Y is also part of the IDS when the IDS contains y percent of the system nodes, $0<x<=y<=100$. The destination node is assumed to be part of the IDS only when the IDS contains all i.e. 100 percent of system nodes.

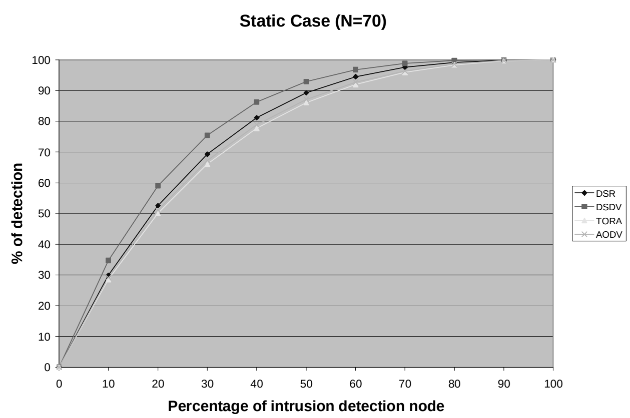

Figure 1: Multi-node Intrusion detection for a static intruder

We show the results for a system with N=70 in Figure 1 when we consider four different routing protocols, AODV, TORA, DSDV and DSR. We see that for the configuration assumed, the different routing protocols perform similarly. This figure gives a relationship between the number of nodes that must be part of the IDS for a given probability of detection. For e.g., if we desire that attacks be detected with a probability of 80 percent then approximately 40 percent of the nodes in the system must be part of the IDS. But at the same time many questions are raised. How would this relationship change when we consider mobility? What if we consider discontinuous longer sequence of packets constituting the attack? How will cooperation amongst the various nodes in the intrusion detection subsystem change the above relationship? Trying to identify attacks based on incomplete information is also not pursued. Can we modify the routing protocols or propose other mechanisms so as to improve the relationship above. Consideration of all these cases is part of future work.

REFERENCES

[1] S. Marti, T.J. Giuli, K. Lai and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", Mobicom 2000.

[2] Y. Zhang and W. Lee, "Intrusion Detection in Wireless Ad Hoc Networks", Mobicom 2000