Signature based Intrusion Detection for Wireless Ad-Hoc Networks: A Comparative study of various routing protocols

Farooq Anjum
Applied Research
Telcordia. Tech Inc.
Morristown NJ 07960
fanjum@telcordia.com

Dhanant Subhadrabandhu and Saswati Sarkar
Dept. of ESE
UPenn
Philadelphia
PA 19104

Abstract— **In this paper we focus on intrusion detection in wireless networks. The intrusion detection community has been concentrating mainly on wired networks. 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. In this paper we consider the signature detection technique and investigate the ability of various routing protocols to facilitate intrusion detection when the attack signatures are completely known. We show that reactive ad-hoc routing protocols suffer from a serious problem due to which it might be difficult to detect intrusions even in the absence of mobility. Mobility makes the problem of detecting intruders harder. We also investigate a relationship between the probability of detecting an intrusion and the number of nodes that must participate in the process of detecting intrusions.**

Keywords-intrusion detection; ad-hoc networks; routing-protocols; signature based detection

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. Intrusion prevention in the form of strong identification and authentication mechanisms alone are not sufficient. A malicious intruder can still launch attacks from both outside and inside the network environment that can weaken and compromise the network integrity resulting in serious consequences. For example, attacks could be in the form of jamming the network nodes so as to prevent them from communicating with each other, draining the batteries of a good node by transmitting irrelevant (junk) packets to it continuously, launching attacks such as TCP SYN-FIN, teardrop, ping-of-death etc resulting in a denial of service. Hence, it is necessary to also focus on the design of efficient intrusion detection mechanisms.

Intrusion detection is normally done by comparing the actual behavior of the system with the normal behavior of the system in the absence of any intrusions. Thus, a basic assumption 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.

There are two main techniques used for intrusion detection namely anomaly detection and misuse detection or signature detection. Anomaly detection essentially deals with the uncovering of abnormal patterns of behavior, where "abnormal" patterns are defined beforehand. Misuse detection relies on the use of specifically known patterns of unauthorized behavior. Thus these techniques rely on sniffing packets and using the sniffed packets for analysis. 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.

Given such a system in which all or some of the hosts are responsible for intrusion detection, a natural question is about the effectiveness of the two main intrusion detection techniques, anomaly detection and misuse detection. Anomaly detection depends on the characterization of normal behavior, which it can be argued is a difficult problem in ad-hoc networks. Of course, if the normal behavior can be characterized then this technique would be able to detect unusual behavior and hence can be used to detect new attacks. This technique is used in a limited form in current commercial systems (designed for wireline systems) on account of the high possibility of false alarms associated with this approach. In addition, this approach also requires extensive "training sets" of system events so as to characterize normal behavior.

Signature based or misuse detection on the other hand looks for events or a set of events that match a predefined pattern. As a result signature based techniques are effective at detecting attacks without too many false alarms. At the same time this technique would be unable to detect novel attacks whose signatures are unknown.

In this paper our objective is to determine the effectiveness of signature-based techniques at detecting attacks in ad-hoc networks. We assume that we know the signatures of attacks and some or all of the nodes in the system execute the intrusion detection logic; such nodes are said to constitute the intrusion detection subsystem. The reason that this question is interesting in an ad-hoc network setting is on account of different characteristics of ad-hoc networks.

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.

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 subsystem so that a given percentage of attacks can be detected.

In order to answer this and earlier questions we use a simulation tool ns2 and investigate the ease of intrusion detection with different routing protocols. The different routing protocols that we consider are AODV, TORA, DSDV and DSR. Our contributions in this paper are as follows. We compare four different routing protocols in terms of their ability to facilitate intrusion detection. We also show that signature based detection techniques will not be effective in ad-hoc networks on account of the different path taken by various packets. This happens with static nodes also and definitely with dynamic nodes. An intruder can take advantage of this by ensuring that the routes taken by the "malicious" packets are all different. Due to this the signature based attack detection will have incomplete information to work with. We also determine the relationship between the probability of detecting an attack and percentage of nodes that have to be part of the intrusion detection subsystem.

II. RELATED WORK

An initial approach to detect intrusions in ad hoc networks has been proposed in [1][2]. The main contribution in [2] is a distributed and cooperative intrusion detection architecture, which is expected to make use of statistical anomaly detection techniques. The design of actual techniques, their performance as well as verification though has not been addressed at all. Reference [1] on the other hand considers specific mechanisms to detect a small set of attacks in wireless networks. The approach followed in [1] is to identify the misbehaving nodes by having limits on the information that should be given out by a node in a given period of time. If a node violates this limit, then such a node is characterized as a malicious node. The approach given in this paper depends on cooperation amongst the various nodes. A limitation though is that the proposed mechanisms will not be effective against a group of malicious nodes. We believe that we are the first to investigate the ability of various routing protocols to facilitate intrusion detection.

III. PERFORMANCE ANALYSIS

There are two types of routing protocols designed for ad-hoc networks, proactive routing protocols and reactive routing protocols. The proactive routing protocols attempt to maintain

routing information from a given node to every other node in the network regardless of the use or need for such routes. Further, in order that the information be consistent and up-to-date, it is updated regularly irrespective of whether there is a need to send any messages on the route or not. Protocols belonging to this family require each node to maintain a set of tables to store routing information. The protocols in this family generally use distance vector shortest-path routing. A node in the system transmits its routing table periodically (time-driven updates) and also when a significant change occurs in the routing table (event-driven updates). Amongst the protocols that we consider DSDV is a proactive routing protocol.

The reactive routing protocols take a lazy approach to routing. The routes to a destination are created only when desired by a source node that desires to send data to a destination. The source node initiates the route discovery process that terminates once a route is found. Once a route has been established, it is maintained by a route maintenance procedure until either the destination becomes inaccessible or until the route is no longer desired. AODV, TORA and DSR are all reactive routing protocols.

In this section we present results of our study. As explained earlier we use ns2 and simulate an ad-hoc network consisting of N number of 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 typically plotted on the y-axis.

In the simulation scenarios, we consider two configurations. In the first configuration none of the nodes in the system is mobile and we refer to this as the static case. In the second configuration called the dynamic case only the intruder node is assumed to be mobile with a speed of 15 m/s. We consider four ad-hoc routing protocols and obtain intrusion detection performance for both cases for all the routing protocols.

A. Static case

We start by considering a network using AODV. We consider that there is only one node in the intrusion detection subsystem. This node is randomly selected to be one of the nodes in the initial path between the source (which is the intruder node) and the destination. The probability of detecting an intrusion for such a scenario is shown in Figure 1. We plot the number of nodes N in the network on the x-axis and the detection percentage on the y-axis. We consider five distinct values of N namely 10, 30, 50, 70 and 90. As we see from this figure, all the attacks will be detected when dealing with small network sizes but as the network size increases the number of attacks detected decreases very rapidly. This figure indicates that the ad-hoc routing protocols will not be effective at detecting intrusions even in the static case.

To understand the reason for this realize that AODV is a reactive routing protocol where routes to a destination are requested only when there is a need to send packets to the destination. In such a case the source sends RREQ packets and starts sending the data packets on getting the RREP packets back. But for a large network there might be multiple paths to the destination. So even when the source is immobile, the RREPs come back over various paths causing the source to continually change the path taken by the data packets. A destination sends back RREPs and each RREP has a given destination sequence number. And according to [3] the route taken by packets is updated either when the various RREPs received by a source have different sequence numbers or when the RREPs have the same sequence number but a different hop count (which indicates the number of hops between the source and the destination). This is also the case for other reactive routing protocols. *This indicates that the data packets should not be sent during the transient phase when the routes are being decided; this capability should be built into the routing protocol* itself instead of depending on the hosts to enforce this. Using some timeouts based mechanism might seem the right approach but this will interfere with delivering packets when mobility is involved. We are currently investigating appropriate mechanisms and will report on this in future work. Note that proactive protocols have been found to be better in this respect since they maintain routes to destination all the time and not just when required. As a result the transient phase occurs for proactive routing protocols only the first time the route is being decided.

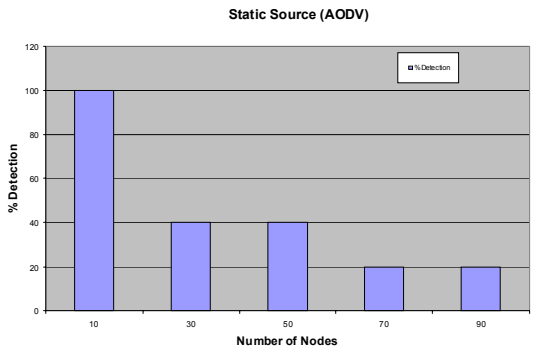

Figure 1: Effectiveness of a one node intrusion detection subsystem for a static intruder

We next consider a same system but now *relax the assumption with respect to the nodes that are considered to be part of the intrusion detection subsystem*. Instead of a node in the initial path between the source and destination we consider any node in the system to constitute the intrusion detection subsystem. This node is not chosen randomly but is chosen to be one of the nodes from a set of nodes through which all the packets that constitute the attack pass through(we exclude the destination node here). If no such node exists then we consider the attack to be undetected and if any such node exists then we consider that the attack has been detected. As can be inferred, this is a very optimistic scenario and we plot the results for such a scenario in Figure 2. The performance of DSR and DSDV is seen to be quite good in such a scenario while AODV and TORA are incapable of detecting all attacks even in this case.

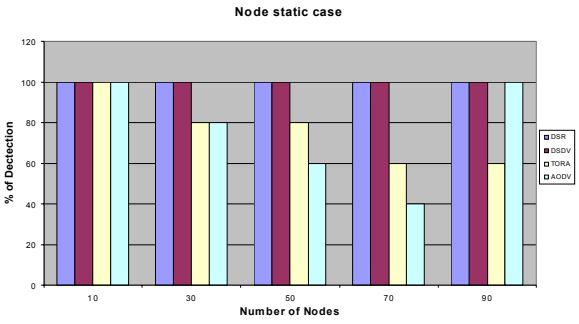

Figure 2: A one node intrusion detection subsystem for a static intruder with different protocols

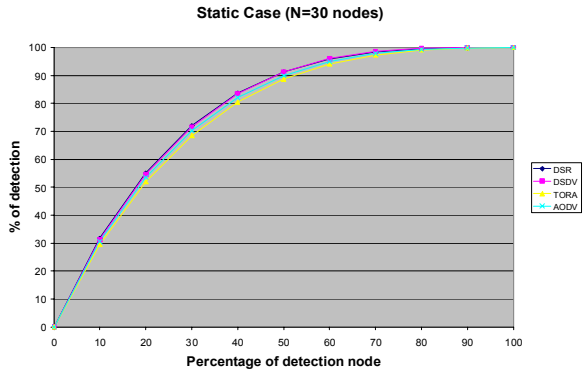

Figure 3: Multi-node Intrusion detection for a static intruder

It can be argued that both the above cases are not practical since we determine the node that forms the intrusion detection subsystem based on improbable conditions. This is because this node is not determined a priori but is rather determined after the simulation based on unrealistic knowledge. Hence, we next consider a system in which *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. We also assume that 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.

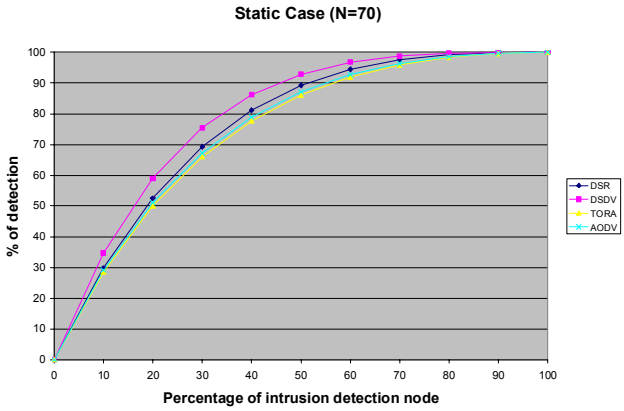

Figure 4: Multi-node Intrusion detection for a static intruder

We show the results for two systems with N=30 and N=70 in Figure 3 and Figure 4 respectively. We see that in such a case the different routing protocols perform similarly. DSDV performs slightly better since it does not have problems associated with the initial transient phase that is present in the reactive routing protocols as explained earlier. Note that the initial transient phase lasts longer for networks with more number of nodes and hence the difference between reactive and proactive routing protocols is more pronounced when N=70. These figures also give 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.

B. Dynamic case

We next consider the dynamic case. As earlier, we start by considering a network using AODV. We assume that the intruder is moving at a speed of 15m/s. Further, we assume that the source moves such that the direction of movement in each trial is different from others. In such a case we again assume that the intrusion is detected if the packets constituting the attack pass through any node in the initial path. Results for such a case are shown in Figure 5. We see that less than half the attacks are detected even for very small networks and no attacks can be detected in large networks.

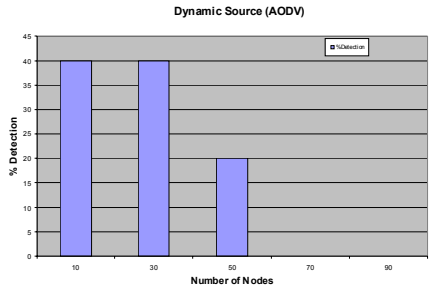

Figure 5: Effectiveness of a one node intrusion detection subsystem for a mobile intruder

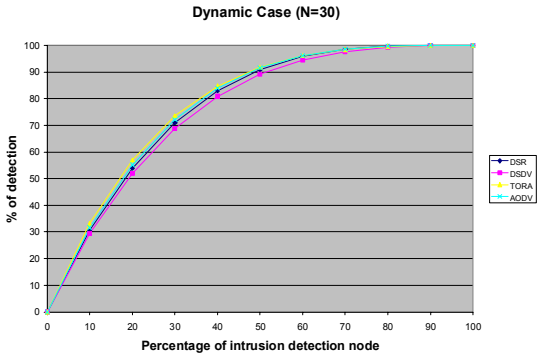

Figure 6: Multi-node intrusion detection for a mobile intruder

As earlier, we change the criterion used to determine the nodes that make up the IDS. We use the same criterion as used in case of scenarios represented by Figure 3 and Figure 4 respectively. The only difference is that now the intruder is assumed to be mobile. We show the results for such a case in Figure 6 and Figure 7 respectively. These figures are similar to those for the case of the static intruder. All the routing protocols are seen to have similar performance. DSDV also loses the advantage that it had in the static case since now new routes are determined as a result of mobile node movement and cannot be determined apriori.

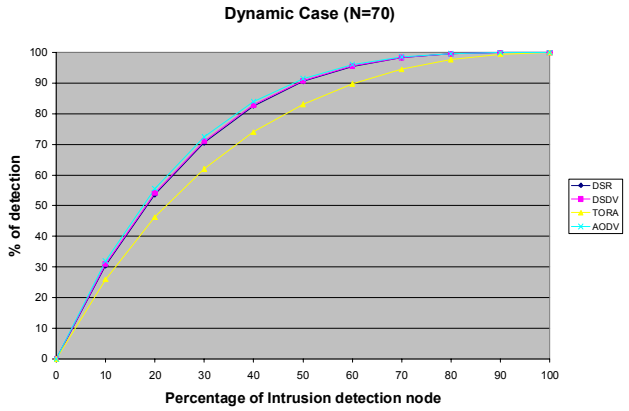

Figure 7: Multi-node intrusion detection for a mobile intruder

IV. CONCLUSION

In this paper we focus on signature based intrusion detection technique and investigate the ability of different ad-hoc network routing protocols to facilitate detection of intrusions. We show that reactive routing protocols are less effective than proactive routing protocols in the absence of mobility. We also investigate the relationship between the probability of intrusion and the number of nodes that participate in detecting intrusions under various assumptions chief of which is the assumption that we know the complete signature constituting an attack.

Note that in this paper we have considered limited mobility (i.e. only source representing the intruder moves) and also we have not considered discontinuous longer sequence of packets constituting the attack. We also do not investigate cooperation amongst the various nodes in the intrusion detection subsystem. Trying to identify attacks based on incomplete information is also not pursued. 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

[3] C. Perkins, E. Royer and S. Das, "AODV routing", Internet Draft draft-ietf-manet-aodv-13.txt, Feb 2003.