Challenges in Intrusion Detection for Wireless Ad-hoc Networks

Paul Brutch
Calvin Ko
Network Associates Laboratories
{Paul_Brutch, Calvin_Ko}@nai.com

Abstract

This paper presents a brief survey of current research in intrusion detection for wireless ad-hoc networks. In addition to examining the challenges of providing intrusion detection in this environment, this paper reviews current efforts to detect attacks against the ad-hoc routing infrastructure, as well as detecting attacks directed against the mobile nodes. This paper also examines the intrusion detection architectures that may be deployed for different wireless ad-hoc network infrastructures, as well as proposed methods of intrusion response.

1. Wireless Ad-hoc Networks

Wireless ad-hoc networks do not rely on a pre-existing network infrastructure, and are characterized by wireless multi-hop communication. Unlike fixed wired networks, wireless ad-hoc networks have many operational limitations. For example, the wireless link is constrained by transmission range and bandwidth, and the mobile nodes may be constrained by battery life, CPU, and memory. Wireless ad-hoc networks are used in situations where a network must be deployed rapidly, without an existing infrastructure. Applications of wireless ad-hoc networks include the tactical battlefield, emergency search and rescue missions, as well as civilian ad-hoc situations, such as conferences and classrooms. Wireless ad-hoc networks are vulnerable to additional threats above those for a fixed wired network, due to the wireless communication link and the dynamic and cooperative nature of the ad-hoc routing infrastructure.

The wireless link does not provide the same level of protection for data transmission as a wired link, allowing adversaries within radio transmission range to make attacks against the data transmitted over the wireless link without gaining physical access to the link. Passive attacks, such as eavesdropping, may violate the confidentiality of the system. Active attacks, such as deleting, modifying, or injecting erroneous messages or the impersonation of a node, may violate the availability, integrity, authentication, or non-repudiation of the system [15]. Other active attacks against the wireless link include jamming to deny service to mobile nodes, and energy exhaustion attacks, referred to as sleep deprivation torture [12], to exhaust the battery life of mobile nodes. The dynamic and cooperative nature of the ad-hoc routing infrastructure also imposes additional security threats. Attacks against the ad-hoc routing infrastructure may be made from external or internal nodes. Ad-hoc routing algorithms rely on node cooperation, where each node may act as a relay. Dynamic changes to the network topology, make it difficult to detect if a node providing false routing information is Byzantine or is just out of sync with the topological changes. These additional security threats must be considered, when designing security mechanisms for a wireless ad-hoc network.

2. Intrusion Detection in Wireless Ad-hoc Networks

Security mechanisms must be deployed in order to counter threats against wireless ad-hoc networks. While cryptographic mechanisms provide protection against some types of attacks from external nodes, cryptography will not protect against malicious inside nodes, which already have the required cryptographic keys. Therefore, intrusion detection mechanisms are necessary to detect these Byzantine nodes. Intrusion Detection Systems (IDS) may be classified based on the data collection mechanism, as well as the technique used to detect events. While the requirement of intrusion detection for both fixed wired and wireless ad-hoc networks are the same, wireless ad-hoc networks impose additional challenges. In general, the effectiveness of solutions designed for fixed wired networks are limited for wireless ad-hoc networks.

2.1. Classifications of IDS

An IDS may be classified as either host-based or network-based, depending on the data collection mechanism. Host-based IDS operate on either the operating system's audit trails, system and application logs, or audit data generated by loadable-kernel modules that intercept system calls. Network-based IDS operate on packets captured from network traffic. In addition, an IDS may be classified based on the detection technique as described below:

- Signature-based detection monitors for the occurrence of predefined signatures or sequences that indicate an intrusion. This technique may exhibit low false positive rates, but does not perform well at detecting previously unknown attacks.
- Anomaly-based detection defines a profile of normal behavior and classifies any deviation of that profile as an intrusion. The normal profile is updated as the system learns the subject's behavior. This technique may detect previously unknown attacks, but may exhibit high rates of false positives.
- Specification-based detection defines a set of constraints that describe the correct operation of a program or protocol, and monitors the execution of the program with respect to the defined constraints. This technique may provide the capability to detect previously unknown attacks, while exhibiting a low false positive rate.

2.2. Limitations of IDS Solutions for Wireless Ad-hoc Networks

IDS solutions for fixed wired networks are often hierarchical and deploy network-based sensors at key traffic concentration points, such as switches, routers, and firewalls. These IDS sensors are physically secured, and use the signature-based detection technique to detect attacks. Alerts generated by these distributed IDS sensors are sent to centralized security servers for analysis and correlation. The centralized security server distributes attack signature updates to the network-based IDS sensors. The effectiveness of IDS solutions that were designed for fixed wired networks are limited for wireless ad-hoc networks as described below:

- Wireless ad-hoc networks lack key concentration points where network traffic can be monitored. This limits the effectiveness of a network-based IDS sensor, since only the traffic generated within radio transmission range may be monitored.
- In a dynamically changing ad-hoc network, it may be difficult to rely on the existence of a centralized server to perform analysis and correlation.
- The secure distribution of signatures may be difficult, due to the properties of wireless communication and mobile nodes that operate in disconnect mode.
- It may be difficult to physically secure a mobile host that could be captured, compromised, and later rejoin the network as a Byzantine node.

3. Detection of Attacks Against the Routing Infrastructure

In a wireless ad-hoc network, security mechanisms must be deployed to detect attacks against the routing infrastructure. External nodes may inject, replay, or distort routing information in order to partition the network or cause excessive load, while inside nodes may advertise incorrect routing information [15]. In this section we will briefly review previous work proposed to detect attacks against the routing infrastructure of fixed wired networks, as well current research proposed for wireless ad-hoc networks.

3.1. Solutions for Fixed Wired Networks

Solutions to detect attacks against the routing infrastructure of a wireless ad-hoc network may build on solutions previously proposed for fixed wired networks. We will briefly review four solutions to detect attacks against routers and the routing protocols in a fixed wired network as follows:

- Distributed Probing. A router may detect neighboring routers, which act as network sinks or misroute packets, by directly sending to each router test packets that have a destination of the router performing the diagnosis [4]. A router can determine the goodness of a tested router based on whether the tester router receives the test packet back within a certain time interval. If the tested router can distinguish between test packets and normal traffic, however, it can avoid detection.
- Principle of Conservation Flow. The WATCHERS protocol was developed to detect routers that violate the principle of conservation flow, where by all data bytes sent to a node and not destined for that node should exit that node [1]. WATCHERS runs on each router, and provides the capability to detect bad routers that drop or misroute packets. Using WATCHERS, a router may test a neighboring router using its own counters, the counters of the tested router, and the counters for each neighbor of the tested router.
- Statistical Anomaly Detection. This technique may be used to detect known and unknown attacks against the routing infrastructure. The JiNao statistical analysis module, based on the SRI NIDES/STAT algorithm, was developed to detect insider OSPF

routing attacks [5]. The NIDES/STAT algorithm compares a subject's current behavior (short-term profile) against its expected behavior (long-term profile), which is established using a training period and is periodically updated. Using statistical measures of activity intensity (OSPF packet volume), categorical (OSPF packet type), and counting (link-state advertisement age), JiNao was able to detect known attacks with a low false positive.

- Protocol Analysis. The behavior of a routing protocol may be monitored with respect to a state transition diagram that models the protocol states, in order to determine when an anomalous state is entered. In JiNao, protocol analysis is performed using real-time Finite State Machines (FSM) pattern matching modules based on knowledge about known attacks against the OSPF routing protocol, in order to detect three types of insider attacks [5]. State transitions in the JiNao FSMs are based on the events as well as the time of an event.

3.2. Solutions for Wireless Ad-hoc Networks

A number of solutions to detect attacks against the routing infrastructure of wireless ad-hoc networks were proposed as an extension of the Dynamic Source Routing (DSR) protocol. In the Route Discovery phase of the DSR protocol, nodes broadcast Route Request (RREQ) messages to neighbors in order to find a route to a destination, and the Route Reply (RREP) message from the destination contains the full source route. In this section we will briefly review some of the proposed solutions as follows:

- Watchdog. The watchdog mechanism was implemented on top of DSR to verify that when a node forwards a packet, the next node in the path also forwards the packet, otherwise the next node is misbehaving [10]. Watchdog runs on each node, operates by listening in promiscuous mode to transmissions of neighboring nodes, and assumes bi-directional links. Watchdog maintains a buffer of recently sent packets, and removes a packet from the buffer when the packet is forwarded by the next hop. If a packet remains in the buffer beyond a threshold value, Watchdog determines that the next hop is misbehaving and sends a message to the source identifying the misbehaving node. Watchdog may not always be effective due to packet collisions, a malicious node deliberately limiting transmission power, or collusion.
- Control Messages. A scheme that proposed adding two control messages to the DSR protocol, Route Confirmation Request (CREQ) and Route Confirmation Reply (CREP), requires intermediate nodes, which have a known route to the destination, request that the next hop in the path send a confirmation message back to the source [9]. When an intermediate node responds to a RREQ for which it has a route in its cache, the node sends back an RREP to the source, and will additionally send a CREQ message to the next hop in the destination's path. The next hop sends a CREP message back to the source if it also knows a path to the destination. When the source receives the RREP and the CREP, it can determine the validity of the path. This method may operate with most on-demand routing protocols to detect malicious nodes, such as blackhole routers, which falsely advertise being on the shortest path. This scheme may not be always be effective due to colluding nodes.
- Neighborhood Watch. As part of the CONFIDANT protocol, a neighborhood watch is used to detect (either by listening to the transmission of the next node or observing the route protocol behavior) intrusive activity made by the next node on the source route, and when a node detects a malicious neighbor, the node sends an alarm message to the other nodes on it's friends list [3]. The CONFIDANT protocol works as an extension of reactive source-routing protocols, such as DSR, and uses a reputation system that rates nodes based on malicious behavior. Alarm messages received from other nodes are evaluated, and the reputation of an accused node is changed only if the source of the alarm is a fully trusted node or the node was similarly accused by several partially trusted nodes.
- Statistical Anomaly Detection. Using statistical anomaly detection to detect false routing information generated by Byzantine nodes is another approach that may be well suited for wireless ad-hoc networks. In a proposed solution, a normal profile may be established that correlates the physical movement of a node to changes in the routing table, with the RIPPER as the proposed classification algorithm and "nearest neighbor" as the clustering algorithm for deviation scores [14].

4. Detection of Attacks Against Mobile Nodes

The requirement for detection of attacks against a mobile node in a wireless ad-hoc network is the same as for hosts in a fixed wired network. In a wired network, hosts are typically protected by network firewalls and network-based IDS. These network-based security mechanisms, however, may not be effective for wireless ad-hoc networks. Without protection from network firewalls, mobile nodes may be directly exposed to attacks from external as well as internal Byzantine nodes. Therefore each mobile node should run some type of node-based IDS, if the node has the available CPU, memory, and battery capacity. While signature-based detection is the primary technique used in fixed wired networks, the secure distribution of signature updates in a wireless ad-hoc network may be difficult, and mobile nodes may operate in disconnect mode. The ideal node-based IDS should be able to detect unknown attacks without requiring signature updates. Potential solutions for a node-based IDS to detect attacks against the node may use anomaly or specification-based detection on the system calls generated by monitored processes running on the node.

Anomaly detection may be used to detect attacks against a network daemon or a setuserid (SUID) program by building a normal profile of the system calls made during program execution. An intrusion can be detected by comparing the normal profile of a program against a running process. If the process execution deviates significantly from the established profile, an intrusion is assumed. One disadvantage of anomaly detection for mobile computing is that the normal profile must be periodically updated and calculating deviations from the normal profile may impose a heavy load on mobile devices. A more light-weight approach using profiles consisting of the type of system call and it's occurrence of frequency was proposed, in which the DP Matching method (traditionally used in speech recognition) is used to calculate the optimal match between a normal profile and a sample profile [11].

The specification-based technique [6] [7] has demonstrated the capability to detect both known and previously unknown attacks against network daemons and SUID programs on Unix platforms. In this technique, the execution of designated programs is monitored and the generated system calls are compared against a set of pre-defined constraints. Any deviation from the defined constraints is considered to be the manifestation of an attack. The specification-based IDS can be preloaded on mobile nodes prior to deployment to the field, and should not require any periodic updates in order to be effective.

5. Architectures for Intrusion Detection in Wireless Ad-hoc Networks

The optimal IDS architecture for a wireless ad-hoc network may depend on the network infrastructure itself. Wireless ad-hoc networks may be configured in either a flat or multi-layered network infrastructure. In a flat network infrastructure, all nodes are considered equal and may participate in routing functions. This infrastructure may be suitable to civilian applications, such as a classroom or conference. In a multi-layered network infrastructure, all nodes are not considered equal. Nodes within transmission range are organized into a cluster, and elect a Cluster-Head (CH) node to centralize routing information for the cluster. The CH nodes form a virtual backbone for the network, and depending on the protocol intermediate gateway nodes may relay packets between CH nodes. This infrastructure be suitable for military applications.

5.1. Stand-alone IDS Architecture

In a stand-alone IDS architecture, each host runs an IDS that independently detects attacks. The original IDS were stand-alone systems developed to protect specific mainframes. Since stand-alone IDS do not cooperate or share information with other systems, all intrusion detection decision are based on information available to the individual node. The watchdog mechanism [10], could be deployed as a stand-alone IDS mechanism and detect Byzantine nodes within transmission range, but not report these malicious nodes to any other node. The node running watchdog would then forward packets only to neighboring nodes that do not appear to misbehave. While the effectiveness of this solution is limited, this architecture may be suitable in an environment where not all nodes are capable of running an IDS or have an IDS installed.

5.2. Distributed and Cooperative IDS Architecture

Cooperation among distributed host-based IDS was originally proposed for fixed wired networks in the Cooperating Security Managers [13]. Intrusion detection for fixed wired network is primarily hierarchical and network-based, so there is no need to incur the overhead associated with the exchange of messages required for this architecture. This IDS architecture is more suitable for flat wireless ad-hoc networks, and a distributed and cooperative architecture was proposed for this environment in which IDS agents residing on every node independently make local intrusion detection decisions, but cooperatively participate in global intrusion detection [14]. In this architecture, if a node detects an intrusion with weak or inconclusive evidence, it can initiate a cooperative global intrusion detection procedure, or if a node detects locally an intrusion with strong evidence, it can independently determine an attack on the network.

A cooperative and distributive IDS architecture could be susceptible to attacks from Byzantine nodes, which could independently make false claims of detecting an attack from a correct node with strong evidence, thus making it difficult to derive a distributed consensus. In the CONFIDANT protocol, nodes cooperate and share alarm messages with other nodes in the wireless ad-hoc network that are in a node's friend list [3]. Since alarm messages are evaluated based on their trustworthiness, this solution should minimize the effect of a Byzantine node, which falsely accuses a correct node.

5.3. Hierarchical IDS Architecture

Hierarchical IDS architectures have been proposed for multi-layered, wireless ad-hoc networks. In a multi-layered wireless ad-hoc network, cluster-head nodes centralized routing for the cluster and may support additional security mechanisms. For example, a three-layered infrastructure may be deployed in the tactical battlefield, consisting of two-layered ground networks and a third layer of Unmanned Aerial Vehicles (UAVs), which provide event correlation for a theater of operations. Neighboring ground nodes detecting that ground node V is acting malicious send an accusation message to the UAV, the UAV will determine that node V is compromised after receiving a threshold of K accusations [8]. Then the UAV may respond, such as broadcasting a message to notify all nodes in the theater.

In addition to correlating events detected by cluster-member nodes, CH nodes may also detect attacks against the virtual backbone's routing infrastructure made by Byzantine CH nodes. In a multi-layered wireless ad-hoc network, the detection of Byzantine CH nodes is essential. A Byzantine CH nodes could potentially reroute, modify, or drop packets transmitted by cluster member nodes, as well as any packets routed through the CH node on the virtual backbone

6. Intrusion Response in Wireless Ad-hoc Networks

The ideal intrusion response for a wireless ad-hoc network is to isolate Byzantine nodes from the rest of the network. For fixed wired networks, the "electronic quarantine" was developed to dynamically create the filtering rules required for desktop firewalls, packet-filtering intranet firewalls, and application-level Internet firewalls, in order to isolate a compromised host within a fixed wired network [2]. In a dynamically changing wireless ad-hoc topology, the centralized solution proposed by the electronic quarantine would not be effective, since the implementation of intranet firewalls and application-level firewalls may not be feasible.

In the distributed and cooperative IDS architecture proposed for wireless ad-hoc networks, one approach suggested that in response to a detected intrusion end-users re-authenticate themselves using an out-of-bound mechanism, and negotiate a new communication channel to exclude compromised nodes [14]. Re-authentication using an out-of-bound mechanism may be appropriate in some but not all environments. The path manger function of the CONFIDANT protocol allows nodes to delete paths containing malicious nodes and to choose not to forward packets for nodes that have bad ratings [3]. Since nodes share information about malicious nodes with their friend nodes, malicious nodes will eventually be detected and isolated from the wireless ad-hoc network.

A hierarchical approach was proposed for intrusion response in multi-layered wireless ad-hoc networks in the digital battlefield, in which high layer UAVs support centralized certification and counter-certification for a theater of operations [8]. A data forwarding policy is used in which only packets for authenticated nodes are forwarded. The Certificate Authority can isolate a suspected node from rest of the network by broadcasting a counter certificate for that node.

7. Conclusions

Research in intrusion detection has been conducted for the past fifteen years, however, its application to wireless ad-hoc networking is fairly recent. This paper presents a brief overview of current research efforts in this area. Commercial IDS solutions are primarily focused on network-based IDS sensors, and these security mechanisms may not be effective in a wireless ad-hoc network. Therefore, researchers have started to develop IDS solutions that are applicable for this environment. A number of research efforts concentrated on developing solutions as an extension of the Dynamic Source Routing (DSR) protocol, and using a simulated environment to evaluate the proposed solutions. Research efforts should continue to explore new methods to detect attacks against the various ad-hoc routing protocols, as well as prototyping existing solutions which appear promising.

References

[1] Bradley, K., Cheung, S., Puketza, N., Mukherjee, B., and Olsson, R. "Detecting Disruptive Routers: A Distributed Network Monitoring Approach, In *Proceedings of IEEE Symposium on Security and Privacy*, May 1998.

[2] Brutch, P., Brutch, T., and Pooch, U. "Electronic Quarantine: An Automated Intruder Response Tool", In *Proceedings of Information Survivability Workshop*, 1998.

[3] Buchegger, S. and Boudec, J. "Performance Analysis of the CONFIDANT Protocol (Cooperation of Nodes: Fairness in Dynamic Ad-ho Networks)", In *Proceedings of MOBIHOC '02*, 2002.

[4] Cheung, S. and Levitt, K., "Protecting Routing Infrastructures from Denial of Service Using Cooperative Intrusion Detection", In *Proceedings of New Security Paradigms Workshop*, 1997.

[5] Jou, Y., Gong, F., Sargor, C., Wu, X., Wu, S., Chang, H., and Wang, F., “Design and Implementation of a Scalable Intrusion Detection System for the Protection of Network Infrastructure”, In *Proceedings of DARPA Information Survivability Conference and Exposition,* 2000.

[6] Ko, C., Ruschitzka, M., and Levitt, K. “Execution Monitoring of Security Critical Programs in Distributed Systems: A specification-based approach,” In *Proceedings of Symposium on Security and Privacy*, 1997.

[7] Ko, C., Brutch, P., Rowe, J., Tasfnat, G. and Levitt, K., “System Health and Intrusion Monitoring using a Hierarchy of Constraints”, In *Proceedings of 4th International Symposium on Recent Advances in Intrusion Detection*, 2001.

[8] Kong, J., Luo, H., Xu, K., Gu, D., Gerla, M., and Lu, S.,“Adaptive Security for Multi-layer Ad-hoc Networks,” *Special Issue of Wireless Communication and Mobile Computing*, 2002.

[9] Lee, S., Han, B., and Shin, M. “Robust Routing in Wireless Ad Hoc Networks”, In *Proceedings of the International Conference on Parallel Processing Workshop (ICPPW’02).* 2002.

[10] Marti, S., Giuli, T., Lai, K., and Baker, M., “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks,” In *Proceedings of the Sixth Annual International Conference on Mobile Communication and Networking*, 2000.

[11] Okazaki, Y., Sato, I., and Goto, S., “A New Intrusion Detection Method based on Process Profiling”, In *Proceedings of 2002 Symposium on Applications and the Internet (SAINT ’02)*, 2002.

[12] Stajano F. and Ross, A., “The Resurrecting Duckling: Security for Ad-hoc Networks, *AT&T Software Symposium*, 1999.

[13] White, G. and Pooch, U., “Cooperating Security Managers: Distributed Intrusion Detection System,” *Computers & Security*, vol. 15, no. 5, 1996.

[14] Zhang, Y. and Lee, W., “Intrusion Detection in Wireless Ad-Hoc Networks,” In *Proceedings of the Sixth Annual International Conference on Mobile Communication and Networking*, 2000.

[15] Zhou, L. and Haas Z., “Securing Ad Hoc Networks,” *IEEE Network Magazine*, vol. 13, no. 6, November/December 1999.