H.N.Pratihari / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 1,Jan-Feb 2012, pp.962-966

Intrusion Detection System (IDS) for Secure MANETs: A Study

H.N.Pratihari
Department of Electronics & Telecommunication
Orissa Engoneering College, Bhubaneswar-752050

Abstract—Flooding-based route discovery is usually preferred in MANETs in order to set up the route with reliability between transmission pair. However, this approach may cause a serious contention in information transfer between adjacent nodes and a considerable amount of control packets. The transfer of information between nodes is made secured by Intrusion detection system (IDS). The architecture of IDS is discussed in the manuscript to achieve the reliable and confidential transmission over MANET which follows some techniques such as Watch Dog, Confident, and CORE.

Keywords- Cryptographic attacks in MANET, IDS, architecture of IDS, Watch Dog, CORE.

I. INTRODUCTION

In a mobile ad hoc network (MANET), a collection of mobile hosts with wireless network interfaces form a temporary network without the aid of any fixed infrastructure or centralized administration. A MANET is referred to as an infrastructure less network because the mobile nodes in the network dynamically set up paths among themselves to transmit packets temporarily. In other words a MANET is a self-configuring network that is formed automatically by a collection of mobile nodes without the help of a fixed infrastructure or centralized management. Each node is equipped with a wireless transmitter and receiver, which allow it to communicate with other nodes in its radio communication range. In order for a node to forward a packet to a node that is out of its radio range, the cooperation of other nodes in the network is needed, this is known as multi-hop communication. Therefore, each node must act as both a host and a router at the same time. The network topology frequently changes due to the mobility of mobile nodes as they move within, move into, or move out of the network. In a MANET, nodes within each other's wireless transmission ranges can communicate directly; however, nodes outside each other's range have to rely on some other nodes to relay messages. Thus, a multi-hop scenario occurs, where several intermediate hosts relay the packets sent by the source host before they reach the destination host. Every node functions as a router. The success of communication highly depends on other nodes' cooperation.

II. VARIOUS TYPES OF ATTACKS IN ADHOC NETWORKS

There are also attacks that target some particular routing protocols, such as DSR, or AODV. Currently routing security is one of the hottest research areas in MANET. Attacks can also be classified according to network protocol stacks. Table 1 shows an example of a classification of security attacks based on protocol stack, some attacks could be launched at multiple layers.

TABLE I. CLASSIFICATION OF SEURITY ATTACKS

Layer	Attacks
Application layer	Repudiation, data corruption
Transport layer	Session hijacking, SYN flooding
Network layer	Wormhole, Black hole, Byzantine, flooding, location disclosure attacks
Data link layer	Traffic analysis, monitoring, disruption MAC (802.11), WEP weakness
Physical layer	Jamming, interceptions, eavesdropping
Multi-layer attacks	DOS, impersonation, replay, man-in-the-middle

III. INTRUSION DETECTION SYSTEM (IDS) ARCHITECTURE

Because MANET has features such as an open medium, dynamic changing topology, and the lack of a centralized monitoring and management point, many of the intrusion detection techniques developed for a fixed wired network are not applicable in MANET. Zhang [2] gives a specific design of intrusion detection and response mechanisms for MANET. Marti [5] proposes two mechanisms: watchdog and path rater, which improve throughput in MANET in the presence of nodes that agree to forward packets but fail to do so. In MANET, cooperation is very important to support the basic functions of the network so the token-based mechanism, the credit-based mechanism, and the reputation-based mechanism were developed to enforce cooperation. Each mechanism is discussed in this paper.

The MANETs can be configured to either of two network infrastructures (i) flat or (ii) multi-layer, depending on the applications. Therefore, the optimal IDS architecture for a MANET may depend on the network infrastructure itself [10]. In a flat network infrastructure, all nodes are considered equal, thus it may be suitable for applications such as virtual classrooms or conferences. On the contrary, some nodes are considered different in the multi-layered network infrastructure. Nodes may be partitioned into clusters with one cluster head for each cluster. To communicate within the cluster, nodes can communicate directly. However, communication across the clusters must be done through the cluster head, yet a cluster head actually may not participate in routing. This infrastructure might be well suited for military applications. In combat, military units cannot depend on fixed communication structures, since these are prone to being destructed by the enemy's army.

Distributed and Cooperative Intrusion Detection Systems: Since the nature of MANETs is distributed and requires cooperation of other nodes, Zhang and Lee [2] have proposed that the intrusion detection and response system in MANETs should also be both distributed and cooperative as shown in Figure 3.1. Every node participates in intrusion detection and response by having an IDS agent running on them. An IDS agent is responsible for detecting and collecting local events and data to identify possible intrusions, as well as initiating a response independently.

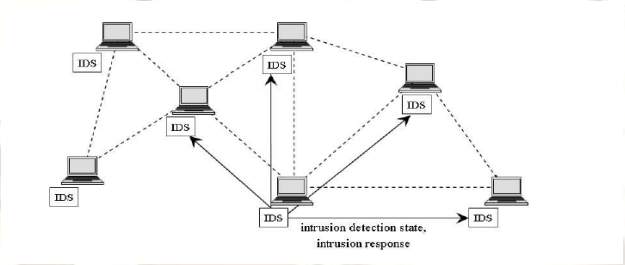

Figure 1. Distributed and Cooperative IDS in MANETs

Hierarchical Intrusion Detection System: Hierarchical IDS architectures extend the distributed and cooperative IDS architectures to multi-layered network infrastructures where the network is divided into clusters. Cluster heads of each cluster usually have more functionality than other members in the clusters, for example routing packets across clusters. Thus, these cluster heads, in some sense, act as control points, which are similar to switches, routers, or gateways in wired networks. Each IDS agent is run on every member node and is responsible locally for its node, i.e., monitoring and deciding on locally detected intrusions.

Sample Intrusion Detection Systems For Manets: Since the IDS for traditional wired systems are not well suited to MANETs, many researchers have proposed several IDS especially for MANETs, which some of them will be reviewed in this sect

Distributed and Cooperative IDS:

Zhang and Lee also proposed the model for distributed and cooperative IDS as shown in Figure . The model for an IDS agent is structured into six modules. The local data collection module collects real-time audit data, which includes system and user activities within its radio range. The local detection engine module for evidence of anomalies will analyze this collected data. If an anomaly is detected with strong evidence, the IDS agent can determine independently that the system is under attack and initiate a response through the local response module (i.e., alerting the local user) or the global response module (i.e., deciding on an action), depending on the type of intrusion, the type of network protocols and applications, and the certainty of the evidence. If an anomaly is detected with weak or inconclusive evidence, the IDS agent can request the cooperation of neighboring IDS agents through a cooperative detection engine module, which communicates to other agents through a secure communication module.

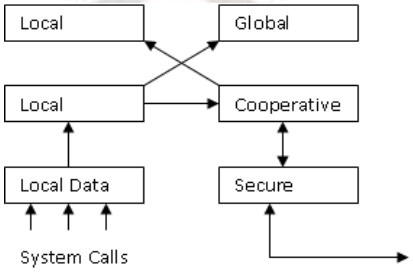

Figure 2. A Model for an IDS Agent

IV. DISTRIBUTED INTRUSION DETECTION SYSTEM USING MULTIPLE SENSORS

Kachirski and Guha [5] proposed a multi-sensor intrusion detection system based on mobile agent technology. The system can be divided into three main modules, each of which represents a mobile agent with certain functionality: monitoring, decision-making or initiating a response. By separating functional tasks into categories and assigning each task to a different agent, the workload is distributed which is suitable for the characteristics of MANETs. In addition, the hierarchical structure of agents is also developed in this intrusion detection system as shown in Figure4.

Monitoring agent: Two functions are carried out at this class of agent: network monitoring and host monitoring. A host-based monitor agent hosting system-level sensors and user-activity sensors is run on every node to monitor within the node, while a monitor agent with a network monitoring sensor is run only on some selected nodes to monitor at packet-level to capture packets going through the network within its radio ranges.

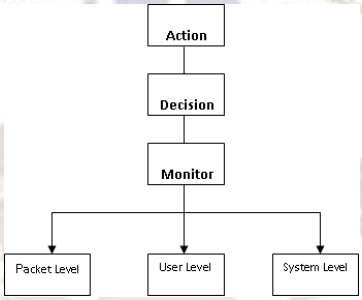

Figure 3. Layered Mobile Agent Architecture

Intrusion Detection Techniques for Node Cooperation In Manets: Since there is no infrastructure in mobile ad hoc networks, each node must rely on other nodes for cooperation in routing and forwarding packets to the destination. Intermediate nodes might agree to forward the packets but actually drop or modify them because they are misbehaving. The simulations in [6] show that only a few misbehaving nodes can degrade the performance of the entire system. There are several proposed techniques and protocols to detect such misbehavior in order to avoid those nodes, and some schemes also propose punishment as well [7, 8].

V. WATCHDOG AND PATHRATER

Marti, Giuli, and Baker [6] proposed two techniques, Watchdog and Path rater, to be added on top of the standard routing protocol in adhoc networks. Dynamic Source Routing protocol (DSR) is chosen for the discussion to explain the concepts of Watchdog and Path rater. The watchdog method detects misbehaving nodes. The watchdog identifies the misbehaving nodes by eavesdropping on the transmission of the next hop. A path rater then helps to find the routes that do not contain those misbehaving nodes. In DSR, the routing information is defined at the source node. This routing information is passed together with the message through intermediate nodes until it reaches the destination. Therefore, each intermediate node in the path should know who the next hop node is. Figure: shows how the watchdog works.

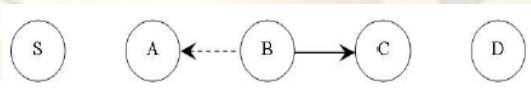

Figure 4. Figure: How watchdog works: Although node B intends to transmit a packet to node ‘C’, node ‘A’ could overhear this transmission.

Assume that node ‘S’ wants to send a packet to node ‘D’, and there exists a path from ‘S’ to ‘D’ through nodes ‘A’, ‘B’, and ‘C’. Consider now that ‘A’ has already received a packet from ‘S’ destined to ‘D’. The packet contains a message and routing information. When ‘A’ forwards this packet to ‘B’, ‘A’ also keeps a copy of the packet in its buffer. Then, ‘A’ listens to the transmission of ‘B’ to make sure that ‘B’ forwards to ‘C’. If the packet overheard from ‘B’ (represented by a dashed line) matches that stored in the buffer, it means that ‘B’ really forwards to the next hop (represented as a solid line). It then removes the packet from the buffer. However, if there's no matched packet after a certain time, the watchdog increments the failures counter for node ‘B’. If this counter exceeds the threshold, ‘A’ concludes that ‘B’ is misbehaving and reports to the source node ‘S’. The watchdog

is implemented by maintaining a buffer of recently sent packets and comparing each overheard packet with the packet in the buffer to see if there is a match. If so, the packet in the buffer is removed and forgotten by the watchdog, since it has been forwarded on. If a packet has remained in the buffer for longer than a certain timeout, the watchdog increments a failure tally for the node responsible for forwarding on the packet. If the tally exceeds a certain threshold bandwidth, it determines that the node is misbehaving and sends a message to the source notifying it of the misbehaving node. The watchdog technique has advantages and weaknesses. DSR with the watchdog has the advantage that it can detect misbehavior at the forwarding level and not just the link level. Watchdog's weaknesses are that it might not detect a misbehaving node in the presence of

- Ambiguous collisions,
- Receiver collisions,
- Limited transmission power,
- False misbehavior,
- Collusion, and
- Partial dropping.

The ambiguous collision problem prevents 'A' from overhearing transmissions from 'B'. A packet collision can occur at 'A' while it is listening for 'B' to forward on a packet. 'A' does not know if the collision was caused by 'B' forwarding on a packet as it should or if 'B' never forwarded the packet and the collision was caused by other nodes in A's neighborhood. Because of this uncertainty, 'A' should not immediately accuse 'B' of misbehaving, but should instead continue to watch 'B' over a period of time. If 'A' repeatedly fails to detect 'B' forwarding on packets, then 'A' can assume that 'B' is misbehaving.

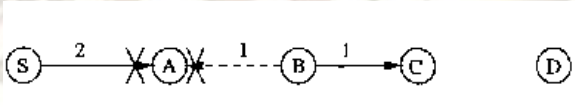

Figure 5. Ambiguous collision, Node 'A' does not hear 'B' forward packet 1 to 'C' because B's transmission collides at 'A' with packet 2 from the source 'S'.

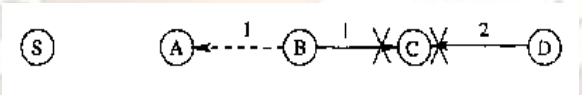

Figure 6. Receiver collision, Node 'A' believes that 'B' has forwarded packet 1 on to 'C', though 'C' never received the packet due to a collision with packet 2.

In the receiver collision problem, node 'A' can only tell whether 'B' sends the packet to 'C', but it cannot tell if 'C' receives it. If a collision occurs at 'C' when 'B' first forwards the packet, 'A' only sees 'B' forwarding the packet and assumes that 'C' successfully receives it. Thus, 'B' could skip retransmitting the packet. 'B' could also purposefully cause the transmitted packet to collide at 'C' by waiting until 'C' is transmitting and then forwarding on the packet. In the first case, a node could be selfish and not want to waste power with retransmissions. In the latter case, the only reason 'B' would have for taking the actions that it does is because it is malicious. 'B' wastes battery power and CPU time, so it is not selfish. An overloaded node would not engage in this behavior either, since it wastes badly needed CPU time and bandwidth. Thus, this second case should be a rare occurrence.

CORE (Collaborative Reputation): As nodes sometimes do not intentionally misbehave, i.e., battery condition is low, these nodes should not be considered as misbehaving nodes and excluded from the network. To do this, the reputation should be rated based on past reputation, which is zero (neutral) at the beginning. In addition, participation in the network can be categorized into several functions such as routing discovery (in DSR) or forwarding packets. Each of these activities has different level of effects to the network; for example, forwarding packets has more effect on the performance of the system than that of routing discovery. Therefore, significance weight of functions should be used in the calculation of the reputation.

The Watchdog mechanism: Every time a network entity (si,m, monitoring entity) needs to monitor the correct execution of a function implemented in a neighboring entity (sj,o, observed entity), it triggers a WD specific to that function (f). The WD stores the expected result er(f) in a temporary buffer in si,m and verifies if the observed result or(f) and er(f) match. If the monitored function is executed properly then the WD removes from the buffer the entry corresponding to the sj,o, er(f) couple and enters in an idle status, waiting for the next function to observe. On the other hand, if the function is not correctly executed or if the couple sj,o, er(f) remains in the buffer for more than a certain time out, a negative value to the observation rating factor ok is reported to the entry corresponding to sj,o in the RT and a new reputation value for that entity is calculated. It should be noticed that the term

expected result corresponds to the correct execution of the function monitored by the WD, which is substantially different from the final result of the execution of the function.

VI. CONCLUSION

This paper presents a brief description of Intrusion Detection System (IDS) to make a secured MANET by IDS which are proposed for ad-hoc mobile networks and also provide techniques of IDS according to distributed architecture of IDS. It has also presented a comparison of techniques such as Watchdog, Confidant, CORE, Route guard, Ocean and Cooperative ideas and reveals their features. By considering all the aspects, MANET is better and secure.

REFERENCES

[1] Tiranuch Anantvalee, Jie Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks" Wireless/Mobile Network Security Journal, pp. 170 – 196, 2006 Springer

[2] Y. Zhang, W. Lee, and Y. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks," ACM/Kluwer Wireless Networks Journal (ACM WINET), Vol. 9, No. 5, September 2003.

[3] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion Detection in Wireless Ad Hoc Networks," IEEE Wireless Communications, Vol. 11, Issue 1, pp. 48-60, February 2004

[4] P. Albers, O. Camp, J. Percher, B. Jouga, L. M, and R. Puttini, "Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches," Proceedings of the 1st International Workshop on Wireless Information Systems (WIS-2002), pp. 1-12, April 2002.

[5] O. Kachirski and R. Guha, "Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks," Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS'03), p. 57.1, January 2003.

[6] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom'00), pp. 255-265, August 2000.

[7] S. Buchegger and J. Le Boudec, "Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes - Fairness In Dynamic Ad-hoc NeTworks)," Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'02), pp. 226-336, June 2002.

[8] P. Michiardi and R. Molva, \Core: A Collaborative Reputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks," Communication and Multimedia Security Conference (CMS'02), September 2002.

[9] D. B. Johnson, and D. A. Maltz, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (Internet-Draft)," Mobile Ad-hoc Network (MANET) Working Group, IETF, October 1999.

[10] P. Brutch and C. Ko, "Challenges in Intrusion Detection for Wireless Ad-hoc Networks," Proceedings of 2003 Symposium on Applications and the Internet Workshop, pp. 368-373, January 2003.

[11] M. G. Zapata, "Secure Ad Hoc On-Demand Distance Vector (SAODV) Routing," ACM Mobile Computing and Communication Review (MC2R), Vol. 6, No. 3, pp. 106-107, July 2002.