



SECURITY IN MOBILE AD-HOC NETWORK USING NOVEL INTRUSION DETECTION SYSTEM

Meenakshi Mishra¹, Niketan Mishra², Soni Changlani³

¹Student (M.Tech. ECE), ²Assistant Professor ECE, ³HOD Dept. of ECE,

Abstract: This paper is based on Security in mobile ad-hoc network using Novel Intrusion Detection System. Mobile ad-hoc network is collection of temporary nodes, that are capable of dynamic forming temporary network, self organize, infrastructure less with nodes contains routing capability, In a mobile ad hoc network (MANET) where security is a crucial issue, A number of neighbor-monitoring, trust-building, and cluster-based voting schemes have been proposed in the research to enable the detection and reporting of malicious activity in ad hoc networks. The resources consumed by ad hoc network member nodes to monitor, detect, report, and diagnose malicious activity, however, may be greater than simply rerouting packets through a different available path. In this paper we present method for determining intrusion or misbehave in MANET using Novel intrusion detection system and protect the network through misbehave.

Key Words: Mobile ad hoc network, intrusion detection, intrusion detection system, attack model.

I. Introduction

Wireless communications offer organizations and users many benefits such as portability and flexibility, increased productivity, and lower installation costs. Wireless local area network (WLAN) devices, for instance, allow users to move their laptops from place to place within their offices without the need for wires and without losing network connectivity. Less wiring means greater flexibility, increased efficiency, and reduced wiring costs. Ad hoc networks, such as those enabled by Bluetooth, allow data synchronization with network systems and application sharing between devices. Handheld devices such as personal digital assistants (PDA) and cell phones allow remote users to synchronize personal databases and provide access to network services such as wireless e-mail, Web browsing, and Internet access. However, risks are inherent in any wireless technology. Some of these risks are similar to those of wired networks; some are exacerbated by wireless connectivity; some are new. Perhaps the most significant source of risks in wireless networks is that the technology's underlying communications medium, the airwave, is open to intruders, making it the logical equivalent of an Ethernet port in the parking lot. The loss of confidentiality and integrity and the threat of denial of service (DoS) attacks are risks typically associated with wireless communications. Unauthorized users may gain access to agency systems and information, corrupt the agency's data, consume network bandwidth, degrade network performance, and launch attacks that prevent authorized users from accessing the network, or use agency resources to launch attacks on other networks. Network traffic can be monitored on a wired network segment, but ad hoc nodes can only monitor network traffic within their observable radio transmission range. MANETs have come into prominence due to potentially rapid infrastructure-less deployment in military and emergency situations. However, the unreliability of wireless links between nodes, possibility of mobile nodes being captured or compromised, break down of cooperative algorithms, all lead to increased vulnerability. Unrelenting attackers will eventually infiltrate any system. It is important to monitor what is taking place in a system and look for intrusions. Intrusion Detection Systems (IDS) do precisely that. An IDS forms the second wall of defense in a high-survivability network. Intrusion prevention measures such as authentication and encryption are not guaranteed to work all the time, which brings out the need to complement them with efficient intrusion detection and response. If an intrusion is detected quickly enough, the intruder can be ejected before any damage is done or any data is compromised. Effective IDS can not only serve as a prevention to prevent intrusions but also provide information about intrusions to strengthen intrusion prevention measures.

II. Background

Intrusion detection systems can be classified broadly into two classes (a) Reputation based schemes, and (b) Incentive based approaches.

Reputation based schemes detect misbehaving nodes and notify other nodes of the misbehaving nodes. Incentive based approaches aims to promote positive behavior to foster cooperation instead of relying on participants to report and punish misbehaving nodes. Zhang et al. have developed a distributed and cooperative intrusion detection system (IDS) where individual IDS agents are placed on each and every node. Each IDS agent runs independently, detects intrusion from local traces and initiates response. The authors have detailed intrusion

detection methods for the following attacks: (i) Falsifying route entry in a node's route, and (ii) Random packet dropping by intermediate nodes. The random packet dropping detection scheme relies on overhearing transmissions of neighboring nodes. Bhargava and Agrawal have extended the IDS model described in to enhance the security in AODV (Ad-hoc on demand Distance Vector) routing protocol. A number of IDS techniques have been proposed in the research literature. Moreover, a number of trust building and cluster-based voting schemes have been proposed to enable the sharing and vetting of messages, and data, generated and gathered by IDS systems. Zhang and Lee describe a distributed and collaborative anomaly detection-based IDS for ad hoc networks. Tseng et al. describe an approach that involves the use of finite state machines for specifying correct AODV routing behavior and distributed network monitors for detecting run-time violation of the specifications. Pirzada and McDonald present a method for building confidence measures of route trustworthiness without a central trust authority. The authors also present a concise summary of previous work in the area of establishing trust in ad-hoc networks. Theodorakopoulos and Baras present a method for establishing trust metrics and evaluating trust. Michiardi and Molva assign a value to the "reputation" of a node and use this information to identify misbehaving nodes and cooperate only with nodes with trusted reputations.

III. Proposed Scheme

Our IDS is based on principle of misuse detection, which can accurately match signatures of known attacks and has a low rate of false alarms. Our approach has focused on Ad-hoc on demand distance vector routing protocols, which are widely used and easy to implement. The generic approach taken while successfully implementing the scheme for AODV protocol allows us to incorporate it in any other MANET routing protocol. Novel intrusion detection system detect the mis-incident happens on the network, in our module we analyze the result through number of mis-incidents comes on the network and then after IDS we protect through mis-incident. We use threshold base mechanism to detect the intrusive process from the network and also find out attacker node and attack time information. After finding out attacker node we block that particular node so in future no intrusion comes to our mobile ad-hoc network. In our module we capture the information about (sender, receiver node info, next hop info, packet sending time, packet type, routing protocol, etc.) and according to threshold we set node as attacker or not.

IV. Intrusion Detection System

An IDS is shown below in figure 1.1 which have three different modules namely Normal Profile, Attacker node and Intrusion information. . Normal profile consists of TCP transmission, UDP transmission and CBR transmission; it also contains the path of packet flow in the network this information is before the attacker node enters in the network. After that attacker node enter the network in place of critical path, it captures the information of normal profile and infect the vulnerable node in network through message passing (probing packets) between abstract network and detailed network and then attacker node set the scan rate, scan port, percentage of vulnerability and infection parameters. If probing port of detailed network and abstract network are same then attacker node sends the infected packets to all the vulnerable nodes and infects the network. Intrusion Information takes the information from both normal profile and attacker node and detects the intrusion by comparing both the information's with also compare maximum and minimum threshold value. It checks for fields like attacker node number, port number, time of intrusion and type of attack.

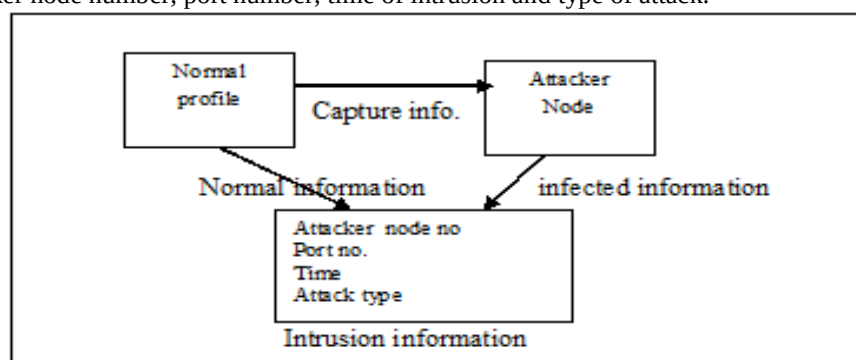


Figure 1.1 Model of Intrusion Detection System

(A) IDS (Intrusion Detection System) Algorithm

```

Create node =ids;
Set routing = AODV;
If ((node in radio range)&&(next hop !=Null))
{
    Capture load(all_node)
    Create normal_profile();

```

```

Threshold_parameter()
  If ((load <= max_limit) &&(new_profile <= max_threshold)&&(new_profile>= min_threshold))
  {
    No any attack ;
  }
  Else {
    Attack in network;
    Find_attack_info();
  }
  Else { "node out of range or destination unreachable"
}
}

```

V. Proposed Architecture

It has six modules in our architecture namely, routing table, TCP block information, CBR packets information, UDP packets and loss information, and data base of IDS. In our intrusion detection system we firstly create the normal profile and after next scenario we create one node as IDS. IDS node check the behaviour of all node if any node deviate from normal behavior than IDS node block that particular node and protect the network through misbehave, in architecture diagram we show each module of IDS. According to algorithm we set threshold parameter for finding attacker node if attacker nodes comes to an our network result deviated from threshold value so that mis activity spread on the network, attacker node un wanted or use less data send to other nodes so our network congested and our performance has been decreases .

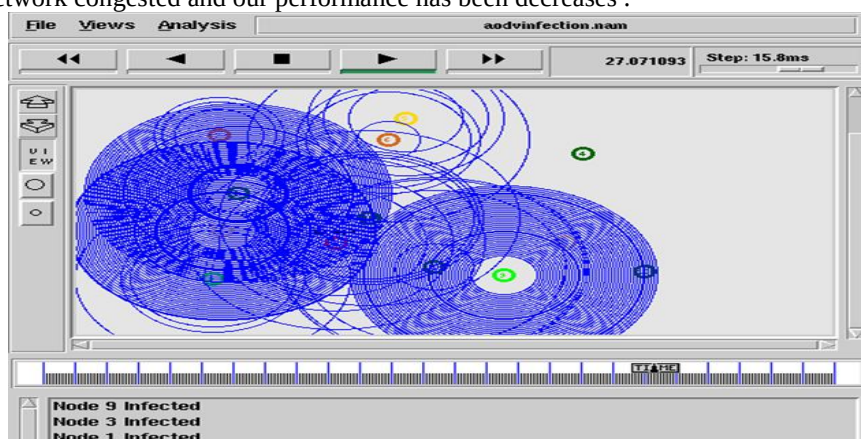


Figure 1.2 Sample Topology Generated by NS-2

In figure 1.2 we show sample topology with 12 mobile nodes and attack simulation, attacker node send the probing packet to all other neighbour and infect the network here node no 9, 3 and 1 are infected via attacker node so that case our performance will decrease because actual data cant by sends through sender node, sender node send only routing packet but network are congested by unwanted packet.

(A) UDP Packet Receive Analysis

Here we analyze UDP packet in all three cases Normal time, attack case and after IDS node time, normal case 45 packet receive by the receiver but attacker node comes to our network only 25 packet receive by the receiver that mean 45% data receiving decreases, after third simulation we add IDS module to our network so receiver receive 45 packets that means 100% data transmitted. Analysis result comes through the gnu_plot, UDP (User data gram protocol) is connection less so our network has unreliable but fast transmission if attacker nodes come to our network, so vulnerable nodes overloaded and network has more congested than the normal case.

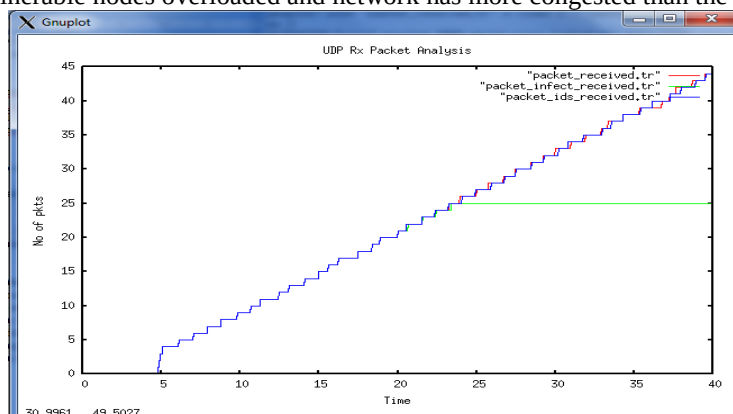


Figure 1.3 UDP Packet Receive Analysis

(B) Packet Delivery Ratio Analysis

The ratio between the number of packets originated by the application layer CBR sources and the number of packets received by the CBR sink at the final destination. Here in AODV and IDS time packet delivery ratio result is very good but in case Attack after 23 msec no any data packet transmission so PDR calculation end.

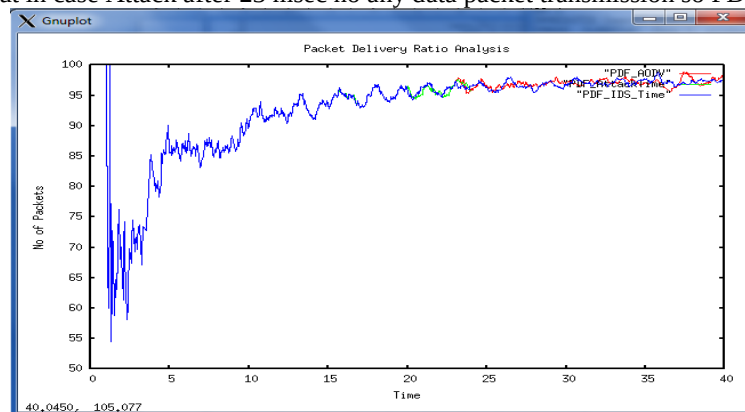


Figure 1.4 Packet Delivery Ratio

VI. Conclusion

We performed a number of tests in NS-2 simulator and analyze the result we get the summery result according to test simulation in normal routing time total number of packet transmitted by the genuine sender is 947 but in case of attacker node packet transmission only 578 that means 39% transmission decreases. But if we set one node as IDS so transmission percentage nearby equal as normal time that result conclude 99.9 percent accuracy comes after attaching IDS node in the network. Other side also PDF packet delivery fraction analysis if attacker node comes on to the network so 6% PDF decrease. And IDS improve the PDF 5.9%. we also analyze routing overhead in normal case only 0.11 % of routing load but attacker node present case 800 times increase routing load, that means very-very routing over head increases it gives poor performance of the network, finally we conclude our result IDS (intrusion detection system) 99.9% data recover.

References

- [1] A. Karygiannis, E. Antonakakis, and A. Apostolopoulos, Detecting Critical Nodes for MANET Intrusion Detection Systems".
- [2] Ketan Nadkarni, Amitabh Mishra, "A Novel Intrusion Detection Approach for Wireless Ad hoc Networks".
- [3] Y. Zhang and W. Lee. Intrusion detection in wireless ad hoc networks. In Proceedings of the 6th annual international conference on Mobile computing and networking, pp. 275–283. ACM Press, 2000.
- [4] Y. Zhang, W. Lee, and Y. Huang. Intrusion detection techniques for mobile wireless networks. ACM/Kluwer Mobile Networks and Applications (MONET), 2002.
- [5] C.-Y. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe, and K. Levitt. A specificationbased intrusion detection system for AODV. In Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, pp. 125–134. ACM Press, 2003.
- [6] Pirzada, Asad Amir, and McDonald, Chris. Establishing trust in pure ad-hoc networks. Proceedings of the 27th conference on Australasian Computer Science - Volume 26, pp 47-54, 2004
- [7] Theodorakopoulos, George and Baras, John. Trust evaluation in ad-hoc networks. Proceedings of the 2004 ACM workshop on Wireless security, pp. 1-10, 2004.
- [8] Michiardi, P. and Molva, R., "Core: A Collaborative Reputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks", Communication and Multimedia Security 2002 Conference.