Cross Layer Based IDS Frame Work Using Machine Learning Algorithms in MANET

J.Paramesh[1], A.Pandiaraj[2], R.Bala Santhosh[3], S.Karthickeyan[4]

[1]Associate Professor, MNM Jain Engineering College, Chennai, India

[2]Assistant Professor, Balaji Institute of Technology and Engineering, Chennai, India

[3, 4]PG Scholar, Computer Science & Engineering, MNM Jain Engineering College ,Chennai, India

Abstract

Wireless ad-hoc network is a temporary network set up by wireless mobile nodes moving arbitrary in the places that have no network infrastructure. Since the nodes communicate with each other, they cooperate by forwarding data packets to other nodes in the network. Thus the nodes find a path to the destination node using routing protocols. However, due to security vulnerabilities of the routing protocols, wireless ad-hoc networks are unprotected to attacks of the malicious nodes. One of these attacks is the Sinking Behaviour and Collision Behaviour Attack against network integrity absorbing all data packets in the network. Since the data packets do not reach the destination node on account of this attack, data loss will occur. Simulated the sinking behaviour and collision behaviour attack in various wireless ad-hoc network scenarios and have tried to find a response system in simulations. The intrusion detection identifies the detection accuracy by using cross-layer features to define a routing behaviour.

Keywords — *cross layer, sinking behaviour attack, collision behaviour attack, mobile ad-hoc networks*

1. Introduction

Wireless ad-hoc networks are composed autonomous nodes that are self- managed without any infrastructure. In this way, ad-hoc networks have a dynamic topology such that nodes can be easily join or leave the network at any point of time. They have many potential applications are used, especially, in military and rescue areas such as connecting soldiers on the battlefield or establishing a new network in place of a network which collapsed after a disaster like an earthquake. Ad-hoc networks are suitability for areas where it is not possible to set up a fixed infrastructure. To support this connectivity, nodes use some routing protocols such as AODV (Ad-hoc On-Demand Distance Vector), Besides acting as a host, each node also acts as a router to discover a path and forward packets to the correct node in the network. provided by the nodes themselves. In such a scenario, a malicious entity (apart from compromising a node) , can deny network services by dropping packets that need to be forwarded, by misrouting packets or by launching other attacks. Our methodology to study AODV based malicious node dropping all the traffic in the network makes use of the vulnerabilities of the route discovery packets of the on demand protocols, such as AODV. In route discovery process of AODV protocol, intermediate nodes are responsible to find a fresh path to the destination, sending discovery packets to the neighbor nodes. In this work there are two kinds of attack can be given as an input and cross layer features are calculate with the help of the attack. The attacks can be created for the AODV Routing Protocol. The Routing Protocol based different OSI layer features are collect from the Cross Layer Architecture. The layers are Application layer, MAC layer, Network layer and Physical layer. The intrusion detection systems based on inter dependencies between all the layers. The intrusion detection system for collision attack is performed to difficult to determined the node that causes collisions in an ad hoc network scenario, both the sender and receiver perform to classify nodes that could have possibly caused a collision under a suspicious list called the NO TRUST region.

Intrusion detection and prevention systems are focused on identifying possible incidents, logging layer information about them, and reporting attempts. In addition, organizations use Intrusion detection system for other purposes, such as identifying problems with security policies, documenting existing threats, and deterring individuals from violating security policies.

As wireless ad-hoc networks lack an infrastructure, they are exposed to a two kinds of attacks. The attacks are

- Sinking Behavior attack
- Collision Behavior attack

Sinking is a malicious behaviour of nodes, where nodes do not cooperate in the routing and forwarding operations of the network. Nodes exhibiting sinking behaviour maliciously drop data or routing messages. The possible objective of this behaviour is to either to selfishly evade from the network responsibilities for resource conservation or to disrupt the network by drop all critical packets. As stated before, cooperativeness of nodes is crucial to the operation of the network. As nodes in the network are autonomous, the neighbour nodes' cooperative behaviour needs to be constantly monitored and enforced. Hence, detecting sinking behaviour is important for the network integrity. Collision behaviour attack is one of the Denial of Service (DoS) attack type, which lead to dropping of messages. Collision behaviour Attacks is that intruder nodes never send true control messages initially. To carry out an intruder node waits for neighbouring nodes to send request messages. When the intruder node receive all the message, without checking its routing table, immediately sends a false reply message giving a route to destination over itself, assigning a high sequence number to settle in the routing table of the victim node, before other nodes send a true one at the time collision will be occurred. Therefore requesting nodes assume that route discovery process is completed and ignore messages and begin to send packets over malicious node. Malicious node attacks all request messages this way and takes current routes.

Malicious nodes dropping all the traffic in the network make use of the vulnerabilities of the route discovery packets of the on demand protocols, such as AODV. In route discovery process of AODV protocol, intermediate nodes are responsible to find a fresh path to the destination, sending discovery packets to the neighbor nodes.

II. Related Work

Studies about lot things in security measure for infrastructure less and autonomous node in mobile ad hoc networks.

In this work there are two kinds of attack can be given as an input and cross layer features are calculate with the help of the attack. The attacks can be created for the AODV Routing Protocol. The Routing Protocol based different OSI layer features are collect from the Cross Layer Architecture. The data collection module layers are Application layer, MAC layer, Network layer and Physical layer. The intrusion detection systems based on inter dependencies between all the layers.

Sinking Behaviour Attack

Sinking behaviour attack is an active attack type. Sinking is a malicious behaviour of nodes, where nodes do not cooperate in the routing and forwarding operations of the network. Nodes exhibiting sinking behaviour maliciously drop data or routing messages. As nodes in the network are autonomous, the neighbour nodes cooperative behaviour needs to be constantly monitored and enforced. Hence, detecting sinking behaviour is important for the network integrity.

Attacking node first agrees to all forward packets and then fails to do so. Initially the node do not behaves correctly and replays true RREP messages to nodes that initiate RREQ message. Afterwards, the node just drops the packets.

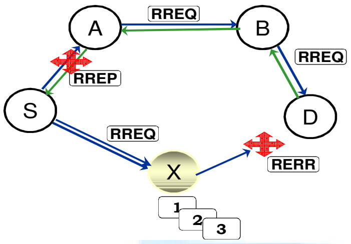


Fig1: Example of sinking behaviour attack

Collision Behaviour Attacks

A collision behaviour attack is an active attack type, which lead to dropping of messages. Collision behaviour Attacks is that intruder nodes never send true control messages initially. To carry out a intruder node waits for neighbouring nodes to send RREQ messages. When the intruder node receives an RREQ message, without checking its routing table, immediately sends a false RREP message giving a route to destination over itself, assigning a high sequence number to settle in the routing table of the victim node, before other nodes send a true one at the time collision will be occurred. Therefore requesting nodes assume that route discovery process is completed and ignore other RREP messages and begin to send packets over malicious node.

Malicious node attacks all RREQ messages this way and takes current routes. Therefore all packets are sent to a point when they are not forwarding anywhere. This is called a Collision behaviour attack.

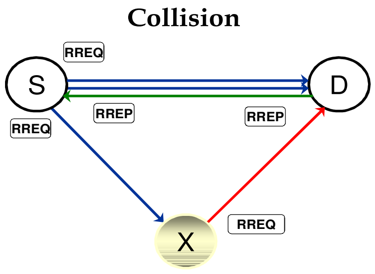


Fig2: Example of Collision behaviour attack

Network Setup

A wireless ad hoc network is a communication network. In this type of network ad hoc nodes are deployed dynamically and communicate with one another to form multi hop wireless ad hoc networks. Here setup a source, destination and malicious nodes. In this module giving network topology as input for network setup module and produce wireless ad-hoc network.

Network is called Independent network Stations communicate directly with each other and do not use an access point. Because of the mobility associated with ad-hoc networks, they are commonly called MANET (Mobile Ad-hoc Network). MANETs are self organized networks whose nodes are free to move randomly while being able to communicate with each other without the help of an existing network infrastructure. MANETs are suitable for use in situations where any wired or wireless infrastructure is inaccessible, overloaded, damaged or destroyed such as emergency or rescue missions, disaster relief efforts and tactical battlefields, as well as civilian MANET situations, such as conferences and classrooms or in the research area like sensor networks.

AODV protocol attacking system design

Attacks against mobile ad-hoc routing protocols are using the Ad-hoc On-Demand Distance Vector (AODV) protocol as an example. Implemented a new routing protocol (SCAODV) which simulates the Sinking behaviour and Collision behaviour attack, and performed tests on different topologies to compare the network performance with and without attack in the network. The cross layer features to use the detection system was determined considerably in the presence of a sinking behaviour and collision behaviour attack. A node may update the route entries in its routing table whenever it receives RREQ, RREP, or RERR messages from its neighbors.

Simulated the Sinking and Collision Behaviour attack in wireless ad-hoc networks and evaluated its damage in the network. Simulations are using NS-2 (Network Simulator version 2) simulation program that consists of the collection of all network protocols to simulate many of the existing network topologies. NS-2 contains wireless ad-hoc routing protocols and it's not having the attacking based protocol. Thus, to simulate Sinking and Collision behaviour attacks. In NS-2 implement the new protocol (SCAODV). To start study by writing a new AODV protocol using C++, to simulate the Sinking and Collision attack. Having implemented a new routing protocol (SCAODV) which simulates the both attack performed tests on different topologies to compare the network performance with and without attack in the network. The throughput in the network was deteriorated considerably in the presence of attack. Afterwards, An IDS solution to eliminate the sinking and Collision behaviour attack effects in the AODV protocol network. Implemented and test the solution into the NS-2.

III. Cross Layer Data Collection

Cross Layer Features

Cross Layer Design (CLD) is a way of achieving information sharing between all the layers. It is a co-operation between multiple layers to combine all the resources. Instead of designing/developing the protocols in isolation, Cross Layer Design take advantage of the interdependencies between them. Cross Layer Feedback can be categorized based on information flow as follows

- Upward Information Flow
- Downward Information Flow

Upward Information Flow

Information flowing upwards from a layer to any layer above it Eg:TCP Packet loss information is given to the application layer so that the application can adapt its sending rate.

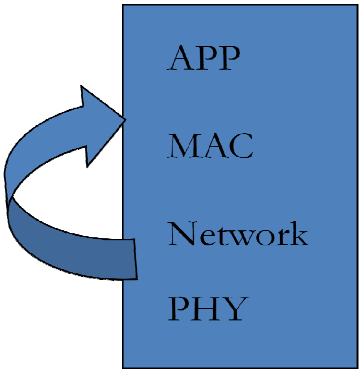


Fig3: Upward Information Flow

Downward Information Flow

Information flowing downwards from a layer to any layer above it Eg:TCP Packet loss information is given to the application layer so that the application can adapt its sending rate.

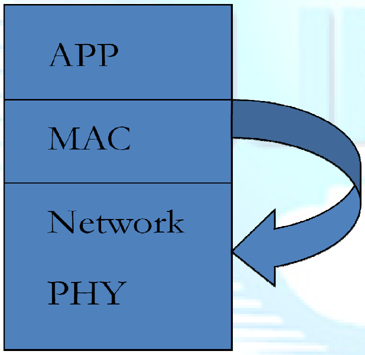


Fig4: Downward Information Flow

B. Application Layer Statistics

The application layer is the interface to the user for running user tasks. Eg: Web browsing, downloading a file using FTP, sending email, watching a video clip etc.

Information's available at Application Layer

Based on applications Qos need it can have delay between data transmission, throughput and packet loss rate.

C Routing Layer Statistics

The function of routing layer is establishing end-to-end connections over the network. The network layer is responsible for routing packets, establishing the network service type (connectionless versus connection-oriented), and transferring packets between the transport and link layers.

Information Available at Transport Layer:

Number of received RREQ messages, Number of received RREP messages, Number of received RERR messages, Number of forwarded RREQ messages, Number of forwarded RREP messages.

D MAC Layer Statistics

The MAC layer is responsible for establishing a reliable and secure logical link over the unreliable wireless link. A sub layer of the data link layer, the media access control (MAC) protocol layer is responsible for allocating the time-frequency or code space among mobiles sharing wireless channels in a region.

Interactions of Link/MAC Layer s

Application Layer:

Different applications have different Qos requirements. At the link/MAC layer the frames can be treated differently based on the Qos needs of the corresponding application.

Transport Layer:

Retransmission information from the link layer could be used to adapt TCP retransmission timer.

Network Layer:

Link Layer hand-off information can be used to reduce the hand-off latency for Mobile-IP when the mobile device changes subnets.

Physical Layer:

Based on current channel conditions the error control mechanisms at the link layer may be adapted to reduce the transmission errors also using the channel condition the frame length can be adapted to improve the throughput.

Battery aware link/MAC Layer:

Adaptation of the FEC/ARQ mechanisms or the physical layer transmit power can be used to increase power consumption.

Information available at link/Mac Layer:

Number of active transmission, Delay between data transmission, Number of retransmission data.

Physical Layer Statistics

To transmit raw bits at a certain power level to achieve a certain transmission range and reduce bit errors.

Information available at physical Layer:

Transmit power, Bit error rate (BER).

IV. Result And Analysis

A.NS Network Simulator

NS is an object oriented discrete event simulator

- Simulator maintains list of events and executes one event after another event.
- Single thread of control: no locking or race conditions.

Back end is C++ event scheduler

- Creating Protocols and interface.
- Fast to run and more control.
    - Front end is OTCL
- Creating scenarios, extensions to C++ protocols.
- Fast to write and change tool command language.

Topology Construction

Number of nodes	25
Simulation time	20 sec
Environment size	1000X1000
Transmission range	200m
Routing Protocol	AODV Protocol
Antenna Type	Omni Type
Simulator Version	N.S 2.34
Traffic Type	CBR
Propagation	Two Ray Ground

Table1: Topology scenario

B. Implementing a New Routing Protocol in NS to Simulate Sinking Behaviour and Collision Behaviour Attack

Implementation of a new manet Routing Protocol in NS-2 is described. In our work, we have used the nodes that exhibit sinking and collision behaviour attack in wireless ad-hoc network that use AODV protocol. Since the nodes behave an attack they have to use a new routing protocol that can participate in the AODV messaging. Implementation of this new routing protocol is explained below in detail:

Names of all files that are labelled as “aodv” in the directory are changed to “SCAODV” such as scaodv.cc, scaodv.h, scaodv.tcl, scaodv_rqueue.cc, scaodv_rqueue.h etc. in this new directory except for “aodv_packet.h”. The key point in our work is that AODV and sinking and collision AODV protocol will send each other the same AODV packets. Therefore, we did not copy “aodv_packet.h” file into the SCAODV directory.

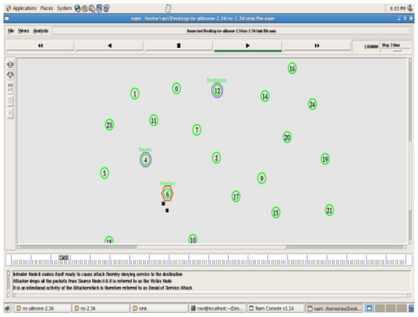
We have changed all classes, functions, structs, variables and constants names in all the files in the directory except struct names that belong to AODV packet.h code. We have

designed aodv and SCAODV protocols to send each other aodv packets.

C. Evaluation of the Simulation

We generate a small size network that has 25 nodes and create a UDP connection between Nodes, and attach CBR (Constant Bit Rate) application that generates constant packets through the UDP connection. CBR packet size is chosen to be 512 bytes long. Duration of the scenarios is 20 seconds and the CBR connections started at time equals to 1.0 seconds and continue until the end of the simulation.

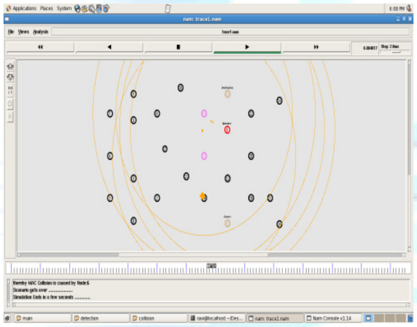
Simulation of sinking behaviour attack the Source node (4) send the packet to attack (6) node but attacking node drop all packets is shown in fig 5



Intruder Node:6 makes itself ready to cause attack thereby denying service to the destination
Attacker drops all the packets from Source Node:4 & it is referred to as the Victim Node
It is an intentional activity of the Attackerwhich is therefore referred to as Denial of Service Attack

Fig5:sinking behaviour attack

Simulation of collision behaviour attack Source node(10) send the packet to node (15) and also send the packet in intruder node (6) is shown in fig6



thereby MAC Collision is caused by Node:6
Scenario gets over ....
Simulation Ends in a few seconds ......

Fig6: collision behaviour attack

Evaluate the packet loss. Therefore we counted how many packets are sent by the sending nodes and how many of them reached the receiving nodes. In this section, we described how many numbers of the packets is loss and compared the sinking and collision behaviour attack. In Fig7 comparison sinking behaviour attack is more vulnerable compare then collision behaviour attack.

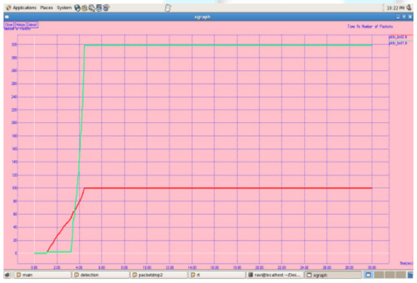


Fig7: packet loss ratio

Evaluate the number of routing packets transmitted per data packet delivered time at the destination. The first two metrics are the most important for best-effort traffic. The routing load metric evaluates the efficiency of the routing protocol. In the conventional wisdom, the longer the path lengths, the higher the probability of a packet drops. Thus, with a lower delivery fraction, samples are usually biased in favour of smaller path lengths and thus have less delay in Fig8.

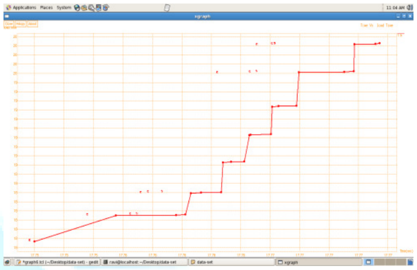


Fig8: Normalized routing load

In scenario, the transmit power can be slightly changed by decreasing the power. The source to broad cast all control messages from various nodes. Therefore we evaluate the reduces the transmitted power.

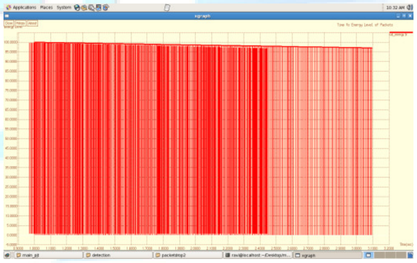


Fig9: Transmitted power

Evaluate the inter arrival time between the nodes. Therefore we counted how time has taken for packets are send and receive between the nodes are generated. In Fig10, we described how data has been are generated the sinking and collision behaviour attack.

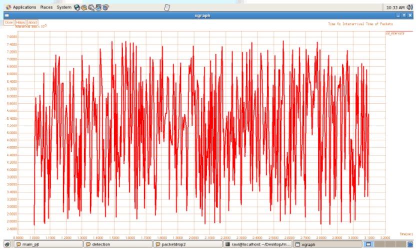


Fig10: packets inter arrival time

V. Conclusion

Analyse effect of the sinking behaviour and collision behaviour attack in an AODV Protocol Network. For this purpose of implemented an AODV protocol that behaves as attack in NS-2. The simulation scenarios where each one has 25 nodes that use AODV protocol and also simulated the same scenarios after introducing one attacking node into the network. In simulation results show the difference between the number of packets lost in the network with and without Attack. To developed a new cross layer design and shared the channel prediction information with the Application layer, MAC layer, Routing layer and Physical layer. As a result all layers able to avoid unnecessary packet transmissions which ultimately save power reduce packet loss and increase the network performance.

Future works simulate the Attack in the Ad-hoc Networks and investigated its affects, by using the AODV routing protocol. But the other routing protocols could be simulated as well. All routing protocols are expected to present different results. The routing protocol for minimizing the attack can be determined. The detection accuracy by using cross-layer features to define a routing behaviour. For learning and adaptation to new attack scenarios and network environments, two machine learning techniques are utilized. Support Vector Machines (SVMs) and Fisher Discriminant Analysis (FDA) are used together to exploit the better accuracy of SVM and faster speed of FDA. Instead of using all cross-layer features, features from MAC layer are associated with features from other layers, thereby reducing the feature set without reducing the information content.

References

[1]. Y. Huang, W. Fan, W. Lee, P. Yu, “Cross-Feature Analysis for Detecting Ad-Hoc Routing Anomalies” icdcs, 23rd IEEE International Conference on Distributed Computing Systems (ICDCS'03), pp. 478-487, 2003.

[2]. Y. Liu, Y. Li, and H. Man, “Short Paper: A Distributed Cross-Layer Intrusion Detection System for Ad Hoc Networks,” Proc.First Int’l Conf. Security and Privacy for Emerging Areas in Comm. Networks 2005 (SecureComm ’05), pp 418-420, 2005.

[3]. Shahid Shehzad Bajwa and Muhammad Khalid Khan, "Grouped Black hole Attacks Security Model (GBHASM) for Wireless Ad-Hoc Networks", The 2nd IEEE International Conference in Computer and Automation Engineering (ICCAE),pp 756, 2010.

[4] D. Johnson, D. Maltz and J. Broch, “DSR the Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks”. Ad Hoc networking, Chapter 5, page 139- 172. Addison-Wesley, 2001.

[5] H. Deng, W. Li and D.P.Agrawal, “Routing Security inWireless Ad Hoc Networks”. University of Cincinnati, IEEE Communication Magazine, October 2002.

[6] G. Vigna, S. Gwalani and K. Srinivasan, “An Intrusion Detection Tool for AODV-Based Ad hoc Wireless Networks”, Proc. of the 20th Annual Computer Security Applications Conference (ACSAC’04).

[7] P. Ning and K. Sun, “How to Misuse AODV: A Case Study of Insider Attacks Against Mobile Ad-Hoc Routing Protocols”, Proc.of the 2003 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY., June 2003.

[8] S. Marti, T. J. Giuli, K. Lai and M. Baker, “Mitigating Routing Misbehavior in Ad Hoc Networks”, Proc. 6th Annual Int’l. Conf. Mobile Comp. and Net., Boston, MA. pp. 255-265. August 2000.

[9]. Geethapriya Thamilarasu and Ramalingam Sridhar, "CIDS: cross-layer intrusion detection system for mobile ad hoc networks", International Journal ERS, Issue: Volume 3, pp 10 – 20, 2009.

[10]. Hidehisa Nakayama, Abbas Jamalipour, Yoshiaki Nemoto,Nei Kato," A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks", IEEE Transaction on Vehicular Technology, Vol. 58, No. 5, pp 16-25 June 2009.