International Journal of Advance Engineering and Research Development (IJAERD)
Volume 1,Issue 6,June 2014, e-ISSN: 2348 - 4470 , print-ISSN:2348-6406

Trust Based Intrusion Detection Systems (IDS) for AODV Routing Protocols over an Ad-Hoc Networks

Dhruvi Marsonia[1], Prof. Purvi Ramanuj[2], Prof. Bhargav Makodia[3]

[1]*M.E. IT Engineering, Shantilal Shah Engineering College, dhruvi.marsonia@gmail.com*
[2]*HOD IT Engineering, Shantilal Shah Engineering College,,purviramanuj@yahoo.com*
[3]*Assistant Professor, Venus International College of Technology,*
bhargavmakodia.ec@venusict.org

Abstract – Ad Hoc Networks are very week to attacks due to their dynamically changing topology, lack of predictable security infrastructures, and vulnerability of nodes, vulnerability of channels and open medium of communication. To address these concerns this work discusses an ad-hoc Network based intrusion detection system (IDS) which can make certain security services required by users. The idea is to implement Network based intrusion detection system (NIDS) for routing in Ad Hoc Networks. As per result, AODV routing protocol with IDS serves promising. Even in presence of malicious nodes within the network, network performance is not degraded. Introduction of trust factor, furthermore improves the network performance.

Key words – AODV; IDS; Packet deliver fraction; Throughput; Delay; Ad-hoc network.

I. INTRODUCTION

To introduce the topic in a nutshell it can be said that, a feature of an ad-hoc network which is a group of nodes connected together by a wireless links for detecting malicious node and creating trust based ad-hoc network. In an ad-hoc network, all mobile nodes agree to relay each other’s packets, and function as routers. Ad-hoc network lacks with a feature of centralized authority; furthermore which leads to miss-management of the entire system. This miss-management is defined as ‘Attack’ in network terminology. Proposed work is based on selfishness attack over the net-work.

II. AD-HOC NETWORKS

An ad hoc wireless network is a collection of two or more devices equipped with wireless communications and networking capability. Such devices can communicate with another node that is immediately within their radio range or one that is outside their radio range. For the latter scenario, an intermediate node is used to relay or forward the packet from the source toward the destination.

An ad hoc wireless network is self-organizing and adaptive. This means that a formed network can be de-formed on-the-fly without the need for any system administration. The term "ad hoc" tends to imply "can take different forms" and "can be mobile, standalone, or networked." Ad hoc nodes or devices should be able to detect the presence of other such devices and to perform the necessary handshaking to allow communications and the sharing of information and services.

III. INTRUSION DETECTION SYSTEM (IDS)

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. IDS come in a variety of “flavors” and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPSes for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IDPSes have become a necessary addition to the security infrastructure of nearly every organization.

IDPSes typically record information related to observed events notify security administrators of important observed events and produce reports. Many IDPSes can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment (e.g. reconfiguring a firewall) or changing the attack's content.

A. Network Intrusion Detection System (NIDS)

Network intrusion detection systems are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. It performs an analysis for a passing traffic on the entire subnet, works in a promiscuous mode, and matches the traffic that is passed on the subnets to the library of known attacks. Once the attack is identified, or abnormal behavior is sensed, the alert can be sent to the administrator. Example of the NIDS would be installing it on the subnet where firewalls are located in order to see if someone is trying to break into the firewall. Ideally one would scan all inbound and outbound traffic, however doing so might create a bottleneck that would impair the overall speed of the network.

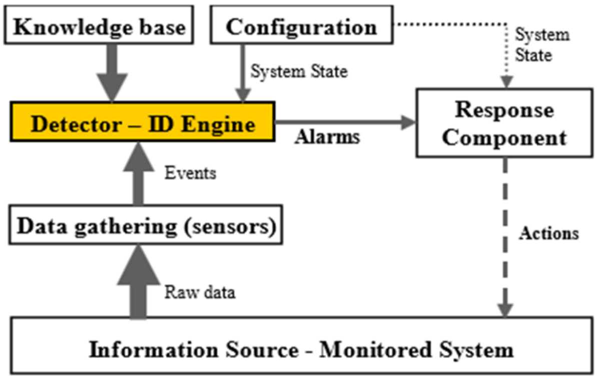

Fig. 1. Basic IDS Frame work

B. Host Intrusion Detection System (HIDS)

Host intrusion detection systems run on individual hosts or devices on the network. A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator if suspicious activity is detected. It takes a snapshot of existing system files and matches it to the previous snapshot. If the critical system files were modified or deleted, the alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission critical machines, which are not expected to change their configurations.

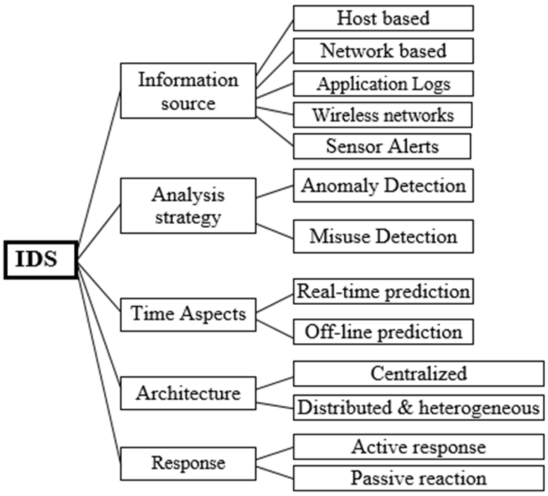

Fig. 2. Classification of IDS

IV. IDS ALGORITHM

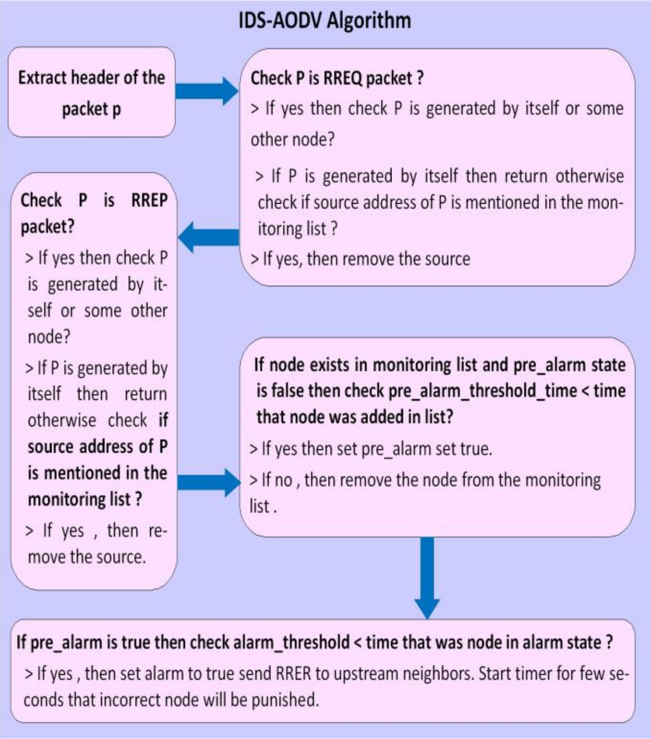
IDS-AODV Algorithm
Extract header of the packet p
Check P is RREQ packet ?
> If yes then check P is generated by itself or some other node?
> If P is generated by itself then return otherwise check if source address of P is mentioned in the monitoring list ?
> If yes, then remove the source
Check P is RREP packet?
> If yes then check P is generated by itself or some other node?
> If P is generated by itself then return otherwise check if source address of P is mentioned in the monitoring list ?
> If yes , then remove the source.
If node exists in monitoring list and pre_alarm state is false then check pre_alarm_threshold_time < time that node was added in list?
> If yes then set pre_alarm set true.
> If no , then remove the node from the monitoring list .
If pre_alarm is true then check alarm_threshold < time that was node in alarm state ?
> If yes , then set alarm to true send RRER to upstream neighbors. Start timer for few seconds that incorrect node will be punished.

Fig. 3. IDS Algorithm

V. SOFTWARE UTILITY/TOOLS

Network Simulator (Version 2), widely known as NS2, is simply an event driven simulation tool that has proved useful in studying the dynamic nature of communication networks.

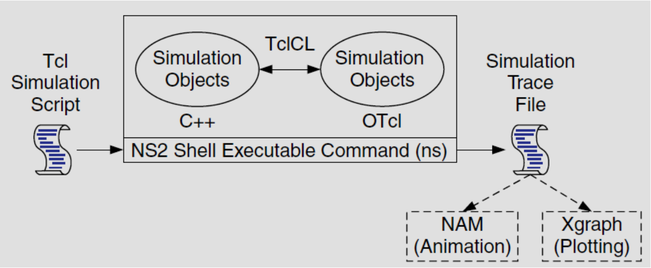

Fig. 4. Basic NS2 architecture

VI. SIMULATION ENVIRONMENT

TABLE I
SIMULATION ENVIRONMENT

Parameter	Description
Routing Protocol	AODV
Number of Nodes	5 to 40
Simulation Time	200 sec
Speed of nodes	Random
Area	1000m x 1000m
Connection type	TCP
Packet size	512B
Queue length	50
Maximum packet size	1000B

V. SIMULATION RESULTS

Simulation is carried out as per the network environment prescribed in table 1. Network performance is evaluated based on network packet deliver fraction, average throughput and end to end delay. Results cab bifurcated based on number of malicious node present in the network. AT present one and two malicious nodes are considered Results for, AODV routing protocol, Selfish AODV, IDS – AODV and Trust based IDS AODV algorithm is considered.

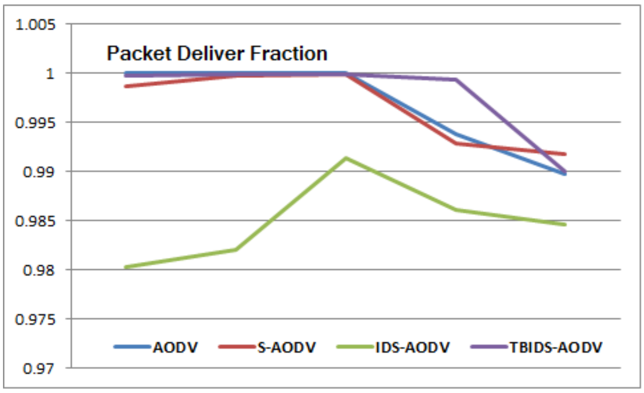

Fig. 5. Packet deliver fraction for network with one malicious node

Figure 5 shows comparison of packet deliver fraction for various AODV routing algorithm with 1 malicious node in the network. Trust based IDS - AODV routing algorithm seems to be promising. Highest value of packet deliver fraction is obtained with TBIDS-AODV.

Trust based algorithm is dependent on the intrusion detection system. An ID gives data relevant to malicious activity of the network.

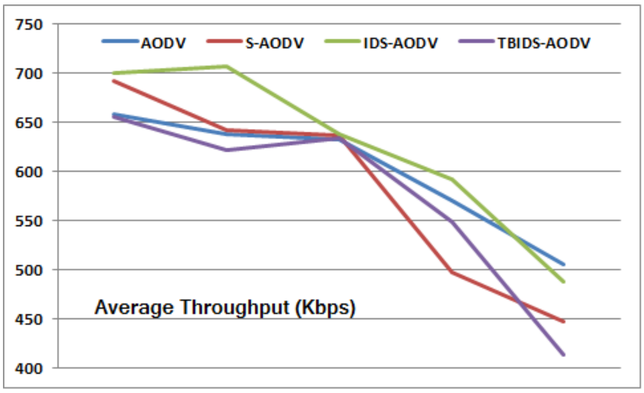

Fig. 6. Average throughput for network with one malicious node

Figure 6 shows comparison of average throughput for various AODV routing algorithms with one malicious node in the network. All routing protocols have drastic variations in the results. Although Trust based IDS - AODV seems to have consistent throughput values.

Figure 7 shows comparison of average end to end delay for various AODV routing algorithm with one malicious node in the network. Consistency in minimum end to end delay values is obtained with trust based IDS - AODV routing algorithm.

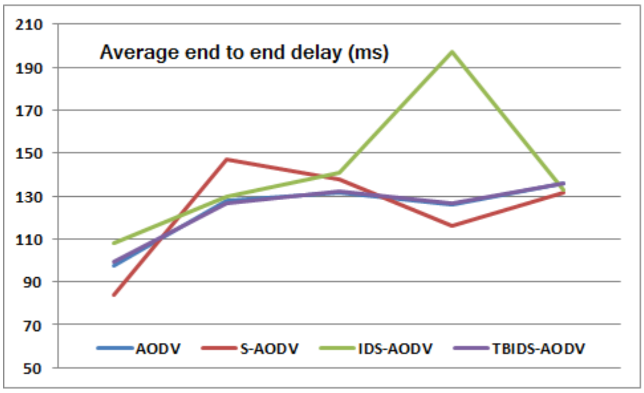

Fig. 7. Average end to end delay for network with one malicious node

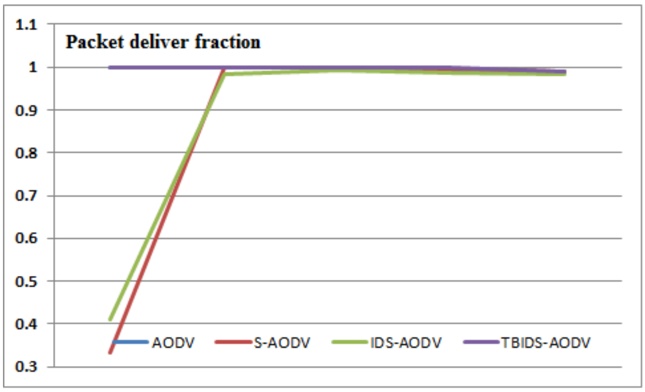

Fig. 8. Packet deliver fraction for network with two malicious nodes

Figure 8 shows comparison of packet deliver fraction for various AODV routing algorithm with 2 malicious nodes in the network. Trust based IDS - AODV routing algorithm seems to be promising. Highest value of packet deliver fraction is obtained with TBIDS-AODV.

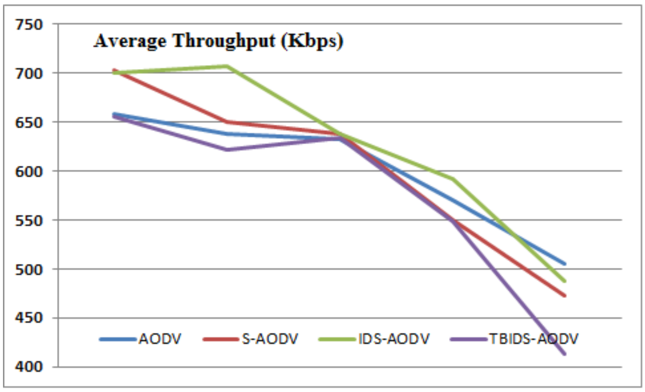

Fig. 9. Average throughput for network with two malicious nodes

Figure 9 shows comparison of average throughput for various AODV routing algorithms with one malicious node in the network. All routing protocols have drastic variations in the results. Although Trust based IDS - AODV seems to have consistent throughput values.

Figure 10 shows comparison of average end to end delay for various AODV routing algorithm with one malicious node in the network. Consistency in minimum end to end delay values is obtained with trust based IDS - AODV routing algorithm.

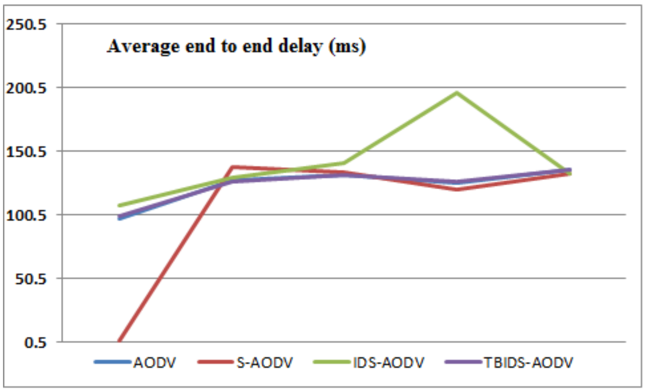

Fig. 10. Average end to end delay for network with two malicious nodes

VI. CONCLUSION & FUTURE SCOPE

Ad-hoc networks are vulnerable due to absence of infrastructure, dynamically changing net-work topology, lack of centralized monitoring and mobility. In presence of selfish node in routing, PDR is reduced and end-to-end delay is increased. For detection of the selfishness attack we have proposed IDS. IDS implantation shoes increased PDR. Furthermore trust factor is assed along with routing algorithm resulting in increased PDR values & minimum end to end delay.

In future, work must be carried out upon creating trust factor for a group of nodes with CRB data traffic. Anomaly detection can be done using machine learning concepts. Various attacks must be taken into consideration.

ACKNOWLEDGMENT

We would like to express our deep gratitude and sincere thanks to Prof. Hardik Patel, Assistant Professor (Sir Bhavshinji Polytechnic, Bhavnagar) for his continuous support and motivation.

REFERENCES

[1] “A Review Paper on Network Layer attacks in MANETs” DhruviMarsonia, Prof. Hardik Patel

[2]. “DoS Attacks in Mobile Ad-hoc Networks: A Survey”,Rutvij H. Jhaveri ,Sankita J. Patel and DeveshC.Jinwala,” 2012 Second International Conference on Advanced Computing & Communication Technologies,IEEE.

[3]. “Detecting unauthorized and compromised node in mobile ad-hoc network” ,by Nikoskomniuos

[4]. “Selfish Node Detection with modified AODV in Ad-Hoc Networks” Niyati Shah , Sharada Valiveti & Dr. K Kotecha Institute of Technology Nirma University Ahmedabad, Gujarat, India.

[5]. A Literature Review of Security Attack in Mobile Ad-hoc Networks Priyank Goyal, Bhiwani, Bhiwani, Haryana,SahilBatra ,International journal ofcomputer application (0975-8887) volume-9 No 12,November 2010,

[6]. Analysis of Different Security Attacks in MANETs on Protocol Stack A Review Gagandeep, Aashima, PawanKumar,International Journal o Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012.

[7] “INTRUSION DETECTION: A SURVEY”AleksandarLazarevic, Vipin Kumar, JaideepSrivastava Computer Science Department, University of Minnesota.

[8] “Investigating Intrusion Detection Systems in MANET and Comparing IDSs for Detecting Misbehaving Nodes”. MarjanKuchaki Rafsanjani, Ali Movaghar, and Faroukh Koroupi

[9] “SELFISH NODE DETECTION TECHNIQUES IN MANET: A REVIEW” Prof.A.M.Kurkure Ms.Bhakti Chaudhari, International Journal of Computer Science and Management Research eETECME October 2013

[10] A Review Paper on Network Layer attacks in MANETs”, Dhruvi Marsonia, Ast. Prof. Hardik Patel “to be published at International Journal for Scientific Research & Development in volume 1 issue 9 in November.