International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 - 5161

Available at http://inpressco.com/category/ijcet

Research Article

Trust based Routing in Ad-Hoc Networks

Dharmesh G. Patel[Å*], Pritesh A .Pandey[Å] and Mayur C. Patel[Å]

[Å]Computer Science & Engineering Department, MBICT, New V.V Nagar, Gujarat, India

Accepted 01 April 2014, Available online 15 April 2014, **Vol.4, No.2 (April 2014)**

Abstract

Ad Hoc Networks are absence of conventional security infrastructures, and vulnerability of nodes, vulnerability of channels and open medium of communication. Establishing trust and security in ad-hoc networks has been a long studied problem. Several methods have been proposed for evaluation and dissemination of trust in such networks, with the goal of providing secure data paths. The idea is to implement Network based intrusion detection system (NIDS) for trust based routing in Ad Hoc Networks. Computer simulation shows that compared to the original ad hoc on-demand distance vector (AODV) routing scheme,, after the creation of selfishness attack and defines the IDS system for the same. Here IDS will be created and reliable trust based routing protocol will be defined accordingly.

Keywords: *MANET, AODV, Intrusion Detection System (IDS), Selfish Attack, Routing Protocol.*

1. Introduction

A Mobile Ad hoc Network (MANET) have a set of mobile hosts to carry out various networking functions like packet of forwarding, routing and service discovery without the help of any pre deployed infrastructure. Such network may operate independently or may be connected to larger internet operating as an Ad hoc network. It is an infrastructure-less network. The interconnections between nodes are capable of changing on a continual and arbitrary basis. A MANET is formed by a group of portable devices (nodes) having almost same functionality. A MANET is dynamic in nature and they constantly move in and out of their network vicinity.

In such network nodes have various limitations due to its adhoc nature. Hence resources like power, computing ability, battery are very precious in such type of networks. So some nodes decided not to cooperate with other nodes and simply aim to save its resources to the maximum while using the network to forward its own packet. These types of node are called “Selfish Nodes”.

The main assumption of the existing systems ad hoc routing protocols is that all anticipating nodes do so in good faith and without maliciously disrupting the operation of the protocol. However, the existence of malicious entities cannot be disregarded in any system, especially in open ones like ad hoc networks.Previous systems are detected all kind of attacking node but packet dropping ratio (PDR) is increased; end-to-end delay ratio is also increased.

The Proposed System considers the AODV Protocol. Implementing Selfishness attack and check the result of packet dropping ratio and end to end delay ratio. After implement Intrusion Detection System (IDS) to detect the selfishness attack and check the same result. After implementing trust factor into the IDS AODV routing mechanism and check the result. Finally compare all the result and analysis of result. All the operation performed in to the Network Simulation Tool -2. All the work done is explained following.

2. Implementation Work

2.1 Implementation of AODV Protocol.

In this system access AODV Protocol. Some changes required on this protocol. AODV have four different messages that it uses for route discovery and route maintenance.Each AODV router is essentially a state machine that processes incoming requests from the network entity. When the network entity needs to send a message to another node, it calls upon AODV to determine the next-hop. Whenever an AODV router receives a request to send a message, it checks its routing table to see if a route exists. Each routing table entry consists of the following fields.

- Destination address
- Next hop address
- Destination sequence number
- Hop count

If a route exists, the router simply forwards the message to the next hop. Otherwise, it saves the message in a message queue, and then it initiates a route request to determine a route. The below figure 1, flow illustrates this process. Upon receipt of the routing information, it updates its routing table and sends the queued message(s). AODV nodes use four types of messages to communicate among each other.

*Corresponding author: **Dharmesh G. Patel**

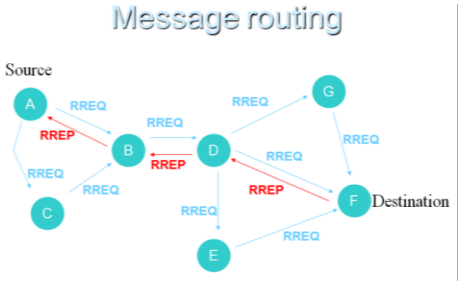

Fig.1 Flow of AODV

Route Request (RREQ) and Route Reply (RREP) messages are used for route discovery. Route Error (RERR) messages and HELLO messages are used for route maintenance.

2.2 Implementation on Selfishness Attack

Implement the finite state machine model for finding Selfish Nodes.

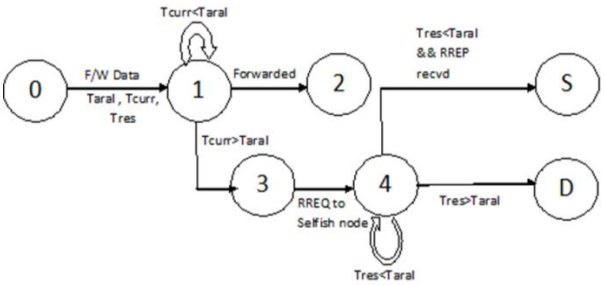

Fig.2 Finite State Machine Model

Figure 2 shows that to implement the Finite state machine model to detect the selfish node. In this model, the packet forwarding function performed in the selfish node is disabled for all packets that have a source address or a destination address different from the current selfish node. However, selfish node participates in the Route Discovery and Route Maintenance of the on-demand protocol.

2.3 Detection of Selfishness Attack using IDS Schema

Since AODV does not operate in promiscuous mode by default, some modifications had to be performed in the internal files. The fact that promiscuous mode was enabled in AODV had no impact in the overall performance of AODV and the tap method that handles the overheard packets is only utilized in the detection of the selfishness attack. Detection of this attack is triggered whenever a node forwards routing traffic to its neighboring nodes. A structure called SELFISH Node was developed to hold information necessary to monitor the neighboring nodes that are suspected for malicious behavior.

The SELFISH Node data structure holds the following information: Node Id: the IP address of the node to which the routing traffic was forwarded. Send Reply: a Boolean value that becomes true whenever the offending node replies to a RREQ packet that was forwarded to it. Pre Alarm: a Boolean value that becomes true if the node does not respond as expected to the forwarded traffic. Alarm: a Boolean value that becomes true whenever we decide that the offending node performs the dropping routing packets attack. Time: a double variable that keeps the time where the offending node was added in the data structure.

Hence, whenever a node forwards routing traffic for which a neighboring node is not the destination it adds each neighboring node to the data structure and waits to observe their behavior. Then in the tap method if it overhears that a neighboring node has replied to the forwarded RREQ, it means that it has acted appropriately and it can be removed from the monitoring list. If this is not the case and the packet was a RREP then the offending node has to forward the packet. If it fails to do so within the pre alarm time threshold time period, which was determined by experiments to be seconds, the pre alarm state becomes true. This remains in the pre alarm state for, seconds which is the alarm threshold time period. If the offending node fails to forward the routing packet within this time limit, it moves to the Alarm state. In case of an alarm the legitimate node marks this node as malicious and stops forwarding traffic to it for seconds and it also sends a RERR message to all its upstream neighbors to inform them that all the routes that include this node are not valid.

2.4 Implementation of Trust Factor

Initially set the threshold value to 100 for hop count. Link monitoring packets (Hello Packets) broadcast by every nodes. On every successful receipt of hello packets from neighbors, every node increments trust value by one in its neighbor table. Decrement trust value by 1 in neighbor table, when node moves away from its range. When a node receives RREP, it compares its neighbor's trust value with threshold value. If neighbor's trust value is greater than threshold value then node chooses that neighbor's path for reliable or trusted communication.

2.5 Performance Metrics

Following performance metrics are used for analyzing the effect of selfishness attack on Ad hoc network.

Packet Delivery Ratio (PDR) It is defined as the ratio of total number of packets that have reached the destination node to the total number of packets created at the source node. The larger this metric, the more efficient MANET will be.

$$PDR = \frac{\sum \text{Packet received by destination}}{\sum \text{Packet sent by source}} \times 100$$

End-to-end Delay: It is defined as time taken for a packet to be transmitted across network from source to destination. The metric should have lower value for the efficient network.

$$Delay = \frac{\text{Sum of delays of each CBR packet received}}{\text{Number of CBR packet received}}$$

3. Analysis of all Results

This work to implement minimum 20 nodes to maximum 60 nodes of network. Here mention below table 1, simulation parameter

Table 1 Simulation Parameters

Property	Value
No of Nodes	20,30,40,50,60
Simulation Time	500sec
Mobility Model	Random Way Point
Coverage Area	750m*7500m
Maximum Queue Length	50
Traffic Type	Constant Bit Rate(CBR)
Send Rate	10 packets/sec
Packet Size	512 bytes

Here implement all scenarios to mention in this work and check the performance. All the measurement is calculated in performance matrix.

Table 2 shows that the comparison of PDR and End-to-End Delay with different nodes in to the AODV protocol and Selfish AODV. Here shows that whennumber of nodes increase and some node is selfish then PDR is decreased compare to AODV.

Table 2 Comparison of PDR and End to End Delay in AODV and Selfish AODV

No of nodes	PDR (AODV)	PDR (SELFISH AODV)	End-to-End Delay (AODV)	End-to-End Delay (SELFISH AODV)
20	69.71 %	69.39 %	46.49 ms	48.34 ms
30	87.94 %	71.79 %	39.8 ms	33.84 ms
40	95.32 %	71.67 %	33.42 ms	38.32 ms
50	95.39 %	72.01 %	29.88 ms	27.62 ms
60	95.47 %	71.01 %	28.78 ms	26.30 ms

Figure 3 shows that when number of nodes increase and when some node is selfish then End-to-End Delay is increased compared to AODV. It is depend on that numbers of selfish nodes are generated.

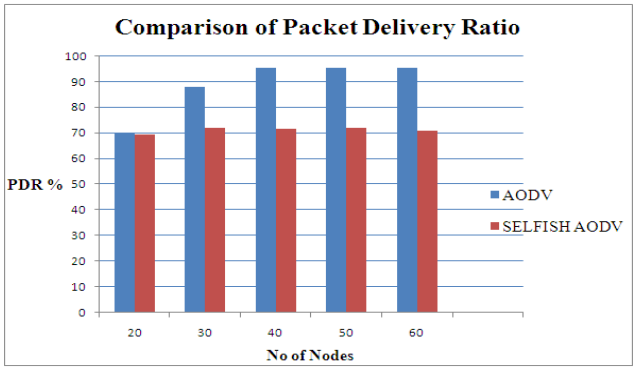

Fig.3 Packet Dropping Ration in AODV & Selfish AODV

Below table 3 shows that the comparison of Packet Delivery Ratio of three different protocol. Figure .4 shows that when number of nodes increase and when some nodes are selfish then PDR is increased compare then normal AODV and Selfish AODV. Below table .4 shows that comparison of End-to-End Delay of three different protocol and figure 5 shows that when number of nodes increase and when some nodes are selfish then End-to-End Delay is increased compare to normal AODV and decreased to Selfish AODV.

Table 3 Comparisonof PDR in AODV, SelfishAODV, IDSAODV

No of nodes	PDR (AODV)	PDR (SELFISH AODV)	PDR (IDS AODV)
20	69.71 %	69.39 %	96.53 %
30	87.94 %	71.79 %	97.19 %
40	95.32 %	71.67 %	97.35 %
50	95.39 %	72.01 %	97.50 %
60	95.47 %	71.01 %	96.76 %

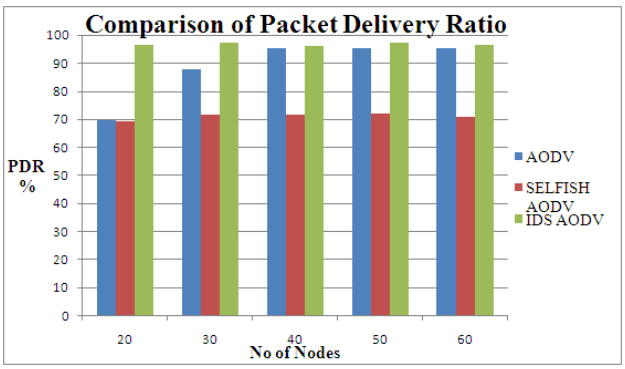

Fig.4 Comparison of PDR in AODV, SELFISHAODV, IDSAODV

Table 4 Comparison of End-to-End Delay for AODV, Selfish AODV, IDSAODV

No of nodes	End-to-End Delay (AODV)	End-to-End Delay (SELFISH AODV)	End-to-End Delay (IDS AODV)
20	46.49 ms	31.84 ms	34.41 ms
30	39.8 ms	27.88 ms	20.66 ms
40	33.42 ms	22.02 ms	28.80 ms
50	29.88 ms	27.62 ms	23.17 ms
60	28.78 ms	26.30 ms	37.77 ms

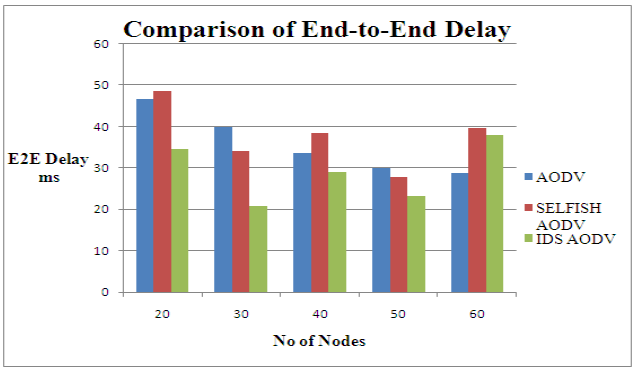

Fig.5 Comparison of E2E Delay in AODV, SELFISHAODV, IDSAODV.

Table 5 Comparison of PDR in IDSAODV and Trust AODV

No of nodes	PDR (IDS AODV)	PDR (Trust AODV)
20	96.53 %	97.68 %
30	97.19 %	97.06 %
40	97.35 %	97.05 %
50	97.50 %	97.62 %
60	96.76 %	96.86 %

This is implemented using various numbers of nodes. The comparison of different of PDR for IDS AODV and Trust AODV shows in table 5. When number of nodes increased and trust is present then PDR is increased compared to IDS AODV to show that figure 6.

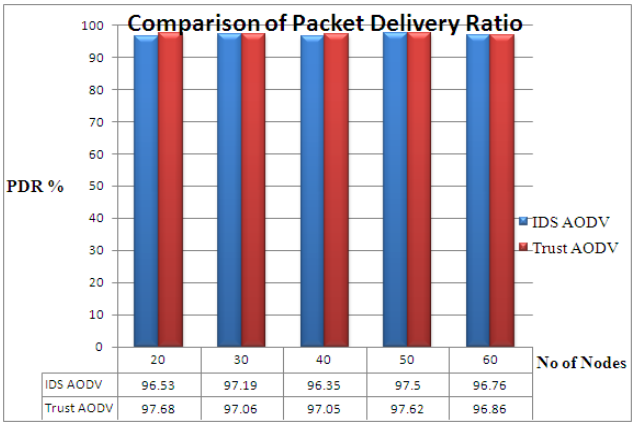

Fig.6 Comparison of PDR in IDSAODV and Trust AODV

Table 6 shows that the End-to-End Delay of IDS AODV and Trust AODV. Figure 7 shows that when number of node increased and when trust is present, and then End-to-End Delay is decreased compare to IDS AODV.

Table 6 Comparison of End-to-End Delay in IDSAODV and Trust AODV

No of nodes	End-to-End Delay (IDS AODV)	End-to-End Delay (IDS AODV)
20	34.41 ms	30.37 ms
30	20.66 ms	27.83 ms
40	28.80 ms	26.62 ms
50	23.17 ms	22.45 ms
60	37.77 ms	35.56 ms

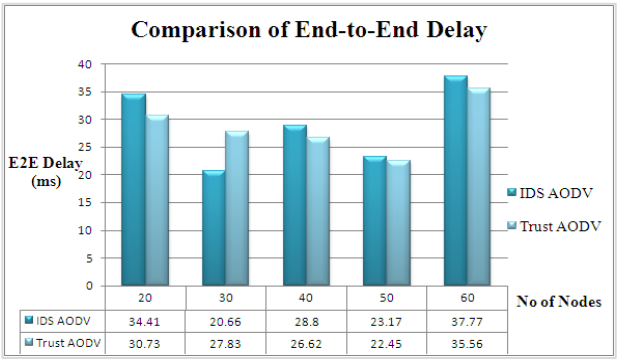

Fig.6 Comparison of End-to-End Delay in IDSAODV and Trust AODV

Conclusions

Ad-hoc networks are limited physical security, infrastructure less and changing network topology, restricted power supply, lack of centralized monitoring and mobility network. In this thesis effect of the selfishness attack in an AODV network is analyzed. For this purpose, AODV protocol is implemented and then selfish node is appended in that to analyze its effectiveness. Different scenarios are simulated where in each scenario some node is selfish while other remain normal AODV nodes. In presence of selfish node in routing, PDR is reduced and End-to-End Delay is increased. For detection of the selfishness attack proposed IDS. After implementing IDS, PDR is increased but End-to-End Delay also increased. To make system more reliable added trust factor in routing. As a result of trust based routing, PDR is increased and End-to-End Delay is decreased.

References

PinkiTanwar, Shweta,(2011), A Survey On Behaviour of Blackhole In Manets, IJRIM 1(4).

Rajiv Ranjan, Naresh Trivedi and AnoopSrivastava(2011), Mitigating of BlackholeAttack in Manets, VSRD, International Journal of Computer Science and Information Tech., Vol.1, pp-53-57.

MahaAbdelhaq, Sami Serhan,RaedAlsaqour and Anton Satria,(2011), Security Routing Mechanism for Black Hole Attack over AODV MANET Routing Protocol ,Australian Journal of Basic and Applied Sciences,vol-5,pp-1137-1145.

S.Tamilarasan and Dr.Aramudan, (2011) A Performane and Analysis of Misbehaving node in MANET using Intrusion Detection System,. IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.5.

PreetiNagrath, AshishKumar,ShikhaBhardwaj (2010), Authenticated Routing Protocol based on Reputation System For Adhoc Networks, International Journal on Computer Science and Engineering(IJCSE), Vol.2, pp- 3095-3099.

http://en.wikipedia.org/wiki/Temporallyordered_routing_algorithm

http://sites.google.com/site/securezrp/routingattacks

http://en.wikipedia.org/wiki/Wireless ad-hoc network

http://www.isi.edu/nsnam/ns/ns-tutorial/ucb-tutorial.html 5th UCB/LBNL Network Simulator (NS): June 1999 Tutorial

http://www.cs.virginia.edu/cs757/slidespdf/cs757-ns2-tutorial1.pdf

http://docs.google.com/browse/160/172.pdf+aodv 172.pdf

http://www.windowsecurity.com/articles/ids-part2-classi_cation- methods-techniques.html.