www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issues 6 June 2016, Page No. 17030-17033

Varying Number of Selfish Nodes based Simulation of AODV Routing Protocol in MANET using Reputation Based Scheme.

***Gurmeet Kaur Lamba*[1], *Prof. Ashish Chaurasia*[2],*Prof.Ajay Lala*[3]**
Department of Computer Science& Engineering
Gyan Ganga Institute of Technology and Science, Jabalpur, M.P., India
gurmeetlamba2009@gmail.com, ashishchaurasia@ggits.org, ajaylala@ggits.org

Abstract

Unlike in fixed networks the Mobile Ad Hoc networks needs more security mechanisms. Attackers may intrude into the network through the subverted nodes. The network topology is highly dynamic as nodes frequently join or leave the network, and roam in the network. In spite of its dynamic nature, mobile users request security services as they move from one place to another. The security solution should protect each node in the network and the security of the entire networks relies on the collective protection of all the nodes. The security solution should protect the network from both the inside and outside intruders into the system. In this paper we implemented AODV protocol based on reputation scheme to detect the selfish node and the evaluation will be done through performance metrics (Packet delivery ratio, Average end to end delay, Average Throughput) in Network Simulator 2.

Keywords

AODV, Selfish node , MANET, Routing Protocol.

1. Introduction

A MANET [1] is a collection of nodes where the nodes will self configure and self organize themselves forming a wireless medium without any requirement of stationary infrastructure like base station. In these networks each node will not only act as a host but also acts as a router. Due to mobility of nodes, the topology of the network is dynamic that is, it changes most of the time. Some examples where the possible use of Ad-hoc networks are in military, in emergency situation like hurricanes, earth quakes, conferences etc. One of the main issues in Ad-hoc networks is to develop a routing protocol which must be capable of handling very large number of nodes with limited bandwidth and power availability. Also they should respond quickly to the hosts that broken or newly formed in various locations. Many protocols have been proposed to solve these problems in the ad-hoc networks.

Mobile Ad-hoc Network is an autonomous group of mobile users that communicate over reasonably slow wireless links. The network topology may vary rapidly and unpredictably over time, because the nodes are mobile. The network is decentralized, where all network activity, including discovering the topology and delivering messages must be executed by the nodes themselves. Hence routing functionality will have to be incorporated into the mobile nodes.Mobile ad hoc network is a collection of independent mobile nodes that can communicate to each other via radio waves. The mobile nodes can directly communicate to those nodes that are in radio range of each other, whereas others nodes need the help of intermediate nodes to route their packets. These networks are fully distributed, and can work at any place without the aid of any infrastructure. This property makes these networks highly robust.

2. Preliminaries

2.1. Routing Protocols

Routing protocols are mainly used to deliver the data cogently and for route discovery and discovers the network topology. The basic goal of routing protocols in the ad-hoc network is to put a foundation of optimal paths between source and destination with the least overhead so that packets are delivered in a timely sequence. These protocols are essential because of the mobility of the nodes. A MANET protocol should function cogently over a wide range of networking context from small ad-hoc group to larger mobile Multihop networks. fig 1 shows the categorization of these routing protocols.

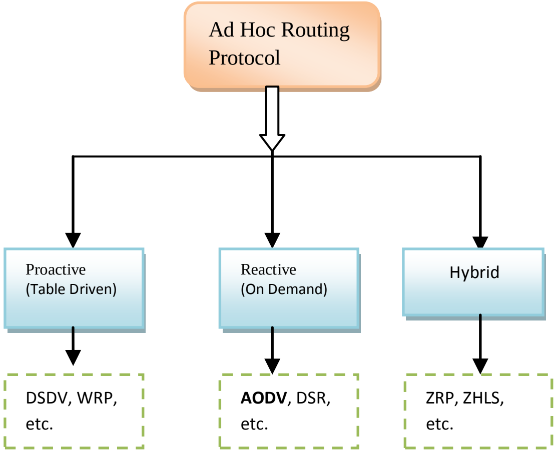

Fig 1: Hierarchy of Routing Protocols

The Routing protocols can be divided into Proactive, Reactive and Hybrid protocols, depending on the routing topology. The Proactive protocols are typically table-driven. Examples are Destination Sequence Distance Vector (DSDV). On the other hand, the Reactive protocols do not timely update the routing information. It is propagated to the nodes only when required. Example of such type includes Dynamic Source Routing (DSR) and Ad Hoc On-Demand Distance Vector (AODV). Hybrid protocols make use of both reactive and proactive approaches. Example are Zone Routing Protocol (ZRP) etc.

2.2. An overview of AODV Routing Protocols

The AODV routing protocol is an adaptation of the DSDV protocol for dynamic link conditions. Every node in this network maintains a routing table, which contains information about the route to a particular destination. Whenever a packet is to be sent by a node, it first checks with its routing table to determine whether a route to the destination is already available. If so, it uses that route to send the packets to the destination. If a route is not available or the previously entered route is inactivated, then the node initiates a route discovery process. The routing messages do not contain information about the whole route path, but only about the source and the destination. Therefore, routing messages do not have an increasing size. It uses destination sequence numbers to specify how fresh a route is.

3. Types of Attack

Mobile ad hoc network is highly vulnerable to attacks. Attacks are classified in two categories

3.1 Passive Attacks

Passive attacks are the attack that does not disrupt proper operation of network. Attackers snoop data exchanged in network without altering it. Requirement of confidentiality can be violated if an attacker is also able to interpret data gathered through snooping. Detection of these attacks is difficult since the operation of network itself does not get affected.

3.2 Active Attacks

Active attacks are the attacks that are performed by the malicious nodes that bear some energy cost in order to perform the attacks. Active attacks involve some modification of data stream or creation of false stream.

3.3 Black hole Attack

In this attack, an attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it. A malicious node sends fake routing information, claiming that it has an optimum route and causes other good no des to route data packets through the malicious one. A malicious node drops all packets that it receives instead of normally forwarding those packets. An attacker listen the requests in a flooding based protocol**.**

3.4 Selfish Nodes

Mobile ad hoc network is highly vulnerable to attacks .In this node is not serving as a relay to other nodes which are participating in the network. This malicious node which is not participating in network operations, use the network for its advantage to save its own resources such as power.

3.5 Worm hole Attack

In a wormhole attack, an attacker receives packets at one point in the network, “tunnels” them to another point in the network, and then replays them into the network from that point. Routing can be disrupted when routing control message are tunnelled. This tunnel between two colluding attacks is known as a wormhole.

4. Methodology

The proposed approach for increasing the efficiency of AODV routing protocol using trust based route selection process. Our solution is based on the concept of behavior trust; for trust level calculation. The Reputation value is calculated [10] using equation below:

$$R_{(i,j)t} = \frac{\sum_{Pkts=0}^{\infty} F_{pkts}}{\sum_{Pkts=0}^{\infty} S_{pkts}}$$

Where Reputation of i and j at time t is the reputation value calculated by monitoring the neighbor j directly at time t and Fpkts is the number of packets forwarded by node j and Spkts is the number of packets sent by node j.

As a result, a node with the highest reputation will get the chance to participate in communication fixed time period cache will get clear, this process refresh the reputation value of each node so that every node will get chance to participate in the communication it will increase performance and efficiency of the network .

4.1 Algorithm

In reputation based monitoring module continuously monitors node behaviour and assign a reputation values to nodes based on their packet forwarding activity in the routing table.

Step1. Each node maintains reputation values of its neighbours and other nodes that have had a transaction with it.

Step 2. Packet forwarding between two nodes depend on the mobility factor. A node observes a packet forwarded by neighbours Q. To calculates the reputation value R (P, Q) equal to the ratio of packet delivered by Q to the total number of packets sent by node P.

Step3. A node P can obtain opinion about Q by requesting reputation value from its neighbours.

Step4. As a result of node with reputation value is greater than threshold value can participate in route discovery process.

5. Simulation Environment

We have implemented selfish node attack in a ns-2 simulator. In our scenario we increase the number of selfish nodes. The simulation is done using ns-2, to examine the performance of the network by varying the number of selfish nodes. The metrics used to evaluate the performance are given below.

Average Throughput: The total number of the data packets generated by each source, counted by k bit/s.
Jitter is as a variation in the delay of received packets.

6. Experimental Setup and Analysis

This paper is applied to ns-2 to validate the detection and isolation efficiency of the proposed method against selfish nodes. We have analyzed the different values while coming across the Ad Hoc on Demand Distance Vector (AODV) Routing Protocol. The major parameters of our experiment are listed in Table1.

Table-1. Simulation Parameters

S.No.	Parameters	Value
1.	Simulator	ns-2
2.	Simulation time	Varies with nodes
3.	No. of nodes	20
4.	No. of Selfish nodes	2,3,4,5
5.	Speed	Random
6.	Traffic type	UDP and TCP
7.	Topology	Network
8.	Routing Protocol	AODV

7. Related Work

Sohail Abbas et al. survey and categorize reputation based schemes according to their passive and active acknowledgment monitoring techniques in multi hop networks such as mobile ad hoc networks selfish or misbehaving nodes can disrupt the whole network and severely degrade network performance [2].

Rajesh Sharma et al. They had discussed a solution on the basis of reputation method to solve routing issues raised by misbehaving nodes [1].

Renu Dalal et al. provide the different ways to achieve trust in mobile Ad-hoc Network. Providing the safe communication between mobile nodes, reorganization the position of nodes, reducing overhead, handling misbehaviour and location updates are such a difficult issues in ad-hoc network so providing trust schemes is an important in this network [3].Santhosh Krishna B. Vet et al. The author focus on single and multiple black hole attacks. The implementations o f black hole comprises active routing misbehaviour and forwarding misbehaviour & design and build our prototype over DSR and test it in Network simulator 2 in the presence of variable active black hole attacks in highly mobile and sparse networks [5].

Isaac Woungang et al. provide a novel scheme for Detecting Black hole Attacks in MANETs is introduced. The BDA-DSR protocol detects and avoids the black hole problem before the actual routing mechanism is started by using fake route request packets to catch the malicious nodes [6].

Poonam K Gar et al. They had discussed and proposed a new algorithm to find route to the destination as a weighted average of the trust value of the nodes in the route, with respect to its behavior observed by its neighboring nodes and the number of nodes in the route is calculated [9].

Sangheetaa Sukumran et al. proposed a solution for on-demand routing protocol using reputation mechanism. This approach calculates the reputation values of the nodes using simple formula. Any node is supposed to maintain a good reputation value in order to receive network services. When a node tries to identify a route, its route request will be forwarded by the neighboring nodes only if it reputation value is higher than the threshold value i.e. this node must be in the white list. Thus a node needs to maintain a good reputation value in order to enjoy network services. A misbehaving node which is isolated has no chance of rejoining the network until the entire network is reformed.

Santosh Kumar et al. conluded that DSR is a generally used routing protocol for mobile ad hoc networks but has very low packet delivery rates and poor performance in lightly loaded networks with high node mobility. In this paper they presented that how the performance will be improved for the reliable data transmission in MANET by applying the reputation based scheme on the DSR protocol with detection of selfish node. Reputation based DSR is able to provide reliable communication. The reputation DSR selects the best route based on the reputation value. But, normal DSR collapses when number of selfish nodes is increased. The results proved that the detection of selfish node in DSR based MANET using reputation based scheme provides better performance in route discovery in mobile ad hoc network [10].

8. Result & Discussion

The result shows the impact of Selfish node attack on throughput and average jitter. The reputation based based scheme shows better result than existing AODV routing protocol.

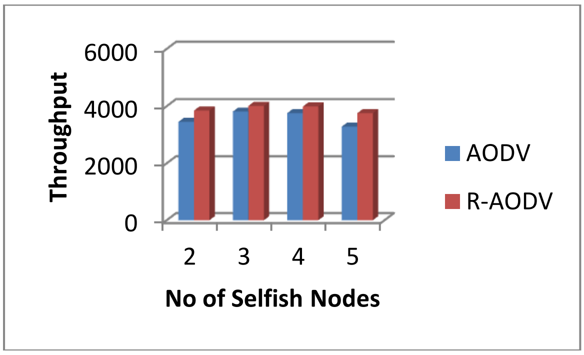

Figure 8.1 . Throughput

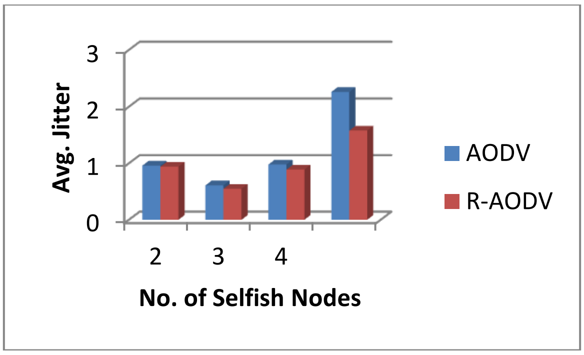

Figure 8.2. Average Jitter

9. Conclusion and Future Work

With development in computing environments, the services based on ad hoc networks have been increased as a result different types of attacks may occur. In this paper, we have analyzed the throughputs which increases with increase in no of selfish nodes. The Reputation based AODV shows better result than existing AODV. The Average jitter also shows better result than existing AODV. In our study, we used the AODV routing protocol. But the other routing protocols could be simulated as well. All routing protocols are expected to present different results. Therefore, the best routing protocol for minimizing the selfish node attack may be determined.

References

[1] Rajesh Sharma and Seema Sabharwal “Dynamic Source Routing Protocol (DSR)”, IJARCSSE, Volume 3, Issue 7,July 2013 pp. 239-241.

[2] Sohail Abbas, Madjid Merabti, and David Llewellyn-Jones “A Survey of Reputation Based Schemes for MANET” 2010.

[3] Renu Dalal1, Manju Khari and Yudhvir Singh “Different Ways to Achieve Trust in MANET” International Journal on Ad Hoc Networking Systems (IJANS) Vol. 2, No. 2, April 2012.

[4] G. Rajkumar, R. Kasiram and D. Parthiban “Optimized QoS Metrics and Performance Comparison of DSR and AODV Routing Protocols”, IEEE-International Conference On Advances In Engineering, Science and Management (ICAESM -2012) March 30, 31, 2012

[5] Santhosh Krishna B.V, Mrs. Vallikannu A.L “Detecting Malicious Nodes for Secure Routing in MANETS Using Reputation Based Mechanism” International Journal of Scientific & Engineering Research, Volume 1, Issue 3, December-2010.

[6] Isaac Woungang, Sanjay Kumar Dhurandher, Rajender Dheeraj Peddi and Mohammad S. Obaidat, Fellow of IEEE and “Detecting Black hole Attacks on DSR-based Mobile Ad Hoc Networks”, 2012.

[7] Ramasamy Mariappan Sangameswaran Mohan “Re-pro Routing Protocol with Trust based Security for Broadcasting in Mobile Ad hoc Network” IEEE 2011.

[8] Sangheethaa Sukumaran, Venkatesh. J, Arunkorath “A Survey of Methods to mitigate Selfishness in Mobile Ad hoc Networks” International Journal of Information and Communication Technology Research Volume 1 No. 2, June 2011.

[9] Poonam, K. Garg, M. Misra “Trust Based Multi Path DSR Protocol”, International Conference on Availability,Reliability and Security IEEE 2010.

[10] Santosh Kumar, Suveg Moudgil, " Detection Of Selfish Node In Dsr Based Manet Using Reputation Based Scheme", International Journal of Research in IT, Management and Engineering, Volume 4, Issue 7, July2014.