INTERNATIONAL JOURNAL OF SCIENTIFIC & ENGINEERING RESEARCH, VOLUME 4, ISSUE 12, DECEMBER-2013
ISSN 2229-5518

Secure and Shortest Path by Modifying RREP Packet of AODV Protocol

Harjot kaur Buttar, Shakti Raj Chopra

Abstract— The mobile Ad hoc networks are the self configuring type of network in which the mobile nodes can move freely in the environment, even when they are communicating with the other mobile nodes. Due the mobility in nature of mobile nodes the problem of link failure will cause. When the route is established between the mobile nodes and intermediate mobile nodes when change its path. The route will be broken and packet loss may cause .Due to this problem the efficiency of MANET will be reduced. In this paper, we are proposing the new technique in which we are enhancing the traditional AODV protocol, to cope up with the problem of link failure.

Index Terms— Mobile nodes, AODV, link Failure, Signal strength.

1 INTRODUCTION

Mobile Ad-hoc Networks are future wireless networks consisting entirely of mobile nodes that communicate on-the-move without base stations. Nodes in these networks will both generate user and application traffic and carry out network control and routing protocols. Rapidly changing connectivity, network partitions, higher error rates, collision interference, and bandwidth and power constraints together pose new problems in network control particularly in the design of higher level protocols such as routing and in implementing applications with Quality of Service requirements [1]. The routers are free to move randomly and organize themselves arbitrarily thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet. Sensor nodes consist of sensing, data processing, and communication components and typically form ad hoc networks. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. MANETs are a kind of wireless ad-hoc networks that usually has a routable networking environment on top of a Link Layer ad hoc network. Even it is very useful in the today's world but it has some limitations such as security issues and performance, especially due to mobility of nodes[2]. The routing protocols are broadly classified as proactive and reactive routing protocols. The reactive routing protocols are the protocols which establish link between source and destination when required .On the other hand the proactive routing are protocols which establish link between source and destination on the basis of predefined routing tables which are stored on the mobile nodes. The simulation result shows that the reactive protocols are more efficient than reactive protocols for mobile ad hoc networks. In our work, we are using AODV reactive type of routing protocol.

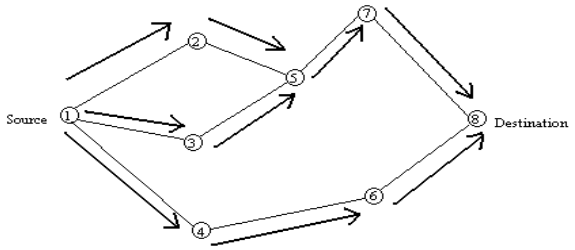
The aim of this paper is to propose an algorithm to find a secure shortest path against wormhole attack. Existing algorithms are mainly concentrated on detecting the malicious node but they are hardware specific like directional antennas and synchronized clocks. But the proposed algorithm is both software and hardware specific. RTOS is included to make the ad hoc network a real time application.

1.1 AODV PROTOCOL

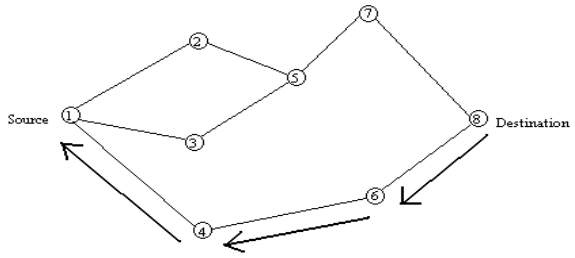
A. Routing Mechanism

The Ad hoc On Demand Distance Vector (AODV) routing algorithm is a routing protocol designed for ad hoc mobile networks. AODV is capable of both unicast and multicast routing. It is an on demand algorithm, meaning that it builds routes between nodes only as desired by source nodes. It maintains these routes as long as they are needed by the sources. Additionally, AODV forms trees which connect multicast group members. The trees are composed of the group members and the nodes needed to connect the members. To find a path to the destination, the source broadcasts a route request packet. The neighbors in turn broadcast the packet to their neighbors till it reaches an intermediate node that has recent route information about the destination or till it reaches the destination [3]. A node discards a route request packet that it has already seen. The route request packet uses sequence numbers to ensure that the routes are loop free and to make sure that if the intermediate nodes reply to route requests, they reply with the latest information only. When a node forwards a route request packet to its neighbors, it also records in its tables the node from which the first copy of the request came.

INTERNATIONAL JOURNAL OF SCIENTIFIC & ENGINEERING RESEARCH, VOLUME 4, ISSUE 12, DECEMBER-2013
ISSN 2229-5518



(a) Propogation of Route Request (RREQ) Packet



(b) Path taken by the Route Reply (RREP) Packet

This information is used to construct the reverse path for the route reply packet. AODV uses only symmetric links because the route reply packet follows the reverse path of route request packet. As the route reply packet traverses back to the source, the nodes along the path enter the forward route into their tables. If the source moves then it can reinitiate route discovery to the destination [4]. If one of the intermediate nodes move, then their neighbors realizes the link failure and sends a link failure notification to its upstream neighbors and so on till it reaches the source upon which the source can reinitiate route discovery if needed.

There are 2 control messages that help to discover the path between the source and the destination, RREQ (Route Request) and RREP(Route Reply). The routing tables include the following parameters.

TABLE I.RREQ Message

Source Address	Request ID	Source sequence number	Destination address	Destination Seq No.	Hop count

TABLE II. RREP Message

Source Address	Destination Address	Destination Sequence Number	Hop Count	Lifetime

B. Performance Metrics

1) Throughput
It is the measure of the number of packets or data successfully transmitted to their final destination via a communication link per unit time [5]. It is measured in bits per second (bit/s or bps).

2) Packet Delivery Ratio
It can be defined as the ratio of the data packets delivered to the destinations to those generated by the sources. Sometimes it is known as Packet Delivery Ratio (PDR) [5], [6]. Mathematically, it can be expressed as:

$$P = \frac{1}{c}\sum_{f=1}^{e}\frac{R_f}{N_f}$$

Where P is the fraction of successfully delivered packets, C is the total number of flow or connections, f is the unique flow id serving as index, R_f is the count of packet received from flow f and N_f is the count of packets transmitted to f.

3) End to End Delay
It can be defined as the average time between packets sent and received. It can be defined as:

$$D = \frac{1}{N}\sum_{i=1}^{s}(r_i - s_i)$$

Where N is the number of successfully received packets, I is unique packet identifier, r_i is time at which a packet with unique id i is received, s_i is time at which a packet with unique id i is sent and D is measured in ms. [7].

2 PROPOSED TECHNIQUE

In our work, we are proposing the made enhancement in the traditional AODV protocol. In traditional protocol the route from the source to destination is selected on the basis of hop counts and sequence number. The route which has minimum number of hop counts and highest sequence number will be selected as the best route. The sequence numbers tells us the freshness of the route. In our work we modify the RREP packet header. When the intermediate nodes reply to source node with the route reply packet, they also send their signal strength corresponding to other nodes. The source calculate the average signals strength on each route and select the best route which is having higher average signal strength.

INTERNATIONAL JOURNAL OF SCIENTIFIC & ENGINEERING RESEARCH, VOLUME 4, ISSUE 12, DECEMBER-2013
ISSN 2229-5518

Condition: Movement of intermediate nodes causes link failure, thereby dropping network throughput, enhancing delay, and reduced packet delivery ratio or data loss

Solution: The network is deployed with the finite number of mobile nodes. The mobiles nodes have the capability to move from one place to other. The ad hoc network is the self configuring type of network, mobiles can leave or join the network when they want. In such type of network many type of inside and outside attacks and link failure are possible which degrade the performance of the system. To prevent degradation and improve performance, enhancement in AODV is needed. Network is deployed in same manner as AODV.

TABLE III.

Source Address	Destination address	Destination sequence number	Signal Strength	Hop count	lifetime

RREQ messages are sending during data transfer. As a response RREP messages are sending but difference is that here message are encapsulate with the header which has the destination address and find out signal strength. Each node checks the vicinity of adjacent nodes. Source nodes calculate average signal strength which lies between1 to 10. Nodes which have maximum signal strength are considered in final path. This helps to improve the performance of the network and prevent from packet loss problem.

3 Simulations and Results

The experiment was conducted on 1000m*1000m square of simulation field. A novel technique including a signal strength factor into the RREP packet of AODV protocol was designed and the network performance metrics was obtained using network simulator II, NS2.

TABLE IV. Simulation Parameters

PARAMETER	Value
No. of Nodes	23
Pause time	0.02s
Simulation Time	5s
Traffic Type	CBR
Data payload	1000bytes/packet

Improved results for all the three parameters i.e. end to end delay, network throughput and packet delivery ratio were obtained. Following graphs show how the network was improved with a little change into the existing protocol.

1. End to End Delay

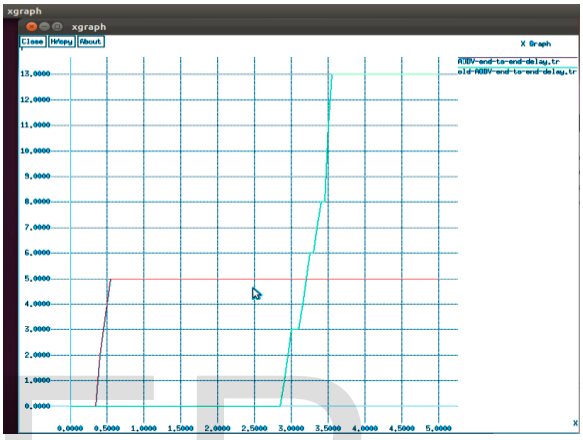


Fig1: Network Delay

From fig1, we could see that the basic AODV induces a larger end to end delay, most of it introduced due to initiation time, as it sends data only after it has discovered the path to the destination. With the novel AODV the delay in packet delivery is much reduced.

2. Network Throughput

Though AODV is considered to be the best protocol in terms of achieving throughput, as only the first arriving RREQs are answered, and further if RREQ from same node arrives, it isnt answered, therefore it leads to lesser number of route replies, thereby reducing MAC load. Then also improvement with a little change may be obtained. From fig.2, it could be observed that the transmision of packets with respect to time(in ms), was improved in the novel AODV, than the basic one.

3. Packet Delivery Ratio

The basic AODV, as a reactive protocol, drops a considerable number of packets during the route discovery phase. Fig.3 shows that, introduction of signal strength field into the RREP packet, leads to the lesser chances of link failure, thereby reducing the need of route discovery.

INTERNATIONAL JOURNAL OF SCIENTIFIC & ENGINEERING RESEARCH, VOLUME 4, ISSUE 12, DECEMBER-2013
ISSN 2229-5518

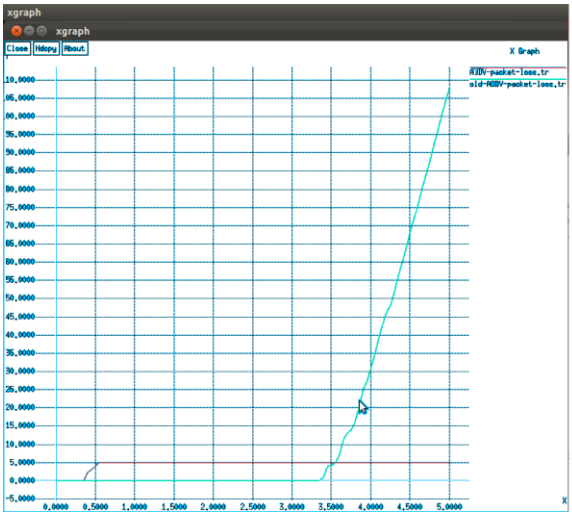


Fig3: Packet Delivery Ratio

4. CONCLUSION

In this paper, we conclude that the network when mobile nodes change their locations the problem of link failure will be there .To overcome this problem new technique is proposed which is based on the signal strength.

REFERENCES

[1] "A QoS architecture for MANETs supporting real-time peer-to-peer multimedia applications", Carlos T. Calafate, Juan-Carlos Cano, Pietro Manzoni, and Manuel P. Malumbres, Polytechnic University of Valencia, Spain, 2004

[2] "Enhancement in AODV protocol to isolate link failure problem in Mobile Ad hoc Network", Deepak kumar, Sapanjot kaur, IJPTT, 2013

[3] "Queue Management In Mobile Adhoc Networks" K Dinesh Kumar, Ramya & M.Roberts, 2010

[4] "Improved AODV Protocol For Solving Link Failure In MANET", Asha Ambhaikar, H.R. Sharma, V. K. Mohabey, IJSER, 2012

[5] "Improving AODV Protocol against Blackhole Attacks", Nital Mistry, Devesh C Jinwala, Member, IAENG and Mukesh Zaveri , Proc. IMECS'10, vol. 2, March 2010

[6] "Performance analysis of
AODV, DSR & TORA Routing Protocols", Anuj K. Gupta and Dr. Anil K. Verma, IACSIT International Journal of Engineering and Technology, vol. 2, No.2, April 2010.

[7] "Comparative Analysis the Performance of AODV,DSDV and DSR Routing Protocols in Wireless Sensor Network" Julia Rahman,* Md. Al Mehedi Hasan, Md. Khaled Ben Islam, IEEE 2012