A Multiparametric Reliable AODV Protocol using Alternate Routing in MANET's using NS-2

Sonal Beniwal
Department of Computer Science and Engineering.
BPSMV, Khanpur Kalan
Sonepat,India

Pinki
Department of Computer Science and Engineering.
BPSMV, Khanpur Kalan,
Sonepat,India

Rashmi Jatain
Department of Computer Science and Engineering
UIET,MDU
Rohtak,India

Abstract: In this paper, we design and formulate a trust-based routing protocol for secure transactions, such as military and disaster relief operations, banking in mobile ad hoc networks (MANETs). The proposed approach is showing the idea of a trust model in the network layer of MANET.AODV is ad hoc on demand distance vector, this protocol starts the route specially when some node claims to send data. In AODV whenever a link breaks an error message is sent indicating the link and packet sending is dropped. In our proposed scheme a packet is sent through alternative path. In this approach a trust node is made with neighbors. Simulation results shows that proposed scheme has less packet loss and packet ratio delivered is more.

Keywords:*MANET,Ad hoc, AODV, Routing Algorithm, Reverse Route*

1. INTRODUCTION

A mobile ad hoc network (MANET)is a kind of wireless network without centralized administration or fixed network infrastructure in which nodes communicate over relatively bandwidth constrained wireless links and perform routing discovery and routing maintenance in a self-organized way. The topology of the MANET may change uncertainly and rapidly due to the high mobility of the independent mobile nodes, and because of the network decentralization, each node in the MANET will act as a router to discover the topology. Nowadays the MANET enables many promising applications in the areas of emergency operations, disaster relief efforts. The Mobile Ad hoc network is one of most commonly used wireless network. As the number of user in this network increases it also suffer from most of the network problems like congestion, packet loss, intrusion etc. In case of multicast such kind of problem is quite common. AODV is the most efficient on demand protocol used in Mobile Adhoc network. This protocol support efficient transmission in Multicast and broadcast communication. It create a loop free efficient routing. But because of some attack or the congestion it provide higher loss. There is the requirement of some improvement over the existing AODV protocol to provide the secure and efficient communication over the network.

The Ad-hoc On-Demand Distance Vector (AODV) routing protocol is designed for use in ad-hoc mobile networks. AODV is a reactive protocol: the routes are created only when they are needed. It uses traditional routing tables, one entry per destination, and sequence numbers to determine whether routing information is up-to-date and to prevent routing loops. An important feature of AODV is the maintenance of time-based states in each node: a routing entry not recently used is expired. In case of a route is broken the neighbours can be notified. Route discovery is based on query and reply cycles, and route information is stored in all intermediate nodes along the route in the form of route table entries. The following control packets are used: routing request message (RREQ) is broadcasted by a node requiring a route to another node, routing reply message (RREP) is unicaste back to the source of RREQ, and route error message (RERR) is sent to notify other nodes of the loss of the link. HELLO messages are used for detecting and monitoring links to neighbors.

AODV is a relative of the Bellmann-Ford distant vector algorithm, but is adapted to work in a mobile environment. AODV determines a route to a destination only when a node wants to send a packet to that destination. Routes are maintained as long as they are needed by the source. Sequence numbers ensure the freshness of routes and guarantee the loop-free routing.

The objective of this paper is route maintenance using alternative path at each node. Study and analysis of different Routing Protocol in Mobile Network. Implement the TAODV protocol to identify reliable route based on trust level analysis. Implementation of proposed Protocol in NS2 environment Analysis of proposed system using XGraph in terms of throughput and packet loss.[2,6]

The remaining paper is described as section2 describes the work related to AODV .The proposed scheme is described in section3.Section4 represents the experimental results.Section5 represents the conclusion and then references.

2. RELATED WORK

Debdutta Barman Roy propose a new Intrusion Detection System (IDS) based on Mobile Agents. The approach uses a set of Mobile Agent (MA) that can move from one node to another node within a network. This as a whole reduces network bandwidth consumption by moving the computation for data analysis to the location of the intrusion. Besides, it has been established that the proposed method also decreases the computation overhead in each node in the network. [1]

Shailender Gupta defined a work on selfish node detection. A selfish node is one that tries to utilize the network resources for its own profit but is reluctant to spend its own for others. If such behaviour prevails among large number of the nodes in the network, it may eventually lead to disruption of network. This paper studies the impact of selfish nodes concentration on the quality of service in MANETs. [2]

Md. Amir Khusru Akhtar presented a mathematical model to detect the selfish node. In this paper Author are presenting the mathematical model to detect selfish nodes using the probability density function. The proposed model works with existing routing protocol and the nodes that are suspected of having the selfishness are given a Selfishness test. This model formulates this problem with the help of prior probability and continuous Bayes' theorem.[3]

. Li Zhao performed a work to detect misbehaviour on data and mitigate adverse effects, Author propose and evaluate a Multipath Routing Single path transmission (MARS) scheme. The MARS combines multipath routing, single path data transmission, and end-to-end feedback mechanism together to provide more comprehensive protection against misbehaviour from individual or cooperating misbehaving nodes. [5]

Zougagh Hicham performed a comparative study of intrusion detection in adhoc nework. In recent years, the use of mobile ad hoc network (MANETs) has been widespread in many applications. Due to its deployment nature, MANETs are more vulnerable to malicious attack. The absolute security in the mobile ad hoc network is very hard to achieve because of its fundamental characteristics, such as dynamic topology, open medium, absence of infrastructure, limited power and limited bandwidth. In this article Author classify the architecture for IDS that have so far been introduced for MANETs, and then existing intrusion detection techniques in MANETs presented and compared. Author then provide some directions for future researches. [6,7,8]

Michael Wayne Probus performed a work on selfish node isolation. This thesis will focus on the topic of Selfish Nodes within a Mobile Ad-Hoc Networks (MANET), specifically sensor networks due to their lower power and bandwidth. The approach used is a reputation based algorithm to isolate the selfish nodes from communication by using past history to determine how reliable the node is. The reputation of each node is determined by their behavior within the network. As a node continuously acts selfishly, their reputation is decreased, until finally meeting the minimum threshold; therefore they are determined to be malicious. [11,12]

3. PROPOSED WORK

In this chapter basic AODV protocol is defined along with its properties and the problem. The AODV protocol itself gives the concept of network reconfiguration to provide the network stability. The AODV protocol is capable to identify the broken link over the network. As the broken link is identified, it find the compromising path to perform the rerouting for network communication .In this chapter the proposed model is also defined with TAODV procol.In our proposed work we are providing an early decision about the node stability:

1.Here each node will inform the node regarding the broken link earlier because of this the route can be changed earlier.

2.A timeout based flooding will be performed by each node periodically. If some node is not responding for n number of trails then the decision will be taken that node is a bad node.

3.The bad node will be marked as the inactive node in routing table and while communicating the earlier decision will be taken regarding this.

4.As the bad node is identified an agent will be set as neighbour to the bad node. The agent will keep watch on this bad link or the node.

5.As the bad link get repaired the agent will inform the node to perform communication from the initial path. [9,10]

In this present work we have improved the communication by representing the node as an intelligent node. In this present work the first time communication performed by the network is same as of existing AODV.It means it will detect the attack or the broken link in same way as of actual AODV. But once the attack is detected it will enable the immediate previous node to attack as the manager node that will track the attack position or the attack node periodically. Till there is attack in the network it will not allow the communication on that route. It means it will identify the preventive path to communicate from the alternate path or the node. As that manager node identify that the broken link or attack is repaired dynamically, it will start the communication from this previous path.

The proposed system will give the following benefits.

1.It not only dynamically reconfigure the network as the attack found, it will also identify the dynamic repairing of the network. If the network is repaired dynamically it will move back to the previous effective path.

2.The nodes are taken as intelligent node and converted to manager node as the attack found on their immediate communication path or the node.

4.SIMULATION AND RESULTS

Hardware Used :

Processor	: Pentium 5
Processor Speed	: 1.5 GHZ
Memory(RAM)	: 256 MB
Hard disk	: 40 GB

Software Used :

Operating system	: Linux 8.0
Language	: OTcl
Software	: NS 2.35

4.1.1 NS2 Overview

NS is a discrete event network simulator where the timing of events is maintained by a scheduler and able to simulate various types of network such as LAN and WPAN according to the programming scripts written by the user. It provides substantial support for simulation of TCP, routing and multicast protocols over wired and wireless networks. It consists of two simulation tools. The network simulator (ns) contains all commonly used IP protocols. The network animator (NAM) is graphical software which is used to visualize the simulations. NS2 fully simulates a layered network from the physical radio transmission channel to high-level applications.

NS2 is an object-oriented simulator written in C++ and OTcl (an object oriented extension of Tcl). The simulator supports a class hierarchy in C++ and a similar class hierarchy within the OTcl interpreter. There is a one-to-one correspondence between a class in the interpreted hierarchy and one in the compile hierarchy. The reason to use two different programming languages is that OTcl is suitable for the programs and configurations that demand frequent and fast change while C++ is suitable for the programs that have high demand in speed. NS2 is highly extensible. It not only supports most commonly used IP protocols but also allows the users to extend or implement their own protocols. The latest NS2 version supports the four ad hoc routing protocols, including DSR. It also provides powerful trace functionalities, which are very important in our project since information need to be logged for analysis. The full source code of NS2 can be downloaded and compiled for multiple platforms such as UNIX, Windows etc.

4.1.2. Performance Metrics

a) **Packet Lost** : The total no. of packets dropped by the node when there exist no route to destination.[13 ,14, 15]

b) **Packet Delay** : It is the average time a Packet takes to reach from source to destination.

c) **Bytes Transmitted** : The rate of successfully transmitted Bytes in the netwok during simulation.

4.1.3. Network Parameters

[1] Area	**[2] 784x569**
[3] Routing Protocol	**[4] AODV**
[5] MAC protocol	**[6] 802.11**
[7] Number of Nodes	**[8] 26**
[9] Queue Length	**[10] 50**
[11] Antenna	**[12] OmniAntenna**

4.2. Analysis Results:

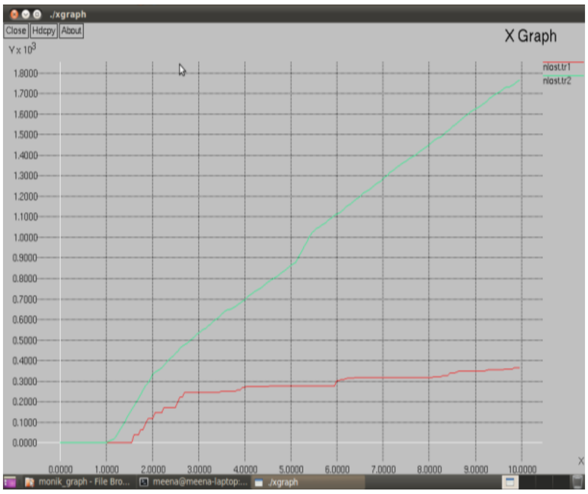

Figure 4.1:Packet Lost (Existing Vs Proposed Approach)

Here figure 4.1 is showing the comparative analysis of packet lost over the network. Here x axis represents the time and y axis represents the packet transmitted. As we can see after implementing the proposed approach the packet loss over the network is decreased.

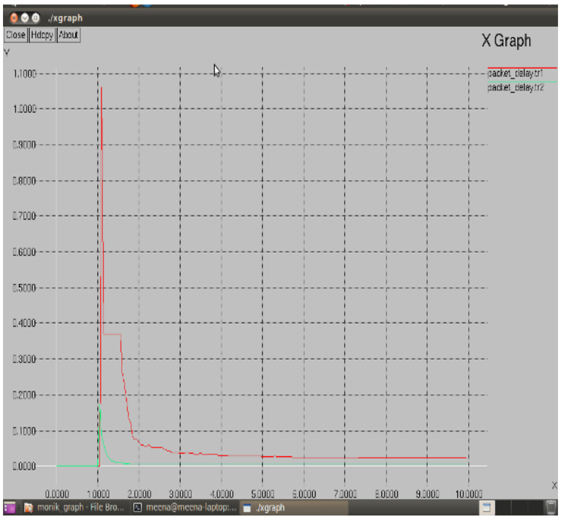

Figure 4.2 : Packet Delay (Existing Vs Proposed Approach)

Here figure 4.2 is showing the comparative analysis of Packet Delay over the network.Here x axis represents the time and y axis represents the Packet Delay of communication. As we can see after implementing the proposed approach the Packet Delay over the network is decreased.

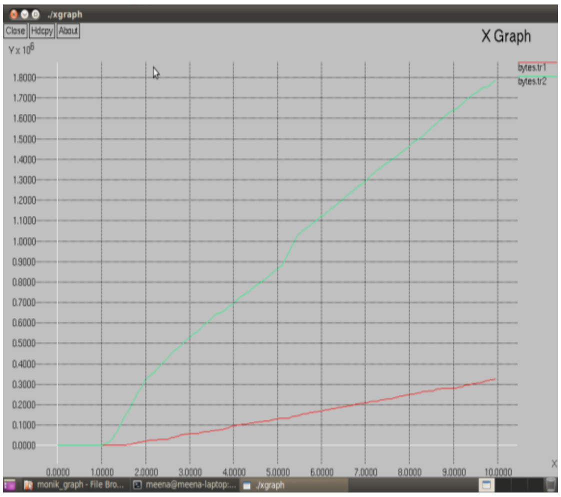

Figure 4.3 :Bytes transmitted (Existing Vs Proposed Approach)

Here figure 4.3 is showing the comparative analysis of bytes transmitted over the network. Here x axis represents the time and y axis represents the btes transmitted. As we can see after implementing the proposed approach the bytes transmitted over the network is increased.

5. CONCLUSION

In this present work we have shown the improvement over AODV protocol to ensure the stability with less delay. In this work we have provided the stability in case of broken link reconfiguration. It means as the broken link is detected the routing path is modified by the AODV protocol. But it does not define to on the previous path back when the link is been repaired. In this present work we have included the concept of manager node. The manager node is maintained just previous to the broken link node. The broken link node will keep a watch on the link and check for its reconfiguration after a short delay. As the link is repaired it will again change the communication path to the previous routing path. The presented work has provided the better stability within efficient time and without using any extra rersources.

6. FUTURE SCOPE

In this present work we deal with the AODV protocol, but in future we can use some other protocol to improve it respective to the network stability. In this work we deal basically with unicasting and the improvement can be done to check it for multicasting. We can also try the same approach on different scenarios also.

7.REFERENCES

[1] Michael Gerharz," A Practical View on Quality-of-Service Support in Wireless Ad Hoc Networks",proceedings of the 3rd IEEE Workshop onApplications 2003.

[2] Youngki Hwang," An Adaptive QoS Routing Protocolwith Dispersity for Ad-hoc Networks", Proceedings of the 36th Hawaii International Conference on System Sciences – 2003.

[3] Robert Akl," NonuniformGrid-Based Coordinated Routing in Wireless Sensor Networks", Hindawi Publishing Corporation Journal of Sensors, Hindawi Publishing Corporation Journal of Sensors Volume 2009, Article ID 491349, 11 pages.

[4] Rajendiran M.," An Improved Routing Algorithm to Enhance Energy Efficiency in Multicast Ad Hoc Networks", European Journal of Scientific Research ISSN 1450-21, 2012.

[5] Sridhar K N," Stability and Hop-Count based Approach for Route Computation in MANET", Computer Communications and Networks, 2005. ICCCN, 17-19 Oct. 2005.

[6] Sima," SIMULATION STUDY OF AODV&DSR", International Journal of Computing and Business Research ISSN (Online) : 2229-6166 Volume 2 Issue 3 September 2011.

[7] Jyoti Jain," OVERVIEW AND CHALLENGES OF ROUTING PROTOCOL AND MAC LAYER IN MOBILE AD-HOC NETWORK", journal of Theoretical and Applied Information Technology. © 2005 - 2009 JATIT.

[8] Aditya Kumar Mishra,' Power-Aware Routing in Mobile Ad Hoc Networks",Proceedings of the 4th annual ACM/IEEE international conference on MobileComputing and Networking, October 1998.

[9] Anuradha Banerjee," Fuzzy-Controlled Adaptive and Intelligent Route (FAIR) Selection in Ad Hoc Networks", European Journal of Scientific Research. ISSN 1450-216X Vol.45 No.3 (2010), pp.367-382.

[10] Hasnaa Moustafa," Source Routing-based Multicast Protocol for Mobile Ad hoc Networks", 10th International Conference on Telecommunication Systems Modeling and Analysis (ICTSM-10), October 2002.

[11] Michael Gerharz," Link Stability in Mobile Wireless Ad Hoc Networks", Proc. of the 27th IEEE Conference on Local Computer Networks (LCN), pp. 30-39, 2002

[12] Arash Dana," A Reliable routing algorithm for Mobile Adhoc Networks based on fuzzy logic", International Journal of Computer Science Issues **Year:** 2011 **Vol:** 8 **Issue:** 3 , 128-133

[13] C. Venkatesh," DYNAMIC SOURCE ROUTING PROTOCOL USING FUZZY LOGIC CONCEPTS FOR AD HOC NETWORKS", In. Transactions of Academic Open Internet Journal, Vol.15,pp 1-14. 2008[14] V. Bharathi," A Performance Enhancement of an Optimized Power Reactive Routing based on AODV Protocol for Mobile AD-HOC Network", ©gopalax -International Journal of Technology And Engineering System(IJTES) Jan – March 2011- Vol2 .No1.

[15] Panagiotis," Path Set Selection in Mobile Ad Hoc Networks", ACM Mobihoc 2002, Lausanne, Switzerland, June 2002.