Classify and Enhance Security Level for using Congestion Control Capability of AODV and xAOMDV Protocol in MANET

Shanti Rathore
Lecturer Dept. of electronics and telecommunication
Govt. polytechnic
Janjgir - champa
Janjgir, chhatisgarh

M. R. Khan, Ph.D
HOD
Dept. of Electronics and Communication
Principal of govt. engg Collage
Jagdalpur,chhatisgarh

ABSTRACT
Every node in Mobile Ad hoc Network (MANET) is freely moves and independent. The dynamic nature of topology in MANET is creating the problem in routing, due to that the routing protocols for MANET is separately designed. In this paper the AODV unipath and AOMDV multipath are one of the, are considered for research. The AOMDV maintained the alternate routings possibilities so that they can be utilized when the primary path fails but the unipath are not handled the situation if the congestion is accurred. The single path protocol is not capable (without modification in routing procedure) to handle congestion. In this paper, we classify the congestion control capability of AODV and AOMDV rotuing protocol. The AOMDV is balanced the load by that the packets dropping due to congestion is minimized and enhanced routing performance. The simulation results show that the AOMDV is provides the better performance than AODV routing protocol. The AOMDV significantly increase the packet delivery ratio and decrease the average delay, the performance is better than other protocols.

Index Terms—Congestion, MANET, AOMDV, Memory Management, Rate Control

1. INTRODUCTION
Mobile ad-hoc network is a collection of temporary nodes that are capable of forming dynamic temporary network, self organize, and infrastructure less with nodes contains routing capability, improving the performance of Transmission Control Protocol (TCP) associated with the presence of multi-hop MANET is one of the research challenges in wireless mesh networks. Mobile Ad-hoc Networks (MANET) is very attractive for time-critical applications. There are a lot of issues and challenges in designing a MANET network. Because of dynamic topology and node changes their position in every second. Now one of the measure challenges is congestion in MANET. If sender node want to send data into the some specific receiver so first broadcast routing packet onto the network and get destination through the shortest path (if we apply AODV) or minimum intermediate hop after getting path sender sends actual data through uni-path link but at the same time more than one sender share common link so congestion occur onto the network that is measure issue for MANET. So various researcher works in that filed for minimization of congestion from network.

Congestion Avoidance and balancing of load will avoid frequent link failures and will definitely improve the existing AOMDV as proposed in the proposed section. The proposed scheme presented in this research, aims to improve the existing routing strategy by using a multipath routing protocol with load balancing in order to distribute the traffic effectively along all nodes on the network.

AOMDV Routing Protocol

The AOMDV [1] (Ad hoc On Demand Multipath multiple path Routing) identifies routes during route discovery. It is designed primarily for Ad hoc networks where link failures and route breaks occur frequently. When single path on-demand routing protocol such as AODV is used in such networks, a new route discovery is needed in response to every route break. Each route discovery is associated with high overhead and latency. Each RREQ carries a field called first hop to indicate the first hop taken by it. Also, each node maintains a first hop-list for each RREQ to keep track of the list of neighbors of the source through which a copy of the RREQ has been received. At the intermediate nodes, each duplicate copy is examined to see if it provides a new node-disjoint path to the source. This is ascertained by examining the first hop field in the RREQ copy and the first hop list in the node for the RREQ. If it does provide a new path, the AOMDV route update rule is invoked to check if a reverse path can be set up. If a reverse path is set up and a valid route to the destination is available at the intermediate node, it sends back a RREP to the source. Only the first arriving RREQ copy is forwarded if a route to destination is unavailable. Route discovery and route maintenance consists of finding multiple routes between a source and destination node. Multipath routing protocols can attempt to find node disjoint, link disjoint, or non-disjoint routes. Node disjoint routes, also known as totally disjoint routes, have no nodes or links in common. Link disjoint routes have no links in common, but may have nodes in common. Non-disjoint routes can have nodes and links in common.

2. RELATED WORK
The previous related research in this field is mentioned in this section. These scheme is provides the new thoughts to do some new work in this field.

According to [2] proposes a way or place where security application can track more traffic instead of applying to all nodes that can save much more cost as compared to provide

security for every node. Critical link are that place, from where maximum traffic can travel and monitoring of those nodes are easy.

According to [3], DoS attack can be launched in two forms. The first form aims to break down the target by sending one or more carefully constructed control packets that make use of the protocol or operating system vulnerabilities. The second form is to overflow the target with a huge amount of rubbish data, which leads to exhaustion of network bandwidth or computer resources.

In the routing table overflow attack, an attacker attempts to create routes to nonexistent nodes [4], [5]. As a consequence, routing loops may appear and introduce severe network congestion. Multiple attackers may completely isolate a victim, by preventing it from finding performed via network-layer packet blasting [6]. The attacker injects a large amount of junk packets into the network. These packets waste a significant portion of the network resources, and introduce severe wireless channel contention and network congestion in the MANET. In a SYN flooding attack, the attacker creates a large number of half-opened Transmission Control Protocol (TCP) connections with a target node, but never completes the handshake to fully open the connection.

The study presented in [5] investigates the influence of flooding attacks with Dynamic Source Routing (DSR) protocol messages to network performance. The packet delivery ratio and packet delay have been evaluated under different flooding frequencies and different numbers of attack nodes. The analysis assumes only the random waypoint mobility model.

Makoto Ikeda, Elis Kulla et. al. "Congestion Control for Multi-flow Traffic in Wireless Mobile Ad-hoc Networks" [7] In this paper, we deal with congestion control for multi-flow traffic in wireless mobile ad-hoc networks (MANET) using OLSR routing. This approach done through OLSR routing we also apply multi flow in AODV routing approach.

Tuan Anh Le, Choong Seon Hong, *Member*, *IEEE*, Md. Abdur Razzaque et. al. in his work titled "An Energy-Aware Congestion Control Algorithm for Multipath TCP" [8] In this paper, they develop ecMTCP. ecMTCP moves traffic from the most congested paths to the more lightly loaded paths, as well as from higher energy cost paths to the lower ones, thus achieving load-balancing and energy-savings. This paper focus congestion control with the help of energy base load balancing mechanism, this work also modified via multipath routing technique for end-to-end delay minimization.

Jingyuan Wang, Jiangtao Wen et. al. in his work titled "An Improved TCP Congestion Control Algorithm and its Performance" [9] In this paper, they propose a novel congestion control algorithm, named TCP-FIT, which could perform gracefully in both wireless and high BDP networks. The algorithm was inspired by parallel TCP, but with the important distinctions that only one TCP connection with one congestion window is established for each TCP session, and that no modifications to other layers (e.g. the application layer) of the end-to-end system need to be made. This work done only transport layer congestion control via TCP improvement method but congestion also occurs in routing time so that work enhance through routing base congestion control technique.

M. Ali, B. G Stewart et. al. In his work titled "Multipath Routing Backbones for Load Balancing in Mobile Ad Hoc Networks" [10] This title presents a new approach based on multipath routing backbones for enhanced load balancing in MANETs. Nodes in MANETs greatly differ with each other in terms of communication and processing capabilities. In this approach, multiple routing backbones are identified from source to destination using intermediate nodes that have better communication and processing capabilities to take part in the mobile routing backbones and efficiently participate in the routing process.

3. PROBLEM STATEMENT

Our objective to provide more security as well as congestion free communication in MANET, because mobile ad-hoc network is more vulnerable as well as dynamic topology base communication that increases insecurity, in our approach we found attacker information and prevent the network through different routing attack as well as congestion attack, the following objective are consider for our approach:

Minimize congestion

Balance to load from network

Find out congestion information

Increases network performance like throughput, packet delivery ratio

Minimize routing overhead

4. OUR CONTRIBUTION

In this paper, we analyze the routing behavior of AODV and AOMDV protocol under various scenarios and get better performance of AOMDV routing as compare to AODV routing, because AOMDV provide multiple path between senders to receiver that increase network performance and decrease the congestion from the network. Now with in a particular time the sender has not deliver the data then the AOMDV is provides the alternative path that is equal or less than reliable than existing path. Then in that case the increment in TTL value is removes the possibility of link failure due to time limit. But if the possibility of load at any link or node is increases then in that the link expiration time always exceeds then to control the link expiration time limit the concept of queue length is added to control the possibility of congestion and link expiration time limit. The queue scheme is raised the storing and forwarding capacity of or processing speed of nodes in network. The combination of these two different methods are improves the AOMDV routing performance and proper load balancing in network. With the help of AOMDV routing we provide reliable communication rather than AODV, so in future we enhance the multipath routing and minimize congestion of AOMDV routing protocol that exist in current scenario.

Simulation Tool and Parameters

Network Simulator (NS-2) [15], is used to simulate proposed scheme. In this simulation, the channel capacity of mobile hosts is set to the value of 2 Mbps. We use the IEEE 802.11 for wireless LANs as the MAC layer protocol. It has the functionality to notify the network layer about link breakage. In our simulation, the number of nodes is 50. The mobile nodes move in a 800×600 m square region for 100 sec simulation time. We assume each node moves independently

with the same average speed. All nodes have the same transmission range of 250 m. In our simulation, the speed is varies from 10 to 30 meters/seconds. Random Way Point mobility model is used. The simulated traffic is Constant Bit Rate (CBR) is attaching with UDP and File Transfer Protocol (FTP) is attaching with TCP.

Performance Metrices

The simulation results are evaluating through performance matrices.

Packet Delivery Ratio (PDR):

This is defined as ratio of number of packets that have successfully reached the destination to the total number of packets sent by the source. This metric is expressed in percentage.

Routing Load:

The routing load refers to the number of routing packets are deliver in network for established connection in between sender and receiver.

Throughput:

Throughput refers to the total number of packets successfully reaching the destination per second. This metric is an indicator of the quality of a routing path and the effectiveness of the load balancing mechanism.

Packets Receiving Analysis

The packet receiving is stands for the number of packets re successfully received at destination. The packets receiving are focus due to unreliable communication.

MAC Buffer overflow:

This occurs, when a node cannot enqueue a packet, as its queue is full due to congestion. In other words, low buffer overflow level indicates is distributed over the entire network.

Result Analysis

In this section, we evaluated the results of original AOMDV and proposed rate control scheme with AOMDV. The rate control scheme is improves the routing capability of multipath protocol and provides the better performance in network.

Data Sending Analysis

The data sending and receiving in network is done in between sender and receiver. The unipath protocol is only deliver data through single path. The connection establishment procedure and route section procedure is responsible for that. The multipath protocol is selecting the more than two paths but only sends or receives data through same path in network. In this graph the data sending analysis in case of AODV and AOMDV protocol in MANET. The data sending of AOMDV protocol is more in a given simulation time as compare to AODV protocol that represents the less receiving of data packets.

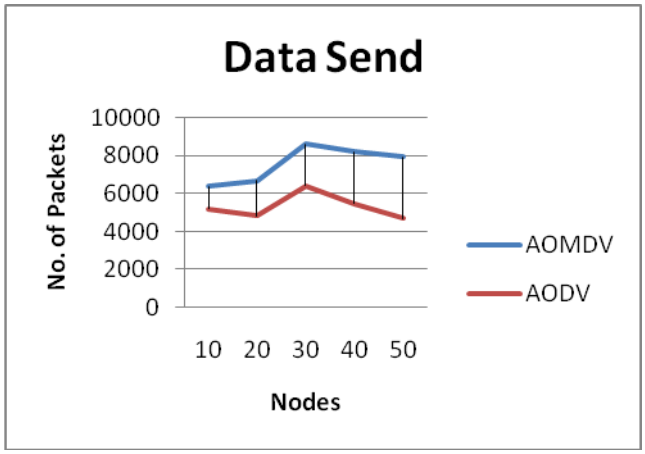

Fig.1 Data Sending Analysis

Data Receiving Analysis

The data receiving in network is depending on the load in network and the load in particular path is selected for data transmission in network. If the selected path is able to handle the flow of data then the receiving is more but if not then no provision of alternative path is present in AODV routing protocol in MANET but the AOMDV has a capability of deliver the data from alternative path by that the receiving is more and also avoided the congested selected path that degrades the data receiving in network. This graph shows the same performance of receiving of AOMDV as compare to AODV protocol in MANET. Here the receiving of AOMDV is much better.

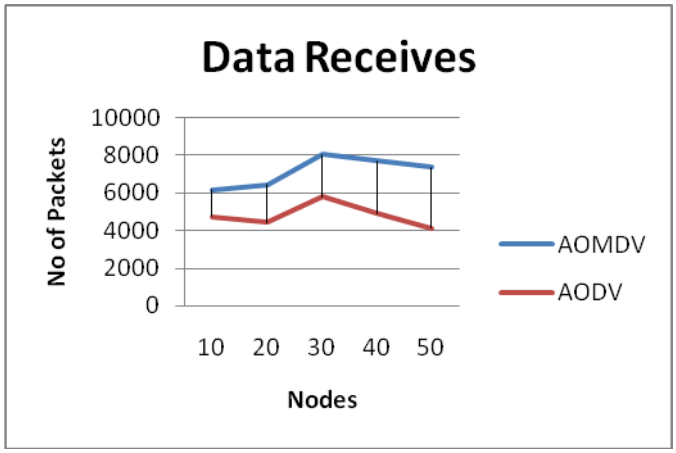

Fig.3 Data Receiving Analysis

Routing Overhead

The routing packets are necessary in MANET for establishment of connection in between sender and receiver. The routing packets flooding through sender is finding the receiver and receiver is selected the path on the basis of minimum hop count. This graph illustrated the routing overhead analysis of AODV and AOMDV. The routing overhead of AOMDV is more up to 30 nodes simulation but in case of dense network of 50 nodes the AODV routing overhead is more as compare to AOMDV. The less routing packets flooding is shows the better performance in network.

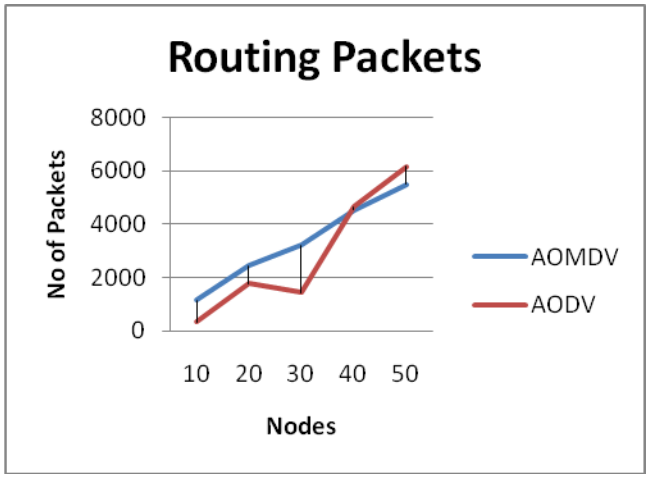

Fig.3 Routing Overhead Analysis

Packet Delivery ratio

The data receiving in network as compare to sending is depend on the network load in network and the capability of routing protocol in dynamic environment of MANET. The percentage of data receiving is evaluated through PDR performance metrics. The higher percentage of receiving is depending on the higher data receiving. In this graph the PDR performance of AODV and AOMDV is observed. The PDR performance of AOMDV is better (in between 96 to 92) because of providing the higher percentage of receiving as compare to AODV routing protocol.

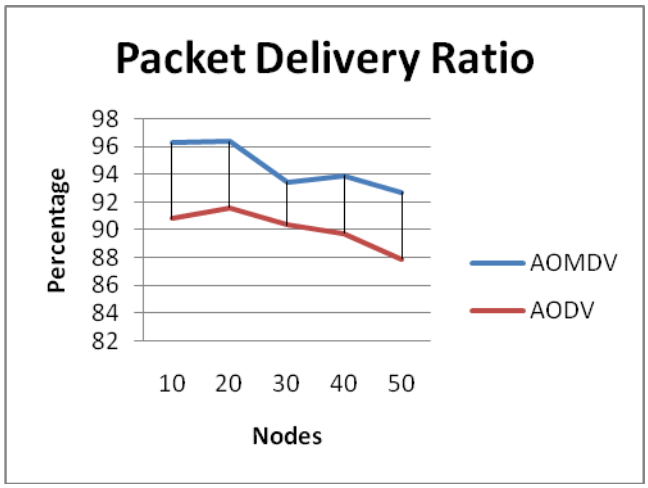

Fig.4 PDR Analysis

Total Drop via Congestion

In dynamic topology and fixed available bandwidth the network is heavy loaded due to that link is congested in MANET. The problem of congestion is occurred due to improper forwarding of data in a particular link/s in MANET. In this drop through congestion analysis, In AODV the possibility of congestion is occurring easily because of data is sending through single path in network and also the receiver ACK (Acknowledgement). But in case of AOMDV the load is balanced in network by proving the alternative path, if the existing one is congested in network. It implies that the packet dropping in AOMDV is less as compare to AOMDV in MANET.

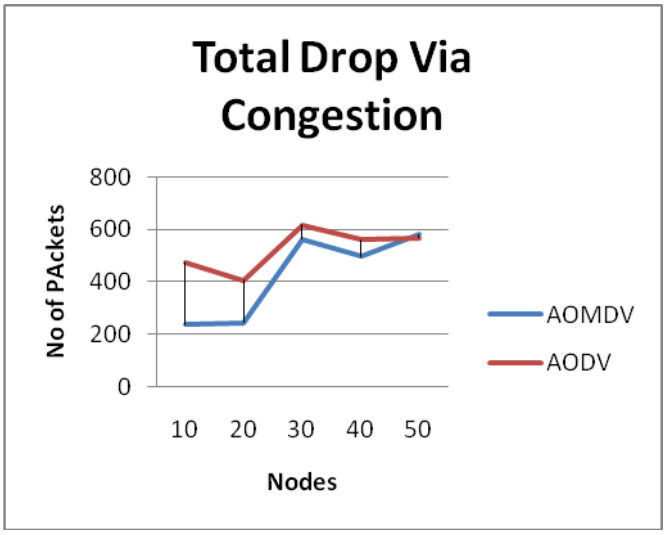

Fig.5 Drop through Congestion Analysis

Queue Overflow

The routers in network is stored the packets first and then it will be deliver to next connected router. The routers are storing a packet temporarily to read its routing information and then forward it. The nodes in a MANET are work as a router and host both and the nodes capacity of data storing temporarily is the buffer capacity of nodes. The Queue overflow condition is occurred in network due to the packets is pending on nodes for forwarding. Because of full of buffer capacity the data packets are pending for forwarding due to that the queue overflow condition is occur. In this graph due to queue overflow the packets dropping in AODV is more as compare to AOMDV protocol. The AOMDV protocol is handled the load due to that the overflow condition is balanced in network.

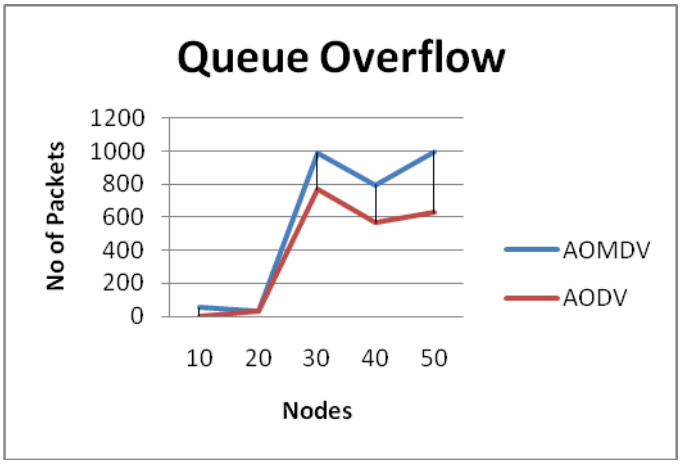

Fig.6 Queue Overflow Analysis

5. CONCLUSION WITH FUTURE ENRICHMENT

In the Mobile Ad hoc Network nodes mobility and the probability of links failure may cause the fault tolerance issues in a single path or unipath AODV protocol is more

important for routing problem therefore, each routing protocol should be fault tolerant in probable route failures. The multipath AOMDV protocol reduces the restriction of single path establishment and provides the alternative route to deliver the data. The proposed congestion control capability of AODV and AOMDV is measuring through performance metrics. Identified that the AOMDV protocol is better for handled the heavy load that is the cause of congestion in MANET. The alternative route proving capability of routing protocol balanced the load properly in network. AOMDV is much effective in dense network as compare to AODV protocol. The AOMDV is also overcome the limitation of fixed available bandwidth and the packet dropping due to queue overflow is also minimized. The multipath routing providing more than one path can better support at high mobility network with high packet delivery ratio and lower control overhead.

6. REFERENCES

[1] M. Mahesh K.and R. D. Samir, "Ad hoc on-demand multipath distance vector routing," *Wireless Communications and Mobile*, vol. 6, no. 7, pp. 969–988, 2006.

[2] Ghanshyam Prasad Dubey, Neetesh Gupta, Amit Sinhal, "Multiple Critical Node Detection in MANET for Secure Communication", Proceedings in International Conference on Computer and Communication (ICCC-2012), pp. 521-529, Bhopal, 2012.

[3] Peng T., Leckie C., Ramamohanarao K. "Survey of Network–Based Defense Mechanisms Countering the DoS and DDoS Problems" ACM Computing Surveys,Vol. 39.Issue- 1, Article no. 3, 2007.

[4] Jawandhiya P. M., Ghonge M. M., Ali M. S., Deshpande J. S. "A Survey of Mobile Ad Hoc Network Attacks" International Journal of Engineering Science and Technology, Vol. 2, No. 9, pp 4063–4071, 2010.

[5] Yi P., Zhou Y–k., Wu Y., Liu N. "Effects of Denial of Service Attack in Mobile Ad Hoc Networks", Journal of Shanghai Jiaotong University (Science), Vol. - 14, No. - 5. pp. 580 - 583, 2009.

[6] Yang H., Luo H., Ye F., Lu S., Zhang L. "Security in Mobile Ad Hoc Networks: Challenges and Solutions", IEEE Wireless Communications, Vol. 11, No. 1, pp. 38 - 47, 2004.

[7] Makoto Ikeda, Elis Kulla, Masahiro Hiyama, Leonard Barolli, Rozeta Miho and Makoto Takizawa "Congestion Control for Mul i-flow Traffic in Wireless Mobile Ad-hoc Networks" 2012 Sixth International Conference on Complex, Intelligent, and Software Intensive Systems, 2012 IEEE.

[8] Tuan Anh Le, Choong Seon Hong, *Member, IEEE,* Md. Abdur Razzaque et. al. "An Energy-Aware Congestion Control Algorithm for Multipath TCP" IEEE Communications Letters, Vol. 16, No. 2, February 2012.

[9] Jingyuan Wang, Jiangtao Wen et. al. in his work titled "An Improved TCP Congestion Control Algorithm and its Performance" 2011 IEEE.

[10] M. Ali, B. G Stewart et. al. In his work titled "Multipath Routing Backbones for Load Balancing in Mobile Ad Hoc Networks" 978-1-4673-0784-0/12, 2012 IEEE.