Mobility based Performance Analysis of AODV and DYMO under Varying Degree of Node Misbehavior

Sudhir Agrawal
Research Scholar RGPV
Bhopal MP India
AP Deptt of EC
TIEIT Bhopal MP India

Sanjeev Jain
Director MITS
Gwalior MP India

Sanjeev Sharma
Associate Professor
SOIT RGPV Bhopal MP
India

Roopam Gupta
Associate Professor
Deptt. Of IT
RGPV Bhopal MP India

ABSTRACT
Node cooperation is the basic paradigm for efficient functioning of MANETs (Mobile Ad hoc Networks). A paradigm shift from this trait causes the nodes to misbehave thereby affecting the network performance. Selfishness to conserve own resources, Maliciousness to disrupt the network fabric or Malfunctioning may cause the nodes to misbehave. MANET characteristics like dynamism of topology, shared wireless channels and open infrastructureless architecture pose security threats to them. This paper examines and analyzes two currently IETF listed reactive routing protocols AODV and DYMO with varying speed of node mobility and varying degree of maliciousness. The performance metrics Packet delivery ratio, Average End-to-end delay & Jitter and Normalized routing overhead are compared when a varying percentage of nodes drop packets.

General Terms
MANET Security

Keywords
Mobile Ad hoc Networks, AODV, DYMO, Node misbehavior.

1. INTRODUCTION
Mobile Ad hoc NETwork (MANET) is a set of mobile devices (nodes), which over a shared wireless medium communicate with each other without the presence of a predefined infrastructure or a central authority. The member nodes are themselves responsible for the creation, operation and maintenance of the network. The nodes which are not in wireless vicinity, communicate with each other hop by hop following a set of rules (routing protocol) for the hopping sequence to be followed. MANETs require these routing protocols to cope well with dynamism of topology, and nodes should cooperate trustfully in order to establish genuine routes [1]. This need for trustfulness of nodes springs to fore the issue of security in MANETs.

Securitizing the routing process is a particular challenge due to open exposure of wireless channels and nodes to attackers, lack of central agency/infrastructure, dynamic topology etc.[2]. The wireless channels are accessible to all, whether meaningful network users or attackers with malicious intent. The lack of central agency inhibits the classical server based solutions to provide security. The dynamic topology entails that at any time any node whether legitimate or malicious can become a member of the network and disrupt the cooperative communication environment by purposely disobeying the routing protocol rules.

A lot of routing protocols have been proposed in the literature [3], including proactive, reactive, and hybrid solutions. Djenouri et al. [4] have shown that reactive protocols are more adaptable to MANET environments than proactive protocols. A number of security attacks have been surveyed in literature [5] along with their proposed countermeasures. A simulation-based analysis of security exposures in MANETs was carried out by Michiardi and Molva [6] where it is assumed that a node may misbehave under the above security attacks. Three types of routing misbehavior have been classified and simulated for DSR (Dynamic Source Routing). Their simulation results showed that network operation and maintenance can be easily jeopardized and network performance severely affected. Nodes misbehave because they are *malfunctioning, selfish* or *malicious* [7]. Malfunctioning nodes are those nodes which suffer from hardware failure or software errors. Selfish nodes are those which in an attempt to save their energy or bandwidth simply sit idle in the network, neither taking part in routing process nor in the communication process other than their own. Malicious nodes are those which take part in the route establishment process thereby entering valid routes between a pair of communicating nodes but silently drop the packets in attempt to sabotage other nodes or even the whole network. A malicious node can claim itself as having the shortest path to all nodes in the network and then it can cause Denial of Service (DoS) by dropping all the received packets, in *Black hole attack*, or selectively dropping packets in *Gray hole attack*. More malicious nodes working in unison can cause severe damage by collaborating in the attacks, such as *wormhole attack*. It is the malicious nodes which pose the greatest threat to the MANET fabric.

To render the network function normally in the presence of misbehaving nodes is a challenging task and demands it necessary to consider ”fault tolerance” as a main objective at the design level of routing protocols. It seems imperative to provide a simulation study that measures the impact of misbehaving nodes in order to provide protocol designers with new guidelines that help in the design of fault tolerant and attack tolerant routing protocols for MANETs. The AODV (Ad Hoc On-demand Distance Vector) and DYMO (Dynamic MANET On-demand) routing protocols are both reactive routing protocols that are listed by the Internet Engineering Task Force (IETF) MANET working group. AODV is considered mature and is described in RFC3561 [8]. DYMO is still in draft phase [9] and actively worked on by the working group and is the focal point of research. There have been few studies [10, 11,12] comparing and analyzing AODV, DSR, DSDV routing protocol performance in presence of misbehaving nodes but as far to our knowledge this is the first work to examine and analyze the performance of DYMO in presence of misbehaving nodes. The object of this paper is to examine the performance of two prominently poised reactive routing protocols AODV and

DYMO with varying number of nodes misbehaving with different speeds of node mobility.

In the rest of the paper, Section 2 briefly introduces AODV and DYMO routing protocols for MANETs and discusses the routing misbehavior. Section 3 describes the simulation environment and methodology in *ns-2*. Section 4 presents the simulation results and analysis and finally, Section 5 concludes the paper.

2. ROUTING PROTOCOLS AND NODE MISBEHAVIOR

2.1 AODV (Ad Hoc On-Demand Distance-Vector Routing Protocol)

The AODV Routing Protocol [8] provides on-demand route discovery in mobile ad hoc networks. Like most reactive routing protocols, route finding is based on a route discovery cycle involving a broadcast network search and a unicast reply containing discovered paths. AODV relies on per-node sequence numbers for loop freedom and for ensuring selection of the most recent routing path. AODV nodes maintain a route table in which next-hop routing information for destination nodes is stored. Each routing table entry has an associated lifetime value. If a route is not utilized within the lifetime period, the route is expired. Otherwise, each time the route is used, the lifetime period is updated so that the route is not prematurely deleted.

2.2 DYMO (Dynamic MANET On demand routing protocol)

The Dynamic MANET On-demand routing protocol (DYMO) is a newly proposed protocol currently defined in an IETF Internet-Draft [9] in its twenty-first revision and is still work in progress. DYMO is a successor of the AODV routing protocol. It operates similarly to AODV. DYMO does not add extra features or extend the AODV protocol, but rather simplifies it, while retaining the basic mode of operation. As is the case with all reactive ad hoc routing protocols, DYMO consists of two protocol operations: route discovery and route maintenance. Routes are discovered on-demand when a node needs to send a packet to a destination currently not in its routing table. A route request message is flooded in the network using broadcast and if the packet reaches its destination, a reply message is sent back containing the discovered, accumulated path. Each entry in the routing table consists of the following fields: Destination Address, Sequence Number, Hop Count, Next Hop Address, Next Hop Interface, Is Gateway, Prefix, Valid Timeout, and Delete Timeout. Figure 1 gives an illustration of difference between AODV and DYMO routing process when node J wants to communicate with node M.

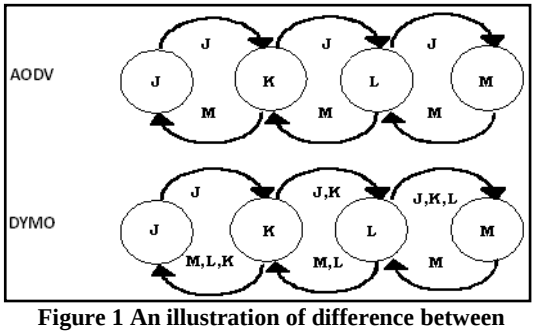

Figure 1 An illustration of difference between AODV and DYMO routing process when node J wants to communicate with node M.

2.3 Node Misbehavior

The attacks on MANET nodes or intrusions into the MANETs may result in compromising of the affected nodes which then tend to misbehave. Also the selfish nature of the resource constrained mobile nodes and adversarial nature of wicked nodes may create anomalies in the network. Some of these resource constrained nodes particularly in an attempt to save their battery power for their individual needs may tend be selfish. In their selfishness they back out from the basic attribute of cooperation. The survivability of a network is defined as the network's ability to fulfill correctly its functions even in the presence of attacks or intrusions [13]. The survivability of the network is endangered if these misbehaviors are left unattended.

2.3.1 Type 1 Node Misbehavior

In type 1 misbehavior model, the Misbehaving Node (MN) does not perform the packet forwarding function [14]. It drops all or some of the data packets which have a source address or a destination address other than that of itself. However it participates in the Route Discovery and Route Maintenance phases of the routing protocol behaving as a normal node. This results in it advertizing a route through itself but on which data traffic may never materialize as it may drop all data packets which it has to forward as a router node. Such behavior can be termed as *malicious* as it results in data loss in the network thereby defeating the very purpose of the network. The blackhole, greyhole, sinkhole or wormhole attacker nodes come under this category.

2.3.2 Type 2 Node Misbehavior

In type 2 misbehavior model, the MN does not participate in the Route Discovery and Route Maintenance phases of the routing protocol. As an attacker node it sits silently in the network as a passive eavesdropper snooping in the information in the network, whereas as a *selfish* node it simply looks out for the communications sourced by itself or targeted to it and does not cooperate in network maintenance and thereby cooperative communication. The impact of this model on the network is to obscure route discovery and maintenance however communication function is undisturbed. A MN of this type uses the node energy only for its own communications.

2.3.3 Type 3 Node Misbehavior

Type 3 misbehavior model is a particular case of type 1 misbehavior model in which the MN behaves in a selective manner. A normally behaving node may become a selfish node if its energy drops below a threshold. It then starts dropping data packets in an effort to conserve its energy for its own and hence becomes a malicious node. An attacker node may randomly drop data packets in an attempt to disrupt the communication but remain undetected by the security mechanisms or may drop packets sourced from or targeted to a particular node in an attempt to attack that particular node.

3. SIMULATION ENVIRONMENT AND METHODOLOGY

The Network Simulator *ns* is a discrete event simulator targeted at networking research [15]. It provides substantial support for simulation of TCP, routing, and multicast protocols over wired and wireless (local and satellite) networks. It began as a variant of the REAL network simulator in 1989 and has evolved substantially over the past few years. In 1995 *ns* development was supported by DARPA through the VINT project at LBL, Xerox PARC, UCB, and USC/ISI. Currently *ns* development is support through DARPA with SAMAN and through NSF with CONSER,

both in collaboration with other researchers including ACIRI. *ns* has always included substantial contributions from other researchers, including wireless code from the UCB Daedelus and CMU Monarch projects and Sun Microsystems. The current stable version are *ns-2* (ver 2.34) and *ns-3* (ver 3.11)

ns-2 provides a good platform for MANET simulation and has been widely used and its results generally accepted by the research community. It contains models and modules at physical and data link layers, medium access control protocols, and the ad hoc routing protocols we want to compare (DYMO and AODV). DYMO is available as a contributed code as DYMOUM at sourceforge.net. The node movement scenario is generated by using the Random waypoint model of mobility. This model allows a node to choose its destination and the nodes moves towards it at a uniform specified speed. When a node reaches its destination it waits for a specified pause time before choosing another random destination and repeating the process. Communications among randomly selected nodes are established using constant bit rate (CBR) traffic. The type 1, node misbehavior which is our focal point of analysis and analysis has been added as separate node definition types in the *ns-2* node model, which allows selection of selfish node or normal node. Using the *ns-2* environment, some common parameters are listed in Table 1.

Table 1Parameters Defined For Simulation In *ns-2*

Parameters	**Values**
Simulation Area	800m x 800m
Radio Range	100m
Link Capacity	2 Mbps
Pause Time	2 seconds
Simulation Time	200 seconds
Buffer Size	50 Packets
Application	Constant bit rate (CBR) Traffic
Packet Size	512 Bytes
Network Density	40 Nodes
Network Mobility	0, 2, 4, 6, 8, 10 m/s
Routing Protocols	AODV/DYMO
Type of Selfish Node	Type 1 (Packet dropper)
Percentage of Misbehaving Nodes	0, 15, 30, 45 %

Network Density: This aspect is represented by the number of nodes in a fixed area where an MANET is run. The node density in our simulation is kept at 40 nodes in a 800m x 800m area (8R where R is the Radio Range), which is neither high density nor low. An average density is kept for our simulations so that effects of node misbehavior can properly be observed without being affected by other factors like congestion etc. The network density of a MANET influences the performance of the routing protocol as a high density network is more immune to the malicious effects of misbehaving nodes as multiple routes between node pairs exist, whereas it also causes higher congestion and bandwidth crunch. On the contrary a low density network may be partitioned due to malicious effects of misbehaving nodes but bandwidth availability is far better.

Network Mobility: The simulations are carried out for 0 m/s to 10 m/s in steps of 2m/s (static to a speed of 36 km/h) to observe various types of network traffic conditions. The performance of routing protocols is affected by speed of node mobility as higher the speed, more are the breaks in the links thereby taxing the routing performance.

Routing protocols: Two types of ad hoc reactive routing protocols which are listed by IETF are compared: AODV and DYMO.

Types of selfish nodes: It is expected that Type 1 selfish node may degrade the network more than Type 2 as it participates in routing discovery and maintenance but refuses to forward packet when it is included in a route so Type 1 node misbehavior is simulated.

Percentage of misbehaving nodes: The network will suffer more when better behaved nodes are compromised to misbehaving nodes. The number of misbehaving nodes is presented by percentage, from 0% to 45%. The remaining nodes are assumed to be well behaved.

For examining the protocols, network performance is evaluated according to the following metrics:

Packet Delivery Ratio, Average End-to-End Delay and Jitter, Normalized Routing Overhead

4. SIMULATION RESULTS AND ANALYSIS

In this paper simulation results of network with average node density with varying speed of node mobility and different percentage of misbehaving nodes are presented and discussed. Figure Sets 2, 3 and 4 demonstrate the results of Packet Delivery Ratio, Average End-to-End Delay and Normalized Routing Overhead versus node mobility. Each set is a simulation result of different percentage of misbehaving nodes; No misbehaving nodes environment (0%), Low misbehaving nodes environment (15%); Moderate misbehaving nodes environment (30%) and High misbehaving nodes environment (45%). We now put forth the performance analysis of AODV and DYMO under the influence of misbehaving nodes, with reference to our performance metrics.

4.1 Packet Delivery Ratio

Figures 2(a) to 2 (d) present the analysis of Packet Delivery Ratio of AODV and DYMO with varying percentage of type 1 misbehaving nodes from 0% to 45%. The analysis is done for node mobility speed ranging from static scenario (0 m/s) to high speed of mobility (10 m/s). It is observed that the PDR of AODV and DYMO goes hand in glove with one another with DYMO showing better performance at higher node mobility. This is expected as DYMO is an extension of AODV.

4.2 Average End-to-End Delay and Jitter

Figures 3 (a) to 3 (d) presents the analysis of Average End-to-End Delay or Latency of AODV and DYMO with varying percentage of type 1 misbehaving nodes from 0% to 45%. The analysis is done for node mobility speed ranging from static scenario (0 m/s) to high speed of mobility (10 m/s). It is observed that the Latency and hence the Jitter of DYMO is better for all scenarios in AODV. This is expected as the path accumulation in DYMO causes routes to be established faster thereby reducing the latency as compared to AODV.

4.3 Normalized Routing Overhead

Figures 4 (a) to 4 (d) presents the analysis of Normalized Routing Overhead of AODV and DYMO with varying percentage of type 1 misbehaving nodes from 0% to 45%. The analysis is done for node mobility speed ranging from static scenario (0 m/s) to high speed of mobility (10 m/s). It is observed that the Routing Overhead is lower for AODV than that of DYMO under all circumstances. This is because DYMO generates and transmits more routing packets than AODV for the same communication.

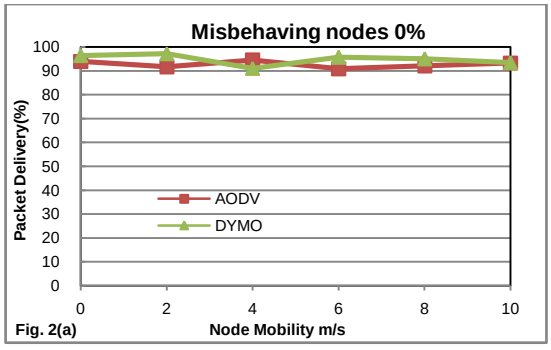

Figure 2(a) PDR for no maliciousness

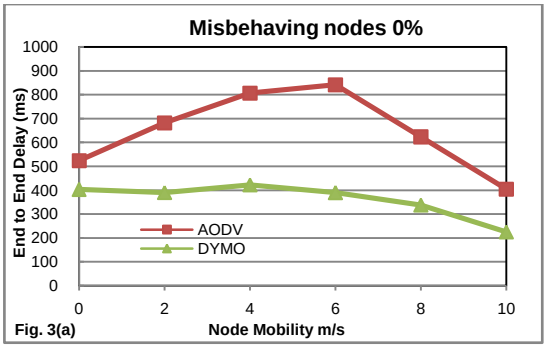

Figure 3(a) End to end delay for no maliciousness

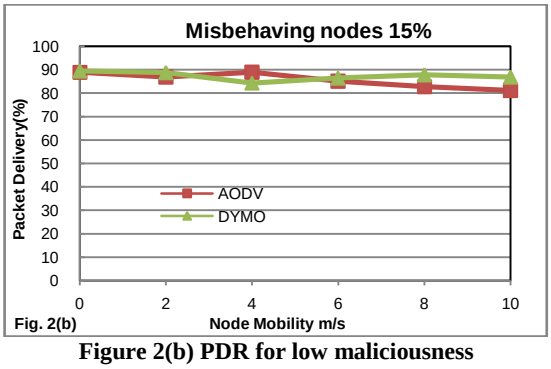

Figure 2(b) PDR for low maliciousness

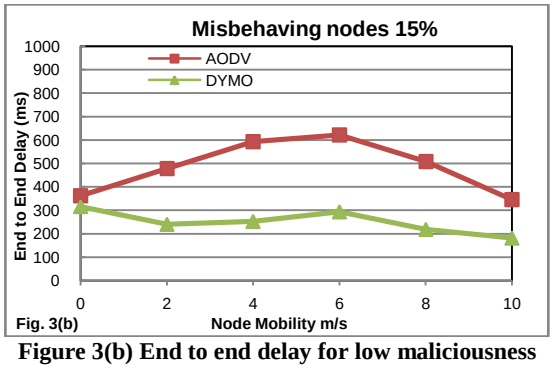

Figure 3(b) End to end delay for low maliciousness

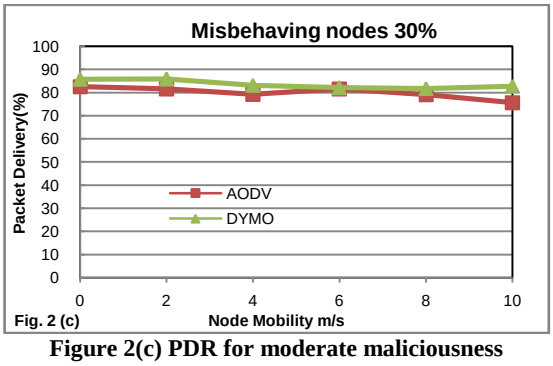

Figure 2(c) PDR for moderate maliciousness

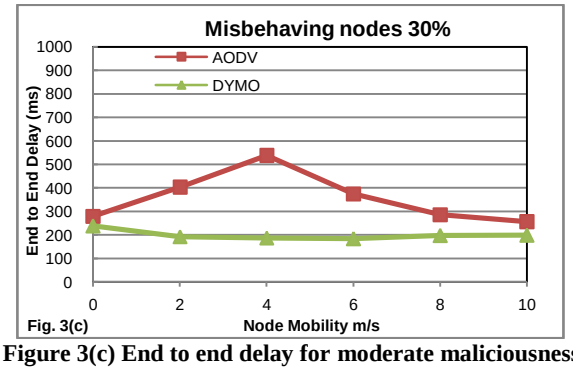

Figure 3(c) End to end delay for moderate maliciousness

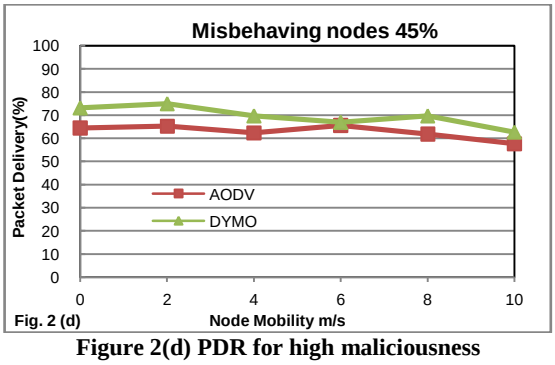

Figure 2(d) PDR for high maliciousness

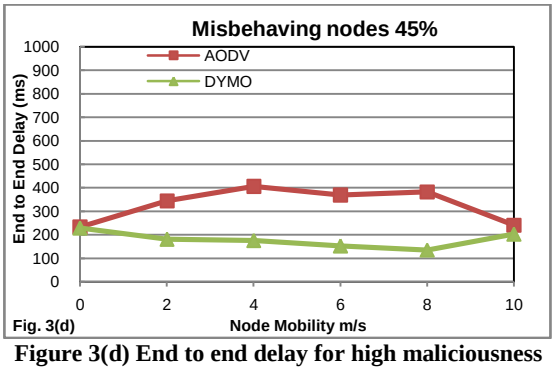

Figure 3(d) End to end delay for high maliciousness

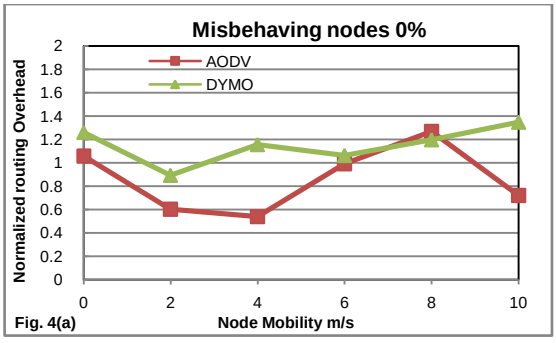

Figure 4 (a) Normalized Routing Overhead for no maliciousness

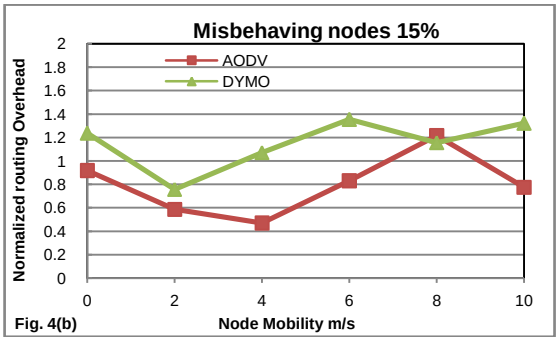

Figure 4 (b) Normalized Routing Overhead for low maliciousness

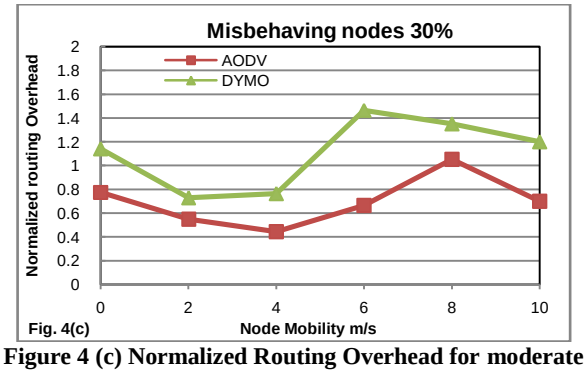

Figure 4 (c) Normalized Routing Overhead for moderate maliciousness

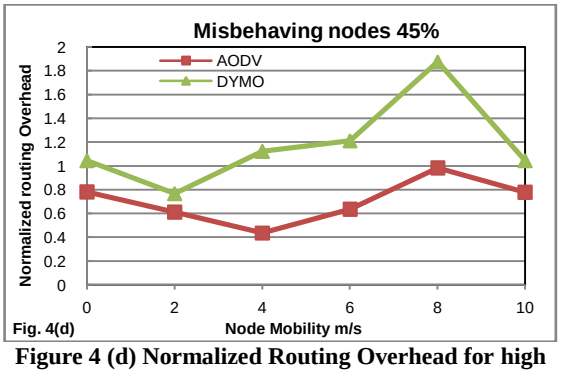

Figure 4 (d) Normalized Routing Overhead for high maliciousness

5. CONCLUSIONS AND FUTURE WORK

This paper compares two most actively researched reactive routing protocols AODV and DYMO under the influence of misbehaving nodes for varying speed of mobility. Network performance is evaluated in terms of Packet Delivery Ratio, Average End-to-End Delay, Throughput and Normalized Routing Overhead, when a percentage of nodes misbehave. The scenarios considered varied from static to high mobility speed of 10m/s. Simulation results show that although the performance of both the routing protocols degrades DYMO proves to be more robust in terms of the tested performance metrics. The throughput of DYMO and AODV protocol are quite similar however, as the mobility speed of the nodes increases the Latency and hence the Jitter also increases for AODV. This is significant for the fact that, as the variations of packet delay or jitter becomes more predictable, the routing mechanisms can factor in that delay to determine whether the packet is lost or not. Instead of a mobile node waiting for say 0.2 seconds for AODV packet, it needs to wait for 0.1 seconds for a DYMO packet to determine whether the packet is lost or not. This saves crucial time that can be utilized to initiate fresh route discovery operations.

Based on simulation analysis, it is clear that DYMO, though a derivative of AODV is more efficient than the latter since it takes advantage of its salient features carefully pruning its weaknesses. Our implementation of the DYMO specification can be further extended twenty-first version of IETF draft for future implementations including MANET Neighborhood Discovery Protocol (NHDP), a newer version of generalized MANET packet and message format, and the three additional kinds of timeouts. The latest version of IETF draft also requires DYMO to support Simple Internet Draft [9] where a sub network of all DYMO routers connect with internet using a single Internet DYMO Router (IDR).

In the future, we intend to use the insight gained in the protocol performance and the effect of misbehaving nodes, to devise and implement a misbehaving node detection and isolation algorithm for MANETs. This will help make MANETs more secure from routing attacks and hence address the security vulnerability problem of MANETs.

6. REFERENCES

[1] Murthy, C.S.R. and Manoj, B.S. 2008. Ad Hoc Wireless Networks. Pearson Education.

[2] Hubaux, J.P., Buttyan, L. and Capkun, S. 2001. The Quest for Security in Mobile Ad Hoc Networks. In Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC).

[3] Zhou, H. 2003. A Survey on Routing Protocols in MANETs. Technical Report. Michigan State University.

[4] Djenouri, D., Derhab, A. and Badache, N. 2006. Ad hoc networks routing protocols and mobility. International Arab Journal of Information Technology.

[5] Agrawal, S., Jain, S. and Sharma, S. 2011. A Survey of Routing Attacks and Security Measures in Mobile Ad Hoc Networks. Journal of Computing.

[6] Michiardi, P. and Molva, R. 2002. Simulation-Based Analysis of Security Exposures in Mobile Ad Hoc Networks. In Proceedings of European Wireless Conference.

[7] Kargl, F., Schlott, S., Klenk, A., Geiss,A. and Weber, M. 2004. Securing Ad Hoc Routing Protocols. In Proceedings. 30th Euromicro Conference.

[8] Perkins, C. Belding-Royer, E. and Das, S. 2003. RFC 3561: Ad hoc On-Demand Distance Vector (AODV) Routing. http://www.ietf.org/rfc/rfc3561.txt.

[9] Chakeres, I. and Perkins, C. 2010. Dynamic MANET On-Demand (DYMO) Routing Protocol. IETF Internet Draft, v.21, (Work in Progress). http://tools.ietf.org/html/draft-ietf-manet-dymo-21.

[10] Bo, S. M., Xiao, H., Adereti, A. and Malcolm, J. A. 2007. A Performance Comparison of Wireless Ad Hoc Network Routing Protocols under Security Attack. In Proceedings of the 3rd International Symposium on Information Assurance and Security (IAS '07).

[11] Babakhouya, A. Challal, Y. and Bouabdallah, A. 2008. A Simulation Analysis of Routing Misbehavior in Mobile Ad Hoc Networks. In Proceedings of the Second International Conference on Next Generation Mobile Applications, Services, and Technologies.

[12] Gopalakrishnan, K. and Uthariaraj, V. R. 2009. Scenario Based Evaluation of the Impact of Misbehaving Nodes in Mobile Ad hoc Networks. First International Conference on Advanced Computing.

[13] Lima, M. Santos, A. D. and Pujolle, G. 2009. A Survey of Survivability In Mobile Ad Hoc Networks. IEEE Communication Surveys & Tutorials.

[14] Marti, S. Giuli, T. Lai, K. and Baker, M. 2000. Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. In Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCom).

[15] The Network Simulator - ns-2, http://isi.edu/nsnam/ns/, retrieved july 2011.