International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:4, No:5, 2010

Performance Comparison of Single and Multi-Path Routing Protocol in MANET with Selfish Behaviors

Abdur Rashid Sangi, Jianwei Liu, Zhiping Liu

Abstract**—**Mobile Ad Hoc network is an infrastructure less network which operates with the coordination of each node. Each node believes to help another node, by forwarding its data to/from another node. Unlike a wired network, nodes in an ad hoc network are resource (i.e. battery, bandwidth computational capability and so on) constrained. Such dependability of one node to another and limited resources of nodes can result in non cooperation by any node to accumulate its resources. Such non cooperation is known as selfish behavior.

This paper discusses the performance analysis of very well known MANET single-path (i.e. AODV) and multi-path (i.e. AOMDV) routing protocol, in the presence of selfish behaviors. Along with existing selfish behaviors, a new variation is also studied. Extensive simulations were carried out using ns-2 and the study concluded that the multi-path protocol (i.e. AOMDV) with link disjoint configuration outperforms the other two configurations.

Keywords**—**performance analysis, single and multi path protocol, selfish behaviors.

I. Introduction

MANETs are considered an easy, quick and cost effective deployment option among other type of networks. Due to such features, the ad hoc network applications are no more limited to military, disaster recovery and emergency management but also extended to personal/local area networks. As MANET is a totally different kind of network, it needs a different set of protocols to perform network activities. Routing protocols are an important part of any network to discover and maintain routes between any given pair of node. Routing protocols in Ad Hoc network are differentiated in terms of hop-by-hop or source routing, reactive or proactive approach, single or multi-path, distance vector or link state based, uni-cast or multi-cast etc.

Reactive approach is considered more efficient than proactive approach as it only discovers and maintains routes between nodes which need to communicate with each other. Multi-path routing protocols creates less overhead as compared to single-path routing protocols and are susceptible to high network load, frequent route failure due to mobility, congested networks etc.[1]

Multi-path routing protocol i.e. AOMDV [2] can provide two different kinds of disjoint paths i.e. Link and Node Disjoint paths. Unlike single-path routing protocol i.e. AODV [4], the AOMDV can discover more than one routes between any given pair of nodes in single route discovery. Such feature of AOMDV comes with almost same cost of overhead and latency incurred by AODV. Study [3] showed that AOMDV is able to reduce the frequency of route discovery by as much as 30% and also achieve remarkable reduction in latency as compared to AODV.

In this paper AOMDV and AODV routing protocol were analyzed, in the presence of selfish behaviors [5], [6] (discussed in Section II) by using simulations.

This paper is organized as follows. Section II gives an overview of existing types of selfish behaviors and our new variation. Section III provides details of two protocols which are studied in context of selfish behaviors. Section IV and V contains simulation results and conclusion with future work, respectively.

II. Selfish Behaviors

To maintain the network operations, all nodes in MANET are believed to cooperate with each other by forwarding data and routing packets to/from destination. On the other hand, due to resource limitations (especially limited battery); the participating nodes can stop cooperating to accumulate their resources. Certain types of selfish behaviors [5], [6] are already studied with single-path routing protocols. Along with above selfish behaviors, this paper also discusses one new variation.

A. Type 1

In this selfish behavior the selfish node stops forwarding the data packets but continue to participate in route discovery and maintenance. In this way, the probability would be high that such selfish node can exist in any discovered route.

B. Type 2

The selfish node which initiate type 2 selfish behavior, would stop forwarding both data and routing packets. These nodes can be consider as resting nodes and such nodes can only consume energy to send/receive data related to them.

A.R Sangi, is a PhD Scholar in Electronics and Information Engineering, Beihang University Department, Beijing, China since 2008. (Mobile: +86-13141311352; e-mail: sangi@ ee.buaa.edu.cn).

Jianwei Liu, is currently professor in Electronics and Information Engineering Department, Beihang University, Beijing, China. (e-mail: liujianwei@buaa.edu.cn)

Zhiping Liu, is currently a associate professor in Zibo Vocational Institute, Shandong, China (email: lzhp716@sina.com)

International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:4, No:5, 2010

C. Type 3 (new variation)

The type 3 selfish behavior is basically a small variation of existing types. In this type of selfish behavior, the selfish nodes participate in route discovery and maintenance process but periodically stop and resume forwarding the data packets.

In this way, the selfish node can accumulate twice more battery life as compared to non-selfish node. A mathematical model designed to show such response is given as under.

$$f(t) = \begin{cases} 1 & \forall\, t \geq 2n-1 \\ 0 & \forall\, t \geq 2n \end{cases} .where \quad n \text{ is an integer}$$

Time is equally spaced at the equal interval of 5 seconds.

III. Routing protocols

A. Single-Path Routing Protocol

AODV [4] is a famous reactive (on-demand), hop-by-hop, single-path routing protocol. Like most of other routing protocols, it is based on two main mechanisms i.e. route discovery and maintenance. Route discovery in AODV starts with broadcasting the route request (RREQ) by source with its ID and a unique destination sequence number to all its neighbors. All neighbors that received specific RREQ for the first time then rebroadcast it after storing the ID of the sender. Storing the sender ID represents the reverse path to the source. The route discovery process ends when the destination node receives a RREQ, it sends a Route Reply (RREP) back to source node. RREP uses the reverse path to source which already is maintained by intermediate nodes.

Being the single-path routing protocol, AODV only discover single path for any destination. In case of the route failure, this single-path routing protocol initiates again another route discovery which put a massive load on the network. Single route to destination node increases the probability of a malicious node existence in discovered path

B. Multi-Path Routing Protocol

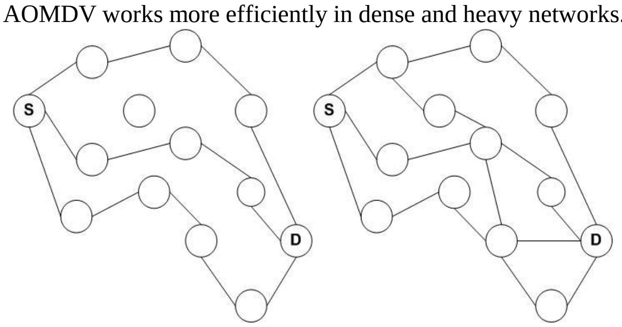
AOMDV [2], [3] on the other hand is a multi-path routing protocol. It is an extension to AODV and also provides two main services i.e. route discovery and maintenance. Unlike AODV, every RREP is being considered by the source node and thus multiple paths can be discovered in one route discovery. Being the hop-by-hop routing protocol, the intermediate node can maintain multiple path entries in their respective routing table. As an optimization measure, by default the difference between primary and an alternate path is equal to 1 hop.

To discover distinct paths, AOMDV suppresses duplicate route requests (RREQs) at intermediate nodes. Such suppression comes in two different variations, resulting in either node (illustrated in Fig. 1 (a)) or link (illustrated in Fig. 1(b)) disjoint. AOMDV can be configured to either discover the link (no common link between any given pair of nodes) or node (in addition to link disjoint, common intermediate nodes are also excluded between any given pair of nodes) disjoints paths.

Disjoint alternate paths are a good choice than overlapping alternate paths, as the probability of their interrelated and concurrent failure is smaller. This property can be helpful in an adversarial environment where malicious activity can also cause additional link failure.

Finding a disjoint path is quite straightforward in source routing (as every node maintain complete path information for every path), but hop-by-hop routing i.e. AOMDV is considered more efficient in terms of creating less overhead

Number of paths in any given source and destination is directly proportional to the number of nodes in entire network. AOMDV works more efficiently in dense and heavy networks.



(a) Node Disjoint (b) Link Disjoint

Fig. 1 AOMDV Multi-path

IV. Simulation

Simulations are performed by using Network Simulator (ns-2) [7]. The simulation software was been modified to perform three types of selfish behaviors. Attack is implemented by incorporating small logics in the back-end implementation of simulated protocols [8]. The result is compiled under four performance metrics [9]. Table I explains the acronyms for these performance metrics.

TABLE I
Acronyms for Performance metrics

Acronyms	Stands for
PR	Packet Received
PS	Packet Sent
TD	Total Delay
THC	Total Hop Count
PDR	Packet Delivery Ratio
AED	Average End-to-End Delay
AHC	Average Hop Count

1) Packet Delivery Ratio: It shows the ratio of total packets received at destination nodes, to total packets which are sent by source nodes.

$$PDR = PR / PS * 100\%$$

2) Average End-to-End Delay [ms]: It shows the average delay (time) in milliseconds spent to deliver each data packet.

$$AED = TD / PR$$

3) Average Hop Count: It shows average number of hops for each data packet.

$$AHC = THC / PR$$

4) Packet Dropping Rate: It shows the number of data packets which were dropped during their journey to destination.

TABLE II
SIMULATION PARAMETERS

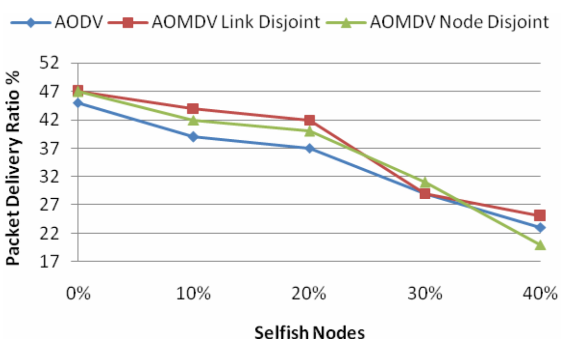
Parameters	Values
Simulation Time	500 Seconds
Space	1000 x 1000
Number of Nodes	50
Pause Time	200 Seconds
Transmit Power	250 m
Connections	25
Traffic Type	CBR
Nodes Speed	20 m/s
Packet Generation Rate	4 packets/s
Packet Size	512 bits
MAC Protocol	802.11
Mobility Model	Random Waypoint
Malicious Nodes	0%,10%, 20%, 30% & 40%

This dropping rate includes the data packets which were dropped due to Type 1 and 2 selfish behaviors.

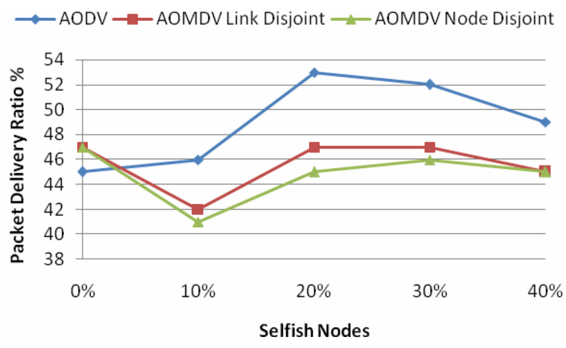
The simulation parameters are given in Table II, all the parameters value are static and only number of selfish nodes is varied between 0% to 40%.

Fig. 2 shows the packet delivery ratio in all types of selfish behaviors. Fig. 2 (a) and (c) shows a kind of similar behavior but with different intensity. AOMDV gives the ratio between 47% when Type1 selfish nodes are 0% but decline to 25% and 20% when selfish nodes are 40% for the link and node disjoint, respectively. AODV achieves 45% delivery ratio while selfish nodes are 0% and achieves 23% delivery ratio in the existence of maximum selfish nodes. In Type3 selfish behavior, delivery ratio is 47% for both link and node disjoint AOMDV when no selfish nodes exist. In the presence of maximum selfish nodes, both link and node disjoint achieve 39% and 40%, respectively. AODV attains lower delivery ratio than both AOMDV options throughout type3 selfish behavior.

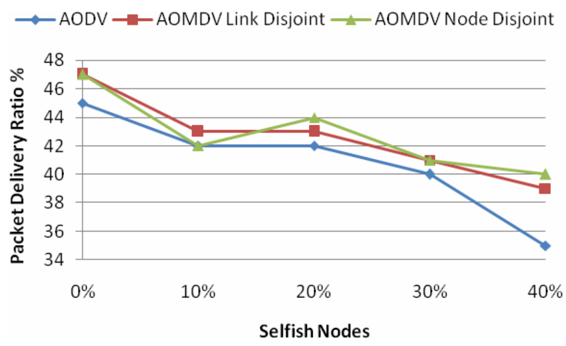
Results are quite different in type2 selfish behavior. AODV gives better delivery ratio than both link and node disjoint options of AOMDV. It is due to the fact that the type2 selfish node stops cooperating completely in any network operation thus such nodes become non-existing nodes. Study [1] shows that AOMDV in comparison to AODV works well in a dense and higher load networks. Type2 selfish nodes basically gradually convert a dense network into sparse network and so degrading the efficiency of AOMDV to such extent.



(a) Type 1



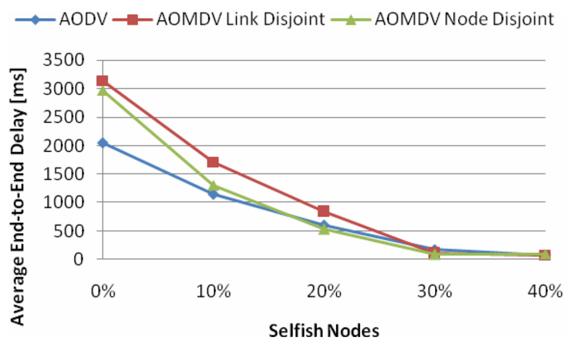
(b) Type 2



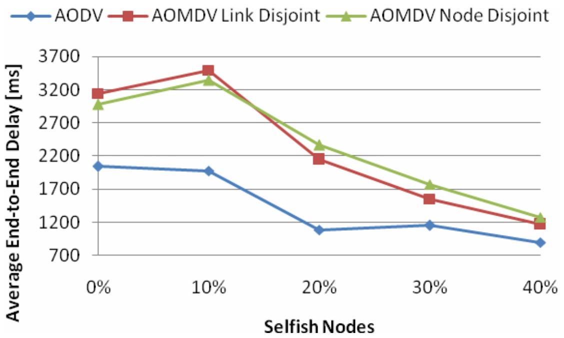
(c) Type 3

Fig. 2 Packet Delivery Ratio

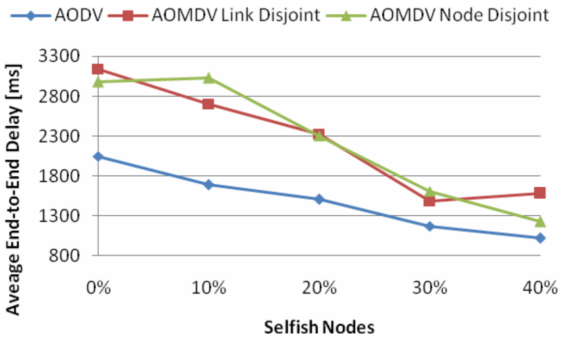
Fig. 3 shows the avg. end-to-end delay which is total delay that all packets took to reach at destination nodes. When selfish nodes are 0%, delivery ratio is also high, it start improving in each type as selfish nodes increase. In type1, delay improves to 95 ms for all protocol configurations because the ratio to successful packet delivery reduces very quickly to below 26% in the existence of maximum selfish nodes. Delay is comparably higher in type3 selfish behavior because the delivery ratio is better. In type2 selfish behavior the delay remains moderate as compared to both type1 and 3 behaviors. In every selfish behavior, delay taken by AODV is better among all protocol configurations. It is because AODV discovers only one path and achieves less packet delivery ratio than AOMDV



(a) Type 1

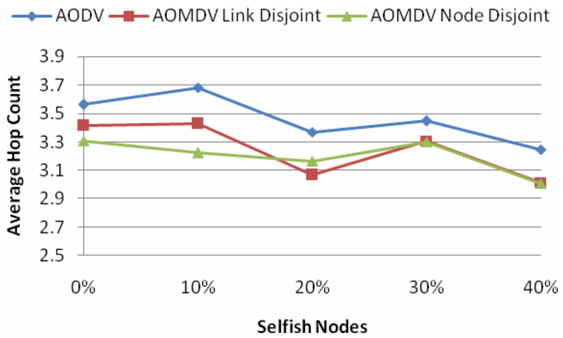


(b) Type 2

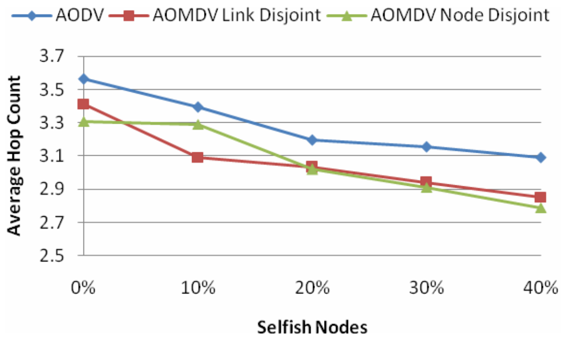


(c) Type 3

Fig. 3 Average End-to-End Delay [ms]



(b) Type 2



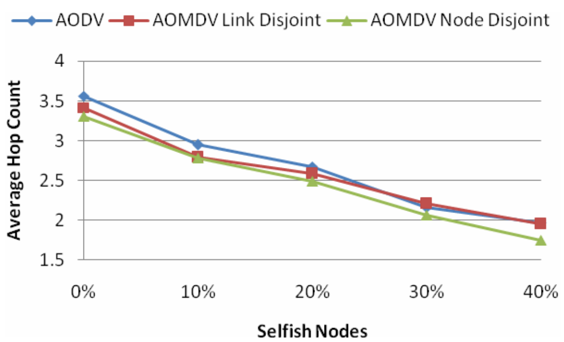
(c) Type 3

Fig. 4 Average Hop Count

Fig. 4 shows the avg. hop count, all packets travelled to successfully reach destination nodes. AODV avg. hop count is higher than AOMDV in each type of selfish behaviors. The reason for this deficiency is that, AOMDV discover multiple paths but uses primarily the shortest one.

In type1 and 3 selfish behaviors the avg. hop count for all protocol configurations, declines with the increase in number of selfish nodes. This decline is associated with the decrease in packet delivery ratio.

In type2 selfish behavior, all protocol configurations are not declining the same way as in type1 and 3. This difference is due to completely non-cooperating selfish nodes. The discovered routes are long and that is why the avg. hop does not decline the same way as in type1 and type3 selfish behaviors.

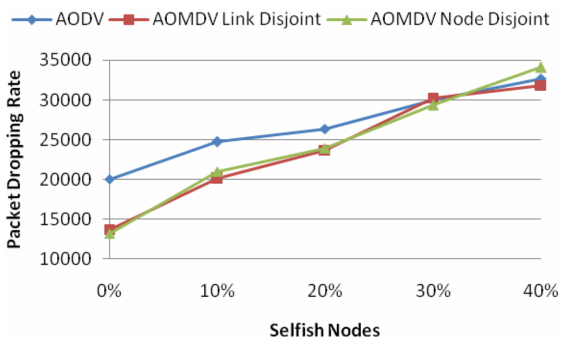


(a) Type 1

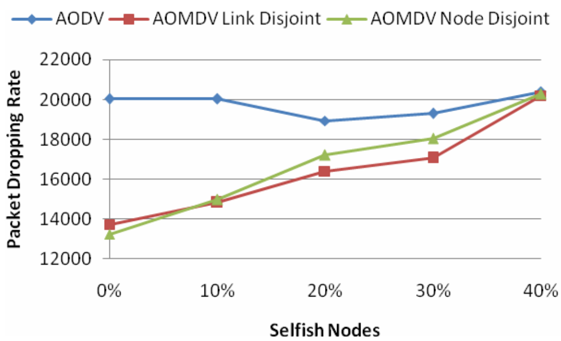
Fig. 5 represents the packet dropping rate in all three types of selfish behaviors. Dropping rate in type1 is almost twice higher than in type3.

Packet dropping rate of AODV at 0% selfish node is higher than AOMDV configurations for all types of selfish behaviors. But in the presence of maximum selfish nodes, the node disjoint and then link disjoint configurations of AOMDV become the frontrunner in dropping the data packets.

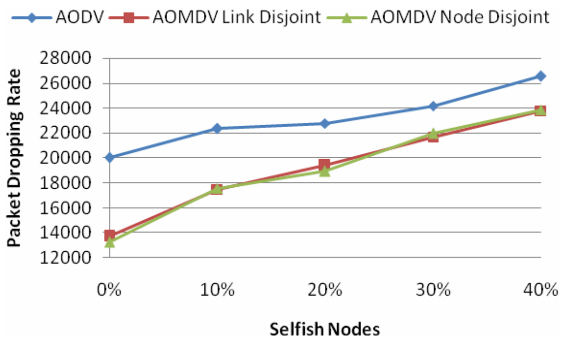
We believe that introducing a secure feedback mechanism on top of multi-path configurations, would provide better results. A feedback mechanism can detect (type1 and 3) selfish behaviors and with the use of multi-path protocol, we can divert the traffic to available alternate path.



(a) Type 1



(b) Type 2



(c) Type 3

Fig. 5 Packet Dropping Rate

V. Conclusion and Future Work

Simulative analysis of single-path and multi-path routing protocol in presence of selfish behaviors, leads us to following conclusions:

- Multi-path protocol i.e. AOMDV, can also work better than single-path i.e. AODV routing protocol in presence of selfish behaviors.
- Multi-path link disjoint path option in presence of selfish behaviors, is also more efficient and provide more number of paths than its counterpart the node disjoint path option between any given pair of nodes.
- Feedback mechanisms [10] are believed to be a good choice to detect and isolate the type1 and type3 misbehaving nodes. Link disjoint option can be a good choice to propose a secure feedback mechanism on to it thus one can blame the link instead a pair of nodes for the selfish behavior.
- The only way to mitigate type2 selfish behavior is to convince such selfish nodes to cooperate. Trust based system is needed to convince type2 selfish behaviors.

Keeping in view the above findings, we conclude that the link disjoint path option of multi-path routing protocol overall performs better than single-path or node disjoint path option of multi-path routing protocol in the presence of selfish nodes. And we consider that link disjoint configuration of AOMDV, can be a good choice to work with feedback mechanism to mitigate type1 and 3 selfish behaviors.

As a future work, we are working to propose a secure feedback mechanism that work on top of multi-path link disjoint routing protocol.

Acknowledgment

This work is supported by the National High Technology Research and Development Program of China under Grant No.2009AA01Z418, China Postdoctoral Science Foundation No.20090460192 and HEC Pakistan.

References

[1] G. Parissidis, V. Lenders, M. May, and B. Plattner, “Multi-path routing protocols in wireless mobile ad hoc networks: A quantitative comparison”, In *NEW2AN*, 2006.
[2] Marina. M.K, Das. S.R., “On-Demand Multipath Distance Vector Routing in Ad Hoc Networks”, Proceedings of the International Conference for Network Protocols, 2001
[3] Marina. M.K, Das. S.R., “ Ad Hoc On-Demand Multipath Distance Vector Routing”, Wireless Communication and Mobile Computing, Vol. 6, Wiley Inter Science, 2006
[4] C. Perking and etl, “Ad Hoc On-Demand Distance Vector (AODV) Routing”, RFC-3561, The Internet Engineering Task Force, 2003
[5] S. M. Bo and etl, “A Performance Comparison of Wireless Ad Hoc Network Routing Protocols under Security Attack”, Proceedings of the Third International Symposium on Information Assurance and Security, 2007
[6] P. Michiardi and R. Molva, “Simulation-based Analysis of Security Exposures in Mobile Ad Hoc Networks”, European Wireless Conference, 2002
[7] Network Simulator – 2 available at http://www.isi.edu/nsnam/ns.
[8] Sangi A.R, Jianwei Liu and Likun Zou, “A Performance Analysis of AODV Routing Protocol under Combined Byzantine Attacks in MANETs”, Proceedings of CISE, Wuhan, China, 2009
[9] S. Corson and J. Macker, “MANET Routing Protocol Performance Issues and Evaluation Considerations”, RFC-2501, The Internet Engineering Task Force, 1999
[10] L. Zhao and J. Delgado-Frias, “Multipath Routing Based Secure Data Transmission in Ad Hoc Networks”, Proceedings of WiMob, 2006