ISSN: 0974-6471, Vol. 10, No. (3) 2017, Pg. 593-596

Oriental Journal of Computer Science and Technology

Journal Website: www.computerscijournal.org

Comparative Study of AODV and ODMRP Routing Protocols

JITENDRA SONI* and KOKILA UIKEY

[1]Assistant Professor, Department of Computer Engineering, Institute of Engineering & Technology, DAVV, Indore (M.P), India.
[2]Department of Information Technology, Institute of Engineering & Technology, DAVV, Indore (M.P), India.

Abstract

Mobile ad-hoc Network [MANET] is the collection of mobile nodes deployed with the short-lived purpose. It is the most innovative and useful variety which provide the facility to establish communication without the prerequisite of any infrastructure. Here, wireless communication medium is usually used for communication and connection establishment purpose. Generally, it is deployed with mobile nodes but can be used for stationary design also. Open nature communication makes it vulnerable for several security threats. This paper has considered the simulation of AODV and ODMRP using Qualnet 5.2 simulator.

Article History

Received: 13 June 2017
Accepted:28 June 2017

Keywords

AODV;
ODMRP;
Qualnet 5.2.

Introduction

Mobile nodes are also combination of few components such as processing unit, storage memory along with transmission and receiving capability. MANET provides special phenomena to provide different level of network services with optimum efforts. Although, MANET doesn't rely on any infrastructure, but route discovery is also important practice for communication. Routing in MANET plays very important and crucial role in communication. It helps to dynamically discover the route instead of using priorly discovered path. The routing techniques can be defined as the approach to discover the route among mobile nodes. Basically they are classified according to their capabilities and nature of operation. It is popularly known as proactive and reactive routing protocols. Proactive routing protocols are traditional approaches known as distance-vector and link-state algorithms.

Subsequently, reactive routing protocols are latest approaches names as AODV, DSR, ODMRP, DYMO etc. Traditional routing protocols perform route discovery at time of establishment of network. It is very time effective routing protocols but suffer with the issue of extra resource consideration. It performs route discovery process for every route which may not used any time during the communication.

CONTACT Jitendra Soni ✉ jitendrasoni2017@gmail.com Department of Computer Science, Institute of Engineering & Technology, DAVV, Indore (M. P.), India.

To link to this article: http://dx.doi.org/10.13005/ojcst/10.03.06

These limitations explore the need of optimum energy consumption based routing protocols. Here, AODV, DSR are the kind of protocols who discover the routes only when they get the demand of communication. So, request based route discovery reduce the wastage resource consumption along with optimum resource consumption. The best part of these reactive routing protocols is they are very adaptive and can manage themselves with the variation in network topology[1].

Study of routing protocols observes that open network and wireless nature make it vulnerable for several security threats. Subsequently single path may become overwhelming when the environment does not support the communication.

On demand multi-path routing protocols help to establish communication in more effective ways. It finds multiple paths for each and every communication link instead of single route establishment. Thus this new route discovery and repairing mechanism only needed the configuration for multi-casting instead on single route discovery. This is route is a mesh based network uses group forwarding concept. It maintains the membership group to perform the multi-casting features[2].

All such protocols concludes that all are good for communication purpose and very much suitable for MANET but suffers with the issue of susceptibility and security threats. According to study, many security threats can be observe due to this vulnerable nature of routing protocols. Here, this paper has perform the study of AODV and ODMRP routing protocol and proposed different solution to diagnose and mitigate the security threats.

Security Issues

Security is one of the leading and important concerns of any network. It becomes more crucial in the scenario of wireless communication. Open nature and vulnerable situation make it prone and susceptible for several security threats. Enemy and attackers attempt to exploit the loopholes of mobile nodes to apply. Another way, vulnerabilities into existing routing protocols and ad-hoc system make it more susceptible and opportunistic for security threats[5]. A lot of loopholes have been observed in AODV and ODMRP routing protocol some of listed below;

1. Source node can be modified by the attacker after modified the RREQ packet during communication.
2. Due to broadcasting nature, analyzing can be done easily which may lead for packet tracing and capturing.
3. Malicious nodes may attempt to route diversion approach to affect the performance by alteration into hop count values. It may lead for packet loss and degrading the communication performance.
4. Unwanted flooding and overwhelming packet sending may be big reason for resource draining approach.
5. In few approach, attacker may attempt to perform traffic analysis and alter the node information to compromise the network privacy.
6. Selective forwarding or dropping is also another thread into wireless network.
7. Now days, passive attacks are becoming more severe than active attack where attacker node directly attempt to exploit the capabilities of mobile node by performing undesirable activity.
8. Jellyfish is one of the hybrid kind of attack where attacker node alter the network situation. A detailed study of jellyfish attack is explained into next paper[3].

Problem Domain

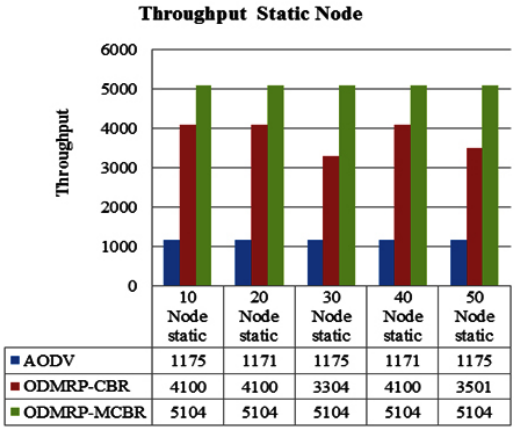
The study of AODV and ODMRP routing protocols observe that both have important significance into MANET. Study of both routing protocols observes that open nature and zero security models make them vulnerable for various security threats. It has been observe that enemy exploit such issues and attempt to compromise the privacy and confidentiality of network communication.

Subsequently, secure routing protocols are designed to avoid such situations but do not cover all situations and manage such things. Their concern is to maintain authentication, integrity and confidentiality along with non-repudiation but do not cover all kinds of security. ODMRP and AODV vulnerabilities may easily manipulate malicious node to destroy the network routing communication.

Solution Domain

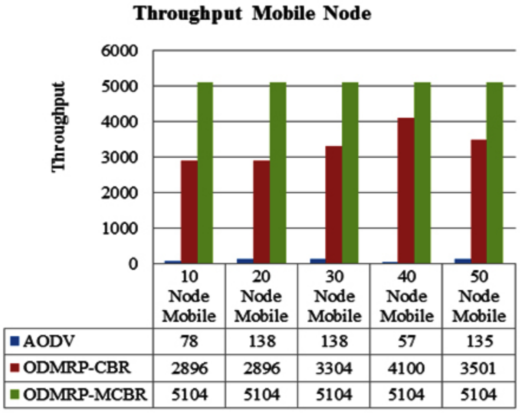
The complete experimental scenarios are classified in below category. A brief description of both is cited below:

Initially, a comparative study for the performance of AODV and ODMRP with AODV has been made. This experimental analysis has been done for 10,20,30,40 and 50 nodes for static and mobile conditions. It has been observed on basis of throughput, PDR, End to End delay and Jitter. A comparative study of the complete work is shown in below graphs.



	10 Node static	20 Node static	30 Node static	40 Node static	50 Node static
■ AODV	1175	1171	1175	1171	1175
■ ODMRP-CBR	4100	4100	3304	4100	3501
■ ODMRP-MCBR	5104	5104	5104	5104	5104

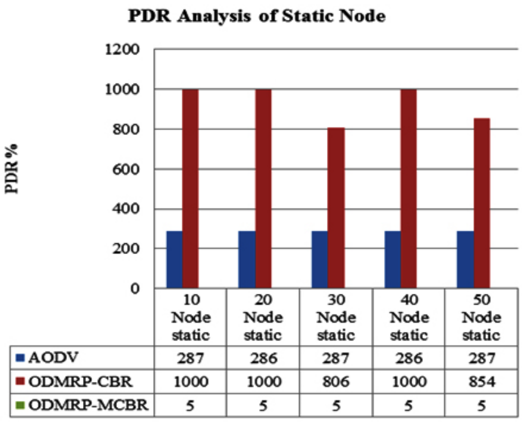
Fig. 1: Throughput Analysis of Static Node



	10 Node Mobile	20 Node Mobile	30 Node Mobile	40 Node Mobile	50 Node Mobile
■ AODV	78	138	138	57	135
■ ODMRP-CBR	2896	2896	3304	4100	3501
■ ODMRP-MCBR	5104	5104	5104	5104	5104

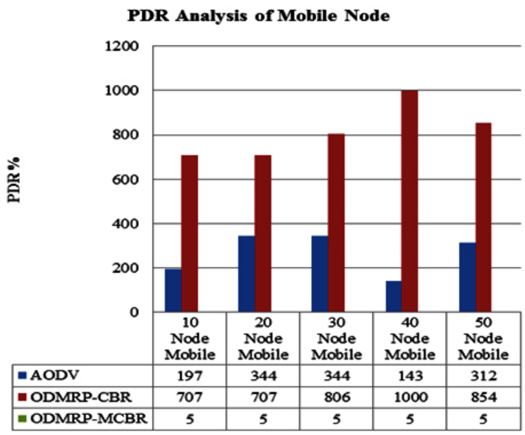
Fig. 2: Throughput Analysis of Mobile Node

- PDR of AODV and ODMRP routing protocols for static node and mobile node are given:



	10 Node static	20 Node static	30 Node static	40 Node static	50 Node static
■ AODV	287	286	287	286	287
■ ODMRP-CBR	1000	1000	806	1000	854
■ ODMRP-MCBR	5	5	5	5	5

Fig. 3: PDR Analysis of Static Node

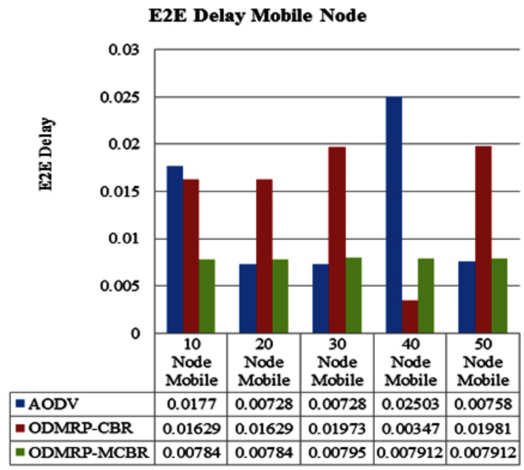


	10 Node Mobile	20 Node Mobile	30 Node Mobile	40 Node Mobile	50 Node Mobile
■ AODV	197	344	344	143	312
■ ODMRP-CBR	707	707	806	1000	854
■ ODMRP-MCBR	5	5	5	5	5

Fig. 4: PDR Analysis of Mobile Node

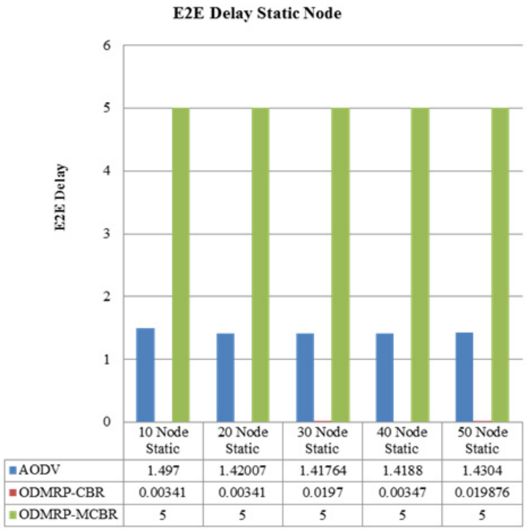
Experimental Analysis

Throughput of AODV and ODMRP protocols for



	10 Node Mobile	20 Node Mobile	30 Node Mobile	40 Node Mobile	50 Node Mobile
■ AODV	0.0177	0.00728	0.00728	0.02503	0.00758
■ ODMRP-CBR	0.01629	0.01629	0.01973	0.00347	0.01981
■ ODMRP-MCBR	0.00784	0.00784	0.00795	0.007912	0.007912

Fig. 5: End to End Analysis of Mobile Node



	10 Node Static	20 Node Static	30 Node Static	40 Node Static	50 Node Static
🟦AODV	1.497	1.42007	1.41764	1.4188	1.4304
🟥ODMRP-CBR	0.00341	0.00341	0.0197	0.00347	0.019876
🟩ODMRP-MCBR	5	5	5	5	5

Fig. 5: End to End Analysis of Mobile Node

static node and mobile node are given:

- End to end delay of AODV and ODMRP routing protocols for mobile node are given:

CONCLUSION

The complete work concludes that better performance has been observed in static node rather than mobile node scenario. The complete experimental analysis generates some observations which are listed below;

1. In static or mobile AODV based network, enhancement into nodes does not give impact on throughput. Only slight variation is observed.
2. In static AODV based network, enhancement into nodes raise the PDR but zero variation has been observed into mobile nodes.
3. In terms of End to End Delay nominal variation has been observed for static node but vast differences has been recorded for mobile nodes.
4. In static or mobile ODMRP based network, enhancement into nodes does not give impact on throughput. Only slight variation is observed
5. In static ODMRP based network, enhancement into nodes raise the PDR but zero variation has been observed into mobile nodes.
6. In terms of End to End Delay nominal variation has been observed for static node but vast differences has been recorded for mobile nodes.

Refernces

1. Md. Saiful Azad, Farhat Anwar, Md. Arafatur Rahman, Aisha H. Abdalla, Akhmad Unggul Priantoro and Omer Mahmoud Performance, ”Comparison of Proactive and Reactive Multicast Routing Protocols over Wireless Mesh Networks”, *IJCSNS International Journal of Computer Science and Network Security*, VOL.**9** No.6, June 2009.
2. Sung-JuLee, Mario Gerla, and Ching-Chuan Chiang, “On-Demand Multicast Routing Protocol”, IEEE 2015.
3. Manjot Kaur 1, Malti Rani 2, “A Novel Defense Mechanism via Genetic Algorithm for Counterfeiting and Combating Jelly Fish Attack in Mobile Ad- Hoc Networks”, IEEE, 2014.
4. Siddlingappagouda Biradar, Pralahad Kulkarni, “Enhancing the quality of service using M-AODV Protocol in MANETs", IEEE, 2015.
5. Gauri Kalnoor, Jayshree Agarkhed, “QOS based multipath routing for intrusion detection of sinkhole attack in wireless network”, *International conference on circuit, Power and computing technologies* ICCPCT 2016.
6. I.Aad and J.P.Hubaux , E.W. Knightly, “Impact of Denial of Service Attacks on Ad Hoc Networks” , IEEE/ACM Transactions on Networking , vol.**16** pp.791-802, Aug 2008
7. C.Jinshong Hwang, Ashwani Kush, Ruchika, “Performance Evaluation of Manet Using Quality of Service Metrics”, *Fifth international conference on Innovative Computing Technology* (INTECH 2015) 978-1-4673-7551-1/15/$31.00© 2015 IEEE.