ORIENTAL JOURNAL OF
COMPUTER SCIENCE & TECHNOLOGY
An International Open Free Access, Peer Reviewed Research Journal
Published By: **Oriental Scientific Publishing Co., India.**
www.computerscijournal.org

ISSN: 0974-6471
March 2017,
Vol. 10, No. (1):
Pgs. 76-81

Packet Drop Attack Detection and Prevention Using Rank Base Data Routing in MANET

RAJAN PATEL[1]*,SUMAIYA VHORA[2] and NIMISHA PATEL[3]

[1]Dept. of Computer Engineering, Sankalchand Patel College of Engineering,
S.P. University, Visnagar, 384351,India.
[2]Finilite Technologies, Ahmedabad, India.
[3]Dept.of Computer Engineering, Sankalchand Patel College of Engineering,
S.P. University, Visnagar, 384351, India.
*Corresponding author E-mail: rajan_g_patel@yahoo.com

http://dx.doi.org/10.13005/ojcst/10.01.10

(Received: January 07, 2017 Accepted: February 15, 2017)

ABSTRACT

Packet drop (grayhole/blackhole) attack is occurs at a network layer to discard the packets in MANET. It is essential to detent and prevent this attack for improving performance of network. This article provides the packet drop attack detection and prevention using RBDR (Rank Based Data Routing) for AOMDV routing protocol. The fields of RBDR are generated with routing information and analysis behavior of network for detecting the malicious paths. The scheme is to identify the malicious paths for preventing the packet drop attack and also able to find the trusted multiple disjoint loop free routes for data delivery in MANET. The simulation is conducted in NS2 using AOMDV reactive routing protocol and analyze with packet loss delivery, average end-to-end delay and packet delivery ratio. The proposed technique can reduce the effect of packet drop attack.

Keywords: AOMDV, Blackhole/Grayhole attack, Rank base data routing, Malicious path.

INTRODUCTION

In MANET, various attacks are possible at different layers. Among them some attacks are possible because of malicious and/or selfish behavior of nodes[1]. At network layer, behavior of malevolent joins like they are claiming itself having a best path (attracting to source node by claiming maximum destination sequence number, minimum hop count etc). Thus sender node may select to send data all via that malevolent node and according to property of malevolent node, they may discards the traffic: if the node discard the all traffic (data) called blackhole attack while in grayhole attack malicious threads discards some of them routing packets[2]. As per the behavior of blackhole or grayhole attack, these attacks are may belong the under the category of packet drop attacks. This article provides the packet drop attack detection and prevention using RBDR (Rank Based Data Routing) for AOMDV[3] routing protocol.

The article is structured as follows: section 2 presents the comparison of a variety of proposed techniques describing the correlated work of preventing and detecting the packet drop attack. Section 3 discusses about proposed scheme based on RBDR. Section 4 represents the simulated results. Finally, concluded in last section.

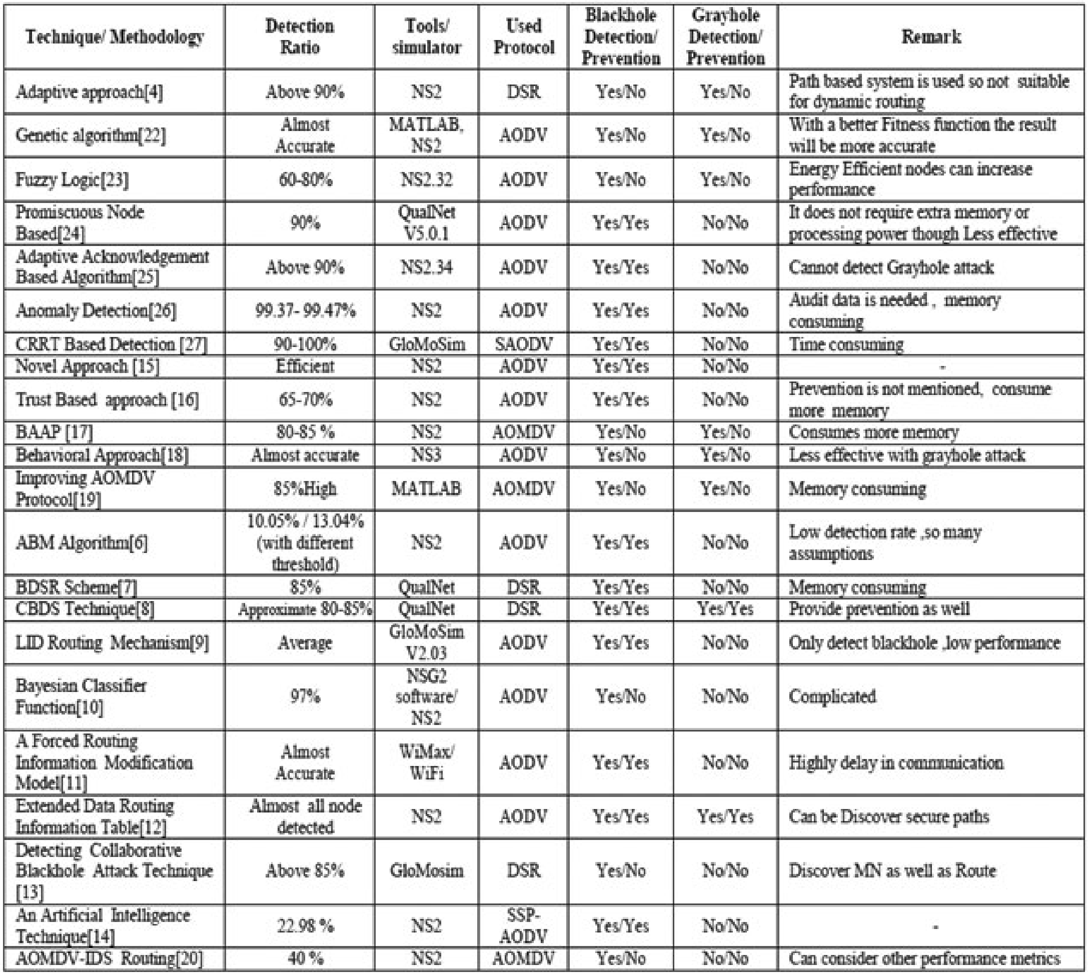
Related Work

With the literature review, table 1[5] represents the comparison based on detection ratio, used tools/simulator, specific technique/method for blackhole / grayhole attack detection and prevention and used routing protocol.

Proposed Work based on RBDR

In our previous paper we have identify RBDR scheme[5] and in this article we have simulate the proposed work using RBDR. RBDR record is used to analysis of malicious behavior in network. RBDR contains five fields illustrated in table II: routing paths, destination sequence number, hop count, route rank and timer. Routing paths field represents the set of paths which claims that it contains route to destination. Destination sequence number is the value which is return with RREP (Route Reply) packet as a destination sequence number of specific route. Hop count field indicates a specific number which is taken by a route to reach at destination. Route Rank field has a digit value which indicates the rank of each path according to constant unchanged destination sequence number and lower value of hop count. It has a value N=1, 2, 3…, n. The less ranked route, assign more priority. As shown in figure 1, S (Source node) wants to communicate with node D (Destination node). M, N and O the intermediate neighbor nodes for A to deliver and find the route to reach the node D.

Table 1: Packet Drop Attack Detection / Prevention Techniques



Technique/ Methodology	Detection Ratio	Tools/ simulator	Used Protocol	Blackhole Detection/ Prevention	Grayhole Detection/ Prevention	Remark
Adaptive approach[4]	Above 90%	NS2	DSR	Yes/No	Yes/No	Path based system is used so not suitable for dynamic routing
Genetic algorithm[22]	Almost Accurate	MATLAB, NS2	AODV	Yes/No	Yes/No	With a better Fitness function the result will be more accurate
Fuzzy Logic[23]	60-80%	NS2.32	AODV	Yes/No	Yes/No	Energy Efficient nodes can increase performance
Promiscuous Node Based[24]	90%	QualNet V5.0.1	AODV	Yes/Yes	No/No	It does not require extra memory or processing power though Less effective
Adaptive Acknowledgement Based Algorithm[25]	Above 90%	NS2.34	AODV	Yes/Yes	No/No	Cannot detect Grayhole attack
Anomaly Detection[26]	99.37- 99.47%	NS2	AODV	Yes/Yes	No/No	Audit data is needed , memory consuming
CRRT Based Detection [27]	90-100%	GloMoSim	SAODV	Yes/Yes	No/No	Time consuming
Novel Approach [15]	Efficient	NS2	AODV	Yes/Yes	No/No	-
Trust Based approach [16]	65-70%	NS2	AODV	Yes/Yes	No/No	Prevention is not mentioned, consume more memory
BAAP [17]	80-85 %	NS2	AOMDV	Yes/No	Yes/No	Consumes more memory
Behavioral Approach[18]	Almost accurate	NS3	AODV	Yes/No	Yes/No	Less effective with grayhole attack
Improving AOMDV Protocol[19]	85%High	MATLAB	AOMDV	Yes/No	Yes/No	Memory consuming
ABM Algorithm[6]	10.05% / 13.04% (with different threshold)	NS2	AODV	Yes/Yes	No/No	Low detection rate ,so many assumptions
BDSR Scheme[7]	85%	QualNet	DSR	Yes/Yes	No/No	Memory consuming
CBDS Technique[8]	Approximate 80-85%	QualNet	DSR	Yes/Yes	Yes/Yes	Provide prevention as well
LID Routing Mechanism[9]	Average	GloMoSim V2.03	AODV	Yes/Yes	No/No	Only detect blackhole ,low performance
Bayesian Classifier Function[10]	97%	NSG2 software/ NS2	AODV	Yes/No	No/No	Complicated
A Forced Routing Information Modification Model[11]	Almost Accurate	WiMax/ WiFi	AODV	Yes/Yes	No/No	Highly delay in communication
Extended Data Routing Information Table[12]	Almost all node detected	NS2	AODV	Yes/Yes	Yes/Yes	Can be Discover secure paths
Detecting Collaborative Blackhole Attack Technique [13]	Above 85%	GloMosim	DSR	Yes/No	No/No	Discover MN as well as Route
An Artificial Intelligence Technique[14]	22.98 %	NS2	SSP-AODV	Yes/Yes	No/No	-
AOMDV-IDS Routing[20]	40 %	NS2	AOMDV	Yes/No	No/No	Can consider other performance metrics

The B node is malicious node in the path S-M-B-D. After getting first routing reply of AOMDV packet for route requested AOMDV packet by node A, every possible multiple disjoint loop free paths is store for destination at the field of routing path in RBDR record. All destination sequence number related to path is recorded in field of destination sequence number of RBDR record.

Suppose Destination sequence numbers are 580, 200,300 with routing paths S-M-B-D, S-N-P-D, S-O-R-D respectively as shown in table II. Again propagate AOMDV RREQ with a higher number of destination sequence number (include a value greater than all received destination sequence number). If any route claims greater value than previous destination sequence number it is clear that the particular route having malicious node. According to lower hop count and constant unchanged destination sequence number assign ranks to every routes which are in RBDR record. The complete flow of proposed work is illustrated in figure 2 which will be implemented in NS2[28] using AOMDV routing protocol.

Table 2: RBDR

Routing Path	Destination Sequence Number	Hop Count	Route Rank	Timer
S-M-B-D	580	2	3	2^3
S-N-P-D	200	2	1	0
S-O-R-D	300	3	2	0

RESULTS

This proposed scheme is used NS2 using AOMDV reactive routing protocol to analyze the packet drop attack detection and prevention. According to table 3, the network is analyze with Packet loss delivery, average end-to-end delay and packet delivery ratio with considering the number of nodes with area of 1000m × 1000m.

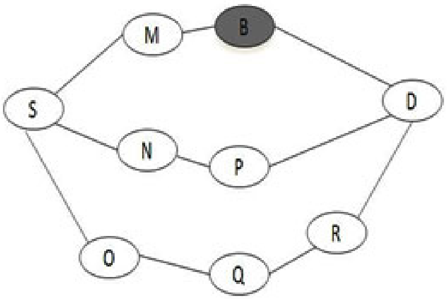
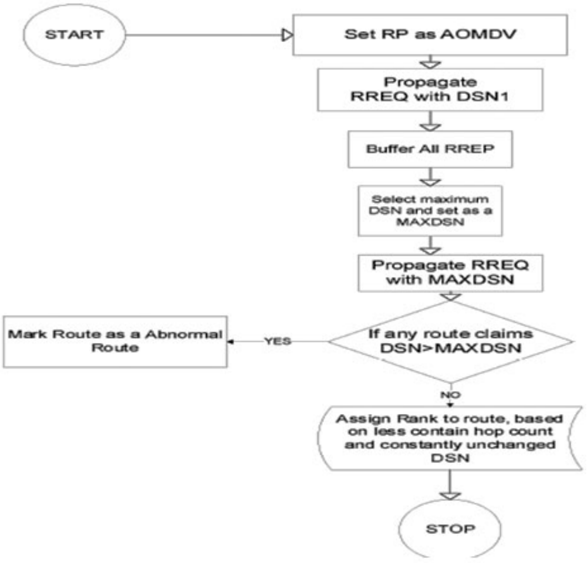


Fig. 1: Routing Scenario


START
Set RP as AOMDV
Propagate RREQ with DSN1
Buffer All RREP
Select maximum DSN and set as a MAXDSN
Propagate RREQ with MAXDSN
Mark Route as a Abnormal Route
YES
If any route claims DSN>MAXDSN
NO
Assign Rank to route, based on less contain hop count and constantly unchanged DSN
STOP

RP: Routing Protocol,DSN: Destination Sequence Number, MAXDSN: Maximum DSN

Fig. 2: Detecting and Preventing of Packet Drop Attack

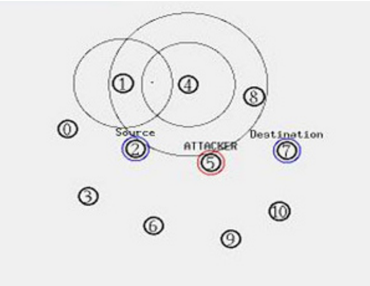


Fig. 3: Simulator Environment

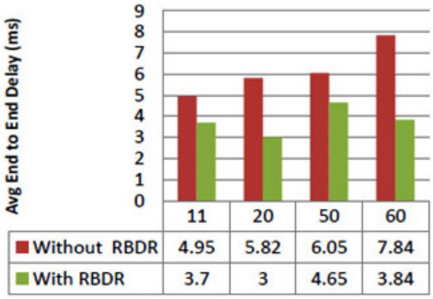


Fig. 4(a): End-to-End Delay

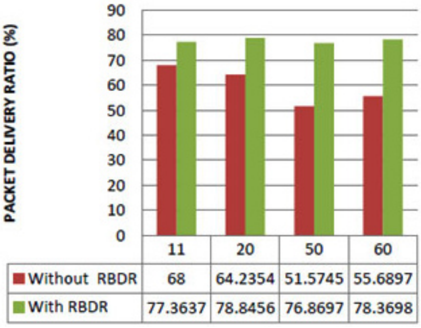


Fig. 4(b): Packet Delivery Ratio

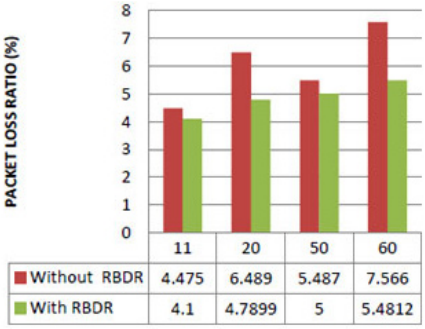


Fig. 4(c): Packet Loss Ratio

Table 3: Simulation Parameters

Parameter	Value
Simulator	NS-2(Version 2.35)
Channel type	Wireless
Radio-propagation model	Propagation/TwoRay Ground
Network interface type	Phy/WirelessPhyExt
MAC Type	Mac/802_11
Interface queue Type	Queue/DropTail /PriQueue
Link layer type	LL
Antenna model	Antenna/OmniAntenna
Topography dimension	1000X1000
Max packet in ifq	11
Traffic Type	UDP, CBR
Routing Protocols	AOMDV

The analysis is conducted using three performance metrics and according to results, the detection ratio is good and also improve the packet delivery ratio. Figure 3 shows the simulation environment with presence of attacker nodes where node 2 is the source node, 7 is the destination node and 5 is an attacker node.Figure 4(a) illustrated reduction of end-to-end delay because of ignoring the malicious path,figure 4(b) also represents improvement of packet loss and figure 4(c) shows the improvement of packet delivery ratio with considering the RBDR in proposed scheme and without RBDR configuration in AOMDV routing protocol.

CONCLUSION

Due to nature of packet drop attack at network layer, drop attacks are either blackhole attack or grayhole attack. With the help of RBDR based scheme, the network behaviour can detect and prevent packet drop attack at network layer for MANET. Hence the network performance and security are increase in MANET. The proposed solution is able to find the trusted path for data delivery. The proposed work is implemented in network simulator NS2 with AOMDV routing protocol with the metrics such as packet delivery ratio, end-to-end delay and packet loss.

REFERENCES

1. http://en.wikipedia.org/wiki/Mobile_ad_hoc_network.
2. Packet drop attack: http://en.wikipedia.org/wiki/Packet_drop_attack
3. Mahesh K. Marina, and Samir R. Das, Ad Hoc On-Demand Multipath Distance Vector Routing, W*ireless communications and mobile computing*, pp. 6:969–988, (2006).
4. Jiwen Cai, Ping Yi, Jialin Chen, Zhiyang Wang, and Ning Liu, An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network, 24th IEEE International Conference on Advanced Information Networking and Applications, pp. 775 - 780, 20-23 (April 2010).
5. Sumaiya vhora,Rajan Patel and Nimisha Patel, Rank Base Data Routing (RBDR) Scheme using AOMDV: A Proposed Scheme for Packet Drop Attack Detection and Prevention in MANET, International Conference on Electrical, Computer and Communication Technologies, pp. 784-788, (March 2015)
6. Ming-Yang Su, Kun-Lin Chiang, and Wei-Cheng Liao, Mitigation of Black-Hole Nodes in Mobile Ad Hoc Networks, International Symposium on Parallel and Distributed Processing with Applications, pp. 162 – 167, (September 2010).
7. Po-Chun Tsou, Jian-Ming Chang, Yi-Hsuan Lin, Han-Chieh Chao, and Jiann-Liang Chen, Developing a BDSR Scheme to Avoid Black Hole Attack Based on Proactive and Reactive Architecture in MANETs, 13th International Conference on Advanced Communication Technology (ICACT), pp. 755 – 760, (February 2011).
8. Jian-Ming Chang, Po-Chun Tsou, Han-Chieh Chao, and Jiann-Liang Chen, “CBDS: A Cooperative Bait Detection Scheme to Prevent Malicious Node for MANET Based on Hybrid Defense Architecture, 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), pp. 1 – 5, (March 2011).
9. Maha Abdelhaq, Sami Serhan, Raed Alsaqour, and Rosilah Hassan, A Local Intrusion Detection Routing Security over MANET Network, International Conference on Electrical Engineering and Informatics, pp. 1-6, (July 2011).
10. Myungsook Klassen, and Ning Yang, Anomaly Based Intrusion Detection in Wireless Networks UsingBayesian Classifier, IEEE 5th International Conference on Advanced Computational Intelligence (ICACI), pp. 257 - 264, (October 2012).
11. Muhammad Raza, and Syed Irfan Hyder, A Forced Routing Information Modification Model for Preventing Black Hole Attacks in Wireless Ad Hoc Network, Proceedings on 9th International Conference on Applied Sciences & Technology (IBCAST) Islamabad, Pakistan, pp. 418 - 422, (January 2012).
12. Gundeep Singh Bindra, Ashish Kapoor, Ashish Narang, and Arjun Agrawal, Detection and Removal of Co-operative Blackhole and Grayhole Attacks in MANETs, International Conference on System Engineering and Technology, pp. 1 - 5, (September 2012).
13. Isaac Woungang, Sanjay Kumar Dhurandher, Rajender Dheeraj Peddi, and Issa Traore, Mitigating Collaborative Blackhole Attacks on DSR-Based Mobile Ad Hoc Networks, Springer-Verlag Berlin Heidelberg, pp. 308-323,(October 2013).
14. Khalil I. Ghathwan, and Abdul Razak B. Yaakub, An Artificial Intelligence Technique for Prevent Black Hole Attacks in MANET, Springer International Publishing Switzerland, pp. 121-131, (June 2014).
15. Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala, A Novel Approach for GrayHole and BlackHole Attacks in Mobile Ad-hoc Networks, Second International Conference on Advanced Computing & Communication Technologies, pp. 556 - 560 , (January 2012).
16. Fidel Thachil, and K C Shet, A trust based approach for AODV protocol to mitigate black hole attack in MANET, International Conference on Computing Sciences, pp.

281 – 285, (September 2012).

17. Saurabh Gupta, Subrat Kar, and S Dharmaraja, BAAP: Blackhole Attack Avoidance Protocol for Wireless Network, International Conference on Computer & Communication Technology (ICCCT), (November 2011).

18. Meenakshi Patel, and Sanjay Sharma, Detection of Malicious Attack in MANET A Behavioral Approach, 3rd International Conference Advance Computing, pp. 388 – 393, (February 2013).

19. Bhavna Sharma, Shaila Chugh, and Vismay Jain, Energy Efficient Load Balancing Approach to Improve AOMDV Routing in MANET, Fourth International Conference on Communication Systems and Network Technologies, pp. 187 – 192, (April 2014).

20. Hitesh Gupta, Shivshakti Shrivastav, and Sanjana Sharma, Detecting the DOS Attacks in AOMDV Using AOMDV-IDS Routing, 5th International Conference on Computational Intelligence and Communication Networks, pp. 380 – 384, (September 2013).

21. Jyoti Rani, and Naresh Kumar, Improving AOMDV Protocol for Black Hole Detection in Mobile Ad hoc Network, International Conference on Control, Computing, Communication and Materials (ICCCCM), pp. 1-8, (August 2013).

22. K.S.Sujatha, Vydeki Dharmar, and R.S.Bhuvaneswaran, Design of Genetic Algorithm based IDS for MANET, International Conference on Recent Trends in Information Technology (ICRTIT) pp. 28 – 33, (April 2012).

23. Monita Wahengbam, and Ningrinla Marchang, Intrusion Detection in MANET using Fuzzy Logic, Emerging Trends and Applications in Computer Science (NCETACS) 3rd National Conference, pp. 189 – 192, (March 2012).

24. Pramod Kumar Singh, and Govind Sharma, An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET, 11th International Conference on Trust, Security and Privacy in Computing and Communications, pp. 902 – 906, (June 2012).

25. Sonali P.Botkar, and Shubhangi R.Chaudhary, An Enhanced Intrusion detection System using Adaptive Acknowledgment based Algorithm, Information and Communication Technologies (WICT) World Congress, pp. 606 – 611, (December 2011).

26. Yibeltal Fantahun Alem, and Zhao Cheng Xuan, Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection, Future Computer and Communication (ICFCC) 2nd International Conference, pp. V3-672 - V3-676, (May 2010).

27. Latha Tamilselvan, and V. Sankaranarayanan, Prevention of Blackhole Attack in MANET," 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, (August 2007).

28. Patel Rajankumar, Patel Nimisha, and Pariza Kamboj, A Comparative Study and Simulation of AODV MENET Routing Protocol in NS2 & NS3, IEEE International Conference on Computing for Sustainable Global Development (INDIACom), pp.889-894, (March 2014).