A Scheme for Detection and Prevention of Packet Drop Attacks is Wireless Sensor Networks

OPEN ACCESS

Volume : 6

Special Issue : 1

Month : September

Year: 2018

ISSN: 2321-788X

Impact Factor: 3.025

Citation:
Sathya, J. (2018). A Scheme for Detection and Prevention of Packet Drop Attacks is Wireless Sensor Networks. *Shanlax International Journal of Arts, Science and Humanities*, 6(S1), pp.82–86.

DOI:
https://doi.org/10.5281/zenodo.1410991

J.Sathya
M.Phil, Research Scholar
Morappur Kongu College of Arts and Science, Morappur

Abstract

Packet drop (gray hole/blackhole) attack is occurs at a network layer to discard the packets in MANET. It is essential to detent and prevents this attack for improving the 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 analyzes 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 nodes1. 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 the property of malevolent node, they may discard the traffic: if the node discards the all traffic (data) called blackhole attack while in gray hole attack malicious threads discard some of them routing packets2. As per the behavior of blackhole or gray hole attack, these attacks 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 AOMDV3 routing protocol.

Proposed Work based on RBDR

In our previous paper we have identified RBDR scheme5 and in this article, we have simulated the proposed work using RBDR. RBDR record is used to analysis of malicious behavior in the 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 a route to the destination. Destination sequence number is the value which is return with RREP (Route Reply) packet as a destination sequence number of a specific route. Hop count field indicates a specific number which is taken by a route to reach 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.

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 a routing path in RBDR record. All destination sequence number related to path is recorded in field of destination sequence number of RBDR record.

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

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 route which are in RBDR record. The complete flow of proposed work is illustrated in figure 2 which will be implemented in NS228 using AOMDV routing protocol.

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 analyzed with Packet loss delivery, average end-to-end delay and packet delivery ratio with considering the number of nodes with area of 1000m × 1000m.

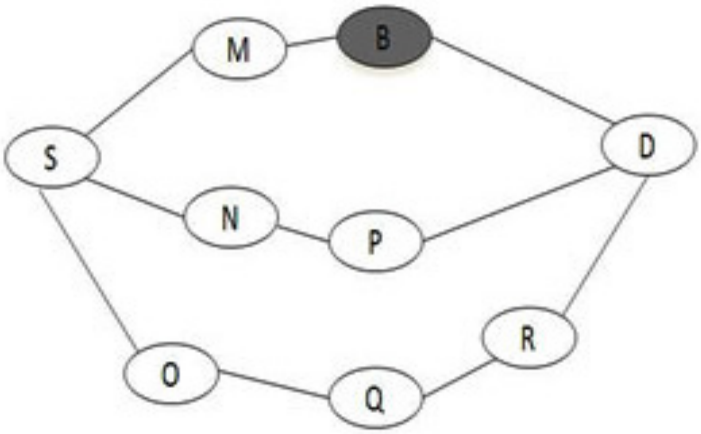


Figure 1 Routing Scenario

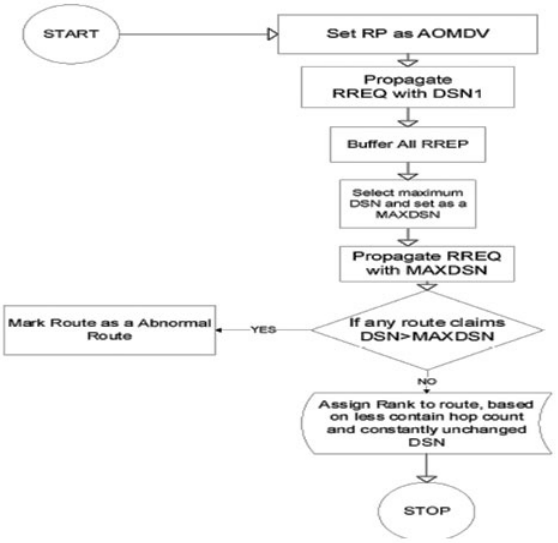


Figure 2 Detecting and Preventing of Packet Drop Attack

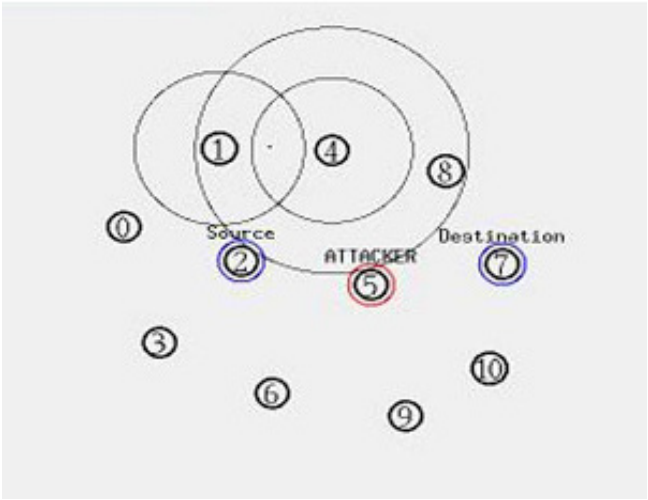
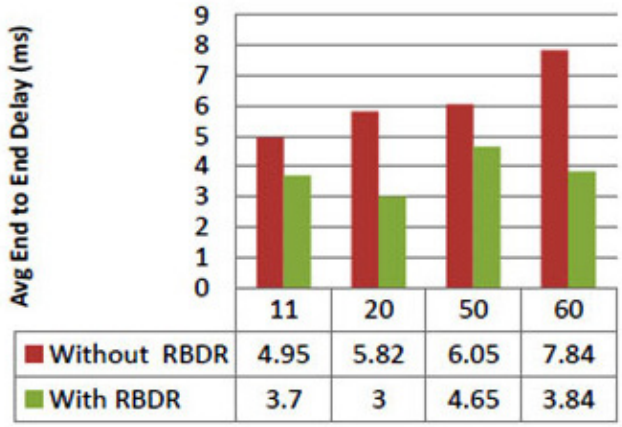
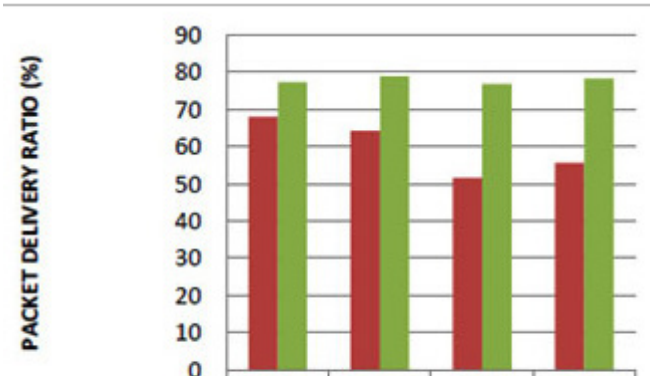


Figure 3 Simulator Environment



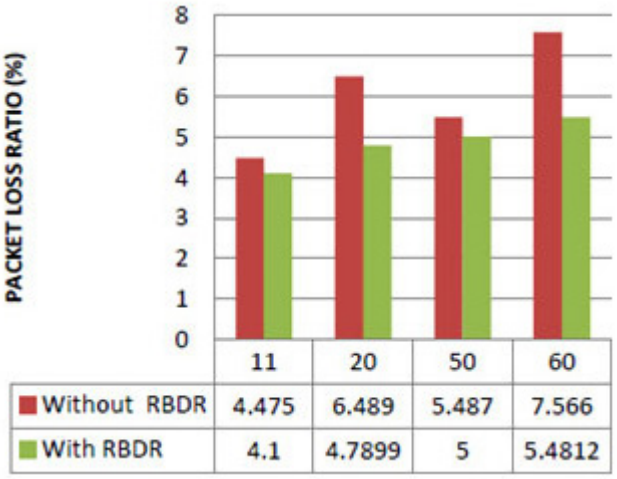
	11	20	50	60
Without RBDR	4.95	5.82	6.05	7.84
With RBDR	3.7	3	4.65	3.84

Figure 4(a) End-to-End Delay



	11	20	50	60
Without RBDR	68	64.2354	51.5745	55.6897
With RBDR	77.3637	78.8456	76.8697	78.3698

Figure 4(b) Packet Delivery Ratio



	11	20	50	60
Without RBDR	4.475	6.489	5.487	7.566
With RBDR	4.1	4.7899	5	5.4812

Figure 4(c) Packet Loss Ratio

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 gray hole 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

http://en.wikipedia.org/wiki/Mobile_ad_hoc_ network.

JiwenCai, Ping Yi, Jialin Chen, Zhiyang Wang., & Ning Liu, (2010), "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.

Mahesh K. Marina., & Samir R. Das, (2006). "Ad Hoc On-Demand Multipath Distance Vector Routing", Wireless communications and mobile computing, pp. 6:969–988,

Ming-Yang Su, Kun-Lin Chiang, and Wei- Cheng Liao, (2010), "Mitigation of Black-Hole Nodes in Mobile Ad Hoc Networks", International Symposium on Parallel and Distributed Processing with Applications, pp. 162 – 167.

Packet drop attack: http://en.wikipedia.org/ wiki/Packet_drop_attack

Sumaiyavhora, Rajan Patel & Nimisha Patel, (2015), "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 Technologie*s, pp. 784-788,

Web Sources

http://www.computerscijournal.org/vol10no1/packet-drop-attack-detection-and-prevention-using-rank-base-data-routing-in-manet/