International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 5 (2015) pp. 12133-12144

http://www.ripublication.com

Performance Analysis and Detection and Correction of Sink Hole Attack In MANET

Sandeep Kumar Arora
Faculty of ECE, Lovely Professional University
sandeep.l6930@lpu.co.in
Nisha Puri
Student,Sai college of Engg.Pathankot
purinisha09@gmail.com
Sanjeev Sharma
Faculty of ECE, Lovely Professional University
Sanjeev.15978@lpu.co.in

Abstract

Mobile Adhoc Network (MANET) is vulnerable to many security issues and network attacks. We presented the comparison of three different routing protocols (AODV, DSR and DSDV) on the basis of different parameters. In this paper, black hole attack is implemented on AODV protocol which reduce the performance parameters of network by exploiting the packet sequence number included in any packet header. The proposed mechanism of Intrusion Detection System (IDS) is also implemented to enhance the network performance. Simulation results using Network Simulator 2(NS2) shows that, in a high mobility environment, malicious node could be detected and the packet delivery ratio has been improved.

Keywords: Packet Delivery Ratio (PDR), Throughput, Normalized Routing Load (NRL), AODV, DSR, Mobile adhoc network (MANET), malicious node, Intrusion Detection System (IDS)

Introduction

A Mobile Ad Hoc Network (MANET) is an infrastructure less and self configuring network, the medium by which they are connected is wireless. In these networks, packet are forwarded between source and destination by intermediate nodes i.e. multi hop, thus they are suited for scenarios where infrastructure is not pre deployed already. MANETS have a dynamic topology i.e. any node can enter or leave a network. Routing protocols can be classified into two categories i.e. Table-driven (proactive) and source initiated (routing) protocols. In proactive routing protocols

each node maintains a routing table having path to every node in the network. These protocols besides updating routing tables periodically also propagate route updates whenever the network topology changes. On the contrary, in reactive routing protocols there is no need for maintaining routing tables. The source node creates a route to destination only when required [1]. Dynamic Source Routing (DSR) and Ad hoc On-Demand Distance Vector (AODV) are source initiated protocols where as Destination Sequence Distance Vector is a proactive protocol. Security is the main issue in MANETS. It may not be possible to detect the malicious behavior of a node or the set of nodes in a network .black hole attack on the AODV routing protocol is one such attack that we have discussed in this paper.

The rest of the paper is organized as follows. Section II discusses the overview of the attacks and prevention. Section III discusses some related work on performance analysis in MANETs. Section IV discusses the research methodology followed. Section V presents the simulations, results and analysis. Section VI concludes the paper and the future work.

Overview of Attacks and Prevention

Malicious Node Attack

A malicious attack can be any action (physical or electronic) taken with the intent compromising legitimate nodes. In a MANET, if malicious nodes are present they pretend themselves to be cooperative but in effect, these nodes either drop the data packets or tamper the data packets they are supposed to pass on. [12]. Malicious attack can conduct denial of service attacks by modifying the message fields. Malicious nodes exhibits behavior like Packet drop, Buffer over flow, Bandwidth consumption etc.

Black Hole Attack

A black hole node exploits a routing protocol. In black hole attack, the attacker node may or may not be authorized in the network i.e. it may be authorized in some other network, when the attacker node receives an route request packet (RREQ) from a neighbouring node it immediately sends route reply (RREP) as having a valid route and a shortest path to an intended destination even though the route is fake thus creating confusion. In this way the attacker node attacks all the route requests. Thus the information packets being received at the attacker node are either being dropped or sent to network where the attacker node is authorized, without informing the source that the data did not reach its intended destination.

Prevention of Black Hole AODV From IDS (Intrusion Detection System)

Intrusion (physical, system or remote) may be from legitimate users of the network or outside the network. Intrusion Detection Systems look for an unauthorized access by checking attack signatures, which usually indicate malicious or suspicious intent. There are various types of IDS and they use various techniques to attain their goal i.e. detecting suspicious traffic. Different ways of classifying IDS

- Anomaly detection
- Signature based misuse
- Host based
- Network based

The primary focus is to identify possible incidents, logging information and reporting attempts about them. Many intrusion detection and prevention systems (IDPSes) can respond to a threat detected by attempting to prevent it from succeeding. [14]

Related Work

Over the past few years new routing protocols for Mobile Adhoc Networks (MANETS) have been proposed but only few have been evaluated for their performance. For instance A.Boukerche[6],Broch,D.Maltz et al [7], presented some evaluations for routing protocols in MANETS. C.Perkins,B.E.Royer et al [9],M. Bouhorma,et al [5] evaluated routing protocols in order to judge their performance using various metrics. V. Kanakaris,D.Ndzi and D.Azzi[4] analyzed performance analysis of routing protocols like AODV, DSR etc and showed their performance. Performance of Any Cast Routing based DSR (ARDSR) and Anycast routing protocol based on AODV (A- AODV) was presented by A. Saeed,L. Khan, N. Shah, et al [3]. Khan.K.[10] gives an efficient distance sequence distance vector (DSDV) routing protocol for MANETS and its performance comparison is done based on various parameters. TamilSelvan,L.and Sankaranarayanan,V. presented the various measures to prevent blackhole attack in MANET. Manikandan, et al [12], the methods to detect the malicious nodes in MANET are described. According to Cao Minh Trang et al [14], a distributed intrusion detection system (IDS) for AODV routing protocol is proposed.

Research Methodology

A Simulation Tool

MANET community uses a simulation research tool known as Network Simulator (NS-2) which is a discrete event simulator. Though there are many such simulators for MANET but most important reasons for using NS2 are that it is easily available and software developing of ns2 is done at a large scale [13]. NS-2 is a sequential simulator. It uses the standard discrete event simulator algorithm. Its input is a description of a network model, and its output is an imaginary history of this network. Different metrics like PDR,NRL etc. can be used to check the performance of a network.

B. Simulation Scenario

Designing simulation scenario is a big task as a detailed simulation results in a sluggish response whereas designing a less detailed simulation can result in incorrect

results. Our approach should be to choose the simulation with appropriate details so that the simulation can give best results in a very short span of time.

C. Performance parameters

1) *Throughput*: Throughput can be defined as the rate at which a message is successfully delivered to the required destination. Throughput is usually measured in bits per sec (bps). AODV, DSR and DSDV routing protocols are evaluated on the basis of their throughput in their respective topologies.
2) *Packet Delivery Ratio*: PDR can be defined as the ratio of number of delivered data packets to the destination. Greater the value of PDR better the performance of the protocol. AODV, DSR and DSDV routing protocols are evaluated on the basis of Packet Delivery ratio (PDR) in their respective topologies.
   ∑ Number of packets received/ ∑ Number of packets sent
3) *Normalized Routing Load*: NRL can be defined as the total number of routing packets transmitted per data packet. AODV, DSR and DSDV routing protocols are evaluated on the basis of NRL in their respective topologies.

Simulations, Results and Analysis

Based on the simulation parameters listed in Table I, three protocols (AODV, DSDV and DSR) have been evaluated for their performance.

Table 1: Simulation Parameters

Simulation Area	1800 x 1840
Simulation Time	25s
Channel Type	Channel/Wireless Channel
Antenna Model	Omni Antenna
Radio Propagation Model	Two Ray Ground
Number of Nodes	20,30,40
Number of Blackhole Nodes	1
Number of Malicious Nodes	1
Number of ids Nodes	1
Packet Size	512 Bytes
Traffic Type	Constant Bit Rate (CBR)
Mobility	Random Waypoint (RWP)

Table 2: Comparison Of Aodv, Dsdv And Dsr Protocols On The Basis Of Qos

Protocol	AODV			DSDV			DSR		
No. of nodes	20	30	40	20	30	40	20	30	40
Throughput	114.71	53.68	62.48	59.49	127.91	109.92	146.941	140.14	132.35
Normalized Routing Load	5.714	3.783	5.032	1.407	1.0	1.587	0.166	0.827	2.216
Packet Delivery Ratio	100	98.70	100	67.04	70.14	56.18	81.62	69.72	64.62

According to table II, DSR routing protocol has maximum throughput and the same is illustrated in the graphical simulation. AODV routing protocol has maximum normalized routing load and packet delivery ratio. Therefore, according to these parameters AODV routing protocol's performance is better than DSR and DSDV.

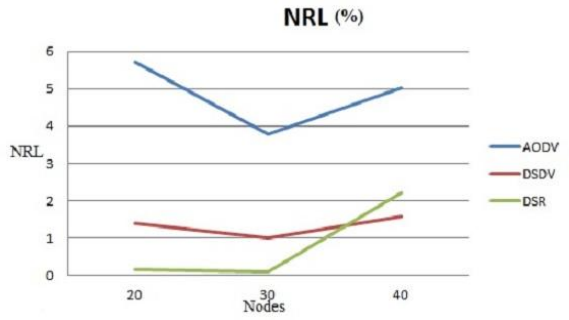

Figure 1: Normalized routing load versus Network Size

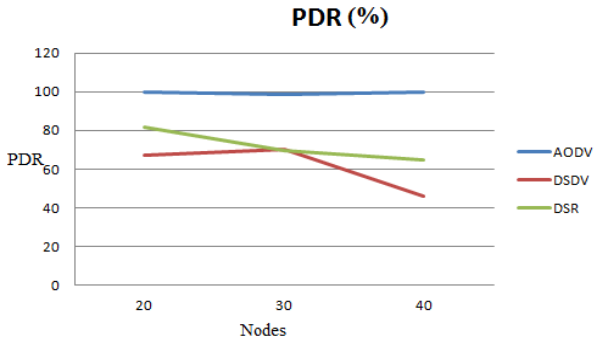

Figure 2: Packet Delivery Ratio versus Network Size

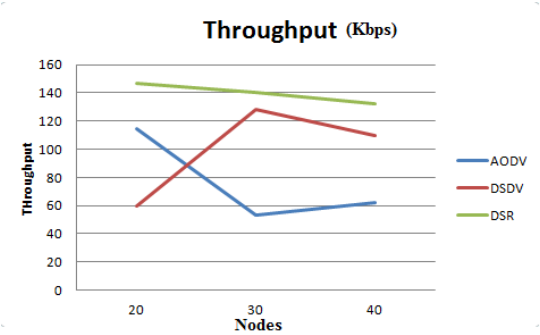

Figure 3: Throughput versus Network size

Table 3: Comparison Between Aodv, Black Hole Aodv Protocol And Malicious Node

Protocol	AODV			blackholeAODV		
No. of nodes	20	30	40	20	30	40
Throughput	114.71	53.68	62.48	2.02	22.11	19.60
Normalized Routing Load	5.714	3.783	5.032	329.800	51.242	87.51
Packet Delivery Ratio	100	98.70	100	3.246	21.428	20.129

Protocol	AODV			malnodeAODV		
No. of nodes	20	30	40	20	30	40
Throughput	114.71	53.68	62.48	166.46	81.72	140.29
Normalized Routing Load	5.714	3.783	5.032	40.00	1.513	0.920
Packet Delivery Ratio	100	98.70	100	14.285	55.666	91.33

According to table III and Fig.6, when we compared AODV and black hole AODV routing protocol, the throughput of AODV routing protocol is comparatively greater than the black hole AODV routing protocol. Similarly, Normalized routing load and packet delivery ratio is more in AODV routing protocol and same is illustrated in Fig.4 and Fig.5 respectively. Also, in the comparative study of AODV routing protocol and malicious AODV node, the throughput and normalized routing load is more in malicious AODV node as illustrated in Fig.9 and Fig.7 respectively. On the contrary, packet delivery ratio is greater in AODV routing protocol as compared to malicious node and same is illustrated in Fig.8.

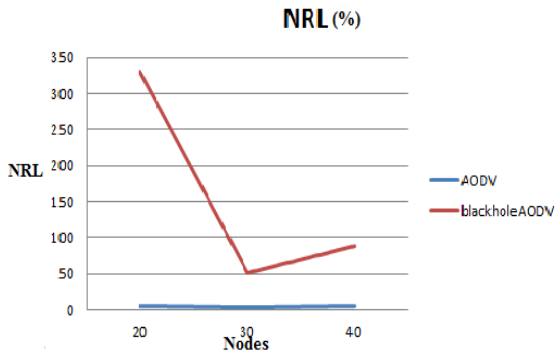

Figure 4: Normalized routing load versus Network Size Network Size of AODV and Black hole AODV

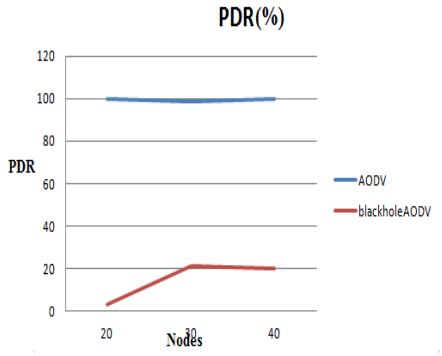

Figure 5: Packet Delivery versus Network Size of AODV and Black hole AODV

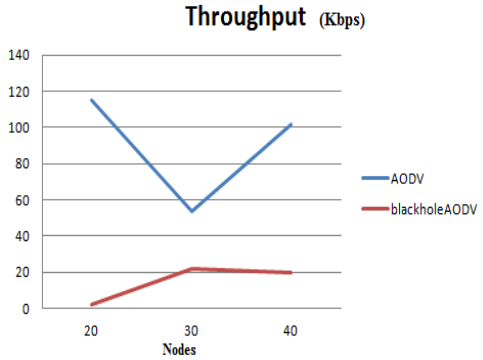

Figure 6: Throughput versus Network Size of AODV Network Size of AODV and Black hole AODV

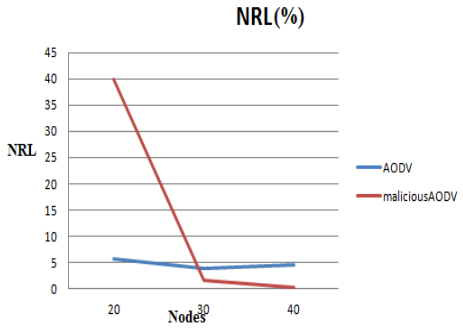

Figure 7: Normalized Routing load versus Network Size of AODV and Malicious Node

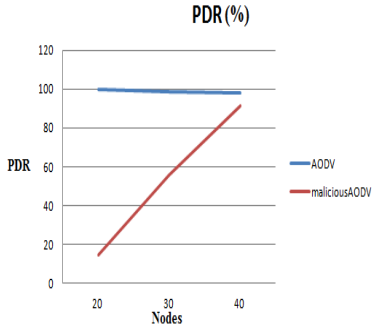

Figure 8: PDR versus Network Size of AODV and malicious node

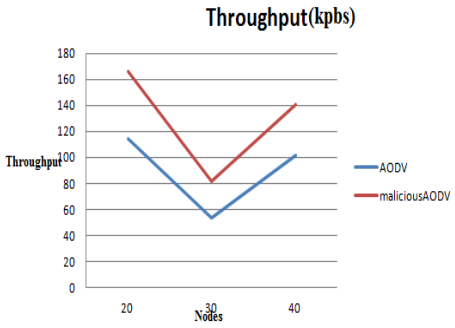

Figure 9: Throughput versus Network Size of AODV and malicious node

Table 4: Comparision Of Blackhole Attack And Ids

Protocol	idsAODV			blackholeAODV		
No. of nodes	20	30	40	20	30	40
Throughput	114.71	53.68	14.19	3.65	9.21	13.53
Normalized Routing Load	2.444	7.296	22.727	128.778	47.886	67.353
Packet Delivery Ratio	100	98.70	71.771	5.844	22.72	22.077

According to Table IV, the throughput and packet delivery ratio is greater in idsAODV routing protocol as compared to blackholeAODV routing protocol and same is illustrated in Fig 12 and Fig.11 respectively. But, normalized routing load of blackholeAODV routing protocol is more as compared to idsAODV routing protocol and the same is illustrated in Fig.10

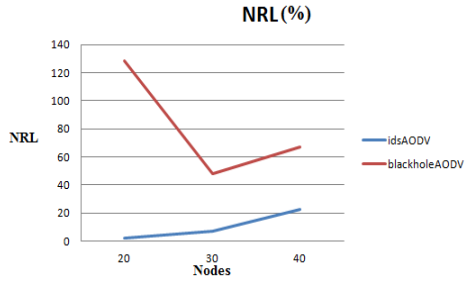

Figure 10: Normalized Routing load versus Network Size of IDSAODV and Black hole AODV

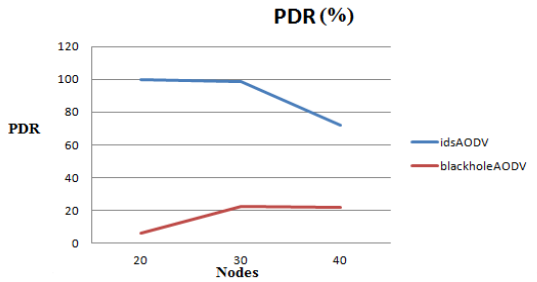

Figure 11: Packet delivery ratio versus Network Size of IDSAODV and Black hole AODV

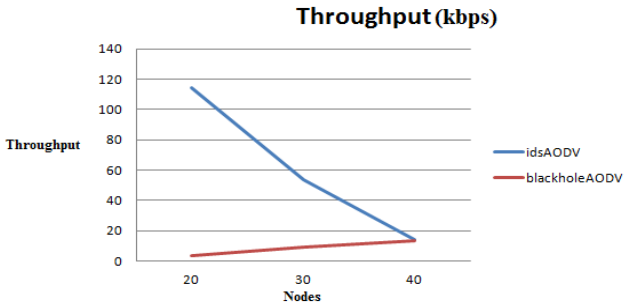

Figure 12: Throughput versus Network Size of ids AODV and Black hole AODV

Conclusion and Discussion

MANETS have the ability to deploy a network in the places where traditional network cannot be deployed. Over the past few years MANETS has been receiving increasing attention especially in networking as such new routing protocols have been proposed. This paper has presented a comparing performance of various protocols for routing packets between mobile nodes in MANETS with scenario consisting of dynamic network size which uses DSDV from table-driven routing protocol compared with AODV and DSR from On Demand routing protocols. Through the analysis and comparison of network simulation results, we can conclude that when the number of nodes is varied, AODV has the highest packet delivery ratio (PDR) and normalized routing load (NRL) while DSR has the highest throughput. Secondly, we made modifications in the network simulator in order to attack the nodes in topology and for that we added new protocols like blackholeAODV and malicious node and compared their performance with AODV routing protocol. Thirdly, we have taken measures to prevent blackhole attack using idsAODV protocol and compared its performance with blackholeAODV protocol. Through the analysis and comparison of network simulation results, we can conclude that throughput and packet delivery ratio (PDR) is decreased to a large extent when black hole node is added in the topology. On the contrary, in case of malicious node, throughput and normalized routing load (NRL) have significantly increased. Further, when idsAODV is compared with blackholeAODV, the packet delivery ratio (PDR) has increased. Thus, every protocol has its own significance and depending on the type of application, the user decides which protocol would suite best. Further, detection of the blackhole attack in other routing protocols as well as implementation of other attacks like wormhole attack, jellyfish attack, eavesdropping in AODV and the other protocols along with their performance evaluation is left as a future work.

References

[1]. J. Khan, S.I.Hyder and K. Khan, "Efficiency and performance analysis of on-demand routing protocols in autonomous system," Australian Journal of Basic and Applied Sciences, Vol.5, No.6, pages 1619-1631,2011.

[2]. V. Kanakaris, D. Ndzi and D. Azzi, "Ad- hoc networks energy consumption: A review of the ad hoc routing protocols," Journal of Engineering and Technology, review 3, pages 162-167, 2010.

[3]. D. B. Johnson, D. A. Maltz and Y. C. Hu, "The dynamic source routing protocol for mobile ad hoc networks (DSR)" IETF MANET WorkingGroup,2004.

[4]. A. K. Gupta, D. Sadawarti and A. K. Verma," Performance analysis of AODV, DSR & TORA routing protocols," IACSIT International [642] Journal of Engineering and Technology, Vol.2, No.2, ISSN: 1793-8236,2010.

[5]. M. Bouhorma, H. Bentaouit and A. Boudhir, "Performance comparison of ad-hoc routing protocols AODV and DSR," International Conference on Multimedia Computing and Systems, ICMCS '09, Pages 511 - 514, 2009.

[6]. A. Boukerche, "Performance evaluation of routing protocols for ad hoc wireless networks" Mobile Networks and Applications, Volume 9, Number 4, pages 333-342, Netherlands, 2004.

[7]. Broch.D.Maltz,D.Johnson,Y.C.Hu and Jetcheva, "A performance comparison of multi-hop wireless ad hoc networks" In Proceedings of the 4th Inc. Conference on Mobile Computing and Networking (ACM MOBICOM'98), pages 85-97,1998.

[8]. A. Saeed, L. Khan, N.Shah, and H. Ali, "Performance comparison of two anycast based reactive routing protocols for mobile ad hoc networks," Computer, 2nd International Conference on Control and Communication, IC4, IEEE Xplore, 2009.

[9]. C. Perkins, B. E. Royer and S. Das, "Ad hoc on demand distance vector (AODV) routing," Internet RFCs, Publisher: IETF, Volume: 1, Issue: 3561, Pages: 1-38,2003.

[10]. Khan, K.Zaman, R.U.Reddy, K.A.Reddy, K.A.Harsha,T.S."An Efficient DSDV Routing Protocol for Wireless Mobile Ad Hoc Networks and its Performance Comparison," Computer Modeling and Simulation, 2008. EMS '08. Second UKSIM European Symposium on Digital Object Identifier.

[11]. Tamil Selvan, L. Sankaranarayanan, V. "Prevention of Blackhole Attack in MANET, "Wireless Broadband and Ultra Wideband Communications,2007.

[12]. Manikandan, T.Sathyasheela, K.B. "Detection of malicious nodes in MANETs,"Communication Control and Computing Technologies (ICCCCT),2010.

[13]. K. Fall and K.Varadhan, "The NS manual (formerly NS notes and documentation)," Collaboration between Researchers at UC Berkeley, and Xerox PARC, 2010.

[14]. Cao Minh Trang,Hyung-Yun Kong,Hong Hee Lee , "A Distributed Intrusion Detection System for AODV"Communications, 2006.

[15]. Mehdi Barati,I Kavyan Atefi,Farshad Khosravi and Yashar Azab Dafial" Performance Evaluation of Energy Consumption for AODV and DSR Routing Protocols in MANET" International Conference on Computer & Information Science (ICCIS), 2012