World Wide Journal of Multidisciplinary Research and Development

WWJMRD 2017; 3(12): 454-458
www.wwjmrd.com
International Journal
Peer Reviewed Journal
Refereed Journal
Indexed Journal
UGC Approved Journal
Impact Factor MJIF: 4.25
e-ISSN: 2454-6615

Hardeep Kaur
M. Tech (Student)
Department of Computer
Science and Engineering
GZS Campus College of
Engineering & Technology,
Bathinda, India

Jyoti Rani
Associate Professor
Department of Computer
Science and Engineering
GZS Campus College of
Engineering & Technology,
Bathinda, India

Enhancing the Performance of Aodv by Securing the Network from Black Hole and Wormhole Attacks.

Hardeep Kaur, Jyoti Rani

Abstract

MANET is the mobile ad-hoc network where various mobile nodes intercommunicate to each other. These nodes moves at specific speed depends upon the type of node, whether it is vehicle node or it is pedestrian node, or it is helicopter node. As there is no central controller which controls the authenticity of the node. So there are various malicious nodes intermediately. These malicious nodes can destroy the relayed data packets. And reduces the network performance by reducting Throughput, End to End Delay, Packet Delivery Ratio and Success Rate. In current research we have focused on to the identifying Black Hole and Worm Hole by having hash key between the source node and the relay node. Black Hole node is such node which destroys the sent data. But warm hole node misroute the packets it receives.

Keywords: Term: MANET, Wormhole, Black Hole

1 Introduction

1.1 Introduction to Mobile ad - hoc networks

MANET contains mobile owners built with Wi-Fi communication units. The leading qualities connected with MANET are usually, the item function with not a central manager, Quickly deployable, self-applied establishing, Multichip radio station communication, Frequent url the break point due to mobile nodes, Concern sources (bandwidth, calculating electric power, battery lifetime, for example.) And just about all nodes are generally mobile so topology can be extremely vibrant. So that the major issues connected with routing standard protocol in MANET is, usually, it must be Thoroughly sent out, Adaptive in order to typical topology alters, Simple working out and maintained, Optimal and never ending loop free course, Optimal by using sources, The item present QoS and Wreck needs to be lower.

1.2 Classification of routing protocols in MANET

The Routing protocols in MANET are usually categorized determined by routing strategy and system composition. According to the routing strategy this routing protocol might be grouped as Table-driven and source initiated, although based on the system composition they are categorized since toned redirecting, hierarchical redirecting and geographic position served Good routing strategy. This routing protocol might be categorized in two ways.

1.2.1 Proactive (Table Driven) Routing Protocol

Each and every node in the network retains routing information to every other node in the network. Route information is generally retained in the routing tables and is periodically updated as the changes in network topology. DSDV along with WRP are the examples of proactive protocols.

1.2.2 Reactive (On-Demand) Routing Protocol

This particular protocol, don't maintain routing details or even routing exercise on the network nodes if you find not any connection. In case a node wishes to post any packet to a different node subsequently this kind of process looks for the option in an on-demand way and also establishes the connection to send and also get the packet. DSR [1], AODV [2] will be the degrees of reactive protocols.

Correspondence:
Hardeep Kaur
M. Tech (Student)
Department of Computer
Science and Engineering
GZS Campus College of
Engineering & Technology,
Bathinda, India

1.2.3 Hybrid Routing Protocol

This can be a combination of very best popular features of preceding two protocols. Node inside of selected long distance through the node concerned, or even just a certain geographical region, tends to be said to be in routing zone. For routing inside the zone, hands-on method along with intended for routing past the area, a hands-on direction-finding standard protocol is employed.

1.3 Types of Attacks

- Denial of Service attack: This attack aims to attack the availability of a node or the whole network. The attack is effective the services will not be available. The attacker generally uses radio signal jamming and the battery exhaustion technique.
- Impersonation: If the confirmation mechanism is not properly implemented a malicious node can act as an honest node and monitor the network traffic. It can also send false routing packets, and gain access to some private information.
- Black hole Attack: In this attack, an attacker uses the routing protocol to present itself as having the shortest path to the node whose packets it wants to intercept.
- Wormhole Attack: In wormhole attack, a malicious node receives packets at one location in the network and passages them to another location in the network, where these packets are resent into the network. This passageway between two colluding attackers is referred to as a wormhole.
- Replay Attack: A replay attack is a form of network attack in which a valid data transmission is maliciously or delayed. This is agreed out either by the originator or by an adversary who stops the data and retransmits it.
- Man- in- the- middle attack: An attacker sites between the sender and receiver and sniffs any information being sent between two nodes. In some cases attacker may imitate the sender to communicate with receiver or imitate the receiver to reply to the sender.
- Eavesdropping: This is a passive attack. The node simply observes the trusted information. This information can be later used by the malicious node. The secret information like location, public key, private key and password can be drawn by eavesdropper.
- Snooping: Snooping is illegal access to another person's data. It is similar to eavesdrop but is not necessarily limited to gaining access to data during its transmission. Snooping can include casual observance of an e-mail that appears on another's computer screen or watching what someone else is typing.
- Sybil Attack: Sybil is named after the woman identified as multiple personality disorder. Sybil attack is implemented when a malicious node claim multiple fabricated or stolen identity and effect the network operations. Sybil attack is damaging the security and trust of network in peer to peer and distributed network. Sybil node gain disproportional amount of resource in network using multiple identities.

Related Work

Lu jin(2014) Have compared three protocols in perspective to the security. These protocols are AODV, SAODV, and FLSL. FLSL has outperformed the AODV and SAODV. FLSL protocol is capable of determining a more secure route among possible routes. While achieving the security, some throughput issues are arising. That means end to end delay is more compare to the other SAODV and AODV. Phung huu phu(2015) Before executing route discovery steps in AODV protocol, each node executes message authentication process with the sender to guarantee the integrity and Non-repudiation of routing messages and therefore, could prevent attacks From malicious nodes. The end-to-end authentication procedure will be added to the current approach in order to improve our current schema. J rajeshwar(2014) is focused on the SAODV. Which is addition of security in AODV. Alekha kumar mishra(2014) A-SAODV(adaptive SAODV), an adaptive mechanism that tunes the behavior of SAODV to improve its performance. They have proposed an extension to adaptive-SAODV of the secure AODV protocol extension, Overhead of cryptographic calculation still persist in the proposed mechanisms. Davide cerri(2014) Propose an Adaptive mechanism that tunes SAODV behavior. Further investigation is needed. In particular, situations with both “good” and “bad” nodes Should be considered in simulation tests, in order to evaluate the behavior of SAODV and of the proposed optimizations under attack. Deepak kumar(2014) Due to the mobility in nature of mobile nodes will leads to problem of link failure. When the route is established between the mobile nodes if during communication Intermediate mobile nodes change its path. The route will be Broken and packet loss occurs. Implement proposed technique and Compare the simulation results with the previous techniques. A. saini(2013) It is shown that the proposed technique of blackhole nodes detection works better than the existing AODV technique and the results are recorded against two parameters-packets received and pdr (packet delivery ratio %). This technique can be extended to large networks and can be measured against more performance parameters such as throughput and delay. D. patel(2009) A scheme of Integrating encryption algorithm with basic AODV routing protocol is found capable of handling both unauthorized and Malicious nodes’ attacks. This technique can be applied to other types of attacks. So that global best technique can be identified. P. bathla(2010) The control packets contain a hop count and sequence Number field that identifies the freshness of routing updates. This technique can be further researched for other types of attacks.

Algorithm

Step1 A network with different mobile nodes is setup. One node will works as source node and one node will works as destination node.

Step2 the Source node Send the false destination request to the neighbor node which are in the intermediate node list. If any node replies, then that node will be considered as malicious node. Else it will be declared as legitimate node.

Step3 Send the route request to the neighbor node for identifying the destination.

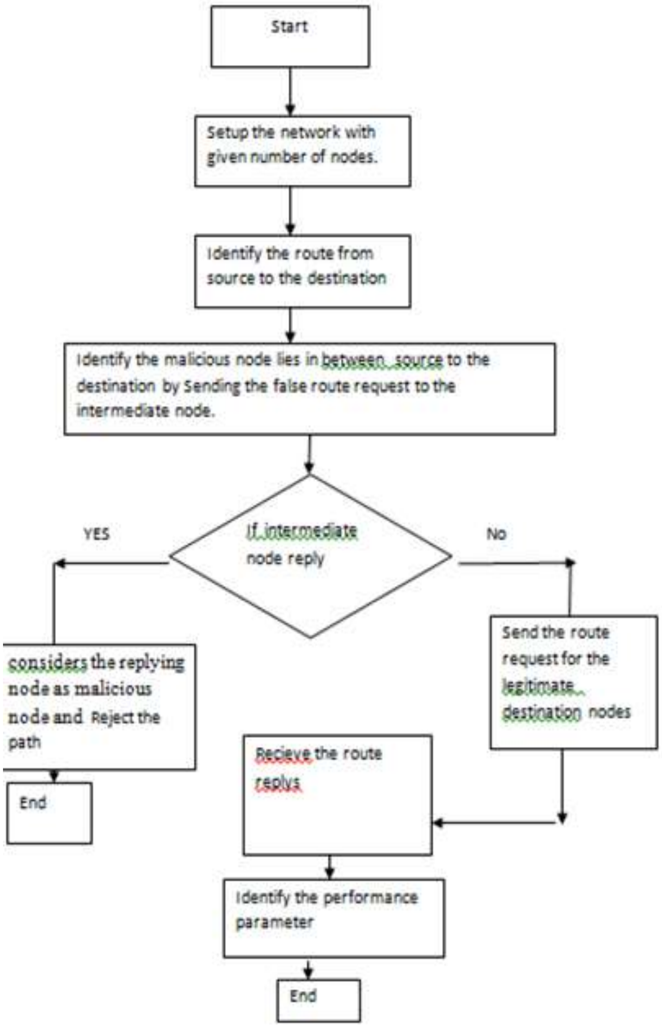
Step4 Receive the route replies.

Step5 Send the data packets on to the route which consists of legitimate nodes.

Step6 Check the network performance under different parameters like Throughput, End to End delay, Packet Delivery Ratio, Success rate.

Step7 Compare the performance on both with and without the attack.

Flowchart


Start
Setup the network with given number of nodes.
Identify the route from source to the destination
Identify the malicious node lies in between source to the destination by Sending the false route request to the intermediate node.
If intermediate node reply
YES
No
considers the replying node as malicious node and Reject the path
End
Send the route request for the legitimate destination nodes
Recieve the route replys
Identify the performance parameter
End

Simulation Setup

Table 1

Parameter	Value
No. of Nodes	50
Protocol	AODV
Communication protocol	TCP,UDP
Application	CBR,FTP
Delay	1ms.
Simulation time	100

This simulation setup includes basic network settings. Such that in NS2 the network can function. This network simulation shows the network in simulated way.

Performance Parameters

Throughput: it is the amount of packet sent per unit interval of time. These the successful packets that has been arrived at the destination.

End to End delay: it is the difference of end time and start time. Start time is at what time packet has been sent. And received time if the time at which packet has been received.

Packet Delivery Ratio: it is the ration of packet sent versus packet dropped. Packets can be dropped due to the congestion or attacker node or with some other problem.

Success Rate: it is the measure of success rate. That means how many packets have been sent and how many packets has been received.

Results and Discussions

7.1 nam simulation for network with attack

Fig.1

This nam simulation shows the attacker node. When any packet arrives at this node all the packets will be dropped. This will deteriorate the performance of the network.

7.2 Nam simulation for network without attack

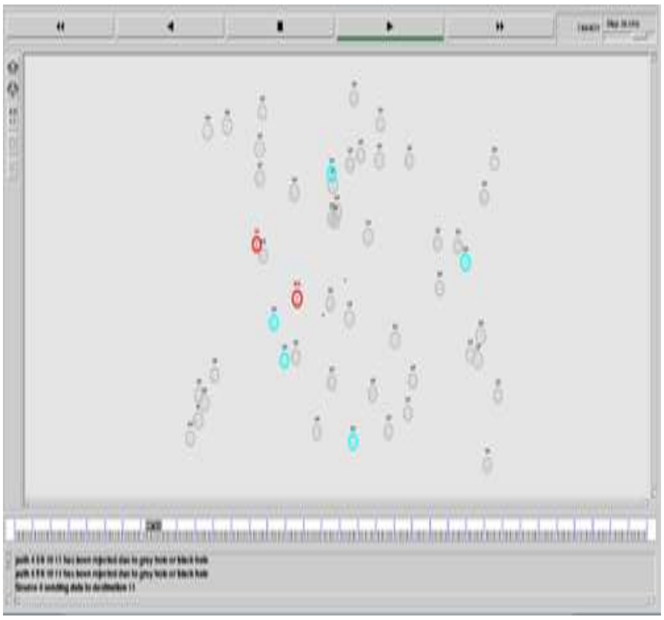
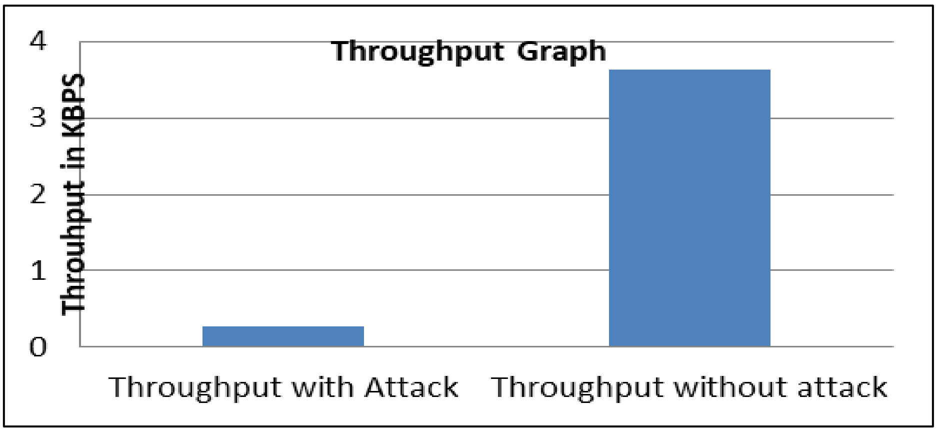


Fig.2

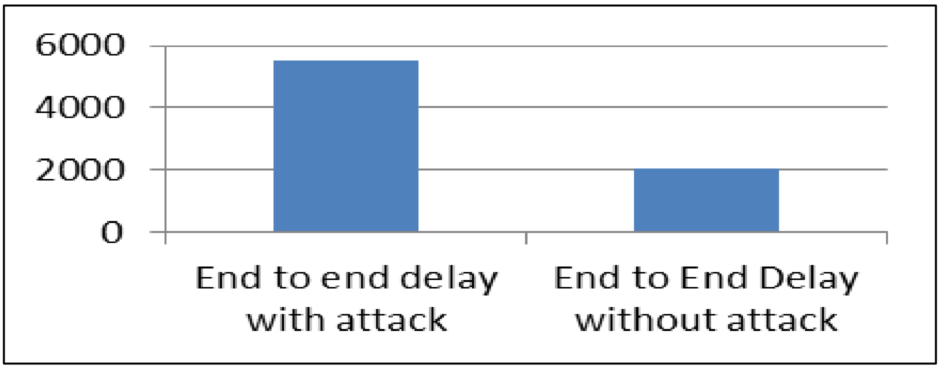
This network shows that the attacker node has been identified. Now when in any path these attacker will be encountered the path will be left. That path will be adopted which has no attacker node

7.3 Throughput graph for network with and without attack



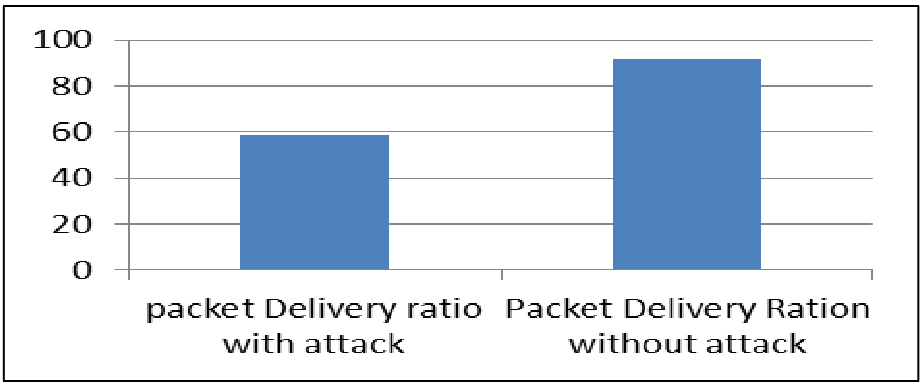
Graph 1

7.4 End to End delay graph for network with and without attack



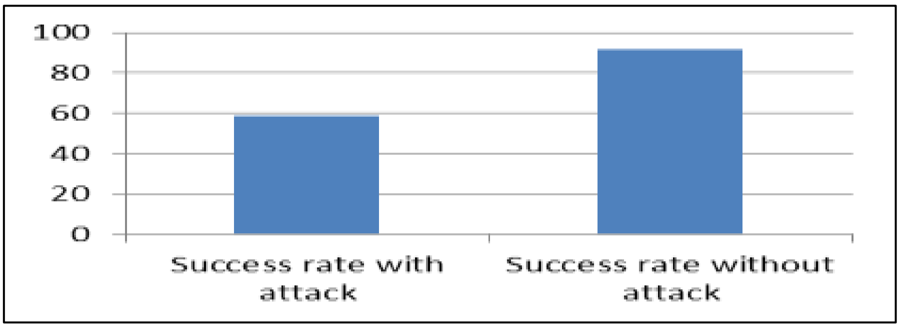
Graph 2

7.5 Packet delivery ratio graph for network with and without attack.



Graph 3

7.6 Success Rate graph for network with attack and without attack



Graph 4

7.7 Percentage Improvement

Table 2

Particular	Percentage
Throughput	92%
End to End Delay	66%
Packet Delivery ratio	35.88
Success Rate	35.88

Above table shows that the network performance on the basis of all the factors has shown the improvement. This means AODV has really improved to SAODV. As secured AODV. Where any attacker node cannot destroy the network performance.

Conclusion and Future Work

MANET is the mobile ad-hoc network. It is infrastructure less network. There is no central controller which can control the network performance and secure the network from various kinds of attacks. There requires updation in protocol. So that the attacker node can be identified and removed. It is the special arrangement where any path which has more packet drop rate will be considered as the path having attacker node. Any new path which has those attacker nodes in the intermediate list will be avoided. So that network performance can be avoided to be downgraded. In proposed technique all the performance parameters like throughput, end to end delay, success rate and packet Delivery ratio has shown the improvement.

Various performance parameters have been measures like Throughput, End to End Delay, packet Delivery ratio and Success rate has shown the improvement. This improvement is 92%, 66%, 35.88%, 35.88% respectively

References

1. Lu Jin, Zhongwei Zhang, Hong Zhou," Performance Comparison of the AODV, SAODV and FLSL Routing Protocols In Mobile Ad Hoc Networks",vol 3 issue 2 pp.23-34,2015.
2. Phung Huu Phu, Myeongjae Yi_, and Myung-Kyun Kim," Securing AODV Routing Protocol In Mobile Ad-Hoc Networks",vol. 3 issue 3, pp. 182–187, 2009.
3. J RAJESHWAR, Dr G NARSIMHA," A Comparative study on secure routing algorithms SAODV And A-SAODV in Mobile adhoc Networks (MANET) The Enhancements of AODV", Volume 3 No 2, pp345-51,December 2012.
4. Alekha Kumar Mishra, 2Bibhu Dutta Sahoo," A Modified Adaptive-Saodv Prototype for Performance Enhancement In Manet", Volume 1: Issue 2, Page: 443, 2009.
5. Davide Cerri and Alessandro Ghioni," Securing AODV: The A-SAODV Secure Routing Prototype",vol 3 issue 3 pp 456-61,2015.
6. Neyre Tekbiyik _, elifuysal-Biyikoglu," Energy efficient wireless unicast routing alternatives for machine-to-machine networks",vol. 3 issue 6 1587–1614,2011.
7. L.F. Xiea,c, Peter H.J. Chongb,∗, I Q1 vanw.H. Hoc, Y.L. Guanb," A survey of inter-flow network coding in wireless mesh Networks with unicast traffic",vo. 3 issue 6 123-30,2015.
8. 1Preeti Bathla, 2Bhawna Gupta," Security Enhancements in AODV Routing Protocol", Vol. 2, Iss ue 2, June 2011.
9. Tayyeba Minhas, Xu Ning, Satish Anamalamudi, Minglu Jin, and Zahid Minhas Khan," Performance Enhancement of AODV Routing Protocol in Wireless Mesh Networks", Vol. 4, No. 6, November 2014.
10. Barinder Singh, Jagdeep Kaur," To Propose Enhancement in Reactive Routing AODV Protocol to Overcome Congestion in MANET", Vol. 4, Issue. 9, pg.296 – 303,September 2015
11. Deepak kumar, Sapanjot kaur," Enhancement in AODV protocol to isolate link Failure problem in Mobile Ad hoc Network", Volume3Issue3- April 2013.
12. Arunima Saini," Security Enhancement in AODV Protocol in MANET", Volume 5, Issue 6,