ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

BLACK HOLE DETECTION AND PREVENTION USING AODV AND SHORTEST DISTANCE TECHNIQUE

Nigahat*, Dr. Dinesh Kumar
* UCCA, Guru Kashi University, Talwandi Sabo
UCCA, Guru Kashi University, Talwandi Sabo

DOI: 10.5281/zenodo.546354

ABSTRACT
Wireless networks are gaining popularity to its peak today, as the users want wireless connectivity irrespective of their geographic position. There is an increasing threat of attacks on the Mobile Ad-hoc Networks (MANET). Black hole attack is one of the security threat in which the traffic is redirected to such a node that actually does not exist in the network. It's an analogy to the black hole in the universe in which things disappear. The node presents itself in such a way to the node that it can attack other nodes and networks knowing that it has the shortest path. MANETs must have a secure way for transmission and communication which is quite challenging and vital issue. In order to provide secure communication and transmission, researcher worked specifically on the security issues in MANETs, and many secure routing protocols and security measures within the networks were proposed. Proposed work include the detection mechanism for black hole attack and mechanism to prevent the black hole attack in MANET using Advanced Ad-Hoc On Demand Distance Vector (A-AODV) protocol.

KEYWORDS: MANET, Black Hole Attack, DSR,AODV, Advanced AODV protocol.

INTRODUCTION
Mobile Ad Hoc Networks (MANETs) is a self-configuring network of wireless mobile nodes that formed network capable of dynamic changing topology. Each node in the network acts as a router, forwarding data packets to other nodes [1]. MANET have many potential applications such as military services in battlefield, disaster relief operations and in commercial environments. Routing in MANET is complex due to its mobility of nodes and dynamic changing topology as compared to traditional wired networks. Limited bandwidth and battery makes routing in MANET more challenging. Due to these fundamental characteristics of MANET, it is susceptible to various kinds of attacks like eaves dropping with malicious intent, spoofing of control or data packets, malicious modification of the packet contents and Denial of service attack like worm hole, sink hole, black and gray hole attacks [7]. These are all network layer attacks. So routing security is one of the important issue for which researchers want to contribute. Routing protocol plays vital role in security of the network. AODV is routing protocol designed and used for MANET to establish route on demand. It does not need to maintain routes which are not active. In this paper, We attempt to provides a solution to detect the multiple black hole nodes present and prevent them from the network. In particular , we are focusing on AODV protocol in MANET .This solution are not only provide protection mechanism against black hole attack but also consequently improve the performance of the network comparing with the existing approaches after detection and prevention of attack. The analysis shows that how severe the attack is and its effects on MANET.

BLACK HOLE ATTACK IN MANET
Black hole is one of many attacks that take place in MANET and is considered as one of the most common attacks made against the AODV routing protocol. The black hole attack involves malicious node pretending to have the shortest and freshest route to the destination by constructing false sequence number [3] in control messages. AODV protocol was created without any security considerations [4]. Thus, no protection mechanism was built to detect the existence of malicious attack. In the AODV, maintaining a fresh route to ensure safe path to destination is very vital due to the rapid change of the network topology. The manipulation done by the malicious node will deny the genuine Route Reply (RREP) message from other nodes especially the reply message coming from the actual destination node.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

LITERATURE SURVEY

[1] Mohamed A. Abdelshafy, MANET routing protocols are designed based on the assumption that all nodes cooperate without maliciously disrupting the operation of the routing protocol. AODV is a reactive MANET routing protocol that is vulnerable to a dramatic collapse of network performance in the presence of blackhole attack. The paper introduces a new concept of Self-Protocol Trustiness (SPT) in which detecting a malicious intruder is accomplished by complying with the normal protocol behavior and lures the malicious node to give an implicit avowal of its malicious behavior. Authors present a Blackhole Resisting Mechanism (BRM) to resist such attacks that can be incorporated into any reactive routing protocol. It does not require expensive cryptography or authentication mechanisms, but relies on locally applied timers and thresholds to classify nodes as malicious. No modifications to the packet formats are needed, so the overhead is a small amount of calculation at nodes, and no extra communication. Using NS2 simulation, Authors compare the performance of networks using AODV under blackhole attacks with and without our mechanism to SAODV, showing that it significantly reduces the effect of a blackhole attack.

[2] Sathish M, Ad hoc On Demand Distance Vector (AODV) routing is an extensively accepted routing protocol for Mobile Ad hoc Network (MANET). The inadequacy of security considerations in the design of AODV makes it vulnerable to black hole attack. In a black hole attack, malicious nodes attract data packets and drop them instead of forwarding. Among the existing black hole detection schemes, just a few strategies manage both single and collaborative attacks and that too with much routing, storage and computational overhead. This paper describes a novel strategy to reduce single and collaborative black hole attacks, with reduced routing, storage and computational overhead. The method incorporates fake route request, destination sequence number and next hop information to alleviate the limitations of existing schemes.

[3] Siddharth Dhama, In the mobile Ad-hoc networks, there exists various challenges in packet data delivery mechanism. Therefore transferring data from one node to other node is challenging. One of such attack is the black hole (BH) attack in a network. We are proposing a mechanism for the detection and prevention of BH attack in the mobile ad hoc network. The routing protocol that we are using is Ad hoc on-demand distance vector routing (AODV). As we know that AODV is vulnerable to BH attack, where a node pretends as a shortest path node and gives false information to the sender. In this paper we not only preventing but also detecting the BH node. The simulator used here to implement the mechanism is NS 2 and result proved the effectiveness of model as the throughput is very high as compared to AODV that does not have proposed mechanism.

[4] Dhiraj Nitnaware, Dynamic MANET On-Demand(DYMO) routing protocol has been used to establish an ad-hoc networks. DYMO is advance version of AODV routing protocol develop to improve the network performance. Security is the major challenge in DYMO routing protocol and prone for various security threats. This research work attempts to develop a mitigation algorithm to avoid and prevent genuine nodes from malicious attack. Black hole attack is one of the security threat in which the traffic is redirected to such a node that actually does not exist in the network. The black hole node presents itself in such a way to the other nodes and networks that it knows the shortest path. The complete research work is classified into three categories which are without attack, with attack and preventive scenario. The performance parameter taken for analysis are throughput and packet delivery ratio against the varying parameters like number of nodes, speed, pause time and area to observe the impact of black hole attack and proposed mechanism with different situation. A Qualnet 5.2 simulator has been used to simulate and evaluate the performance of proposed solution. The complete experimental setup concludes that improvement in mobile node increase the network performance but also increase the black hole impact. Subsequently, improvement in node speed degrades the black hole impact.

PROPOSED METHODOLOGY

We propose a solution that is an enhancement of the basic AODV routing protocol, which will be able to black holes acting in the given network topology. We present a technique to identify multiple black holes cooperating with each other and a solution to discover a safe route avoiding cooperative black hole attack. Our solution assumes that nodes are already authenticated and hence participate in communication. Our approach to combat the Black hole attack is to make use of a ‘Fidelity Table’ wherein every participating node will be assigned a fidelity level that acts as a measure of reliability of that node. In case the level of any node drops to 0, it is considered to be a malicious node, termed as a ‘Black hole’ and it is eliminated. The source node transmits the RREQ to all its neighbors.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

Proposed system works in two steps

(1) Identification of relationships between cluster head neighbors in ad hoc network
(2) Routing Mechanism

Algorithm Steps:

Begin
Step1: Source cluster head(S) broadcasts RREQ.
Step2: S receives RREP.
Step3: S selects the shortest and next shortest path according to hop count.
Step4: S checks Friendship table for one-hop neighbour nodes.
Step5: If neighbour node is a friend then
Route data packet.
Else
Send false packets to the stranger.
Invoke the trust estimator.
Calculate k_{trust} for stranger applying Formula(1).
Add status of stranger to the friendship table of S
End if
Step6: If $k \leq k_{trusti} \leq 1$ then
Route data packet.
Else
Broadcasts stranger as black hole.
End if
Step7: Update the friendship table of S after each time interval t_{stamp}.
Step8: Repeat step 4 to 7 until the destination node gets the data packet.
End

Simlulation Model

We used the network simulator (ns-2). A hypothetical network was constructed for the simulation purpose and then monitored for a number of parameters. We simulate our model for 50 nodes. Pause time is varied from 0 to 900 sec. Each mobile node in the MANET is assigned an initial position within the simulation dimensions (1000×1000) meters and joins the network at a random time. The packets are generated using CBR with rate of 4 packets per sec. The simulation takes place for 900 seconds every run. Nodes are normally distributed when initialized, and the initial position for the node is specified in a movement scenario file created for the simulation using a feature within ns-2. The nodes move randomly among the simulation area. We simulate proposed system with relative to the base protocol AODV. Appropriate graphs are then generated to show the performance of the proposed system.

RESULTS AND DISCUSSION

The proposed system is implemented using NS2(Network simulator 2) to implement the black hole and its prevention technique using ADOV with shortest distance.

Performance Evaluation

The performance of the proposed system is evaluated on the basis of Packet Delivery Ratio and End-to- End Delay.

Packet Delivery Ratio

PDR is the proportion to the total amount of packets reached the receiver and amount of packet sent by source. If the amount of malicious node increases, PDR decreases. The higher mobility of nodes causes PDR to decrease.

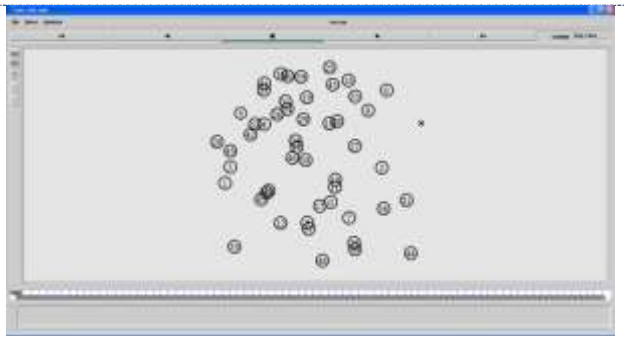
$$PDR\ (\%) = \frac{\text{Number of packets successfully delivered to destination}}{\text{Number of packets generated by source node}}$$

Detection Delay

It is the average delay to detect the attacker making the attack in the network

Network Topology

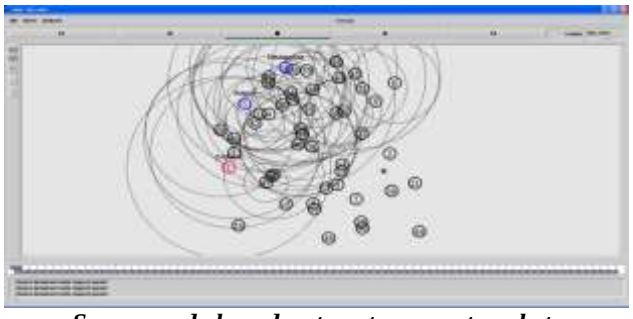
ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7



AODV routing without Attack

Source broadcast request packet to the network. Reply arrived from the destination via the shortest path. Source transfers the data over the path in which reply arrived to the destination.

Black hole Attack
Route request broadcast



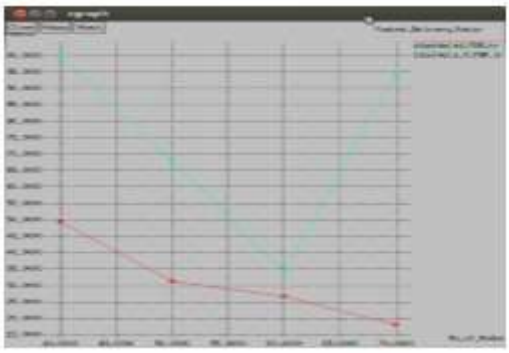
Source node broadcast route request packet.

Attacker send false route reply that it contains shortest route to destination. But originally it does not contain shortest route. Attacker does not forward the packet to the destination.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

Comparative Graph

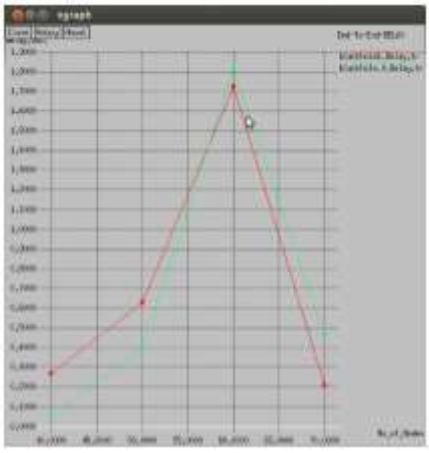
Packet_delivery_Ratio



Number of nodes vs Packet_delivery_Ratio

Packet Delivery Ratio of without blackhole attack is higher than that of blackhole attack of AODV. Because the blackhole attack of AODV sends the false route reply to source,so source sends the packets the attacker. Attacker drops the all packets.

End-To-End-Delay



Number of nodes vs End-To-End-Delay

Delay of without blackhole attack is slightly lower than that of blackhole attack of AODV.

CONCLUSION

MANETs is an emerging technological field and hence is an active area of research. Because of ease of deployment and defined infrastructure less feature these networks find applications in a variety of scenarios ranging from emergency operations and disaster relief to military service and task forces. Providing security in such scenarios is critical. A number of challenges like the Invisible Node Attack remain in the area of routing security of MANETs. Although researchers have designed efficient security routing, optimistic approaches which can provide a better tradeoff between security and performance, a lot more is yet to be done. Future research efforts should be focused not only on improving the effectiveness of the security schemes but also on minimizing the cost to make them suitable for a MANET environment. There is increasing use of wireless devices and hence there is a need to secure these devices. In this proposed work we have detected and prevented the black hole attack in the network based on AODV with shortest distance Algorithm. Various results has been proposed on the proposed system which are then compared with the existing system. Proposed system is evaluated on the basis of PDR and Delay. It is concluded that the proposed system gives the better results than that of the existing system.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

FUTURE SCOPE

In future, performance of the proposed system can be improved by improving the PDR and decreasing the packet delay. Further data encryption can be added to the proposed system to provide the further security. Multiple black hole attacks detection and prevention technique can also be implemented in the proposed system to improve the performance.

REFERENCES

[1] Mohamed A. Abdelshafy,Peter J. B. King,"Resisting Blackhole Attacks on MANETs",2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC)
[2] Sathish M, Arumugam K, S.Neelavathy Pari,"Detection of Single and Collaborative Black Hole Attack in MANET",IEEE WiSPNET 2016 conference.
[3] Siddharth Dhama,Sandeep Sharma, Mukul Saini,"Black Hole Attack Detection and Prevention Mechanism for Mobile Ad-Hoc Networks", 2016 IEEE
[4] Dhiraj Nitnaware,Anita Thakur, "Black Hole Attack Detection and Prevention Strategy in DYMO for MANET", 2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN).
[5] Rakesh Ranjan, Nirnemesh Kumar Singh, Mr. Ajay Singh,"Security Issues of Black Hole Attacks in MANET", International Conference on Computing, Communication and Automation (ICCCA2015).
[6] Binod Kumar Mishra, Mohan C. Nikam, Prashant Lakkadwala,"Security Against Black Hole Attack In Wireless Sensor Network–A Review", 2014 Fourth International Conference on Communication Systems and Network Technologies.
[7] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao, "A survey of black hole attacks in wireless mobile ad hoc networks", Human-centric Computing and Information Sciences, Springer, December 2011
[8] Nitish Balachandran, "Surveying Solutions to Securing On-Demand Routing Protocols in MANETs", Int. J. Advanced Networking and Applications, Volume:04 Issue:01 Pages:1486-1491 (2012)
[9] Muthumanickam Gunasekaran and Kandhasamy Premalatha, "SPAWN: a secure privacy-preserving architecture in wireless mobile ad hoc networks" EURASIP Journal on Wireless Communications and Networking, Springer , December 2013
[10] Mahfuzulhoq Chowdhury, Md Fazlul Kader and Asaduzzaman, "Security Issues in Wireless Sensor Networks: A Survey", International Journal of Scientific & Engineering Research, Volume 7, Issue 8, August-2016.
[11] Azeem Irshad, Wajahat Noshairwan, Muhammad Shafiq, Shahzada Khurram, Ehtsham Irshad, Muhammad Usman, "Security Enhancement in MANET Authentication by checking the CRL status of Servers" Cite seer, 2014
[12] Ms.Supriya and Mrs.Manju Khari, "Manet security breaches : threat to a secure communication platform", International Journal on AdHoc Networking Systems (IJANS) Vol. 2, No. 2, April 2012.
[13] Shikha Jain, "Security threats in manets: A Review" International Journal on Information Theory (IJIT), Vol.3, No.2, April 2014
[14] Delan Alsoufi, Khaled Elleithy, Tariq Abuzaghleh and Ahmad Nassar, "Security in wireless sensor networks –improving the leap protocol" International Journal of Computer Science & Engineering Survey (IJCSES) Vol.3, No.3, June 2012.
[15] Gaurav Soni and Kamlesh Chandrawanshi, "A novel defence scheme against selfish node attack in MANET", International Journal on Computational Sciences & Applications (IJCSA) Vol.3, No.3, June 2013
[16] Priyanka Goyal, Vinti Parmar, Rahul Rishi, "MANET: Vulnerabilities, Challenges, Attacks, Application" , IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011, ISSN (Online): 2230-7893.
[17] Rutvij H. Jhaveri, Jatin D. Parmar,Ashish D. Patel,Bhavin I. Shah, "MANET Routing Protocols and Wormhole Attack against AODV", IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.4, April 2010.
[18] P.Visalakshi, S.Anjugam, "Security issues and vulnerabilities in Mobile Ad hoc Networks (MANET)-A Survey", International Journal of Computational Engineering Research (IJCER) National Conference on Architecture, Software system and Green computing, 2012, ISSN: 2250-3005
[19] Mamatha. T, "Network Security for MANETS", International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-2, Issue-2, May 2012
[20] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks",2012