International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-2, Issue-3, May-2014

A Review on Black Hole Detection on Mobile Ad-hoc Network

Kavita rathi, Geeta Kumari

***Abstract:*-MANET is a network with unrestricted mobility in nature and no centralised control. Mobile node can move from one network to another frequently. MANET is infrastructure less so any node can enter and exit the system at any time. Malicious node can enter easily in the network and degrade the performance of the network by modifying, updating and drop the data packet. MANET is vulnerable to various attack such as black hole, grey hole and coverage hole etc so the security is main issue in adhoc network. In this paper, many mechanisms have been proposed to detect the black hole in the network using an efficient adhoc on demand distance vector routing protocol (AODV) which improve the performance of the network by detecting black hole attack in MANET.**

***Keyword:* - MANET, AODV, black hole, grey hole and coverage hole attack.**

I. INTRODUCTION

Mobile ad-hoc network is collection of multiple nodes. There is no existing infrastructure, host movement frequently from one place to another. In mobile ad hoc network two nodes communicate with each other when they are radio range of each other. Topology of the network change frequently when mobile node moves from one place to another. There is continuous breakage and establish of link when node moves [1]. In this network, data are routed via intermediate node. There are used various routing protocol to route the useful information from source node to destination node.

MANET is highly vulnerable to various type of attack such as black hole attack, gray hole attack and coverage hole etc. MANET is vulnerable because it has no centralised control and highly dynamic in nature i.e. topology change frequently, host movement frequently.

The rest of paper is organised as follows:

In section 2 we present some MANET vulnerabilities and we give the overview of AODV in section 3.In section 4, we focus on type of attack in the mobile adhoc network. In section 5 we describe the need of detection of black hole attack on MANET. In section 6 we briefly outline the related work on black hole in MANET .Finally in section 7, we conclude our work.

II. MANET VULNERABILITIES [1]

A. ***Decentralised control:*** - MANET has no central node which can monitor on underline network. Ad-hoc network are wide in nature and attacker node can enter easily in the network and disturbed the performance of the network.

B. ***Resource Constraints:*** -In MANET, resource availability is an important issue. In this type of dynamic network threat comes easily so the security mechanism is necessary to avoid the attack on the network.

C. ***Specific power supply:***- In MANET, each mobile node have limited battery so node work in selfish manner when it know it has limited battery power.

D. ***Dynamic topology :***- In MANET, node are mobile in nature so it move easily from one place to another, topology change frequently due to which trust level is disturbed between nodes.

E. ***Bandwidth restriction:***-In MANET, There are used variable low capacity link which can cause various type of effect in network such as interference and signal attenuation etc.

F. ***No predefined boundary:*** - In MANET there is no predefined physical boundary. Node move freely from one network to another and communicate one network to another through the radio range.

G. ***Scalability constraints :***- MANET are dynamic in environment so scale of the network are change frequently due to which security mechanism is an important issue[1].

III. AODV IN MANET

AODV is an on demand and reactive routing protocol in mobile adhoc network. AODV support both multicasting and unicasting in the network. It has uniform packet size

Manuscript received May 21, 2014

Mrs. Kavita Rathi, Computer Science, Deen Bandhu Chhotu Ram University of Science & Technology Murthal, Sonepat, India, 8930220999., (e-mail: kavita1217@gamil.com).

Geeta Kumari, Computer Science, Deen Bandhu Chhotu Ram University of Science & Technology Murthal, Sonepat, India, 9466666258., (e-mail: geetayadav9084@gmail.com).

and only one source destination pair[9]There are two phase in AODV:-

A. ***Path establishment*** [8]:- When a source node wants to communicate with destination node then first step from source to destination is route establishment. Source node initially checks its routing table that it has a route to destination in destination node entry. If there is a route then source send the message to destination through this route else sources broadcast the message in network and establish the route and then send the message to destination.

B. ***Path maintenance [8]***:- Path maintenance is an important step in AODV. Each node has a lifetime entry in its routing table. If the time is expiring for a entry, it is deleted from the table. Aodv maintain the route which is in used.

IV. ATTACK ON MANET

A. ***Black Hole Attack:*** - In Black hole attack, malicious node enter the network and gives the false routing information in the network [1]. When sender sends the packet in the network, then the black hole node can show that this has the shortest route from source to destination. Black hole node show higher sequence number than the neighbours. Then black hole node take the data and drop it, the packet cannot reach to the actual destination so it disturb the performance 0f the network.

B. ***Grey Hole Attack:*** - Gray hole attack is the extension of black hole attack [1].Sometime it behave like malicious node and sometime it like healthy node. Both type of network degrade the performance of the network.

V. NEED OF DETECTION OF BLACK HOLE ATTACK IN MANET

In the original AODV, It is assumes that the entire node in the network are trusted node which is not true each time. MANET is an infrastructure less network and mobile in nature. Some node are malicious node which can enter in the network and break the trust of the network by doing various type of attack on the network and degrade the performance of the network. So the detection of these nodes is an important issue in MANET. By detection of these nodes, we can increase the performance of the network and make the network more secure.

Table1: Existing Technique in Black Hole attack

Author's Name	Technique	Advantage
Chun Hsin Wang And Young Tang Li	Few detection node pair in a network technique	Packet delivery rate improve 17% of original aodv
Ramcharan,R1 and Ruban Thomas,D2	ES-AODV algorithm	Improve both security and performance of the network
Satoshi Kurosawa	Dynamic Learning Method	Effective in highly dynamic environment
Sonal1 and Kiran Narang	Fuzzy Logic Based Algorithm	Reduce data loss over the network
Mehdi Medadian and ahmad Mebadi	Combat with black hole attack by negotiation with neighbours who laim to have a route to destination	Better Security and performance in the term of packet delivery

VI. RELATED WORKS

MANET[1] are vulnerable to various type of DOS attack such as black hole and gray hole attack which are widely occur in ad-hoc network and disturb the performance of the network such as packet delivery ratio, throughput and end-to-end delay etc. In this paper, there are used various technique on black hole detection and improve the performance of network. There are used various security mechanism on the ad-hoc network to make it secured.

Ramachandran, R1, ruban Thomas, d2 [2] present a performance analysis algorithm in wireless ad-hoc network called ES-AODV. This algorithm provides better security and performance than original AODV. This protocol find malicious node which can disturb the communication and established trusted end to end route in the network. This protocol is extension of AODV called ES-AODV which has main focus on network layer. All routing protocol has main focus on shortest path to the destination but ES-AODV focused on secure path free of malicious node not on the shortest path. This protocol ensured trust level information provided by neighbour would be checked by its predecessor. Authenticity was provided by computation of the signature by private key and its trust level.

Table 2: Route Request Packet Structure in ES-AODV [2]

Source Address	Destination Address	Source sequence Number
Destination sequence Number	Last Address	Broadcast Id
Hop Count	ES, Previous node IP	ES, Cumulative

Issac Woungang and Sanjay kumar Dhurandhar [3] proposed ant swarm inspired energy efficient ad-hoc on demand routing protocol for mobile ad-hoc network called ACO-EEAODR in which energy load is balanced among the node resulting network lifetime is increased.

Mehdi Medadian and Ahmad mebadi [4] proposed to combat the black hole attack by negotiation with neighbour who claim route to destination. In this technique, all nodes in the network show the honesty of itself. When a node is first receiver of route reply packet they send the data to source and start judgment process about the replier. All neighbour node give opinion about that node after that it is decided that node is malicious or not. To judgement about the node is start with node activity in the network. The judgements Rule are [4]:-

Rule1:

If a node delivers many data packets to destinations, it is assumed as an honest node.

Rule2:

If a node receives many packets but don't sent same data packets, it's possible that the current node is a misbehaviour node.

Rule3:

When the rule2 is correct about a node, if the current node has sent number RREP packets; therefore surely the current node is misbehaviour.

Rule4:

When the rule2 is correct about a node, if the current node has not sent any RREP packets; therefore the current node is a failed node.

This technique has minimum delay and maximum performance than the conventional AODV in the presence of black hole attack.

Satoshi Kurosawa and Hidehisa Nakayama [5] proposed black hole detection in mobile ad-hoc network using Dynamic learning Method. In this method they proposed anomaly detection using updating of the training data at a regular time interval. When the new data enter into the system, distance is compared with threshold value. If the distance from input data space is less than threshold then new data is normal data and we update training data else it is abnormal data.

Sonal and Kiran Narang [1] proposed black hole detection using fuzzy logic. There are used two factor for improvement i.e. packet loss and data rate. In the proposed algorithms there used the concept of priority. The higher priority node can take part in communication. In this algorithms three phase are taken at sender side [1]:-

Phase 1: Packet loss is low and data rate is high then priority is high.

Phase 2: Packet loss is medium and data rate is high then priority is medium.

Phase 3: Packet loss is low and data rate is low then priority is low.

They set the priority at receiver side, when the energy is low then priority is low otherwise high and takes part in communication. It provides better solution to reduce data loss over the network [1].

Swati Saini and Vinod siroha [6] has proposed an algorithm to detect the black hole attack on MANET. They used Fuzzy Logic Based Mechanism for detection of the black hole node in mobile adhoc network using AODV routing protocol. This system is providing better performance and packet delivery ratio [6].

P.Agrawl [7] has proposed a technique to detect the black hole attack and gray attack in the wireless adhoc network. Initially he assumed that the entire networks are divided into small part. Some nodes are strong node, which are used as a backbone network and other node are normal node. Strong nodes are assumed to be trustful node. The drawback of this technique is that if the attacker attack on any strong node then there is no external security is provided.

VII. CONCLUSION

In this paper, we study various techniques which can improve the performance of the network by detecting black hole attack in the network. Here we have discussed various vulnerability in MANET and also discussed about various attack on MANET. Each author have given their own technique to reduce the black hole and gray hole in network and try to make the wireless network more secure. The performance of each technique is much better than original AODV but each technique have their own disadvantages also.

REFERENCES

[1] Sonal and Kiran Narang2" Black Hole Attack Detection using Fuzzy Logic" Volume 2 Issue 8, August 2013

[2] Ramachandran, R 1and Ruban Thomas.D2 "Performance Analysis of Effective Security Algorithm for Wireless Ad Hoc Networks" 978-1-4673-5090-7/13/$31.00 ©2013 IEEE

[3] Isaac Woungang, Sanjay Kumar Dhurandher, Mohammad S. Obaidat and Alexander Ferworn, Waqas Shah "An Ant-Swarm Inspired Energy-Efficient Ad Hoc On-Demand Routing Protocol for Mobile Ad Hoc Networks" 978-1-4673-3122-7/13/$31.00 ©2013 IEEE

[4] Mehdi Medadian#1, Ahmad Mebadi*2, Elham Shahri" Combat with Black Hole Attack in AODV Routing Protocol" 978-1-4244-5532-4/09/$26.00 ©2009 IEEE

[5] Satoshi Kurosawa and Hidehisa Nakayama "Detecting Black hole Attack on AODV-based

[6] Mobile Ad Hoc Networks by Dynamic Learning

[7] Method" International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007.

[8] Swati Saini1 and Vinod Saroha2 "Analysis and Detection of Black Hole Attack in

[9] MANET" International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064

[10] H.Deng; W.Li; D.Agarwal, "Routing security in wireless ad hoc networks", [J]. Communication Magazine, IEEE, (2002), 70-75.

[11] Yashwanth, M"Enhanced AODV (EN-AODV) in Adhoc network"2010

[12] www.drrbpatel.org/lecture/CSE-302-MANET-AODV.ppt

Mrs Kavita Rathi is n Assistant Professor at Deen Bandhu Chhotu Ram University of Science & technology and has Bachelors and Master's Degree in Computer Science and Engineering her research interest area is networking and image processing. She has published various research papers in national and international conferences and journals. She has attended several workshops and faculty development programs.

Geeta Kumari is a Student of M.Tech .at the department of Computer Science at Deen Bandhu Chhotu Ram University of Science & technology, her research interest area is networking

.