International Journal of Advanced Trends in Computer Applications
www.ijatca.com

AN ANALYTICAL SURVEY OF BLACK HOLE ATTACK AND ITS PREVENTION MECHANISMS IN WANET

[1]Navdeepak kumar, [2]Lipsa Walia
[1]M.tech Scholar, Electronics and Communication Department, RBIEBT, Mohali
Makkarnavdeepak@yahoo.com
[2]Assistant Professor, Electronics and Communication Department, RBIEBT, Mohali
Walia_lipsa@yahoo.co.in

Abstract: *Wireless Ad-Hoc Network is in advance attractiveness at the present days due to suppleness and communication not including the infrastructure or central access point. The mobile nodes generate their own topology whenever communicate with each other. Due to this dynamic nature of WANET there is raising the chance of attack due to the lack of security. Black hole attack is one of the main security threats which take place in network layer. Black Hole attacks are launched by participating malicious nodes which behave like a valid node and generate the shortest path to destination node. It will drop the packet intentionally, which degrade the performance of network. In this paper, a review on different prevention techniques for the black hole attack in WANET is presented.*

Keywords: *Wireless Ad-hoc Network, Black-hole Attack, Routing protocols, Detection and prevention techniques.*

1. Introduction

A Current technological advance in wireless networking have popularized the use of portable devices, raising the dependence of people on them for executing anywhere and anytime critical applications, like business-critical applications in financial transactions or life-critical applications in healthcare. Such dependence claims simultaneously for high level of reliability, security and availability to assure secure and reliable service operation even under failures, intentional threats or accidents. Wireless ad hoc networks – mobile or stationary – have envisioned supporting ubiquitous computer connectivity by self-organized portable devices, also called nodes, communicating among themselves in a wireless and multi-hop fashion [2].

A Wireless Ad hoc Network is a self design decentralized network in which Nodes are dynamic in behavior. Nodes can communicate with each other directly exclusive of any central management [1]. Otherwise the process of sending the data from source to destination is complete with the help of routing protocols. In WANET the node can behave as a host as well as a router at same time. When a node acts like a router it will check it's nearest neighboring nodes to destination and forwards the packet from node to node. Nodes should be skilled to come in and go away from network as they desire. Due to the movable personality of nodes and dynamic topology behavior, it needs the effectual routing protocol to continue the communication among the network as well as between nodes in the network [9]. In this paper various schemes are discussed which are used to detect and prevent collaborative black hole node in WANET.

2. Routing Protocol in Wireless Ad-hoc Networks

The procedure of transfer and getting information from one node to another is finished with the help of routing protocols. In WANET all nodes behave as router. The multi-hop, mobility, vast network range joint with device heterogeneity and bandwidth and battery power limits, all these factors make the design of routing protocols a major challenge. In an Ad hoc network, mobile nodes get nearer together for an era of time to swap information. While exchange information, the nodes may continue to move. A routing protocol is required at that time when a packet wants to be transmitted to a destination through several nodes. Many protocols have been recommended keeping applications and network in view.

2.1 Classification of Routing Protocols

WANET routing protocols are categorized into three main categories: Table driven (proactive), On-Demand driven (Reactive) and Hybrid.

2.1.1 Proactive Routing Protocol:

In table-driven routing protocol every node updates routing tables which have record of adjacent of nodes and reachable nodes but also the number of hops. If the size of network rises, the operating cost also increase which outcome in turn down in performance. Destination sequenced distance vector (DSDV) and Optimized link state routing (OLSR) are proactive protocol.

There are a variety of proactive routing protocols. Example: DSDV, OLSR, WRP etc.

2.1.2Reactive Routing Protocols:

In On-Demand routing protocol, route is discovered when it is desired. Nodes begin route detection when demanded. A route is obtained by begin of a route detection procedure by the source node. These routing protocols have two major components [3]:

1) Route discovery- In this stage source node begin route discovery on require request. Source nodes ask its route cache for the presented route from source to destination otherwise if the route is absent it starts route discovery [3]. The packets of the source node contain the address of the target node plus address of the midway nodes to the destination.

2) Route maintenance- because of dynamic topology of the network cases of the route disappointment among the nodes occurs as a result of link breakage etc, so route repairs are necessary. Reactive protocols have acknowledgement method owing to which route protection is probable.

There are a variety of reactive routing protocols. Example: DSR, AODV, LMR etc.

2.1.3 Hybrid Routing Protocol:

Hybrid protocols join attributes from both reactive and proactive routing protocols. Proactive protocols have extra operating cost and a smaller amount latency while reactive protocols have a smaller amount overhead and more latency. Thus a Hybrid protocol is required to defeat the limitations of both proactive and reactive routing protocols. It uses the on demand method of reactive protocol and the table maintenance method of proactive protocol hence to keep away from latency and overhead troubles in the network. Hybrid protocol is suitable for huge networks wherever big numbers of nodes are present.

There are many hybrids routing protocols for WANET like ZRP, SHRP etc.

3. BLACK HOLE ATTACK IN WANET

Black hole node works similar to black hole in the universe. In WANET, black holes happen in the network layer wherever incoming or departure traffic is noiselessly discarded, free of informing to the source with the purpose of the information did not attain its proposed receiver. Malicious nodes know how to discover the active route and note down the destination address or able to send a route reply packet (RREP). When a main node transmits the RREQ message for whichever destination, the malicious node without delay replies by an RREP message [5]. Malicious node attracts every part of the traffic towards itself and doesn't ahead to other nodes. Malicious node launch RREP to the afterward node which goes to the active route. Now source node starts to transmit the packets to the malicious node trusting with the intention that this data will arrive at the destination [8]. The malicious node will not forward the packet. It will drop the packets in the route.

3.1 There are two types of black hole attack [10]:

3.1.1 Single Black hole attack:

In Single Black Hole Attack only single node operates as hateful node surrounded by a region. That malicious node promotes itself as a node of nearest and easiest path to the destination. At what time packet received at black hole node then it dispose of the packet. The main node transfer data packet to the receiver node via malicious node and this single node drops all the data packets somewhere else.

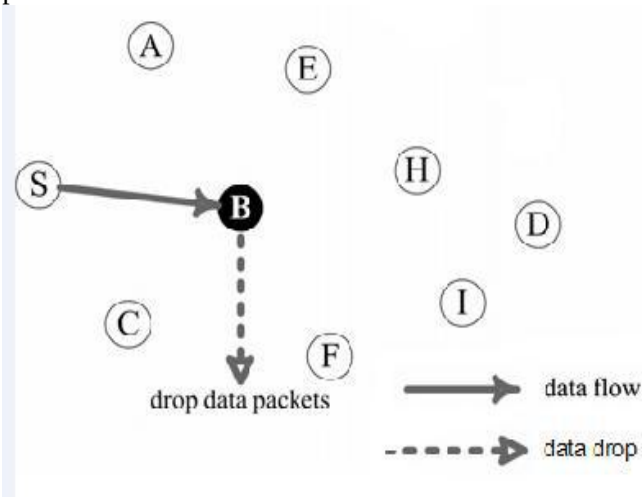

Figure-1: Single black hole attack

3.1.2 Cooperative Black hole attack:

In this attack many malicious nodes operate simultaneously to forward regular routing plan to them and generate that route according to them to succeed the attack. This is very harmful and dangerous attack as compare to the single black hole attack.

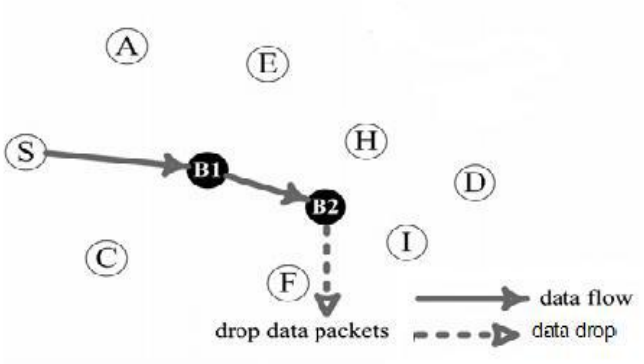

Figure-2: Collaborative black hole attack

4. RELATED WORK

Chavda Ketan S et.al [1] used a technique to improve the AODV routing protocol under the black hole attack. In this approach the protected route between source and destination node using NS-2 Network simulator for simulation was founded. The Wireless Channel used as a channel which was Two Ray Ground radio propagation model. AODV routing protocol and UDP were used at network and transport layer. All the data packets were CBR (continuous bit rate) packets. This algorithm was applied in the presence of attack and had increased the throughput and packet delivery ratio.

Salehi Mahmood et.al [3] proposed a new black hole attack with DSR protocol and compared the simulation results with ordinary black hole attack. In this paper a new attack named Deep Black Hole attack which promotes fake RREPs more strongly than ordinary black hole attack had introduced. They had used the NS-2 for the simulation of DSR protocol parameters. The new attack has two phases. In the advertisement phase node makes fake RREPs in reply to received RREQs and also regarding overheard RREPs. But in the packet drop phase node generates and sends a new fake RREP having a artificial source route which is almost shorter than the main source route and contains malicious node itself as a hop in the route. With the help of fake RRRPs it receives the packet from other nodes and starts dropping their packets silently. To avoid this DSR algorithm which by default helps to find the activated original node had been used.

Ullah Irshad et.al [5] proposed the Reactive and Proactive Protocols against the Black Hole Attack on MANET. This paper had compared the simulation results of proactive (OLSR) and Reactive (AODV) routing protocol under the black hole attack. The parameters taken were throughput, network load and end-to-end delay and Simulation is done in Optimized Network Engineering Tool (OPNET).They have used OPNET for modeling the nodes, picking its statistics and then operating its simulation to get the result used for the analysis. In the End-to-End delay under black hole attack both protocols were compared. AODV showed high delay as of OLSR because of its route search and reactive behavior. But in the throughput and network load AODV performed better results.

Arora Neeraj et.al [6] performed the analysis over the performance of MANET routing Protocols like AODV, OLSR and ZRP with or exclusive of black hole attack and have compared their analysis results .In this the performance analysis the various parameters like packet delivery ratio, average throughput, average end to end delay and Packet Drop Rate using NS-2 simulator under different scenarios have been judged. In the comparison the hybrid protocol (ZRP) performed better among other protocols in MANET.

Dangore Monika Y et.al [9] used the AODV routing protocol for Detection and had overcome the Black Hole Attack. The network parameters like Throughput, Packet Delivery Ratio and Average End to End Delay had been calculated for honest network and a network with black hole attack using the NS-2. The algorithm used some steps for detection of malicious node.

1. If a node sends various information packets to destinations, it is understood as a truthful node. 2. If a node obtains numerous packets but doesn't pass identical information packets, it is probably a malicious node.

Rani Jyoti et.al [10] proposed to diminish the black hole attack using AOMDV (Ad hoc on Demand Multipath Distance Vector) routing protocol with some improvements in it. These developments formulate the protocol vigorous against black hole attack and multipath route discovery process. This approach was based on to avoid multiple black hole attacks when transitional nodes respond to the RREQ packet. Then there would be various connections to the destination. But only one path from source to destination could be opted. At that time intermediate node will generate a route which did not contain any node whose legality threshold crosses the lower level. In this work RREQ and RREP packets were also improved.

5. Conclusion and future scope

A Black Hole attack is main security trouble in WANET. Its detection and prevention of attack is major issue of worry. In this paper an analysis of different routing protocols to generate a smooth network for increasing the efficiency of network with or without the black hole attack is discussed. Every routing protocol has its personal techniques to discover and protect the routes from source node to destination node. But still WANET have not a comfortable solution against the security attacks due to its dynamic topology nature. Future work is wished-for to a skilled detection and exclusion algorithm with optimization technique for minimum delay and secured data packets under Black hole attack.

References

[1] Chavda, Ketan S., and Ashish V. Nimavat. "Removal of black hole attack in AODV routing protocol of MANET." 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT). IEEE, 2013.

[2] Khattak, Hizbullah. "A hybrid approach for preventing Black and Gray hole attacks in MANET." Digital Information Management (ICDIM), 2013 Eighth International Conference on. IEEE, 2013.

[3] Salehi, Mahmood, Hamed Samavati, and Mehdi Dehghan. "Evaluation of DSR protocol under a new Black hole attack." Electrical Engineering (ICEE), 2012 20th Iranian Conference on. IEEE, 2012.

[4] Sarma, Kishor Jyoti, Rupam Sharma, and Rajdeep Das. "A survey of Black hole attack detection in Manet." Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014 International Conference on. IEEE, 2014.

[5] Ullah, Irshad, and Shahzad Anwar. "Effects of black hole attack on MANET using reactive and proactive protocols." International Journal of Computer Science Issues 10 (2013): 152.

[6] Arora, Neeraj, and N. C. Barwar. "Performance Analysis of Black Hole Attack on different MANET Routing Protocols." International Journal of Computer Science and Information Technologies (IJCSIT) 5.3 (2014).

[7] Vasudha Sharma, Sanjeev Khambra "Performance Comparison Study of AODV, OLSR and TORA Routing Protocols for MANETS." International Journal of Computational Engineering Research/ISSN (2012): 2250-3005.

[8] Patel, Meenakshi, and Sanjay Sharma. "Detection of malicious attack in manet a behavioral approach." Advance Computing Conference (IACC), 2013 IEEE 3rd International. IEEE, 2013.

[9] Dangore, Monika Y., and Santosh S. Sambare. "Detecting and overcoming Blackhole attack in AODV protocol." Cloud & Ubiquitous Computing & Emerging Technologies (CUBE), 2013 International Conference on. IEEE, 2013.

[10] Rani, Jyoti, and Naresh Kumar. "Improving AOMDV protocol for black hole detection in Mobile Ad hoc Network." Control Computing Communication & Materials (ICCCCM), 2013 International Conference on. IEEE, 2013.

[11] Siddiqua, Ayesha, Kotari Sridevi, and Arshad Ahmad Khan Mohammed. "Preventing black hole attacks in MANETs using secure knowledge algorithm." Signal Processing And Communication Engineering Systems (SPACES), 2015 International Conference on. IEEE, 2015.