International Journal of Engineering Applied Sciences and Technology, 2017
Vol. 2, Issue 4, ISSN No. 2455-2143, Pages 19-25
Published Online February-March 2017 in IJEAST (http://www.ijeast.com)

REVIEW ON MANET- APPLICATIONS AND ROUTING PROTOCOLS WITH THE DETECTION AND PREVENTION OF BLACK HOLE ATTACK

Saurabh Kumar
Research Scholar (CSE)
Gurukul Vidyapeeth , Punjab

Tanya Gupta
Assistant Professor (CSE)
Gurukul Vidyapeeth , Punjab

Abstract—**MANET (Mobile Ad-Hoc Network) operates without centralized access point and physical fixed infrastructure. MANET is considered as astatic in nature. MANETs are distributed and self-directed networks. The development of different types of routing protocols has occurred in the recent past. MANETs are susceptible to different security attacks. In this paper, we have discussed the security attacks in MANET. The techniques and the methods for the detection and the prevention of Black Hole attack in network are also summarized. Black hole attack is a security threat by which the traffic is redirected to a node which actually does not exist in the network. The study of the existing work has shown that the work done on MANET security issues were dependent of varied reactive routing protocols but still a need is there for avoiding Black hole attack.**

Keywords —**MANET; Routing Protocols; Security attacks; Black Hole attack**

I. INTRODUCTION

Mobile Ad-hoc Network (MANET) [1] is a self-configuring infrastructure-less network. The absence of an infrastructure in ad hoc networks poses great challenges in the functionality of these networks. In MANET, all the devices are connected by wireless links. Every device in a MANET is free to move independently in all the directions. It can change its links to other devices frequently. Nodes are randomly connected with each other using arbitrary topology. They can act as both routers and hosts. The primary challenge in building a MANET [2] is equipping each device to continuously maintain the information which is necessary to properly route the traffic. More frequent connection tearing and re-associations can place an energy constraint on the mobile nodes. As MANETs are illustrated by limited bandwidth and node mobility, so, there is demand to take into account the energy efficiency of the nodes [3].

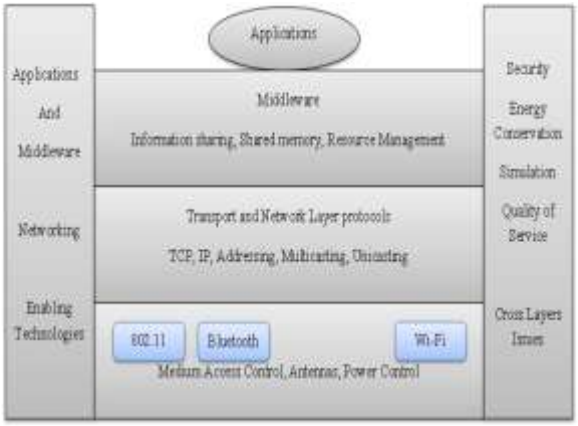
Applications
Applications
And
Middleware
Middleware
Information sharing, Shared memory, Resource Management
Security
Energy
Conservation
Simulation
Networking
Transport and Network Layer protocols
TCP, IP, Addressing, Multicasting, Unicasting
Quality of
Service
Enabling
Technologies
802.11
Bluetooth
Wi-Fi
Medium Access Control, Antennas, Power Control
Cross Layers
Issues

Fig.1. MANET Architecture

Above figure depicts MANET architecture [4] and shows a layered architecture in which the base layer consists of the technologies utilized in MANETs. The technologies have WI-FI, Bluetooth, and 802.11. The data packets are transferred via transport layer and network layer before it reach the application layer. The transport layer gives end-to-end services to data packets with the provision of connection-oriented data stream support by protocols such as User Datagram Protocol (UDP), TCP/IP, Stream Control Transport Protocol (SCTP) and Datagram Congestion Control Protocol (DCCP). The network layer is used for forwarding of the packets via in-between nodes by using techniques like unicasting /multicasting. When this is done, the data packets are being transferred via middleware before they are used with the users by different applications. The middleware is dependable for the collaboration between the mobile nodes in the network with the sharing of the information among the nodes analyzing the necessities and even controls the resources access. Once it is passed with all the layers, the end users used varied devices and applications to communicate via MANET [5].

MANET has become very vast in these days due to increase in its scalability, node mobility, dynamic nature etc. The applications of MANET are as follows [6]:

A. Emergency Services

It can be used in emergency operations where natural disasters or any accidents occur, where no network exists to provide them reliefs. It provides information from effected area, to the people for their help or to any local control posts. As soon as the control post comes to know about situation, they give responsibilities to the workers to help them as soon as possible and provide doctors and others help which they want at that time.

B. Military Battlefield

Military equipments contain some kind of computer equipments. Military take advantage of common place network technology to keep an information network between the vehicles, soldiers and military information headquarters using ad-hoc networks. From this field, the basic techniques of ad-hoc networks have originated.

C. Entertainment

Ad hoc networks can also link temporary multimedia network palmtop computers to share and spread information among participants at conference and classroom using notebooks, laptops and computers. It can be used as home networks where devices can communicate to exchange information directly. It can be used as peer to peer network in multi user game and in theme parks.

D. Commercial Environments

It can be used for the purpose of business in dynamic databases and mobile offices. In the field of E-commerce, it can help in the purchasing, like, we can purchase anything from anywhere and electronic payments can be made. In vehicular service, it can be used to transmit the information of road accident, inter vehicles network and road transmission. In sports stadium, taxicab utilizes ad-hoc networks.

E. Personal Area Network (PAN)

The interconnection between short range devices like mobile, PDA, laptops come under PAN communication in ad-hoc networks. The wired system is replaced by the wireless communications.

Routing Protocol [7] is second hand to find suitable routes between communicate nodes. It is a self-directed collection of mobile users that speak moderately over bandwidth constraint wireless link. Since the nodes are mobile, the network topology may change unpredictably over time. The network is de-centralized and all the network activities like discover the topology and delivering messages must be execute by the nodes [8]. They do not use any access point to bond to other nodes .It must be able to switch high mobility of the nodes.

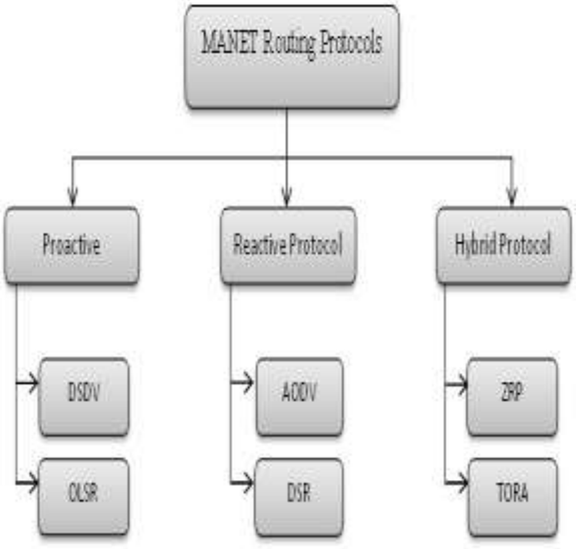

Fig.2.Routing protocols in MANET

MANET routing protocols could be broadly secret into three major categories as depicted in the table 1 as shown below:

Table-1 Routing protocols in MANET [9]

Routing Protocols		
Proactive	Reactive	Hybrid
It possesses in order of the purpose route before it is needed for the routing of data to the purpose.	A different proactive, reactive routing protocol does not make the nodes to start a route discovery process until a route to purpose is required.	The hybrid routing protocols occupy both reactive and proactive property by maintaining intra zone information pro-actively and inter-zone information reactively
The benefit of	The benefit of	Often re-active

these protocols is that a source node does not need route discovery actions to find a route to a purpose node.	these protocols is that overhead messaging is reduced which results in less usage of bandwidth.	or pro-active feature of a particular routing protocol might not be enough; instead a mixture might yield better solution
Disadvantage of this protocol is, it is slow as it has vast amount of traffic as these have to maintain a reliable and up-to-date routing table which requires substantial messaging overhead and thus uses large piece of the bandwidth to keep information up to date	Disadvantage of these protocols is the delay in discover a new route which leads to higher latency	The different types of hybrid routing protocols are: Core Extraction Distributed Ad Hoc Routing Protocol (CEDAR) Zone Routing Protocol (ZRP), Zone - Based Hierarchical Link State Routing Protocol (ZHLS).
The benefit of these protocols is that a source node does not need route discovery actions to find a route to a purpose node.		

Table-2 Main characteristics of routing protocols [10]

Routing Protocols	Route Acquisition	Flood	Delay	Multipath capability
DSDV	Priority computation	NO	NO	NO
DSR	On demand when required	Yes (More usage of caching lessens flood scope)	YES	Not Explicitly (Can quickly restores a route)
AODV	On demand when required	Yes, Conservative for reducing scope of flood	YES	Not exactly, the recent research shows viability
ZRP	Hybrid	Outside a source zone	Only if the destination is out sourced	NO

II. RELATED WORK

Alex Hinds, Michael Ngulube, Shaoying [12], focused on the range of available MANET routing protocols and discussed several features ranging from early protocols (e.g. DSDV) to higher level (e.g. MAODV).Protocol focused on Perkins' efforts to develop and improve MANET routing. ArunBiradar [13], focused on Mobile Ad Hoc Networks (MANETs) that consists of mobile platforms that are freely mobile. These are self-organizing and adaptive networks. These networks allow the spontaneous formation and deformation of mobile networks. The shortest path problem in MANETS requires that the path from the source node to the destination node be calculated, thereby, minimizing the sum of the total costs associated with the path Bow-Nan Cheng; Moore, S [14], proposed a comparative analysis of various routing protocols in MANET. Various routing protocols has been analysed like AODV, OLSR and OSPF-MDR. Their performance has been evaluated in terms of routing overhead traffic, end-to-end message completion rate, and end-to-end delay, to examine performance vs. Trade-off. ChetanaKhetmal,Prof.ShailendraKelkar,Mr.NileshBhosale, [15], has implemented black hole attack based on AODV, termed as BAODV Routing Protocol. NS2 Simulator is used for simulating MANET [using BAODV, SAODV, MANET, and CBR with FTP by taking 50 nodes]. SAODV is also proposed which is a secure routing protocol that verifies the destination nodes by exchanging the random numbers. SAODV has shown effective prevention of black hole attack (BHA) with better routing efficiency. Khalil, I.;

Bataineh, S.; Qubajah, L.; Khreishah, A[16], proposed Authenticated Routing for Ad hoc Networks with zoning (ARANz) based routing protocol for secure routing in MANET. It improves the routing by dividing the area into zones. It also saves the bandwidth. The performance of the Authenticated Routing for Ad hoc Networks with zoning (ARANz) is compared with other routing protocols and it has been seen that this algorithm works well. K. Chadhaand S. Jain [17], has presented the preventive measure for black hole attack in MANET. The black hole attack possess a serious security threat to the routing services by attacking the reactive routing protocols resulting in drastic drop of data packets. AODV (Ad hoc On-demand Distance Vector) routing being one of the many protocols often becomes an easy victim to such attacks. In such kind of attacks, a node advertises a shortest path for the given route request and redirects the data path through itself getting an easy access to all the data. NishuGarg,R.P.Mahapatra [18],has focused on incorporation of security mechanisms into the routing protocols in ad hoc networks. Fixed security solutions such as IPSec do not apply. The author studied AODV and developed a security mechanism to protect its routing information. M.Ramaiya,RohitGupt, Rachit Jain [19],has proposed DSDV, dynamic source routing (DSR) protocol and self-organizing on-demand distance vector (AODV) for efficient routing in different scenarios in Mobile Ad Hoc Network (MANET). Dynamic source routing, Mobile ad hoc networks (DSR), Ad Hoc on-demand distance vector (AODV) and Destination sorted by distance vector routing (DSDV) Zone Routing Protocol (ZRP) routing protocol are also discussed.

III. SECURITY ATTACKS IN MANET

All the mentioned protocols are susceptible to variety of security attacks. The attacks could be broadly classified in two categories namely passive attack and active attack [20].

In passive attack, the attacker does not obstruct with the usual operation of the routing protocol, however, only get the information via listening to the network traffic.

In active attack, the attacker changes the exchanged data that has deletion of the information too. Less attacks that are mostly encounter which disrupt the normal network behavior are worm hole, grey hole and black hole attack. In this review, we have focused on Black hole attack [21].

In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it . In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. After the establishment of route, the node will decide whether to drop all the packets or forward it to the unknown address. The method how malicious node fits in the data routes varies [22].

Below figure 5 shows the problem of black hole attack. In the figure, the node S is trying to send the data packet to node M and starts the route discovery process. M node will proclaim it as an active route for the particular destination when it has RREQ packets received from the source node. Then it will send the response to the S node before some another node. Node S believes that it is the adjacent active route to the destination and completion of active route discovery takes place. Node S ignores another replies and starts transferring the data packets to node M. The node M drops the data packets [23].

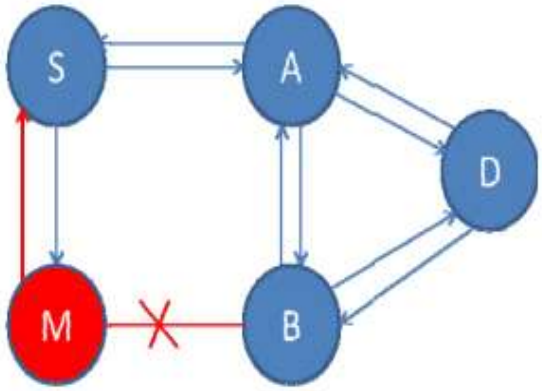

Fig.3.Black hole attack

Black hole is generally divided into two types [24]:

A. Single Black Hole Attack

In this type of attack, only single malicious node attacks on the route. The DSR protocol is susceptible to the well identified black hole attack.

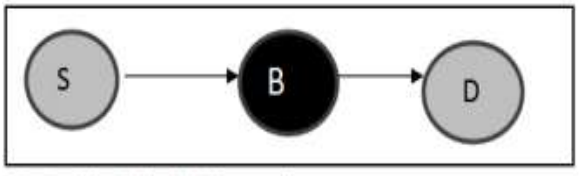

Fig.4. Single black hole attack

B. Co-operative Black Hole Attack

This type of attack means that the malicious nodes operate in a group. In this, the more composite form of the attack is Co-operative Black Hole Attack in which the multiple malicious nodes conspire jointly resultant in complete disturbance of the routing with packet forwarding functionality of the network.

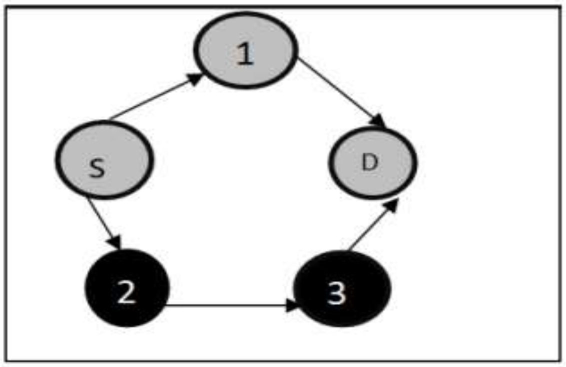

Fig.5. Co-operative black hole attack

The review of the techniques utilization of black-hole attack detection is shown in Table 3 by considering three aspects, namely, Speed, Power utilized and performance. The techniques discussed are, Cross layer cooperation, Trustiness and Neigbors, Route redundancy and Message Parameters, Fuzzy Logic, Mobile Agents and Clustering Algorithms.

Table-3 Summary of techniques used in Black hole attack

Techniques	Speed	Power utilized	Performance
Cross layer cooperation	Good	Low power utilized as computation level is less	Acceptable but cannot withstand in the co-operative attack
Trustiness and Neigbors	Good for black hole but slow in co-operative black hole attack	Moderate power utilized but more will be used in the centralized as compare to hybrid and distributed	Good with single black hole attack but cannot withstand in the co-operative attack
Genetic Algorithm	Moderate as soon as necessary data is presented	More power is utilized as the extensive output in these algorithms mainly in centralized node case	Good and could be utilized by means of co-operative black hole attack
Route redundancy and Message Parameters	Low with the use of multiple RREP with the sequence number in the process of detection	More power can be utilized for the processing of the control packets mainly in centralized strategies case	Good and secure
Fuzzy Logic	Moderate	More power utilized because of the heavy computation done on data for producing the attack degree in each node	Excellent and could be utilized with the cooperative black hole attack
Mobile Agents	Moderate	Moderate power utilized	Good and could be utilized by means of co-operative black hole attack
Clustering Algorithms	Moderate	More utilization of power	Excellent and could be used with cooperative black hole attack

IV. CONCLUSION

Because of the inherent infrastructure of MANET, the routing protocols are susceptible to black hole attack. Number of researchers has shown different technique types for preventing and detecting this type of attack. In the paper, different routing methods with their characteristics and the techniques used for the detection of the black hole attack are discussed with the existing solutions. For analyzing these methods, the comparison table is provided. Detecting a black hole attack in MANET is still taken as a challenging task.

From this review, following behavioral characteristics of black hole attack are examined:

- Black hole attack snoops on the neigbors for discovering the node to prepare for sending RREQ.
- Black hole attack propagates RREP by claiming that it contains direct link to the destination for some received RREQ.
- Black hole attack attempts for locating itself in the range of transmission of some source node for replying as soon as possible.

V. REFERENCES

1. R. K. Singh and P. Nand, “Literature review of routing attacks in MANET”, *International Conference on Computing, Communication and Automation (ICCCA)*, Noida, pp. 525-530, 2016.
2. M. Y. Barange and A. K. Sapkal, “Review paper on implementation of multipath reactive routing protocol in manet”, *International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, Chennai, pp. 227-231,2016.
3. M. Alinci, E. Spaho, A. Lala and V. Kolici, “Clustering Algorithms in MANETs: A Review”, *Ninth International Conference on Complex, Intelligent, and Software Intensive Systems*, Blumenau, pp. 330-335, 2015.
4. K. Liu, W. Shen, B. Yin, X. Cao, L. X. Cai and Y. Cheng, “Development of Mobile Ad-hoc Networks over Wi-Fi Direct with off-the-shelf Android phones”, *IEEE International Conference on Communications (ICC)*, Kuala Lumpur, pp. 1-6, 2016.
5. Asha and G. Mahadevan, “An adaptive cross-layer architecture to optimize QoS provisioning in MANET*”,* 3rd International Conference on Devices, Circuits and Systems (ICDCS), *Coimbatore*, pp. 115-119, 2016.
6. A. Kannammal and S. S. Roy, “Survey on secure routing in mobile ad hoc networks”, *International Conference on Advances in Human Machine Interaction (HMI)*, Doddaballapur, pp. 1-7, 2016.
7. H. Moudni, M. Er-rouidi, H. Mouncif and B. El Hadadi, “Performance analysis of AODV routing protocol in MANET under the influence of routing attacks”, *International Conference on Electrical and Information Technologies (ICEIT)*, Tangiers, pp. 536-542, 2016.
8. V. Matre and R. Karandikar, “Multipath routing protocol for mobile adhoc networks”, *Symposium on Colossal Data Analysis and Networking (CDAN)*, Indore, pp. 1-5, 2016.
9. D. N. Patel, S. B. Patel, H. R. Kothadiya, P. D. Jethwa and R. H. Jhaveri, “A survey of reactive routing protocols in MANET”, *International Conference on Information Communication and Embedded Systems (ICICES2014)*, Chennai, pp. 1-6, 2014.
10. R. Shenbagapriya and N. Kumar, “A survey on proactive routing protocols in MANETs”, *International Conference on Science Engineering and Management Research (ICSEMR)*, Chennai, pp. 1-7, 2014.
11. A. Daas, K. Mofleh, E. Jabr and S. Hamad, “Comparison between AODV and DSDV routing protocols in mobile Ad-hoc Network (MANET)”, *5th National Symposium on Information Technology: Towards New Smart World (NSITNSW)*, Riyadh, pp. 1-5, 2015.
12. Alex Hinds, Michael Ngulube, Shaoying Zhu, “A Review of Routing Protocols for Mobile Ad-Hoc Networks (MANET)”, *International Journal of Information and Education Technology*, vol. 3, no. 1, 2013.
13. ArunBiradar, “Effectiveness of Genetic Algorithm In Reactive Protocols For MANET”, *International Journal of Engineering Research & Technology* (IJERT), vol. 2, issue 7, 2013.
14. Bow-Nan Cheng; Moore, S., “A comparison of MANET routing protocols on airborne tactical networks”, *In Military*

Communications Conference – (MILCOM'12), vol., no., pp.1-6, 2012.

15. Chetana Khetmal, Prof.Shailendra Kelkar Mr.NileshBhosale, "MANET: Black Hole Node Detection in AODV*", International Journal of Computational Engineering Research*, vol. 03, 2013
16. Khalil, I.; Bataineh, S.; Qubajah, L.; Khreishah, A., "Distributed secure routing protocol for Mobile Ad-Hoc Networks", *In 5th International Conference on Computer Science and Information Technology (CSIT),* pp. 106-110, 2013.
17. K. Chadha and S. Jain, "Impact of black hole and grey hole attack in AODV protocol", *In International Conference on* Recent Advances and Innovations in Engineering (ICRAIE), pp. 1-7, 2014.
18. NishuGarg, R.P. Mahapatra, "MANET Security Issues", *International Journal of Computer Science and Network Security (IJCSNS),* vol. 9, no. 8, 2009.
19. M. Ramaiya and Rohit Gupta, "A Review of Reactive, Proactive & Hybrid Routing Protocols for Mobile Ad Hoc Network", *National Conference on Security Issues in Network Technologies (NCSI),* no.11, 2014.
20. L. Prashar and R. K. Kapur, "Performance analysis of routing protocols under different types of attacks in MANETs", *5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO),* pp. 405-408, 2016.
21. N. Sharma and A. Sharma, "The Black-Hole Node Attack in MANET," *Second International Conference on Advanced Computing & Communication Technologies*, Rohtak, pp. 546-550,2012.
22. S. Dhama, S. Sharma and M. Saini, "Black hole attack detection and prevention mechanism for mobile ad-hoc networks", *3rd International Conference on Computing for Sustainable Global Development (INDIACom),* New Delhi, pp. 2993-2996,2016.
23. M. A. Abdelshafy and P. J. B. King, "Resisting blackhole attacks on MANETs", *13th IEEE Annual Consumer Communications & Networking Conference (CCNC),* Las Vegas, NV, pp. 1048-1053,2016.
24. Sathish M, Arumugam K, S. N. Pari and Harikrishnan V S, "Detection of single and collaborative black hole attack in MANET", *International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET),* Chennai, pp. 2040-2044,2016.