A THROUGH INVESTIGATION ON ROUTING PROTOCOLS AND ROUTING ATTACKS IN MOBILE AD HOC NETWORKS

A.Arulselvan Gnanamonickam
Assistant Professor, Software System, KG College of Arts and Science, Coimbatore, India.

ABSTRACT: Mobile ad hoc networks (MANETs) consist of set of mobile nodes which is differentiated through a self-motivated and connected wireless links repeatedly, through by means of distinct routing protocols. Due to lack of definite central authority, mobility property, security in MANET possess several challenging issues. Several numbers of routing protocols and routing schema have been proposed and developed in the literature to deal with the security issues in MANET. The major focus of this survey paper is to the study of existing routing attacks and routing algorithm against MANET .This survey study on increasing a well-organized routing method in such an extremely self-motivated and resource management in MANET. At present several numbers of routing protocols have been proposed in literature against MANET. Several numbers of routing protocols in MANET are easily susceptible to a variety of kinds of attacks. In this survey, study on existing routing attacks such as such as link spoofing, black holes attacks and wormhole attacks during routing in MANET. This work survey gives the major issues of the state-of-the-art routing protocols, also examined and analyzed the solutions with table comparison .The performance accuracy of the various attacks is also examined based on the parameters like packet efficiency, routing overhead and throughput.

INDEX TERMS: Mobile ad hoc networks (MANET), routing protocols, single black hole attack, collaborative black hole attack, Gray hole Attack, Packet drop Attack; Wormhole Attacks ,Network layer.

1. INTRODUCTION

A mobile ad hoc network (MANET) is an assortment of mobile devices with the purpose of be able to converse through each other not including the make use of a predefined -infrastructure. In adding together the mobility is one of the major important properties in MANET, it has been created speedily at a very low cost, as it mightn't depend on existing network infrastructure. Because of this mobility property in MANET, it can be easily applicable to any applications such as disaster assistance, disaster operations, armed service, vehicle, campus and robot networks etc. [1]. Unlike the traditional network, a MANET is differentiated through comprises a self-motivated, constantly varying network topology appropriate to mobility of nodes [1]. However there are numerous issues concerning MANETs, like protection difficulty, restricted communication bandwidth [2], dynamic connection establishment [3] and limited hardware foundation processing ability [4].

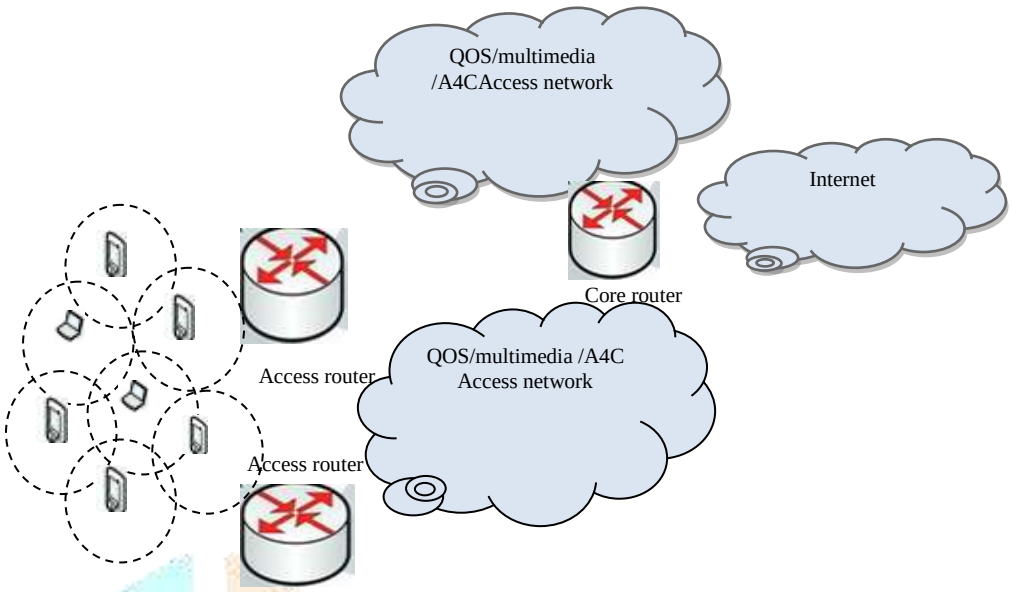

Figure .1: Overall architecture of MANET

Because of these problems routing performance in MANET becomes difficult .On the other hand management of resource constraints during routing i.e., restricted bandwidth and limited battery power possess a major challenging task in MANET. In MANET investigate focused on provided with the purpose of routing examination through lowest amount communication cost in terms of bandwidth and battery power. But still the management of resources with security threats possess several challenges, which is focused and researched in the wired and wireless networks [5], the in the same way difficult condition has been also occurred during this inherent design defects [6].

To conquer security problem in routing for MANET, recent work several number of routing protocols have been proposed and examination is done for each protocols. These proposed protocols are categorized into two types that are reactive routing protocols and proactive routing protocols. In reactive routing protocols for example consider Ad hoc On Demand Distance Vector (AODV) protocol is proposed in recent work [7] to find the routes between nodes in MANET. In proactive routing protocols for example consider Optimized Link State Routing (OLSR) protocol [8], attain routes through cyclic replace of topology information between nodes. But these protocols majorly rely on cooperation among nodes suitable to be deficient in centralized-administration and presume with the intention of each and every one nodes be truthful and well-mannered. During these routing protocols malicious node is able to initiate routing attack to interrupt routing operation or denial-of-service (DoS) attacks [9] to reject services to legal nodes.

Most of the previous work focused mainly on providing preventive schemes to protect the routing protocol in a MANET and these schemes are based on key management or encryption techniques to prevent unauthorized nodes from joining the network. The main drawback of these approaches is to introduce a heavy traffic load to exchange and verify keys, which is very expensive in terms of the bandwidth constraint for MANET nodes with limited battery and limited computational capabilities. In Hu et al. discuss these preventive schemes (e.g., authenticated routing for ad hoc net AODV (SAODV) [11]) in detail. But new attacks and countermeasures against a network layer attack, such as link spoofing and withholding of routing traffic have not been discussed in the literature.

In recently several number of the research works is done to protect MANET against routing attacks. These research works mainly rely on key management or encryption techniques to find unauthorized nodes in MANET. The main drawback of key management or encryption techniques is with the purpose to establish an intense traffic load for key exchange and management process between nodes, which is very costly in conditions of the bandwidth restriction designed for MANET nodes. So in practical applications these methods will not directly apply to MANET. Among them several number of attacks, black hole attacks becomes one of the major important issue to MANET for routing. Some of the research is done in recent work [10-11] to solve the black hole attack and prevent black hole attack in MANET, but still it is incapable to prevent entirely. However, these methods are not applicable to detect the network layer attacks, such as link spoofing and wormhole attacks have not been conversed in the literature [12].

In this survey we mainly focus on the study of the existing routing protocols against the routing attacks such as link spoofing, wormhole attacks, black hole attacks and flooding attacks in a MANET. The entire survey is summarized as follows. In section 2

mainly study the details of existing categories of routing protocols against several number of routing attacks in MANET .In the Section 2 provide the information about the inference of existing routing protocols methods against routing attacks .How to solve the inference from the existing methods is also discussed in Section 3 .In Section 4 analysis the results of existing routing protocols is compared and graphically represented. At end of the work we conclude the survey work and scope of the future work is discussed in detail 5.

2. SURVEY OF ROUTING PROTOCOLS AND ROUTING ATTACKS IN MANET

In this work the section 2 becomes very important since it majorly study the details of existing routing protocols against routing attacks in MANET. These routing protocols are majorly categorized into three types such as proactive, reactive and hybrid routing protocols.

Proactive (table-driven) Routing Protocol: This type of protocol is also named as table-driven routing protocol. In this table-driven routing protocol, mobile nodes might be periodically communicated through each nodes based on their routing information of the neighbors nodes in MANET. During routing process each nodes in the MANET maintain separate routing table to record the node information and hop count value of the path is also recorded in routing table. The major shortcoming of this type of routing protocol is that network overhead communication cost problem is raised if the size of the network size increases. The major merit of this protocol is that malicious attacker is easily prevented in MANET. For example consider destination optimized link state routing (OLSR) [13] protocol is under the category of Proactive (table-driven) Routing Protocol with improved packet delivery ratio and attack detection results , but major shortcoming of this OLSR protocol is that higher routing overhead problem occurs during routing process.

Reactive (on-demand) Routing Protocol: The type of protocol is performed based on transmission of data packets between nodes. The key advantages of Reactive (on-demand) Routing Protocol are that it requires less bandwidth during broadcast communication. The major shortcoming of these protocols is it leads to high packet loss. For example consider two methods such as Enhanced Classified Ad-hoc on Demand Distance Vector protocol (ECAODV) [14]and dynamic source routing (DSR) [15] protocol have proposed in recent work and discussed in the literature.

ECAODV performs a routing protocol based on the unique key management is designed for less cost and establishing secure communication among nodes in MANET. The proposed ECAODV create session key using sign encryption and symmetric Blowfish encryption schema among nodes with secure data communication is performed. The ECAODV establishes high security process through less communication cost and computational complexity. The major key advantage of this protocol is that it solves routing overhead problem, but the major issue of the protocol is that high packet loss is occurred during routing.

Hybrid Routing Protocol: The Reactive (on-demand) Routing method problem is solved by using hybrid routing protocol. The hybrid routing protocol combines the procedure of proactive and reactive routing protocols to solve the issues of these protocols. Many of the Hybrid Routing is developed based on the hierarchical or layered network structure. Some of the routing protocols are temporally-ordered routing algorithm (TORA) [15] and zone routing protocol (ZRP) [16].

This routing protocol is mainly applied to detect routing attacks in MANET, these should be described in detail in the following section

Attacks and attacks detection methods: A wormhole attack [17] is individual of the majority superior and rigorous attacks in MANETs. In this wormhole attack, attackers store the information about the packets at individual position and replay to one more position by means of a confidential high rapidity network. In recent work, packet leashes schema [17] is developed to detect and prevent the wormhole attack against MANET. In this packet leashes schema, two categories of leashes such as temporal leashes and geographical leashes are introduced to detect and prevent wormhole attack. In temporal leash schema, each and every node determines the packet running out time relies on the speed light c and based on the distance L between the nodes. The major shortcoming of this temporal leash schema is that it desires each and every one node to comprise strongly synchronized clocks.

Statistical analysis of multipath (SAM) is proposed in [18] to detect and prevent the wormhole attack through use of multipath routing schema. This SAM method detects the wormhole attack via determining the frequency of every one link with the intention of emerges in each and every one of the attained routes beginning single route discovery. In this schema the nodes with very highest frequency is

recognized as the wormhole attack in MANET. The major advantages of this SAM schema is that it requires less communication and computation overhead during multipath routing for MANET, But the major shortcoming of this schema is that it is not easily applicable to non-multipath routing protocol (AODV protocol).In a black hole attack, an unauthorized node sends false routing information to source node to find exact routing information. For example consider, in AODV, the unauthorized attacker be able to send a false routing information in the direction of the source node to choose the route with the intention of passes during the attacker

In recent work, Jaisankar et al [19] develop a novel security schema to detect black hole attack which consists of two major part, recognition and reaction. In the, recognition stage, each and every node contains field_next_hop information in the direction of the RREP packet, earlier than source node sends the data packets. The RREP packet is inspecting among middle node and destination node. Each node in the network maintain the black identification table (BIT), to detect the black hole attack and BIT consists of the following fields such as <source, target, current_node_ID, Packet_received_count (PRC), Packet_forwarded_count (PFC), Packet modified count (PMC)>. Then the PMC is continuously altered based on the BIT. If the behavior of the node is identified as corrected then count value is multiplied to PMC or else it is distinguish from sending packets. If the specific node is identified as black hole, then it is stored in isolation table (IT) along with their ID. The novel security schema achieves a high packet delivery ratio and less packet loss than the traditional schemas.

Nital Mistry et al [20] proposed a modified AODV routing protocol based on the newly added table Cmg_RREP_Tab to detect black hole attack depending on the MOS_WAIT_TIME and RREP_WAIT_TIME. In the modified AODV routing protocol schema, RREP_WAIT_TIME is determined based on sending RREP request to source node. MOS_WAIT_TIME is determined by dividing the RREP_WAIT_TIME value by two .The information RREP_WAIT_TIME, their request is stored in newly table Cmg_RREP_Tab to store the information about black hole nodes to control message beginning these nodes. The results of the proposed schema attains 81.811% DR for varied network size, 70.877% PDR is attained for varied mobility. Conversely, the major shortcoming of this protocol is that end-to-end delay results is increased 13.28% for varied network size, and 6.28% for varied mobility adjusting, it becomes unsuccessful to discover the collaborative black hole attack.

Ming-Yang Su [21] develops a novel anti-black hole mechanism (ABM) system to detect the black hole attacks in MANET. In initial stage of the work nodes perform the ABM function in a sniff mode. Regarding the unbalanced differentiation among the routing information transmitted beginning a doubtful node, an assessment of the mistrustful node be able to be predictable through ABM. If the present value of ABM goes beyond the pre-specified threshold value, then it is considered as black hole .Jaydip Sen et al [22] develop a novel schema to detect cooperative black hole attack in MANET. In consists of two malicious nodes and interrupt the packets during transmission, it fall them not including forwarding it. To sustain such attack the general procedure of the AODV routing protocol is modified into new routing protocol schema based on the Data Routing Information (DRI) table for each nodes in MANET. In this two parameters is used to detect black hole attacks, one is used to store the information of data packet through destination node in the route and another one is used to store the information of data packet through source node in the route.

The major objective of the flooding attack is to weaken the network resources such as bandwidth of the network and battery power. Yi et al [23] develop a novel mechanism to detect and prevent the flooding attack in the AODV protocol. In this method each node maintains the information of RREQ. If the value of RREQ rate exceed to pre-specified threshold function, then the corresponding node is considered as the flooding attack node and added to blacklist. But the major shortcoming of this approach if the specific node is flooding attack if it doesn't attain the threshold value then it is considered as normal node. Desilva et al [24] develop an adaptive schema to alleviate the result of a flooding attack. It makes use of a numerical examination to distinguish malicious RREQ floods and keep away beginning the promoted of such packets. This schema is similar to [23], instead of predefined threshold, threshold is decided relying on statistical analysis, which decreases the collision of the flooding attack.

3. INFERENCE FROM EXISTING METHODS AND SOLUTION

- In recent work, packet leashes schema [17] is developed to detect and prevent the wormhole attack against MANET. In this packet leashes schema, two categories of leashes such as temporal leashes and geographical leashes are introduced to detect and prevent wormhole attack.The major shortcoming of this temporal leash schema is that it desires each and every one node to comprise strongly synchronized clocks.
- Statistical analysis of multipath (SAM) is proposed in [18] to detect and prevent the wormhole attack through use of multipath routing schema. The major advantages of this SAM schema is that it requires less communication and computation overhead

during multipath routing for MANET ,But the major shortcoming of this schema is that it is not easily applicable to non-multipath routing protocol (AODV protocol).

- Jaisankar et al [19] and Nital Mistry et al [20]. Conversely, the major shortcoming of this protocol is that end-to-end delay results is increased 13.28% for varied network size, and 6.28% for varied mobility adjusting, it becomes unsuccessful to discover the collaborative black hole attack.
- Ming-Yang Su [21] develops a novel anti-black hole mechanism (ABM) system to detect the black hole attacks in MANET. The major shortcoming of this ABM schema is that packet loss rate is 14.76% for cooperative black hole attack and fails to detect collaborative black hole attacks.
- Yi et al [23] develop a novel mechanism to detect and prevent the flooding attack in the AODV protocol. But the major shortcoming of this approach if the specific node is flooding attack if it doesn't attain the threshold value then it is considered as normal node.
- Desilva et al [24] develop an adaptive schema to alleviate the result of a flooding attack. This schema is similar to [23], instead of predefined threshold, threshold is decided relying on statistical analysis, which decreases the collision of the flooding attack.

Table 1 Comparison of link spoofing, black holes attacks and wormhole attacks Detection Schemes

Schema	Simulator	Detection type	Year	Results	Defects
Leashes: temporal leashes and geographical leashes.	NS2 simulator	Wormhole attack	2005	High packet delivery ratio	The major shortcoming of this temporal leash schema is that it desires each and every one node to comprise strongly synchronized clocks.
Statistical analysis of multipath (SAM)	-	Wormhole attack	2010	Higher packet delivery ratio and lower packet loss rate	But the major shortcoming of this schema is that it is not easily applicable to non-multipath routing protocol (AODV protocol).
AODV Protocol	NS2 simulator	Black hole attack	2010	Conversely, the major shortcoming of this protocol is that end-to-end delay results is increased 13.28% for varied network size, and 6.28% for varied mobility adjusting,	Conversely, the major shortcoming of this protocol is that end-to-end delay results is increased 13.28% for varied network size, and 6.28% for varied mobility adjusting, it becomes unsuccessful to discover the collaborative black hole attack.
anti-black hole mechanism (ABM)	-	Black hole attack	2010	No simulation results	The major shortcoming of this ABM schema is that packet loss rate is 14.76% for cooperative black hole attack and fails to detect collaborative black hole attacks.
AODV protocol in which Data Routing Information (DRI)	QualNET	Black hole attack	2011	The PDR is always Achieves higher than 90%	-
Simple mechanism to prevent the	NS2 simulator	flooding attack	2005	Less PDR ratio	Flooding threshold has to be set lower than which the

flooding attack in the AODV protocol					flooding attackmight not be detected. Higher packet loss rate
Adaptive technique	QualNET	flooding attack	2005	The packet delivery ratio(PDR) is not improved	The other types of the attacks not detected.

SOLUTION: Among them all of the existing routing protocols and routing methods is only applicable to the specific attacks. However these security routing protocols, not entirely solves the QOS parameters such as end to end delay, packet delivery ratio, throughput etc.,not improving the effectiveness with reduced network cost for a MANET environment .This work will be extended to apply detect the all types of attacks in MANET. In the future work the present issue is solved by applying the single method to detect all types of attack. To perform this process classification methods or other data mining methods which detects each attack and optimal to find route path .Also focus on exploring, as well as preventing all possible attacks to make a MANET a secure and reliable network.

4. EXPERIMENTATION RESULTS

In order to assess the performance accuracy of the different schema under various attacks simulated a mobile ad hoc network (MANET). For experimentation work considers the following assumption with the purpose of the network has no preexisting transportation and with the purpose of the employed Ad hoc On Demand Distance Vector (AODV) protocol. The schemas were implemented in the network simulation tool NS2Simulator. In the simulation model 25 mobile nodes placed randomly inside a 1000 x 1000 meter square region area with transmission range of 250 m. Each and the channel capacity was 512 bytes. In initial stage of the simulation, each node stay designed for a pause time 10 seconds, then moves towards a destination through a speed consistently lying among zero and the maximum speed. The maximum speed is set 20 m/s, correspondingly, and pause times at 10 seconds. The simulation setup time of the experiment was 900 seconds.

Table 2. SIMULATION PARAMETERS

Examined protocol	**AODV**
Simulation tool	NS2Simulator
Simulation time	**900 seconds**
Number nodes	**25**
Transmission range	**250 m**
Maximum speed	**20 m/s**
Pause time	**10 s**
Maximum connections	**10**
Packet size	**4 pxt/sec**

In this section measure the experimentation results of the different routing attacks under number of nodes. In Figure 2 it measures the experimentation results of node density effects based on the packet efficiency. The packet efficiency of the different attacks is determined based on the number of 30 nodes in the MANET network. It also shows that packet efficiency of black hole, wormhole and flooding attack is slightly varied with each other. In this survey implementation of flooding attack achieves higher packet efficiency when compare to other existing attacks based on the source to destination communication based on hop count ,here the neighboring nodes maintain route table to update the route information form source to destination in MANET. This becomes increased packet efficiency.

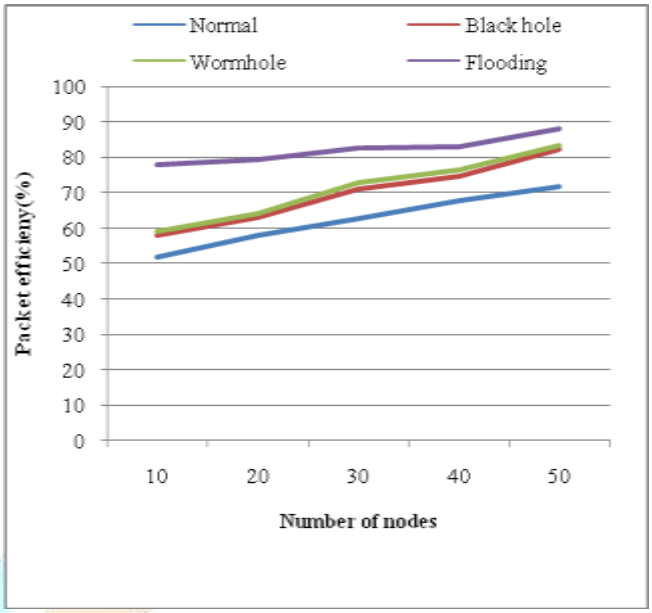

Figure 2: Packet Efficiency normal and under attack scenarios withno mobility and varying total number of nodes in simulation

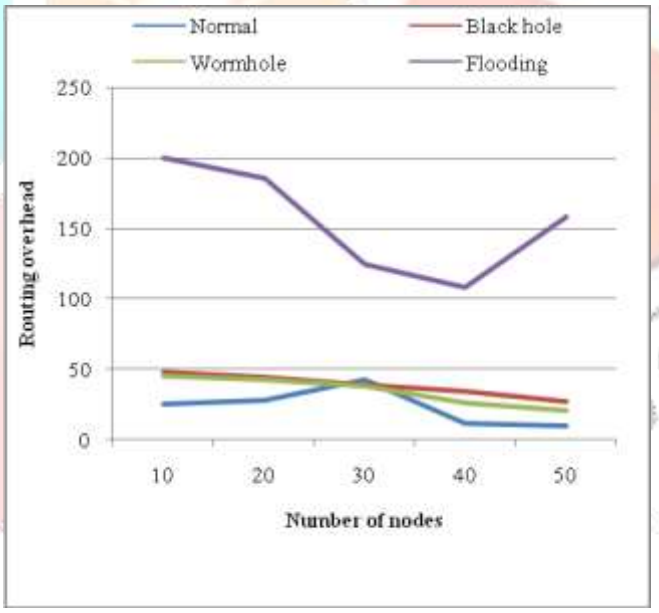

Figure 3: Routing Overhead normal and under attack scenarios with no mobility and varying total number of nodes in simulation.

Figure 3 shows performance comparison results of the routing attacks based on the routing overhead under several numbers of nodes in the MANET. Figure 3 observed that the performance comparison of routing overhead for flooding attack becomes very high when compare to other type of attack, since they send false reply in the direction of the routing process and create extra routing packets.

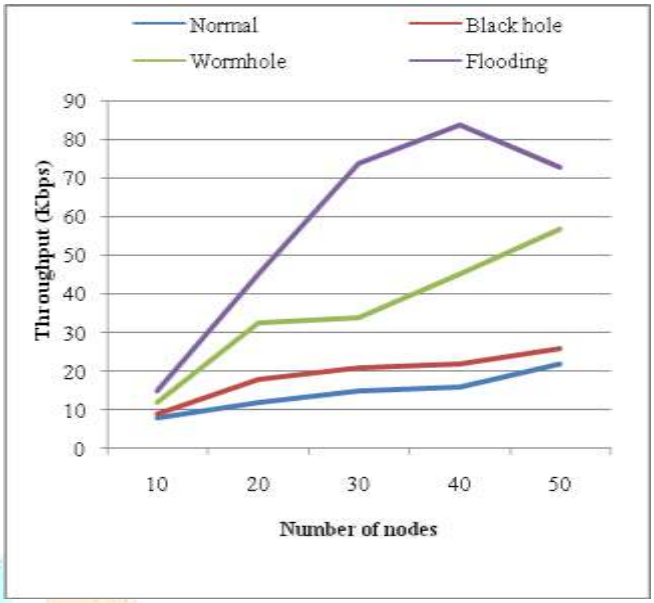

Figure 4: Throughput normal and under attack scenarios with no mobility and varying total number of nodes in simulation

Figure 4 shows the performance comparison results of the routing attacks based on the throughput under several numbers of nodes in the MANET effect of the attacks on throughput. If the packet delivery ratio of the routing attacks is increased it automatically increases throughput. It is observed that the flooding attack doesn't attain the degradation in throughput since hello packets maintain the intermediate busy and information packets do not obtain distributes. This will increase the throughput results for flooding attacks under 30 nodes and the numbers of senders have been also increased.

5. CONCLUSION AND FUTURE WORK

A MANET is anew emerging network technology because of the mobility and it is attracted by several numbers of researchers in recent years. Providing a security to MANET becomes a major serious issue in recent years. However there are numerous issues concerning MANETs, like battery power, protection difficulty, restricted communication bandwidth, computational power and it lacks a consistent centralized management. In this survey, majorly concentrated to the study of the conventional routing algorithm and attacks against MANET. The major issues of the existing conventional routing algorithm and attacks are also studied in detail. To solve routing problem in MANETs, have been also developed and examined by several number of researchers in the literatures against various categories of the attacks such as black hole, wormhole attack and link spoofing attack problem .In comparison of all routing protocols methods hybrid routing protocol becomes more advantages which solves the defects of existing routing protocols. This survey also determines the attacker's misconduct exploit is the key factor. It will advantage new researchers to understand the existing and every one proposed resolution to precise attack. In the future work the present issue is solved by applying the single method to detect all types of attack. To perform this process classification methods or other data mining methods which detects each attack and optimal to find route path .Also focus on exploring, as well as preventing all possible attacks to make a MANET a secure and reliable network.

REFERENCES

1. S. Ci et al., "Self-Regulating Network Utilization in Mobile Ad-Hoc Wireless Networks," IEEE Trans. Vehic. Tech., vol. 55, no. 4, July 2006, pp. 1302–10.
2. Sarma N, Nandi S (2010) Service differentiation using priority-based MAC protocol in MANETs. International Journal of Internet Protocol Technology 5(3):115–131. doi: 10.1504/IJIPT.2010.035383
3. Yang S-J, Lin Y-C (2009) Static and Dynamic RED Tuning for TCP Performance on the Mobile Ad Hoc Networks. Journal of Internet Technology 10(1):13–21

4. Dow CR, Lin PJ, Chen SC, Lin JH, Hwang SF (2005) A Study of Recent Research Trends and Experimental Guidelines in Mobile Ad-hoc Networks. Paper presented at the IEEE 19th International Conference on Advanced Information Networking and Applications, Tamkang University, Taiwan, 28-30 March 2005
5. Zhou L, Chao H-C (2011) Multimedia Traffic Security Architecture for the Internet of Things. IEEE Network 25(3):29–34. doi: 10.1109/MNET.2011.5772059
6. Humaira Ehsan, Farrukh Aslam Khan. Malicious AODV Implementation and Analysis of Routing Attacks in MANETs. 11th International Conference on Trust, Security and Privacy in Computing and Communications, IEEE, 2012.
7. C. Perkins, E. Belding-Royer, and S. Das, "Ad Hoc Ondemand Distance Vector (AODV) Routing," IETF RFC 3561, July 2003.
8. Th. Clausen et al., "Optimized Link State Routing Protocol," IETF Internet draft, draft-ietf-manet-olsr-11.txt, July 2003.
9. A. Shevtekar, K. Anantharam, and N. Ansari, "Low Rate TCP Denial-of-Service Attack Detection at Edge Routers," IEEE Commun. Lett, vol. 9, no. 4, Apr. 2005, pp. 363–65.
10. Raja Mahmood RA, Khan AI (2007) A Survey on Detecting Black Hole Attack in AODV-based Mobile Ad Hoc Networks. Paper presented at the International Symposium on High Capacity Optical Networks and Enabling Technologies, Dubai, United Arab Emirates, 18-20 November 2007
11. Saini A, Kumar H (2010) Comparison between Various Black Hole Detection Techniques in MANET. Paper presented at the National Conference on Computational Instrumentation, Chandigarh, India, 19-20 March 2010.
12. B. Wu et al., "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks," Wireless/Mobile Network Security, Springer, vol. 17, 2006
13. Jacquet P, Muhlethaler P, Clausen T, Laouiti A, Qayyum A, Viennot L (2001) Optimized Link State Routing Protocol for Ad Hoc Networks. Paper presented at the IEEE International Multi Topic Conference, Lahore, Pakistan, 28-30 December 2001
14. Noorul Amin, Nizamuddin, Abdelmuttlib Ibrahim, "ECAODV: Enhanced Classified Ad-Hoc on Demand Distance Vector Routing Protocol". Emerging Trends and Applications in Information Communication TechnologiesCommunications in Computer and Information Science Volume 281, 2012, pp 92-100.
15. Khiavi, M. V., Jamali, S., & Gudakahriz, S. J. (2012). Performance comparison of AODV, DSDV, DSR and TORA routing protocols in MANETs. International Research Journal of Applied and Basic Sciences, 3(7), 1429-1436.
16. Gandhi, S., Chaubey, N., Shah, P., & Sadhwani, M. (2012, January). Performance evaluation of DSR, OLSR and ZRP protocols in MANETs. In Computer Communication and Informatics (ICCCI), 2012 International Conference on (pp. 1-5). IEEE.
17. Y-C. Hu, A. Perrig, and D. Johnson, "Wormhole Attacks in Wireless Networks," IEEE JSAC, vol. 24, no. 2, Feb. 2006.
18. L. Qian, N. Song, and X. Li, "Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks Through Statistical Analysis of Multi-path," IEEE Wireless Commun. And Networking Conf. '05.
19. Jaisankar N, Saravanan R, Swamy KD (2010) A Novel Security Approach for Detecting Black Hole Attack in MANET. Paper presented at the International Conference on Recent Trends in Business Administration and Information Processing, Thiruvananthapuram, India, 26-27 March 2010.
20. Mistry N, Jinwala DC, IAENG, and Zaveri M (2010) Improving AODV Protocol againstBlack hole Attacks. Paper presented at the International MultiConference of Engineers and Computer Scientists, Hong Kong, 17-19 March, 2010
21. Su M-Y (2011) Prevention of Selective Black Hole Attacks on Mobile Ad Hoc Networks Through Intrusion Detection Systems. IEEE Computer Communications 34(1):107–117.
22. Jaydip Sen, Sripad Koilakonda, Arijit Ukil, "A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks," Second International Conference on Intelligent Systems, Modelling and Simulation, 2011.
23. P.Yi, Z.Dai, S.Zhang, Y.Zhong. "A New Routing Attack in Mobile Ad Hoc Networks," International Journal of Information Technology vol. 11, no. 2, pp. 83-94, 2005.
24. S.Desilva, and R.V.Boppana, "Mitigating Malicious Control Packet Floods In Ad Hoc Networks," Proceedings of IEEE Wireless Communications and Networking Conference 2005, , vol. -4, pp. 2112-2117, March 2005