A Survey on Detection and prevention of flooding attack in MANETs

[1]Ankita patel,[2]Ankitpatel

[1]Department of Information Technology, [2]Department of CSE,
[1]Shri S'adVidyaMandal Institute of Technology, [2]Shri S'adVidyaMandal Institute of Technology,
[1]Bharuch, Gujarat, India, [2]Bharuch, Gujarat, India

***Abstract* - MANET is one of the wireless networks that have attracted concentration of many researchers as the demand for MANETs is increasing day by day. Due to lack of centralized architecture and dynamic topology, MANET is prone to various security attacks. Our focus is to detect and prevent flooding attack in MANET. Flooding attack is a kind of the security threat in which attacker node send a huge amount of packets to other nodes. Our aim is to provide a solution which can detect the attacker and prevent it from entering the route. Our aim is to overcome the limitations of existing approaches for prevention of flooding attack. We would then simulate our approach on the network simulator and test our approach using various parameters such as PDR (Packet delivery ratio), throughput, delay.**

***IndexTerms* - detection,prevention,flooding attack,ad-hoc network.**

I. INTRODUCTION

MANET is a known as wireless ad-hoc network. It is a one kind of small network that is connected with mobile network through a wireless link. The MANET is a continuously self-configuring and infrastructure-less network of a mobile devices which is wireless in specific. It is a collection of wireless mobile nodes which communicates with each other without use of any centralized authority [1].

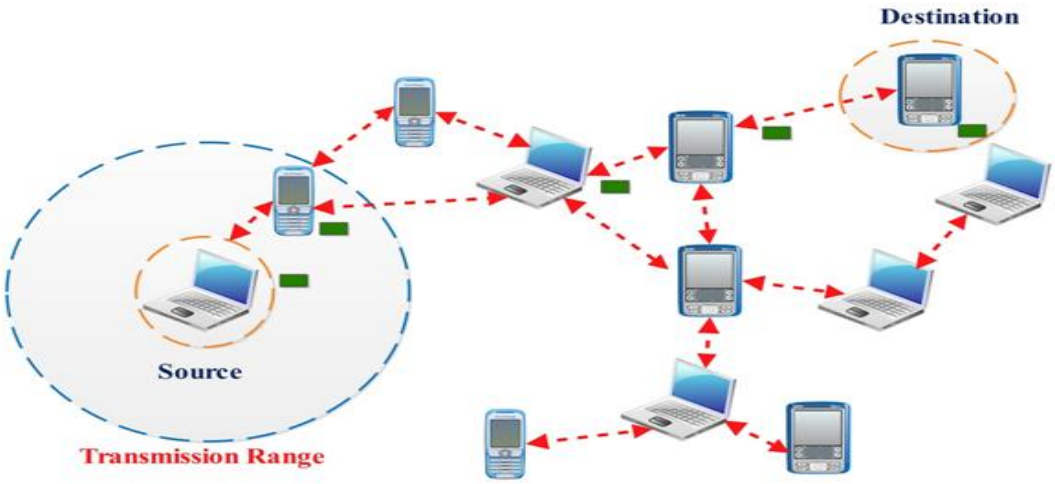


Figure 1.1 Architecture of MANET [1]

A. CHARACTERISTICS ON MANET

- Distributed operation - There is a distributed network among all the nodes [1].
- Multi hop routing - There is a one intermediate node which is used to transfer data to outside the range [1].
- Autonomous terminal - It means separate node that is work as host node and also work as router node [1].
- Dynamic Topology - Nodes are for to move itself with different speed thus, the network topology may change randomly and at any time [1].
- Light weight terminal - It has a low power capacity and small memory size [1].
- Shared Physical Medium - In this characteristic there is no restriction to access the channel [1].

B. ADVANTAGES OF MANET

- It is free from centralized network.
- It is very expensive.
- Improve Scalability and flexibility.
- It is very robust.
- It is scalable because we can add more nodes [1].

C. Problem Definition

According to Literatureanalysis node and meaning in ad-hoc network and source node always search for destination node. So when it detects flooding attack message and packet loss increases. So using proposed system improves according of existing system.

II. Classification of routing protocol

There are main three classification of routing protocol.

- Proactive
- Reactive
- Hybrid

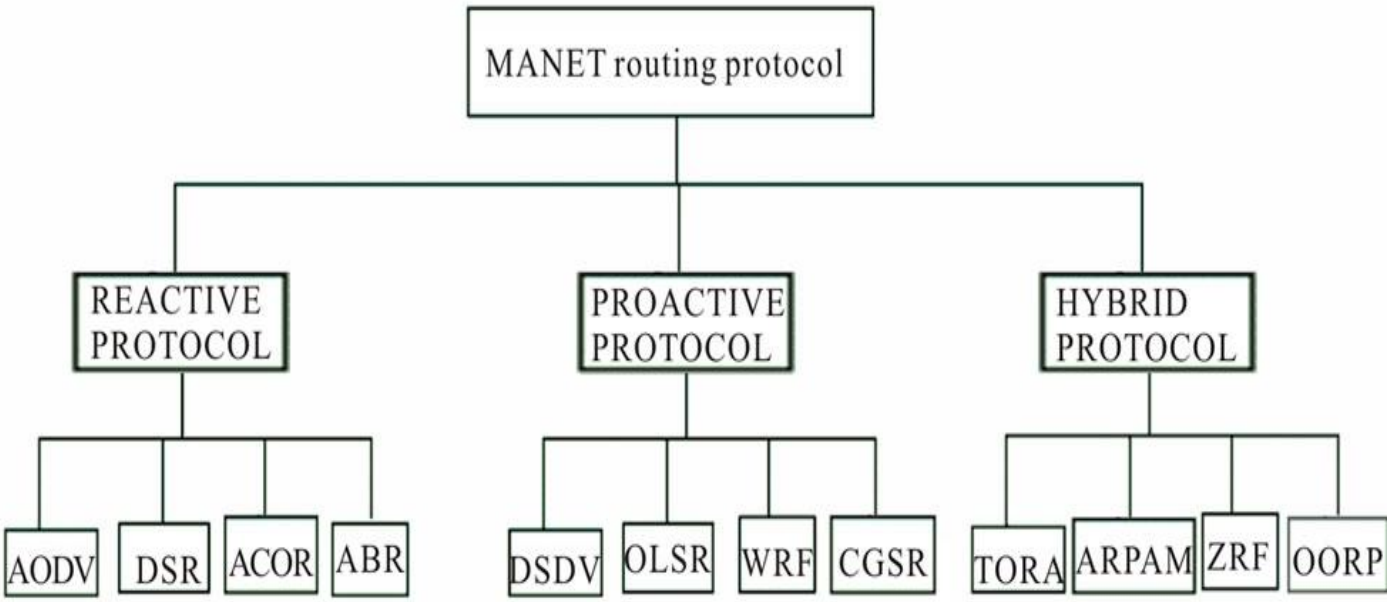


Figure 2.1 Classification of routing protocol [2]

A. Proactive protocol

It is also known as a Table driven routing protocol. It stores all the routing information in the routing table of all nodes which are in network. If any update regarding network changes, each node should notify and update operation is completed[2].

Example:- DSDV(Destination Sequence Distance Vector), OLSR(Optimized Link State Routing), WRP(Wireless Routing Protocol)

B. Reactive protocol

It is also known as an on demand routing protocol. If there is no communication it does not stored any routing information and routing activity at the network nodes [2].

Example:- AODV(Ad-hoc On Demand Distance Vector), DSR(Destination Source Routing)

C. Hybrid Routing protocol

Hybrid routing protocol is combination of proactive routing protocol and reactive routing protocol. It is increase scalability [2].

Example:-ZRP(Zone Routing Protocol)

III. Attack

There are two different level of attack. The first level is for routing mechanism and second level is for damaging the security mechanism. There are classified in two types attack.

- Active attacks
- Passive attacks

A. Active attack

The attackers reduce the performance of network and make the change in data. Active attacks are also divided in to two categories.

- Internal Attack - Internal attacker takes out nodes which are part of network.

- External Attack - External attacker takes out nodes which are not the part of network.

B. PASSIVE ATTACK

It listens the tack between the nodes. The attacker does not break into the system.

- Flooding attack - Flooding attack is an active attack. In which attacker exhausts the network resources and distributed the routing operation. The flooding attack occurs where network is unable to process genuine request. Since it is weighted down by invalid request. It is most advantages of naturally utilizes every path through the network, it will also the shortest path.

A. HELLO FLOODING

The attacker node spread the hello packet with high power. In this flooding method source node transmit the packet to the destination node by best path. As a shown in figure2.3, here the attacker broadcasts hello packet with very high Power transmission than the base station. As a shown in figure 2.4, here the legitimate nodes consider attacker as the parent as well as neighbour node and start forwarding the packets.

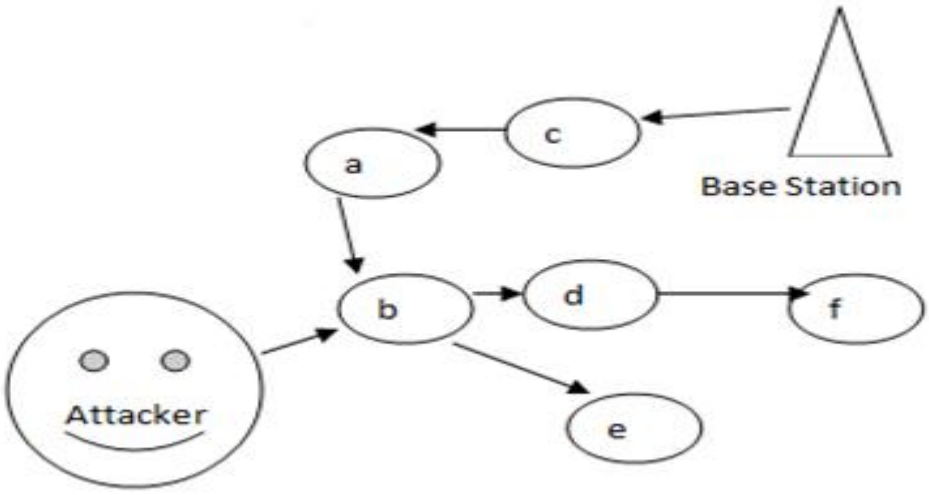


Figure 2.3. Hello flooding broadcast mechanism[1]

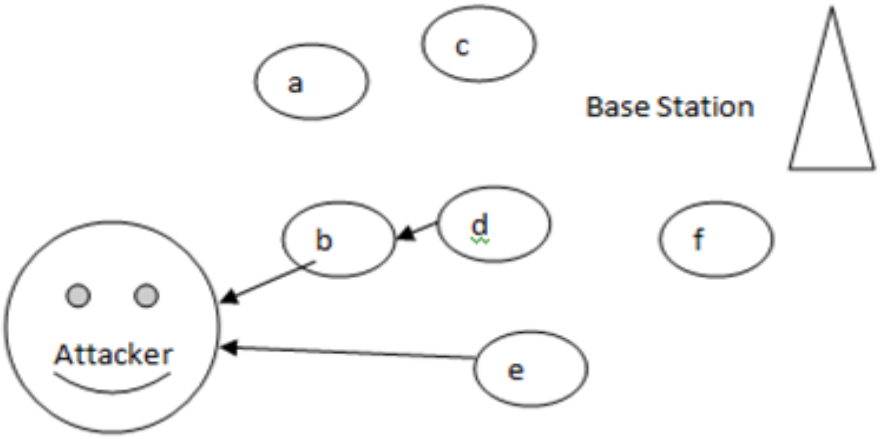


Figure 2.4. Hello flooding packet transmission[1]

B. RREQ FLOODING

The attacker select the IP address that not a part of network and broadcast the neighboring node in RREQ packet as shown in figure.

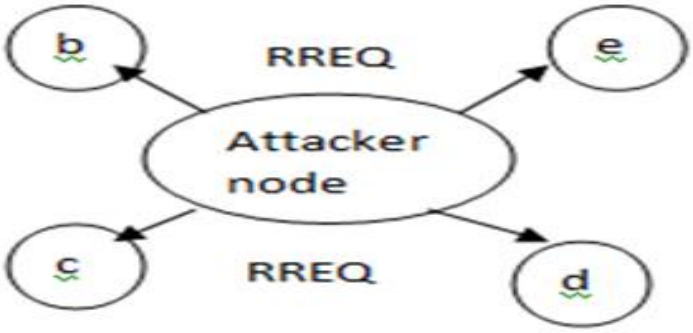


Figure 2.5. RREQ mechanism[1]

C. DATA FLOODING

The attack worst node make the path for all nodes and then start sending useless packets to require the network bandwidth in shown figure.

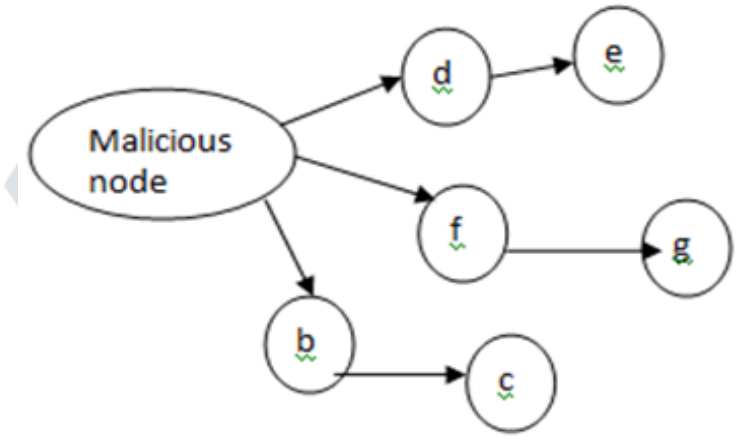
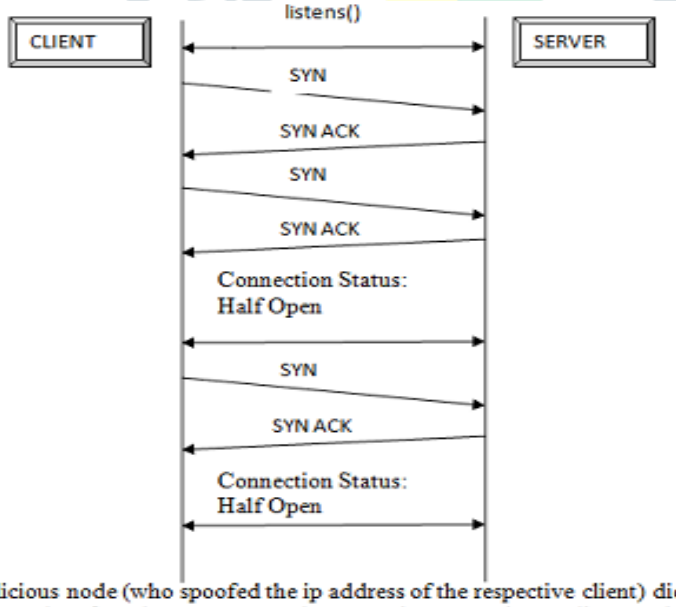


Figure 2.6. Data flooding mechanism

D. SYN FLOODING

The attacker sends more amount data of synchronization packet to the destination node. As shown in figure.



malicious node (who spoofed the ip address of the respective client) didn't send final ACK to the server, therefore the server not only wastes its energy by sending continuous SYN ACK to the request but also denies the request of other clients.

Figure 2.7 SYN flood mechanism

IV. LITERATURE REVIEW

C.M. Nalayini et.al in[1] this paper aims to understand the MANET structure, its properties, routing knowledge and the necessity to develop an efficient algorithm or technique to prevent, detect and control different of flooding attack in MANET. The wireless networks are used for almost all kinds of data transmission security of the data that is being transmitted has a very important role.

BandanaMahapatraet.al in [2] this paper, a novel technique is discussed which is used to identify the flooding attack and measure to overcome them using multi agent system. The Multi Agent system solved efficiently load balancing problem as well as provided alternative solution but increased the computational overhead on part of the node while generating agents or causing increase in overall network traffic by launching multiple routing messages as Agents. These technique is used for checking for possibilities of flooding attack in the network, identifying malicious nodes and taking effective measures to block the node. Every agents launch additional cost on the node hence death of an agent due to flooding attack can be considered as a heavy loss on the part of the node.

JasmeenMangat et.al in[3] this paper, a new form of attack is discussed named spoofed flooding attack in which the attacker node participate the node ID capture attack. The attacker node clones the ID of some genuine node and floods the network with RREQ packets. The node are presents a scheme to detect and prevent of attack. The performance has been analysed based on remaining energy of the network, throughput and packet delivery ratio. This attack is new to the mobile and hoc network, so in future more energy efficient schemes can be designed.This attack is combination of flooding and clone attack. The attacker node clones the ID of some genuine node and floods the network with RREQ packets.

Opinder Singh et.al in [4] this paper, MANETS and a new approach is discussed which can detect flooding attack. In SAODV approach, concept of dispersion is used for detecting malicious nodes in the network.This technique, statistical threshold value is obtained from mean and mean deviation (Dispersion). This value is used to find out the Route Request (RREQ) flooding attacker nodes in the MANET. The proposed technique is efficient because threshold values are computed on the basis of RREQs made by each node in the network. The simulation result has significant performance in the terms of throughput, delay, packet delivery ratio. These approach has significant performance in the teams of throughput,delay,packet delivery ratio and efficient threshold values.

Malik N. Ahmed et.al in[5] this paper proposed The Key Assignment Algorithm is an Identification-based Digital signature, encouraged by the Head_CA to send ID-based Digital signature keys to many mobile nodes, in order to secure the nodes within the boundary level for awareness of malicious node attacks. The individual key has been randomly driven through from the neighbor node to the destination node, in the form of a packet. The key generation algorithm evolves an existing key management scheme to a new secure node Key management scheme.It provides security goals like authentication,integrity etc by using encryption Techniques & some secure protocol. It introduced heavy traffic load to exchange and verify keys.

Shishir K. Shandilya et.al in[6] the author proposed trust estimation technique which uses the routing protocol to detect & mitigate the effect of RREQ flooding attack in the networks with high node mobility. In this work, based on the trust value they categorized the nodes in three categories: Friends, acquaintance and stranger. Stranger are the non-trusted node, friends are the trusted node and acquaintance has the trust values more than stranger and less than friends. Based on relationship they define the threshold values. It efficiently reduces the flooded RREQ packets from the network. It does not work well with higher node mobility.

Neetu Singh Chouhan et.al in[7] the authors proposed the separate approach for RREQ flooding and data flooding. To resist the RREQ flooding, they defined the neighbor suppression method which prioritizes the node based on the number of RREQ received. A node gets higher priority if it sends less numbers of RREQ packets and defined the threshold value. To deal with data flooding they used path cutoff method. In this method when node identifies that sender is originating data flooding then it cut off the path and sends the route error message. It may cut off the path when many data packets are transmitted to the victim node.FAP in this method flooding packet still exists in the network.

NitinMohil et.al in[8] the author mainly focused on preventing denial-of-service (DoS) attacks & illustrates how intruders can exploit the route discovery procedure of reactive routing protocol to DoS attacks in MANET. to detect DoS and propose an anomaly-based intrusion detection system that uses a combination of chi-square test & control chart to first detect intrusion and then identify an intruder and show that it generate low detection & high false alarm rates.. Adaptive Intrusion Detection & Prevention (AIDP) finally isolates the nodes from the network to prevent intrusion. It reduces the control packet overhead & increases the network throughput with very high success rate and very low false alarm rate. Processing overhead on the network.

Jian-hua Song et.al in[9] the author proposed a new mechanism to prevent RREQ flooding attack. This technique can detect the malicious nodes and attacker nodes, which are disturbing the network communication. In this technique there are two thresholds RATE_LIMIT and BLACKLIST_LIMIT, which are used to limit the RREQ message. RATE_LIMIT parameter indicates no. of RREQ that can be known and managed. Here each node monitors the RREQ and maintain a count table for RREQ received. Whenever a RREQ request is received a condition check is performed, if the rate of received RREQ is less than the RATE_LIMIT then received RREQ processed normal otherwise a second condition check is performed, where received RREQ is compared with another threshold BLACKLIST_LIMIT, if the rate of RREQ is greater than the BLACKLIST_LIMIT then it is assume that particular node trying to flood the network with fake RREQ messages otherwise the received RREQ Messages. It switches the network with high mobility. This technique does not able to differentiate between genuine nodes and fake RREQs from the malicious node.

kashiflaeeq et.al in [10] In this paper proposed thatRFAP(RREQ Flooding Attack Prevention (RFAP)) technique is used to identify the malicious flooder node. In RFAP if the node breaks the predefine threshold value, it gets punishment. If anyone breaks the law first time the punishment may be less in particular place in this technique it followed by Custody list.This technique recover malicious node after reasonable punishment.It cannot stop the illegal data packets.

Methods	Advantages	Disadvantages
Effective Filtering Technique	It Switches the network with high mobility.	This technique does not able to differentiate Between genuine nodes and fake RREQs from the malicious node.
The flooding attacks prevention Scheme	It may cut off the path when many data packets are transmitted to the victim node.	FAP[flooding Attack Prevention] in this method flooding packet still exists in the network
A Trust Based Security scheme	It efficiently reduces the flooded RREQ packets from the network.	It does not work well with higher node mobility
Key management scheme	It provides security goals like authentication ,integrity etc by using encryption Techniques & some secure protocol	It introduced heavy traffic load to exchange and verify keys
Adaptive intrusion Detection & Prevention Scheme	It reduces the control packet overhead & increases the network throughput with very high success rate and very low false alarm rate	Processing overhead on the net

V. CONCLUSIONS

Flooding attack in MANET results in exhaustion of battery power, degradation of throughput and wastage of bandwidth. In this report we have analyzed different techniques to detect and prevent flooding attack on AODV routing protocol in MANET. In this work we only concentrated with RREQ flooding attack and used routing table of nodes to detect attack and prevent attack. There is also DATA flooding attack which degrades the performance of MANET by consuming bandwidth of the network and battery of the network.

REFERENCES

[1] Singh, Opinder, Jatinder Singh, and Ravinder Singh. "SAODV: Statistical Ad hoc On-Demand Distance Vector Routing Protocol for Preventing Mobile Adhoc Network against Flooding Attack." Advances in Computational Sciences and Technology 10.8 (2017): 2457-2470.

[2] Mahapatra, Bandana, and SrikantaPatnaik. "Security Measure to Detect and Avoid Flooding Attacks using Multi-Agent System in MANETS." International Journal of Electrical and Computer Engineering (IJECE) 7.2 (2017): 919-925.

[3] Verma, Karan. "IP-CHOCK Reference Detection and Prevention of Denial of Service (DoS) Attacks in Vehicular Ad-Hoc Network: Detection and Prevention of Denial of Service (DoS) Attacks in Vehicular Ad-Hoc Network." Handbook of Research on Advanced Trends in Microwave and Communication Engineering. IGI Global, 2017. 398-420.

[4] Shahabi, Sina, MahdiehGhazvini, and Mehdi Bakhtiarian. "A modified algorithm to improve security and performance of AODV protocol against black hole attack." Wireless Networks 22.5 (2016): 1505-1511.

[5] Manohari, Prasanta Kumar, and Niranjan Ray. "Multipath routing protocols in MANETs: A study." Innovation and Challenges in Cyber Security (ICICCS-INBUSH), 2016 International Conference on. IEEE, 2016.

[6] Ahmed, Malik N., et al. "F3TM: Flooding Factor based Trust Management Framework for secure data transmission in MANETs." Journal of King Saud University-Computer and Information Sciences 29.3 (2017): 269-280.

[7] Jiang, Fuu-Cheng, Chu-Hsing Lin, and Hsiang-Wei Wu. "Lifetime elongation of ad hoc networks under flooding attack using power-saving technique." Ad Hoc Networks 21 (2014): 84-96.

[8] Shandilya, Shishir K., and SunitaSahu. "A trust based security scheme for RREQ flooding attack in MANET." International journal of computer applications 5.12 (2010): 4-8

[9] Bhalodiya, Shruti, and KrunalVaghela. "Study of Detection and Prevention Techniques for Flooding attack on AODV in MANET." International Journal of Science and Research (IJSR) 4.1 (2015): 433-436.

[10] Sawant, Khushboo, and Dr MK Rawat. "Survey of DOS flooding attacks over MANET environment." International Journal of Engineering Research and Applications 4.5 (2014): 110-115.

[11] Jatthap, Sheetal, and PankajDashore. "Battery Capacity Based Detection and Prevention of Flooding Attack on MANET." International Journal 4.9 (2016).

[12] Kumar, SB Mohan, KM Anand Vijay, and N. S. Suhas. "A policy based preventive measure against flooding attack in MANETs." Recent Trends in Electronics, Information & Communication Technology (RTEICT), IEEE International Conference on. IEEE, 2016.

[13] Chouhan, Neetu Singh, and ShwetaYadav. "Flooding attacks prevention in MANET." International Journal of Computer Technology and Electronics Engineering 1.3 (2011): 68-72.

[14] Mahapatra, Bandana, and SrikantaPatnaik. "Security Measure to Detect and Avoid Flooding Attacks using Multi-Agent System in MANETS." International Journal of Electrical and Computer Engineering (IJECE) 7.2 (2017): 919-925.

[15] Nadeem, Adnan, and Michael P. Howarth. "A survey of MANET intrusion detection & prevention approaches for network layer attacks." IEEE communications surveys & tutorials 15.4 (2013): 2027-2045.

[16] Gurung, Shashi, and Siddhartha Chauhan. "A novel approach for mitigating route request flooding attack in MANET." Wireless Networks: 1-16.

[17] Patel, Meenakshi, Sanjay Sharma, and DivyaSharan. "Detection and prevention of flooding attack using svm." Communication Systems and Network Technologies (CSNT), 2013 International Conference on. IEEE, 2013.

[18] Pandikumar, T., and HabtewoldDesta. "RREQ Flooding Attack Mitigation in MANET Using Dynamic Profile Based Technique." International Journal of Engineering Science 12700 (2017).