TO ALLEVIATE THE ATTACK AND INTENSIFY EFFICIENCY IN MANET

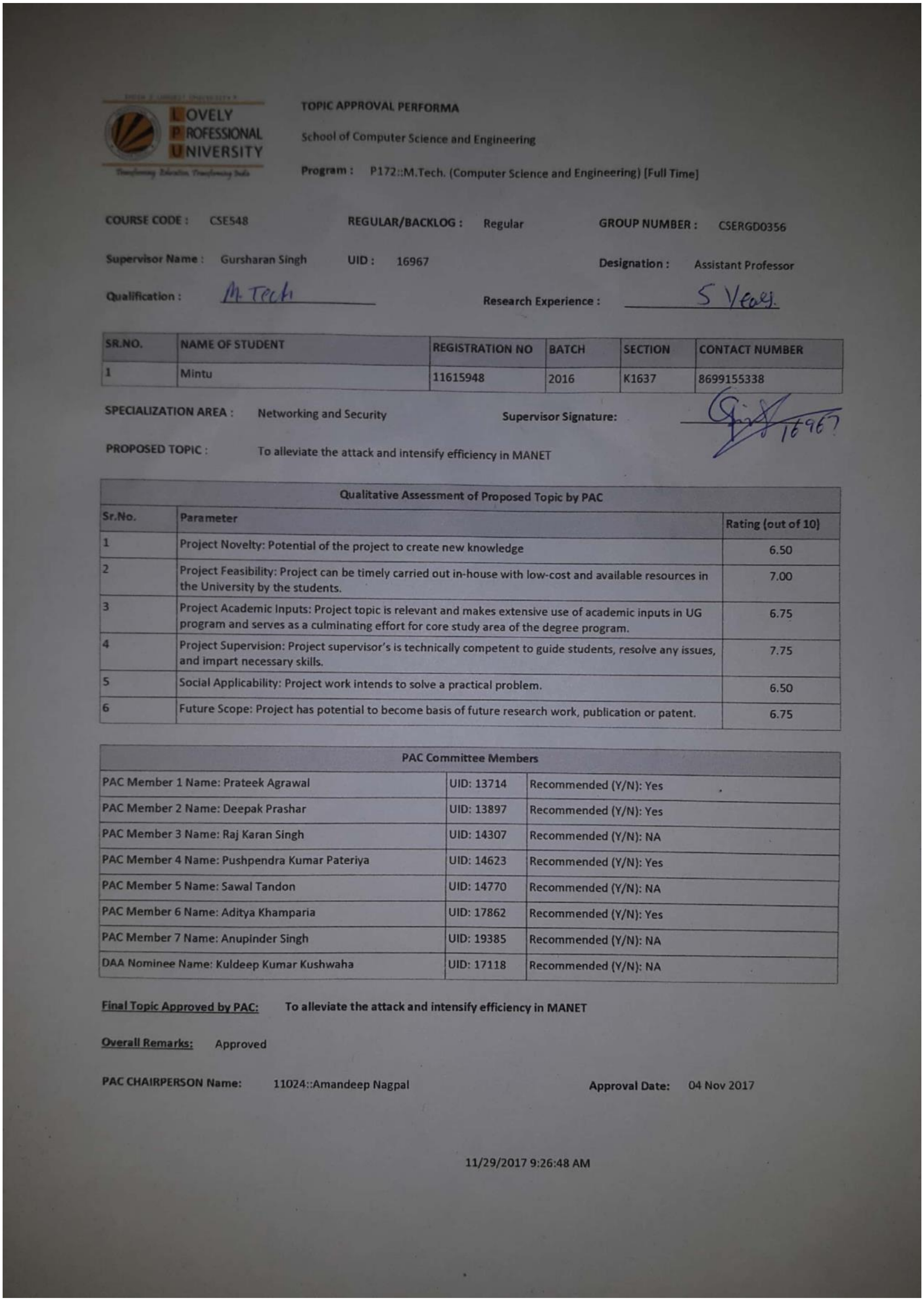
Dissertation submitted in fulfilment of the requirements for the Degree
Of

MASTER OF TECHNOLOGY
In
COMPUTER SCIENCE AND ENGINEERING

By
MINTU
11615948

Supervisor
GURSHARAN SINGH

School of Computer Science and Engineering
Lovely Professional University
Phagwara, Punjab (India)
December 2017



LOVELY PROFESSIONAL UNIVERSITY

Transforming Education, Transforming India

TOPIC APPROVAL PERFORMA

School of Computer Science and Engineering

Program : P172::M.Tech. (Computer Science and Engineering) [Full Time]

COURSE CODE : CSE548 **REGULAR/BACKLOG :** Regular **GROUP NUMBER :** CSERGD0356

Supervisor Name : Gursharan Singh **UID :** 16967 **Designation :** Assistant Professor

Qualification : M. Tech **Research Experience :** 5 Years.

SR.NO.	NAME OF STUDENT	REGISTRATION NO	BATCH	SECTION	CONTACT NUMBER
1	Mintu	11615948	2016	K1637	8699155338

SPECIALIZATION AREA : Networking and Security **Supervisor Signature:** 16967

PROPOSED TOPIC : To alleviate the attack and intensify efficiency in MANET

Qualitative Assessment of Proposed Topic by PAC		
Sr.No.	Parameter	Rating (out of 10)
1	Project Novelty: Potential of the project to create new knowledge	6.50
2	Project Feasibility: Project can be timely carried out in-house with low-cost and available resources in the University by the students.	7.00
3	Project Academic Inputs: Project topic is relevant and makes extensive use of academic inputs in UG program and serves as a culminating effort for core study area of the degree program.	6.75
4	Project Supervision: Project supervisor's is technically competent to guide students, resolve any issues, and impart necessary skills.	7.75
5	Social Applicability: Project work intends to solve a practical problem.	6.50
6	Future Scope: Project has potential to become basis of future research work, publication or patent.	6.75

PAC Committee Members		
PAC Member 1 Name: Prateek Agrawal	UID: 13714	Recommended (Y/N): Yes
PAC Member 2 Name: Deepak Prashar	UID: 13897	Recommended (Y/N): Yes
PAC Member 3 Name: Raj Karan Singh	UID: 14307	Recommended (Y/N): NA
PAC Member 4 Name: Pushpendra Kumar Pateriya	UID: 14623	Recommended (Y/N): Yes
PAC Member 5 Name: Sawal Tandon	UID: 14770	Recommended (Y/N): NA
PAC Member 6 Name: Aditya Khamparia	UID: 17862	Recommended (Y/N): Yes
PAC Member 7 Name: Anupinder Singh	UID: 19385	Recommended (Y/N): NA
DAA Nominee Name: Kuldeep Kumar Kushwaha	UID: 17118	Recommended (Y/N): NA

Final Topic Approved by PAC: **To alleviate the attack and intensify efficiency in MANET**

Overall Remarks: Approved

PAC CHAIRPERSON Name: 11024::Amandeep Nagpal **Approval Date:** 04 Nov 2017

11/29/2017 9:26:48 AM

DECLARATION STATEMENT

I hereby declare that the research work reported in the Dissertation -II entitled "**TO ALLEVIATE THE ATTACK AND INTENSIFY EFFICIENCY IN MANET**" in partial fulfillment of the requirement for the award of Degree for Master of Technology in Computer Science and Engineering at Lovely Professional University, Phagwara, Punjab is an authentic work carried out under supervision of my research supervisor Mr. Gursharan Singh. I have not submitted this work elsewhere for any degree or diploma.

I understand that the work presented herewith is in direct compliance with Lovely Professional University's Policy on plagiarism, intellectual property rights, and highest standards of moral and ethical conduct. Therefore, to the best of my knowledge, the content of this dissertation represents authentic and honest research effort conducted, in its entirety, by me. I am fully responsible for the contents of my dissertation work.

Signature of Candidate

MINTU

11615948

SUPERVISOR’S CERTIFICATE

This is to certify that the work reported in the M.Tech Dissertation/dissertation proposal entitled “**TO ALLEVIATE THE ATTACK AND INTENSIFY EFFICIENCY IN MANET”** submitted by **Mintu** at **Lovely Professional University, Phagwara, India** is a bonafide record of his original work carried out under my supervision. This work has not been submitted elsewhere for any other degree.

Signature of Supervisor

(Gursharan Singh)

Date: ____________

Counter Signed by:

1) **Concerned HOD:**
   HoD’s Signature: ________________

   HoD Name: ____________________

   Date: ___________________

2) **Neutral Examiners:**

External Examiner

Signature: _______________

Name: __________________

Affiliation: ______________

Date: ___________________

Internal Examiner

Signature: _______________

Name: __________________

Date: ___________________

ACKNOWLEDGEMENT

I take this opportunity to present my votes of thanks to all those guidepost who really acted as lightening pillars to enlighten our way throughout this project that has led to successful and satisfactory completion of this study.

I am grateful to our **Lovely Professional Universit**y for providing me with an opportunity to undertake this project in this university and providing us with all the facilities.

I am really thankful from my heart to **Mr. Gursharan Singh,** who allowed me to do this project under his guidance. I am highly thankful to my family and friends for their active support, valuable time and advice, whole hearted guidance, sincere cooperation and pains-taking involvement during the study.

Lastly, I thankful to all those, particularly the various friends, who have been instrumental in creating proper, healthy and conductive environment and including new and fresh innovative ideas during the project, without their help, it would have been extremely difficult for me to prepare the project in a time bound framework.

TABLE OF CONTENTS

CONTENTS **PAGE NO.**

TABLE OF CONTENTS

LIST OF FIGURES

ABSTRACT

The mobile Ad-hoc network is the decentralized and self-configuring type of network in which mobile nodes join or leave the network any time. Due to decentralized nature of the network security, routing and quality of service are the three major issues. To establish path from source to destination reactive routing protocol can be implemented. The AODV is the reactive routing protocol in which source node flood route request packets in the network. The nodes which are adjacent to destination will respond back with the route reply packets. The path which has minimum hop count and maximum sequence number will be selected as the best path from source to destination. The mobile nodes can join or leave the network and sometime malicious nodes enter the network, which are responsible to trigger various active and passive attacks. The flooding attack is the active type of attack in which malicious nodes send raw packets on the channel. Due to this, channel gets overload and packet loss may occur within the network. This leads to reduction in network throughput and increase network packet loss. In this research, the technique of mutual authentication will be proposed which detects and isolates malicious nodes from the network which are responsible to trigger flooding attack.

Keywords:-**MANETs, AODV, Mutual authentication technique, Flooding attack.**

CHAPTER 1

INTRODUCTION

1.1 MANET

MANET remains for mobile Ad-hoc network. They are self-designing and framework less in nature. With the help of wireless link, the various mobiles are connected with each other. As there is no central controller present within the network, the nodes are free to move within the network. These networks presented another specialty of network foundation and can be appropriate for a domain where either the framework is lost or where send a framework isn't extremely savvy. The mainstream IEEE 802.11 "WI-FI" convention is equipped for giving ad-hoc network provision at low level, when no entrance point is accessible. Versatile specially appointed networks can work in an independent mold or could be associated with a bigger network, for example, the Internet [1]. Portable specially appointed networks can turn the fantasy of getting associated "anyplace and whenever" into reality. Regular application cases incorporate debacle recuperation or a military operation.

There is limited bandwidth and node mobility of the mobile Ad-hoc networks. Thus, the various factors such as the energy efficiency of the nodes, topology changes and unreliable communication are to be considered and analyzed in proper manner within the network. There are numerous protocols present within the MANETs [2]. The amount of battery of the participating node consumed by the routing protocol determines its efficiency. Also the amount of traffic routed within the network is an important factor.

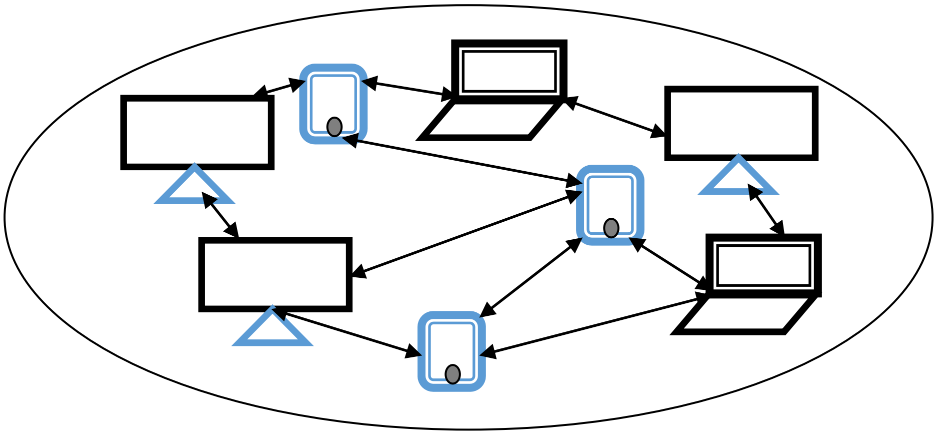


Fig. 1.1: MANET

With the non-attendance of centralized or settled framework within the Ad-hoc network it is also seen that there is a possible wireless scenario present within it. There are numerous challenges present within the infrastructure less networks due to its functionality. The traffic within the network is accepted and routed from the intermediate nodes to the destination within the mobile nodes of MANET. The network can thus act as both router and host as per the working of the nodes within it. Within the mobile nodes, the energy constraint is represented by the most recent link breakage and re-associations occurring within the network. A wireless distributed network that is self-organized in nature and is multi-hop is noted as a versatile Ad-hoc network. The discovery of a route within the network is the main objective here. The setup and maintaining of the routes present amongst the nodes is done with the help of the routing protocol [3]. There is link breakage and invalidation of end-to-end route occurring within the network due to the constant change in the topology of network is these types of networks.

1.2 CHALLENGES OF MANET

The network can be generated by the mobile nodes at various locations as per the requirement. There is no central controller present within the network as it decentralized type in nature. There are many challenges within these types of networks:

- A self-configuring type of network in which the nodes are permitted to move freely as per the requirement in known as MANET. When the position of the mobile node is changes, the topology of the network changes according to it. It is difficult to design such efficient routing protocol that can facilitate such network. The important challenge here is the multicast routing [3].
- The other major challenges within the mobile Ad-hoc networks are the security and reliability of the network. There are numerous internal and external types of attacks possible. At any duration within the network, the attacker node can enter the network and cause an attack. The key management and self-authentication method within the mobile Ad-hoc networks is very difficult to be designed.

- There is a need of fixed resource reservation within various real time applications for providing quality of service. The QoS is very difficult to be ensured and thus the designing of such mechanism is also very tough.
- When the nodes from various devices gather the mobile Ad-hoc network is generated. Another disadvantage of MANETs is the power consumption. For the purpose of sensing environment conditions and deploying the network at farther places, the wireless sensor networks are deployed. The recharging or replacing of battery within the sensor nodes present at such far places is not possible. For managing the power consumption there have been various requirements provided [4].
- Within the network the nodes can move as per the requirement. Thus, the designing of a protocol that provides Location-aided routing is a very tough task.
- A hidden terminal and exposed terminal issue is also present within the mobile networks. For solving such problems, there is a need to present reliable solutions.
- The position of mobile nodes can be changed at any duration. This causes link failure within the network and degrades the overall performance of the network.

1.3 SECURITY GOALS OF MANET:

- **Availability:** Within the Denial of Service attacks the jamming techniques are utilized by the attackers on the physical and media access control layer. This is done to provide interference in the communication occurring within the physical channel. The routing protocol can be disrupted by the attacker on the network layer. The high level services can be brought down by the higher layers [5].
- **Confidentiality**: It is to be taken care by this feature that the important information is never shared amongst the unauthorized users. The messages in this case cannot be seen by any other user.
- **Integrity:** The integrity ensures that the message that is being transmitted is not corrupted. It is possible that the attacker can change the message and to confirm that no alterations are made by any external user, the integrity is to be ensured [6].
- **Authentication:** The validity of the user is to be ensured within the authentication. For instance, the accessing of Gmail account through email ID can be done if one knows the

username and password of the ID. A valid user is considered to be the one that knows both the validating fields. If they are not known, the user is considered to be unauthorized [7].

- **Non-repudiation**: Through this property it is to be confirmed that the message sent from the user who generated cannot deny the fact that it has sent the message.

1.4 SECURITY ATTACKS IN MANET

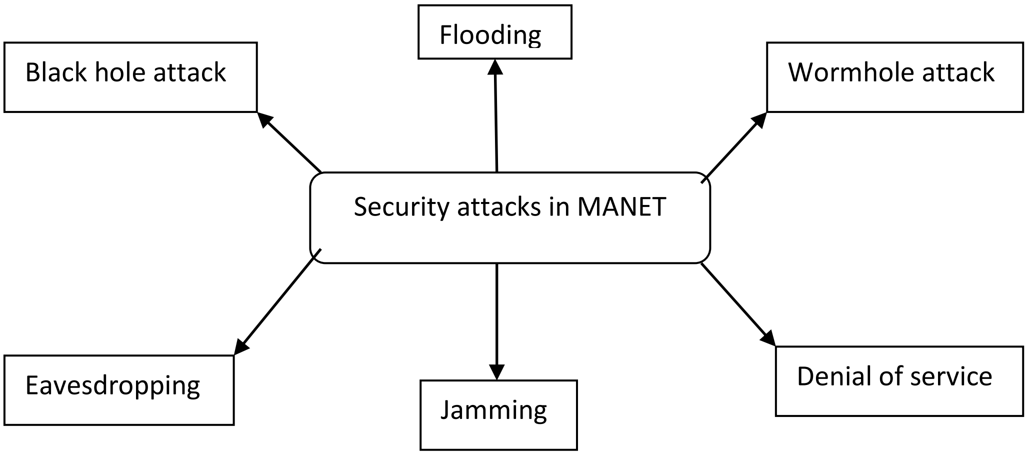


Fig. 1.2: Security attacks in MANET

- **Eavesdropping:** A passive type of attack in which the malicious nodes sniff within the traffic of network is known as eavesdropping. In this case messages are read out by using inadvertent receivers. This information will be the secret information of the network such as passwords, private keys etc. As in case of MANET, the shared medium for communication is wireless which use RF spectrum. The data transmitted through the above spectrum can be easily intercepted by the receivers which are tuned to proper frequency on which data is transmitted [8].

- **Black hole Attack:** The malicious nodes present within the network are responsible for triggering this type of active attack. The selection of path from source to destination is to be done by the reactive routing protocols. An essential on-demand routing protocol that creates courses according to the necessity of the source hub is known as the AODV protocol. A course disclosure process is started inside the network when there is a need to set up a course to the goal [9].

- **Wormhole attack:** An attack that can be caused within or outside the network by the malicious node is known as a wormhole attack. This attack is one of the most dangerous network layer attacks. The packets are received from one end of the network and the rest of the traffic is sent to another side. There is delay of other services within the network due to the occurrence of this type of attack. This attack can be detected by packet leases it will put a limit on highest amount of packet transmission distance by either using geographical or temporal type. The path which is used for information passing is usually not part of the actual network this make it difficult to detect the wormhole attack.

- **Jamming Attack:** It is an active type of attack. In jamming attack number of packets is sent to specific node by the malicious node. The node is not able to handle a large number of packets. Due to which there will be blocking in the network. This attack is also taken place in network by other way. In this the attacker will find out the frequency at which destination node is receiving the signal from sender. Then the attacker will send the signal at that particular frequency which will cause delay in reception of original message [10].

- **Denial-of-Service Attack:** The required services cannot be accessed by the legitimate nodes in the denial-of-service attack. Large numbers of burst packets are sent with respect to the legitimate nodes in this scenario by showing illegal sources as legal ones. The services are disrupted this due to the overcrowding within the network [9]. The network performance measurement parameters such as throughput and bandwidth get depleted which debase the general execution of the network.

- **Flooding attack:** It is a type of active attack. The bandwidth, consumption of node resources network resources are exhausted by attacker. The network performance is degraded by attackers as they disrupt the routing operation to cause severe degradation. The genuine requests are weighted by invalid requests that enable network to process it due to flood attack. The buffer of host memory gets filled by the above mentioned reason [11]. Once this buffer is full, connections can no longer be made and this results in DOS.

1.5 DIFFERENT TYPES OF FLOODING ATTACK:

A Flooding attack is broadly classified into the following types:

- **Hello flooding:** The attacker node broadcasts a hello packet with very high power (powerful transmitter). Therefore the other nodes in the network assume that this attacker node is the parent node and starts forwarding packets towards this node hoping it to be the best route to the destination. This will lead to increase in delay in the network and also convince the other nodes that this attacker node is their neighbor, so that all the other nodes will respond to the HELLO message and waste their energy. The attacker node performs a selective replay attack as its power overwhelms other transceivers

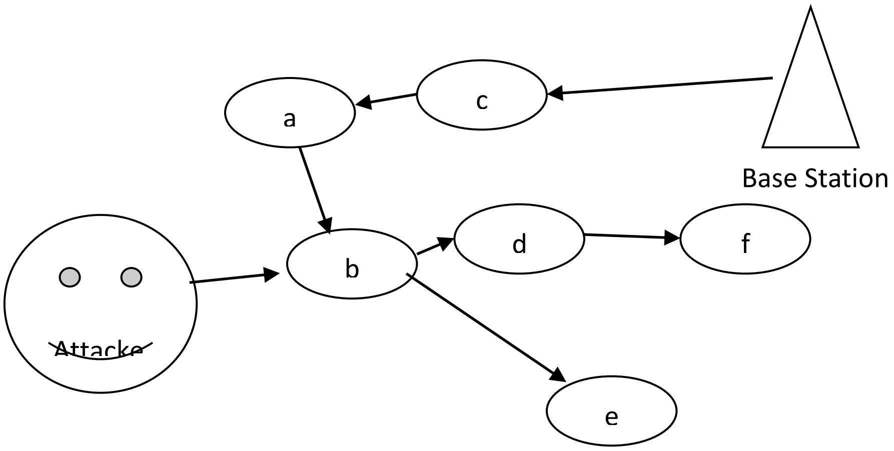


Fig. 1.3 (a): Hello Flooding broadcast mechanism

In above shown Fig. 3 (b), the attacker broadcast hello packet with very high power transmission then the base station.

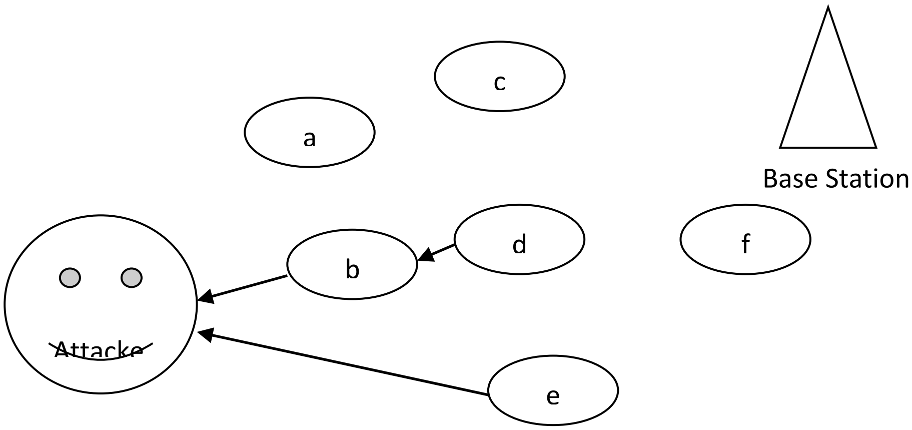


Fig. 1.3 (b): Hello flooding packet transmission

In the above shown Fig. 3 (b), the legitimate nodes consider attacker as the parent as well as neighbor node and start forwarding the packets.

- **RREQ flooding:** The attacker selects IP addresses that are not a part of the network and broadcasts several RREQ packets as shown in Fig 4. The attacker deactivates the RREQ rate so this consumes more bandwidth.

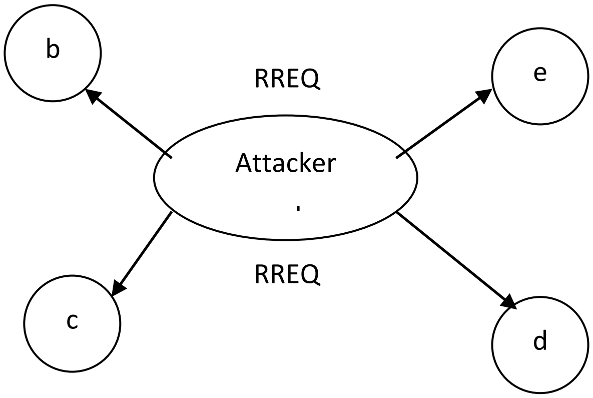


Fig. 1 4: RREQ mechanism

- **Data flooding** In this attack, malicious node first construct path to all the nodes and then starts sending useless data packets to exhaust the network bandwidth as shown in Fig 4. It is hard to detect the data packet [12].
- **ICMP (Internet Control Message Protocol) flooding:** An attacker generates a stream of ICMP ECHO packet [13] to target the victim node. Thereby the victim wastes its power and network resources by sending replies to all the ICMP requests.

- **UDP flooding:** In this attack, the attacker sends n number of UDP packets to the victim in order to overwhelm the victim’s network bandwidth [14]

CHAPTER 2

LITERATURE SERVEY

Sukiswo, et.al, (2015), have recommended the use of MANET technology to get rid of situations faced by mobile users without help of settled system framework. This helps in interface with no settled framework. The MANET network has high versatility that makes it more defenseless against assault. The routing scheme made by routing protocols gets affected by attacks in MANET. In this paper [15], authors have designed an Ad-hoc on-demand Multi-path Distance Vector (AOMDV) routing protocol based MANET network. The network is considered with flooding and rushing assault. The system conditions uncovered rushing assault, flooding assaults, and the rushing and flooding assault all the while are the three situations utilized as a part of this examination. The Packet Delivery Ratio (PDR), Throughput, and Delay are the three parameters that are utilized for AOMDV protocol investigation. If there should arise an occurrence of rushing assault the estimation of gathering bundles are 2950 packets, while flooding assault diminish gathering bundles until 769 packets.The simulation results show that Packet Delivery Ratio esteems diminished by 17.596% and throughput esteems diminished by 84.23%. The estimation of deferral is increments from typical state of 59.15 ms to 269.734 ms at flooder hubs assaults.

M. Rmayti, et.al, (2015), have analyzed that flooding attacks are one of the security dangers that prompt denial of service (DoS) in PC networks. The assailant mean to intrude on a portion of the network benefits as these assaults comprises of an over the traffic generation. The flooding assault not just effect to a few nods, it can likewise harm entire system. Many routing protocols are helpless against these assaults, particularly those utilizing receptive component of course revelation, as AODV. In this paper [16], creators have proposed a measurable way to deal with resistance against RREQ flooding assaults in MANETs. This discovery system can be connected on AODV-based Ad-hoc organizes. They have utilized the Hello message to give an occasional check of neighbor nods. To confirm the current of a flooding assault in the network a weighted moving normal of got course ask for sum has been utilized. To find the wellspring of flooding, the weighted moving normal of produced course asks for sum is figured. The recreation consequences of proposed plot demonstrate that these assaults can be recognized with a low rate of false cautions.

Khushboo Sawant, et.al, (2015), have recommended MANET as the most up- coming fields for researchers. The independent nodes mobility is considered as an essential network property. An important role is played by routing protocol in route delivery between communicating nodes. The network have to suffers from performance issues among all of them security is consider as a main concern in this work. In this paper [17], authors have clarified the incident of flooding attack and exposed the area being affected by this attack the aim of authors is to recognize the presence of DoS flooding attack using secure routing protocols. In networking research NS is considered as a discrete event simulator. To verify the proposed scheme analysis has been performed on NS2 simulator. They have also described the restrictions of the simulator model. Ns-2 is written in C++ and OTcl object oriented simulator. There is class chain of command in C++ and comparable in OTcl mediator that has been supported by test system. There is a balanced correspondence between a class in the translated chain of command and one in the gather progressive system.

Sourabh Singh Verma, et.al, (2015), have analyzed that MANET can be influenced by different sorts of assaults. In this number of mobile nodes is present that are decentralized and needs collaboration to exchange movement. In this network number of nodes can be malevolent that can take an interest or lead to denial of service (DOS) assaults. The network QOS parameters get affected by these attacks one of them is flooding attack. In this paper [18], authors have given flooding nodes that are flooding in network for various time interims. Flooding can be delegated takes after: Request flooding that includes data flood attacks and Hello attack. The authors have considered request flooding under multi features conditions and parameters. In order to evaluate those malicious nodes NS2 simulator has been used and six different results has been taken and analyzed. The results show that this attacks drastically affects the QOS and throughput, it likewise demonstrates the packet delivery portion is conversely relative to transfer speed involved by surge demands.

Kuldeep Singh, et.al, (2015), have analyzed that in order to complete a particular task there is need of access point on temporary or urgent basis by Mobile Ad-hoc networks that is not required by wired network. They are susceptible to different attacks due to its insecure environment setup and common target of malicious nodes is to affect the backbone routing protocol. In this paper [19], authors have analyzed Ad-hoc On-Demand Multipath Distance Vector Protocol (AOMDV) and Ad-hoc On Demand Distance Vector Routing Protocol (AODV) is two protocols. The Black-hole, Gray-hole, Flooding and Rushing attack are considered by authors and studied their impact on above mentioned two protocols. They have analyzed the results as far as Throughput, Packet Delivery Ratio, Normalized Routing Overhead, and End to end latency, Packet-loss and Mean Hop Count parameters. It has been seen that flooding attack can lead to exponentially increases in routing overhead that can affect the network in drastic way.

Sourabh Singh Verma, et.al, (2015), have analyzed that different attacks can affect the decentralized MANET in drastic way so there is need of cooperation to transfer such traffic. There are large number of nodes are present in the network and any node can be a malevolent node that can take an interest in communication that results into denial of Service (DOS) attacks. There is one assaults name as flooding assault that comes under DoS attack that impact the QoS of the network. In this paper [20], authors have given review on different flooding nodes that are flooding in network for various time interims. The simulation has been performed to test it and they have used NS-2 simulator to assess malevolent nodes and six distinctive outcome is broke down which demonstrates intense impact of such assault on QOS and throughput. The outcome additionally demonstrates how packet delivery portion is contrarily extent with transfer speed involved by flood request.

Taranpreet Kaur, et.al, (2014), have concluded that MANET is a get together of mobile nodes that have ability of design any immediately network without the help of any settled foundation or brought together supervision. The MANETs turn out to be exceedingly powerless against various assaults because of self-course of action and self-upkeep capacities. In this way, to give a safe correspondence between mobile nodes security has become a big challenge. The flooding assault is considered as a security risk in whom the intruder will over-burden the system with extra useless packets to abuse the network transmission capacity and assets. In this paper [21], authors have proposed a reputation mechanism based on clustering behavior that helps in identifying the flooding malevolent nodes in military war zone network. This scheme has two-fold nature, subsequently it proficiently settle the bogus location of authentic nodes as vindictive ones.

Scheme is implemented in NS2. Execution of new plan is contrasted and AODV protocol in light of different execution measurements it is seen that proposed procedure has better execution regarding different measurements.

Elakkiya.M, et.al, (2014), have considered AD-hoc (MANET) networks are a developing zone of mobile computing. In ad-hoc environment number of challenges has to face by users because of asset need of these networks. This has been used mostly in those situations where are no resources to set up network or in case of emergency or temporary operations. This results in arise of new requirements and problems in MANET. The efficient MANET operations cannot be achieved using conventional networks. Different security problems have been arises due to wireless nature of correspondence and absence of security framework. There are different attacks to which this network is vulnerable out of all DOS attacks is considered to be most affected. There are different types of Denial of service attack by which network is get affected and one of these types is flooding attack in which useless packets are send by malicious nodes to consume the valuable network resources. All on demand routing protocols are affected by flooding attack. In this paper [22], authors have introduced an opportunistic routing technique to remove this attack. This routing scheme will consider relative velocity rather than distance between nodes. The simulation results have been brought for a system with malevolent nodes and after that with proposed plan. For the performance analysis, the plots between the offered load(kbps) and different parameters, for example, PDR (Packet Delivery Ratio), Delay (m/s), Overhead (packets) are considered. The outcomes demonstrate that the proposed trust show consolidated in customary AODV joined with a key administration and bio-metric identity plan could proficiently moderate various assaults in MANET. As on now the proficiency can be demonstrated with the simulation results.

Alka Chaudhary, et.al, (2014), have seen that internal and external attacks affects the Mobile Ad-hoc networks because of its dynamic typologies, no reasonable line of insurance and asset limitations like complex properties. The MANET has been saved to much extent using intrusion detection networks. In this paper [23], authors have proposed a new novel sugeno-type fuzzy derivation network for Ad-hoc flooding assault based intrusion detection network. The performance of attack present in MANETs has been detected to much extent using present intrusion detection network. In MANET the flooding attack can also be detected with high obvious positive rate and low false positive rate. In future they have seen that there is need to develop and intrusion detection network that will have the capacity to network a wide range of MANET's unusual exercises.

Meenakshi Patel, et.al, (2013), has recommended the use of of intruder to dispatch assault; one of them is flooding due to inadequacy of foundation and dynamic nature of MANET. Two sorts of routing name as proactive and reactive and out of both AODV reactive routing as it utilize flooding to support out route. The flooding, black hole and gray hole like DoS attack has been launched by attacker that comes under mostly occurred attacks in MANET. In this paper [24], authors have proposed a AODV behavioral based new technique that recognize and counteract flooding assaults in MANET. They have utilized PDER, CO and PMIR as measurements in their method that helps to predict flooding attacks. In order to test the proposed method they have used NS-3 as simulator and have concluded that the proposed method is prove to be better than existing techniques. They have divided that whole paper into two sections name as behavioral and classification stage and behavior of every node has been detected in behavioral stage through simulator.

Karan Verma, et.al, (2013), have presented Vehicular Ad-hoc Networks (VANET) as a application subset of Mobile Ad-hoc Network (MANET) and considered as substantial approach to the Intelligent Transportation Network (ITS). The drivers get support through VANET and safety has been achieved along with driving comfort that results in safe, cleaner and more intelligent environment. There are number of security threats like User Datagram Protocol (UDP)- based flooding which is a typical type of Denial of Service (DoS) assaults like security threats. In the above mentioned attack a large number of identities are forge by malicious node like Internet Protocol (IP) spoofing addresses keeping in mind the end goal to upset the correct elements of the reasonable information exchange between two quick moving vehicles**.** In this paper [25], authors have proposed a new method that helps in detecting and defending network through UDP flooding assaults under various sorts of IP spoofing. A capacity effective information structure and Bloom channel has been used to detect attacker. This approach is light in weight that is easy to be deploying in required resources with low cost. The simulation results of proposed scheme shows that this method is efficient as well as effective in terms of defending UDP flooding assaults under various sort of IP spoofing types.

Kashif Laeeq, (2013), have presented that it is insecure to perform the MNAET operation whose one of the principle reasons utilization of insecure routing protocol. The AODV like reactive routing protocol has been utilized in operation of ad-hoc networks that fulfill the needs of routing. It is vulnerable to use a course development period of protocol in which the communication can be easily disrupted by malicious node. In this malevolent node sends mass RREQ course ask for packets to void tends to that possess the system assets and it is known as RREQ Flooding Attack (RFA). There are different plans to relieve the RFA however they are deficient towards alleviating the assault. One of the fundamental issues introduce in greater part of proposed arrangements isn't to retake malevolent node after discipline. In this paper [26], authors have introduced a RFAP scheme that mitigates the RREQ flooding attack in MANET which is an recapture shape of AODV. The simulation results have been performed on NS-2 simulator and results show that it is more reliable as compared to existing AODV.

CHAPTER 3

PROPOSED WORK

3.1 SCOPE OF STUDY

The mobile Ad-hoc network is the decentralized kind of network in which portable nodes can join or leave the network whenever. Because of its decentralized nature, many malevolent nodes enter the network, which are capable to trigger different sorts of dynamic and detached assaults. The flooding assault is the dynamic sort of assault which is activated by the malevolent nodes. In the flooding assault the malevolent nodes flood the network with unlimited number of raw packets due to which the channel gets heavily loaded and packet-loss may happen in the network. In this research work, method will be proposed which detects and isolates malevolent nodes from the network which are capable to trigger flooding assault in the network.

3.2 OBJECTIVES

1. To analyze various intrusion detection networks for mobile Ad-hoc network.

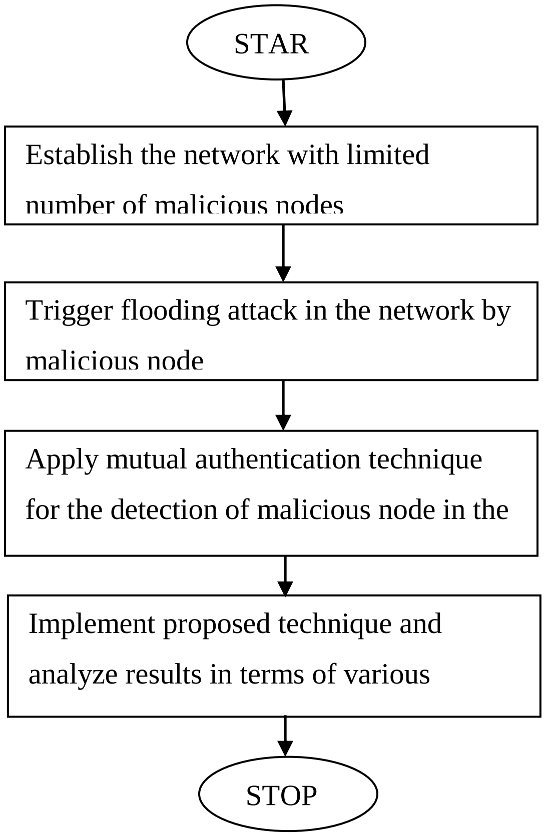
2. To propose technique for isolation of flooding attack based on advanced mutual authentication technique.

3. Implement proposed technique and compare with existing in terms of various parameters.

CHAPTER 4

RESEARCH METHODOLOGY

This research is based on detection of malevolent nodes from the network which are capable to trigger flooding assault. The flooding assault is the dynamic kind of assault in which malevolent nodes flood the network with vast number raw packets. Due to this, the channel gets overloaded and packet-loss may occur in the network. In this research work, the mutual authentication method will be proposed for detection and isolation of malevolent nodes. In the proposed technique the key server will be created in the network. Each node needs to get registered with the key server. In the registration process the nodes will also define their data transmission rate. When any node needs to interface with some other node, then it needs to prove its identity to the key server. The node which violates the rule of assigned data rate that is, the node which sends the data above the assigned data rate will be detected as malicious node. The proposed improvement leads to detection of malicious nodes from the network.



STAR

Establish the network with limited number of malicious nodes

Trigger flooding attack in the network by malicious node

Apply mutual authentication technique for the detection of malicious node in the

Implement proposed technique and analyze results in terms of various

STOP

Fig. 4: Flow Chart of Purposed Methodology

CHAPTER 5

EXPECTED OUTCOMES

Following are the various expected outcomes of this research:

1. The proposed algorithm will be based on detecting the malevolent nodes from the network. When the malevolent nodes are detected from the network, the network throughput will increased at steady rate.

2. The malicious nodes will be detected from the networks which are responsible for triggering flooding attack and this leads to reducing the delay and packet-loss.

3. The secure and efficient path will be established from source to destination which is maximum reliable.

4. The propose technique can also increase security of the network which can also ensure data integrity

CHAPTER 6
CONCLUSION

In this work, it has been concluded that mobile Ad-hoc network is decentralized kind of system because of which malevolent nodes enter the network and leave whenever they want. To establish path from source to destination routing protocols are required which is classified into reactive, proactive and hybrid. The reactive routing protocol has maximum efficiency in which source node flood route request packet and nodes which are adjacent of destination respond back with route reply packets. Due to decentralized nature of the network, many malicious nodes enter which are dependable to trigger different dynamic and detached assaults. This research is based on detecting malicious nodes from the network which are mindful to trigger flooding assaults. The proposed method will be based on authentication technique in the network.

REFERENCES

[1] Gang Ding and Bharat Bhargava, “Peer-to-peer File-sharing over Mobile Ad-hoc Networks”, Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops (PERCOMW’04), vol.6, pp.1-5, 2005.

[2] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester, “An Overview of Mobile Ad-hoc Networks: Applications and Challenges”, IJSER, vol. 3, pp. 132-138, 2005.

[3] C. Siva Ram Murthy, B.S. Manoj, "Ad-hoc Wireless Networks: Architectures and Protocols", Prentice Hall PTR, vol. 2, pp. 45-48, 2004.

[4] Naeem Raza, Muhammad Umar Aftab, Muhammad Qasim Akbar, Omair Ashraf, Muhammad Irfan, “Mobile Ad-Hoc Networks Applications and Its Challenges”, Communications and Network, vol. 8, pp. 131-136, 2016.

[5] Asad Amir Pirzada, Marius Portmann, "Wireless Mesh Networks for Public Safety and Crisis Management Applications", IEEE Internet Computing, vol. 12, pp. 18-25, 2008.

[6] Aarti, IJARCSSE, “Study of MANET: Characteristic, Challenges, Applications and Security Attacks”, vol.3, pp. 252-257, 2013.

[7] Deepak Chayal, Dr. Vijay Singh Rathore, “Assessment of security in mobile ad-hoc networks (MANET), vol.2, pp.137-139, 2010.

[8] Meenakshi Yadav, Nisha Uparosiya, “Survey on MANET: Routing Protocols, Advantages, Problems and Security”, International Journal of Innovative Computer Science & Engineering, vol.1, pp.12-17, 2014.

[9] Mahsa Seyyedtaj, Mohammad Ali Jabraeil Jamali, “Different Types of Attacks and Detection

Techniques in Mobile Ad-hoc Network", International Journal of Computer Applications Technology and Research vol.3, pp. 541 – 546, 2014.

[10] Pooja Chahal, Gaurav Kumar Tak, Anurag Singh Tomar, "Comparative Analysis of Various Attacks on MANET", International Journal of Computer Applications, vol.111, pp.42-45, 2014.

[11] Priyanka Goyal, Sahil Batra, Ajit Singh, "A Literature Review of Security Attack in Mobile Ad-hoc Networks", International Journal of Computer Applications, vol.9, pp.11-15, 2010.

[12] C.M. Nalayini, Dr. Jeevaa Katiravan, Arvind Prasad. V, "Flooding Attack on MANET – A Survey", Special Issue Published in International Journal of Trend in Research and Development (IJTRD), vol. 5, pp. 20-28, 2017

[13]Hyojin Kim, Ramachandra Bhargav Chitti, and JooSeok Song, Member,2010 IEEE "Novel Defense Mechanism against Data Flooding Attacks in Wireless Ad-hoc Networks".

[14] Schuba, C.L., I. V.,Kuhn, M.G., Spafford, E.H., Sundaram, A., and Zamboni, D.(1997). Analysis of a denial of service attack on TCP. In Proceeding of 1997 IEEE Symposium on Security and Privacy, pages 208-223, Oakland, CA.

[15] Sukiswo, Muhamad Rifqi Rifquddin, "Performance of AOMDV Routing Protocol Under Rushing and Flooding Attacks in MANET", Proc. of20l5 2nd Int. Conference on Information Technology, Computer and Electrical Engineering (ICITACEE), vol. 4, pp. 386-390, 2015.

[16] M. Rmayti, Y. Begriche, R. Khatoun, L. Khoukhi, D. Gaiti, "Flooding Attacks Detection in MANETs", 2015 International Conference on Cyber Security of Smart cities, Industrial Control System and Communications (SSIC), vol. 5, pp. 181-186, 2015.

[17] Khushboo Sawant, Manoj Kumar Rawat, Aakansha Jain, "Implementation of Energy Aware

Secure Routing Protocol over Flooding Environment in MANET", IEEE International Conference on Computer, Communication and Control (IC4-2015), vol. 4, pp. 809-814, 2015.

[18] Sourabh Singh Vermaa, Dr. R. B. Patelb, Dr. S. K. Lenka, "Investigating Variable Time Flood Request Impact Over QOS", 3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015), vol. 57, pp. 1036- 1041, 2015.

[19] Kuldeep Singh, Amanat Boparai, Vrinda Handa, Prof. Sudesh Rani, "Performance Analysis of Security Attacks and Improvements of Routing Protocols in MANET", Computer Science, Computer Engineering, and Social Media (CSCESM), 2015 Second International Conference, vol. 21, pp. 163-169, 2015.

[20] Sourabh Singh Vermaa, Dr. R. B. Patelb, Dr. S. K. Lenkac, "Investigating Variable Time Flood Request Impact Over QOS In MANET", 3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015), vol. 57, pp. 1036 – 1041, 2015.

[21] Taranpreet Kaur, Amanjot Singh Toor, Krishan Kumar Saluja, "Defending MANETs against Flooding Attacks for Military Applications under Group Mobility", IEEE Proceedings of 2014 RAECS VIET Panjab University Chandigarh, vol. 5, pp. 201-207, 2014.

[22] Elakkiya.M, Dr.Edna Elizabeth.N, "Opportunistic routing to forgo flooding attacks in MANET", Elsevier 2014 International Journal of Engineering Development and Research (IJEDR), Conference Proceeding (NCETSE-2014), vol. 8, pp. 34-40, 2014.

[23] Alka Chaudhary, Vivekananda Tiwari, Ani! Kumar, "A Novel Intrusion Detection System for Ad-hoc Flooding Attacl(Using Fuzzy Logic in Mobile Ad-hoc Networks", IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), vol. 16, pp. 172-176, 2014.

[24] Meenakshi Patel, Sanjay Sharma, Divya Sharan, "Detection and Prevention of Flooding

Attack Using SVM", 2013 International Conference on Communication Systems and Network Technologies, vol. 12, pp. 533-537, 2013.

[25] Karan Verma, Halabi Hasbullah, Ashok Kumar, "An Efficient Defense Method against UDP Spoofed Flooding Traffic of Denial of Service (DoS) Attacks in VANET", Advance Computing Conference (IACC), 2013 IEEE 3rd International, vol. 8, pp. 821-827, 2013.

[26] Kashif Laeeq, "RFAP, A Preventive Measure against Route Request Flooding Attack in MANETS", Multitopic Conference (INMIC), 2013 15th International, vol. 9, pp. 142-148, 2013.