International Journal of Future Generation Communication and Networking
Vol.10, No.3 (2017), pp.11-20
http://dx.doi.org/10.14257/ijfgcn.2017.10.3.02

Detection of Jamming Attack in MANET Using Watchdog Technique

Aditi Sharma[1] and Joy Karan Singh[2]

[1]*M. tech student, Department of CSE CT Institute of Technology and Research Maqsudan, Jalandhar*
[2]*Assistant Professor, Department of ECE CT Institute of Technology and Research Maqsudan, Jalandhar*
[1]*sweetgagan608@gmail.com*, [2]*joysachar@gmail.com*

Abstract

Mobile ad-hoc networks (MANET) are more receptive to security attacks because of their distinctive features i.e. dynamic configuration and no static infrastructure etc. The necessity for a protected MANET networks is powerfully attached to the privacy and security attributes. Jamming attack is one of them. This attack influenced the network by decreasing the network performance. In this paper, a comparative analysis is performed for AODV routing protocol on the basis of jammer attack and Watchdog Technique over MANET. In this paper work we are evaluate the performance of mobile ad hoc networks with jamming attack and with a novel mechanism (Watchdog Technique). The network performance is evaluated in terms of the QoS parameters i.e. packet loss, energy, PDR, retransmission attempts and throughput using NS-2 simulator.

Keywords*: MANETs, Jamming Attack, Throughput, PDR, Energy, Retransmission attempts, Packet loss*

1. Introduction

Wireless network has become very popular in the computing and mobile network world. There are basically two types of wireless network, infrastructure network (wired network) and infrastructure less network which is known as ad hoc network. The infrastructure network consists of fixed and wired gateways. While the infrastructure less network is a multi-hop wireless network and have no pre-defined infrastructure. The nodes or terminals in ad hoc networks are dynamic in nature i. e they have the capacity of moving and are connected in an arbitrary fashion with another different nodes. Routing is to find and maintain routes between nodes in a dynamic topology with possibly uni-directional links, using minimum resources. Therefore, routing is the core part of ad hoc communications. The ad hoc networks are mostly used in many civilian forums, military, business and emergency *etc.* Desirable properties of ad-hoc routing protocols are as follows:

- *Distributed operation*: This signifies that there is no central node in the network should be centralized it should free to establish a connection with any node of any network.
- *Loop free*: To improve the working, the routing protocol should guarantee that the path is followed in network should be loop free. This will prevent any type of wastage of bandwidth or CPU consumption.
- *Demand based operation*: To reduce the control overhead in the network and thus not waste the network resources the protocol should be reactive. This means that the protocol should react only when needed.

ISSN: 2233-7857 IJFGCN

- *Unidirectional link support*: The radio environment can cause the formation of unidirectional links and with the help of this we can improve the routing protocol performance.

1.1. MANET

Mobile Ad-hoc Network (MANET) attached in a dynamic manner and it is an assembly of wireless mobile nodes. Without any fixed infrastructure nodes making a temporary network where all nodes are arbitrarily free to move. In the network nodes are act as routers, which take part in finding and maintenance of routes to other nodes [1]. Wireless connection in MANET is highly misplay and due to mobility of nodes it goes down usually. Due to highly dynamic environment coherent routing is a very difficult task in Mobile Ad-hoc Network [2].

1.2. MANET Routing Protocols

The primary objective of routing protocol is to discover the route. In the routing protocol for MANET undertakes to setup and maintain routes between nodes. In MANET, continuously changing network topology is main reason behind link breakage and invalidation of end-to-end route in network. There is highly dynamic nature of wireless network imposes severe restrictions on routing protocols [13].

Routing protocols in MANETs are classified into three different categories according to their functionality:

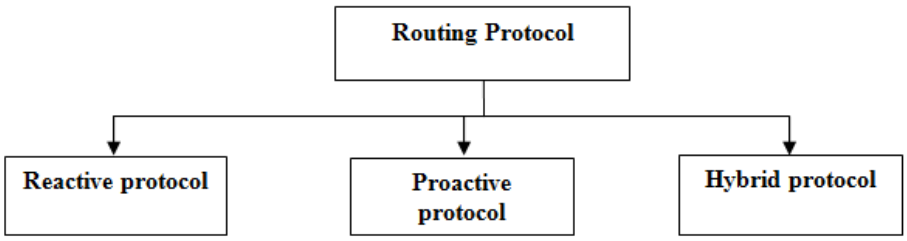

Figure 1. MANET Routing Protocol

1) Reactive Protocols:

Reactive protocols are also familiar as on demand driven reactive protocols. The reason behind they are known as reactive protocols is, they do not start route discovery by themselves, until they are requested, when a source node request to find a route the protocol starts finding suitable route for communication . These protocols setup routes when demanded. When a node need to communicate with another node in the network, and the source node does not have a route to that node which it wants to communicate, at that time reactive routing protocols will establish a route for the source to destination node. Normally reactive protocols have the following features

- Do not find route until demanded.
- When tries to find the destination “on demand”, it uses flooding technique to propagate the queue.
- Do not consume bandwidth for sending information.
- They consume bandwidth only, when the node start transmitting the data to the destination node.

2) Proactive Protocols

Proactive protocols are also known as on table driven protocols. These protocols constantly maintain the updated topology of the network. Every node in the network knows about the behavior of other node in advance. All the routing information is normally kept in tables. Whenever there is a change in the network topology, these tables are updated according to the change. The nodes interchange the topology information with each other; they can have route information any time when they required it.

3) Hybrid Protocols

Hybrid protocols make use the strengths of both reactive and proactive protocols, and merge them together to get better results. The network is split into sectors, and use different protocols in different sectors *i.e*. one protocol is used within a sector, and the other protocol is used between them. Zone Routing Protocol (ZRP) is an example of Hybrid Routing Protocol. ZRP uses proactive procedure for route establishment within the nodes neighborhood, and for the communication within neighborhood it takes the advantage of reactive protocols. These local neighborhoods are known as zones, and the protocol is named for the same reason as zone routing protocol.

AODV Routing protocol

AODV stands for Adhoc on-demand distance vector routing protocol. AODV is a very popular routing protocol for Mobile Ad-hoc Networks which do not have static topology. The algorithm of AODV is appreciative due to limited bandwidth that is available in the media that are used for wireless communications. It is the combination of the concepts from DSR and DSDV algorithms. It is on demand based protocol and hop-by-hop routing is done. Node sequence number feature is taken from DSDV thus makes the algorithm, topology and routing information dependent. AODV a very useful and required algorithm for MANETs because it is purely on-demand. Each mobile host in the network acts as an important router and routes are obtained as needed, thus making the network self-starting. Each node in the network possesses and updates a routing table with the routing information entries of its neighboring nodes. Two separate counters are maintained to store a node sequence number and a broadcast-id. When a node wants to communicate with another it increments its broadcast-id and starts its path discovery by broadcasting a route request packet RREQ to its neighbors node.

In this paper, we esteem a particular category of DoS attacks called Jamming. In actual fact, the mobile host in mobile ad hoc networks is a part of wireless medium. Thus, the radio signals can be jammed or interfered, which make the message to be amoral or missed. If the attacker has a strong transmitter, a signal can be launched that will be strong enough to conquer the directed signals and distort communications. There are several attack schemes that a jammer can do in order to interfere with other wireless communications.

2. Jamming Attack

The jammer is an entity with the aim of attempting to involve in the sending and receiving of data within the wireless communications of network. For blocking the legal traffic of the wireless channel, the jammer continuously emits RF signals. The jamming attacks have common properties which involve the usage of MAC protocols for their interactions [2]. A ratio of the number of packets sent out by any justifiable traffic source to the number of packets to be sent by the MAC layer is taken. This attack has a number of sources instead of just one source. These sources send the rough packets to the transmission channels and to the jammed channels as well. This results in packet loss which further decreases the efficiency and reliability of the system. The problems such as the unavailability of free channel, delay in transmission and new packet drops due to the absence of buffer space are seen.

Physical Jamming (Physical Layer): Another simple however, disruptive form of DoS attack is the Physical or Radio jamming found in the wireless networks. The reasons behind such attacks are the continuous emission of radio signals or the sending of random bits to other channels. The monopolizing of the wireless medium can be done for causing such attacks by the jammers which can result in denying a complete access to the channel. The channel is to be made idle and the carrier sensing time required is usually large. The nodes enter into a large exponential back-off period, so these results in affecting the adverse propagating affect.

Virtual Jamming (MAC Layer): The virtual carrier sensing is utilized in IEEE 802.11 for checking the availability of the wireless medium. The attacks on RTS/CTS frames or the DATA frames can be used for introducing jamming at the MAC layer. The MAC layer provides a benefit of providing the adversary node to consume less power while it targets these attacks. The consumed power is less as compared to the physical radio jamming. In this paper, the DoS attacks made at the MAC layer are discussed. These attacks result in collision of RTS/CTS control frames or DATA frames.

- *Constant Jammer:* A constant jammer is the signal alternator that does not obey any MAC protocol and it continuously released radio signal that represents random bits.
- *Deceptive Jammer:* They dispatch semi-valid packets. This means that the payload is bootless but the packet header is sustainable.
- *Random Jammer:* Substitutes between sleeping and jamming the channel. In the first modus the jammer jams for a casual period of time (it can behaves like a constant jammer or as a deceptive jammer), and in the second modus (the sleeping mode) the jammer spins its transmitters off for a different random period of time [6]. The energy efficiency is regulates as the ratio of the length of the jamming period upon the length of the sleeping period.
- *Reactive Jammer:* A reactive jammer attempts not to misspend resources by only jamming when it recognize that somebody is transmitting. Its object is not the sender but the receiver, taxing to input as much noise as possible in the packet to improve as many bits as possible given that only a small amount of power is required to modify sufficient bits so that when a checksum is execute over that packet at the receiver it will be categorized as not valid and therefore discarded [6].

The motive of jamming attack is to fill up the communication channel with purposeless signals, due to which verified or permissible user cannot use it. Jamming slowly down the receiving and sending of messages at the destination. It is very difficult to prevent and find out the jamming attacks but still some detection algorithms are struggling to prevent the prospects of jamming attack. Another motive of Jammers is to conceal themselves from the detection algorithms so that they can begin with jamming of some particular region. [13].

3. Related Work

A numeral of previous works has been done for the detection of jamming attacks.

Wood *et al.* [2003] represented a novel mapping service to find out jamming attacks. JAM (Jamming Area Mapping) is a service that delivered quick and exact jamming attack reply. With the aid of this mapping service, we acquire the geographic information which informs us about the jamming area. In this technique extra particular hardware is not required which build it cost effective [1].

P. Yi *et al.* [2005] proposed an easy method so that flooding attacks can be averted. In this method, every node monitors and delibrates the request rate of neighborhood nodes. Now when the request appears it contrast the request rate of adjacent node with the predefined threshold. If the threshold value exceeds, then node record the ID of that node

in a check-list. In future if any request appears from the node stored in the check-list, is discarded [2].

Liu *et al.* [2012] proposed a novel two-phase jamming detection method for sensor networks. In first phase, some signs of jamming are identified speedily. When signs are found then second phase of detection is applied. In this technique we don't requires any extra communication or hardware [12].

Babar *et al.* [2013] represented the game theoretic model of the jamming attack. This paper suggested a game theory based detection technique which is utilized to detect all kinds of jamming attack. This method provides better performance in words of delay, energy and throughput also [13].

S. T. *et al.* [2014] represented a profile based technique which is utilized to detect and suspend the flooding attack on MANET with the help Adhoc on Demand Distance Vector (AODV) routing protocol. In this technique every single node has a profile value. These profile values are put on the base of behavior of MANET. Whenever the node attempts to overreach the fixed threshold value, the attack will be identified and isolated. The key benefit of this technique is that threshold value is not defined; it is based on the average request permitted in the network which changed with the number of request in the network [15].

4. Simulation Environment

To analyze the consequence of jamming attack AODV routing protocol is used. Our focus is to find out the attacker node that rushes the network with RREQ packets. Simulation is brings out in NS2 simulator with 22 nodes in the network. The simulations are divided into scenarios with the normal AODV Jammer attack on the network and with the novel mechanism. The simulation was run for 6.5 simulation seconds with data rate 1 packet at 0.05 sec. The pause time for the simulation is considered to be constant. The details are record in Table 1. Simulation is performed to show the jamming attack and after that detection is done with the help of an efficient method. Some other parameters are shown in table 1.

Table 1. Simulation Parameters

Name	Simulation parameters
Protocol	AODV
Simulator	NS-2
Simulation area	800m×800m
Number of sensor nodes	22
MAC type	Mac/802_11
Attacker Node	1
Operation mode	Active
Application traffic	CBR
Data rate	1 packet at 0.05 sec
Packet Size	1000 bytes
Simulation time	6.5sec
Attack Name	Jamming Attack
Type of Attack	Reactive Jammer

4.1. Energy Spent

Average energy consumed by the sensor nodes in the network is one of the essential metrics to assess the energy efficiency of routing protocol. Comparison graph of Watchdog algorithm and AODV jamming is shown in Figure 2, which shows that energy consumed by Watchdog algorithm is low as compare to AODV jamming. The reason behind this change that Watchdog algorithm is effectively work for isolate the jamming attack that can be observe from the graphical result shown in Figure 2.

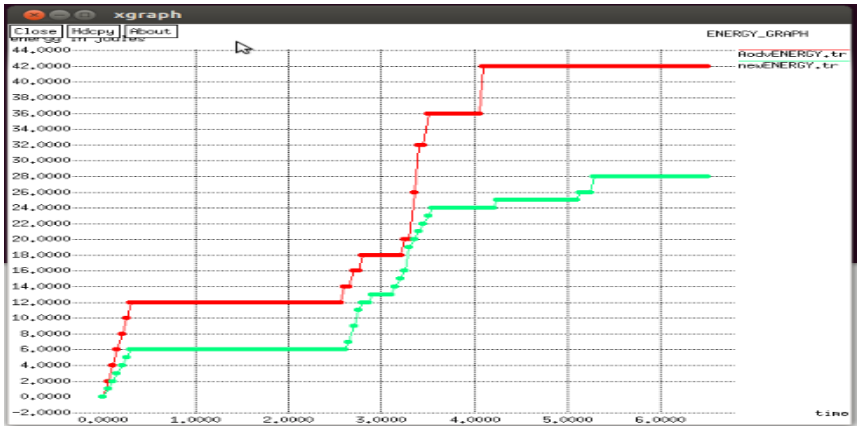

Figure 2. Energy Spent Graph

4.2. Throughput

The throughput represents the ratio of numbers of data packets sent by the source node to the number of data packets received by the destination. Comparison graph of Watchdog algorithm and AODV jamming is shown in Figure 3, which shows that throughput of Watchdog algorithm is high as compare to AODV jamming. The reason behind this change that Watchdog algorithm is effectively work for isolate the jamming attack that can be observe from the graphical result shown in Figure 3.

$$\text{Throughput} = \frac{\text{No. of data packets sent}}{\text{No. of data packets received}}$$

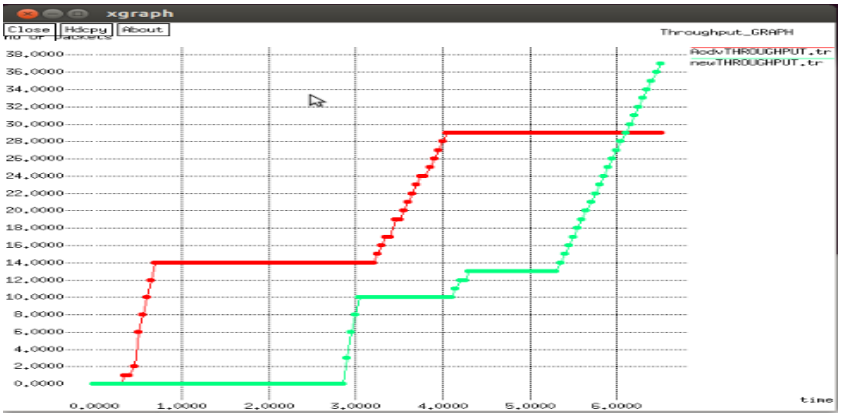

Figure 3. Throughput Graph

4.3. Packet Delivery Ratio (PDR)

The packet delivery ratio is the ratio of total number of packets received at destination node to that of total number of packets sent by the source node. Comparison graph of Watchdog algorithm and AODV jamming is shown in Figure 4, which shows that packet delivery ratio of Watchdog algorithm is high as compare to AODV jamming. The reason behind this change that Watchdog algorithm is effectively work for isolate the jamming attack that can be observe from the graphical result shown in Figure 4.

$$\text{Packet delivery ratio} = \frac{\text{Total no. of packets receive}}{\text{Total no. of packets sent}}$$

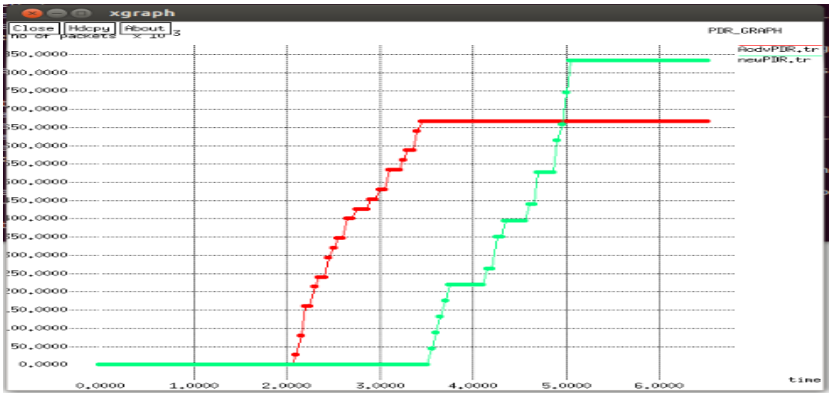

Figure 4. PDR Graph

4.4. Packet Loss

Packet loss is defined as total number of packets dropped in the network. Comparison graph of Watchdog algorithm and AODV jamming is shown in Figure 5, which shows that packet-loss of Watchdog algorithm is very low as compare to AODV. The reason behind this change that Watchdog algorithm is effectively work for isolate the jamming attack that can be observe from the graphical result shown in Figure 5.

Packet loss = Total number of packet send – Total number of packet received

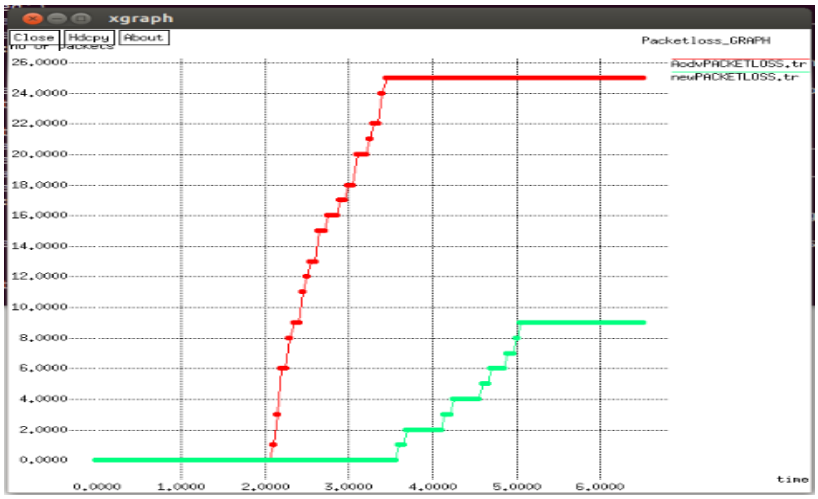

Figure 5. Packetloss Graph

4.5. Retransmission Attempts

Retransmission attempts happened in network only when the delivery of packet is dropped or lost without reaching to the destination nodes. In the comarison of Retransmission attempts of the Watchdog algorithm and AODV jamming, the performace of the Watchdog algorithm is higher than AODV jamming shown in Figure 6.

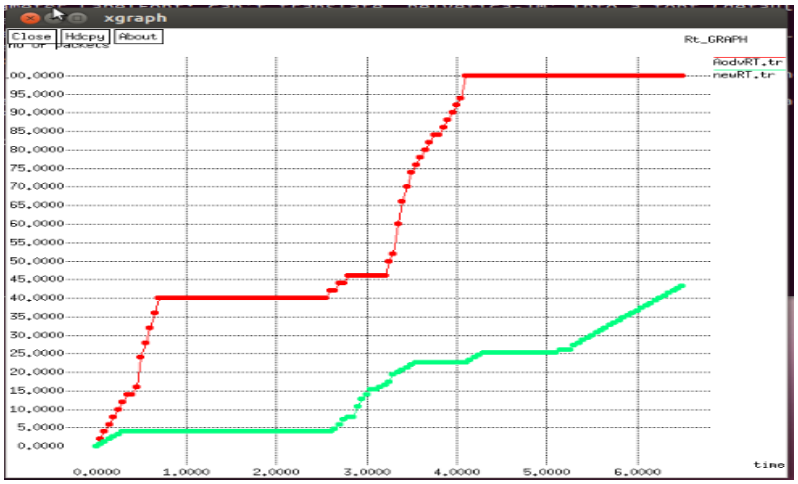

Figure 6. Retransmission Attempts Graph

5. Conclusion

Wireless Sensor Networks are commanly used in various fields for data monitoring purposes. They are helpful in mainly industrial, civilian and scientific applications. So it is important to detect jamming attack quickly because this attack seed DDoS on WSN. This paper recommends an efficient procedure for detection of these attacks. In this procedure monitor mode is used to isolate the harmful path. To isolate the attack the source deluge (flood) ICMP packets in the network. Nodes which collect ICMP packets go to the monitor mode. One node which is neighbor to the harmful node detects malicious node and send message to source node to isolate the path. Now source node isolate the path and the other path will be select for the communication.

The scheme has been assessed using the simulator NS-2. The results of our implementation present superior impact to overcome the jamming attack. This method noteworthy refins system performance and we find that the method is efficient because it detect jamming attack with less retransmission attempts, less energy spent, more throughput, less packet loss and more packet delivery ratio.

Acknowledgment

The authors would like to acknowledge the Department of Computer Science Engineering, CT Institute of Technology & Research Jalandhar, India for the facilities provided during this research.

References

[1] A. D. Wood, J. A. Stankovic, and S. H. Son "JAM: A Jammed-Area Mapping Service for Sensor Networks" Proceedings of the 24th IEEE International Real-Time Systems Symposium (RTSS'03),IEEE, 2003.
[2] P. Yi, "A New Routing Attack in Mobile Ad Hoc Networks," Int'l. J. Info. Tech., vol. 11, no. 2, 2005.
[3] Lazos L., Liu S., and Krunz M., "Mitigating Control-Channel Jamming Attacks in Multi-channel Adhoc Networks" ACM, WiSec'09, March 16–18,Zurich, Switzerland, 2009.
[4] Dempsey T., Sahin G., and Morton Y., "Passive and Active Analysis in DSR-Based Ad Hoc Networks," Ad Hoc Networks. Springer Berlin Heidelberg , pp. 623-638 , 2010.
[5] Chen T., and Kuan W., "A Robust Mutual Authentication Protocol for Wireless Sensor Networks"ETRI Journal, Volume 32, Number 5, October 2010.
[6] Cicho J., Kapelko R., Lemiesz J., and Zawada M., "On Alarm Protocol in Wireless Sensor Networks", IEEE, 2010.
[7] Şen S., Clark J., and Tapiador j., "Security Threats in Mobile Ad Hoc Networks", IEEE, 2010.
[8] Defrawy K., and Tsudik G., "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs", IEEE, Vol. 10, No. 9, September 2011.
[9] Vinit Garg, Manoj Kr.Shukla, Tanupriya Choudhury, Charu Gupta, "Advance Survey of Mobile Ad-Hoc Network," IJCST Vol. 2, Issue 4, (2011), ISSN: 2229-4333.
[10] Humayun Bakht," Survey of Routing Protocols for Mobile Ad-hoc Network" , International Journal of Information and Communication Technology Research, Volume 1 No. 6, (2011), ISSN-2223-4985.
[11] Donggang L., Raymer J., and Fox A., "Efficient and timely jamming detection in wireless sensor networks" Mobile Adhoc and Sensor Systems (MASS), 2012 IEEE 9th International Conference on IEEE, 2012.
[12] D. Liu, J. Raymer, A. Fox "Efficient and Timely Jamming Detection in Wireless Sensor Networks" in 9th International Conference on Mobile Adhoc and Sensor Systems MASS, page 335-343. IEEE Computer Society, December 2012.
[13] S. D. Babar, N. R. Prasad, R. Prasad "Game Theoretic Modelling of WSN Jamming Attack and Detection Mechanism" Published in Wireless Personal Multimedia Communications (WPMC), 2013.
[14] Rajakumar P., Prasanna T., and Pitchaikkannu A. "Security attacks and detection schemes in MANET," Electronics and Communication Systems (ICECS), 2014 International Conference on IEEE, 2014.
[15] Sathish. T, Sasikala. E" Dynamic Profile Based Technique to Detect Flooding Attack in MANET" in International Journal of Innovative Research in Computer and Communication Engineering Vol.2, Special Issue 1, March 2014.
[16] Kapur R., and Khatri S., "Analysis of attacks on routing protocols in MANETs," Computer Engineering and Applications (ICACEA), 2015 International Conference on Advances in IEEE, pp.791-798, 2015.
[17] Khan M., Jadoon Q., and Khan M., "A Comparative Performance Analysis of MANET Routing Protocols under Security Attacks," Mobile and Wireless Technology 2015, Springer Berlin Heidelberg, pp.137-145, 2015.

