A COMPREHENSIVE REVIEW ON PERFORMANCE OF AODV PROTOCOL FOR WORMHOLE ATTACK

Gurmeet Kaur[1], Amanpreet Kaur[2]

[1]M .Tech Student, Centre for Computer Science & Technology, Central University of Punjab, Bathinda, Punjab, India
[2]Assistant Professor, Centre for Computer Science & Technology, Central University of Punjab, Bathinda, Punjab, India

Abstract

Wireless Networking is becoming very popular and interesting technology especially in these days as everyone wants wireless connectivity at anywhere anytime. It contains numerous wireless network technologies such as WiFi, WiMax, HSDPA and WiBro etc. Based on structural arrangement, wireless networks are categorized into two main categories: fixed infrastructure wireless networks and infrastructure less wireless networks. Mobile Ad-Hoc Networks (MANETs) come under the category of infrastructure less wireless networks, which is an autonomous system of mobile hosts connected by wireless links. Nodes are free to move and can join or leave the network at any time whenever required. Wireless ad hoc networks eradicate various problems which may come out while setting up the infrastructure. Communication among nodes in these networks is accomplished via different routing protocols. But these protocols have different security flaws and using these flaws, an attacker can launch many kinds of attacks. Wormhole attack is one of the serious attack in the context of mobile ad-hoc network, which can disrupt any routing channel completely. In this work, an attempt has been made to compare the performance of on-demand reactive routing protocol: Ad hoc On Demand Distance Vector (AODV) with two approaches: normal and attack. The performance metrics evaluated for the two examined approaches are Throughput, Packet Delivery Ratio, Delay and Jitter.

Keywords: *MANETs, Mobility, Network Security, Replay, Routing, Tunnel, Wormhole Attack.*

----------***----------

1. INTRODUCTION

The original idea of MANET started out in the early 1970s and during this period of time, MANET was called "packet radio" network sponsored by DARPA. The whole life cycle of ad hoc networks could be categorized into three generations and present ad hoc networking systems are considered the third generation, which was started out in 1990s [1].

A MANET is a type of ad hoc network that can change locations and configure itself on the fly. Because MANETs are mobile, they use wireless connections to connect to various networks. This can be a standard WiFi connection, or another medium, such as cellular or satellite transmission [2].

E. M. Shakshuki et al [3] have well described the mobile ad hoc networks. According to them, it is a group of mobile (or temporarily stationary) devices, which may participate in the network either directly or indirectly via bidirectional wireless links as nodes are equipped with both a wireless transmitter and a receiver that communicate with each other. Wireless networks can be classified into two major categories [4]:

1.1. Infrastructure Based Wireless Network

It provides communication among mobile hosts through central controller that is AP (Access Point) means to say that nodes cannot communicate directly. The access points also work as a bridge. Example includes traditional cellular systems (base station infrastructure). The features of infrastructure based wireless networks are summarized as follows [5]:

- Having fixed, wired backbone.
- Mobiles can communicate directly with access points.
- Suitable for locations where access points can be placed.

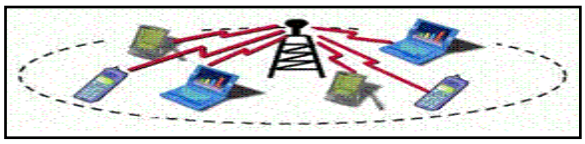

Fig -1: Infrastructure Based Wireless Network

1.2. Infrastructure less Wireless Network

As the name suggests, it does not has any fixed infrastructure for the communication. Each node can communicate directly with other nodes and there is no any need of an access point. One crucial point is that these networks do not have routers so the wireless nodes work as routers. Example includes an ad hoc network. Some of the features of these networks are as follows [5]:

- No wired backbone.
- All nodes are capable of movement.
- All nodes serve as routers called multi-hop routers.
- Reduced administrative cost.

- Ease of deployment.

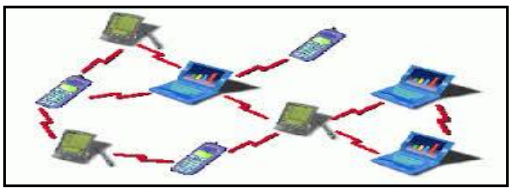

Fig 2: Infrastructure less Wireless Network (Mobile Ad Hoc Network)

The characteristics, security complexities and numerous application scenarios of MANET are summarized in table 1 [6] [7] [8]:

Table -1: Characteristics, Security Complexities & Application Scenarios of MANET [6] [7] [8]

Characteristics	**Security Complexities**	**Application Scenarios**
An independent, distributed and non-infrastructure wireless network.	Due to usage of open air medium, MANET is much more attack prone system.	MANETs can be employed in various military or police exercises.
Allow multi-hop routing.	Lack of centralized controller.	Include emergency services such as disaster relief operations.
Having dynamic network topology.	Dynamically changing network topology allows any malicious node to join the network without being detected.	Mine site operations.
Include heterogeneity among various devices such as mobile phone, laptop, personal digital assistance, MP3 player and personal computer etc.	Lack of clear line of defense.	Urgent business meetings.
Scalable in nature.	Due to various energy and bandwidth constraints.	Robot data acquisition.
Provide intrinsic mutual trust.		In the era of education, entertainment and sensor networks etc.
Allow frequent routing updates.		

Although MANET is emblematic and ubiquitous in nature, but as communication among nodes takes place via open air medium, they face acute security problems.

2. ROUTING PROTOCOLS IN MANETS

There are various MANET routing protocols as no single routing protocol works well in all environments [9]. The reason is that the traditional protocols (which have already written for the wired network) do not work well in MANET. So there was a need to write new protocols for mobile ad-hoc networks [10].

S. R. Jathe & D. M. Dakhane [11] described that in a network of two or more computers, a set of instructions or a common set of rules is required that each computer should follows to communicate each other. Such a set of instructions or rules is called PROTOCOL. Depending upon the many ways by which computers can communicate, the routing protocols in mobile ad-hoc network can be divided into three categories:

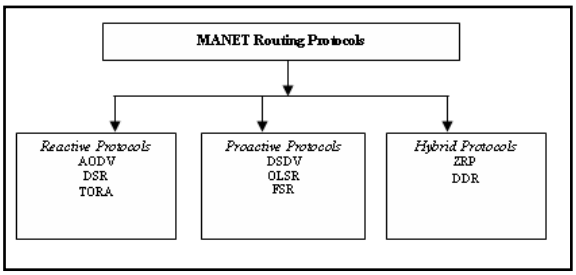

Fig -3: Classifications of MANET Routing Protocols

Demand oriented or reactive routing protocols compute the route to a specific destination only on an on-demand basis. So, there is no any need to maintain the routing table containing all the nodes as entries in each node. Examples include AODV (Ad-hoc On-demand Distance Vector), DSR (Dynamic Source Routing), TORA (Temporally Ordered Routing Algorithm) etc [12].

Table oriented or proactive routing protocols maintain up-to-date routing information from each node to every other node in the network. Examples include DSDV (Destination

Sequenced Distance Vector), OLSR (Optimized Link State Routing) etc [12].

To avoid congestion, data loss, routing overhead and long delay times, the hybrid protocols have been developed. Hybrid routing protocols are the mixture of demand based and table based routing protocols. Examples include CBRP (Cluster Based Routing Protocol), DDR (Distributed Dynamic Routing) and ZRP (Zone Routing Protocol) etc.

2.1. AODV (Ad-hoc On-demand Distance Vector Routing)

The first version of AODV has published in November 2001 by Working Group for routing of the IEFT community. AODV belongs to the category of routing protocols which are demand oriented. To reduce the traffic overhead, routes are only established whenever required due to purely on-demand nature. AODV supports unicast, broadcast and multicast. It uses sequence numbers to solve the count-to-infinity and loop creation problem [13]. N. Gandhewar & R. Patel [14] have described that AODV uses four types of control messages as defined below:

- **RREQ:** It is a route request message. Suppose a node 'S' wants to talk to node 'D' and 'S' is not in range of 'D', then 'S' sends a RREQ to its neighbors. If a neighbor of the source node 'S' does not know a route to the destination 'D', it rebroadcasts the RREQ.
- **RREP:** It is a route reply message. If a neighbor of source node 'S' does know a route to the destination 'D', then it unicasts a RREP back to the source node.
- **RERR:** It is route error message, which is mainly used when a node detects that a link with adjacent neighbor is broken.
- **HELLO:** These are simple messages that nodes send at certain time intervals to all its neighbors to let them know that it is still there.

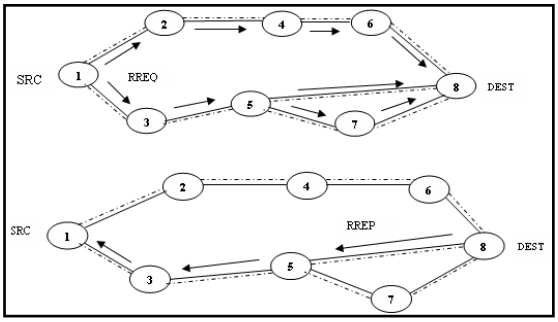

Fig -4: Communication between Source and Destination with RREQ & RREP

A. Boukhalkhal et al [15] have compared some silent features of AODV with other ad hoc routing protocols as shown in table 2.

In table 2, N: the total number of nodes in network
M: the average number of nodes in cluster
D: the number of maximum desired destination
K: network diameter

Table -2: Comparison of Ad-Hoc Routing Protocols

Characteristics	AODV (Demand Oriented)	DSDV (Table Oriented)	CBRP (Hybrid)
Distributed	Distributed in nature	Distributed in nature	Distributed in nature
Loop-free	Looping is not there in AODV	Looping is not there in DSDV	Looping is not there in CBRP
Multicast	Supports unicast, broadcast and multicast	No multicasting	No multicasting
Sequence number	Uses sequence number	Uses sequence number	Sequence number is not used by CBRP
Communication complexity	O(2N)	O(N)	O(N)
Storage complexity	O(D)	O(N)	O(N/M)
Time complexity	O(2K)	O(K)	O(2K)

3. WORMHOLE ATTACK

Security in MANET plays a vital role for basic network functions. Availability, Authorization, Confidentiality, Integrity and Non-repudiation are some basic requirements that effective security architecture must ensure in order to combat passive and active attacks [9] [16] [17].

3.1. Wormhole Attack in AODV

G. K. Singh et al [18] and S. Gupta et al [19] defined wormhole attack as an active attack. During this attack, two colluding nodes, that are far apart, are connected by an underlying tunnel. This transparent tunnel gives an illusion that those colluding nodes are neighbors to each other. In this attack, an attacker tunnels packet received at one point

in the network to another colluding node which will replay them.

Wormhole attacker affects the original functionality of MANET routing protocols such as AODV, DSR and OLSR etc, but this research work emphasizes on wormhole attack in AODV routing protocol. A simplified view of wormhole attack is shown in fig. 5. Suppose source wants to communicate with destination. And this communication is possible through shortest path provided by AODV protocol (called normal route). But if two malicious nodes are kept at two different locations in the network and a malicious node accepts the traffic at one location, tunnels them through wormhole link to another malicious node and replays packets into the network at that location, then this is called wormhole route. It illustrates that AODV routing is completely disrupt by attack. It affects various QOS parameters too such as delay, jitter, throughput, packet delivery ratio and power consumption etc [18] [20].

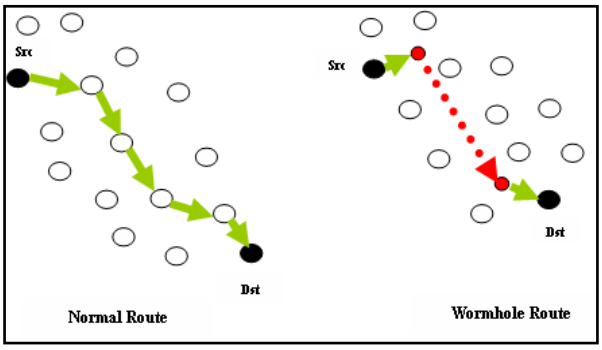

Fig -5: Scenario of Wormhole Attack

3.2. Types and Side Effects of Wormhole Attack

F. A. Jenefer & D. Vydeki [21] have described various types of wormhole attacks as follows:

All Pass: Here malicious nodes can pass all the packets regardless of their size.

All Drop: Here malicious nodes can drop all the received packets in the network.

Threshold: Sometimes, there is a constraint as a threshold value in network and malicious node can drop all the packets having size greater than or equal to the threshold value.

Replay: Here, one malicious node can replay the packets after tunnelling in the network.

Tunnelling: Wormhole attack also called tunnelling attack. So here, a malicious node tunnels the packets from one location to another location in the network via wormhole link.

Propagation Delay: The propagation delay in the network is increased as more time is taken by malicious nodes to send packets from source to destination.

Depending upon above types, wormhole attack affects MANET in the form of four security threats named modification, interception, fabrication and interruption as follows [10]:

Modification: Here one malicious node can modify the packet before forwarding that packet to next node in the network. As a result, data or message will lose their integrity.

Interception: Here an unauthorized user (acts as malicious node as a part of network) can intercept the packet and can modify it to forward to the next node. As a result, data integrity and confidentiality will lose.

Fabrication: Along with data modification, generation of unused and unwanted packets is also come under the category of an "attack", called fabrication attack. Here, a malicious node can create a large number of unused packets and send it into the network beyond its capacity. As a result, network will fail.

Interruption: Here malicious node can interrupt the message to receive by the destination node.

Due to above side effects of wormhole attack, basic security goals such as authorization, confidentiality, integrity and availability get violated.

4. SIMULATION SETUP

In order to perform the simulation of normal AODV and AODV under attack environment, a number of simulations have been performed by vary number of nodes.

4.1. Environment Used

To construct a real distributed testing environment, the cost is very high. So simulation is widely used in network research. Simulation is the manipulation of the model of a system that is used to observe the behavior of a particular system in a setting similar to real-life [22]. For this work, NS2.35 network simulator was used, which is a discrete event simulator. This study was performed on Intel Core i7 computer system using Ubuntu Linux 12.04 Operating System.

4.2. Simulation Methodology

This study is based on simulation. Firstly, to simulate normal route using AODV, a network topology is created using NS2 Tcl script. Secondly, to perform wormhole attack, two malicious nodes are kept at two different locations in the already created topology and the required coding is done to create wormhole link/tunnel with the help of other malicious nodes in the network, which bypass normal route.

Then the results are analyzed graphically and the comparison of the performance of two examined approaches (normal and attack) is drawn. The parameters used to carry out simulation are summarized in table 3.

Table -3: Simulation Parameters

Parameters	**Value**
Simulator	NS-2 Version 2.35
Number of Nodes	10, 20, 30, 40, 50
Topography Dimension (m*m)	1186*584
Simulation Time	60 seconds
Traffic Type	CBR
Signal Propagation Model	Two Ray Ground Model
MAC Type	802.11 MAC Layer
Packet Size	512 bytes
Data Rate	2.0 Mb
Mobility Model	Random Waypoint
Node Mobility Speed	0-60 m/s
Routing Protocol	AODV
Interface Queue	Drop Tail/Priority Queue
Channel	Wireless Channel
Link Layer Type	LL
Antenna Type	Omni direction
Minimum Number of Malicious Nodes	2
Performance Parameters	Throughput, PDR, Delay and Jitter
Examined Approaches	Normal and Attack

5. RESULT ANALYSIS & COMPARISON

Performance of normal AODV and AODV under attack is analyzed in terms of throughput, PDR, delay and jitter using NS2 and various parameters are described in table 3. After configuring, results are extracted from it using AWK scripts. Following are the results of simulation on NS2:

5.1. Throughput

Network throughput is measured as the total number of packets received at the destination over a period of time and is expressed in kbps. In fig. 6, results of throughput for both normal AODV and AODV under attack are plotted and it can be noticed here that throughput is increased in normal AODV as compared to AODV under attack. The reason behind low throughput in case of attack is replay and tunneling nature of wormhole attack. More is replaying of packets more will be dropping.

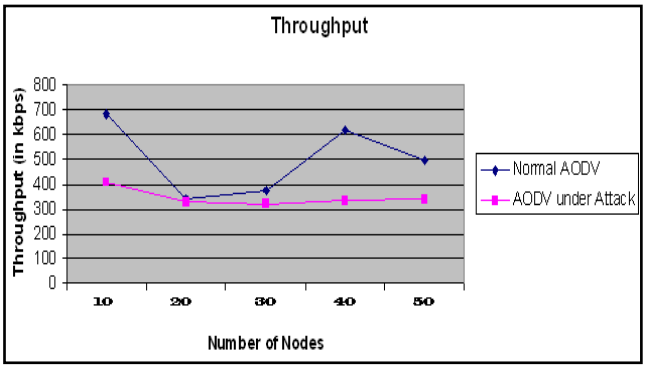

Fig -6: Comparison of Throughput of Normal AODV and AODV under Attack with Increase in Number of Nodes

5.2. Packet Delivery Ratio

PDR is the ratio of packets received at destination node to that of number of packets sent by source node. It is measured in percentage. In fig. 7, it is observed that the value of PDR for normal AODV is high initially. But as the nodes are increased, PDR is gradually decreases. As replay of packets in case of attack is more, so packets delivered at destination is more. As a result, packet delivery is more in AODV under attack for higher number of nodes.

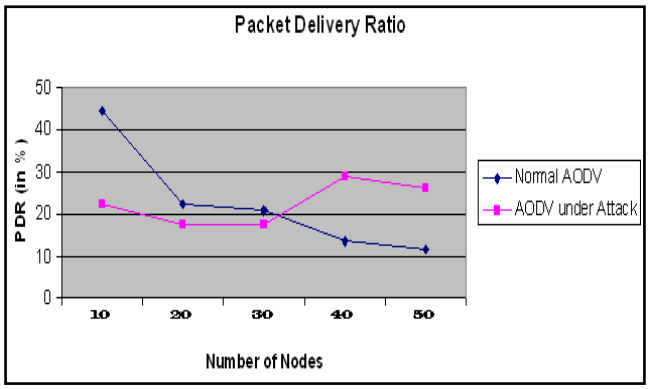

Fig -7: Comparison of PDR of Normal AODV and AODV under Attack with Increase in Number of Nodes

5.3. Delay

Delay is the total time taken for the packet to reach from source to destination and measured in seconds. In fig. 8, the time taken for packets to reach destination is high for AODV under attack.

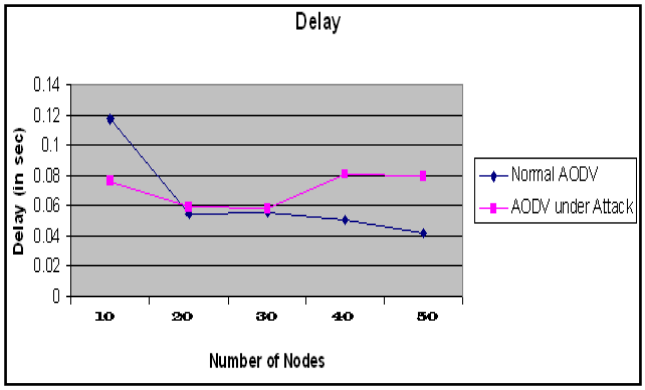

Fig -8: Comparison of Delay of Normal AODV and AODV under Attack with Increase in Number of Nodes

5.4. Jitter

Jitter is the variation of delay. Fig. 9 clearly depicts that the rate of jitter increases in case of AODV under attack as the number of mobile nodes and tunnel length (number of hops) increases.

Fig -9: Comparison of Jitter of Normal AODV and AODV under Attack with Increase in Number of Nodes

6. CONCLUSIONS AND FUTURE WORK

A wormhole attack is a very serious threat to the important security objectives (Privacy, Integrity and Availability) of the mobile ad hoc network and it must be treated as a highest priority threat. Performance of AODV protocol is analyzed under normal condition and wormhole attack condition. The overall results show that normal AODV performs well for all the performance metrics in random waypoint mobility model except PDR. MANET faces more challenges due to topology keeps changing regularly as nodes are mobile in nature. Till now, many approaches have been developed for the detection and isolation of these wormhole nodes but these mechanisms do not take into account the impact of different mobility models. This research work will focus on analyze these two approaches for AODV using another mobility model such as reference point group mobility model.

REFERENCES

[1]. Chapter-3 Overview of Mobile Ad Hoc Networks, Available at: http://www.shodhganga.inflibnet.ac.in/bitstream/10603/4106/.../11_chapter%203.pdf, pp. 19-36.

[2]. Available at: http://www.techterms.com/definition/manet.

[3]. E. M. Shakshuki, N. Kang, and T. R. Sheltami, "EAACK – A Secure Intrusion – Detection System for MANETs", *IEEE Transactions on Industrial Electronics*, vol. 60, no. 3, pp. 1089-1098, March 2013.

[4]. N. Khemariya, and A. Khuntetha, "An Efficient Algorithm for Detection of Blackhole Attack in AODV based MANETs", *International Journal of Computer Applications*, vol. 66, pp. 18-24, March 2013.

[5]. C. E. Perkins, "Ad Hoc Networking with AODV", Available at: http:// www.psg.com/~charliep/txt/Daedeok2002/AODV-Daedeok.pdf.

[6]. A. Kaur, and M. Mittal, "A Comprehensive Review on Performance of AODV and DSDV Protocol using Manhattan Grid Mobility Model", *International Journal of Research in Engineering and Technology*, vol. 03, pp. 496-505. March 2014.

[7]. J. Hoebeke, I. Moerman, B. Dhoedt, and P. Demeester, "An Overview of Mobile Ad Hoc Networks: Applications and Challenges", Department of Information Technology (INTEC), Ghent University, Belgium.

[8]. C. M. Cordeiro, and D. P. Agarwal, "Mobile Ad Hoc Networking", OBR Research Center for Distributed and Mobile Computing, ECECS, University of Cincinnati, USA.

[9]. R. Agrawal, R. Tripathi, and S. Tiwari, "Performance Comparison of AODV and DYMO MANET Protocols under Wormhole Attack Environment", *International Journal of Computer Applications*, vol. 44, no. 9, pp. 9-16, April 2012.

[10]. V. K. Upadhyay, and R. Shukla, "An Assessment of Worm Hole Attack over Mobile Ad-Hoc Network as serious threats", *Int. J. Advanced Networking and Applications*, vol. 05, pp. 1858-1866, 2013.

[11]. S. R. Jathe, and D. M. Dakhane, "Indicators for Detecting Sinkhole Attack in MANET", *International Journal of Emerging Technology and Advanced Engineering*, vol. 2, pp. 2250-2459, Jan. 2012.
[12]. S. Gandhi, N. Chaubey, N. Tada, and S. Trivedi, "Scenario-based Performance Comparison of Reactive, Proactive & Hybrid Protocols in MANET", *IEEE International Conference on Computer Communication and Infomatics*, 2012.
[13]. AODV, Available at: http://www.rainer-baumann.ch/public/qec.pdf.
[14]. N. Gandhewar, and R. Patel, "Detection & Prevention of Sinkhole Attack on AODV Protocol in Mobile Ad Hoc Network", *Fourth International Conference on Computational Intelligence and Communication Networks, IEEE Computer Society*, pp. 714-718, 2012.
[15]. A. Boukhalkhal, M. B. Yagoubi, M. Djoudi, Y. Ouinten, and M. Benmohammed, "Simulation of Mobile Ad hoc Routing Strategies", *IEEE Transactions*, pp. 128-132, 2008.
[16]. B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A Survey of Routing Attacks in Mobile Ad Hoc Networks", *IEEE Wireless Communications*, vol. 14, no. 5, pp. 85-91, Oct. 2007.
[17]. P. G. Argyroudis, and D. O'Mahony, "Secure Routing for Mobile Ad Hoc Networks", IEEE Communications Surveys & Tutorials, Third Quarter, vol. 7, no. 3, pp. 2-21, 2005.
[18]. G. K. Singh, A. Kaur, and A. L. Sangal, "Performance Analysis of DSR, AODV Routing Protocols based on Wormhole Attack in Mobile Ad-hoc Network", *5th IEEE International Conference on Advanced Computing & Communication Technologies*, pp. 31-36, 2011.
[19]. S. Gupta, S. Kar, and S. Dharmaraja, "WHOP: Wormhole Attack Detection Protocol using Hound Packet", 2011 IEEE International Conference on Innovation Technology, pp. 226-231, 2011.
[20]. C. P. Vandana, and A. F. S. Devaraj, "Evaluation of Impact of Wormhole Attack on AODV", *International Journal of Advanced Networking and Applications*, vol. 4, no. 4, pp. 1652-1656, 2013.
[21]. F. A. Jenefer, and D. Vydeki, "Performance Analysis of Mobile Ad Hoc Network in the Presence of Wormhole Attack", *International Journal of Advanced Computer Engineering and Communication Technology*, vol. 1, no. 1, pp. 13-18, 2013.
[22]. J. Singh, K. Kumar, M. Sachdeva, and N. Sidhu, "DDoS Attack's Simulation using Legitimate and Attack Real Data Sets", International Journal of Scientific & Engineering Research, vol. 3, pp. 1-5, June 2012.