VOL. 13, NO. 4, FEBRUARY 2018 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

# IMPLEMENTATION ON IDENTIFYING PACKET MISBEHAVIOR IN NETWORK VIRTUALIZATION

S. Reshmi[1] and M. Anand Kumar[2]
[1]Department of Computer Science, Karpagam University, Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India
[2]Department of Information Technology, Karpagam University, Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India
E-Mail: reshmismca@gmail.com

## ABSTRACT

Background/Objectives: This paper deals with the implementation on identifying packet misbehavior in network virtualization with the help of two algorithms namely Obfuscation and Heuristics algorithm to safeguard the packets against intruders. Methods/Statistical Analysis: Black hole, gray hole, cooperative black hole and cooperative gray hole attacks are eliminated using these two algorithms in network virtualization. Findings: These algorithms use a special concept in finding the attacks and eradicate these terrible attacks in the very initial stage. Acknowledgement packets or even the resend packets are attacked by malicious nodes, these all are identified and packets are transmitted safely to the destination. Applications/Improvements: Based on the packet deliverance, throughput and node itinerant performance of the packets are evaluated. To discover the fault, heuristics algorithm is used. This proposed work protects from the third parties and confuses them completely by obfuscation algorithm which is used.

**Keywords:** network virtualization, black hole attack, heuristics algorithm, obfuscation algorithm, gray hole attack, packet loss, clogging, latency, bandwidth, congestion factor.

## INTRODUCTION

A network packet is a systematic unit of statistics carried by a packet-switched network. A single packet contains the user information and information to control which provides data to be provided [2]. The header information is added which is fully secured using obfuscation algorithm and important information is wrapped and sent to the destination. Packet sieving is a kind of firewall technique used to control network admittance by monitoring inward and departing packets and allowing them to reach the destination [2].

Data travels in the form of packets over the internet. Each packet carries maximum of 1500 bytes and a wrapper with both header and footer [3]. The information in the wrapper tells computer what sort of data are in the packet, how it hysterics together with others, and from where it is originated. In the destination edge, the receiving information assembles the packets like a brainteaser and recreates it [3].

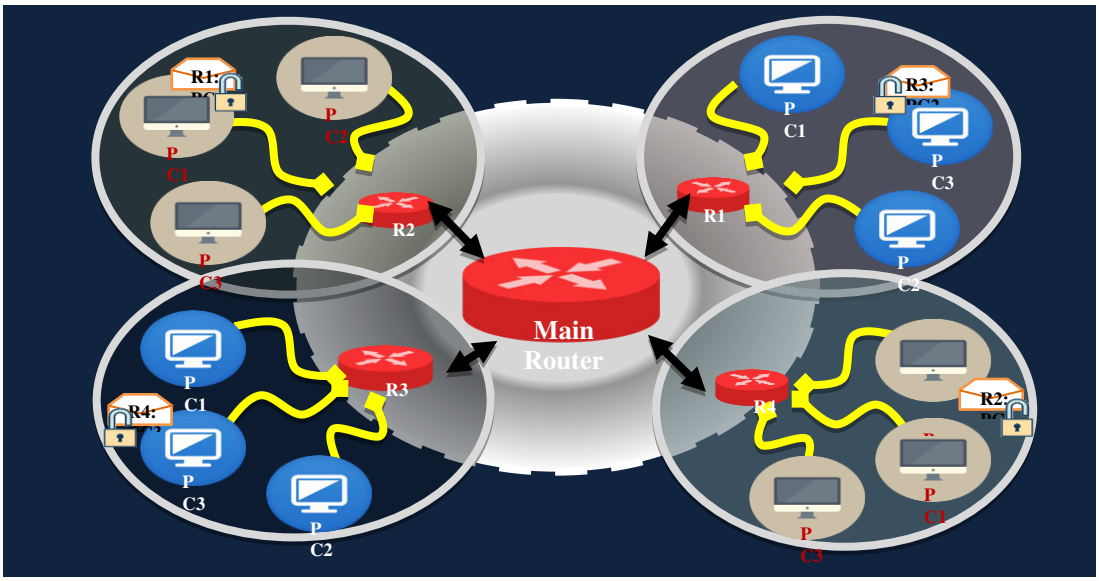



**Figure-1.** Architecture diagram of packet transmission via routers.

## LITERATURE SURVEY

In this paper, detecting the maliciously router is maneuvered the tributary of packets. The effectual attacks are concerned which a router drops packets randomly and selectively. In fact, it's very exigent to trait the lost packets to a malicious feat. All the packets are stored inside a temporary place and when it overflows then packets are dropped drastically. Based on traffic tariff and

size of clipboards clogging occurs, this is tested using heuristics and obfuscation algorithms.

The work [8] proposes an algorithm called Trust Value algorithm to detect the black hole based on the trust values. In which they consider mainly on analyzing the traffic pattern techniques in the wireless nodes results in reduction of packet drop ratio to improve the security of WLAN.

The work [9] proposes an algorithm to detect black hole attacks. In this, first a false request is broadcasted to the destination and when there is an attack then it will reply to that request and a list of black hole nodes is send via alarm packet.

The work [14] proposes a table called Data Routing Information Table to detect and eliminate the black hole attacks in the source node. This source node will check the next and previous node of a route to check the malicious nodes in the path. Opnet 14.5 simulator is used for evaluating and by this approach the packet overhead is decreased.

The research work [15] proposes a solution to detect Black hole attack using Hint-based Probabilistic routing protocol. Insinuation values for each node are figured out and are stored in its own buffer. The network performance is scrutinized for packet distribution, packet plunge, throughput and overhead proportion. The research work [17] proposes a solution to scrutinize the malevolent node to eliminate the Black hole attack, the solution thus called as hash function. This method snubs the first response and opts for subsequent finest conduit.

The paper [18] proposes a technique based on arrangement of infringement detection. This technique is mainly used to eliminate black hole attacks in which individual nodes' behaviors are scrutinized. This technique detects run-time desecration of the stipulation, and is simulated by NS2 for better performance. A new mechanism has been proposed by the author [19] called Bayes' Theorem and prior probability. This method searches for unreliable nodes and if any such unreliable node is identified, then this is eliminated using the above said mathematical model to improve the performance and to secure the routing.

To detect and eliminate black hole attack, the paper [21] proposes an algorithm called secure knowledge algorithm. Before declaring node as malicious node, first liberation of data to destination node is considered and finds the reasons for packet drop. This packet drop declares the node as black hole node. Here delivery ratio is determined using NS2 simulation tool. The work [22] uses a synchronization technique to forestall the black hole attacks. This is used to transmit the synchronization based on the progression of time. This will compare the internal and peripheral time based on the threshold time, if threshold time is less than the time normal node, then nodes are listed and attacks are detected.

The paper [24] for each node of the Extended Data Routing Information is maintained and associated with the concept of DRI to detect and avert black hole and gray hole attacks. To keep track of all sort of malevolent nodes and to detect them, Extensive Data Routing Information is used. This ensures in providing secure path while broadcasting the data from source to destination and knobs all different occurrences of attacks present in the network.

## PACKET LOSS AND METHODS TO FIX IT

Packet loss occurs when mislaid of packets are in the path between the source and destination. It is mainly due to network clogging, measured in percentage and calculates latency [1]. Packet loss is the concept of dumping packets in a network when router is swarmed and extra packets are omitted. Packet loss occurs are based on clogging and packet loss attack. Packet loss may or may not be troublesome to the recipient of the data, depending on the type of network service and the brutality of the loss. With best services, loss packets are recovered and handled accordingly [2].

Latency is the quantity of time a message takes to navigate a system. Here it calculates based on the packet delivery, which is how much time it takes for a packet of information to dig up from one nominated point to another [3]. Jitter is the term refers to the amount of time it takes a bit to transfer from source to destination. It varies from over time which is based on delay of packets in a system which holds the packet for a longer time. The system may be single appliance or a complete system which includes routers and links [4].

**Table-1.** Packet loss measurements.

| Device | Ordeal | CVSS | Protocols | Packet size (bytes) | Packet loss |
|---|---|---|---|---|---|
| A | IP Unicast tempest | 4.5 | ARP | 80 | 20 |
| B | UDP attack | 6.3 | ICMP | 80 | 34 |
| C | IP Mislead | 2.7 | RARP | 80 | 9 |
| D | Ethernet blemish | 7.8 | DHCP | 80 | 55 |
| E | TCP / IP attack | 9.1 | PPTP | 80 | 49 |

There are few methods to fix the packet loss, through which packet loss can be identified. By unplugging modem and router for some time and plugging it again resets the connection completely [3]. Based on the data rate of a system and its frequency band, the packet loss are identified and rectified. Through this bandwidth and throughput are measured [2] [6]. Bandwidth is measured with the help of data rate of a system and its frequency, whereas throughput is measured based on the performance of a system when there is a delay in transmitting [3] [7].

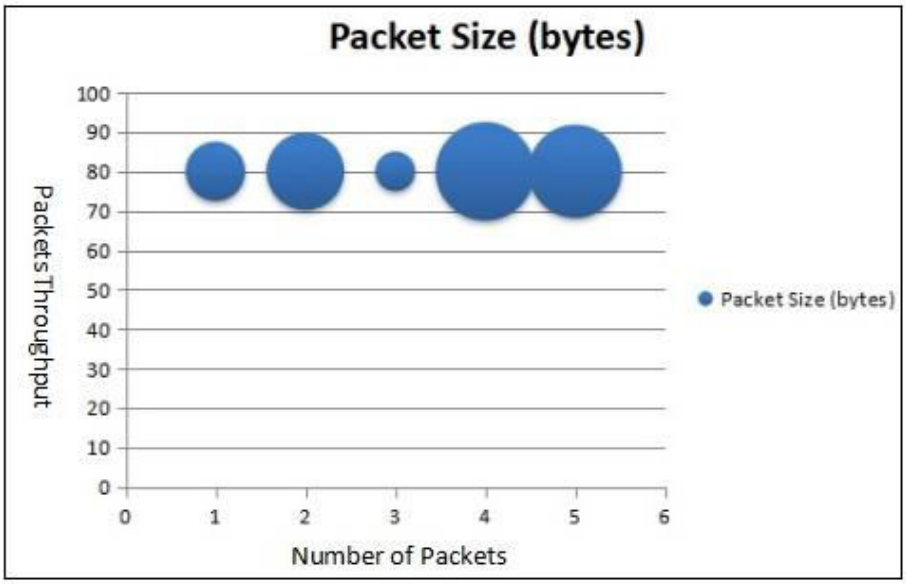
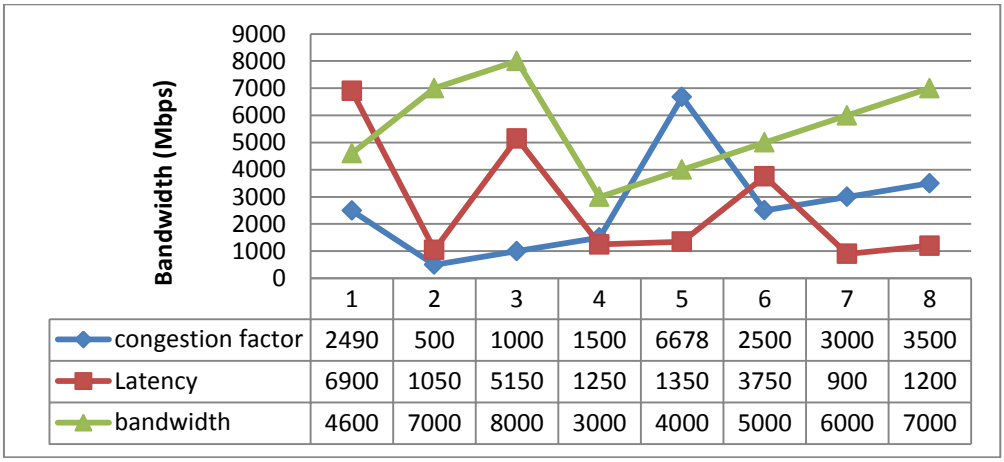



**Figure-2.** Packet size in bytes.

Delays are caused due to errors in the path, aloofness, clogging and other capabilities involved in transmission. These errors are very critical while transmitting data [11]. Jitter helps in arriving packets to the destination with discrepancy in timing and order. Dropping of packets are due to many reasons like clogging in linking, recital of device (router, switch etc), any issues in software and hardware working with or even cabling [12].

**Clogging in links**

In a network a data must trek from one place to another place. If one system requests for a data of information it is sent via the links with more secured concepts. The data is wrapped and labeled accordingly. If a single system requests for the content, then it is sent without any disturbances [12]. But if multiple systems request for different packets or same set of packets at the same time then problem occurs. All data arrive at a stretch and congestion occurs [5].




| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| congestion factor | 2490 | 500 | 1000 | 1500 | 6678 | 2500 | 3000 | 3500 |
| Latency | 6900 | 1050 | 5150 | 1250 | 1350 | 3750 | 900 | 1200 |
| bandwidth | 4600 | 7000 | 8000 | 3000 | 4000 | 5000 | 6000 | 7000 |

**Figure-3.** Latency, bandwidth with congestion factor.

At this juncture, each packet has to wait in a queue for their turn and is sent to the destination with more secure methods. If the network device overloaded with the packets then there will be lack of rooms to

accommodate the new upcoming data, then throwing away of packets happens obviously which are not noticeable [4]. User notices the mislaid packets, slows down the transmission speed by which time is consumed and re-transmits the data. For critical applications threshold level decreases and packet loss occurs heavily [6].

**Recital of router/switch/firewall**

If router/switch/firewall is not able to keep up the packet traffic. Hardware and software faces the traffic, if too it arrives at the device then the memory or CPU are not able to handle the extra traffic pressure. Beyond the capacity of a place if traffic is huge then packet loss occurs drastically [7].

**Software and hardware concern or cabling**

The problems in the network are because of the issues or bugs that cause irregularity in transmission of packets. This stops the deployment stage and will not detect the performance issues for awhile [23]. With the help of capturing the packets and system log the issues are identified using the detection and troubleshooting techniques [3].

Packet dropping also occurs physically through malfunctioning. If there is any mistakes in hardware or cabling then error messages occur and are seen on system logs or copper cabling and fiber optic respectively [20].

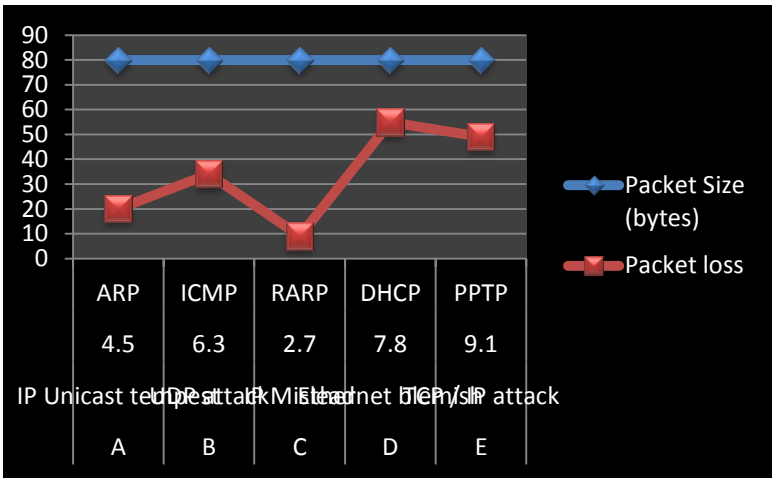



**Figure-4.** Chart for packet loss in networks.

**PROPOSED SCHEME AND PROBLEM ANALYSIS**

To reduce the consequences of packet loss due to network congestion, increase the bandwidth with data rate and implement the quality by prioritizing the packet in traffic. By replacing the hardware with new equipments that knob the throughput or further equipment is added to increase the throughput - is the remedial for the performance of a device.

**Table-2.** Test case for individual device with recovery time.

| Device | Ordeal | Rate (FPS) | Frequency (HZ) | Recovery time |
|---|---|---|---|---|
| A | IP Unicast tempest | 4005 | 400 | < 5s after test ends |
| B | UDP attack | 1290 | 1200 | reset requires |
| C | IP Mislead | 1599 | 768 | > 0.45s after test ends |
| D | Ethernet blemish | 48 | 3434 | < 10s after test ends |
| E | TCP / IP attack | 1600 | 1078 | reset requires |

Packet loss is calculated based on the packet loss ratio that is total number of packet lost / total numbers of packets send. Packet loss is also caused due to high latency, upstream / downstream issues as well as faulty hardware or cabling, packets are lost. For hardware, software fault or cabling, upgrade the software on exaggerated devices.

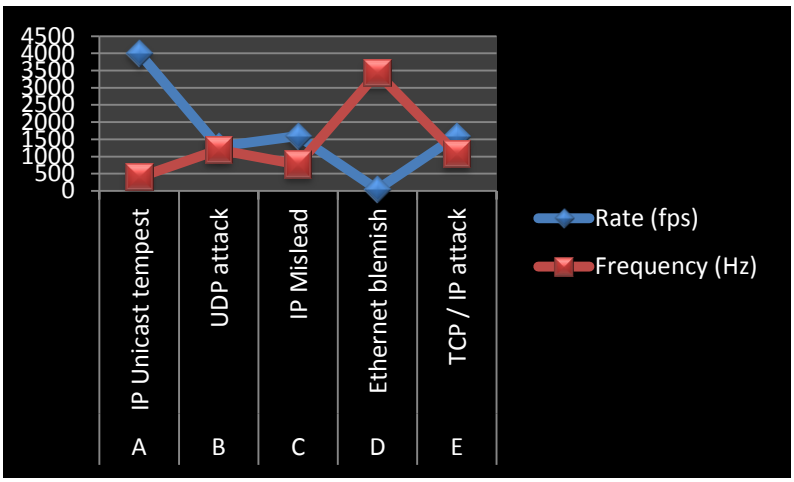



**Figure-5.** A chart to show the rate and frequency for different protocols.

The proposed system uses two different types of algorithm through which dropped packets are identified separately and sent to the destination in the shortest path. Initially set of packets are sent in a queue, which is reversed using obfuscation algorithm. If the data in the packets are reversed then it is very difficult for the intruder or hacker to fetch it. These inverted data are then encrypted for security purpose and encrypted data are sent to queue in more secure manner to the destination via router by classifying packets. This is done with the help of heuristics algorithm which finds the shortest path to reach the packets soon to the destination [2].

In certain circumstances collision or dropping packets occurs then the whole polluted data are fetched, schedules it in a queue manner and analyze the packets. The missed packets are identified and delay time is set to make the receiver understand the delayed packets to merge with the original. These delayed packets are combined with other packets and are sent to decrypt the data for retrieving. The obfuscation algorithm is used to decrypt the data and resultant packets are received by the receiver in the destination place.

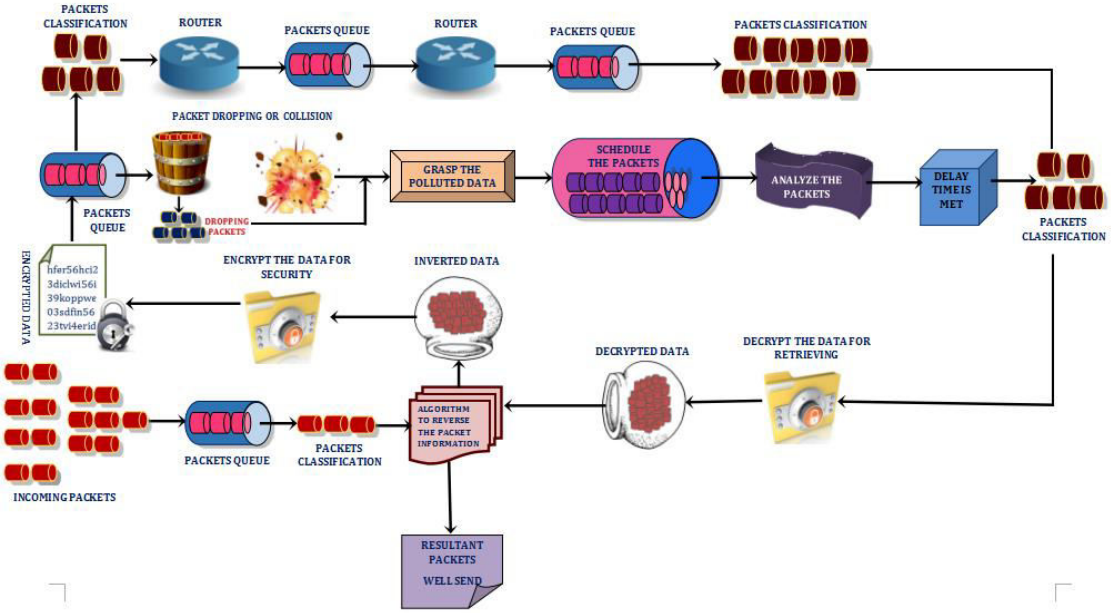



**Figure-6.** Architectural diagram of proposed system.

## IMPLEMENTATION PROCESS

When a packet is transferred it is not sure that all packets reach correctly to the destination. Here two different problems occur: Gray hole attack and Black hole attack. One is based on the dropping packets randomly that is in‘t’ seconds or in ‘n’ packets and another is based on packet loss normally. To overcome this two algorithm say heuristics and obfuscation algorithm are used [4].

| No. of nodes | Packet loss % | Packet size (bytes) |
|---|---|---|
| 1 | 34 | 56 |
| 2 | 22 | 60 |
| 3 | 12 | 76 |
| 4 | 22 | 55 |
| 5 | 12 | 66 |
| 6 | 5 | 87 |
| 7 | 9 | 77 |

Heuristics algorithm is to discover and find the solution close to the best one very fast, easily and in short period of time [2]. Obfuscation algorithm is a process applied to the information to intentionally make it difficult and to reverse without knowing the algorithm that is applied, and original data are hidden with random characters. Using this algorithm, one can hide the coding without others being able to easily understand, that is to confuse the third parties [2].

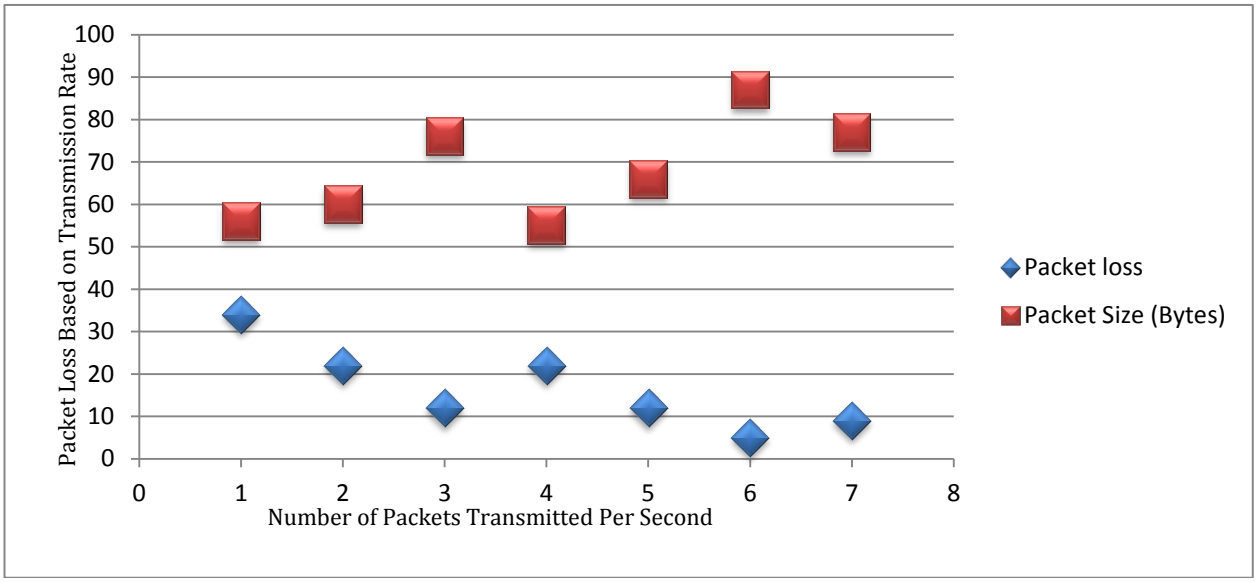



**Figure-7.** Demonstration of packet loss structure.

**Recital criterion**

In order to clearly analyze and understand the attacks, a few performance metrics are enacted by which something may be judged or decided. This measures conduct, state and recital of a packet infrastructure. The performance of packet deliverance is based on the quantifiable measures that can artifact, defends and grab the success or failure of packet transmission.

The recital criterion is used to measure or keep in track of performance of each packet delivery. This is used mainly to similitude the performance of each packets from the sender and are sent to the receiver. Here the safety, time conception, resources, quality of service etc are judged. This is a key to evaluate how packets are transmitted to their own target places more accurately. A good performance metrics yield the results based on improvements. This criterion is used to improve packets performance while transmitting and its behavior with respect of missing them.

If the performance of a packet changes then the packet misbehaves and chooses the wrong path for destruction. While sending packets from source to destination, that is a continuous process of transmitting data without any disturbances then the metrics will show an affirmative upshot for each action. If not different path with different approach is a semantic role. To check the networks operations throughputs and time slots are used to compare the internals of each set of packets.

**To estimate the performance**

**A. Packet deliverance proportion**

Total number of packets is send to the receiver by the sender but it's not sure that all the packets reach the destination completely. So addressing the packet and sending to the destination is said to be triumphant delivery of a packet over a network.

To send the packet the sender needs to know the node and socket's address of the recipient. And it is necessary to keep in track of the delivered packet information and calculate its ratio to discover the malevolent nodes. This proportion is between the number of packets and the destination packets initiated in the upper layer.

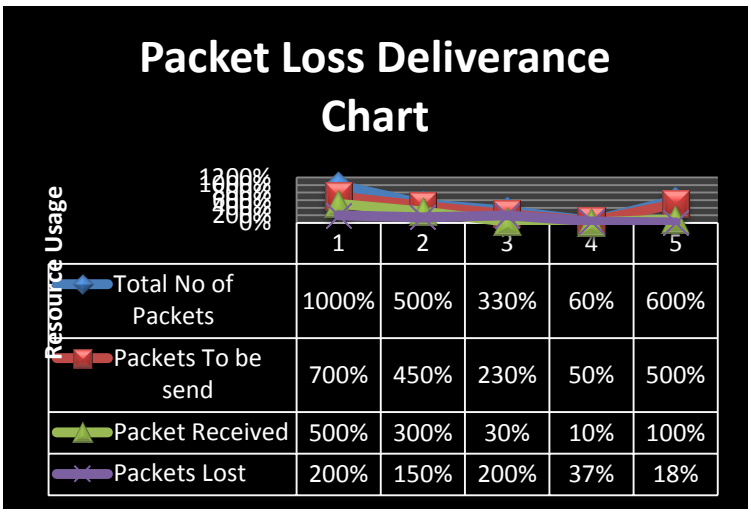



**Figure-8.** Packet deliverance proportion chart.

**B. Throughput**

Throughput is used to determine the recital of internet and network connections. It helps in identifying the amount of data transmitted from one place to another and measures its units in a prescribed time. The maximum throughput in a network is higher than the actual throughput accomplished by the packets that are send every time.

Throughput = Data Transfer Rate **X** Performance Ratio

However, the actual data transfer may be inadequate due to network traffic, throughput helps in identifying it. It also measures system speed, its efficiency and retort time through which the total amount time between source and destination is calculated. It depends on line clogging, bandwidth and fault amendment. Successful network throughput is based on triumphant message delivery over a channel and is measured in bits per second or packets of data per second or related to time period.

**Table-3.** Packet delivery ratio based on nodes.

| **Protocol** | **Number of nodes** | **Throughput** (kbps) | **Delay** (ms) | **Packet delivery ratio** |
|---|---|---|---|---|
| AODV | 100 | 1461.41 | 500.5 | 89.5 |
| DSDV | 50 | 829.75 | 437.9 | 96.24 |
| DSR | 200 | 576.99 | 280.3 | 189.78 |

Throughput is the usual rate of flourishing message delivered to the destination via connecting path. Throughput is tested with the help of AODV, DSDV and DSR.

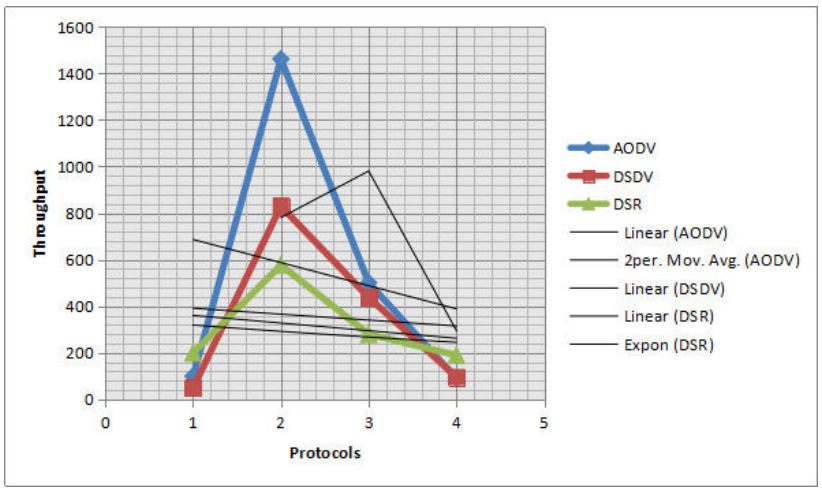



**Figure-9.** A chart to exhibit throughput with protocols.

A routing protocol called ad-hoc on-demand distance vector (AODV) premeditates for wireless and mobile ad-hoc networks. On demand this protocol ascertains routes to the destinations by the support of unicast and multicast routing. Destination-Sequenced Distance-Vector Routing (DSDV) is a table-driven routing scheme for ad-hoc mobile networks. This is mainly used to decipher routing loop difficulty.

Another routing protocol is Dynamic Source Routing (DSR). This is also for wireless networks which is similar to AODV and does not rely on routing table at each intermediary because it uses addressing the path.

### C. Node itinerant

Broadcasting packets are with the aim of sending duplicate copies sent to the different types of links and ensures that every device with broadcasting domain receives properly. Node itinerant indicates the movable or transportable velocity of nodes from source to destination. Travelling the content from one place to another is itinerant.

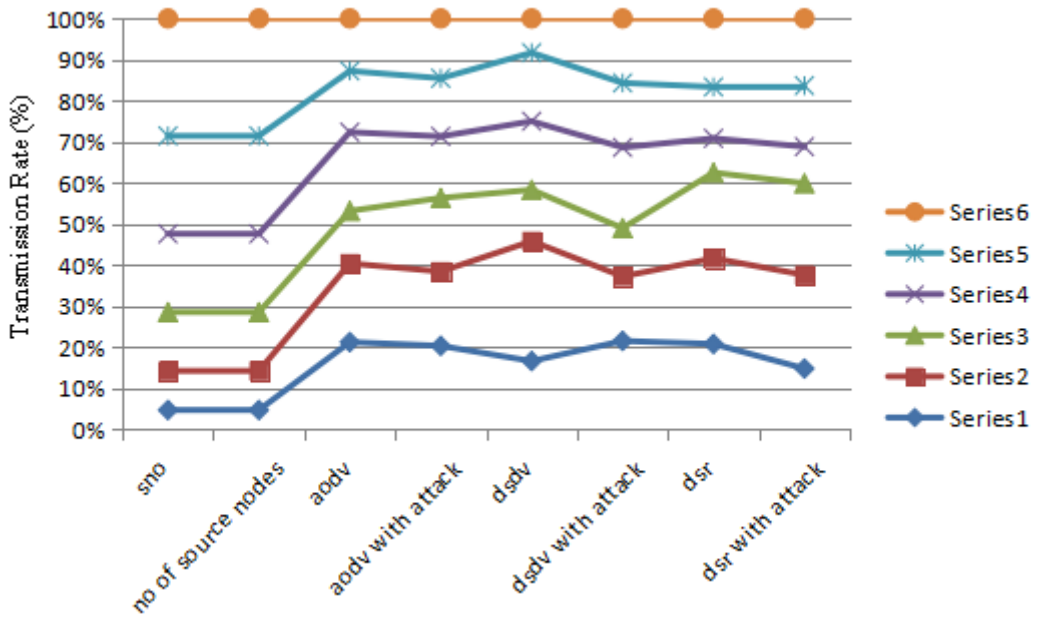



**Figure-10.** A chart to expose the transmission of nodes.

If the quantity of plummet packets increases in the haulage path then the trounced data would be highly increasing, then the following are identified:

### D. Packet plummeting

A malevolent node crushes few packets that are to be transferred, even those packets plummets from the path. When packets fail to reach the destination on time, packets are lost. This is mainly due to network clogging. Losses of packets are measured in percentages.

There are many effects of getting packets plummeting like error reduction, slight irregular movement called jitter and gaps between the packets are created. This tends to severe defacement of acknowledged data, corruption or even over burden of nodes in the network.

TCP/IP detects the loss of packets and retransmits it to ensure consistent message, which reduces throughput and clogging is evaded. Network clogging plays a vital role in reduction of service quality. This is due to overload of packets transmission which affects the throughput either by increasing or decreasing.

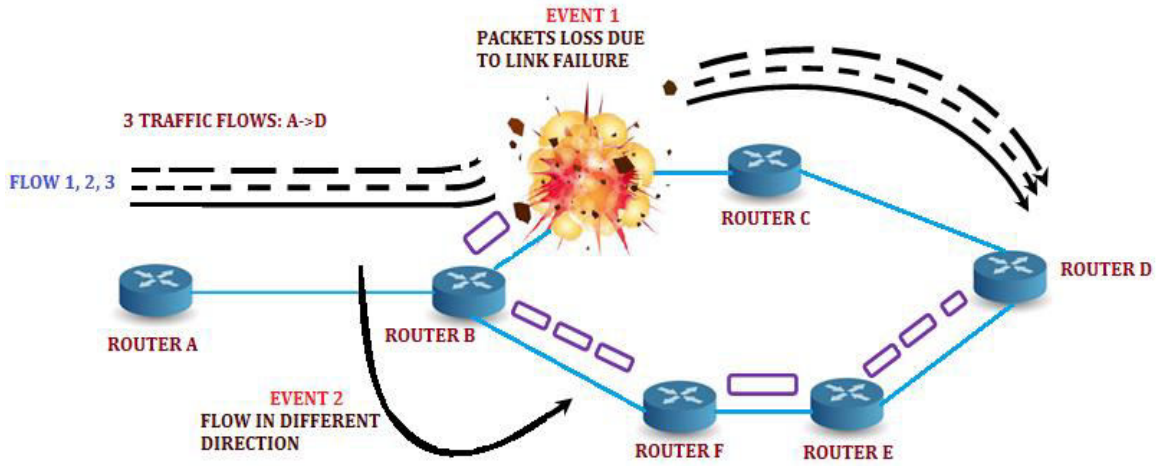



**Figure-11.** Packet collision & paves shortest path to reach destination.

**E. Packet reassessment**

A malevolent node amends the whole set of packets that are to be send to the destination and that data is protected from identifying it and alteration is done before sending to the destination end.

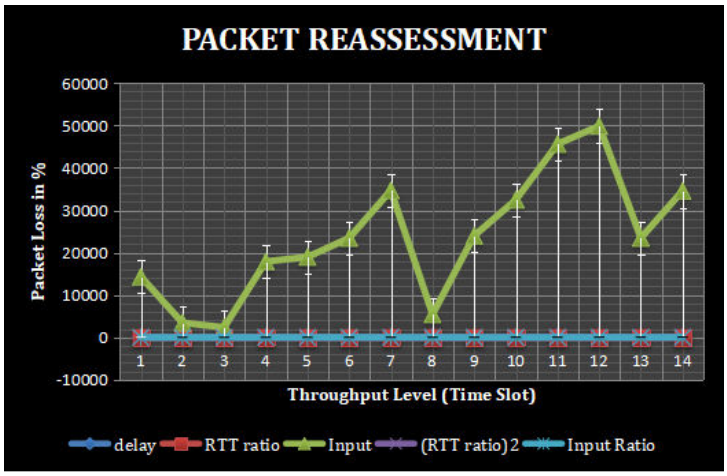



**Figure-12.** A chart to review different kind of packets.

**ALGORITHM**

When packet is send from source to destination, it is not sure that all packets are send completely.

//black hole attack
Initialize pkt = 0;
In packet launch program,
Check the size of a packet and Split the packet
Encrypt each packet parts
Send the packets with obfuscation algorithm
//confuse the hacker
if(pktsnd != pktrec)
Use Heuristics algorithm to discover the fault
pktack = request for pkt again;
Resend the pkt;
exit
else
Receive the ack;
Check with pktsender and receiver
exit
Send next set of packets with security measures
//gray hole attack

Initialize pkt = 0;

In packet launch program,

Check the size of a packet and Split the packet randomly

Encrypt each packet parts randomly

Combine two set of packets with its parts

Send the packets with obfuscation algorithm by sending the packets randomly in different time period

//confuse the hacker

if(pktsnd in different 't' seconds != pktrec in a fixed time)

Use Heuristics algorithm to discover the fault

//checks with time period and in every 'n' packets

pktack = request for pkt again based on 't' seconds and 'n' pkts;

Resend the pkt;

exit

else

Receive the ack;

Check with sourcepkt and destinationpkt

exit

repeat the whole procedure

Send next set of packets with security measures

Exit

## SECURITY MEASURES

There are two important measures as mentioned before through which packet dropping can be avoided. Two algorithms play a vital role in the recovery and sending the packets in proper manner. These are obfuscation and heuristics algorithm which are used as security measures in transmitting packets to the destination. The following are the overall process where measures are used for transmitting packets.

**Steps:**

1. Find out the network path
2. Initialize a variable to assign the packet to be sent
3. Create duplicates along with the original packets
4. Secure the packets using obfuscation algorithm which helps in confusing
5. Wrap with the packet with more security measures.
6. If traffic occurs the network path is changed and send to different secured way
7. Send duplicate packets via the traffic path so that an intruder gets confused.
8. If the receiver == senders message, separate original with duplicates, save the content and repeat the process until all packets are reached.
9. If mismatches then previous packets are deleted and resend it

**Packet send**

To send packets from one place to another it is mandatory to secure from misleading, for which obfuscation and heuristics algorithm are utilized. Obfuscation algorithm is used to confuse the third parties and to veil the content from them. Using this it is also possible to reverse the content and do the process of transmission.

Heuristics Algorithm is used to send the packets in very short path, so that the chances of packet loss are less. First it will discover different paths to traverse and using heuristics it is calculated with values and bandwidth. It is probable to find the solution and the solution found is an acceptable one. Requests get changed dramatically minute by minute or hourly wise. For choice based decision, this algorithm is used.

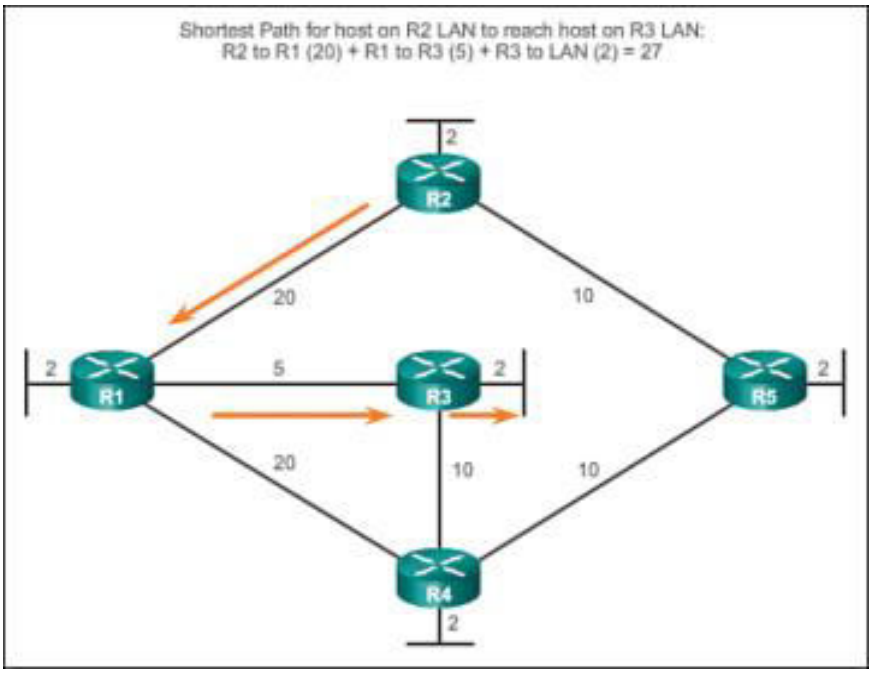



**Figure-13.** Sample diagram for shortest path identification.

**Dispatcher algorithm for n packets**

1. Input the content to the Packet with header and footer to dispatch.
   INPUT: SUM_PKT (k) of Packet n, Transmission Hdr+Ftr
2. Content are secured using obfuscation algorithm by reversing the recipient address and content
   OUTPUT: SCH_PKT (k), Reverse Hdr + Ftr
   SEND
3. PROCEDURE:

i. function SCH_PKT (k)
ii. Partition_Schedule (SUM (k dup) + SUM (k orig))
iii. Initialize (SCH_PKT(k))
iv. Node i = Wrap + Encrypt // using obfuscation algorithm
v. i = GetNeighbor (m)
vi. for each member i of SUM_PKT
vii. Compute _eval(i)
viii. end for
ix. trajectoryu = BuildTrajectory (eval of each NIC Vector)
x. if (send_pkt == SUM_PKT)
xi. Fetch the Content
xii. Transmit for ACK
xiii. for each packet p of m
xiv. Find shortest path SP1 → SP5 // using heuristics algorithm
xv. Hit = random (trajectoryu)
xvi. Update (SCH_PKT)
xvii. end for
xviii. end function

**Recipient algorithm for packet acknowledgement**

4. Initialize Ack_Number = SUM_PKT
5. SNDDATA < minimum size of SCH_PKT
6. Slow down Latency level significantly
7. If (BW value <= value of the starter)
8. Then
9. Requisition of packets resend
10. Else
11. Clogging Avoidance
12. If traffic, Shortest Path to Dispatcher // using heuristics algorithm
13. If (Pkt_Rec = Pkt_Snd)
14. Then
15. Accept it
16. Else
17. Request for Ack
18. Resend the PKT
19. Check for the duplicates
20. If dup_pkt(k)
21. Then
22. Split (orig(k) and Dup(k))
23. Else
24. Request for wrapping to send//using obfuscation algorithm

**Retransmission of lost packets**

1. If BW == Latency == Pkt_Loss
2. Then
3. Count No of Pkt_Loss
4. Combine Entire Pkt_Loss
5. Wrap it and resend again
6. If(Max_Loss) == (SUM_PKT)
7. Then
   Node i(p) SCH_PKT
8. Else
   SND_RECR_END
9. Chk_Content == Base_Content
   Update the catalog
10. Generate Report

## RESULTS AND DISCUSSIONS

In network virtualization, many packets misbehave and are dropped due to many reasons. Here initially it is wrapped and protected perfectly using obfuscation algorithm and sent to the destination. If there is any problem in the path are identified and these packets are send in different path to reach the destination on or before time. The attacks like black hole, gray hole or cooperative black hole or cooperative gray hole are tackled with heuristics and obfuscation algorithm.

Due to any fault in hardware, software or any cables or devices, dropping of packets exists which are dealt easily in this paper. Heuristics is the best problem solving technique through which the packets are sent more quickly than before. Intruders or third parties are not able to identify the packets to fetch because obfuscation algorithm confuses and generates a duplicate set of information wrapped same as original are sent. The original is send by protecting it, encrypting it and by appending header and footer. These deals with bandwidth, low latency, congestion factor, packet size, packet total length and its value.

## CONCLUSIONS

Packet loss occurs due to network congestion and many other factors. This paper deals with low latency level, end to end delay variance and high level throughput to recover the packets and resend it. Prospects of successful transmission are enhanced using the recovery methods. Packets collision, dropping and other caused are maintained at its finest level in a period of time. Bungling connections with exemption problems, wavering in the congestion porthole are eradicated using obfuscation algorithm but high level utilization is maintained less in delays are identified.

End to end approach deals with error free congestion structure with more evaluation of packets and exists to increase the performance over wireless networks. Due to obfuscation and heuristic algorithms, packet drop, misleading the packets are reduced which leads to successive transmissions. The network thus befalls into more efficient, well-organized, and competent with a comparatively optimized productivity.

## REFERENCES

[1] Ira Nath and Dr. Rituparna Chaki. 2012. BHAPSC: A New Black Hole Attack Prevention System in Clustered MANET. International Journal of Advanced Research in Computer Science and Software Engineering. 2(8), ISSN: 2277 128X, pp. 113-121.

[2] Reshmi S and M. Anand Kumar. 2016. Survey on Identifying Packet Misbehavior in Network Virtualization. Indian Journal of Science and Technology, INDJST & ISSN (Online): 0974-5645, 9(31): 1-11.

[3] Reshmi S and M. Anand Kumar. 2016. Secured Structural Design for Software Defined Data Center Networks. International Journal of Computer Science and Mobile Computing, IJCSMC & ISSN 2320-088X, Impact Factor: 5.258, 5(6): 532-537

[4] M. Anand Kumar, Dr. S. Karthikeyan. 2011. Security Model for TCP/IP Protocol Suite. Journal of Advances in Information Technology. 2(2): 87-91.

[5] M. Anand Kumar and Dr. S. Karthikeyan. 2012. Investigating the Efficiency of Blowfish and Rejindael (AES) Algorithms. International Journal of Computer Network and Information Security. 4(2): 22-28

[6] M. Anand Kumar and Dr. S. Karthikeyan. 2012. A New 512 Bit Cipher - SF Block Cipher. International. Journal of Computer Network and Information Security. 4(11): 55-61.

[7] Dr. M. Anand Kumar.and Dr. S. Karthikeyan. 2013. An Enhanced Security for TCP/IP Protocol Suite. International Journal of Computer Science and Mobile Computing. 2(11): 331-338.

[8] Rajendra Aaseri, Pankaj Choudhary, and Nirmal Roberts. 2013. Trust Value Algorithm: A Secure Approach against Packet Drop Attack in Wireless Ad-Hoc Networks. International Journal of Network Security & Its Applications (IJNSA). 5(3).

[9] Nishu Kalia, Harpreet Sharma, and Nishu Kalia. 2016. Detection of Multiple Black hole nodes attack in MANET by modifying AODV protocol. International Journal on Computer Science and Engineering (IJCSE), ISSN: 0975-3397, 8(5): 160-174.

[10] Manar Jammala, Taranpreet Singh, Abdallah Shami, Rasool Asal, Yiming Li. 2014. Software-Defined Networking: State of the Art and Research Challenges. Elsevier's Journal of Computer Networks. 72(1), Doi no: 10.1016/j.comnet.2014.07.004.

[11] Munoz-Arcentales Jose, Zambrano-Vite Sara, Marin-Garcia Ignacio. 2013. Virtual Desktop Deployment in Middle Education and Community Centers Using Low-Cost Hardware. International Journal of Information and Education Technology. 3(6), Doi no: 10.7763/IJIET.2013.V3.355.

[12] Mohamed Ali Kaafar, Laurent Mathy, Thierry Turletti, Walid Dabbous. 2006. Real attacks on virtual networks: Vivaldi out of tune. In Proceedings of the SIGCOMM workshop on Large Scale Attack Defense LSAD. 1(1), Doi no: 10.1145/1162666.1162672.

[13] A. J. Younge, R. Henschel, J. T. Brown, G. von Laszewski. 2011. Analysis of Virtualization Technologies for High Performance Computing Environments. Cloud Computing (CLOUD), 2011 IEEE International Conference. 1(1), Doi no: 10.1109/CLOUD.2011.29.

[14] Ali Dorri and Hamed Nikde. 2015. A new approach for detecting and eliminating cooperative black hole nodes in MANET. Information and Knowledge Technology (IKT), 7th Conference on IEEE.

[15] Pooja and Chauhan. R. K. 2015. An assessment based approach to detect black hole attack in MANET. Computing, Communication & Automation (ICCCA), 2015 International Conference on. IEEE.

[16] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, Yoshiaki Nemoto. 2007. Detecting Black hole Attack on AODV based Mobile Ad hoc networks by Dynamic Learning Method. International Journal of Network Security. 5(3), Doi no: 10.1.1.183.2047.

[17] Anand A. Aware and Kiran Bhandari. 2014. Prevention of Black hole Attack on AODV in MANET using hash function. Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), 3rd International Conference on IEEE.

[18] Kriti Patidar and Vandana Dubey. 2014. Modification in routing mechanism of AODV for defending black hole and worm hole attacks. IT in Business, Industry

and Government (CSIBIG), 2014 Conference on IEEE.

[19] Vishvas Kshirsagar, Ashok M. Kanthe, and Dina Simunic. 2014. Analytical approach towards packet drop attacks in mobile ad-hoc networks. Computational Intelligence and Computing Research (ICCIC), 2014 IEEE International Conference on IEEE.

[20] N. M. Mosharaf Kabir Chowdhury, Raouf Boutaba. 2009. Network Virtualization: State of the Art and Research Challenges. Communications Magazine, IEEE. 47(7), Doi no: 10.1109/MCOM.2009.5183468.

[21] Ayesha Siddiqua, Kotari Sridevi, and Arshad Ahmad Khan Mohammed. 2015. Preventing black hole attacks in MANETs using secure knowledge algorithm", Signal Processing and Communication Engineering Systems (SPACES), 2015 International Conference on IEEE.

[22] Harsh Pratap Singh and Rashmi Singh. 2014. A mechanism for discovery and prevention of cooperative black hole attack in mobile ad-hoc network using AODV protocol. Electronics and Communication Systems (ICECS), 2014 International Conference on IEEE.

[23] Imtithal A. Saeed, Ali Selamat, Ali M. A. Abuagoub. 2013. A Survey on Malware and Malware Detection Systems. International Journal of Computer Applications. 67(16), Doi no: 10.5120/11480-7108.

[24] Gundeep Singh Bindra, Ashish Kapoor, Ashish Narang and Arjun Agrawal. 2012. Detection and Removal of Co-operative Black hole and Gray hole Attacks in MANETs. IEEE International Conference on System Engineering and Technology.

[25] Radhika Saini, Manju Khari. 2011. Defining Malicious Behavior of a Node and its Defensive Methods in Ad Hoc Network. International Journal of Computer Applications. Doi no: 10.5120/2422-3251.

[26] Rekha Kaushik, Jyoti Singhai. 2011. Detection And Isolation of Reluctant Nodes Using Reputation Based Scheme in an Ad-Hoc Network. International Journal of Computer Networks & Communications. 3(2), Doi no: 10.5121/ijcnc.2011.3207.

[27] Singh HP, Singh VP, Singh R. 2013. Cooperative blackhole/ grayhole attack detection and prevention in mobile ad hoc network: A review. International Journal of Computer Applications. 64(3). DOI: 10.5120/10613-5330.

[28] Hongmei Deng, Wei Li, Dharma P. Agrawal. 2002. Routing Security in Wireless Ad Hoc Network. IEEE Communications Magazine. 40(10), Doi no: 10.1109/MCOM.2002.1039859.

[29] Mohammad Al-Shurman, Seong-Moo Yoo, Seungjin Park. 2004. Black hole attack in mobile ad hoc networks. Proceedings of the 42nd annual southeast regional conference, ACM. Doi no: 10.1145/986537.986560.

[30] Mojtaba Alizadeh, Wan Haslina Hassan, Mazleena Salleh, Mazdak Zamani, Eghbal Ghazi Zadeh. 2013. Implementation and Evaluation of Lightweight Encryption Algorithms Suitable for RFID. Journal of Next Generation Information Technology. 4(1), Doi no: 10.4156/jnit.vol4.issue1.9.