DOI: http://dx.doi.org/10.26483/ijarcs.v8i8.4651

ISSN No. 0976-5697

Volume 8, No. 8, September-October 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A REVIEW ON OBFUSCATION AND HEURISTICS ALGORITHM IN NETWORK VIRTUALIZATION

Reshmi. S
Research Scholar, Department of Computer Science,
Karpagam University, Karpagam Academy of Higher Education,
Coimbatore, Tamil Nadu, India,

Dr. M. Anand Kumar
Associate Professor, Department of Information Technology,
Karpagam University, Karpagam Academy of Higher Education,
Coimbatore, Tamil Nadu, India,

Abstract: This paper examines and reviews the Obfuscation and Heuristics algorithm in Network Virtualization to protect the packets against unwanted modifications. These two algorithms are mainly focused to eliminate two major attacks say black hole attack and gray hole attack in the network virtualization. These attacks stop the packets in the focal point to reach the destination, which will not intimate the source about the arrival of content in the destination. The Obfuscation and Heuristics Algorithms helps in investigating mislaid packets in network while transmitting to end users. Obfuscation algorithm makes code harder to analyze which added to protect against malicious modifications of a program. Heuristic algorithm is a technique designed for faster recovery. Based on the speed of packet transfer from source to destination this is achieved to eliminate those attacks.

Keywords: network virtualization; black hole attack; heuristics algorithm; obfuscation algorithm; gray hole attack; packet recovery; packet acknowledge.

I. INTRODUCTION

Virtualization is an act of creating a virtual thing. It gives the figment of your imagination of efficiently running various self-regulating computers known as “virtual machines” [1]. Network Virtualization is the amalgamation of hardware and software resources. Software developers use network virtualization to test the software for development in simulation of network environment to operate it. It used to split up the bandwidth into conduit each of which is independent and secured. It is also used to admittance all resources on the network in a system [2]. It is used to perk up the productivity, efficiency and time consuming. Storage spaces can be communal or re-owed, new drives can be easily supplemented or reassigned [3].

II. PACKET LOSS

A packet is a piece of information which when needed is sent to the destination. For example, in network if a person request for any links it will be sent via packets from source node and reconstructed in the destination end [3]. Packet loss occurs when more number of packets is misled or dropped while traveling from one end to another and is measured as percentage. This happens due to network clogging. When substance disembarks for a persistent stage at a router or network fragment at a velocity greater than it is send through, then there is no other alternative than packet plunge [4][1].

Due to flawed networking hardware, drivers etc., packet loss occurs or packets get corrupted many times while transmitting. Because of packet loss throughput is reduced accidentally due to failure in networks or intentionally to balance bandwidth flanked by various dispatcher when competency is reached utmost [5] [1]. For consistent liberation, extra time is needed for retransmission. For retransmission of packets latency decides the accuracy of packets in both ends. If there is no retransmission, lower latency occurs and high latency occurs for retransmitted packets. Receiver sends the acknowledgement to the sender about the packets they receive and comparison is done to find out dropped packets [6].

In the below Figure 1, a piece of information is sent from PC2 to PC5 via switches and routers. Here, for example, when information is transmitted from PC2 to PC5, it goes via switch1 and router1 to router2 and switch2. If there is no proper Ethernet connection between PCs then the packets are not transmitted. And even if intruders interpret the path then also the packets won’t reach the destination fully and even on time.

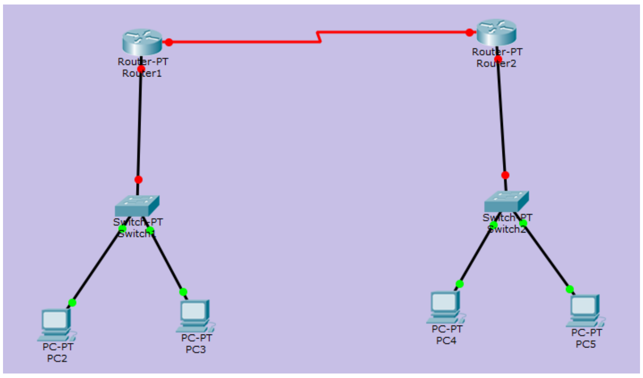
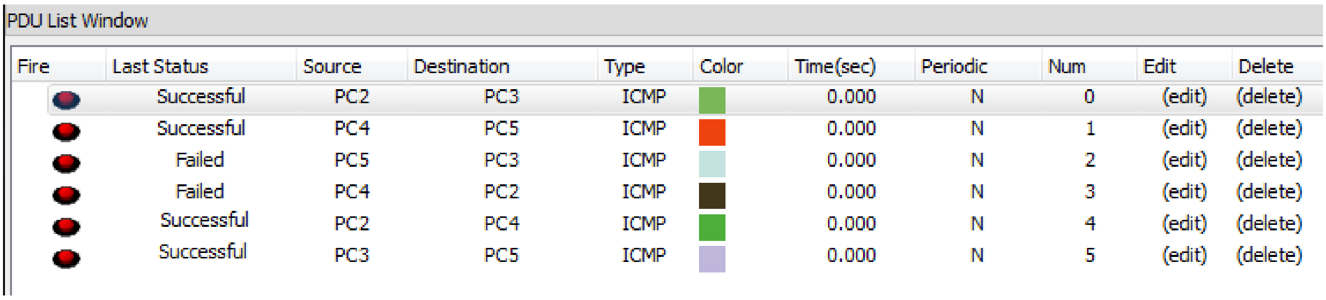


Figure 1. Architecture diagram of Packet transmission in networks

When a packet or information is sent from one PC to another status varies because of congestion, the following PDU (Protocol Data Unit) list window shows the status of the packet transmission.

Table I. PDU List Window



PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	PC2	PC3	ICMP	🟩	0.000	N	0	(edit)	(delete)
●	Successful	PC4	PC5	ICMP	🟥	0.000	N	1	(edit)	(delete)
●	Failed	PC5	PC3	ICMP	🟦	0.000	N	2	(edit)	(delete)
●	Failed	PC4	PC2	ICMP	🟫	0.000	N	3	(edit)	(delete)
●	Successful	PC2	PC4	ICMP	🟩	0.000	N	4	(edit)	(delete)
●	Successful	PC3	PC5	ICMP	🟪	0.000	N	5	(edit)	(delete)

There are two main ways to help reduce the effect of packet loss due to network clogging:

- Increase the bandwidth of the heaving link(s).
- Implement Quality in service which gives precedence in the traffic period.

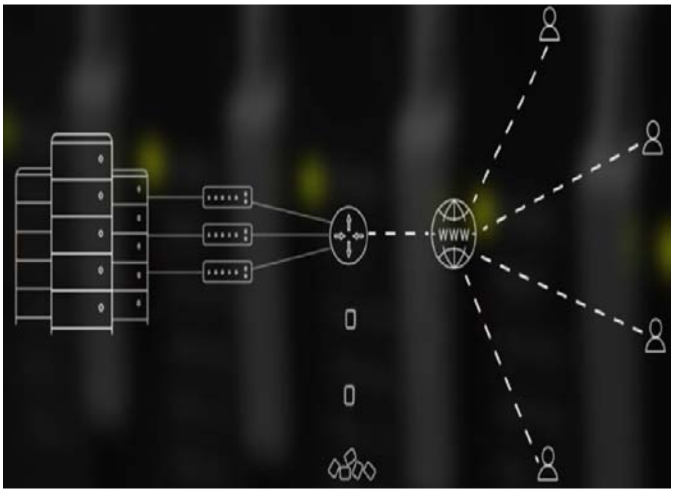


Figure 2. Diagram for Packet Loss Issue in network virtualization

Rather than tangible objects, the chime is used to send special packets of information and lingers for its response back. This is a packet that does not reach the destination properly, and in case of packet loss more time is consumed to resend it. Jitter is concept in which the difference between the minimum and maximum latency results of a chime test. [7]. It is handy to see how speckled the latency results are so that network permanence can be determined. Usually, jitter should be lower than 25 milliseconds.

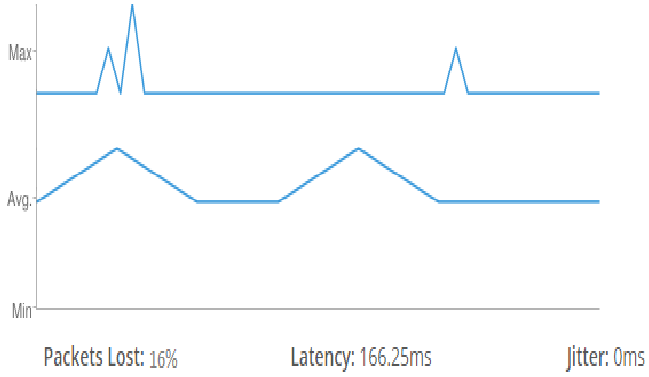


Figure 3.A chart representation for Packet Loss with latency and jitter

Latency describes the time taken to transfer a packet from one place to another. Ideal latency is zero whereas average latency is around 100 milliseconds. There are few reasons of losing packets like high memory usage, too lofty to develop, mammoth passage, flawed pattern amendment [8].

III. SECURITY MEASURES

There are few attacks for packet misbehavior say black hole attack, gray hole attack. All these attacks deal with the packet loss so to recover this there are few methods and algorithms [9][3].

A. Packet Recovery

For packet loss recovery, original data packages are used along with the duplicates which are not necessary and are paired that are one original and another surplus one [10] [5]. A new optimized accurate method called heuristic algorithm is designed using some tricky methods to pair and mismatch the packets to send and recovered using shortest path tricks [11] [10] [9]. Some duplicate packets are added and probabilities of successful recovery of original packages are done.

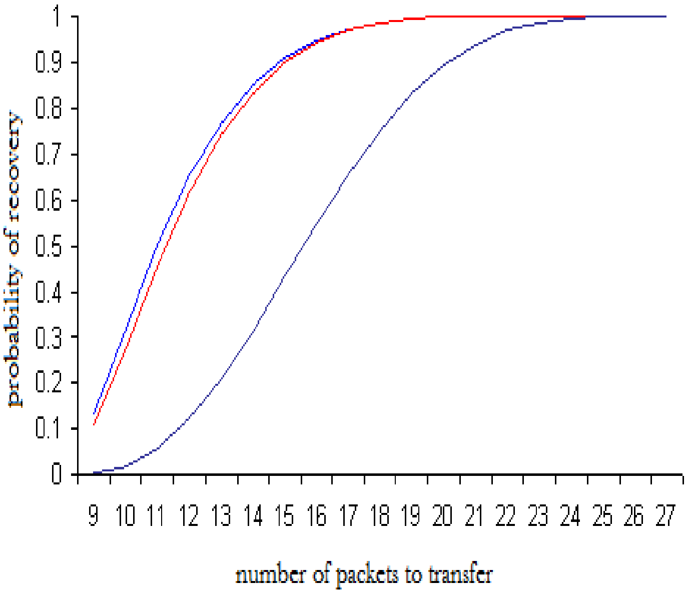


Figure 4. A chart for Packet Recovery

Steps:

1. Initialize a variable say ‘h’, randomly select the packet with duplicates.
2. Let the loop execute from 1 to k and check the condition with (k<n).
3. With the current package, find the nearest place incrementing by 1.
4. Combine the duplicates with the original packets and send it to the destination.
5. If the receiver == senders message, split original and duplicate, save the content and repeat the process until all packets are reached.
6. Sort all the procedure in the destination and calculate the total number of packets.

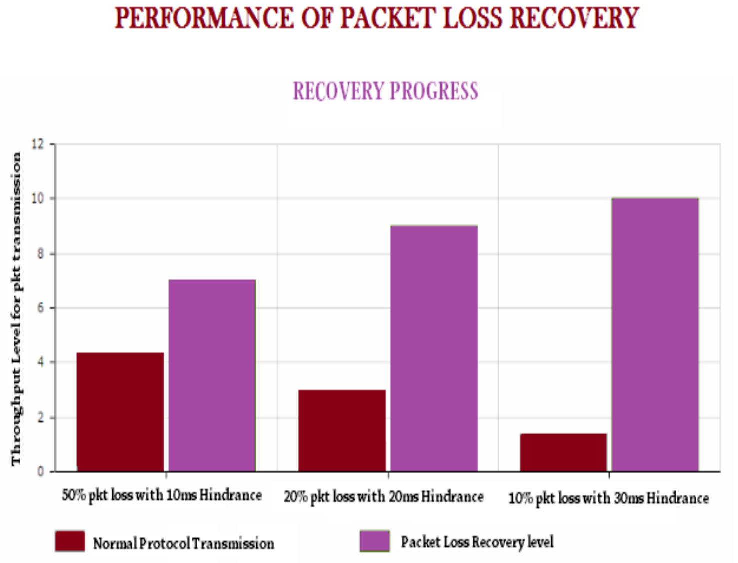


Figure 5. A chart to represent progress in recovery

B. Packet Acknowledgement

After the packets are received in the destination it is must to intimate the sender about the content. If any packets are not matching then retransmission happens [12] [11]. So here acknowledgement plays the vital role.

Steps:

1. Time is set and numbers of packets are calculated before transmitting.
2. Receiver requests for the packets from the sender
3. Sender sends the packet one by one with duplicate copies
4. Acknowledgement is sent by the receiver about the received packets and requests for the next set of packets
5. If packet loss or mismatches, receivers’ requests for the retransmission of packets to the sender.

For sender and receiver side algorithm a special type of algorithm called obfuscation algorithm is implemented to hide the content. Obfuscation algorithm is a process of making the algorithm or the concept difficult which will not be understood by the intruders. It is the concept of reversing, through which one can hide the coding without others being easily understand.

1) Sender Side Algorithm:

a) Sender sends the packets sequentially, so initially sequence number is 0 and maximum sequence value is total packets(N) – 1

```
SEQNUM = 0
SEQMAX = N – 1
```

b) Repeat the steps from c) to e)

c) If the request number is greater than initial sequence number then maximum sequence number is reduced by initial value and appended with the requesting number and requesting number is incremented and equated to the initial sequence number

```
If (REQNUM > SEQNUM)
Then
SEQMAX = REQNUM + (SEQMAX – SEQNUM)
REQNUM++
SEQNUM = REQNUM
```

d) If no transaction happens then transmit packets in sequential order

```
SEQNUM <= SEQMAX
Then
    Sort and Send in Order
```

e) This entire process is reversed by implementing obfuscation algorithm to confuse the intruders.

2) Receiver Side Algorithm:

a) Initialize Request Number by 0 say REQNUM = 0

b) Check whether the sending window is minimum so that the sender can send packets carefully

```
SNDWND < minimum size of window
```

c) Slow down the threshold level drastically

```
If (TH value <= value of the starter)
Then
    Slowly send the packets
Else
    Congestion Evasion
```

d) If the packet received is equal to the request number then accept the packet and request for next set of packets or else reject it.

```
If (Pkt Rec = REQNUM)
Then
    Accept it
    REQNUM ++
Else
    Ignore it
```

e) Send again the request number to the sender requesting for other packets

f) If the content holds the highest value then the packets are sent to the destination and acknowledgement is received.

```
If ((MaxValueSent <= 0) && (MaxValueAck <= 0))
    Packets are sent
    Acknowledgement received
```

g) Count the number of duplicates received and send via acknowledgement

```
NumofDups <= 0
```

3) Retransmission of Packets

a) If threshold value is less than the starting value then retransmission occurs

```
If (TH < Start Value / 3)
Then
          Retransmit SndPackets ()
```

b) Send Packets function deals with full sized packets with duplicates for protection
c) Get Initial Sequence Number and its size
d) If final sequence value is less than the initial one the append the size with this

```
If (FinalSeqNum < = IntSeqNum)
Then
          IntSeqNum = IntSeqNum + Size
          Size = Size – 1
Else
          IntSeqNum = IntSeqNum + MaxSizedPkt
```

e) Finally check whether the content matches by both ends with the help of MaxSent and FinalSeqNum.

IV. RESULTS AND DISCUSSIONS

In network virtualization, it is hard to notice and thwart packets that are being dropped. This work deals with few attacks say black hole in which packets drops in the middle path before reaching the target. In case of dropping packets, gray hole attack differs from black hole attack [13] [14] [9]. Black hole attack drips entire packets while gray hole attack beads only fraction of packets, that is router can accomplish the attack selectively. Dropping packets for a network destination is done by selecting every *n* packet or in calculating seconds as *t* or selecting packets in random order and are dropped or discarded going to the destination known as gray hole attack [15] [9]. By the malevolent bustle, the overall routine gets corrupted.

Cooperative Gray hole attack edifices a group to cooperate and achieves this attack. Gray hole itself cannot be identified easily as it toggles its behavior between nodes that are normal and malicious and if cluster of these malicious nodes joins together to perform an attack then the situation is worst [16] [17] [12].

To tackle these four attacks, there are two algorithms namely, Heuristics Algorithm and Obfuscation Algorithm. Heuristics is the problem solving in fastest manner. Through this packet loss recovery are identified in better way. And Obfuscation Algorithm is to confuse the intruder which is embedded in the algorithm [18] [19] [9]. This is implemented while coding. Since it deals with number of packets, the variable length, numeric value and so on are concentrated and processed accordingly [20].

V. CONCLUSION

The security problem of accountability was identified by providing levels of services when Virtual network hosted on third party infrastructures. This required misbehavior detection system which monitors and identifies the misbehavior's forwarded to destination. Through this review packets can be recovered easier. With the help of those algorithms simplest and fastest method is implemented and content are secured by reversing the algorithm that is in the base level itself, so it is hard to identify the content by an intruder.

VI. REFERENCES

[1] Kurose, J. F. & Ross, K. W. (2010). Computer Networking: A Top-Down Approach. New York: Addison-Wesley. P 30.

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

[3] 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.

[4] Radhika Saini, Manju Khari, “Defining Malicious Behavior of a Node and its Defensive Methods in Ad Hoc Network”, International Journal of Computer Applications, 2011 April, 20(4), Doi no: 10.5120/2422-3251.

[5] Reshmi. S, M. Anand Kumar, “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, Vol.5 Issue.6, June- 2016, pg. 532-537.

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

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

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

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

[12] A. J. Younge, R. Henschel, J. T. Brown, G. von Laszewski, “Analysis of Virtualization Technologies for High Performance Computing Environments”, Cloud Computing (CLOUD), 2011 IEEE International

Conference, 2011 July, 1(1), Doi no: 10.1109/CLOUD.2011.29.

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

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

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

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

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

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

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

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