ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(31), DOI: 10.17485/ijst/2016/v9i31/88459, August 2016* ISSN (Online) : 0974-5645

Survey on Identifying Packet Misbehavior in Network Virtualization

S. Reshmi[1*] and M. Anand Kumar[2]

[1]Karpagam University, Coimbatore - 641021, Tamil Nadu, India; reshmismca@gmail
[2]Department of Information Technology, Karpagam University, Coimbatore - 641021, Tamil Nadu, India; anand2kumarm@gmail.com

Abstract

Background/Objectives: The pros in using network virtualization for the users and the resources offers effectual, meticulous, and protected sharing of the networking resources. **Methods/Statistical Analysis:** In network there is a problem of accountability that any malicious router can drop packets that are supposed to impart packets instead of throw-outs. To understand the packet dropping issues in detail this paper recognizes the foremost attacks and to tackle these attacks algorithms are initiated. **Findings:** A concise assessment on two major attacks are dealt in this article: black hole attack and gray hole attack. If there is any malevolent node in the network, the number of data packets is not reaching the destination, since the packets dive in middle path. To overcome these issues, we identify proposed mechanisms against the attacks and improve the network recital in terms of package globule degree. **Applications/Improvements:** Heuristics algorithm and obfuscation algorithm are the algorithms which help in exploring lost packets in network while transmitting to end users.

Keywords: Black Hole Attack, Gray Hole Attack, Heuristics Algorithm, Network Virtualization, Obfuscation Algorithm, Virtual Routing and Forwarding

1. Introduction

Virtualization is one of the important technologies, which acts virtually instead of actually doing something and with the help of this sharing of system resources is done transversely multiple environments[1]. From physical resources the infrastructure service is decoupled where service is operated. It is used to emulate a complete computer system in order to allow a guest OS to be run. There are different types of virtualization in which this paper concentrates on network virtualization. Virtualization makes the work simpler and faster. Virtual Machines run multiple operating systems and applications to share the resources of a single physical computer. We can reduce the desktop management headaches by saving time and energy[2,3].

Virtualization that decouples the physical hardware and software network resources from operating system into a single component is referred to as network virtualization[4]. Bandwidth are excruciated into networks or frequencies to integrate the presented resources in a network, which are individualistically protected[1]. The excruciated networks properties are safeguarded, restricted and regimented to deliver. Virtual network is final artifact of network virtualization[1]. Logical Partitioning has its own resources which helps in partitioning the system in network virtualization. Network tests are solved by this. It helps in reducing the cost of managing a network devices and resources[5].

Within virtualized infrastructure virtual networks are created using Network Virtualization, which tends to support multifaceted requirements. Virtual environment is formed with different virtual networks, which is separated from another network resources[1]. In this case, network virtualization is more helpful by separating the traffic zone, such that other traffic does not mix with other resources while transmitting data to end users[6]. For good and efficient production of the administrator, the

** Author for correspondence*

complications of networks are hidden. Documentations, tactics and pictures are controllable and storage area network is used to store the contents in the server for ubiquitous network access, elasticity, consistency, speed, litheness and security[1,3].

2. Network Virtualization

Network Virtualization has a few security issues. First we need to take a broad view on attacks' stratagems and spot their effects on organized systems[6], which tends to ailment the system by moving the nodes to distant positions and finally detaching the marked nodes[5,7].

Malicious lumps send misleading data in receipt of a request or send manipulated information. The main classes of attacks are described briefly which are carried out by malicious nodes on positioning system behavior:

- Turmoil: Faults in locating nodes, by generating DOS attack[5,8].
- Seclusion: Only one node is targeted which is in the isolated place of network[9]. To accomplish a traffic scrutiny, the target is intimated by partner node and this conducts delay probes sent by the victim[5].
- Repugnance: This intimates the victims that the partaking nodes are resided far place to reduce fascinating[5].

2.1 Security Attacks

The networking device named router forwards a small package to destination. Any malevolent router drops small package or tiny proportion of packages by introducing additional malevolent fatalities[3]. In this paper a study on scrutinizing the attack focused on package crashing are dealt.

2.1.1 Black Hole Attack

One type of Denial of service attack is packet loss or drop or Black hole attack. This is focused on transmitting packages or a packet to the destination but it fails due to congestion. This is very rigid to spot out and thwart. This attack will not intimate the source about the arrival of content in the destination, because this superfluous or throw down the content from both directions[10].

The paper[5], dynamic learning algorithm is used to identify the above attack. An abnormality recognition scheme by reforming the data in systematic stint interludes, which uses an entry point to recognize black hole attacks. After every time interval a value is tallied up. This work recommends a method to recognize the black hole attack is numerical based indiscretion discovery approach, related with the dissimilarities among order numbers of destination for acknowledged response. At

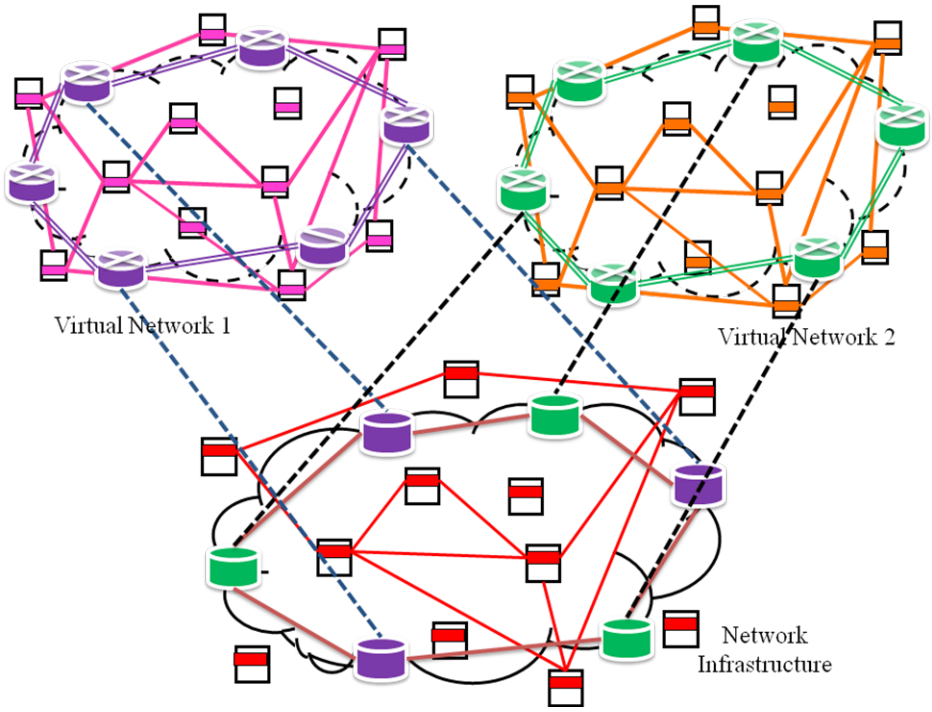

Figure 1. Architecture diagram of virtualization in networks.

a minimal price this attack is found out and this won't require tuning of protocols. And irregularity discovery of nodes is the focal downside.

In paper[11] algorithm to prevent ad hoc networks for black hole attacks. According to them, the response packets are verified with routers. When RREP is sent, the node either on link or on target is considered as malevolent. This method is not useful when collision occurs.

In paper[12], the principle lump transmits a ping packet demanded route to the terminus. The source node buffers RREP (Route Reply) packets until two packets are found. Source nodes identify the best and safest route based on the number of hops and nodes hence forbid the attack. This deals and solves single black hole detection not as a shackle of nodes.

In paper[13], values are documented in two different tables. One is the classification number of last packet sent to every node and the next is the final package established. These tables are reorganized automatically, whenever packet is passed on or established. This is faster since the black hole nodes estimate the traffic passing from its locale and classification of tables are reviewed, which omits the uncovered package.

The work[14], suggests AODV (Ad-hoc On-Demand Distance Vector) decorum to thwart the attacks, the main idea is that source node accepts the second route response instead of first to define a route. Thus, source node discovers a new route with the cost which has malevolent node in the subsequent hop because it does not detect fake RREP packet which is used to attack routing table.

The cluster head attack is not measurable, which affects the entire data. In this attack the attacker becomes the head of huddles, which obtains data from all of its huddle members, combines it and is not accelerated. LEACH protocol is subjugated by the malevolent node to publicize itself as a huddle head to seize packet which drops it randomly. In paper[15] the consequences of gray hole attack are less associated than that of black hole attack.

The work[16] suggests DPRAODV (Detection, Prevention and Reactive AODV) protocol to detect, prevent and react in the existence of black hole attacks. The foremost strategy is to append a section to check reliable of RREP packets into source node i.e., a comparison of the dynamic updated threshold with Source Node value. When the order number is higher than threshold value, then the lump is appended to the black list and the target node is unstated.

In paper[17] black hole detection process is established if the source lump does not receive route request packet which means black hole appears. Source node sends some fake data packages to the terminus lump, meanwhile the packets which are sent are scrutinized by the neighbouring nodes, and if it is lost, they are informed to source. This works for gray holes as it is detected by its neighbouring normal nodes. This technique cannot work for Cooperative Gray holes because the method detects malicious nodes based on the data fetched from the nearby node is the limitation.

In paper[18], the confirmation request and reply are used to evade black hole attacks. The intermediate node sends RREPs and confirmation request to the target lump. After receiving confirmation request, if the intended route is present then CREQ is sent to source. To check for proper route, RREP and CREP are compared for synchronization. One drawback is that black hole is not to be avoided because two nodes will work parallel in collusion, when confirmation response supports incorrect path.

The work[19] anticipated a Black Hole Attack Avoidance Protocol i.e., used for avoiding black hole attack lacking the control over hardware and physical medium of wireless network. To give better path preference, BAAP avoids malicious nodes using authenticity table to form relation disjoint multi-path throughout. Based on the values updated in the authenticity table, non-malicious nodes segregate the black hole nodes and a conduit is created between source and destination to avoid black hole nodes.

To destroy black hole, the paper[20] uses On-Demand Distance Vector (AODV) procedure. A propagation model is a ground radio propagation model where the Wireless channels work. At network layer, the AODV is functioned based on dissimilar system execution measurements, example, parcel transportation degree, standardized navigation overhead normal end to end delay, and bundle conveyance. The AODV directing principle is one that is developed next to the system layer as the directing convention. User Datagram protocol is applied and utilized at the vehicle and transport layer.

In paper[21], a node does not detect every node in the neighbour, but spots the next hop. Here, each node maintains a packet digest buffer in the name of FwdPacketBuffer. There are three concepts: a) Buffer will accept the digest packets when it is forwarded out. b) The accomplishment of the forwarded packet

is eavesdropped and digest are freed. c) The identified node compares the threshold and calculates the earwig rate. The inclusive throughput is measured to scrutinize the performance crashes by the gray hole of the entire network under different number of attackers. In work[50] ant colony optimization is used to detect black hole attack by modifying AODV protocol based on increasing throughput and packet delivery ratio and simultaneously decrease end-to-end delay.

In paper[51], fixed infrastructure has to be created otherwise nodes in the network need to cooperate with each other. In the route malicious nodes are located itself and these nodes are detected using valid and invalid address. In the work[52] to detect malevolent nodes a hash function is used to compute Message Digest which is to protect data transmission and data veracity in AODV by providing ID number. This system more cost effective which overcomes black and gray holes.

2.2.2 Gray Hole Attack

Another category of attack directed to drop portion of packets. The malevolent router selects the attack by dropping packages either in definite time of a day (in every *n* packet or every *t* seconds) or only certain portion is selected capriciously. If all the packets are dropped by the malevolent router that comes, a networking tool called traceroute is used to identify the attack hurriedly[10].

The cluster head attack is not measurable, which affects the entire data. In this attack the attacker becomes the head of huddles, which obtains data from all of its huddle members, combines it and is not accelerated. LEACH protocol is subjugated by the malevolent node to publicize itself as a huddle head to seize packet which drops it randomly. In paper[15] the consequences of gray hole attack are less associated than that of black hole attack.

In work[17] if acknowledgement not received to the source node then black hole is detected. Base lump directs fake data packs to the destination, at the same time as the neighbouring lumps start monitoring movement of the packs, if lost, they are informed to source, hence it is listed as black hole in the network. This works for gray holes as it is detected by its neighbouring normal nodes. This technique cannot work for Cooperative Gray holes because the method detects malicious nodes based on the data fetched from the nearby node is the limitation.

In paper[21], a node does not detect every node in the neighbor, but spots the next hop which is based on sequence structure. Here, each node maintains a packet digest buffer in the name of FwdPacketBuffer. There are three concepts: a) Buffer will accept the digest packets when it is forwarded out. b) The accomplishment of the forwarded packet is eavesdropped and digest are freed. c) The identified node compares the threshold and calculates the earwig rate. The inclusive throughput is measured to scrutinize the performance crashes by the gray hole of the entire network under different number of attackers.

In paper[22], the evaluated procedure is a) Package Distribution Ratio (PDR) is used to set a secure path between two ends by isolating gray and black hole attacks b) Replicate Gray hole attack using Ad-hoc procedure c) Judge against the fallouts of ad-hoc procedures d) The new proposed efficient security technique is AODV protocol's gray hole attack.

In paper[23], an algorithm is proposed to eliminate the nodes with higher sequence number and it is entered in the blacklist which is helpful in detecting gray hole. The peak value is calculated and packet order number is checked. To detect, the following is done: a) Order value for routing board. b) Order value for package reply. c) Elapsed stint of ad hoc network d) Total number of packets received e) Reply Forward Ratio (RFR).

In work[24], a malicious node is isolated and a notification about malevolent is given to all nodes in the network. This notification comprises of following procedures: a) Information gathering from neighborhood, b) Recognizing indigenous irregularity, c) Accommodating incongruity discovery, d) Total fright raiser. Here, the Gray holes are identified with the help of neighbouring nodes. This mechanism does not work if the neighbouring nodes collude to perform Gray hole attack and there is no refuge for delivery of packs.

In the paper[25], three related algorithms are proposed to detect gray hole attack. 1) Proof algorithm creation – a signature algorithm related to proof is generated by each node, 2) Checkup algorithm – Whenever packet dropping attack has happened, this algorithm is invoked to spot the node is malevolent or not, 3) Verdict algorithm – the malevolent node is sketched, based on the information given.

In paper[26], the neighbouring node enquires about the assumed node in package apprise structure. The two constraints in network are throughput and delay, where throughput decreases and delay increases. By this approach, throughput has recovered more. The nodes which are malevolent are disseminated over the network

layer where eradication takes place. Dissemination is also done where lots of resources are wasted for communicating, but here uni-casting is used to save it and those malevolent nodes are identified through biased multicasting process.

In the work[27], a trace gray algorithm was presented to detect gray hole attack, which is based on agent based approach. In spite of all source route availability, the incorrect positives are evaded by the hop node. Mobile Mediator is used to append the code size with regulator. Based on the mobile data and code, a break period is assigned and how large the timeout hiatus is verified. In each destination, a timeout phase is set and if mobile agent doesn't reach there then gray hole occurs.

In paper[28], to avoid the presence of gray hole attack, the proposed protocols of AODV and DSR routing are modified to evade the existence of gray hole attack. These types of AODV protocol are rheostat packages, say request, reply and error packets in route. The trust value is calculated for these packets independently. DSR is a non-cryptographic technique, which uses IDS nodes for the gray-hole detection. The limitations in this are if IDS nodes do not cover the whole network, which includes suspected nodes, then discovery and isolation of gray hole nodes may not be possible.

On Synchronous data[29], to detect gray hole attack uses variance in adjournment formerly and subsequently packet drop. Packet drop can occur when there is congestion and one cannot judge that packet drop in a network is due to malicious activity. So the difference in delay before and after is calculated and the cause for packet loss is recognized. In the work[52] to detect malevolent nodes a hash function is used to compute Message Digest which is to protect data transmission and data veracity in AODV by providing ID number. This system more cost effective which overcomes black and gray holes.

2.1.3 Cooperative black Hole Attack

A shackle of malevolent nodes is termed as cooperative black hole attack[12]. A black hole erroneously replies the requests to the terminus and crashes wholly receiving packs. Damage in the entire network happens hardly when malevolent lumps work as a set simultaneously, referred to as cooperative black hole attack[30,49]. This attack occurs when several malevolent nodes cooperate to each other in order to absorb data packets. This attack is more hazardous because malicious nodes which are nearby are collected together to form a group and is collaborated to get away from the detection process[31].

In this work[30], in search of target node and IP, a node makes a transmission of request. The route responses are send by the black or gray holes for the corresponding requests. If any of the routes responds similar to restricted IP, a discovery pattern is originated for these malevolent nodes. The backbone node receives the transmitted message. These transmitted message selects one of permitted IP addresses which sends acknowledgement to the Back Bone nodes. This message selects free IP address randomly. The neighbours are alerted by the source node for the response. It sends fake packets to the targeted place, at the same time the neighboring nodes starts monitoring the package which drifts to the next hop. The information about the replying node is informed to source node when dummy packet is lost. Depending upon the information received, the SN detects the location of the two attacks.

The work[32], presented an algorithm and it cannot tackle attacks of gray hole because the node is related each other. This paper introduces a table called Data Routing Information Table (DRI). A method is proposed to recognize diverse categories of black hole nodes which work as a collection with ad-hoc procedure. Traverse scrutiny concept is also used to check the upcoming nodes which are malicious or not. Besides owing in the direction of intensive traverse scrutiny, when network is attacked by the attacker, the algorithm takes more time to finalize.

In paper[33], instead of transferring the whole data on one occasion, it is separated into tiny blocks and are send to the destination. The malicious nodes are noticed & removed then and there it occurs to avoid traffic and send data faster to another end. Each node has its own neighbour who takes care of the traffic. The lost data is verified with the help of acknowledgement sent by the destination, which estimates the availability of black hole. However, in this mechanism, this algorithm reports about the misbehaving of the node, when in fact it is not.

In paper[34] an algorithm was proposed which uses Data Routing Information table and traverse scrutiny in AODV routing protocol to modify the information. Route request message of the source node is replied by distinct node; an additional board is preserved. First bit of this board is information on data packet of the routing and another bit "Through" node which delivers the data packet information. Cooperative Black holes are identified with help of reliable nodes and DRI table entries in cross checking list. The results show that packet delivery ratio

is less than 60% and it cannot address Gray hole attacks.

Authors in the paper[35] presented an algorithm that includes concept like calculation on sequence number and cryptographic algorithm RSA to eliminate the cooperative black hole attack. It provides security for transmitting the packets but it includes computational overhead.

The work[36] presented an enhancement by introducing fidelity table. Each node assigns a fidelity level where nodes are measure. An acknowledgement is sent back on receiving data packets to the target place and a fidelity level of the transitional node is increased as well. The malevolent node is identified and secluded, if fidelity level becomes zero. The algorithm has many drawbacks[36]: 1) the fidelity tables for each node are maintained and overhead and processing delay is incremented by exchanging the nodes periodically. 2) Additional overhead and time delays are introduced.

In the work[37], each sturdy node contains normal nodes, which is used to help in finding attacks. These sturdy nodes have the ability to adjust its transmitter between large and short assortments. The sturdy nodes are used to check whether the data packages arrived at the destination if not then it will ask nodes to scrutinize the behavior of data passed. If misbehavior is found while checking, then to detect the two attacks a protocol is introduced to the network. Malicious nodes are publicized to the network via message broadcast.

In paper[38], revealing procedure of the source node for gray and black hole attacks: First segregating the data packets into equal parts, next transmitting the number of messages to the targeted place, then propagating the messages to all neighbors, and after confirming that the targeted node recognizes the number of messages, the source starts sending the data. Destination received the data packets by setting up a timer, which is based on the attacks removed, if data doesn't reach the target place and a boundary is set in the destination where if broadcasted data packages is less than the margin set, then eradicated method is commenced to remove the above two attacks. Revealing procedure by target node of black hole attack: the timer is set to zero if then also the data packets are counted, but even if session expires the data package numbers are sent to source node. Revealing procedure by nearby nodes: To count number of data packs of neighbors, each node starts a poker chip. Eradicate process by source node: source nodes get the intimation about the malevolent nodes via vote and a poker chip is created for each malicious node. If neighbors' votes exceed its limits, a new route to reach the destination is created and this information is stored in the black and gray hole tables. The network gets the information about the malevolent node which is to be omitted. Eradicate procedure by neighboring nodes: malicious nodes send packets which is counted and examined by the source node. If the approved messages are less than the limit, then it is intimated to the base node.

2.1.4 Cooperative Gray Hole Attack

This attack structures a group to cooperate and accomplish this attack. Gray hole itself cannot be identified easily as it toggles its behavior between nodes that is normal and malicious and if cluster of collude is to perform an attack then the situation is worst[31].

In this work[30], in search of target node and IP, a node makes a transmission of request. The route responses are send by the black or gray holes for the corresponding requests. If any of the routes responds similar to restricted IP, a discovery pattern is originated for these malevolent nodes. The backbone node receives the transmitted message. These transmitted message selects one of permitted IP addresses which sends acknowledgement to the Back Bone nodes. This message selects free IP address randomly. The neighbors are alerted by the source node for the response. It sends fake packets to the targeted place, at the same time the neighboring nodes starts monitoring the package which drifts to the next hop. The information about the replying node is informed to source node when dummy packet is lost. Depending upon the information received, the SN detects the location of the two attacks.

In paper[33], instead of transferring the whole data on one occasion, it is separated into tiny blocks and are send to the destination. The malicious nodes are noticed & removed then and there it occurs to avoid traffic and send data faster to another end. Each node has its own neighbor who takes care of the traffic. The lost data is verified with the help of acknowledgement sent by the destination, which estimates the availability of black hole. However, in this mechanism, this algorithm reports about the misbehaving of the node, when in fact it is not.

In the work[37], each sturdy node contains normal nodes, which is used to help in finding attacks. These sturdy nodes have the ability to adjust its transmitter between large and short assortments. The sturdy nodes are used to check whether the data packages arrived at the destination if not then it will ask nodes to scrutinize the behavior of data passed. If misbehavior is found while checking, then

to detect the two attacks a protocol is introduced to the network. Malicious nodes are publicized to the network via message broadcast.

In paper[38], revealing procedure of the source node for gray and black hole attacks: First segregating the data packets into equal parts, next transmitting the number of messages to the targeted place, then propagating the messages to all neighbors, and after confirming that the targeted node recognizes the number of messages, the source starts sending the data. Destination received the data packets by setting up a timer, which is based on the attacks removed, if data doesn't reach the target place and a boundary is set in the destination where if broadcasted data packages is less than the margin set, then eradicated method is commenced to remove the above two attacks. Revealing procedure by target node of black hole attack: the timer is set to zero if then also the data packets are counted, but even if session expires the data package numbers are sent to source node. Revealing procedure by nearby nodes: To count number of data packs of neighbors, each node starts a poker chip. Eradicate process by source node: source nodes get the intimation about the malevolent nodes via vote and a poker chip is created for each malicious node. If neighbors' votes exceed its limits, a new route to reach the destination is created and this information is stored in the black and gray hole tables. The network gets the information about the malevolent node which is to be omitted. Eradicate procedure by neighboring nodes: malicious nodes send packets which is counted and examined by the source node. If the approved messages are less than the limit, then it is intimated to the base node.

In paper[39], Credit Based AODV (CBAODV), a new algorithm was proposed by modifying AODV protocol. In this, first every adjacent node accepts the permanent value assigned by each node as the neighbor recognition value. This value increases by the etiquette when it receives request and decreases when it receives response pack. The gray hole attacker is identified, when neighbor disclosures negative recognition value, then gray hole attacker is found out. Current established paths are removed from its steering table which is leaving through that node. Each node assigns a recognition value for every route request and are sent and subtracts the recognition value when a reply is obtained from them. This algorithm is able to identify cooperative gray hole nodes.

2.2 Security Algorithms

The existing system has many methodologies and procedure to solve those attacks. The existing system uses a separate control and data planes in the network. Network virtualization separates the functionalities into network infrastructure, virtual network and end users. The security issues in network virtualization deals with unauthorized network access which controls the traffic attacks and packet forwarding functionality not to be mentioned. To solve these attacks there are a few algorithms, they are:

2.2.1 Heuristics Algorithm

The artificial intelligence optimization in Mathematics is heuristic. It is a technique designed for faster tricky resolving while other methods are laborious. Classic methods flop in judging an estimated solution. This is achieved by optimization, wholeness, accurateness or meticulousness for speed. Heuristics is a problem solving tool which also solves non-routine problems.

Heuristics-based techniques[40] rely on signatures of known attack payloads. If the heuristics pattern matches with the signatures stored in the database, then the antiviral systems or intrusion detection systems are used to scan a network folio and flag for malicious. Unfortunately, attackers can easily evade to detect novel attack vectors heuristics is unsuccessful. More importantly, the rate at which heuristics based system has restructured the signature database is very sluggish than the attackers who overcome the Web.

In work[41] for different type of vehicle delay of LRP (Long Range Planning) is faced, considering its facilities. Location allocation and vehicle routing problems are two categories of LRP. To resolve the LAP (Link Access Protocol) and the VRP (Virtual Routing Protocol), the authors developed some heuristic methods based on the Simulated Annealing (SA) technique. In work[42] Tabu Search (TS) and SA heuristics routines are compared for the quadratic obligation crisis. Simulated Annealing accomplishes better for higher quality boards though TS performs better for lower quality goals, for a number of wide ranges of problem instances.

In paper[43] an extension of the capacitated VRP is considered, in which there are two categories of customers. They are named as Linehaul customers and Backhaul customers and are referred to as routing vehicle problem. The delivery of quantity of product from the warehouse is

required by the linehaul customers and given quantity of the manufactured goods are elated to the warehouse. First a bunch route is created and then heuristics are utilized. These heuristics uses grouping method called travelling salesman problem. Asymmetric cost matrix problem is also used for inter-intra route exchanges.

In paper[44], quadratic assignment problem is used for grouping optimization problem. High quality solutions are found through Meta-heuristic algorithms. To resolve QAP computation time are applied. The authors in this paper[45] Meta-heuristic algorithms are compared based on quality and runtime, where a meaningful result are possible between meta-heuristics algorithms. This will ensure reasonable comparisons in quality and runtime.

2.2.2 Obfuscation Algorithm

A process applied to information to deliberately make it difficult to reverse without knowing the algorithm that was applied is meant to be Obfuscation. An obscured code is created which are not understood by the humans. Here theoreticians renovate legible code into muddied code using numerous methods. Using this algorithm, one can hide the coding without others being able to easily understand.

In paper[46], static heuristic scanning or the white-box approaches are focused. The scanning approach is in the form of hexadecimal targets the malware to detect. This hexadecimal is used to understand the whole structure code and functionality of variety of forms of antagonistic or invasive software. The virus scan is done based on the virus database which stores its signature so that when a portion of malware matches with sample set then the data file is infected. Variety of packer detectors and unpacking section with heuristics scanning engine are incorporated to solve the obfuscated malware problem.

In paper[47], to save the content from the intruders the obfuscation modernizes the original code to muddied form. In spite of that malware records are crammed during runtime which is to be considered initially. Malware can be detected anytime whenever malicious node is loaded. It can be performed during loading either statically or dynamically.

In paper[48], SAVE is used to detect malware. Static Analyzer of Vicious Executables is a malware recognition scheme which creates a vigorous signature. It highlights to detect obfuscated and metamorphose malware. The goal of this system is to create a common hub signature where all sort of malware is rectified by amalgamation of numerous structures of code. The paper[49] proposes an obfuscation-buoyant approach to identify malevolent network content. They use mainly page content related features to evaluate different machine learning algorithms on a sample dataset and the authors account that their classification methods outstripped signature-based tools.

Table 1. Comparison between heuristics and obfuscation algorithms

S. No	Heuristics Algorithm	Obfuscation Algorithm
1.	The word 'heuristic' is taken directly from the Greek verb, heuriskein which means 'to discover'.	Obfuscated means to darken or too obscure or to confuse and to make so confused or opaque as to be difficult to perceive or understand.
2.	Finds solutions among all possible ones. They are considered as approximately not accurate.	Using this algorithm, one can hide the coding without others being able to easily understand.
3.	These algorithms, usually find a solution close to the best one and they find it fast and easily.	A process applied to information to intentionally make it difficult to reverse without knowing the algorithm that was applied.
4.	Heuristics is problem solving tools which also solves non-routine problems.	Programs known as obfuscators transform readable code into obfuscated code using various techniques.
5.	This solution may not be the best of all the actual solutions to this problem, or it may simply approximate the exact solution. But it is still valuable because finding it does not require a prohibitively long time.	An algorithm is to be generated to confuse the third parties. One of the challenges is to produce a compact algorithm using least number of lines.
6.	Heuristics may produce results by themselves, or they may be used in conjunction with optimization algorithms to improve their efficiency	Obfuscation transforms the true purpose of the original program code into a misleading or unreadable form in hopes of hiding the program's true intentions.
7.	With the help of heuristics algorithm virus scanning is also done	The process of hiding original data with random characters, to protect data from the third parties.

2.2.3 Comparison of Heuristics Algorithm and Obfuscation Algorithm

3. 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 network huge amount of content is passed via routers as packets due to which traffic occurs. This type of attack is incorrect forwarding behavior where packets may get lost in the path.

In case of dropping packets gray hole attack differs from black hole attack. Black hole attack drips entire packets while gray hole attack beads only fraction of packets, that is router can have accomplished the attack selectively. Dropping packets for a particular 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. By the malevolent bustle, the overall routine gets corrupted.

A black hole is a malevolent node that fallaciously replies for the request made by the other end. Based on the request unwanted packets are dropped. Cooperative black hole attack is the mishmash of various black hole attacks, which when work together huge damage happens. Single attack is less powerful than this which escapes from the revealing process.

Cooperative Gray hole attack structures a group to cooperate and accomplish 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 join together to perform an attack then the situation is worst[31].

To tackle these four attacks, there are two algorithms namely, Heuristics Algorithm and Obfuscation Algorithm. Heuristics is the problem solving technique. It also solves non-routine harms to fetch accurate result. Heuristics algorithm takes a guess approach to solve the problems. It will not compute the exact values but on input, but close too optimal i.e. it finds exact solution. Obfuscation Algorithm is to confuse and to make intruders confused. It is opaque to be understandable by the third parties. Without knowing the algorithm that was applied, a process is used for information to intentionally make it critical by reversing is referred to as Obfuscation Algorithm. The simple methods to obfuscate are by using shuffle individual bits, by converting modular representation, by representing in variable length numeric system, which produces short arithmetic progressions.

4. 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 packets forwarded to destination. With the help of hypervisor, a virtual network is created in which the heuristic and obfuscation algorithm is implemented to avoid those attacks. The obfuscation algorithm is used to mask the data by encrypting and is used with heuristic algorithm to avoid security issues.

5. References

1. Jammala M, Singh T, Shami A, Asal R, Li Y. Software-defined networking: State of the art and research challenges. Journal of Computer Networks. 2014 Oct; 72(1). DOI: 10.1016/j.comnet.2014.07.004.
2. Jose M-A, Sara Z-V, Ignacio M-G. Virtual desktop deployment in middle education and community centers using low-cost hardware. International Journal of Information and Education Technology. 2013 Dec; 3(6). DOI: 10.7763/IJIET.2013.V3.355.
3. Kaafar MA, Mathy L, Turletti T, Dabbous W. Real attacks on virtual networks: Vivaldi out of tune. Proceedings of the SIGCOMM workshop on Large Scale Attack Defense LSAD. 2006 Sep; 1(1): 139–46. DOI: 10.1145/1162666.1162672.
4. Younge AJ, Henschel R, Brown JT, von Laszewski G. Analysis of virtualization technologies for high performance computing environments. 2011 IEEE International Conference on Cloud Computing (CLOUD). 2011 Jul; 1(1): 9–16. DOI: 10.1109/CLOUD.2011.29.
5. Kurosawa S, Nakayama H, Kato N, Jamalipour A, Nemoto Y. 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: 10.1.1.183.2047.
6. Chowdhury NMMK, Boutaba R. Network virtualization: State of the art and research challenges. Communications Magazine. 2009 Jul; 47(7). DOI: 10.1109/MCOM.2009.5183468.
7. Saeed IA, Selamat A, Abuagoub AMA. A survey on malware and malware detection systems. International Journal of Computer Applications. 2013 Apr; 67(16). DOI: 10.5120/11480-7108.
8. Saini R, Khari M. Defining malicious behavior of a node and its defensive methods in ad hoc network. International Journal of Computer Applications. 2011 Apr; 20(4). DOI:

10.5120/2422-3251.
9. Kaushik R, Singhai J. Detection and isolation of reluctant nodes using reputation based scheme in an ad-hoc network. International Journal of Computer Networks and Communications. 2011 March; 3(2). DOI: 10.5121/ijcnc.2011.3207.
10. Ghoniemy SSA. Performance analysis of mobile ad-hoc network protocols against black hole attacks. International Journal of Computer Vision and Image Processing. 2013 Jun; 3(2). DOI: 10.4018/ijcvip.2013040105.
11. Deng H, Li W, Agrawal DP. Routing security in wireless ad hoc network. Communications Magazine. 2002 Oct; 40(10). DOI: 10.1109/MCOM.2002.1039859.
12. Al-Shurman M, Yoo S-M, Park S. Black hole attack in mobile ad hoc networks. Proceedings of the 42nd Annual Southeast Regional Conference, ACM; 2004 Apr. DOI: 10.1145/986537.986560.
13. Alizadeh M, Wan Haslina H, Salleh M, Zamani M, Zadeh EG. Implementation and evaluation of lightweight encryption algorithms suitable for RFID. Journal of Next Generation Information Technology. 2013 Feb; 4(1). DOI: 10.4156/jnit.vol4.issue1.9.
14. Tseng F-H, Chou L-D, Chao H-C. A survey of black hole attacks in wireless mobile ad hoc networks. Human-centric Computing and Information Sciences. 2011 Nov; 1(4). DOI: 10.1186/2192-1962-1-4.
15. Tripathi M, Gaur MS, Laxmi V. Comparing the impact of black hole and gray hole attack on LEACH in WSN. Procedia Computer Science. 2013 Dec; 19(1). DOI: 10.1016/j.procs.2013.06.155.
16. Sharma A, Singh R, Pandey G. Detection and prevention from black hole attack in AODV protocol for MANET. International Journal of Computer Applications. 2012 Jul; 50(5). DOI: 10.5120/7764-0837.
17. She C, Yi P, Wang J, Yang H. Intrusion detection for black hole and gray hole in MANETs. KSII Transactions on Internet and Information Systems. 2013 Jul; 7(7). DOI: 10.3837/tiis.2013.07.012.
18. Lee S, Han B, Shin M. Robust routing in wireless ad-hoc networks. Proceedings of International conference on Parallel Processing Workshops. 2002 Aug; 18(21). DOI: 10.1109/ICPPW.2002.1039714.
19. Gupta S, Subrat K, Dharmaraja S. BAAP: Black hole Attack Avoidance Protocol for wireless network. International Conference on Computer and Communication Technology, Computer and Communication Technology (ICCCT), 2nd International Conference on IEEE. 2011 Sep; 1(1): 468–73. DOI: 10.1109/ICCCT.2011.6075136.
20. Khin EE, Phyu T. Impact of black hole attack on AODV routing protocol. International Journal of Information Technology, Modeling and Computing. 2014 May; 2(2). DOI: 10.5121/ijitmc.2014.2202.
21. Cai J, Yi P, Chen J, Wang Z, Liu N. An adaptive approach to detecting black and gray hole attacks in ad hoc network. 2010 24th IEEE International Conference on Advanced Information Networking and Applications (AINA). 2010 Apr; 1(1): 775–80. DOI: 10.1109/AINA.2010.143.
22. Arora SK, Monga H. Combined approach for the analysis of black hole and worm hole attack in MANET. Indian Journal of Science and Technology. 2016 May; 9(20). DOI:10.17485/ijst/2016/v9i20/90391.
23. Kanthe AM, Simunic D, Prasad R. A mechanism for gray hole attack detection in mobile ad–hoc networks. International Journal of Computer Applications. 2012 Sep; 53(16). DOI: 10.5120/8507-2511.
24. Sen J, Chandra MG, Harihara SG, Reddy H, Balamuralidhar P. A mechanism for detection of gray hole attack in mobile ad hoc networks. International Conference on Information and Communication Systems. 2007 Dec; 1(1):1–5. DOI: 10.1109/ICICS.2007.4449664.
25. Xiaopeng G, Wei C. A novel gray hole attack detection scheme for mobile ad-hoc networks. International Federation for Information Processing (IFIP) International Conference on Network and Parallel Computing. 2007 Sep; 1(1): 209–14. DOI: 10.1109/NPC.2007.88.
26. Aarti, PR. Prevention and elimination of gray hole attack in mobile ad-hoc networks by enhanced multipath approach. International Journal of Engineering Trends and Technology. 2015 May; 23(5). DOI: 10.14445/22315381/IJETT-V23P242.
27. Taggu A, Taggu A. Trace Gray: An application-layer scheme for intrusion detection in MANET using mobile agents. 2011 Third International Conference on Communication Systems and Networks (COMSNETS). 2011 Jan; 1(1). DOI: 10.1109/COMSNETS.2011.5716475.
28. Mohanapriya M, Krishnamurthi I. Modified DSR protocol for detection and removal of selective black hole attack in MANET. Computers and Electrical Engineering. 2014 Feb; 40(2). DOI: 10.1016/j.compeleceng.2013.06.001.
29. Pal S, Li H, Sikdar B, Chow J. A mechanism for detecting gray hole attacks on synchrophasor data. IEEE International Conference on Communications. 2014 June; 1(1): 4131–36. DOI: 10.1109/ICC.2014.6883968.
30. Vishnu K, Paul AJ. Detection and removal of cooperative black/gray hole attack in mobile ADHOC networks. International Journal of Computer Applications. 2010 Feb; 1(22). DOI: 10.5120/445-679.
31. 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.
32. Ramaswamy S, Fu H, Sreekantaradhya M, Dixon J, Nygard K. Prevention of cooperative black hole attack in wireless ad hoc networks. International Conference on Wireless Networks. 2003 Jun; 1(1). DOI: 10.1.1.84.9717.
33. Banerjee S. Detection/removal of cooperative black and gray hole attack in mobile ad-hoc networks. Proceedings of the World Congress on Engineering and Computer Science 2008. 2008 Oct; 1(1). DOI: 10.5120/445-679.
34. Wahane G, Lonare S. Technique for detection of coopera-

tive black hole attack in MANET. International Conference on Advances in Engineering and Technology. 2014 Jul; 1(1):1–8. DOI: 10.1109/ICCCNT.2013.6726621.
35. Kaur J, Singh T. A secured data transmission method using enhanced proactive secret sharing scheme to prevent blackhole attack in MANETs - A review. International Journal of Computer Applications. 2015 Jun; 119(10). DOI: 10.5120/21104-3827.
36. Tamilselvan L, Sankaranarayanan V. Prevention of co-operative black hole attacks in MANET. Journal of Networks. 2008 May; 3(5). DOI: 10.4304/jnw.3.5.13-20.
37. Agrawal P, Ghosh RK, Das SK. Cooperative black and gray hole attacks in mobile ad hoc networks. Proceedings of the 2nd International Conference on Ubiquitous Information Management and Communication. 2008 Dec; 1(1). DOI: 10.1145/1352793.1352859.
38. Jain S, Jain M, Kandwal H. Advanced algorithm for detection and prevention of cooperative Black and Gray hole attacks in mobile ad hoc networks. International Journal of Computer Applications. 2010; 1(7). DOI: 10.5120/165-290.
39. Lokare DA, Kanthe AM, Simunic D. Cooperative gray hole attack discovery and elimination using credit based technique in MANET. International Journal of Computer Applications. 2014 Feb; 88(15). DOI: 10.5120/15427-3850.
40. Seifert C, Welch I, Komisarczuk P. Identification of malicious web pages with static heuristics. Proceedings of the Australasian Telecommunication Networks and Applications Conference IEEE. 2008 Dec; 47(1). DOI: 10.1109/ATNAC.2008.4783302.
41. Wu TH, Low C, Bai JW. Heuristic solutions to multi-depot location-routing problems. Journal Computers and Operations Research. 2002 Sep; 29(10). DOI: 10.1016/S0305-0548(01)00038-7.
42. Paul G. Comparative performance of Tabu search and simulated annealing heuristics for the quadratic assignment problem. Operations Research Letters Elsevier. 2010 Nov; 38(6). DOI: 10.1016/j.orl.2010.09.009.
43. Toth P, Vigo D. A heuristic algorithm for the symmetric and asymmetric vehicle routing problems with backhauls. European Journal of Operational Research. 1999 Feb; 113(3). DOI: 10.1016/S0377-2217(98)00086-1.
44. Ghandeshtani M, Seyedkashi N. New simulated annealing algorithm for quadratic assignment problem. The Fourth International Conference on Advanced Engineering Computing and Applications in Sciences. 2010 March; 1(1). DOI: 10.1.1.681.4982.
45. Silberholz J, Golden B. Comparison of meta-heuristic, handbook of meta-heuristic algorithms. International Series in operations Research and Management Science. 2010 Sep; 146(1). DOI: 10.1007/978-1-4419-1665-5_21.
46. Wu Y, Chiueh TC, Zhao C. Efficient and automatic instrumentation for packed binaries. Proceedings of the 3rd International Conference and Workshops on Advances in Information Security and Assurance, Springer Berlin Heidelberg. 2009 June;1(1): 307–16. DOI: 10.1007/978-3-642-02617-1_32.
47. Brosch T, Morgenstern M. Runtime packers: The Hidden Problem? Black Hat USA [Internet]. 2006. Available from: http://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Morgenstern.pdf.
48. Sung AH, Xu J, Chavez P, Mukkamala S. Static Analyzer of Vicious Executables (SAVE). Proceedings of the 20th Annual Computer Security Applications Conference 2004, IEEE Computer Society. 2004 Dec; 1(1). DOI: 10.1109/CSAC.2004.37.
49. Yung-Tsung H, Yimeng C, Tsuhan C, Chi-Sung L, Chia-Mei C. Malicious web content detection by machine learning. Expert Systems with Applications. 2010 Jan; 37(1). DOI: 10.1016/j.eswa.2009.05.023.
50. Arora SK, Vijan S, Gaba GS. Detection and analysis of black hole attack using IDS. Indian Journal of Science and Technology. 2016 May; 9(20). DOI: 10.17485/ijst/2016/v9i20/85588.
51. Vangili A, Thangadurai K. Detection of black hole attack in mobile ad-hoc networks using ant colony optimization – simulation analysis. Indian Journal of Science and Technology. 2015 Jul; 8(13). DOI:10.17485/ijst/2015/v8i13/58200.
52. Amiri R, Rafsanjani MK, Khosravi E. Black hole attacks detection by invalid Ip addresses in mobile ad hoc networks. Indian Journal of Science and Technology. 2014 Jan; 7(4). DOI: 10.17485/ijst/2014/v7i4/48626.
53. Hizbullah K, Iqbal UA, Insafullah. A Khattak approach for detection and removal of black and gray hole attacks in MANET. Indian Journal of Science and Technology. 2016 Jan; 9(4). DOI:10.17485/ijst/2016/v9i4/77755.