“VCPHCF-RTT” Estimation in Private Virtual Cloud Infrastructure

Ritu Maheshwari, Anil Rajput, Anil K. Gupta

Abstract: ***For the security of proposed model of Private Virtual Cloud Infrastructure model, Security Agent technique has been designed to fight against IP-Spoofing based DDoS Attacks. Virtualization Enhancement has been done in Cloud using proposed and designed Security Agent VCPHCF-RTT. Performance Parameters have been analysed after introspection to existing cloud security mechanisms and tried to resolve focussed Research Problem, Issues and Challenges. VCPHCF-RTT improves the efficiency of the probabilistic HCF technique using HCF for virtual intermediate nodes between the Virtual Machines of Client VM and Server VM along with RTT. It helps in reducing the probability of guessing the RTT and VCHCF parameter values at the intermediate virtual routers by the attackers. VCPHCF-RTT technique has been examined to lessen down the probability of random IP spoofed packets correctly, efficiently and effectively. Through this, detection rate of the malicious packets have been improved up to 99% which is 80-85% improved for probabilistic Hop Count Filtering approach and 90% improved for conventional i.e. CHCF approach. It prevents the VM server from the IP spoofed DDoS attacks and it also eradicates the CPU cycles wastage. VCPHCF-RTT focuses on lessening down IP spoofing based attacks. The computation time has been reduced comparatively. Detection rate of malicious packets has been improved tremendously up to 99.7%.***

Index Terms: Distributed Denial of Service (DDoS), Clouds, Virtual Machines (VM), Filter, Hop Count Filtering (HCF), Time-to-live (TTL), Virtual Cloud PHCF with RT Time (VCPHCF-RTT)

I. INTRODUCTION

Availability is an important aspect of Internet/network security. DDoS attacks poses giant threat to the service availability on the network/ Internet. Anybody can send any packet to anyone without any authentication, while the receiver processes every packet arriving for a provided service. Cloud Security issue is one of the biggest challenges that hampers the growth of Cloud for its various service provisioning. There exists the requirement of great research work in the area of Infrastructure based cloud security for smooth provisioning of services to the customers of cloud. Several DDoS mitigation techniques, those have been proposed so far in the area of cloud security possesses certain limitations. More research work is required to be performed in the area of cloud security at infrastructure level. [3]. DDoS attack is prone to fills the bandwidth of the large networks with huge amount of illegitimate requests or packets consuming more bandwidth and makes the service unavailable for the internet users. The attacker scans millions of machines to compromise them for launch DDoS attack. These machines are scanned for their vulnerabilities and weakness and then compromised and named as slave machines or zombies. These zombies can lure more infected machines or zombies. When the attack starts, it becomes cumbersome to identify the identity of the real attacker and orders are continuously sent by the attackers to the zombies to perform the assaults. The attackers does not steal, delete or amend or eradicate the information carried on networks, an attempt is always made by them to impair a network service, thus making the network services unavailable to the legitimate users. [6].

The Probabilistic HCF using RTT (VCPHCF-RTT) technique has been proposed and it will be implemented. Results will be gathered at the intermediate nodes or hops between the virtual machines of the Client VM and Server VM. Detection rate as well as the computation time will be considered as the basis of comparison for malicious packets. Purpose is to secure cloud environment from malicious attacks at infrastructure level so as to enable the efficient access of cloud services to customers and to maintain its integrity and its characteristics for better service provisioning.

Hop Count ensures number of hops which a packet traverses while moving from the sender to the receiver [15][8]. HC is inferred from the TTL field. Hop Counts between the source and destination are used to assess the packet authenticity [14]. IP TTL field never allows packets for looping forever. TTL initial value is set by the sender. At each node, TTL value is decremented by one. The packet is discarded after TTL reaching zero. Hop Count Estimation is done by subtracting the received TTL value from the closest initial TTL bigger than the received packet’s TTL at the receiver end. Internet server can easily infer the hop-count information from the IP Header’s TTL field on the other end [12][13].The initial TTL values are limited to few possibilities that include 30, 32, 60, 64, 128, and 255 and are operating system dependent[4]. Thus, the initial TTL value which are set by the operating system can be inferred easily without explicitly knowing what actually the Operating System is [9][10].

Probability based technique is used for uncertainty assessment and analysis of statistical/ mathematical models. [13]. Uncertainties characterizes the probabilities associated with events in this technique.

Manuscript published on 30 December 2018.
* Correspondence Author (s)

Ms. Ritu Maheshwari*, Department of Computer Science, Barkatullah University, Bhopal (Madhya Pradesh), India.

Dr. Anil Rajput, Department of Mathematics, CSA Govt. PG Nodal College, Sehore (Madhya Pradesh), India.

Dr. Anil K. Gupta, Department of Computer Science, Barkatullah University, Bhopal (Madhya Pradesh), India,

The probability of that event is the frequency of occurrence of that event which is illustrated as the ratio of the no. of times the event occurs to the total no. of samples or experiments during considering large number of samples. An event's '0' probability means that the event will never occur, and event's '1' probability means that event will always occur. The Virtual Cloud Probability Hop Count Filtering RT Time method has been put up and proposed for implementation. Results are accumulated at Virtual Machine Server and at the intermediate virtual hops.

In this paper, section II presents *Software Tools and Requirements for Virtual Cloud*, section III presents *A Brief Review on Hop Count Filtering*, section IV presents *Working Principle of Proposed Security Agent: "VCPHCF-RTT"*, section V presents *Probabilistic Approach for Private Virtual Cloud Infrastructure*, section VI presents *Private Virtual Cloud Infrastructure using "VCPHCF-RTT"*, section VII presents *EXPERIMENTAL RESULTS OF "VCPHCF-RTT"*, section VIII presents *Result Analysis of "VCPHCF-RTT"*, section VII presents *5-Step Proposed Methodology for Security Agent "VCPHCF-RTT"* and section IX presents *Final Outcomes of "VCPHCF-RTT"* and section X presents *Conclusions*.

II. SOFTWARE TOOLS & REQUIREMENTS FOR VIRTUAL CLOUD

A. Software Tools

- Eucalyptus and Amazon EC2
- Hypervisor: Xen 3.1.2 VMM/VMware/KVM
- CloudSim Simulator, Euca2ools for Cloud
- Multiplexing Tools, VM Emulators
- Host Operating System: Linux/ Ubuntu 12.04
- Guest O.S. : UBuntu 11; Clients: UBuntu 11.10
- Packets Type: TCP/UDP/ICMP
- Packet Transmission Rate: Min. 350 Packets/ Second
- VM : 4 GB Capacity/ 2 GB Variable Partition Space
- Sample Data: CAIDA's 2010 DDoS Attack Data Set

B. Simulation Requirements

- Simulation of TCP-SYN Flood Attack/ HTTP Flood Attack/ ICMP/ UDP
- Filtering at Network Layer
- VM Using Google Secure Sandbox
- Cloud's IaaS Infrastructure
- Cloud Controller (Public/ Private Key)/ Cluster Controller (No. of Nodes)
- White List (WL)/ Black List (BL)/ Malicious List (ML)/ Suspicious List (SL)
- IaaS Cluster of Nodes (Node Controllers for VMM)

C. Parameters

- Detection Rate
- Computation Time

III. A BRIEF REVIEW ON HOP COUNT FILTERING

Ayman Mukaddam et al. [15] proposed conventional HCF method for victim side that is ineffective and time consuming. Xia Wang et al. [17] lacks in improving the packet filtering technique which is required to eliminate random IP spoofing. The algorithmic work of Krishna Kumar et al. [18] suggested a requirement of the shared key between every pair of adjacent router-router pairs and need a tremendous computational time as well as memory space. B.R. Swain et al. [6] proposed probabilistic technique that does not ensure about the legitimacy of remaining unchecked packets. Hence, this technique also lacks in ensuring 100% detection of malicious packets out of total packets. Haining Wang et al. [11] proposed a technique that leaks the information for the attacker that can find the appropriate way through creating an effective IP2HC table henceforth overcoming HCF. Hence, this is also an ineffective way to prove legitimacy of packets.

IV. ISSUES & CHALLENGES OF CLOUD

- IP Spoofing Attack Mitigation in Cloud
- Hypervisor Security
- Active/Inactive VM Security
- Security Vs. Performance
- Virtualization Enhancement

V. WORKING PRINCIPLE OF PROPOSED SECURITY AGENT: "VCPHCF-RTT"

Conventional HCF technique drops 90% of erroneous packets, probabilistic HCF drops upto 85% of malicious packets but VCPHCF-RTT, drops upto 100% of illegitimate packets. In VCPHCF-RTT, focus is on applying the probabilistic distributed HCF with RT Time at every intermediate virtual hop and every packet is checked once for its legitimacy at the virtual hops which after then those packets are are transferred to the virtual client.

Firstly, the erroneous packets have been detected appropriately at each intermediate virtual router using distributed HCF technique that ensures us to prevent flooding based IP spoofing attacks at the virtual machine server. This VCPHCF technique has been applied to the intermediate routers initially for total number of packets. This technique has been applied in combination with the Round Trip Time (RTT) to lower down the estimation of guessing the parameter values of both VCHCF and RTT simultaneously to be true. This unique and new combination of VCHCF and RTT has been proved more effective in preventing the random IP spoofing attacks at both intermediate routers and at the victim side. Secondly, the VCPHCF along with RTT is being initially applied to total number of packets. The malicious packets, so discarded, does not contain any genuine packets as both VCPHCF and RTT technique are effective enough to prevent dropping of genuine packets. From Probabilistic view, few packets will definitely, remains "not-detected malicious" while considering a threshold value of packets to be erroneous out of total packets. The detected genuine packets are passed to the victim server and the "not-detected malicious" packets are passed on to the next hop for further application of probability based VCHCF and RT Time technique on to them.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

This process is carried out until "not-detected malicious" packet counts becomes zero.

During all these process, the effectiveness of probability associated VCPHCF RT Time approach has been examined over probabilistic HCF and conventional HCF along with RT Time approach on account of the Detection rate of malicious packets. Hence, working of VCPHCF-RTT plays an important Role lying on the virtual machine monitor to allow only legitimate packet transmissions between the Virtual Intermediate routers and the virtual machine clients and between the virtual machine server and the virtual intermediate hops. In Short, Step by Step process can be given for proposed security agent that is as follows:

Step 1 of the VCPHCF-RTT illustrates the total number of packets to be handled while in transmission and calculating their probability of being spoofed through Poisson distribution model. Step 2 illustrates the calculation of total number of intermediate routers and distributing the packets at each intermediate router for filtering and counting for malicious ones. Step 3 illustrates the elimination of illegitimate packets from the legitimate ones. Genuine packets will be sent to the virtual machine server for request and IP spoofed packets will be tagged and discarded. Step 4 illustrates the counting of number of unchecked packets due to probabilistic elimination that will also be handled for further checking of their legitimacy so that no packet should be left unchecked. Step 5 will ensure the completion of the process till all the packets get checked for their legitimacy.

5-STEP PROCESS FOR "VCPHCF-RTT"

Step 1: Calculate the probable malicious IP spoofed packets using probabilistic model of Poisson Distribution.

Step2: Apply probabilistic Hop Count Filtering module at intermediate virtual hops.

Step 3: Hop Count Filtering based legitimate packets filtered thereof will be sent to the VM server and the erroneous packets found at the intermediate virtual hops will be discarded. Unchecked packets due to probability will be tagged.

Step 4: Check whether there is any tagged unchecked packet remains.

Step 5: If YES, then, tagged checked packets will be sent to the next intermediate hop for the same process repetition. If NO, then, stop the process.

VI. PROBABILISTIC APPROACH FOR PRIVATE VIRTUAL CLOUD INFRASTRUCTURE

The probability concept is applied to compute the total packets being malicious which an uncertain problem is. Supposing the no. of packets arriving at the VM server with a poison's distribution model is *lambda*. Further, suppose that each packet reaching at the virtual server being erroneous with the probability ***p*** or non-malicious with the probability ***1-p***. So now the joint probability of ***n*** packets among the total traffic is malicious and 'm' packets among the total traffic are non-malicious which is as follows:

Let ***N1*** signifies the number of erroneous packets and N2 signifies the number of non-malicious packets. Also suppose ***N=N1+N2*** be the total number of trafficking packets which arrives at virtual server.

Conditioning on ***N*** now gives,

#1: $\mathrm{P}\,\{\mathrm{N1} = \mathrm{n};\ \mathrm{N2} = \mathrm{m}\} = \sum\sum_{i=0}^{\infty} \mathrm{P}\,\{\mathrm{N1} = \mathrm{n};\ \mathrm{N2} = \mathrm{m} \mid \mathrm{N} = \mathrm{i}\}\ \mathrm{P}\{\,\mathrm{N} = \mathrm{i}\}$

Because P {N1 = n; N2 = m | N = i} = 0, when i ≠ n+m, the above equation yields that,

#2: P {N1 = n; N2 = m}

$= \mathrm{P}\,\{\mathrm{N1} = \mathrm{n};\ \mathrm{N2} = \mathrm{m} \mid \mathrm{N} = \mathrm{n{+}m}\}\ e^{-\lambda}\,\frac{\lambda^{n+m}}{(n+m)!}$

Also if it is apparent that among those ***n+m*** packets each packet of being malicious is having the probability of ***p*** and the conditional probability of those ***n*** packets out of them as malicious is actually the binomial probability of `n' successes out of ***n+m*** trials. Therefore,

#3: $\mathrm{P}\,\{\mathrm{N1} = \mathrm{n};\ \mathrm{N2} = \mathrm{m}\} = \binom{m+n}{n} p^{\mathrm{n}} (1-p)^m\ e^{-\lambda}\,\frac{\lambda^{n+m}}{(n+m)!}$

#4: $= (\frac{(m+n)!}{m!n!} p^n (1-p)^m)\ e^{-\lambda}\,\frac{\lambda^{n+m}}{(n+m)!}$

#5:= $(p^n (1-p)^m\ e^{-\lambda p} e^{-\lambda(1-p)} \lambda^m \lambda^n)$ / m! n!

#6:= $e^{-\lambda p}\,\frac{(\lambda p)^n}{(n)!}\ e^{-\lambda(1-p)}\,\frac{(\lambda(1-p))^m}{(m)!}$

Here equation (#3) shows the probability/susceptability of ***n*** packets being malicious and ***m*** packets not being malicious but legitimate. So by taking the value of probability to 1, by mentioning the value of rate of arrival **λ** in no. of packets per time unit' and probability of error in a packet ***p*,** the values of ***n*** and ***m*** can be obtained.

The weakness in the system is due to vulnerability in cloud which can cause expected or unexpected harm. Cloud computing is prone to DDoS attack as the public internet is used for its connectivity. Cloud security is required at various levels to confirm proper implementation of cloud computing such as: data storage security, host server security, application security, and internet or network security [1].

Private Clouds are the proprietary networks that reside within the enterprise for the usage of the organization or for a specific group of customers. Private clouds use advanced virtualization technologies and automated management technologies to improve scalability and effective utility of localized data centers [4]. Virtual Private Clouds are the result of creation of service provider through the available public cloud resources.

This cloud model is based on a deep stack of VM's dependent layers, Application Programming Interfaces, Services and Applications where the higher layer functionality and security is dependent on the lower ones. The IaaS model cover up cloud physical infrastructure layer which include storage, servers and networks, virtualization layer i.e. hypervisors, and virtualized resources layer i.e. VMs, virtual storage, virtual networks. Its service delivery has got several security issues based on the cloud deployment model [2]. Infrastructure also pertains to the path for transmission along with hardware where data is processed and stored. Data used to be transmitted from source to destination through several third-party infrastructure based devices. In IaaS model, the cloud service provider supplies a set of virtualized infrastructural components like virtual machines and storages on which consumers can create and run applications.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

The application resides on the virtual machines and the virtual operating system. Isolation should consider VMs’ storage, networks, processing, memory and cache memories in Iaas Infrastructure. Dynamic resource allocation and service provisioning in IaaS is provided by virtualization.

Through virtualization, multiple Operating Systems can co-reside on the same physical machine without intervening each other. Virtual Machine Monitor that is also known as Hypervisor [5] allows multiple Virtual Machines (VMs) to run on a single host operating system or directly on the underlying hardware simultaneously to support sharing of resources. Association of multiple servers with single host removes the physical separation between the servers that increases the threats of malicious attacks on virtual machines and root to access the virtual machine monitor. Through this vulnerability exploitation, attacker can gain access to the machine and can target several areas of a virtualized cloud infrastructure like hypervisor, hardware, guest operating systems and the applications within individual Virtual Machines. The PaaS model covers application servers, web servers, IDEs, APIs and Services layers. PaaS layer is dependent on the virtualization of resources which are distributed through IaaS. The SaaS model cover up services and applications offered as a service for the end users. SaaS layer is dependent on a layer of platforms to host the services and a virtualization layer is needed to optimize the utilization of resources while delivering its services to multiple tenants.

Enabling virtualization technology has got the ability to conceal the physical features and to provide the user with an abstract environment for accessing that helps to create abstract infrastructure and resources making them available to clients as isolated VMs. A hypervisor is a piece of platform-virtualization software supporting multiple operating systems and enabling them to run on a host computer simultaneously. But, this generation of virtualized resources for sharing purposes amplifies the attack surface. Some mechanisms are required to guarantee secure communications between VMs, strong isolation and mediated sharing. Operating Systems virtualization level, Applications virtualization level, Storage virtualization level and Network virtualization level are used. Virtualization depends on technical isolation. Virtual machines may generate threat of attacks in the environment if are not deployed properly on isolation basis. Poor isolation leads to inter-attacks between two VMs or between VMs and associated hypervisors.

VII. PRIVATE VIRTUAL CLOUD INFRASTRUCURE USING “VCPHCF-RTT”

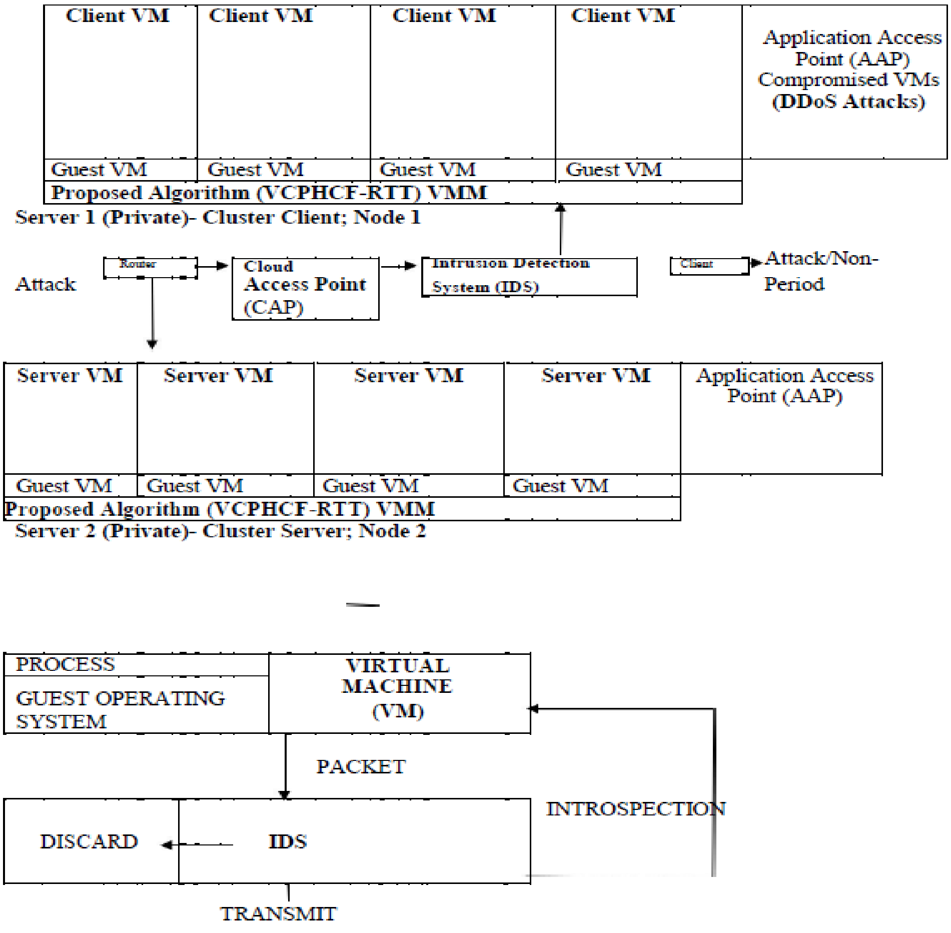


Fig.1 : Proposed Model of Private Virtual Cloud Infrastructure using Security Agent “VCPHCF-RTT”

Fig. 1 Proposed Model of Private Virtual Cloud Infrastructure using Security Agent “VCPHCF-RTT”

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

VIII. EXPERIMENTAL RESULTS OF VCPHCF-RTT

Table 1: Results of VCPHCF-RTT

Total Erroneous/Malicious and Non-Malicious Packets (M)	400000
Total Erroneous/ Malicious Packets introduced (Standard Count)	28000
Probability associated Total Erroneous/ Malicious Packets (m)	29335
Total Malicious Packets Detected at hop = 4(Actual Count)	27494
Allowed NOT DETECTED Malicious Packets to the VM Server (Count-m)	506
Percent of Malicious Packet Detected by using no. of Hops = 4	98%
Total Malicious Packets Detected at hop = 30 (Actual Count)	27860
Allowed NOT DETECTED Malicious Packets to the VM Server (Count-m)	140
Percent of Malicious Packet Detected by using no. of Hops = 30	99.50%
Total Malicious Packets Detected at hop = 1(Actual Count)	23705
Allowed NOT DETECTED Malicious Packets to the VM Server (Count-m)	4295
Percent of Malicious Packet Detected by using no. of Hops = 1	84.66%
Total Malicious Packets Detected at hop = 2 (Actual Count)	26242
Allowed NOT DETECTED Malicious Packets to the VM (Count-m)	1758
Percent of Malicious Packet Detected by using no. of Hops = 2	93.72%
Total Malicious Packets Detected at hop = 3 (Actual Count)	27320
Allowed NOT DETECTED Malicious Packets to the VM (Count-m)	680
Percent of Malicious Packet Detected by using no. of Hops = 3	97.57%

IX. RESULT ANALYSIS OF "VCPHCF-RTT"

The problem covers focussing on mitigation of Distributed DoS attacks applying Probabilistic Hop Count Filtering and RT Time to reduce computation time and increase the detection rate of erroneous packets in private virtual cloud infrastructure. For this, VCPHCF-RTT technique has been proposed. Our technique has utilized the number of hops up to 4. Proposed technique VCPHCF-RTT has been evaluated with the PHCF Technique at the virtual machine server as in Fig. 2. It has been shown that VCPHCF-RTT has showcased effective results in finding detection rate of malicious packets maximizing up to 99.33%. VCPHCF-RTT technique has also been considered for different samples ranging from {10000, 15000, 20000, 25000, 30000, 35000, 40000} for number of hops = 4.

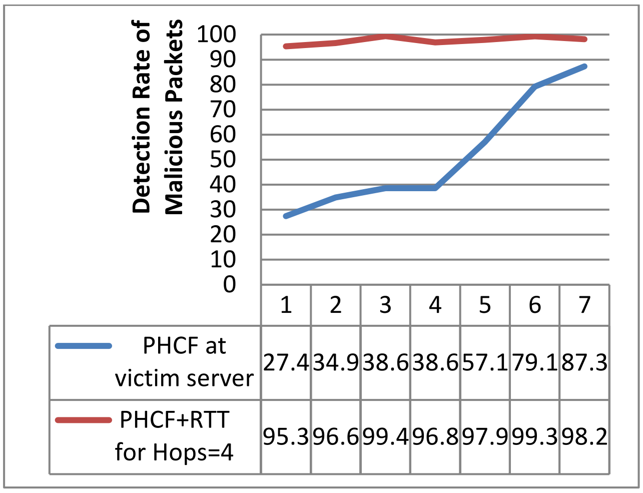


Fig. 2 Comparison of "VCPHCF-RTT" for Hops=4 with PHCF at victim virtual server

As shown in Fig. 3, VCPHCF-RTT technique is also evaluated for hops = 30 with other existing techniques like PHCF and CHCF at the victim server, it has been found that proposed technique has given the optimum results with up to 100% detection rate of malicious packets. So, VCPHCF-RTT technique can be implemented using real time cloud environment in combination with some other new techniques. Doing this, several other attacks on Virtual Machine Server can also be mitigated effectively and efficiently apart from IP spoofing.

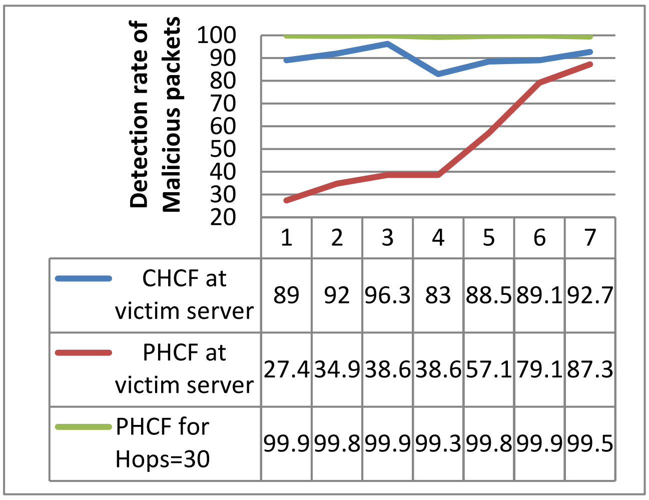
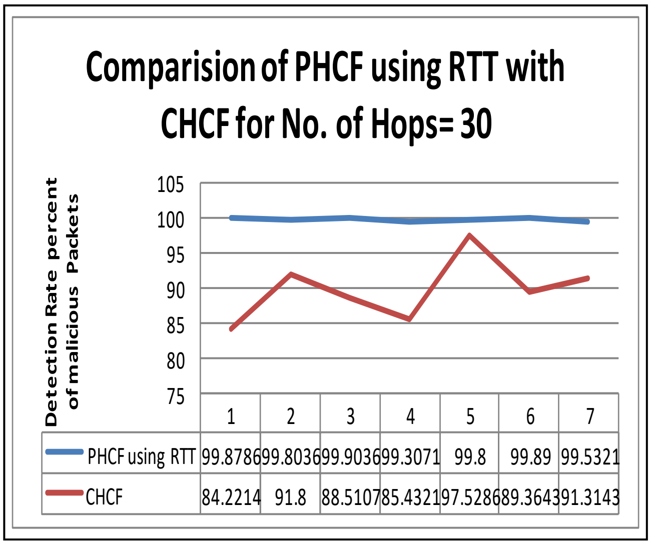


Fig. 3 "VCPHCF-RTT" with PHCF and CHCF for hops=30 at the Victim Virtual Server

Of course, VCPHCF-RTT has given its outstanding performance by giving up to 100% Detection rate of erroneous/ malicious packets. But, other techniques can also be utilized well as they have never been used before. These techniques can be utilized in mitigating other possible threats on Virtual Machine server apart from IP spoofing attacks which have been taken up by proposed technique.

Comparison has also been done between VCPHCF-RTT and conventional HCF technique for no. of hops equals to 30 and it has been shown in fig. 4 that VCPHCF-RTT technique has outperformed well.

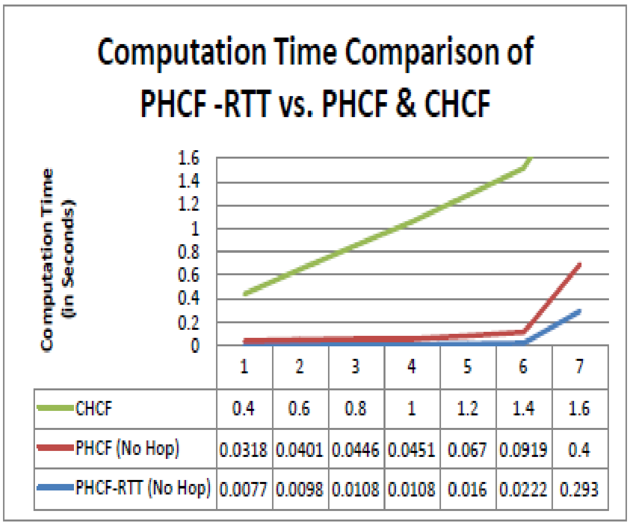
Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)



	1	2	3	4	5	6	7
PHCF using RTT	99.8786	99.8036	99.9036	99.3071	99.8	99.89	99.5321
CHCF	84.2214	91.8	88.5107	85.4321	97.5286	89.3643	91.3143

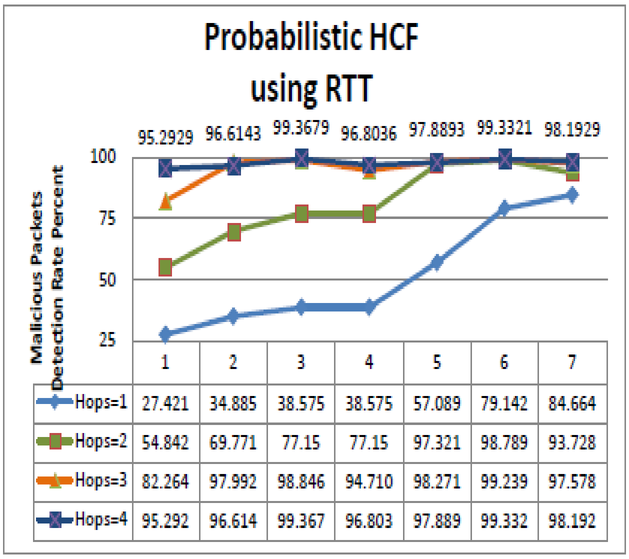
Fig. 4 VCPHCF-RTT" vs. CHCF for no. of Hops = 30

X. FINAL OUTCOMES OF "VCPHCF-RTT"



	1	2	3	4	5	6	7
CHCF	0.4	0.6	0.8	1	1.2	1.4	1.6
PHCF (No Hop)	0.0318	0.0401	0.0446	0.0451	0.067	0.0919	0.4
PHCF-RTT (No Hop)	0.0077	0.0098	0.0108	0.0108	0.016	0.0222	0.293

Fig. 5: Computation Time of VCPHCF-RTT Vs Other Techniques



	1	2	3	4	5	6	7
Hops=1	27.421	34.885	38.575	38.575	57.089	79.142	84.664
Hops=2	54.842	69.771	77.15	77.15	97.321	98.789	93.728
Hops=3	82.264	97.992	98.846	94.710	98.271	99.239	97.578
Hops=4	95.292	96.614	99.367	96.803	97.889	99.332	98.192

Fig. 6: Detection Rate of Malicious Packets using VCPHCF-RTT at different Hops

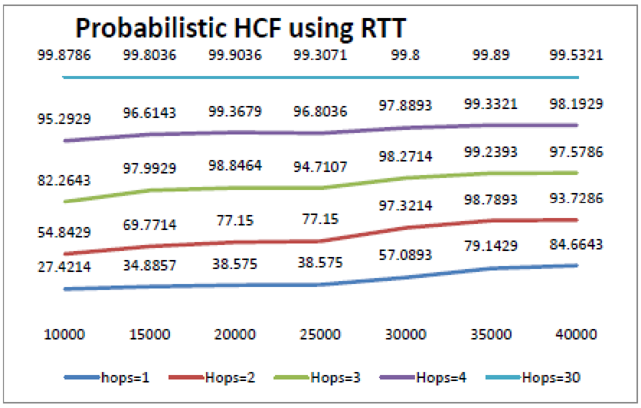
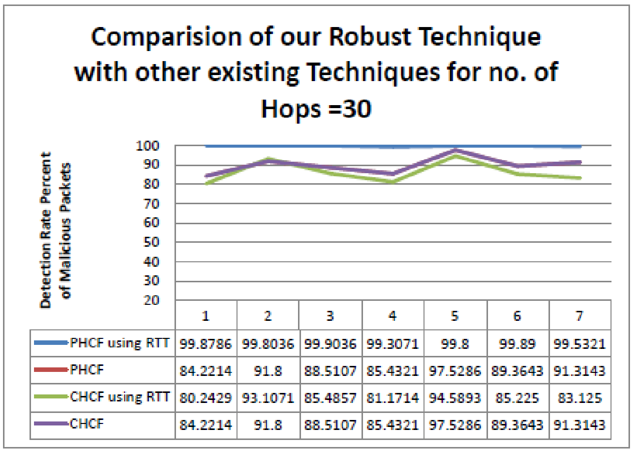


Fig. 7: Detection Rate from VCPHCF-RTT for Hops: 30



	1	2	3	4	5	6	7
PHCF using RTT	99.8786	99.8036	99.9036	99.3071	99.8	99.89	99.5321
PHCF	84.2214	91.8	88.5107	85.4321	97.5286	89.3643	91.3143
CHCF using RTT	80.2429	93.1071	85.4857	81.1714	94.5893	85.225	83.125
CHCF	84.2214	91.8	88.5107	85.4321	97.5286	89.3643	91.3143

Fig. 8: Detection Rate Comparison of VCPHCF-RTT with Other Techniques for Hop: 30

XI. CONCLUSION

The IP Spoofing technique that has been proposed using security agent *Virtual Cloud Probabilistic HCF using RTT (VCPHCF-RTT*) in private virtual cloud infrastructure has been implemented using tools and techniques mentioned in this research paper. 5-Step Process has been given to execute Security Agent: "VCPHCF-RTT". Experimental Results have been gathered after running our proposed security agent "VCPHCF-RTT" at the virtual machine monitor or hypervisor of both the client Virtual Machine and Server Virtual machine. "VCPHCF-RTT" has been designed purposively to filter out illegitimate packets at the maximum highest detection rate up to 100%. Detection rate and the computation time for erroneous packets is considered as the basis of evaluation. This security agent "VCPHCF-RTT" can be considered as unique and robust technique for almost 100% IP spoofed packet filtering while communicating between VM Client and VM Server of the proposed model. VCPHCF-RTT technique is examined to reduce the chance of random IP spoofing of packets effectively and genuinely. Detection rate of the malicious packets has now been raised up to 99% which is 85% for Probability associated HCF one and 90% for conventional HCF approach. It prevents the Virtual Machine server from the IP Spoofing based DDoS attacks and also reduces the CPU cycles wastage.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

REFERENCES

1. L. Chi-Chun, H. Chun-Chieh, K. Joy, “A Cooperative Intrusion Detection System Framework for Cloud Computing Networks,” IEEE 39th International Conference on Parallel Processing Workshops, pp. 280-284, 2010.
2. K. Kourai, T.Azumi, S. Chiba, “A Self-Protection mechanism against Stepping Stone Attacks for IaaS Clouds,” IEEE 9th International Conference on Ubiquitous Intelligence and Computing, pp. 539-546, 2012.
3. R. Shrivastava, R. Sharma, A. Verma, “MAS based Framework to protect Cloud Computing against DDoS Attack,” International Journal of Research in Engineering and Technology, IJRET, vol. 2(12), pp. 36-40, December, 2013.
4. L. Sheng-Wei, Y. Fang, “Securing KVM – based Cloud Systems via Virtualization Introspection,” IEEE 47th Hawaii International Conference on System Science, pp. 5028-5037, 2014.
5. A. Kumara M.A., C.D. Jaidhar, “Hypervisor and Virtual Machine Dependent Intrusion Detection and Prevention System for Virtualized Cloud Environment,” 1st International Conference on Telematics and Future Generation Networks, pp. 1-6, 2015.
6. B.R. Swain, Bibhudatta Sahoo, “Mitigating DDoS attack and Saving Computational Time using a Probabilistic approach and HCF method,” IEEE International Conference on Advance Computing, NIT, Rourkela, India, pp. 1170-1172, 6-7, March 2009
7. R. Maheshwari, C. Rama Krishna, M. Sridhar Brahma “Defending Network System against IP Spoofing based Distributed DoS attacks using DPHCF-RTT Packet Filtering Technique,” IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques, KIET, Ghaziabad, India, pp. 211-214, 8th February 2014.
8. P. Jayashree, K.S. Easwarakumar, V. Anandharaman, K. Aswin, S. Raja Vijay, “A Proactive Statistical Defense Solution for DDOS Attacks in Active Networks,” 1st IEEE International Conference on Emerging Trends in Engineering & Technology, Anna University, Chennai, India, pp. 878-881, 16-18, July, 2008.
9. J. Sen, “A Robust mechanism for defending distributed denial of service attacks on web servers,” International Journal of Network Security and its Applications, vol. 3 (2), pp. 162-179, March 2011.
10. Q. Wu, R. Zheng, J. Pu, Shibao Sun, “An Adaptive Control Mechanism for Mitigating DDoS Attacks,” IEEE International Conference on Automation and Logistics, Henan University of Science and Technology, Luoyang, China, pp. 1760-1764, 5-7, August, 2009.
11. H. Wang, C.Jin and K. Shang, “Defense Against Spoofed IP Traffic Using Hop-Count Filtering,” IEEE Transaction on Networking, vol. 15 (1), pp. 40-53, February, 2007.
12. F. Zhang, J. eng, Z. Qin, M. Zhou, “Detecting the DDoS Attacks Based on SYN proxy and Hop-Count Filter,” IEEE International Conference on Communications, Circuits and Systems, University of Electronic Science and Technology, China, pp. 457-461, 11-13, July, 2007.
13. I. B. Mopari, S.G. Pukale, M.L. Dhore, "Detection and defense against DDoS attack with IP spoofing," IEEE International Conference on Computing, Communication and Networking, Vishwakarma Institute of Technology, Pune, India, pp. 1-5, 18-20, December, 2008.
14. C. Jin, H. Wang, K. G. Shin, “Hop-count filtering: an effective defense against spoofed traffic,” 2003, [Online]. Available: http://www.citeseerx.ist.psu.edu
15. A. Mukaddam, I. H. Elhajj, “Hop count variability,” 6th IEEE International Conference on Internet Technology and Secured Transactions, American University of Beirut, Lebanon, pp. 240-244, 11-14, December , 2011.
16. B. Krishna Kumar, P.K. Kumar, R. Sukanesh, "Hop Count Based Packet Processing Approach to Counter DDoS Attacks," International Conference on Recent Trends in Information, Telecommunication and Computing, PET Engineering College, Thirunelveli, India, pp. 271-273, 12-13, March, 2010.
17. [17] A Wang, Xia, Li Ming, Li Muhai, "A scheme of distributed hop-count filtering of traffic," International Communication Conference on Wireless Mobile and Computing, pp. 516-521, 7-9 Dec.2009.
18. [18] B. Krishna Kumar, P.K. Kumar, R. Sukanesh, "Hop Count Based Packet Processing Approach to Counter DDoS Attacks," International Conference on Recent Trends in Information, Telecommunication and Computing, PET Engineering College, Thirunelveli, India, pp. 271-273, 12-13, March, 2010.

AUTHOR PROFILE

Ms. Ritu maheshwari, Ph.D Scholar, B.E. (CSE) from RGPV Bhopal MP, India, MBA (IT & Finance) from DAVV Indore, MP, India, M.E. CSE from Panjab University, Chandigarh, Ph.D (CS) pursuing from BU, Bhopal MP India Ritu Maheshwari has received Honour by WORLD BOOK OF RECORDS, United Kingdom, in the event of INDO-UK CULTURAL FORUM LONDON (ENGLAND) held in Indore (MP) on 28th July 2018 for Matchless Contribution in the Betterment of the Society. She had received Appreciation Letter for the best performance in Academic, Research and Administration while working as Assistant Professor (CSE) in FET, MRIU, Faridabad (Haryana) for the session July 2014 to June 2015. She is pursuing my Ph.D in Computer Science from Barkatullah University (BU), Bhopal (M.P.). She completed her M.E. (Computer Science and Engineering) from National Institute of Technical Teachers’ Training & Research (NITTTR), Panjab University (PU), Chandigarh with 85% Honours in the year 2013 and had been the Branch Topper and won Academic Excellence Award. She completed her Masters in Business Administration (MBA) with specialization in IT & Finance from RGPGPI, Devi Ahilya Vishwa Vidyalaya (DAVV), Indore (MP) in the year 2005 with 67% marks. She completed her B.E. (Computer Science & Engineering) with 73.38%, from JIT (Khargone) RGPV, Bhopal (MP) in the year 2002. She is having 15 years of total experience with 12 years of teaching experience in both Engineering and Management wing and 3 year of Industrial Experience in Software Development. She is having my 16 Research Publications in several recognized National & International Journals/ Conferences/ Seminars. Her field of research is Network Security and Cloud Security. She has also won Best Paper Award titled “Analysis of DPHCF-RTT Packet Filtering Technique against DPHCF and DCHCF

Techniques” in recognition of the most outstanding paper in the International Conference on Science, Technology and Management at YMCA, New Delhi on 1st February 2015. She had done several Research Projects on IT & Automation: Impact of its adoption in various Organizations, Printers on Demand, Business Software for the Agents / Development Officer of Life `Insurance Corporation of India etc. She has guided 4 M.Tech Projects, 2 B.Tech Projects and 1 MBA Project. She has attended and participated in several FDPs/ SDPs/ Workshops/ Conferences/ Seminars at National and International levels. She is confident, committed, Passionate, enthusiastic & self motivated having excellent computing skills.

Dr. Anil Rajput, Professor, Deptt. Of mathematics & Computer Science, CSA Govt. PG Nodal College, Sehore, MP India PhD, M. Phil., M. Sc., MCA

Dr. Anil Rajput is having total 25 years of Research Experience. He is an Approved Supervisor for Ph.D. Degree in the subject Mathematics and Computer Science in the following Universities: Barkatullah University, Bhopal and MP Bhoj Open University, Bhopal. His Area of Research includes: Fixed Point Theory, Game Theory, Wavelets Analysis, ICT & A.I, Data Mining . He Guided Total 35 No. of Ph.D. , Total 8 under Submission and total 8 Registered under him. He has published total 78 Research Papers in several National and International Conferences and Journals. He attended 95 Seminars / Conferences/ Workshops/ Training Programs/ FDPs. He has published total 02 Text Books (i) Business Mathematics (ii) AI & Expert System

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)