Intrusion detection using the Hop Count Inspection Method (HCIM) Algorithm

RPS Bedi

Deputy Registrar,PTU Jalandhar

Abstract:

Intrusion Detection and Cloud Computing are the latest buzzword now a day's and emerges as one of the key service of the Utility computing which builds on decade of research in the field of networking, web and software services. Cloud Computing offers a service oriented architecture, reduced information technology overhead for the end-user, great flexibility and reduced total cost of ownership. Depending on the type of resources provided by the Cloud, distinct layers can be defined as Infrastructure as a Service (IaaS), Platform as service (PaaS) and Software as a Service (SaaS), from which later will deliver various Applications to the clients over the Web. SaaS has become a vital service for the technology vendors to provide a wide variety of application services, application products and on-demand services to their clients according to their utility and demand over the web as a key channel. But recent attacks on the clouds especially Distributed Denial of Service (DDoS) poses as a crucial threat to this key technology of the future.

1. Introduction

Cloud Computing has come up as a key service of the Utility computing. It is built on decade of research in the field of networking, web and software services. In this thesis, implementation of intrusion detection with the help of cloud computing methods is done. Transformation of Computing to a model consisting of services that are customized and delivered in the same manner as traditional utilities like water, gas, electricity and telephony. In this type of model, based on their requirements users access services without regard to the place where the services are hosted or how they are being offered. Many computing systems have promised to deliver this utility computing vision and having grid computing, cluster computing and most recently is Cloud computing.

Cloud Computing[1] as a utility, had been thought of a great revolution in the field of computing, which will upgrade IT industry in a big way, can make software a better attractive service and would shape the way IT hardware is conceptualized and purchased. No big efforts are required to the software professionals with imaginary thoughts for new Internet services in hardware to deploy their services or the human cost to operate it. So, the computing world is swiftly changing towards developing software for millions to use as a service, instead of running on their own computers.

2. CLOUD COMPUTING

Cloud Computing (Buyya et al. 2009) refers to the applications offered as services over the Internet as well as the hardware and systems software in the datacenters which provide these services**.** Cloud computing (Figure 1.0) is a model to allow requested network access, which is very convenient, to a shared group of configurable computing resources such as servers, storage, networks, applications and services which can be offered and released immediately with lesser service provider interaction or management effort.

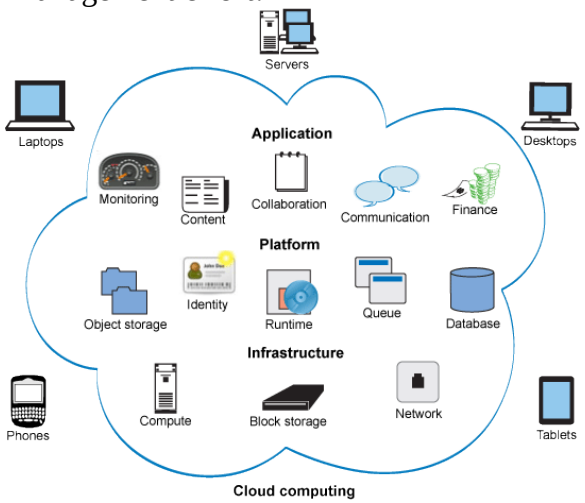

Figure 1.0 A Cloud Computing Environment.

Source Internet (free pictures)

These days, it is common to access content across the Internet infrastructure. This infrastructure has data centers that are monitored and maintained by content providers throughout. An extension of this paradigm is Cloud computing, wherein the capabilities of business utilities are exposed as useful services that can be accessed over a network. By charging consumers for accessing these services, the Cloud service providers are given incentives in terms of profits to be made. Cloud computing ensures reliable services that are delivered through next-generation data centers which are built on storage technologies[2] and virtualized computation .With the help of data from a "Cloud" ,consumers will be able to use applications and data anywhere in the world , when required. Computing services should be scalable, highly reliable and autonomic that can support dynamic discovery and ubiquitous access.

3. The Hop Count Inspection Method (HCIM) Algorithm

The inspection algorithm calculates the source IP address and the final TTL value from each IP packet and then set the initial TTL value and subtracts the final TTL value for calculating the hop-count. The source IP address gives the index into the table to recover the correct hop-count for this IP address. If the calculated hop-count is same as the stored hop-count, the packet has been valid otherwise; the packet is likely to be spoofed. It is observed that a spoofed IP address

may happen to have the same hop-count as the one from a zombie to the victim. In this scenario, HCF will not be capable to recognize the spoofed packet. But with a restricted range of hop-count values, HCF is extremely successful in calculating spoofed IP addresses.[*] **Algorithm HCIM**

Step 1: For each packet count the number of hops as H_{count} // By Hop Counter or Simple Inspection
Step 2: Retrieve the stored Hop count index as H_{stored}
Step 3: For each packet
if (H_{count} != H_{stored})
then 'discard the packet' // Packet is malicious
else
'allow the packet' // Packet is legitimate
Step 6 : end if

4. Proposed Algorithm

Hop Count Inspection with Malicious Probability Rate (HCI-MPR)

Step 1: For given value of 'λ' and 'p' calculate 'm' (5) , no of malicious packets such that

P(M = m) = 1 (Joint probability of malicious packets)

Step 2: Initialize count = 1

Step 3: For each value of count =1 to m

Extract final value of TTL (Time to Live) as T_f

Investigate the initial value of TTL as T_i

Compute Hop count $H_c = T_f - T_i$

Retrieve the stored Hop count index as H_s

For each packet

if (H_c != H_s)

then 'discard the packet' // Packet is malicious

else

'allow the packet' // Packet is legitimate

Step 4: Increment count as count ++

Step 5: Repeat step 3 until count < = m.

Step 6: if count > m exit .

In our approach we are calculating the number of malicious packets from a given number of packets using a analytical approach (3.1). We first sample the number of packets on the basis of arrival at the server per a time unit. By taking that number of packets, the average arrival rate of the packets and the error probability of a packet we calculate the number of packets being malicious. Then we apply the simple HCIM (Hop-Count Inspection Method) Algorithm (3.5) to filter out first that many numbers of packets which was found out using the probabilistic approach. When we will reach at the exact number of packets, we simply release all the rest packets towards the server assuming that these are not malicious. It may also happen that we may lose some malicious packets being undetected but we save the computational time in a great extent than the actual HCIM Algorithm.

5. Implementation

The simulation has done by using *GlomoSim*(ver. 2.0) (Pandey & Fujinoki 2008) simulator using *CloudSim* (Buyya , Ranjan & Calheiros 2009) Toolkit to evaluate the performance of our proposed DDoS detection algorithm i.e Hop Count Inspection with Malicious Probability Rate (HCI-MPR)with results from the experiment and are compared to the traditional The Hop Count Inspection Method (HCIM) Algorithm. We tested our detection algorithm on a 2.67GHz processor, Windows environment.

6. About GlomoSim

GlomoSim (ver. 2.0) is a scalable simulation environment which is being designed using the parallel discrete-event simulation capability provided by Parsec. GlomoSim currently supports protocols for a wide variety of network. Most network systems are currently built using a layered approach that is similar to the OSI seven layer network architecture. The plan is to build GlomoSim using a similar layered approach. Standard APIs will be used between the different simulation layers. This will allow the rapid integration of models developed at different layers by different people. The goal is to build a library of parallelized models that can be used for the evaluation of a variety of wireless network protocols. The proposed protocol stack will include models for the channel, radio, MAC, network, transport, and higher layers.

7. Experimental Setup

Our simulation includes 2 source, 2 intermediate routers and 1 destination node .Out of which 2 source nodes 1 node is attacker and 1 node is a legitimate user. The bandwidth of legitimate traffic is set constant and the simulation of attack traffic is achieved by randomly generating many pairs of Constant Bit Rate (CBR). The various parameters for the simulation are as follows

1. Simulation Time 250 s
2. No of Nodes 10
3. Node Placement Uniform
4. Terrain Dimension 3000*3000 m^2
5. Noise Figure 20 db
6. Temperature 295k
7. Bandwidth 20kbps

The simulation has been done for various parameters as performance matrices which will be analyzed below.

7.1 Performance Evaluation

The proposed algorithm Hop Count Inspection with Malicious Probability Rate (HCI-MPR) is evaluated with the traditional Hop Count Inspection Method (HCIM) Algorithm on various performance parameters as

- Computation Time
- Detection Rate
- False Positive Rate

7.1.1 Computation Time

The one of the vital parameter of the performance evaluation is the computation time , which can be seen as a network performance factor. The wide variety of sample input is taken to analyze the proposed algorithm on the simulator.

7.1.2 Detection Rate

The other critical parameter of the performance evaluation is the detection rate. The detection rate will depend on the gravity of the DDoS attack, as some attacks can hamper the performance of the network to a great extent, so as to provide a mitigation approach for DDoS attacks, we have taken wide variety of sample input to analyze the proposed algorithm on the simulator for detection rate.

7.1.3 False Positive Rate

False Positive is the rate of *legitimate packets that are incorrectly detected as malicious* under the traffic. The rate is a vital measure of the performance of the proposed algorithm as it can be used to measure the effectiveness of the algorithm. While dealing with the DDoS attack some legitimate packets can go undetected and it can affect the system further in terms of low network performance and less availability of resources

8. Conclusion

Our works focus on Distributed Denial-of-Service (DDoS) attack which is considered one of the harmful attacks. For Cloud computing, which is emerging as a key technology of the future this attack had made the things crucial for the organizations which are providing their key service to the customers especially under Software as a Service (SaaS). This attack will harm the network within no time or without any prior knowledge which is providing servicers under SaaS. As this attack is very much harmful, so many defense mechanisms were developed to mitigate the attack to make the systems free form harm. The attack strategies are also of different types. They may need the help of network services or may not need to mitigate the attack. Till now so many network supported solution were proposed but proposals without the support of network were very rare. Traditionally HCIM (Hop count Inspection Method) method was there to mitigate the attack.

As the HCIM algorithm seems to be less effective for large data rates for mitigating DDoS attacks, hence we proposed an Analytical approach to work on these attacks. Then we proposed a algorithm **HCI-MPR** (Hop-Count Inspection with malicious probability rate) which made it possible to mitigate the DDoS attacks Effectively. We have compared the result of our approach with the result of HCIM method; we have collected the sample required for the attacks. The simulation results shows that our approach is taking less amount of time than the HCIM method in terms of computation time and also it could detect DDoS attacks more effectively as the detection rate of the proposed algorithm is much impressive than the traditional one.

9. Future Scope of Work

There are still several issues regarding the DDoS attacks on Cloud Computing environment that warrant further research as the existing network may connect multiple stub networks which could make a single IP address to appear and have multiple valid hop-counts at the same time ,

which further require enchantment in the our proposed algorithm HCI-MPR to check the credential of the sender for legitimate packets .Secondly we need a systematic procedure for setting the parameters according to the Cloud environment for our proposed algorithm so that it shows effective results against real spoofed DDoS traffics.

References:

1) Buyya Rajkumar, Yeoa Chee Shin, Venugopal Srikumar, Broberg James and Brandic Ivona (2009, pp 599-616) "*Cloud computing and emerging IT platforms: Vision, hype and reality for delivering computing as the 5thutility"* Future Generation Computer Systems Elsevier, Available online 11 December 2008.
2) Jensen Meiko, Schwenk Jorg, Gruschka Nils and Iacono Luigi Lo (2009) "*On Technical Security Issues in Cloud Computing"* IEEE International Conference on Cloud Computing.
3) Armbrust Michael, Fox Armando, Griffith Rean, Joseph Anthony D, Katz Randy H, Konwinski Andrew, Lee Gunho, Patterson David A, Rabkin Ariel, Stoica Ion and Zaharia Matei (2009) "*Above the Clouds: A Berkeley View of Cloud Computing"* Technical Report No. UCB/EECS-2009-28.
4) Greengard Samuel (2009) "Top 10 Trends in IT for 2009" , Baseline Online Magazine , published in CSI vol. no 33 , no 10 .
5) Kandukuri Balachandra Reddy, Paturi V Ramakrishna and Dr. Rakshit Atanu (2009) "*Cloud Security Issues*" IEEE International Conference on Services Computing.
6) Dikaiakos Marios D, Pallis George, Katsaros Dimitrios, Mehra Pankaj and Vakali Athena (2009) "CloudComputing-*Distributed Internet Computing for IT and Scientific Research*" IEEE Internet Computing .
7) Wang Cong, Wang Qian, Ren Kui and Lou Wenjing (2009) "*Ensuring Data Storage Security in Cloud Computing"* IEEE.
8) Xiong Kaiqi and Perros Harry (2009) "*Service Performance and Analysis in Cloud Computing*" Congress on Services – I , IEEE .
9) Buyya Rajkumar, Ranjan Rajiv and Calheiros Rodrigo N (2009) "*Modeling and Simulation of Scalable Cloud Computing Environments and the CloudSim Toolkit: Challenges and Opportunities"* IEEE.
10) Viega John (2009) "*Cloud Computing and the Common Man*" Computer , Published by the IEEE Computer Society .
11) Kumar Arun Raj and Selvakumar P. and S (2009) "*Distributed Denial-of-Service (DDoS) Threat in Collaborative Environment - A Survey on DDoS Attack Tools and Traceback Mechanisms*" 2009 IEEE International Advance Computing Conference (IACC 2009) Patiala, India.
12) Wu Qingtao, Zheng Ruijuan , Pu Jiexin and Sun Shibao (2009) "*An Adaptive Control Mechanism for Mitigating DDoS Attacks*" Proceedings of the IEEE International Conference on Automation and Logistics Shenyang, China.

13) Sachdeva Monika, Kumar Krishan, Singh Gurvinder and Singh Kuldip (2009)"*Performance Analysis of Web Service under DDoS Attacks"* 2009 IEEE International Advance Computing Conference (IACC 2009) Patiala, India.
14) Maciá-Fernández Gabriel, Díaz-Verdejo Jesús E and García-Teodoro Pedro (2009) "*Mathematical Model for Low-Rate DoS Attacks Against Application Servers*" IEEE Transactions On Information Forensics and Security, Published by the IEEE Computer Society 2009.vol. 4, no. 3.
15) Xinlei Li, Kangfeng Zheng and Yixian Yang (2009) "*A DDoS attack defending scheme based on network processor"* WASE International Conference on Information Engineering.
16) Xie Yi and Yu Shun-Zheng (2009) "*Monitoring the Application-Layer DDoS Attacks for Popular Websites*" IEEE/ACM Transactions on Networking, vol. 17, no. 1.
17) Liu Simon (2009) "*Surviving Distributed Denial-of-Service Attacks"* Computer.org/ITPro,
18) Published by the IEEE Computer Society.
19) Poroor Jayaraj and Jayaraman Bharat (2009) **"** *DoS Attacks on Real-Time Media through Indirect Contention-in-Hosts***"** IEEE Internet Computing Published by the IEEE Computer Society .
20) Ranjan Supranamaya, Swaminathan Ram, Uysal Mustafa and Nucci Antonio (2009) "*DDoS-Shield: DDoS-Resilient Scheduling to Counter Application Layer Attacks*" IEEE/ACM Transactions on Networking vol. 17, no. 1.
21) Gregory ,Conti and Ahamad Mustaque (2009) "*A Framework for Countering Denial-of-Information Attacks"* IEEE Security & Privacy , Published by the IEEE Computer Society.
22) Vouk Mladen A (2008, pp 23-26) "*Cloud Computing – Issues, Research and Implementations*" Proceedings of the ITI 2008 30th Int. Conf. on Information Technology Interfaces,Cavtat, Croatia.
23) Lin Zong, Guang-Min Li , Yang Hu Dan (2008) "*Global abnormal correlation analysis for DDoS attack detection*" IEEE .
24) Pandey Ashwini K., Fujinoki Hiroshi (2008) "*Study of MANET Routing Protocols by GloMoSim Simulator"*.
25) Wang Wei and Gombault Sylvain (2008) "*Efficient Detection of DDoS Attacks with Important Attributes"* Third International Conference on Risks and Security of Internet and Systems: *CRiSIS'2008.*
26) Khor Soon Hin and Nakao Akihiro (2008) "*sPoW: On-Demand Cloud-based eDDoS Mitigation Mechanism"IEEE* .
27) Bouzida Yacine and Cuppens Fr´ed´eric and Gombault Sylvain (2006) "*Detecting and Reacting against Distributed Denial of Service Attacks*" IEEE .
28) Jin Cheng, Wang Haining and Shin Kang G (2003) "*Hop-Count Filtering: An Effective Defense Against Spoofed DDoS Traffic" CCS'03*. ACM 1581137389/ 03/0010.

29) J. P. Anderson, *"Computer Security Threat Monitoring and Surveillance"*, Technical Report April 1980, http://csrc.nist.gov/publications/history/ande80.pdf
30) Denning, Dorothy E., "An Intrusion Detection Model" Proceedings of the Seventh IEEE Symposium on Security and Privacy, May 1986, pages 119–131
31) Sebring, Michael M., and Whitehurst, R. Alan., "Expert Systems in Intrusion Detection: A Case Study," The 11th National Computer Security Conference, October, 1988
32) Lunt, Teresa F., "IDES: An Intelligent System for Detecting Intruders," Proceedings of the Symposium on Computer Security; Threats, and Countermeasures; Rome, Italy, November 22–23, 1990, pages 110–121.
33) Lunt, Teresa F., "Detecting Intruders in Computer Systems," 1993 Conference on Auditing and Computer Technology, SRI International
34) Sarah Sorensen, "Protecting Your Network From Attacks" 2006.
35) J. P. Pereira, "A Strategy to Secure Network", 2006.
36) Dea-Woo Park, "A study about dynamic intelligent network security systems to decrease by malicious traffic" IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.9B, September 2006
37) Michael E. Locasto, Ke Wang, Angelos D. Keromytis, and Salvatore J. Stolfo, "FLIPS: Hybrid Adaptive Intrusion Prevention", 2006
38) Norbik Bashah, Idris Bharanidharan Shanmugam, and Abdul Manan Ahmed, "Hybrid Intelligent Intrusion Detection System" World Academy of Science, Engineering and Technology, pages 23-26, November 2006.
39) Karen Scarfone and Peter Mel, "Guide to Intrusion Detection and Prevention Systems" February 2007
40) Palak Agarwal, "TCP Stream Reassembly and Web based GUI for Sachet IDS" February 2007.
41) Supachai Tangwongsan, and Labhidhorn Pangphuthipong, "A Model of Network Security with Prevention Capability by Using Decoy Technique" World Academy of Science, Engineering and Technology, pages 184-189, November 2007.
42) http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf
43) HE XIAO DONG, "Automated Intrusion Prevention Mechanism In Enhancing Network Security" March 2008.
44) Jack TIMOFTE, "Intrusion Detection using Open Source Tools" Revista Informatica Economică VOL.2 (46), pages 75-79, 2008.
45) Rui Santos, "Intrusion Prevention with L7-Filter" GSEC Gold Certification August 2008.
46) Renuka Prasad.B, Dr.Annamma Abraham, Chandan. C, Prabhanjan.A, and AjayBilotia "Information Extraction for Offline Traffic" IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.9, pages 309-315, September 2008
47) U. Aickelin, J. Twycross and T. Hesketh-Roberts, "Rule Generalisation in Intrusion Detection Systems using SNORT" International Journal of Electronic Security and Digital Forensics (IJESDF), Vol. 2, pp.20–26, 2008.

48) technet.microsoft.com."http://technet.microsoft.com/en-s/library/dd632948.aspx." Retrieved 2009-09-10.
49) Intrusion detection system "http://en.wikipedia.org/wiki/Intrusion detection system", cited October 2009.
50) OSI model "http://en.wikipedia.org/wiki/OSI model", cited August 2009.
51) Whitman, Michael, and Herbert Mattord. Principles of Information Security. Canada: Thomson, 2009. Pages 290 & 301
52) Pereira J. P., "Comparison of Firewall, Intrusion Prevention and Antivirus Technologies" accessed 2009.
53) Ceilyn Boyd John Zao David Mankins, Rajesh Krishnan and Michael Frentz. Mitigating distributed denial of service attacks with dynamic resource pricing. *Proceedings of 17th Annual Conference on Computer Security Applications , 2001. ACSAC 2001*, pages 411-421, 2001.
54) Xinzhou Qin Wenke Lee Ravi K. Prasanth B. Ravichandran Joao B. D. Cabr- era, Lundy Lewis and Ramon K. Mehra. Proactive detection of distributed denial of service attacks using mib tra±c variables - a feasibility study. *Integrated Network Management Proceedings*, pages 609-622, 2001.
55) John C. S. Lui David K. Yau and Feng Liang. Defending against distributed denial of service attacks with max-min fair server-centric router throttles. *2002 Tenth IEEE International Workshop on Quality of Service*, pages 35-44, 2002.
56) Guangsen Zhang and Manish Parashar. Cooperative defence against ddos attacks. *Department of Electrical and Computer Engineering, The State University of New Jersey*, February 2006.
57) S. Specht and R. Lee. Taxonomies of distributed denial of service networks, attacks, tools, and countermeasures. *Technical Report CE-L2003-03*, 164, May 2003.