International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 4 Issue 1 –DECEMBER 2013.

Detecting DDoS Attack by Monitoring Outgoing Messages

G.Kavitha [#1], S.Yuvaraj [*2]

[#] *Professor & Head, Department of CSE, Excel Engineering College, Komarapalayam, TamilNadu, India.*

[*] *Assistant Professor, Department of CSE, Excel Engineering College, Komarapalayam, TamilNadu, India.*

[1]hod_cse_eec@yahoo.in

Abstarct:-In the internet nowadays the security attacks are spread by the compromised machines. The compromised machines are nothing but the computers that spreads these security attacks which includes spamming, spreading malware, DDoS and identity theft. Among these security attacks spamming leads to more number of compromised machines which has been detected by using spam zombies. The spam zombies uses a detection algorithm named SPOT which detects the spam content present or not by monitoring outgoing messages in a network. The existing system has been developed in a way by improving the performance of SPOT by detecting virus/worm attachment. Semantic aware statistical (SAS) algorithm is used to detect virus/worm attachment present in the message. By using these two detection algorithms SPOT, SAS only the compromised machines involved in spamming and spreading malware has been detected. The machines which involved in the DDoS, most probably occurs in the Wireless Mobile Ad-hoc networks where the problem takes place in both of its routable networking environment and in wireless sensor networking. The main aim of this paper is to overcome by seeing the effect of DDoS in routing load, packet drop rate, end to end delay. In addition to these parameters a secure IDS system is developed to detect this kind of attack and the developed IDS system will helps to block the effects of DDoS. The evaluation shows that in addition to the existing system the proposed system is efficient and effective of detecting compromised machines in a network.

Keywords: spot, sas, spam zombies

I. INTRODUCTION

The existence of compromised machines in the internet is the major security challenge on the internet nowadays. These compromised machines are increasing rapidly and used to launch launch various security attacks including spamming, spreading malware, DDoS, and identity theft . At the same time, identifying and cleaning of those machines in a network remain a challenge for system administrators of networks of all sizes. This paper focuses on the detection of the compromised machines in a network that are involved in DDoS attacks. The existing system has detected that spamming provides a critical economic incentive for the controllers of the compromised machines to recruit these machines and it has been analysed many compromised machines are involved in spamming. To overcome this spamming existing system has developed a spam zombie detection algorithm commonly called as SPOT.SPOT is developed based on statistical method called Sequential Probability Ratio Test (SPRT) which separates the compromised versus the machine is not compromised by monitoring outgoing messages in a network.

By introducing the SPOT algorithm the machines involved in spamming has been identified, in the similar way the machines involved in virus/worm attachment also detected. In this case the existing system uses a powerful algorithm because computer worm is a great threat to modern network security despite various techniques that have been proposed up to date. To provide security to those worms spreading out over Internet,pattern based signatures have been widely adopted in many network intrusion detection system but all signature-based techniques are facing fundamental countermeasures. In order to generate high quality signatures of such worms, SAS, a novel Semantics Aware Statisticalalgorithm is proposed that generates semantic aware signatures automatically and it involves a signature matching process. The developed signatures will be used to matching the upcoming packets whether they have virus/worm attachment.

II. RELATED WORK

The proposed work is also based on the detection of compromised machines that involved in DDoS attacks. In most cases the these types of attacks will occur in Wireless Mobile ad-hoc network (MANET) which is emerging technology that has a great strength in commercial applications such as building, traffic surveillance. MANET does not contain any centralized controller and also each node contain routing capability, in which the devices in MANET is independently free to move in any direction that change its connections to other devices frequently. Because of no central controller exists the major challenges wireless mobile ad-hoc networks face today is security. MANET has a routable networking environment on top of a link layer ad hoc network in which it is a type of a wireless ad hoc network and also also contains wireless sensor network in which MANET faces the problems faced by sensor network. There are many security

attacks in MANET and DDoS (Distributed denial of service) is major threat that includes routing load, packet drop rate, end to end delay.

The related work is developed in a way which will provide security to these types of DDoS attacks by using an intrusion detection system. IDS is developed which can able to detect the attacks without prior knowledge of any type of attacks by using two types of intrusion detection systems.

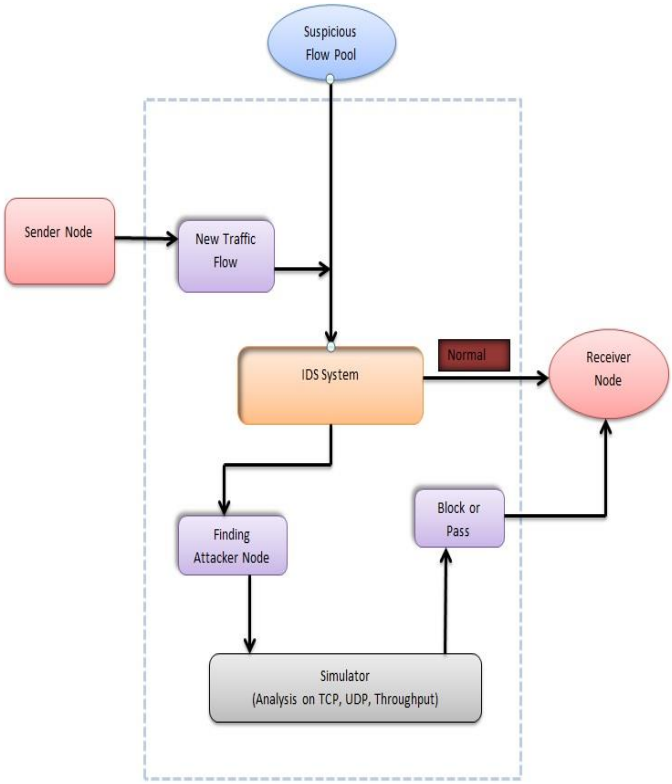

Figure.1 System Architecture

III. SYSTEM IMPLEMENTATION

The increasing popularity of electronic mail service helps us to communicate with each other and can able to share the resources. At the same time several people and companies found it an easy way to spread a massive amount of unsolicited messages and also it provide virus/worm attacks and DDOs attacks to users at a very low cost.These unwanted bulk messages or junk emails are called spam messages. The majority of spam messages has been found by using SPOT detection system. SPOT is designed based on a powerfulstatisticaltoolcalledSequentialProbabilityRatioTest,which has bounded false positive and false negative error rates.

In the similar way the spreading of virus/worms has also been detected by using the SAS worm detection system. SAS places between the pattern-based signatures and the semantic-derived detection methods which balances between security and the signature matching speed. SAS is more robust than most pattern-based signatures, sacrificing little speed in signature matching that uses SAS scheme in which the number of compromised machines detection has been increased. By using these SPOT and SAS detection systems the compromised machines that spreads spam and virus/worm has been identified. At the same the machines spreading the DDOs must be identified in order to detect more number of compromised machines in the network. To monitor the machines involved in the DDOs Intrusion detection must be needed. This can be categorized into two models:

1. Signature-based intrusion detection
2. Anomaly-based intrusion detection

The benefits of this IDS technique are it can be able to detect attack without prior knowledge to the attacker. Intrusion attack is very easy in wireless network as compare to wired network but one of the serious attacks to be considered in ad hoc network is DDoS attack. To overcome the DDoS, should use multiple nodes and simulations should be done through different criteria such as NORMAL, DDoS and IDS (intrusion detection case). The normal case is that number of sender and receiver nodes and transport layer mechanism should be set. It includes the mechanism as TCP and UDP with routing protocol such as AODV (ad-hoc on demand distance vector) routing. After setting all parameter simulate the simulator is used to analyse the results. In the IDS (Intrusion detection system) one node is set as IDS node, which node watch the all radio range mobile nodes.Once the abnormal behavior comes to the network, it first check the symptoms of the attack and find out the attacker node. Then by using the attacker node path it block the attacker node. IDS block the attacker node which will remove from the DDOS attack. In our simulation result we performed some analysis in terms of routing load , UDP analysis , TCP congestion window, Throughput Analysis and overall summery.

MODULES

4.1 User Registration

In this module, user registers his/her personal details in database. Each user has unique id, username and password and digital signature. After using these details he can request file from server.

4.2 Upload & Send files to users

In this module, server can upload the files in the database. After verify user digital signature file could be transfer to correct user via mobile ad-hoc network.

4.3 Attack on Ad-Hoc Network

In this module, to see what the attack on ad-hoc is network is Distributed Denial of Services (DDoS). A DDoS attack is a form of DoS attack but difference is that DoS attack is performed by only one node and DDoS is performed by the combination of many nodes.

All nodes simultaneously attack on the victim node or network by sending them huge packets, this will totally consume the victim bandwidth and this will not allow victim to receive the important data from the network.

4.4 Criteria for Attack detection

In this module, we use multiple nodes and simulate through different criteria are NORMAL, DDoS and IDS (intrusion detection case). Normal Case We set number of sender and receiver nodes and transport layer mechanism as TCP and UDP with routing protocol as AODV (ad-hoc on demand distance vector) routing. After setting all parameter simulate the result through our simulator.

4.5 IDS Case

In IDS (Intrusion detection system) we set one node as IDS node, that node watch the all radio range mobile nodes if any abnormal behavior comes to our network, first check the symptoms of the attack and find out the attacker node , after finding attacker node, IDS block the attacker node and remove from the DDOS attack. In our simulation result we performed some analysis in terms of routing load , UDP analysis , TCP congestion window, Throughput Analysis and overall summery.

4.6 Simulation Results

In this module, we implement the random waypoint movement model for the simulation, in which a node starts at a random position, waits for the pause time, and then moves to another random position with a velocity.

a. Throughput
b. Packet delivery fraction
c. End to End delay
d. Normalized routing load

IV. RESULTS

An effective intrusion detection system is developed which is set by monitoring outgoing messages in a network. IDS was designed based on a simple and powerful statistical tool which detects the compromised machines that are involved in the DDoS attacks. The benefits of this IDS technique are it can be able to detect attack without prior knowledge to the attacker. Intrusion attack is very easy in wireless network as compare to wired network but one of the serious attacks to be considered in ad hoc network is DDoS attack. To overcome the DDoS, should use multiple nodes and simulations should be done through different criteria such as NORMAL, DDoS and IDS (intrusion detection case). The normal case is that number of sender and receiver nodes and transport layer mechanism should be set. It includes the mechanism as TCP and UDP with routing protocol such as AODV (ad-hoc on demand distance vector) routing. After setting all parameter simulate the simulator is used to analyse the results. In the IDS (Intrusion detection system) one node is set as IDS node, which node watch the all radio range mobile nodes.Once the abnormal behavior comes to the network, it first check the symptoms of the attack and find out the attacker node. Then by using the attacker node path it block the attacker node. IDS block the attacker node which will remove from the DDOS attack. In our simulation result we performed some analysis in terms of routing load , UDP analysis , TCP congestion window, Throughput Analysis and overall summery.

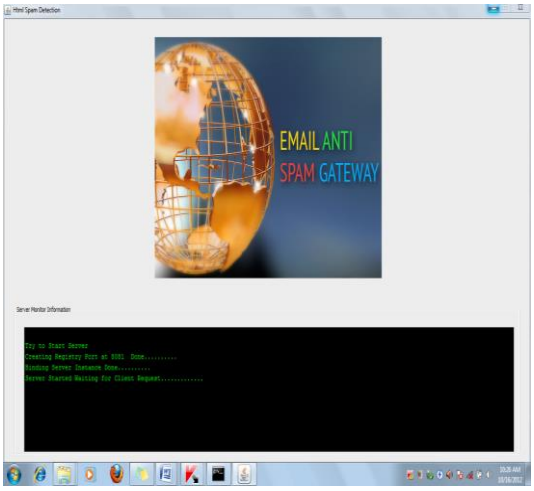

Figure 2. Server

The above Fig 4.1 represents the server in which all the operation performed will be displayed such as user account creation, compose mail, received mail etc. Even the operation such as attachment details will also be denoted in the server during the compose mailprocesstakesplace.Theselistmaystoredintheintrusiondetecti ngsystem which will uses it for collecting the details about the senders details such as IP address and the details about the amount of data send.

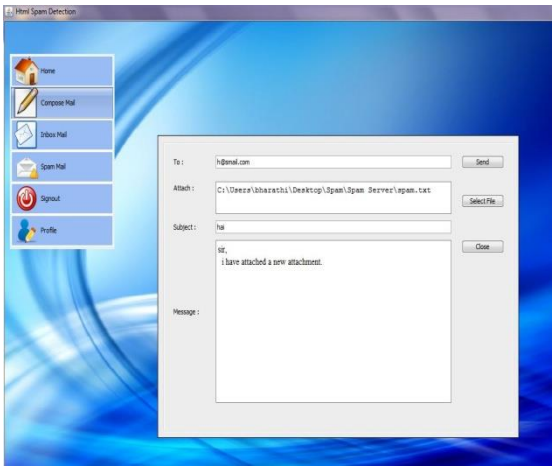

Figure 3. Compose Mail Process

The above Fig 4.2 may contains login form in which it isused to login using their username and password which will verify for the account details and will login into their account. The new users can also able to have an account by signup processin which the users can have an new account. As the login happen the entry into the homepage appears. The process such as compose mail takes place in which the mail has been composed. Once the mail composed the intrusion detecting system will indicate that it is attacker mail or normal mail.

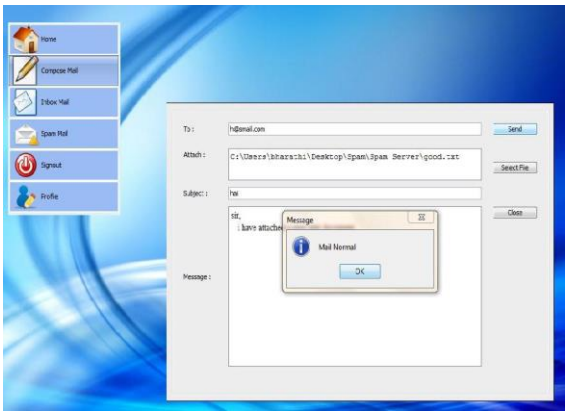

Figure 4. Normal Mail

The front page may contains login form in which we used to login using their username and password which will verify for the account details and will login into their account. Then new users can also able to have an account by signup processin which the users can have an new account. As the login happen the entry into the homepage appears. The process such as compose mail takes place in which the mail should be composed. Once the mail composed the intrusion detecting system will indicate that it is attack mail or normal mail. In the above process it shows that the composed mail is normal and don't contain any attacker node.

V. REFERENCES

[1] Duncan, C., Jacky, H., Kevin, M., & Joel, S: Catching Spam Before It Arrives: Domain Specific Dynamic Blacklists, Proceedings of the 2006 Australasian Workshops on Grid Computing and E-research, Hobart, Tasmania, Australia,. pp. 193-202. (2006)

[2] The Spam Problem and the Brightmail Filtering Engine Technical White Paper, Brightmail Anti-Spam Enterprise Edition Version 5.5.

[3] Liang, L.: A comparison of email filtering techniques, Master Thesis, Dalhousie University. (2005)

[4] Rejeb, J., Le, T. T., &Anand, N.:High Speed and Reliable Anti-Spam Filter‖, Proceedings of IEEE International Conference on Software Engineering Advances (ICSEA2006), Tahiti, French Polynesia, October 29 - November 3, 2006, (ISBN 0-7695-2703-5) pp. 66-66. (2006).

[5] Delany, S. J., & Derek, B.: Catching the Drift: Using Feature Free Case-based Reasoning for Spam Filtering, In: R Weber & M. Richter (eds.) Case-Based Reasoning Research and Development, Procs of the 7th International Conference on Case-based Reasoning (ICCBR 2007), pp. 314-328. (2007)

[6] Yong Tang and Shigang Chen: An Automated Signature-Based Approach against Polymorphic Internet Worms, ieee transactions on parallel and distributed systems, vol. 18, no. 7, july .(2007)

[7] Kumar Simkhada, TarikTaleb, Yuji Waizumi, Abbas Jamalipour, Nei Kato, and Yoshiaki Nemoto: An Efficient Signature-Based Approach for Automatic Detection of Internet Worms over Large-Scale Networks.

[8] Zhichun Li MananSanghi Yan Chen Ming-Yang Kao Brian Chavez:Hamsa: Fast Signature Generation for Zero-day Polymorphic Worms with Provable Attack Resilience, Northwestern University Evanston, IL 60208, USA flizc,manan,ychen,kao,cowboyg@cs.northwestern.edu.

[9] James Newsome, Brad Karp, Dawn Song:Polygraph: Automatically Generating Signatures for Polymorphic Worms

[10] Deguang Kong, Yoon-Chan Jhi, Qihe Pan, Sencun Zhu, Peng Liu, and Hongsheng Xi: SAS: Semantics Aware Signature Generation for PolymorphicWorm Detection

[11] J.P. John, A. Moshchuk, S.D. Gribble, and A. Krishnamurthy, "Studying Spamming Botnets Using Botlab," Proc. Sixth Symp. Networked Systems Design and Implementation (NSDI '09), Apr. 2009.

[12] J. Jung, V. Paxson, A. Berger, and H. Balakrishnan, "Fast Portscan Detection Using Sequential Hypothesis Testing," Proc. IEEE Symp. Security and Privacy, May 2004.

[13] J. Klensin, "Simple Mail Transfer Protocol," IETF RFC 2821, Apr. 2001.

[14] J. Markoff, "Russian Gang Hijacking PCs in Vast Scheme," The New York Times, http://www.nytimes.com/2008/08/06/technology/06hack.html, Aug. 2008.

[15] P. Wood et al., "MessageLabs Intelligence: 2010 Annual Security Report," 2010.