RESEARCHERID
THOMSON REUTERS

ISSN: 2277-9655
[Tajer* *et al.*, 6(8): August, 2017] Impact Factor: 4.116
IC™ Value: 3.00 CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

DETECTION OF FLOODING ATTACKS ON MOBILE AGENTS USING SKETCH TECHNIQUE AND DIVERGENCE MEASURES

Jean Tajer, Mo Adda[*1] & Benjamin Aziz[2]
[*1&2]University of Portsmouth, School of Computing, Portsmouth, United Kingdom

DOI: 10.5281/zenodo.839137

ABSTRACT

This paper deals with detection of SYN flooding attacks which are the most common type of attacks in a Mobile Agent World. We propose a new framework for the detection of flooding attacks by integrating Divergence measures over Sketch data structure. The performance of the proposed framework is investigated in terms of detection probability and false alarm ratio. We focus on tuning the parameter of Divergence Measures to optimize the performance. We will evaluate the performance of the proposed divergence measure via the receiver operating characteristic. Our analysis results prove that our proposed algorithm outperforms the existing solutions.

KEYWORDS: Mobile Agents, SYN flooding, Divergence Measures, Threshold, Sketch Technique.

I. INTRODUCTION

The traditional technique used in most distributed applications including the Internet, is the client-server approach. This approach involves, a client which is normally a system that relies on the services located on a remote system that is referred to as a server. Servers are usually more powerful than clients and provides mechanisms for clients to access their resources [19]. Clients usually access the resources on servers by using message passing or remote procedure call. However, as the demand of these applications and the number of users who wish to do using wireless and portable devices increases significantly, it was realized that the traditional client-server approach was lacking in terms of bandwidth use and server flexibility, load balancing, availability. In order to solve the inadequacies of the client-server approach, a new paradigm is needed which is the use of mobile agents [33].

Mobile agents are software that can migrate from nodes to nodes in a computer network and perform a computation on the behalf of the user. It has a unique ability to transport itself from one system in a network to another. Mobile agent are considered autonomy, active, mobility, goal oriented and communicative [32]. As a result of these unique properties, mobile agent systems usually benefit from the following: reduction in network load, improvement in network latency, asynchronous execution, protocol encapsulation, dynamic adaptation, fault-tolerance and robustness. Mobile agents work in conjunction with a mobile agent platform which provides appropriate execution environment for the mobile agent. This platform needs to be available at each potential host willing to entertain a visiting mobile agent. In this thesis all the background information on the concept of mobile agent is given.

Many Mobile Agent platforms have been developed during the last decade. The platforms have been programmed using different programming languages such as Java, TCl, C/C++ and other miscellaneous codes. Some of these platforms have been developed for commercial purposes and others for research [19]. In our research, we will use the Aglet platform to design our model and to test the real behavior of the Mobile Agent in the network area.

However, one of the main technical concern of the mobile agent is security. Sander and Tschudin raised two types of security problems that need to be solved. The first is host protection against malicious agents. The second is agent protection against malicious hosts. Many techniques have been developed for the first problem, such as access control, password protections, sand boxes etc. But the second problem appears to be difficult to solve. This paper will discuss how to detect the anomalies on a mobile agent network.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

The rest of this paper is organized as follows. Related work is provided in Section 2. Section 3 provides the security issues that a Mobile Agent can counter while visiting another host in the network. We will discuss about Sketch data structure which it will provide grained analysis and to derive probability distributions and we will introduce a dynamic threshold to differentiate network anomalies from normal behavior in Section 4. Section 5 describes our proposed approach design. In Section 6, we present our experimental works and check the capability, reaction and performance of the mobile agents based on the developed design and will evaluate the performance of the measure divergence via the receiving operating characteristic (ROC). Finally in Section 7, we present the conclusion and our future work.

II. RELATED WORK

From one side several researches have been proposed security solutions to detect and prevent attacks in real traffic. Most of these proposed solutions emphasize on many different detection and prevention strategies.

SYN flooding attack detection has been an interested issue for security researchers. The authors in [2] present the effects of correlation analysis on the DDoS detection. They propose a covariance analysis method for detecting SYN flooding attacks.

Authors in [7] compare two different algorithms (CUSUM and adaptive threshold) for the detection of SYN flooding attack. They conclude that CUSUM performs better then adaptive threshold in terms of detection accuracy of low intensity attacks. However, both of these algorithms face problems of false alarm ratio under normal IP traffic variation.

Sketch data structure uses the random aggregation for more grained analysis than aggregating the whole traffic in one time series. It has been used to summarize monitored traffic in a fixed memory, and to provide scalable input for time series analysis. Authors in [8] propose the use of CUmulative SUM (CUSUM) over the sketch for network anomaly detection.

Authors in [10] apply Chi-square on Sketch data structure, in order to detect divergence between current and previous distributions of the number of SIP INVITE request. In fact, Chi-square must be near zero when probability distributions are similar, and it increases up to one whenever the distributions diverges (e.g. under Invite flooding attacks). In addition, they used the dynamic threshold proposed in [11] during their experimental analysis.

From other side, several researches have been conducted over mobile Agents.

Some studies concentrate their work on the fault tolerance techniques in mobile agents, network management applications based on mobile agent technologies and how the fault tolerance techniques can improve their performance [25], [26].

In addition, some works have been performed to integrate the mobile agents with the e-commerce. Some technical relevant issues are well presented [28], [29], [30].

Some researches concentrated their work on security concerns (i.e denial of service, alteration, masquerading) of mobile agents and how to protect them by several techniques like obfuscated code, trusted hardware, mutual itinerary record, , path histories and State Appraisal [21], [22],[23],[24]. However, these techniques present several drawbacks like decrease the efficiency and performance of mobile agents, provide some complicated and large code that increase the latency of the network.

Our research combines the mobile agents and the detection methods. It emphasizes on how a mobile agent can detect a flooding attacks. We develop a general framework that increases the detection accuracy and reduces the false alarm by integrating divergence measure over Sketch technique in a Mobile Agent world.

III. MOBILE AGENTS SECURITY THREATS AND COUNTERMEASURES

Security is one of the key factors of MAS. In fact, a MA is one of the potential threats to computer systems and vice versa, from the host system to the MAS itself. In this part, we will talk about the main security issues related to MAS.

The security threats for MASs could be divided as follows:

- Eavesdropping: The classical eavesdropping threat involves the interception and monitoring of secret communications. The threat of eavesdropping, however, is further exacerbated in mobile agent systems because the agent platform can not only monitor communications, but also can monitor every instruction executed by the agent, all the data it brings to the platform, and all the subsequent data generated on the platform. Since the platform has access to the agent's code, state, and data, the visiting agent must be wary of the fact that it may be exposing proprietary algorithms, trade secrets, negotiation strategies, or other sensitive information. Even though the agent may not be directly exposing secret information, the platform may be able to infer meaning
- Alteration: The final form of attack by a host on an agent is the alteration of the agent. The host can alter an agent by changing the data, code and control flow. A malicious host may try to change the code of an agent so that the agent performs other tasks than were intended by its creator. A host may also try to change the data contained in the agent.
- Denial of Services: A host may deny an agent a specific service provided by the host. It is possible for a host to both intentionally and unintentionally deny an agent a service. A host may deny an agent service so that the agent is not able to complete its task. Another possible attack is the host could terminate the agent altogether. Furthermore, a host may deny a request from an agent on a time-sensitive task so that the agent is unable to complete its task in its allotted time.
- SYN flood attack: it consist on sending many TCP connection requests to a target. This latter will accept the establishment of the connection and notify the client. Except that, this one will never use them. Thereby, the server will be drown by unused connections and, eventually, will not reply to legitimate users requests.

There are many security services that can be used for securing the agents systems.

- Authentication, the host needs to know the sender of the delivered agent. The agent authentication process includes verifying the entity that programmed the agent and also verifying the entity that forwarded it to the host. The agent and the host need to know with whom they are talking and dealing with, here the encryption or credentials can be used.
- Integrity, checking the integrity of the agents is a technique that makes sure no one has made any changes to the agents, the agents travelling form on host to another, and communicates and exchanges their data with other hosts and other agents.
- Authorization, the incoming agents should have a specific right to access the host information, so different agents have different authority, to protect the hosts and also to protect themselves.

For simplicity, we are going in this article to focus on the SYN flooding attacks and see how the mobile agents will act against these anomalies.

IV. BACKGROUND

Sketch technique

In this section, we review the K-ary Sketch data structure. Using Sketch data structure makes our framework flexible and scalable for grained analysis. No matter how many flows exist in the traffic, Sketch generates fixed-number of time series [3], [4] for anomaly detection. Sketch provides more grained analysis than aggregating whole traffic in one time series.

The Sketch data structure is used for dimensionality reduction. It is based on random aggregation of traffic attribute (e.g. number of packets) in different hash tables. A Sketch S is a 2D array of H × K cell (see Fig.1), where K is the size of the hash table, and H is the number of mutual independent hash functions (universal hash functions). Each item is identified by a key κn and associated with a reward value νn. For each new arriving item (κn, νn), the associated value will be added to the cell S[i][j], where i is an index used to represent the hash

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

function associated with ith hash table ($0 \leq i \leq d-1$), and j is the hash value ($j = hi(\kappa n)$) of the key by the ith hash function.

Data items, whose keys are hashed to the same value, will be aggregated in the same cell in the hash table, and their values will be added up to existing counter in the hash table. Each hash table (or each row) is used to derive probability distribution as the ratio of the counter in each cell to the sum of whole cell in the line. The derived probability distributions (we get K probability set, one per line) are used as inputs for divergence measures

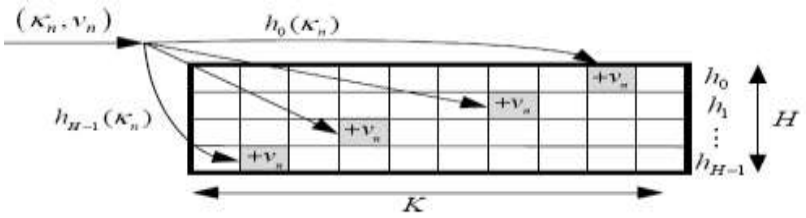

Fig. 1. Sketch Data structure

Threshold

In order to differentiate network anomalies from normal behavior on the mobile agent, the use of a detection threshold for Power Divergence (PD) is mandatory. Instead of using a static threshold, we use a dynamic one: Jacobson Fast algorithm for RTT (Round - Trip Time) mean and variation [15], [18]. Let PD(n) be the current value of the Power Divergence. PD(n) and PD(n+1) are respectively the current and next exponentially smoothed average estimates of Power Divergence. Let σ(n) be the deviation between the current Power measure PD(n) and the average measure $\bar{}$PD(n). The exponentially smoothed average of σ(n) is denoted by $\bar{\sigma}$ (n). The estimated threshold h(n+1) is then given as follows:

$$\bar{}PD(n+1) = (1-\alpha)\ x\ \bar{}PD(n) + \alpha\ x\ PD(n) \quad (1)$$

$$\alpha(n) = |\bar{}PD(n) - PD(n) \quad (2)$$

$$\bar{}\sigma(n+1) = (1-\alpha)\ x\ \bar{}\sigma(n) + \alpha\ x\ \sigma(n) \quad (3)$$

$$h(n+1) = \lambda\ x\ \bar{}PD(n+1) + \mu\ x\ \bar{}\sigma(n+1) \quad (4)$$

Where α, λ and μ are all tunable parameters that can be adjusted numerically in order to improve the detection accuracy.

V. PROPOSED APPROACH

The approach used in this paper to detect the DDoS attacks is based on probabilistic decision measure. In fact, the idea is to estimate the subjective prior distribution of the mobile agent traffic and to use it as a baseline probability. This probability distribution is denoted by q = [q1……. qw]. In presence of attacks over the mobile agent network, the probability distribution changes. One can use this change to detect the attacks. However, with the traffic variations, this probability distribution changes also even in the absence of attacks. This is called false alarms/attacks. The objective then is to find a method that detects the attacks and remove the false alarms. This motivates the need for a quantitative measure of information or more generally a decision theoretic measure of divergence between the basic probability q and some other distribution p. Power Divergences are generalizations of this decision measure and are associated with strictly convex functions.

The Power Divergence has been first defined in [7] and equivalent variants (up to a scale factorβ) of this divergence are discussed in [35]. The divergence measure is therefore the decision measure that generalizes the Kullback-Leibler measure and Hellinger distance to a broad class of divergence of orderβ. In fact, the Power

Divergence is a measure of distance between two probability measures of order β given as follows:

$$PD\ (P||Q) = \frac{\sum_{i=1}^{w} Pi\ (Pi/Qi)^{\beta-1} - 1}{\beta\ (\beta - 1)} \quad (5)$$

Where P is the posterior probability distribution and Q is the prior probability distribution. This divergence presents some interesting special cases. For β = 0.5, this divergence is 4 x HD (P || Q) [36], and for β = 2 it is

equal to 0.5 x $\chi 2$ (P || Q) divergence. Obviously, this power divergence outperforms then the existing solutions: HD and $\chi 2$ (some results will be provided later in the paper).

In fact, by changing the values of β, one can optimize the detection of attacks compared to Chi-Square and HD. In our experiments described later, we will show numerically that for different values of β, the detection efficiency changes. The optimal value of β can then be obtained.

P and Q are derived from the Sketch data structure in two consecutive discrete intervals. Firstly, the shared counters of the sketch are continuously updated from ongoing traffic during a time interval T. At the end of each interval, the probability Pi,j is calculated as the ratio of each counter to the sum of the whole counters in one hash table:

$$\text{Pi, j} = \frac{\text{S [i][j]}}{\sum_{j=1}^{w} \text{S [i][j]}} \qquad (6)$$

We obtain d probability distributions in each interval (P1 ……Pd), where Pi is the distribution (P1 ….Pd) resulted from the i^{th} hash table. Qi is the probability distributions resulted from previous interval. The probability distributions of Qi is calculated in the same manner as Pi (Eq. 5).

When the Power Divergence is larger than dynamically updated threshold, we raise an alarm. However, Power Divergence induces only two spikes (at the start and at the end of attack). As we want to continuously raise alarms for whole duration of the attack, the distribution Qi will stop sliding by keeping its value until the end of the attack. However, with the variations of normal traffic, and the similarity of DDoS attacks with flash crowd, we suppose that flooding attacks will span for many intervals, in contrast to flash crowd and normal variation. Thus reduce the false alarms. Therefore, we will trigger an alarm only if the deviation lasts more than Δ intervals.

VI. EXPERIMENTAL WORKS

In this section, we present the performance analysis results for integrating divergence measures over Sketch, for detecting SYN flooding attacks in a mobile agent network.

For the sake of simplicity, we focus our analysis on the detection of TCP SYN flooding attacks, as it is the widely used attack for DDoS in these days.

Dataset

The following techniques and tools are used: Two workstations with 8 GB and 768 MB of RAM respectively, which run Windows Server 2003 and a number of Mobile Agents are used.

We have considered the above describe mobile agents will have to execute the similar path. To measure the capability of the proposal towards eavesdropping threat, a test environment is set up using the above mentioned computers (see Fig. 2). Computer A is considered to act as trusted server (TS) and computer B runs many host nodes simulated through various port numbers as well as the home node in a virtualized mode. Ethereal will be running regularly over computer A. its job is to collect packets in the mobile agent network and store them for a period of 4h00 from 18/03/2017 08h30 to 12h30. These traces are used to test the efficiency of divergence measures. IP addresses in the traces are scrambled by a modified version of tcpdriv tool, but correlation between addresses are conserved. We analyze these 8h30 traces using Sketch data structure, with a key of the Sketch (κn = DIP), and a reward vn = 1 for SYN request only, and vn = 0 otherwise. We set the Sketch width K to 1024, and the number of hash H to 5.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

Fig. 2. Experimental Lab

Afterward, we inject 12 real distributed SYN flooding attacks with different intensity inside this trace. These attacks are inserted each 30 minutes (on instants t=20, 50, 80, 115,145,170, etc.) and span for 10 minutes. These different intensity attacks are shown in Figure 4. The first attack begins with a value of 900 SYN/min and decreases until 280 SYN/min.

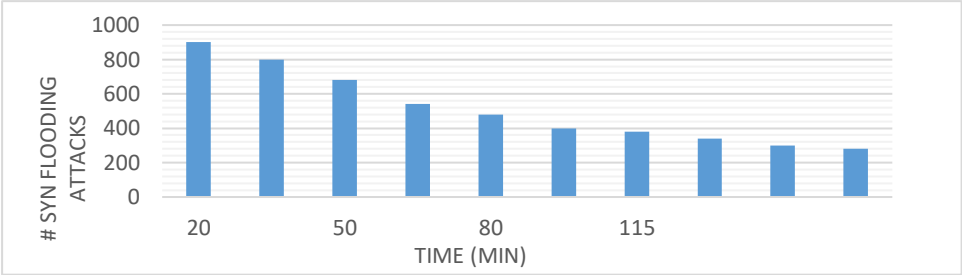

Fig. 3. SYN flooding Attacks

Fig. 4 & Fig. 5 show the variation of total number of mobile agents' packets before and after the injection of SYN flooding attacks. By comparing these variations, we might not notice the differences between both figures without deep inspection. Inserted attacks don't induce heavy deviations in the time series of the total number of SYN requests. This can be explained by the fact that the intensity of SYN flooding attacks is not large compared to the intensity of the total number of SYN segments. In such cases, the detection of attacks is very challenging, because no heavy changes in the time series describing the variations of the total number of SYN, and the intensity of the SYN flooding attacks is buried by the large number of SYN (see Fig. 3) before attacks injection.

Evaluation Strategy

In this section, we present the evaluation results of the application of these divergence measures on the mobile agent IP traces.

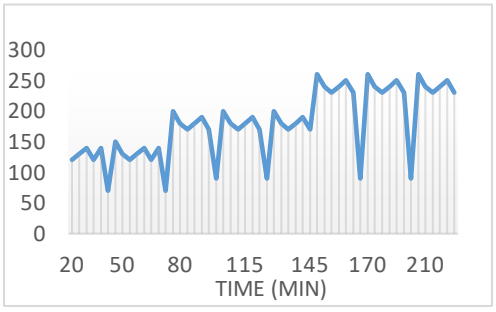

Fig. 4. Total number of mobile agents' packets

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

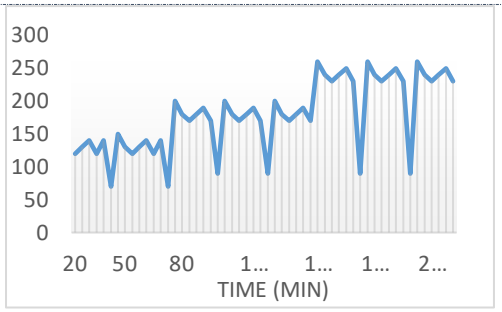

Fig. 5. Total number of mobile agents' packets after SYN flooding attacks injection

We will focus our study on the Power Divergence. Due to space limitation, we provide in this section, the results for only two values of β = 0.5 and 2.

The value of β = 0.5 makes the Power Divergence (PD) proportional to Hellinger Distance (HD).

Fig. 6 shows the variation of Power Divergence for β = 0.5 with the dynamic threshold given in Equation 5. Power Divergence is able to detect all the SYN flooding attacks but with 4 false alarms.

For the value of β= 2, Fig. 7 shows the variation of Power. We can notice that via this value of β, all the attacks have been detected (100%) with only 1 false alarm.

The intensity of spike is proportional to the intensity of the attack.

We conclude that the value of β= 2 outperforms β = 0.5 in terms of true detection and false alarm rate.

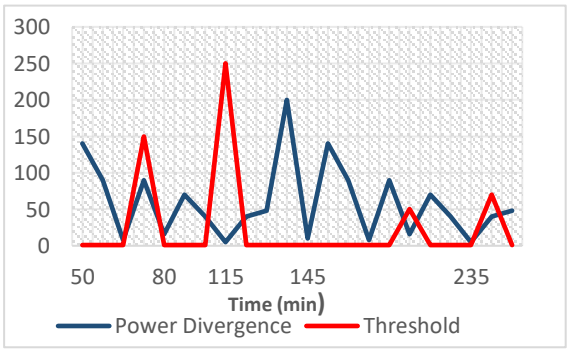

Fig. 6. Power Divergence for β=0.5

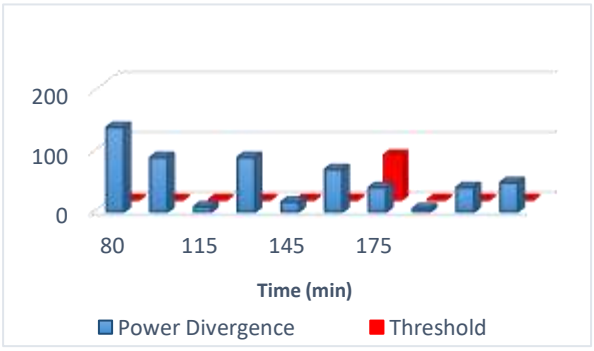

Fig. 7. Power Divergence for β= 2

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

Receiver Operating Characteristic (ROC)

To evaluate the performance of Power Divergence with different value of β, we investigate the detection rate and the false alarm rate. Receiver Operating Characteristic (ROC) is used for accuracy analysis when varying the value of the threshold h. ROC curve shows the variation of the true positive (Eq. 7) in term of false alarm rate (Eq. 8):

$$DR = \frac{\text{TP}}{\text{TP} + \text{FN}} X\ 100 \qquad (7)$$

Where TP is the number of true positive alerts, and FN is the number of false negative. The false alarm rate is defined as the ratio of false alarms to the number of raised alarms:

$$FAR = \frac{\text{TP}}{\text{TP} + \text{FP}}\ X\ 100 \qquad (8)$$

For β = 0.5, ROC curve is presented in Fig. 8, where PD can achieve a detection rate of 100% with 43% of false alarm.

The ROC for β = 2 is presented in Fig. 9, where PD achieves a detection rate of 100% with 10% of false alarm. The comparison between the two curves shows that PD accuracy increases when increasing the value of β.

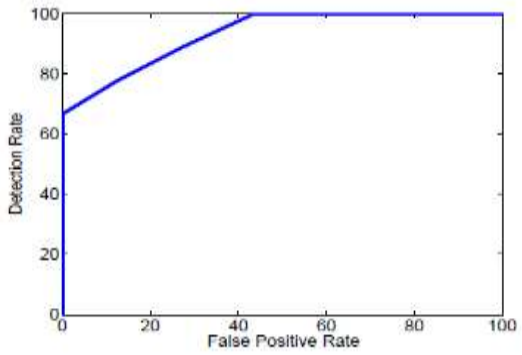

Fig. 8. ROC for Power Divergence for β= 0.5

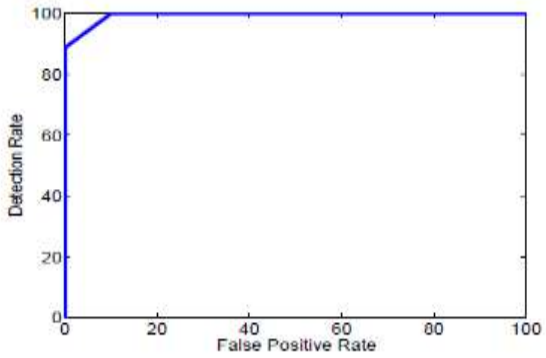

Fig. 9. ROC for Power Divergence for β= 2

VII. CONCLUSIONS

In this paper, we proposed a new framework based on Sketch and Divergence Measures for anomaly detection on a mobile agents network. The proposed approach evaluated on real traces with DDoS SYN flooding attacks. We compared the performances in terms of true positive and false alarm ratio, over real mobile agents IP traces with injected real distributed SYN flooding attacks at known instants.

We showed that, in a mobile agents network, Power Divergence presents some interesting special cases. For β = 0.5, this divergence is 4 x HD (P || Q) and for β = 2 it is equal to 0.5 x χ^2 (P || Q) divergence. Obviously, this power divergence outperforms then the existing divergence measures (Chi square & Hellinger Distance)

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

measures. In fact, by changing the values of β, one can optimize the detection of attacks compared to the existing divergence measures.
We also evaluated the performance of the PD via the detection rate and the false alarm rate. We noticed that PD accuracy increases when increasing the value of β.

In our future work, we will focus on providing additional information to pinpoint malicious flows, in order to trigger automatic reaction against ongoing attacks over the mobile agents.

VIII. REFERENCES

1. Moore, D., Voelker, S., Savage, M.: Inferring Internet Denial of-Service Activity. In: Proceedings of USENIX Security Symposium (SSYM'01), 9–22 (2001).
2. HU,Jiang-Ping,Zhi-XinLIU,Jin-HuanWANG,Lin WANG, Xiao-Ming HU: Estimation, Intervention and Interaction of Multi-agent Systems. Acta Automatica Sinica 39, no. 11, pp 1796-1804 (2013).
3. Salem, O., Vaton, s., Gravey, A.: A novel approach for anomaly detection over high –speed networks. In: Proceedings of the 3rd European Conference on Computer Network Defense (ECND'07), vol. 30, 2009, pp. 49–68 (2001).
4. Cormode, G., Muthukrishnan, S.: An improved data stream summary: The count-min sketch and its applications. J. Algorithms, vol. 55, pp. 29–38 (2004).
5. Tang, J., Cheng, Y., Zhou, C.:Sketch-based SIP Flooding Fetection Using Hellinger Distance. In: Proceedings of the 28th IEEE conference on Global telecommunications (GLOBECOM'09), 3380–3385 (2009).
6. Broniatowski, M., Leorato, S.: An estimation method for the neyman chi-square divergence with application to test of hypotheses. In: J. Multivar. Anal., pp. 1409–1436 (2006).
7. Havrda, J., Chavrat, F: Quantification method of classification processes: The concept of structural α-entropy. In: Kybernetika, vol. 3, pp. 30–35 (1967).
8. Rathie, P., Kannappan, P.: A directed-divergence function of type β. In: Inform. Contr., vol. 20, 38–45 (1972).
9. Haussler, D., Opper, M.: Mutual information, metric entropy, and cumulative relative entropy risk. In: Ann. Statist., vol. 25, 2451–2492 (1997).
10. MAWI working group traffic archive, http://mawi.wide.ad.jp/mawi/.
11. Bishop, M.: Introduction to security network. In: Addison Wesley, 1 edition, (2004).
12. VOIP Security and Privacy Threat Taxonomy, public release, 24 October 2005
13. Nassar, M., Niccolini, S.: VOIP Instrusion Detection and Prevention System. In: ACM SIGCOMM, New York (2007).
14. Nassar, M., State, R., Festor, O.: Voip Honeypot Architecture". In: Integrated Network Management (IM 2007), pages 109-118. IEEE, Munich, May 2007
15. Jacobson, V.: Congestion avoidance and control. In: SIGCOMM Comput. Commun. Rev., vol. 25, 157–187 (1995).
16. Dagiuklzd, T., Markl, J., Rokos, M.: Low cost tools for secure and highly available voip communication services. In: snocer 2
17. http://www.webbasedconferencing.org/blog/vishing-spiting-eavesdropping-security-threats-to-voip-primer
18. Sengar, H., Wijesekera, D., Jjodia, S.: Detecting VOIP Flodds Using the Hellinger Distance. In: IEEE, Vol.19 (2008).
19. Lange, D., Oshima, M.: Mobile Agents with Java: The Aglet API. In: Volume 1, Issue 3, 111–121(1997).
20. Guido, J., Frances M., Brazier, T., Tanenbaum, A.: Security in a Mobile Agent System. In: IEEE Symposium on Multi-Agent Security and Survivability (2004).
21. Michelle, S., Wangham, J., Obelheiro, R.: A Security Scheme for Agent Platforms in Large-Scale Systems. In: IFIP International Conference on Communications and Multimedia Security Mobile, 104-116 (2013)
22. Gray, R., Kotz, D., Cybenko, G., Rus.: Security in a multiplelanguage, mobile agent systems. In: LNCS 1419 Springer-Verlag (1998)
23. Karnik, N.: Security in Mobile Agent Systems. In: PhD thesis, University of Minnesota (1998)
24. Zubair, M., Manzoor, U.: Mobile Agent based Network Management Applications and Fault-Tolerance Mechanisms. In: The Sixth International Conference on Innovative Computing Technology (2016).
25. Alkasassbeh, M., Adda, M.: Network fault detection with Wiener filter-based agent. In: Journal of Network and Computer Applications 32(4) (4):824-833 (2009).
26. Rahwan, T., Rahwan, I., Ashri, R.: Agent-based Support for Mobile Users using AgentSpeak(L). In: Agent-Oriented Information Systems Volume 3030 of the series Lecture Notes in Computer Science, pp 45-60.
27. Tu, Griffel, Lamersdof: Integration of intelligent and mobile agent for E-commerce.
28. Kowalczyk, R., Ulieru M, Unland, R.: Integrating Mobile and Intelligent Agents in Advanced e-Commerce: A Survey, Agent-Oriented Information Systems Volume 3030 of the series Lecture Notes in Computer Science, pp 45-60.
29. Jansen W., Karygiannis: T. Mobile Agent Security. In: National Institute of Standards and Technology, Gaithersburg, MD 220899.
30. HU, J., Zhi-Xin, L., WANG, J.: Estimation, Intervention and Interaction of Multi-agent Systems. In: Acta Automatica Sinica 39, no. 11 : 1796-1804 (2013).
31. Manzoor, U., Nefti, S., Rezgui, Y.: Categorization of malicious behaviors using ontology-based cognitive agents. In: Data & Knowledge Engineering, Volume 85, 40-56 (2013).
32. Manzoor, U., Nefti, S.: iDetect: Content Based Monitoring of Complex Networks using Mobile Agents. In: Applied Soft Computing, Volume 12, Issue 5, 1607-1619 (2012).

33. Chen, Bo., Harry, H., Cheng, Palen, J.: Integrating mobile agent technology with multi-agent systems for distributed traffic detection and management systems. In: Transportation Research Part C: Emerging Technologies 17, no. 1, 1-10 (2009).
34. Rathie, P., Kannappan, P.: A directed-divergence function of type _. In: Inform. Contr., vol. 20, 38–45 (1972).
35. Haussler, D., Opper, M.: Mutual Information, Metric Entropy, and Cumulative Relative Entropy Risk. In: Ann. Statist., vol. 25, 2451–2492 (1997)..

CITE AN ARTICLE

Tajer, Jean , Mo Adda, and Benjamin Aziz. " DETECTION OF FLOODING ATTACKS ON MOBILE AGENTS USING SKETCH TECHNIQUE AND DIVERGENCE MEASURES." *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY* 6.8 (2017): 112-21. Web. 5 Aug. 2017.