International Journal on Applications in Information and communication Engineering
Volume 5 : Issue 2 : December 2019, pp 78 – 85 www.aetsjournal.com ISSN (Online) : 2394 – 6237

NETWORK PERFORMANCE WITH DDOS ATTACK USING IAFV FOR BOTNET IDENTIFICATION

NIRANJANI.K , RAMYA PRIYATHARSINI T G , KANIMOZHI.P

Abstract— Oneof the most dangerous attacks is Denial-of-Service (DoS). It's a kind of volumetric attack. Proposeda framework to evaluate the network's performance under this attack with various network parameters.Among all the network attacks, the Distributed Denial of service (DDoS) attack is easier to carry out, more harmful, hard to be traced and difficult to prevent. So, this threat is more serious. The DDoS attack makes use of many different sources to send a lot of useless packets to the target in a short time, which will consume the target's resource and make the target's service unavailable.The bots may be either themselves malicious users that have been preliminarily infected (e.g., worms and /or Trojans). In order to quantify the botnet learning ability in this work, Emulation Dictionary Rate (EDR) is introduced. Implemented a novel detecting algorithm for DDoS attacks based on IP Address Features Value (IAFV) to read the characteristics of the network based on time delay, throughput and packet delivery ratio. In the proposedsystem,a hybrid algorithm for botnet identification is implemented to analyze the network performance at the time of attack. Numerous relevant parameters including throughput, time delay and packet delivery ratio are evaluated. Using IAFV time series to describe the state change features of network flowand detecting DDoS attack is equivalent to classifying IAFV time series virtually. It has Support Vector Machine (SVM) classifier to get the optimal solution based on the existing information under the condition that the sample size tends to be infinite or be limited.

Index Terms— Denial of Service, IAFV,Emulation Dictionary Rate, Botnet,Support Vector Method

I. INTRODUCTION

A network especially the Internet is the primary target of the natural attackers' habitat to hide a broad variety of threats. One of the most popular threats is the Denial-of-Service (DoS) attack which can be broadly categorized as a volumetric attack where the target destination is overwhelmed by a huge number of requests eventually leading to the impossibility of serving to any of the users. Distributed Denial-of-Service (DDoS) attacks are usually launched through the botnet, an "army" of compromised nodes hidden in the network. The bots may be either itself malicious users acting consciously or they may be legitimate users that have been preliminarily infected. The existence itself of an anomalous request rate is uncovered and its detection is not an important one. The main challenge is instead ascertaining whether the anomaly is caused by a DDoS attack. If so, performing a correct/early identification of the botnet hidden in the network is a challenging task.

This work suggests three basic things: i) introduce an abstract model for the aforementioned class of attacks, where the botnet emulates normal traffic by continually learning admissible patterns from the environment ii) develop an inference algorithm that is shown to provide a consistent estimate of the botnet possibly hidden in the network iii) verify the validity of the proposed inferential strategy on a test bed environment. The test results show that for several scenarios of implementation, the proposed botnet identification algorithm has an observation time of less than one minute to identify correctly almost all bots without affecting the normal users' activity.

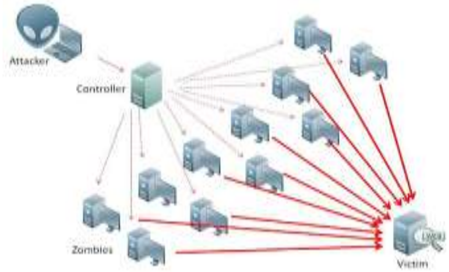

Figure1: DoS Architecture

Niranjani. K , Faculty of Information Technology , Dhanalakshmi Srinivasan Engineering College , Tamil Nadu , India.
Ramya Priyatharsini . T.G , Faculty of Information Technology , Dhanalakshmi Srinivasan Engineering College , Tamil Nadu , India.
Kanimozhi P , Faculty of Information Technology , Dhanalakshmi Srinivasan Engineering College , Tamil Nadu , India.

II. Related Work

The earliest DoS paradigms (see, e.g., TCP SYN flooding), relied on specific protocols' vulnerabilities and re characterized by the repetition of one (or few) requests with a hugerate [1]. In this situation, the single source of the attack can be identified by computing its unusually large request rate. The distributed variants of such attacks exploit basically thesame kind of vulnerabilities and repetition schemes, but for the fact that the large request rate is now obtained by aggregating many small individual bot rates. Nevertheless, in such attacks, the bots can be still identified at a single-user level. Indeed, normal traffic patterns are typically characterized by a certain degree of innovation, while the repetition scheme implicitly emphasizes the bot character. In fact, several useful inferentialstrategies have been proposed for such kind of DDoS attacks. The literature about DDoS attacks is rich. With no pretence of completeness, introduce briefly some recent works on the subject and refer the Reader to the survey in [2] for a more comprehensive summary.

In [3], statistical methods to identify DDoS attacks are proposed, relying on computingentropy and frequency-sorted distributions of selected packet attributes. The DDoS identification is then based on the detectionof anomalies in the characteristics of the packet attributes. In [4], the Authors propose a hierarchical method based on macroscopic-level network monitoring to capture shifts inspatial-temporal traffic patterns, which are then used to inform a detection system about where and when a DDoS flooding attack possibly arises in a source network. The work presented in [5] relies on the application of an entropy detection method, where the key to identify the DDoS attack is the randomnessof some attributes in the packets' headers.

In [6], two new information metrics, the generalized entropy metric and theinformation distance metric, are employed to detect low rateDDoS attacks, by evaluating the dissimilarity betenlegitimate and attack traffic. A mathematical model to examineshrewDDoS attacks (where TCP flows are constrained toa small fraction of their ideal rate at low attack costs) is introduced in [7]. The Authors propose a methodology aimedat capturing the adjustment behaviors of TCP congestion window at the victim's side, in order to evaluate the interplay beten attack patterns and network environment. More closely connected to this work is the new class of application-layer DDoS attacks, which is recently emerging as one of the most powerful threats [8]–[11]. In such attacks, the malicious traffic patterns are disguised as normal onesby leveraging the many possibilities offered at the application layer (for instance, when surfing through a website, more and more b-pages are likely to be explored as time elapses). By assigning a sufficient degree of variability to each individual bot's pattern, identification strategies based on single-user inspection become harmless. Building on such new possibilities, in this work shall introduce a formal model for DDoS attacks where the botnet gets at its disposal a certain emulation dictionary to build the traffic patterns.

The DDoS class considered in this work builds upon and generalizes some dangerous threats that have been recentlydocumented in the literature. To the best of our knowledge, this is the first attempt to provide a systematic analysis and to devise suitable countermeasures for such kind of attacks. A short and limited version of this work appears in the conference publication [27]. The main novelties introduced inthis work include: complete proofs of all theoremsdiscussion and examples aimed at illustrating the physical interpretationand the relevant implications of the theoretical resultsa comprehensive and formal illustration of a botnet identification condition and of the corresponding identification algorithman extended campaign of experiments on a testbed environment.

This work deals with the design and analysis of inference strategies aimed at identifying a botnet in the context of distributed denial-of-service attacks. In our setting i) the network analyst collects traffic patterns from across the network and has access to the message contentii) the meaning of themessages produced by an individual user provides no specialinformation about its nature, legitimate or malicious and iii)no specific assumptions are made about the characterizationof the traffic patterns of a normal user. In this respect, theinference strategies proposed in this work are non-parametric.Starting from the attacks documented in the literature,introduced a formal model for randomized DDoS attackswith increasing emulation dictionary, which is defined by thefollowing main features i) the botnet emulates the normaltraffic patterns bygleaning admissible messages from anemulation dictionary and ii) the botnet is given the strongpower of learning an emulation dictionary that becomes richerand richer as time elapses, so as to guarantee a sufficientvariability across messages. In order to quantify the botnetlearning ability, in this work introduce the EmulationDictionary Rate (EDR), namely, the increase of dictionarycardinality per unit time.Notably, the considered class of DDoS attacks is moregeneral and powerful than many attacks documented in theliterature. The assumption of such great power in the attacker'shands might perhaps look overly pessimistic. At the sametime, a worst-case analysis is perfectly suited to security applications and allows getting important insights as regards thebotnet identifiability under challenging operational conditions.The fundamental descriptive indicator employed in thiswork to ascertain the nature of network users is the MessageInnovation Rate (MIR), the number of distinct messagesper unit time, transmitted by a given group of users. Therelevance of the MIR for botnet identification purposes arisessince, in view of the coordination in the DDoS attack, theusers belonging to a botnet are expected to exhibit a smallerdegree of innovation than normal users, which act by theirown nature independent of each other.

III. EXISTING SYSTEM

Distributed Denial-of-Service (DDoS) attacks are launched in the network through the botnets. Botnets are bunch of compromised nodes hidden in the network. The tools for finding DDoS mitigation should be enabled accordingly as early as possible and reliable discrimination of the normal users from the compromised ones. Unfortunately the recent emergence of attacks performed at the application layer has multiplied the number of possibilities that a botnet can exploit to conceal its malicious activities. New challenges arise which cannot be addressed by simply borrowing the tools that have been successfully applied so far to earlier DDoS paradigms.

The main challenge is ascertaining whether the anomaly is caused by a DDoS attack and if so, performing a correct/early identification of the botnet hidden in the network. These operations are crucial to achieve successful DDoS mitigation since discriminating legitimate users from malicious users would allow the destination to ban the malicious users without denying the service to the legitimate users.

Our first contribution determines the MIR for a botnet B,with either deterministic or Poisson transmission scheduling.Denoting by λB the transmission rate corresponding to theoverall transmission activity in B and by α the EDR, it shows that the MIR converges in probability to the followinginnovation rate

$$R(\alpha, \lambda_B) = \frac{\alpha \lambda_B}{\alpha + \lambda_B}$$

Our second contribution consists of devising an algorithmthat, under a suitable Botnet Identification Condition (BIC),guarantees that the botnet hidden in the network is correctlyidentified as time elapses.Finally, as a third contribution, all of the aforementionedtheoretical results are tested and validated on a testbed environment. The experimental outcomes are definitely encouraging.

The basic quantities that will be usedto describe the network activity are implemented. The first quantity relates to thetransmission activity of the network users. Each user employsa certain scheduling, which is identified by the transmission epochs of its own messages. More in general, for any givensubnet S of the network, we can define the aggregate patternthat comprises all (ordered) transmission epochs of the usersbelonging to S, formally: TS (1), TS(2), . . . , where TS(i) isthe i^{th}(random) transmission epoch of users belonging to S. Likewise, the pattern of an individual user u becomesTu (1), Tu (2) . . . with a slight abuse of notation(which will be used throughout the work), it have writtenu in lieu of {u}. The total number of transmissions occurredin S, up to a given (deterministic) time t is denoted by

NS (t)Δ|{i : TS (i) ≤ t}|.

As an indicator of the transmission activity, introduced the empirical transmission rate at time t, namely,

$$\lambda s(t) \triangleq \frac{Ns(t)}{t}$$

As a second indicator of the network activity, defined a quantity that relates to the content of the messages sent by network users. This work is interested in the new messages that are incrementally produced by the users during their activities, namely Message Innovation Rate (MIR). In order to obtain a formal definition of the MIR, let DS (t) denote the empirical dictionary composed by the distinct messages sent, up to time t, by users within S. For the sake of clarity, it is remarked that if the same message is sent, e.g., twice from users belonging to S, it appears only once in the dictionary DS (t). The empirical Message Innovation Rate (MIR) is:

$$\rho s(t) \triangleq \frac{|Ds(t)|}{t}$$

IV. PROPOSED SYSTEM

Introduced an abstract model for the DDoS class of attacks, where the botnet emulates normal traffic by continually learning admissible patterns from the environment. Devised an inference algorithm that is shown to provide a consistent (i.e., converging to the true solution as time elapses) estimate of the botnet possibly hidden in the network.Verifying the validity of the proposedinferential strategy on a testbed environment. Tests results show that for several scenarios of implementation, the proposed botnet identification algorithm needs an observation time in the order of less than one minute to identify correctly almost allbots, without affecting the normal users' activity. Implemented a hybrid algorithm for botnet identification to analyze the network performance at the time of attack. Used IAFV time series to describe the state change features of network flow. Detecting the DDoS attack is equivalent to classifying the IAFV time series virtually. SVM classifier can get the optimal solution based on the existing information under the condition that the sample size tends to be infinite or be limited. Large number of relevant parameters including throughput, time delay and packet delivery ratio are used to test the proposed algorithm.

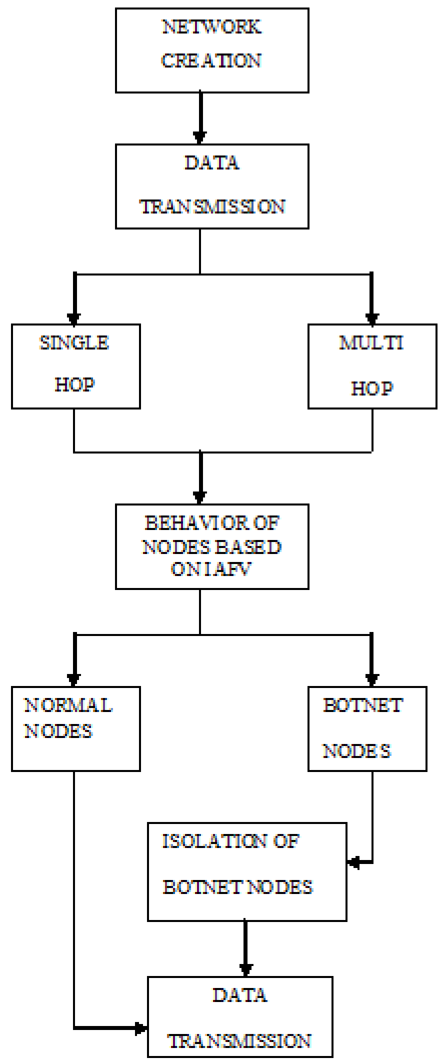

Figure 2: Data Flow Diagram of the proposed model

Definition of IP Address Feature Value and Algorithm

The attack flows of DDoS have some features like the abrupt traffic change, flowdissymmetry, distributed source IP addresses and concentrated target IP addresses,etc. In this paper, we propose the concept of IAFV (IP Address Feature Value) toreflect the four features of DDoS attack flow.

The network flow F in the certain timespan T is given in the form of < (t1, S1, D1), (t2, S2, D2)…(tn, Sn, Dn)>. For the ith packetp, ti is the time, Si is the source IP address and Di is the destination IP address. Classifyall the packets by source IP and destination IP, which mean all packets in a certainclass share the same source IP address and destination IP address. A class which isconsisted of packets with a source IP Ai and a destination IP Aj is noted as SD (Ai, Aj).Carry out the following rules to the above mentioned classes:If there are two different destination IP address Aj, Ak, which makes class SD(Ai, Aj)and class SD(Ai, Ak) both nonempty, then remove all the class with a source IP addressof Ai.If there is only one class SD (Ai, Aj) containing the packets with a destination IP addressAj, then remove all the classes with a destination IP address Aj.Assume that the remaining classes are SDS1, SDS2…SDSl, classify these classesby destination IP address, that is all the packets with the same destination IP addresswill be in the same class. The class made up of packets of the same destination IPaddress Aj is noted as SDD (Aj), these classes isSDD1, SDD2…SDDm, the IAFV (IPAddress Features Value) is defined as:

$$IAFV_F = \frac{1}{m}\left(\sum_{i=1}^{m} SIP(SDDi) - m\right)$$

inwhich SIP(SDDi) is the number of different source IP addresses in the class SDDi.In order to analyze the state features of the network flow F more efficiently and excludethe disturbance of a normal flow, the definition of IAFV classify the packets ofF by source IP address and destination IP address. A DDoS attack is usually composedof several attack sources rather than a single one with the true source IPaddress, so the class with packets from the same source IP address Ai to differentdestinations belongs to a normal flow, thus the classes with a source IP address Ai can be removed. After that, if there is a destination address Ak makes Ai and Aj inSD(Ai, Ak) and SD(Aj, Ak) the same, then the destination IP address Ak is not visitedby multiple sources, which implies a normal flow, thus the class with packets going tothe destination Ak can be removed. The above mentioned two steps can reflect theasymmetry of a DDoS attack flow as well as a decrease in the disturbance of the normalflow. DDoS attack is a kind of attack that sends useless packets to the attacktarget from many different sources in the hope of exhausting the resources of thetarget. This act can produce lots of new source IP addresses in a short time, whichwill lead to an abnormal increase of SIP(SDDi) for some classes of F, that is, the number ofdifferent sources to different destination will increase abnormally, causes the flow to be in aquite different state in a short time. The definition of IAFV sums up the different source IPaddresses of each SDDi of F in a certain period, then subtract the number of differentdestination IP addresses m, and divide m at last. So IAFV can reflect the characteristicsof a DDoS attack including the burst in the traffic volume, asymmetry of the flow,distributed source IP addresses and a concentrated destination IP address.

The process of IAFV method is given below:

Input: an initial network flow data F, a sample interval Δt, a stopping criterion C, an arrival time of an IP Packet T, a source IP address S, a destination IP address D, an IP address class set SD, SDS and SDD, an IP address features IAFV.

Output: IAFV time series which characterize the essential change features of F.

Processing Procedure:

1. Initialization-related variables;
2. **while** (criterion C is not satisfied){
3. Read the T, S and D of an IP packet from F;
4. **if** (T is not over the sample interval Δt){
5. flag= New_SD(S, D,SD);
   // Judge whether (S, D) is a new element of SD
6. Add_SD (flag, S, D, SD);
   // add a new element (S, D) to SD
   }
7. **if** (the arrival time of IP Packet exceeds the sample interval Δt){
8. remove_SD (SD);
   // remove all (S, D) with same S and different D from SD.
9. Add_SDS (SD, SDS);
   //add all (S, D) of SD with different S and same D to SDS.
10. classify_SDS (SDS, SDD);
   // classify SDS by D and then add all (S, D) of SDS to SDD.
11. m=Size (SDD);
   //count the number of the elements in SDD.
12. $IAFV_F = \frac{1}{m}\left(\sum_{i=1}^{m} SIP(SDDi) - m\right)$
   //calculate IAFV of SDD

13. **return** IAFV;
}
}

Detection Method Based on IAFV

To raise the detection rate, decrease the false alarm rate, and enhance the adaptabilityof detection method, we propose a simple but robust scheme to detect DDoS attacksby extracting IAFV time series from normal flow and DDoS attack flow respectively,and use the SVM (Support Vector Machine) classifier to detect DDoS attacks.

By sampling the network flow data F with sampling interval Δt, and calculating theIAFV of every sample, we can get the IAFV time series sample set A after samplingN times, A(N,Δt)={IAFVi,i=1,2,…,N}, N is the length of the time series. After UsingIAFV time series to describe the state change features of network flow, detectingDDoS attack is equivalent to classifying IAFV time series virtually.SVM classifier can get the optimal solution base on the existing information underthe condition that the sample size tends to be infinite or be limited. It can establish amapping of a non-linear separable data sample in higher dimensional characteristicspace by selecting the non-linear mapping function (kernel function), construct theoptimal hyperplane, and transform a non-linear separable data sample into a linearseparable data sample in the higher dimensional characteristic space. Furthermore, itcan solve the problem of higher dimension, and its computational complexity is independentof the data sample dimension.Therefore we use the SVM classifier, which can be established by learning fromthe IAFV time series of the normal flow samples and DDoS attack flow samples, toclassify the IAFV time series gotten by sampling network flows with sample intervalΔT, and identify DDoS attack.The SVM classifier is

$$\eta = \sum_{i=1}^{M} \beta i Y i K(\emptyset i, \emptyset) + b$$

in which η is the classification result for sample to be tested, βi is the Lagrange multipliers, Yi is the type of classification, Yi∈{-1,1}, K(ϕ□i,ϕ) is the kernel function, bis the deviation factor, ϕi is the classificationraining data sample, i=1,2,…,M,ϕ□is the sample to be tested.

V. EXPERIMENT RESULTS

As regards the measuring stage that precedes the botnetidentification algorithm, the following pipeline is adopted.Packets are preliminarily filtered by using popular softwarepackage for packet capturing and network protocol analysis.At the output of such preliminary filtering stage i) only thetraffic directed to the destination that is being monitored isretained ii) among the surviving packets, only the applicationlayertraffic is retained iii) the resulting packets are dividedon the basis of their source IP address and are finally fed tothe botnet identification algorithm.

The normal users have noattacking intent, they perform ordinary surfing activity. About20 min of (application-layer) traffic have been collected, from10 independent users, which were students and researchersworking in the laboratory, and carrying on their surfing activityalmost independently. In order to help understanding the natureand significance of the dataset, we report that the total numberof TCP flows is about 26800, the median of flows across usersis 2846, the minimum number of flows is 1042, the maximumnumber of flows is 3925, and the average packet size is 776bytes. Supported by these numbers, and by a trace-by-traceinspection, we conclude that the activity of the users duringthe monitored period is reasonably sustained, and compatiblewith typical traffic, meaning that the patterns are neither trivial(users effectively send requests) nor anomalous (users do notoverload the destination with huge rates).

The collected streams have been partitioned into chunks of2 min. In the forthcoming analysis we take two perspectives.In one scenario, the number of normal users is 10; each userhas multiple 2-min chunks and, per each trial, choosesrandomly one trace per user. In the other scenario, 2-minchunks belonging to the same user have been treated as if theywere coming from distinct users. In this way, multiply(fictitiously) the number of normal users. This is clearly an approximation e.g., fictitious users stemming from thesame user might feature an additional-and-spurious degree ofdependence. On the other hand, this (possible) increase ofdependence goes in the direction of (possibly) increasing thefraction of normal users mistakenly marked as bots. Therefore,thesimulations performed in the “multiplied”scenario areexpected to provide a conservative performance assessment.

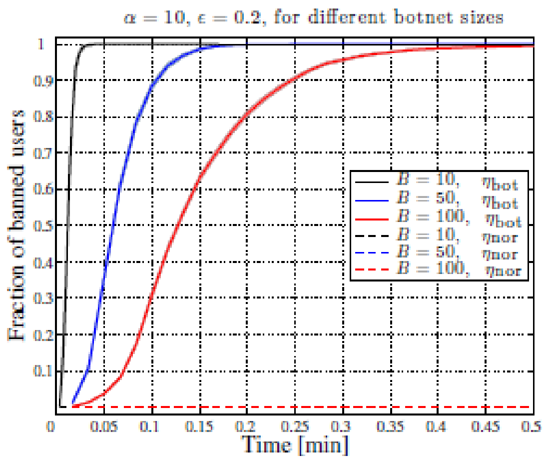

Figure 3:Fraction of banned users as a function of time, for different botnet sizes B, in the constant attack-rate regime

The setting considered in this work encompasses naturallythe relevant scenario of spoofed source IP addresses, which isbecoming rather common in DDoS attacks. In such scenario,

each bot can change its source IP address by (randomly)choosing from a collection of spoofed addresses. In the randomizedDDoS attack considered in this work, the bot trafficstreams are constructed by picking subsequent messages independentlyfrom an emulation dictionary that is shared amongall the bots. Accordingly, a botnet of B nodes employing a setof A randomly spoofed addresses (with A > B), is equivalentto a botnet of A nodes performing the attack. Since the goalof the network analyst is banning the machines that launch theattack (not associating a physical machine to its IP address),concludes that the performed analysis applies directly to thecase of spoofed IP addresses, provided that the number of botsis replaced by the number of IP addresses globally employedby the botnet. For the sake of brevity, such “effective” numberwill be still denoted by B.

There are at least two meaningful regimes to examine thecase of increasing number of bots and/or spoofed addresses:i) the regime where B increases, while the individual bots’transmission rate, λbot, is constant, implying a growth ofthe total DDoS attacking rate Bλbot ii) the regime whereB increases while keeping the attacking rate constant. Asregards the former regime, differently from the analysis of theprevious section, varying B corresponds to varying the relativeproportion of bots and normal users. This notwithstanding,the evidences arising from the simulation pertaining to suchscenario are very similar to those observedandare accordingly not reported. In summary, in this regime thedependence of ηbot upon B is not obvious (no monotonicbehavior emerges with respect to B, which is partly explainedby noting that increasing B should augment the botnet “visibility”,but also the number of possible algorithm mistakes)and the performance is little sensitive to variations of B.

VI. CONCLUSION AND FUTURE WORK

Distributed Denial of Service (DDoS) attacks launched by bots are capable to learn the application layer interaction possibilities, so as to avoid repeating one simple operation many times. The main contributions of this work are as follows: i) introduced a formal model for the class of randomized DDoSattacks with increasing emulation dictionary ii) proposed an inference algorithm aimed at identifying the botnets executing such advanced DDoS attacks and ascertained the consistency of the algorithm, namely the property of revealingthe true botnet as time elapses iii) evaluated the proposed methodologies on a testbed environment.In future, the proposed algorithm can be tested over more datasets in order to examine the impact on performance of the nature of the site under attack. The different behaviors of users surfing on the web can be analyzed. Conducting a refined convergence analysis in order to characterize from an analytical viewpoint, the time needed to reach a prescribed accuracy. The dependence of such time upon the network/botnet size and other relevant system parameters can be taken into considerations. Examining the problem from an adversarial perspective where the botnet -identification strategy and the kind of DDoS attack are jointly optimized by looking for equilibrium solutions that manage the attacker's and defender's conflicting requirements. Generalizing the theoretical analysis and tools to multi – clustered DDoS attacks where several botnets (using different emulation dictionaries) launch their attacks simultaneously.

REFERENCES

[1] T. He, A. Agaskar, and L. Tong, "Distributed detection of multi-hop information flows with fusion capacity constraints," IEEE Trans. Signal Processing, vol. 58, no. 6, pp. 3373–3383, Jun. 2010.

[2] M. Barni and B. Tondi, "Binary hypothesis testing game with training data," IEEE Trans. Inf. Theory, vol. 60, no. 8, pp. 4848–4866, Aug.2014

[3] M. Barni and F. P´erezGonz´alez,"Coping with the enemy: advances in adversary-aware signal processing," in Proc. IEEE ICASSP, Vancouver,Canada, May 2013, pp. 8682–8686.

[4] M.Barni and B.Tondi,"The source identification game: an information theoretic perspective," IEEE Trans. Inf. Forensics and Security, vol. 8, no. 3, pp. 450–463, Mar. 2013.

[5] L. Feinstein, D. Schnackenberg, R. Balupari, and D. Kindred,"Statistical approaches to DDoS attack detection and response," in Proc. DARPA Information Survivability Conference and Exposition, Washington, DC, USA, Apr. 2003, pp. 303–314

[6] S. Ferretti and V. Ghini, "Mitigation of random query string DoS via gossip," Commun. in Comput. and Inf. Sci., vol. 285, pp. 124–134, 2012.

[7] T. He and L. Tong, "Detection of information flows," IEEE Trans. Inf. Theory, vol. 54, no. 11, pp. 4925–4945, Nov. 2008.

[8] T. He and L. Tong, "Distributed detection of information flows," IEEETrans. Inf. Forensics and Security, vol. 3, no. 3, pp. 390–403, Sep. 2008.

[9] N. Hoque, D. Bhattacharyya, and J. Kalita, "Botnet in DDoS attacks: trends and challenges," IEEE Commun. Surveys Tuts.vol.17, no. 4, pp.2242–2270, fourth quarter 2015.

[10] Kailkhura, S. Brahma, B. Dulek, Y. S Han, and P. Varshney,"Distributed detection in tree networks: Byzantines and mitigation techniques," IEEE Trans. Inf. Forensics and Security, vol. 10, no. 7,pp. 1499–1512, Jul. 2015.

[11] J. Kim and L. Tong, "Unsupervised and nonparametric detection of information flows," Signal Processing, vol. 92, no. 11, pp. 2577–2593, Nov. 2012.

[12] J. Luo, X. Yang, J. Wang, J. Xu, J. Sun, and K. Long, "On a mathematical model for low-rate shrew DDoS," IEEE Trans. Inf. Forensics and Security, vol. 9, no. 7, pp. 1069–1083, Jul. 2014.

[13] S. Marano, V. Matta, T. He, and L. Tong, "The embedding capacity of information flows under renewal traffic," IEEE Trans. Inf. Theory, vol. 59, no. 3, pp. 1724–1739, Mar. 2013.

[14] S. Marano, V. Matta, and L. Tong, "Distributed detection in the presence of Byzantine attacks," IEEE Trans. Signal Process, vol. 57, no. 1, pp.16–29, Jan. 2009.

[15] S. Marano, V. Matta, and P. Willett, "Distributed detection with censoring sensors under physical layer secrecy," IEEE Trans. Signal Process.,vol. 57, no. 5, pp. 1976–1986, May 2009.

[16] M. Mardani and G. B. Giannakis, "Estimating traffic and anomaly maps via network tomography," IEEE/ACM Trans. Networking, DOI: 10.1109 /TNET .2015 .2417809, date of publication, Apr. 2015.

[17] M. Mardani, G. Mateos, and G. B. Giannakis, "Dynamic anomalography: tracking network anomalies via sparsity and low rank," IEEE J. Sel. Topics Signal Process., vol. 7, no. 1, pp. 50–66, Feb. 2013.

[18] M. Mardani, G. Mateos, and G. B. Giannakis, "Recovery of low-rank plus compressed sparse matrices with application to unveiling traffic anomalies," IEEE Trans. Inf. Theory, vol. 59, no. 8, pp. 5186–5205, Aug. 2013.

[19] V. Matta, M. Di Mauro and M. Longo,"Botnet identification in randomized DDoS attacks," Proc.EUSIPCO,Budapest,Hungary,Aug./Sep.2016, pp.2260–2264.

[20] P. Venkitasubramaniam, T. He, and L. Tong, "Anonymous networking amidst eavesdroppers," IEEE Trans. Inf. Theory, vol. 54, no. 6, Jun.2008

[21] Y. Xiang, K. Li, and W. Zhou, "Low-rate DDoS attacks detection and traceback by using new information metrics," IEEE Trans. Inf. Forensics and Security, vol. 6, no. 2, pp. 426–437, Jun. 2011.

[22] J. Yuan and K. Mills, "Monitoring the macroscopic effect of DDoS flooding attacks,"IEEETrans.Depend.SecureComput. vol. 2, no. 4, pp. 324–335, Oct. 2005.