International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 10 • Issue 2 pp. 437-443 June 2018-Dec 2018 www.csjournals.com

An Enhanced DDOS Attack Estimation and Protection Approach Employing Statistical Data Packets Movement

Aswath Muntaha[1], MD Ateeq Ur Rahman[2]
[1]Research Scholar, Dept. of ComputerScience& Engineering, SCET, Hyderabad
umair.ameen95@gmail.com
[2]Professor and Head, Dept. of ComputerScience & Engineering,SCET, Hyderabad
mail_to_ateeq@yahoo.com

Abstract—In a randomized DDoS assault with expanding copying word reference, the bots endeavor to conceal their vindictive action by masking their activity designs as "ordinary" movement designs. In this work, we expand the DDoS class presented in [1], [2] to the instance of a multi-bunched botnet, whose principle include is that the copying lexicon is part finished the botnet, offering ascend to various botnet groups. We propose two systems to recognize the botnet in such difficult situation, one in light of bunch expurgation, and the other one on an association run the show. Consistency of the two calculations under perfect conditions is determined, while their execution is inspected over genuine system follows.

Index Terms—Distributed Denial-of-Service, DDoS, Cyber-Security, Signal Processing for Network Security.

I. INTRODUCTION

More regularly, Distributed Denial-of-Service (DDoS) assaults hit the features for their hazardous effect on a few genuine undertakings. A DoS assault is acknowledged through a massive volume of solicitations sent to an objective goal site, which is overpowered until the point that its assets immerse, and the support of true blue clients is denied. The capability of being "disseminated" originates from the way that such demands are sent by a net of scattered machines (the bots), which can be malignant clients acting deliberately, or honest to goodness clients that have been contaminated, e.g., by worms or potentially Trojans. The bots can be composed by at least one botmasters, and the troupe of bots is all inclusive alluded to as the botnet. The objective of the safeguard is recognizing the individuals from the botnet, keeping in mind the end goal to boycott the bots, without denying the support of typical clients. The least difficult, incorporated DoS assaults (e.g., TCP SYN flooding) abused vulnerabilities in the convention stack, depending basically on rehashed, high-rate transmissions of a similar demand from a solitary client. In such conditions, the irregular transmission rate was adequate to recognize the wellspring of the assault.

Conversely, in a DDoS assault the individual bot's rate is kept direct, while the worldwide assaulting rate must be substantial. By and by, without advance complexity, the traded off machines can be as yet distinguished at a solitary client level. Truth be told, movement examples of ordinary clients are typically described by a specific level of development (for example, as time slips by, unmistakable website pages are probably going to be gone to), while the redundancy plot verifiably demonstrates the atypical bot character. This work centers around an additionally difficult variation of DDoS assault, to be specific, on the current class of use layer DDoS assaults. This exceptional type of assaults goes past the least difficult reiteration based assaults, by abusing the plentiful scope of conceivable outcomes accessible at the application layer [3], [4]. In such novel assaults, the bots pick haphazardly their solicitations from an arrangement of acceptable messages (an imitating lexicon), attempting so to camouflage their activity designs as typical ones. The improved level of fluctuation in the message choice (e.g., the generally expansive number of pages open in surfing through a site), makes the individual bot's examples so reach to keep from single-client assessment. To the extent we know, the principal formal portrayal of the previously mentioned class of randomized DDoS assaults has been given in [1], [2], for the situation where the botnet is made by a solitary group utilizing one and a similar imitating lexicon.

Numerous useful circumstances, notwithstanding, it is normal that the imitating word reference is scattered through the botnet, such that particular gatherings of bots approach distinctive bits of the general copying lexicon. This could occur for various reasons. One case is that, because of different imperatives (e.g., data transfer capacity, vitality), the botmaster sends to the bots just bits of the educated lexicon. Another case is a truly decentralized DDoS, where the botnet is clusterized in discrete gatherings (maybe planned by various botmasters, offering ascend to a progressive DDoS) acting freely, and, specifically, playing out the word reference learning undertaking independently.

International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 10 • Issue 2 pp. 437-443 June 2018-Dec 2018 www.csjournals.com

II. THE MULTI-CLUSTERED DDOS ATTACK

Give NS(t) a chance to signify the general number of transmissions happened, up to time t, in a given subnet S. The transmission movement of S is evaluated regarding the experimental transmission rate:

$$\hat{\lambda}_S(t) \triangleq \frac{N_S(t)}{t} \quad (1)$$

At the point when a constraining (as t → ∞) rate exists, it is meant by λS.

A moment pointer relates rather to the message content. Keeping in mind the end goal to describe the fluctuation in the action of system clients, we center around the new messages that these last deliver as time slips by. Such inconstancy can be measured as far as a Message Innovation Rate (MIR), which has been initially presented in [1]. Give us a chance to gather into an experimental lexicon, DS(t), all the unmistakable messages sent, up to time t, by the clients having a place with a given subnet S. The observational MIR can be as needs be characterized as:

$$\hat{\rho}_S(t) \triangleq \frac{|\mathscr{D}_S(t)|}{t} \quad (2)$$

The restricting MIR, when it exists, is meant by ρS. Our model for multi-bunched DDoS is enlivened to late sorts of utilization layer DDoS [3], [4], and is a speculation of the DDoS class initially proposed in [1]. We accept that the botnet is made of C non-covering groups, every one of which approaches an imitating lexicon (at time t) indicated by Ec(t), for c = 1, 2, . . . ,C. A bot of the c-th group performs typical movement imitating by picking acceptable messages from Ec(t). So as to ensure a non-suspicious advancement rate, the word reference is found out in a consistent manner, to be specific, its cardinality increments with t. To measure abundance of the imitating word reference, we present the Emulation Dictionary Rate (EDR) if the c-th group:

$$\alpha_c \triangleq \lim_{t\to\infty} \frac{|\mathscr{E}_c(t)|}{t} \quad (3)$$

At the point when a bot of the c-th bunch transmits, it picks (consistently at arbitrary) a message from the accessible copying lexicon Ec(t).

Because of the transmission action, to any subnet B of the botnet we can relate a specific observational word reference, DB(t). At time t + s, such an exact lexicon is potentially expanded by epitomizing the particular messages (which were not at first contained in DB(t)) picked amid interim s by the bots in B.

A. Botnet MIR

The suggestions with respect to the previously mentioned arrange markers have been analyzed in detail in [1], [2]. For culmination, the correlated outcomes are gathered in the expected hypothesis,which fundamentally rethinks Theorem 1 in [1], [2] to deal with the multi-grouped setting.

THEOREM 1 (MIR of a multi-grouped botnet).*Give Btot a chance to be a multi-bunched botnet, and let the transmission strategies be either synchronous with steady transmission rate, or autonomous Poisson forms, with rates* λu, *for* $u \in \mathcal{B}_{\text{tot}}$.*Let* $\mathcal{B} = \bigcup_{c=1}^{C} \mathcal{B}_c$,

Where $\lambda_{\mathcal{B}_c} = \sum_{u\in\mathcal{B}_c} \lambda_u$ *a subnet of the* c*-th botnet group, and let* αc *theEDR of the* c*-thgroup. If* $\mathcal{B}_c \neq \emptyset$, *the (limiting) MIR of* $\mathcal{B}_c$ *is:*

$$\rho_{\mathcal{B}} \leq \sum_{c:\mathcal{B}_c\neq\emptyset} \frac{\alpha_c \lambda_{\mathcal{B}_c}}{\alpha_c + \lambda_{\mathcal{B}_c}} \quad (4)$$

Where $\lambda_{\mathcal{B}_c} = \sum_{u\in\mathcal{B}_c} \lambda_u$ *is the total transmission rate of*Bc. *Besides, the general MIR of B satisfies the disparity:*

$$\rho_{\mathcal{B}} \leq \sum_{c:\mathcal{B}_c\neq\emptyset} \frac{\alpha_c \lambda_{\mathcal{B}_c}}{\alpha_c + \lambda_{\mathcal{B}_c}} \quad (5)$$

which is happy with equity when the imitating word references of the diverse groups are commonly disjoint.

As respects the individual-bunch MIR in (4), the outcome comes straightforwardly from Theorem 1 in [1], [2]. As respects the general MIR in (5), the outcome originates from the way that the MIR is sub-added substance, while the fairness takes after on the grounds that disjointeness of the copying word references suggests disjointness of the comparing experimental lexicons and, subsequently, additively of the relating MIRs.
This module is utilized to transfer required record from capacity gadget to client account and send the document into goal account. There are a wide range of sorts of documents: information records, content documents, program documents, catalog documents, et cetera. Distinctive kinds of records store diverse sorts of data.

This component is in charge of identifying P2P customers by breaking down the rest of the system streams after the Traffic Filter part. For each host h inside the checked system we distinguish two stream sets, meant as Stcp(h) and

International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 10 • Issue 2 pp. 437-443 June 2018-Dec 2018 www.csjournals.com

Sudp(h), which contain the streams identified with effective active TCP and UDP association, separately. We consider as fruitful those TCP associations with a finished SYN, SYN/ACK, ACK handshake, and those UDP (virtual) associations for which there was at least one "ask for" parcel and an ensuing reaction bundle.

III. BOTNET IDENTIFICATIONALGORITHMS

The likelihood of an effective botnet distinguishing proof depends on the way that bots and typical clients are relied upon to carry on diversely as respects their level of development. Indeed, the individuals from a botnet bunch create their transmission movement by picking messages from one and a similar imitating word reference. The suggested shared traits between two individuals from the same botnet bunch are relied upon to develop as far as a MIR that is lower than the MIR that would be acquired, e.g., if the two clients were ordinary. This is on the grounds that the common autonomy of the exercises of two ordinary clients, or of a typical client and a bot, infers regularly a low level of relationship (some incomplete cover could emerge due to, e.g., regular interests, mainstream pages, unconventional site structure), which is reflected in a little crossing point between the relating (individual) observational lexicons. Such heuristic contention has been made exact in [1], [2]. In particular, given two disjoint subnets, S1 and S2, two MIRs are presented, in particular, the whole of MIRs: $\hat{\rho}_{\text{sum}}(\mathcal{S}_1, \mathcal{S}_2) \triangleq \hat{\rho}_{\mathcal{S}_1} + \hat{\rho}_{\mathcal{S}_2}$ also, the MIR of a reference

$$\hat{\rho}_{\text{bot}}(\mathcal{S}_1, \mathcal{S}_2) \triangleq \frac{\hat{\alpha}'(\mathcal{S}_1, \mathcal{S}_2)(\lambda_{\mathcal{S}_1} + \lambda_{\mathcal{S}_2})}{\hat{\alpha}'(\mathcal{S}_1, \mathcal{S}_2) + \hat{\lambda}_{\mathcal{S}_1} + \hat{\lambda}_{\mathcal{S}_2}}$$

express reliance upon t being stifled for simplicity of documentation. The esteem ˆα′(S1, S2) in the last recipe is a reference EDR evaluated from the information. The point by point technique to figure it is accessible in [2], and isn't accounted for here for space requirements. At that point, for ϱ ∈ (0, 1), a transitional edge is characterized as: $\gamma(\mathcal{S}_1, \mathcal{S}_2) = \hat{\rho}_{\text{bot}}(\mathcal{S}_1, \mathcal{S}_2) + \epsilon\,[\hat{\rho}_{\text{sum}}(\mathcal{S}_1, \mathcal{S}_2) - \hat{\rho}_{\text{bot}}(\mathcal{S}_1, \mathcal{S}_2)]$. The heuristic thinking about identifiability converts into the accompanying conditions. At the point when the two subnets have a place with the same botnet group (underneath alluded to as "joint case"), the exact MIR, ˆρS1∪S2 , focalizes toward ˆρbot as time passes, as anticipatedby Theorem 1. Next, consider the case that one subnet contains typical clients as well as bots having a place with bunches not contained in the other subnet. In such case (beneath alluded to as "almost disjoint case") it is practical to expect that the level of reliance between the two subnets is lower than the level of reliance watched when both subnets have a place with the same botnet group. The above contentions prompt:

$$\text{Joint case} \quad \Rightarrow \quad \hat{\rho}_{\mathcal{S}_1 \cup \mathcal{S}_2} < \gamma(\mathcal{S}_1, \mathcal{S}_1), \tag{6}$$

$$\text{Nearly-Disjoint case} \quad \Rightarrow \quad \hat{\rho}_{\mathcal{S}_1 \cup \mathcal{S}_2} \geq \gamma(\mathcal{S}_1, \mathcal{S}_1). \tag{7}$$

As a matter of fact, when (7) is precisely confirmed (the confirmation of (6) being ensured, for t sufficiently vast, by Theorem 1), we might state that the Botnet Identification Condition (BIC) is satisfied. Expanding upon the formula abridged by (6) and (7), in [1], [2] a calculation is proposed (named BotBuster), which shows

Algorithm: $\hat{\mathcal{B}}$=BotClusterBuster(traffic patterns, ϵ, κ, ξ)

$\mathcal{N} = \{1, 2, \ldots, N\}$; $\hat{\mathcal{B}} = \emptyset$
for $i \in \mathcal{N}$ **do**
  $\hat{\mathcal{B}}_i = \{i\}$
  for $j \in \mathcal{N} \setminus \{i\}$ **do**
    if $\hat{\rho}(\hat{\mathcal{B}}_i \cup \{j\}) < \gamma(\hat{\mathcal{B}}_i, \{j\})$ **then** $\hat{\mathcal{B}}_i = \hat{\mathcal{B}}_i \bigcup \{j\}$
  end
  if $|\hat{\mathcal{B}}_i| = 1$ **then** $\hat{\mathcal{B}}_i = \emptyset$
  if $\hat{\lambda}_{\hat{\mathcal{B}}_i} \leq \frac{\kappa}{1+\kappa} \xi \hat{\lambda}_{\mathcal{N}}$ **then** $\hat{\mathcal{B}}_i = \emptyset$ (cluster expurgation)
end
$\hat{\mathcal{B}} = \bigcup_{i=1}^{N} \hat{\mathcal{B}}_i$

the accompanying fundamental highlights for the case that a solitary botnet (i.e., C = 1) is covered up in the system: I) under the BIC, the genuine botnet is assessed reliably; ii) the calculation has multifaceted nature O(N2), and is further open to parallelization. Be that as it may, there is an issue that disallows effective relevance of the BotBuster calculation to the multi-bunched case tended to in this work. Such issue identifies with the way that (as trial confirmation uncovers) the BIC isn't generally checked by and by. Subsequently, amid its stream, the calculation once in a while creates, alongside the (almost)right botnet, fake gatherings of clients that are not the privilege botnet. In the single-bunch case, such pathology is remediated by picking, toward the finish of the method that sweeps every one of the hubs as turns, the evaluated botnet with the most noteworthy cardinality [1], [2]. Such decision depends on the perception that the cardinality of gatherings incorrectly set apart as botnet is normally considerably littler than the cardinality of a genuine botnet. In the multi-grouped case, deciding on a similar maximum cardinality administer is obviously impeding, since it would choose just the biggest botnet bunch, which may be a to a great extent deficient measure of security to confront the DDoS assault. In this manner, distinctive procedures are vital. In the approaching areas we plan two systems suited to confront a multi-grouped DDoS assault.

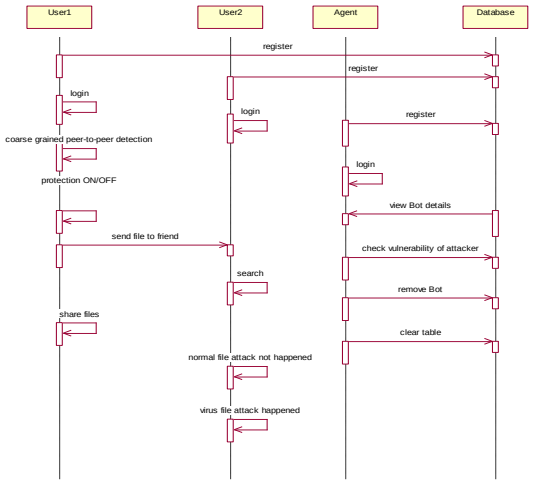
Since bots are malignant projects used to perform gainful pernicious activities, they speak to significant resources for the bot ace, which will naturally endeavor to expand usage of bots. This is especially valid for P2P bots in light of the fact that so as to have a practical overlay organize (the botnet), an adequate number of associates should be constantly on the web. At the end of the day, the dynamic

International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 10 • Issue 2 pp. 437-443 June 2018-Dec 2018 www.csjournals.com

time of a bot ought to be practically identical with the dynamic time of the basic bargained framework.

The separation between two streams is in this way characterized as the Euclidean separation of their two relating vectors. We at that point apply a bunching calculation to segment the arrangement of streams into various groups. Each of the got bunches of streams, Cj (h), speaks to a gathering of streams with comparable size. For each Cj (h), we consider the arrangement of goal IP delivers identified with the streams in the groups, and for every one of these IPs we consider its BGP prefix (utilizing BGP prefix declarations).

In this module used to decide the topographical area of site guests in view of the IP addresses for applications, for example, misrepresentation location. We can discover the IP address of the assailant.



A. Fundamental Routine for Multi-Clustered Botnet Identification

We begin by analyzing the calculation BotCluster Buster, whose pseudo-code is accounted for at the highest point of this page. We think about the activity of the calculation at a given time age. For effortlessness, reliance upon time is stifled. At first, the calculation chooses the principal client as rotate (this task will be rehashed for all N hubs). Client 1 is at first announced as a bot (ˆB 1 = {1}). At that point, by methods for (6) and (7), it is announced whether clients 1 and 2 frame a botnet. Assuming this is the case, ˆB 1 = {1, 2}, generally B1 = {1}. At that point, it is proclaimed whether the at present evaluated botnet ˆB 1 frames a botnet with client 3, et cetera. Toward the finish of this circle, a competitor botnet bunch ˆB 1 is acquired (if the applicant group has cardinality equivalent to one, it is consequently disposed of). In the wake of repeating such inward circle over the whole arrangement of turns, the calculation winds up with a succession of competitor bunches, specifically, ˆB 1, ˆB 2, . . . , ˆB N. We comment that, uniquely in contrast to the BotBuster calculation of [1], [2], all the competitor botnet bunches created in the middle of the road calculation steps ought to be held, to consider the conceivable nearness of different botnet groups. The circumstance is pictoriallyrepresented inFig. 1:

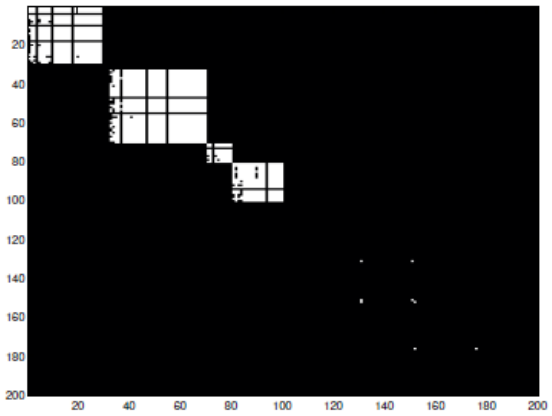
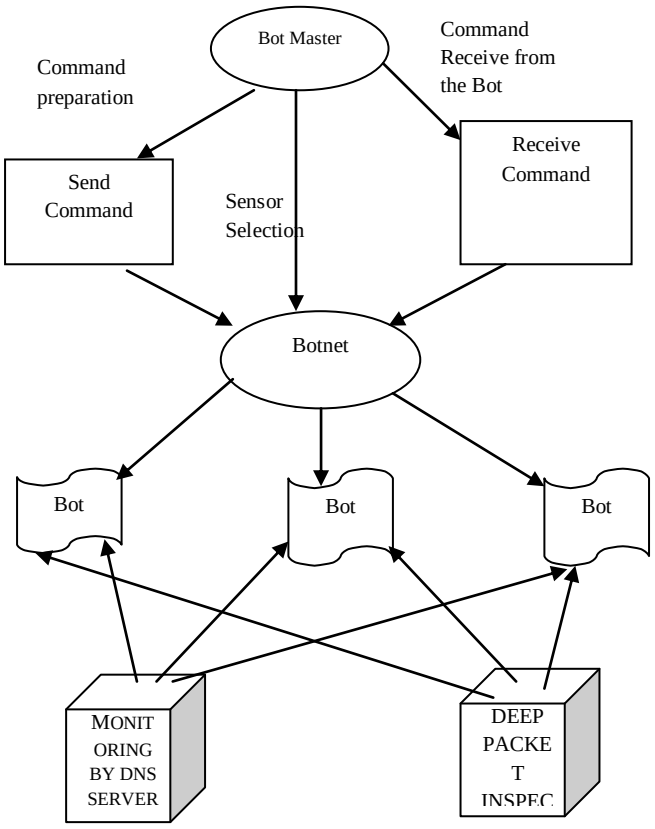


Fig. 1. Candidate botnet clusters: screenshot of the algorithm's output.

Where we show the hopeful botnet bunches assessed by the calculation at a specific time, with reference to a system made by 100 typical clients and 100 bots, with 4 genuine botnet groups, with sizes 10, 20, 30, 40. The I-th "push" of the picture speaks to the yield of the calculation when client I is picked as a rotate. A white pixel signifies "evaluated bot nearness", a dark pixel signifies "assessed bot nonappearance". Likewise, if the (I, j)-th pixel is white, the calculation is evaluating that client j is a bot when client I is picked as rotate. From Fig. 1, we can value the development of 4 bunches, relating to the genuine botnet groups (bots are requested in order to seem very much clusterized in the picture, a decision made just for clearness, since the calculation is unmistakably invariant to changes). Then again, we likewise observe that a few little misleading groups is wrongly recognized by the calculation. The pseudo-code for UnionBotBuster can be recovered from the pseudo-code of BotClusterBuster, by basically avoiding the guideline alluded to bunch expurgation. Be that as it may, since by and by the BIC is just around confirmed, the association lead would support consideration of deceptive bunches. In this way, some refined foundation to choose the best bunches is attractive.

International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 10 • Issue 2 pp. 437-443 June 2018-Dec 2018 www.csjournals.com



IV. OUTPUT RESULTS

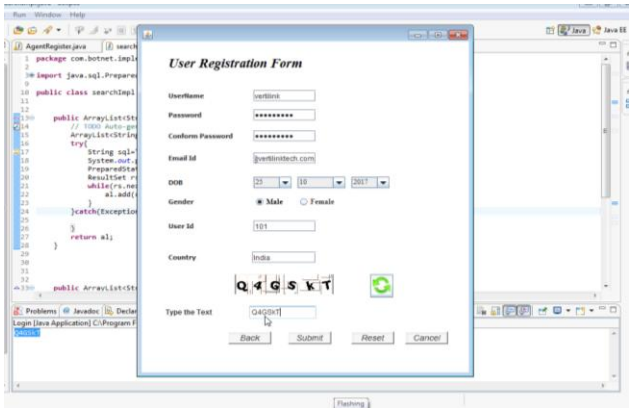


Fig 1: Registration Page

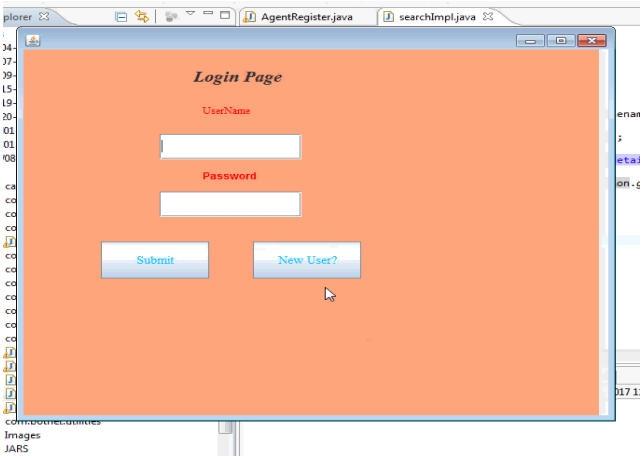


Fig 2: Login Page

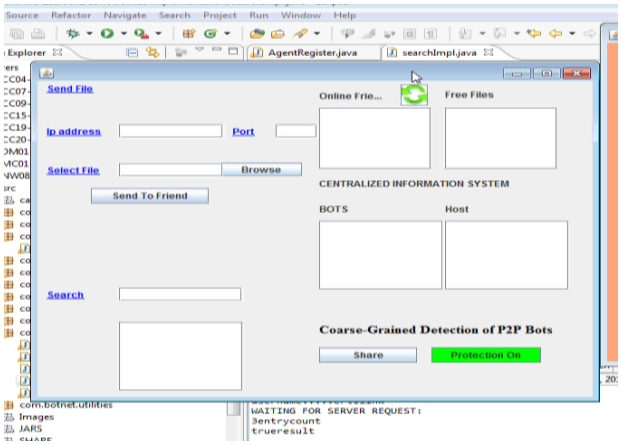


Fig 3: User Home Page

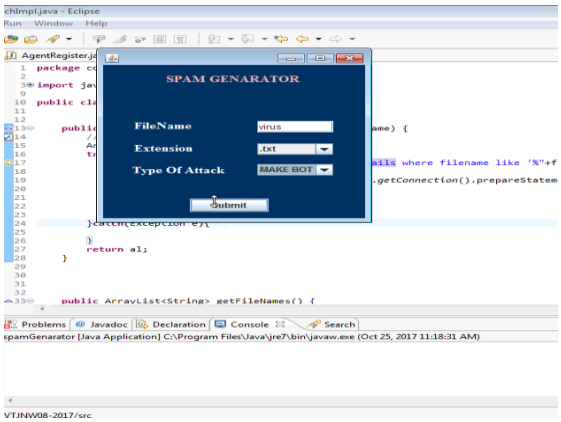


Fig 4: Spam Generator

International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 10 • Issue 2 pp. 437-443 June 2018-Dec 2018 www.csjournals.com

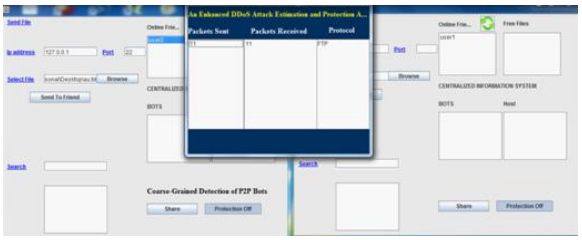


Fig 5: Traffic Innovation

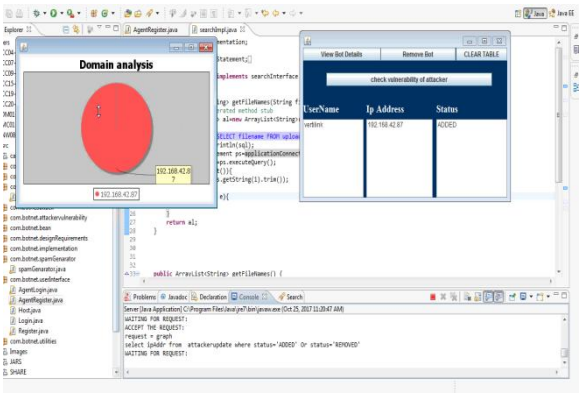


Fig 6: View Bot Details Page

V. CONCLUSION

We displayed, novel botnet identification framework that can distinguish stealthy P2P botnets, whose pernicious exercises may not be recognizable. We thought about Distributed Denial of Service (DDoS) assaults propelled by bots that are proficient to take in the application layer connection conceivable outcomes, in order to abstain from rehashing one basic task commonly. Such upgraded ability of the assailant makes it difficult to distinguish one of those numerous bots depending just on its individual movement designs. The primary commitments of this work are as per the following: I) we presented a formal model for the class of randomized DDoS assaults with expanding copying lexicon; ii) we proposed a surmising calculation went for recognizing the botnets executing such progressed DDoS assaults, and we found out consistency of the calculation, to be specific, the property of uncovering the genuine botnet as time passes; iii) we assessed the proposed procedures on a test bed situation. To give a depiction of the execution conveyed by the BotBuster calculation: for a system with 100 ordinary clients and 100 bots, 90% of the bots are accurately speculated in about a fourth of moment, while the portion of typical clients that are mistakenly prohibited is practically speaking zero. There are numerous inquiries that stay open, and that may merit advance examinations. To say a couple: testing the calculation over more datasets, with a specific end goal to inspect the effect on execution of the idea of the website under assault, as well as the diverse practices of clients surfing on the web; leading a refined union investigation keeping in mind the end goal to describe, from an explanatory perspective, the time expected to achieve a recommended exactness, and the reliance of such time upon the system/botnet estimate and other pertinent framework parameters; analyzing the issue from an ill-disposed point of view where the botnet-distinguishing proof procedure and the sort of DDoS assault are together advanced by searching for harmony arrangements that deal with the aggressor's and protector's clashing prerequisites; summing up the hypothetical examination and instruments to multiclusteredDDoS assaults, where a few botnets (utilizing distinctive imitating lexicons) dispatch all the while their assault.

VI. REFERENCES

[1] V. Matta, M. Di Mauro, and M. Longo, “Botnet identification in randomizedDDoS attacks,” in *Proc. EUSIPCO*, Budapest, Hungary, Aug./Sep. 2016, pp.

2260–2264.

[2] V. Matta, M. Di Mauro, and M. Longo, “DDoS Attacks with RandomizedTraffic Innovation: Botnet Identification Challenges and Strategies,” *IEEETrans. Inf. Forensics and Security*, vol. 12, no. 8, pp. 1844–1859, Aug.2017.

[3] “Taxonomy of DDoS attacks.” http://www.riorey.com/types-of-ddosattacks/#attack-15.

[4] S. Ferretti and V. Ghini, “Mitigation of random query string DoS via gossip,”*Communications in Computer and Information Science*, vol. 285 CCIS,

pp. 124–134, 2012.

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

[6] L. Feinstein, D. Schnackenberg, R. Balupari, and D. Kindred, “Statisticalapproaches to DDoS attack detection and response,” in *Proc. DISCEX*,Washington, DC, USA, Apr. 2003, pp. 303–314.

[7] J. Yuan and K. Mills, “Monitoring the macroscopic effect of DDoS floodingattacks,” *IEEE Trans. Depend. Secure Comput.*, vol. 2, no. 4, pp. 324–335,Oct. 2005.

[8] Y. Xiang, K. Li, and W. Zhou, “Low-rate DDoS attacks detection andtraceback by using new information metrics,” *IEEE Trans. Inf. Forensicsand Security*, vol. 6, no. 2, pp. 426–437, Jun. 2011.

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

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

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

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

[13] L. Gy¨orfi, M. Kohler, A. Krzy˙zak, H. Walk, *A Distribution-FreeTheoryofNonparametricRegression*, 2nd ed. New York: Springer-Verlag, 2002.

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

[15] P. Venkitasubramaniam, T. He, and L. Tong, "Anonymous networking amidsteavesdroppers," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, Jun. 2008.

AUTHOR'S

Ms. ASWATH MUNTAHA has completed B.Tech from Shadan Women's College of Engineering &Technology, Khairatabad, Hyderabad, JNTUH. Presently, she is pursuing her Masters in Computer Science fromShadan College of Engineering and Technology, Hyderabad, TS, India.

Mr. MD ATEEQ UR RAHMAN received his B.E Degree from P.D.A College of Engineering, Gulbarga, Karnataka, India in 2000. In 2004, He obtained M.Tech degree in Computer Science & Engineering from Visvesvaraya Technological University, Hyderbad, India. He is currently pursuing Ph.D from Jawaharlal Nehru Technological University, Hyderabad, India. Presently he is working as Associate Professor in Computer Science & Engineering Dept, S.C.E.T Hyderabad. His areas of interest include Spatial Databases, Spatial Data Mining, Remote Sensing, Image Processing and Networks protocols etc.