International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 02 | Feb-2018 www.irjet.net p-ISSN: 2395-0072

THROUGHPUT EVALUATION OF WIRELESS NETWORKS UNDER VARIOUS ATTACKS

Madhan.S[1], Mumtha.P[2], Priya.V[3],Sivasankari.M[4]

[1]*Assisstant Professor, Dept. of Computer Science and Engineering, University College of Engineering- Thirukkuvalai*
[2,3,4] *Student, Dept. of Computer Science and Engineering, University College of Engineering-Thirukkuvalai Tamilnadu, India.*

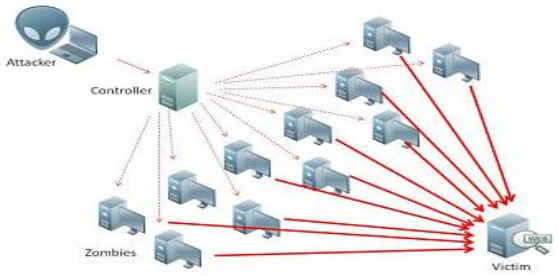
Abstract - *One of the most dangerous attack is Denial-of-Service (DoS). It's a kind of volumetric attack. Proposed a framework to evaluate the network's performance under this attack with various network parameters. Among all the network attacks, the Distributed Denial of service (DDoS) attack is easier to carry out, more harmful, hard to be traced and difficult to prevent. So, this threat is more serious. The DDoS attack is implemented by the attackers by using many different sources to send a lot of useless packets to the target in a short time, which will consumes 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). 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. The main objective of the proposed method is to compare the performance metrics under different attacks. In the proposed system, a hybrid algorithm for botnet identification is implemented to analyze the network performance at the time of attack. The proposed method deploys exclusive nodes called DPS nodes are used in the network to monitor the behavior of the nodes in the network continuously. When the DPS node identifies a node with an abnormal behavior, it will announce that node as a wormhole node to the network by broadcasting a message. All communicative messages will be abandoned by the network from the wormhole node. The proposed scheme detects black hole attack based on which maximum request the node can be received. If in any route reply message, the sequence number were greater than this, the source node would reject the reply on the path. The proposed methods are implemented using NS2 simulator and the results are discussed.*

***Key Words*: IAFV, Wormhole, Botnet, Blackhole.**

1. 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 recommends three basic things: i) developed an abstract model for the above mentioned class of attacks, where the botnet imitates normal traffic by repeatedly learning bearable patterns from the environment ii) generated an inference algorithm that is diplayed to provide a steady assessment of the botnet possibly concealed in the network iii) confirm the legitimacy of the suggested inferential strategy on a test bed environment iv) recognize wormhole nodes using Detection and Prevention System nodes(DPS). Determine black hole nodes using fake RREP in the network. 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.



Dos Architecture

2. RELATED WORK

Nazrul Hoque et al. [1] proposes a comprehensive overview of DDoS attacks, their causes, types with a taxonomy and technical details of various attack launching tools. A detailed discussion of several botnet architectures, tools developed using botnet architectures and pros and cons analysis are also included. Furthermore, a list of important issues and research challenges is also reported in the paper.

Laura Feinstein, Dan Schnackenberg et al. [2] presents methods to identify DDoS attacks by computing entropy and frequency-sorted distributions of selected packet attributes. Jian Yuan and Kevin Mills et al. [3] propose a method for early attack detection. Using only a few observation points, the proposed method can observe the macroscopic effect of Distributed DoS flooding attacks. Also shows that such macroscopic-level monitoring might be used to capture shifts in spatial-temporal traffic patterns caused by various DDoS attacks and then to inform more detailed detection systems about where and when a Distributed DoS attack possibly arises in transit or source networks.

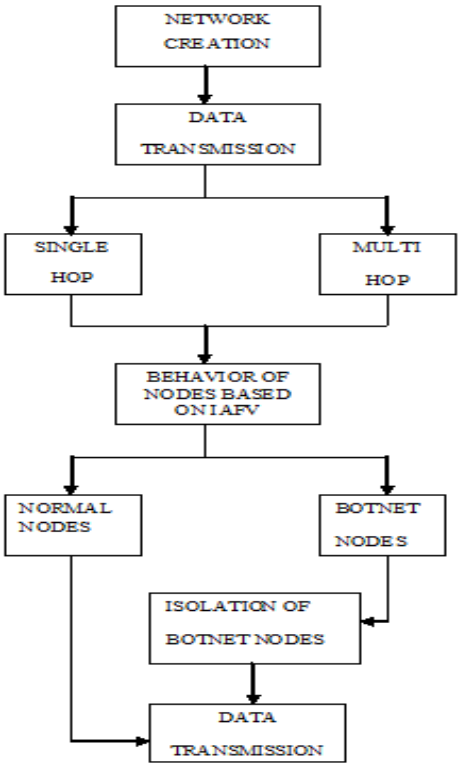
Yang Xiang et al. [4] proposes two new information metrics such as the generalized entropy metric and the information distance metric to detect low-rate DDoS attacks by measuring the difference between legitimate traffic and attack traffic. The Internet Protocol trace back algorithm can find all attacks as well as attackers from their own local area networks (LANs) and discard attack traffic.

Vincenzo Matta et al. [5] propose two strategies to identify the botnet in such challenging scenario, one based on cluster expurgation, the other one on a union rule. Consistency of both algorithms under ideal conditions is ascertained, while their performance is examined over real network traces.

Mariannne et al. [6] proposes a system in which each node will be assigned a cost depending in its participation in routing.

3. EXISTING SYSTEM

Provided a model for the DDoS attack, where the botnet create a general traffic by regularly learning permissible patterns from the environment. Formulated an inference algorithm which is used to determine the possible number of botnets hidden in the network. Verifying the validity of the proposed inferential 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 all bots, without affecting the normal users' activity. Implemented a IAFV 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.



Data Flow Diagram of the proposed model

IP Address Feature Value and Algorithm

The DDoS attack exhibit some key features like the abrupt traffic change, flow dissymmetry, distributed source IP addresses and concentrated target IP addresses, etc. In this scheme, we recommend the concept of IAFV (IP Address Feature Value) to replicate the four features of DDoS attack flow.

4. PROPOSED SYSTEM

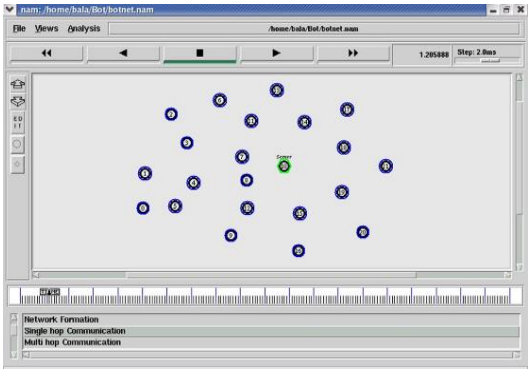
In the proposed system, we are going to identify the botnet, occurrence of warmhole attack and blackhole attack using HYBRID algorithm which is the combination of BotBuster Algorithm and IAFV algorithm. The main objective of the project is identifying the misbehaving node in the network.

MODULES

- Network Formation
- RREQ & RREP to nodes
- Botnet Identification
- WormHole node Identification-(DPS)
- BlackHole node Identification
- Throughput Evaluation

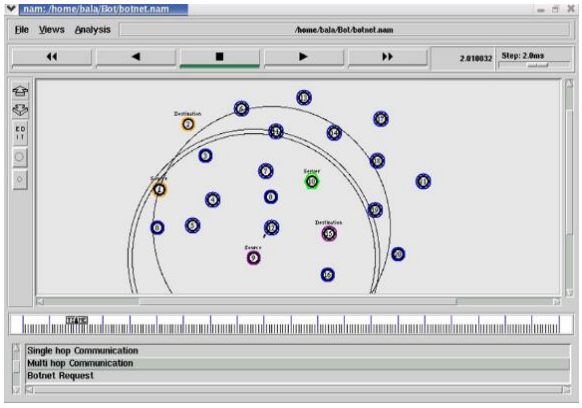
Network Formation

A network is formed using the nodes, DPS nodes and a server according to the attack.



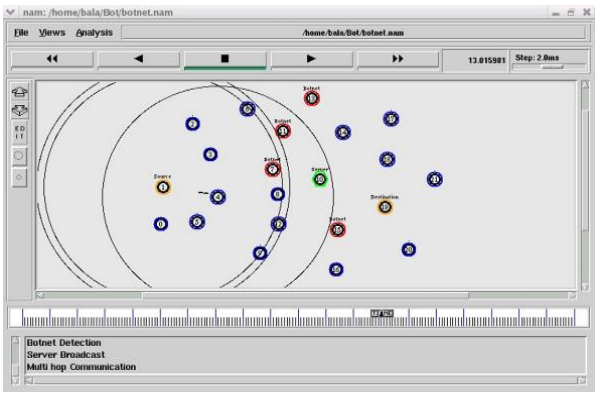
RREQ & RREP to nodes

The nodes in the network are allowed to communicate among them using single and multi hop communication. The values of RREP & RREQ are calculated. Normal nodes will initiate Route REQuest and Route REPly.



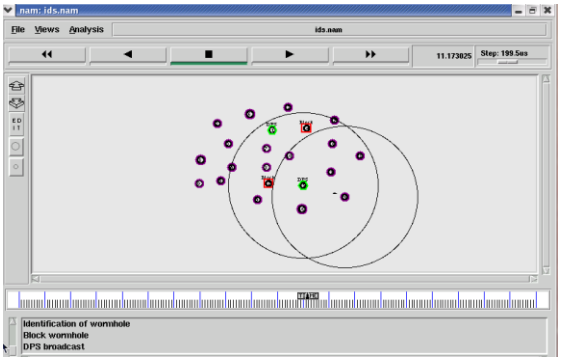
Botnet Identification

The botnet nodes are identified using the RREP & RREQ values.



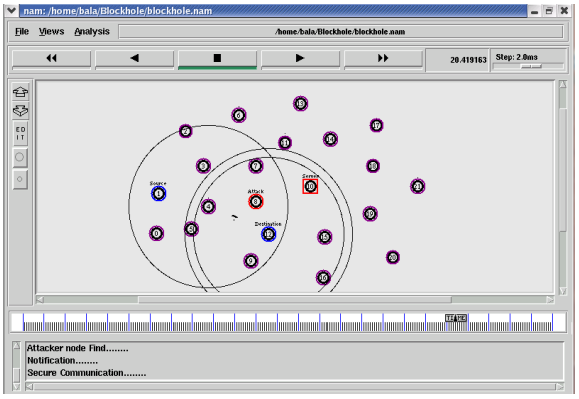
WormHole node Identification-(DPS)

The activities of all nodes are monitored by the DPS node. The nodes that behave abnormally will be monitored carefully Those malicious nodes are called as wormhole nodes and will be intimated to the remaining nodes.



BlackHole node Identification

Each node has to send acknowledgement to the previous node.The node that doesn't forward the packet will be identified as black hole node.



HYBRID ALGORITHM

Algorithm: $\hat{\mathcal{B}}_{\text{new}}$=BotBuster

$\mathcal{N} = \{1, 2, \ldots, N\}$; $\hat{\mathcal{B}}_{\text{new}} = \emptyset$;
for $b_0 \in \mathcal{N}$ **do**
  $\hat{\mathcal{B}} = \{b_0\}$;
  for $j \in \mathcal{N} \setminus \{b_0\}$ **do**
    if $\hat{\rho}(\hat{\mathcal{B}} \cup \{j\}) < \gamma(\hat{\mathcal{B}}, \{j\})$ **then**
      $\hat{\mathcal{B}} = \hat{\mathcal{B}} \bigcup \{j\}$;
    end
  end
  if $|\hat{\mathcal{B}}| > \max(1, |\hat{\mathcal{B}}_{\text{new}}|)$ **then**
    $\hat{\mathcal{B}}_{\text{new}} = \hat{\mathcal{B}}$;
  end
end

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.

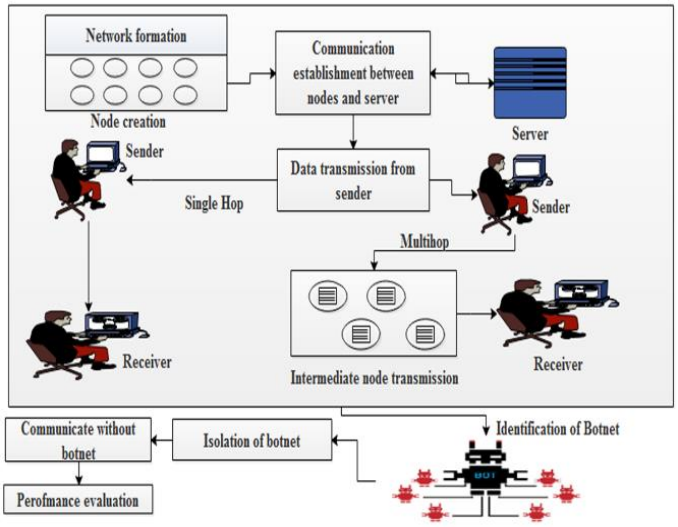
Processing Procedure:

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. $IAFV_F = \frac{1}{m}(\sum_{i=1}^{m} SIP(SDDi) - m)$
    //calculate IAFV of SDD
13. **return** IAFV;
}
}

BotNet Attack

A **botnet** is a number of inter -connected devices, which makes use of the internet with hidden botnets in it. Botnets can be used by the attackers to perform distributed denial-of-service attack (DDoS attack), steal data, send spam, modification of data and allows the attacker to access the device and its connection. The term is usually used with a negative or malicious connotation. Botnets are bunch of compromised nodes hidden in the network. Botnets always used to send request to the server and thereby create network traffic.

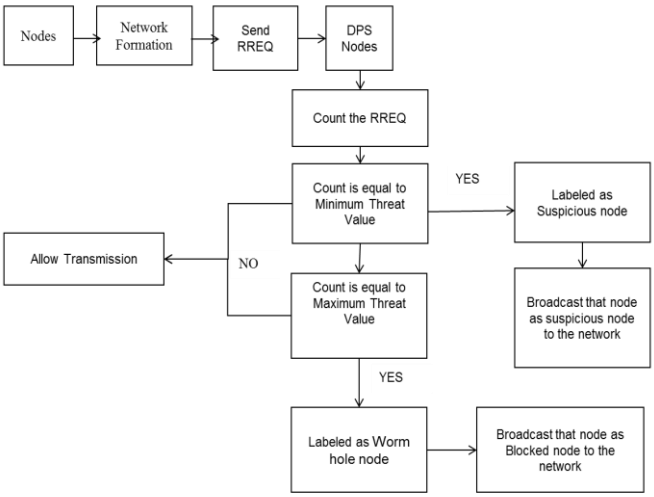
Architecture



WormHole Attack

Wormhole nodes makes use of the fake nodes which showsoff itself as a shortest path from the source node to the destination; because of this the user may get confused and they will proceed through this way. The attacking node records the content of the packets while transferring it from one node to other distinct located node. The attack can be easily done by the attacker without knowing about the basic features of the network by just compromising any authentic nodes.

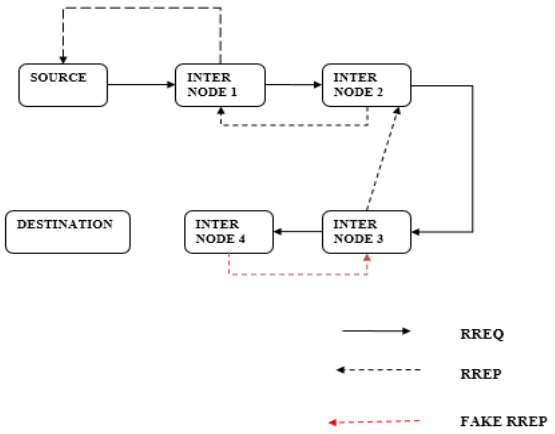
Architecture



BlackHole Attack

Black hole denotes to the region in the network where arriving or departing stream of traffic is discarded, without intimating to the source that the data did not attained its envisioned receiver end.

Architecture



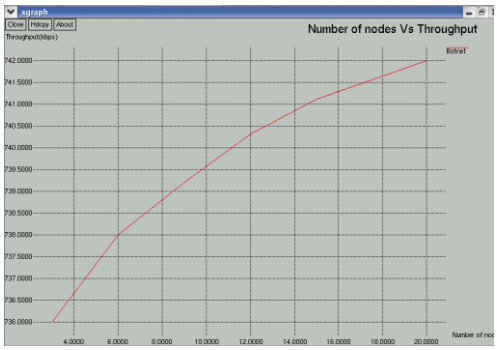
5.THROUGHPUT EVALUATION EXPERIMENT RESULTS

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

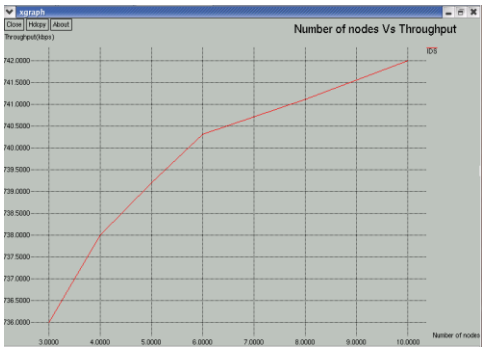
The normal users have no attacking intent, they perform ordinary surfing activity. About 20 min of (application-layer) traffic have been collected, from 10 independent users, which were students and researchers working in the laboratory, and carrying on their surfing activity almost independently. In order to help understanding the nature and significance of the dataset, we report that the total number of TCP flows is about 26800, the median of flows across users is 2846, the minimum number of flows is 1042, the maximum number of flows is 3925, and the average packet size is 776 bytes. Supported by these numbers, and by a trace-by-trace inspection, we conclude that the activity of the users during the monitored period is reasonably sustained, and compatible with typical traffic, meaning that the patterns are neither trivial (users effectively send requests) nor anomalous (users do not overload the destination with huge rates).

The collected streams have been partitioned into chunks of 2 min. In the forthcoming analysis we take two perspectives. In one scenario, the number of normal users is 10; each user has multiple 2-min chunks and, per each trial, chooses randomly one trace per user. In the other scenario, 2-min chunks belonging to the same user have been treated as if they were 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 the same user might feature an additional-and-spurious degree of dependence. On the other hand, this (possible) increase of dependence goes in the direction of (possibly) increasing the fraction of normal users mistakenly marked as bots. Therefore, the simulations performed in the "multiplied" scenario are expected to provide a conservative performance assessment.

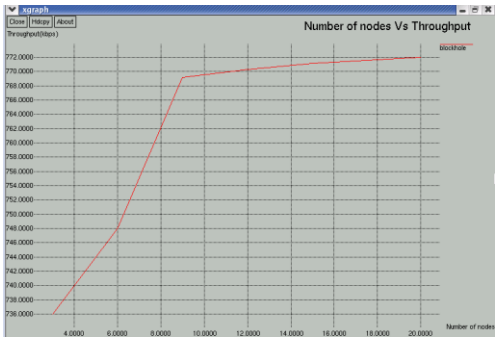
BOTNET



WORMHOLE



BLACKHOLE



The setting considered in this work encompasses naturally the relevant scenario of spoofed source IP addresses, which is becoming 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 randomized DDoS attack considered in this work, the bot traffic streams are constructed by picking subsequent messages independently from an emulation dictionary that is shared among all the bots. Accordingly, a botnet of B nodes

employing a set of A randomly spoofed addresses (with A > B), is equivalent to a botnet of A nodes performing the attack. Since the goal of the network analyst is banning the machines that launch the attack (not associating a physical machine to its IP address), concludes that the performed analysis applies directly to the case of spoofed IP addresses, provided that the number of bots is replaced by the number of IP addresses globally employed by the botnet. For the sake of brevity, such "effective" number will be still denoted by B. There are at least two meaningful regimes to examine the case 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 of the total DDoS attacking rate Bλbot ii) the regime where B increases while keeping the attacking rate constant. As regards the former regime, differently from the analysis of the previous section, varying B corresponds to varying the relative proportion of bots and normal users. This notwithstanding, the evidences arising from the simulation pertaining to such scenario are very similar to those observed and are accordingly not reported. In summary, in this regime the dependence of ηbot upon B is not obvious (no monotonic behavior emerges with respect to B, which is partly explained by 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.

6. 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 DDoS attacks 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 revealing the 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´erez Gonz´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.

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

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

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.

[8] B. 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.

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

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

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

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

[19] 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.