International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 3 Issue: 12
ISSN: 2454-4248
253 – 257

Queuing Based Model for Malicious Packets Detection and Removal in Networks Using Packet Correlation Analysis

Aakash Tiwari
Rungta College of Engineering and Technology, Bhilai
Dept. of Computer Science and Engineering
Bhilai, Chhattisgarh, India
aakashtiwari91@gmail.com

Asst. Prof. Toran Verma
Rungta Colege of Engineering and Technology, Bhilai
Dept. of Computer Science and Engineering
Bhilai, Chhattisgarh, India
Vermatoran24@gmail.com

***Abstract*—** DDoS presents a genuine risk to the Internet since its beginning, where loads of controlled hosts surge the casualty webpage with monstrous bundles. Besides, in Distributed Reflection DoS aggressors trick pure servers (reflectors) into flushing parcels to the nodes. Be that as it may, a large portion of current DDoS location systems are related with particular conventions and can't be utilized for obscure conventions. It is discovered that as a result of being empowered by the same assaulting stream, the responsive streams from reflectors have innate relations: the parcel rate of one merged responsive stream may have straight associations with another. In view of this perception, the Correlation based Detection (RCD) calculation is proposed. The preparatory reproductions demonstrate that RCD can separate reflection streams from authentic ones proficiently and viably, subsequently can be utilized as a useable marker for DDoS.

***Keywords*—** *DDoS attacks, defense, deployment, Types of DDoS Attack, Malicious packets.*

*****

I. INTRODUCTION

A computer virus is a self-sufficient pernicious, self-engendering piece of code that can spread quickly in computer networks. Frequently, the virus proliferates by exploiting uncertain system associations, unprotected shared stockpiling, broken email conventions, Instant Messengers or Peer to Peer (P2P) document offering networks to no appropriately set access rights.

The Simple Mail Transfer Protocol (SMTP), for example, is a standout amongst the most widely recognized engendering implies Received June 10, 2009, whereby the viruses spreads by appending itself as an email connection or by installing itself into HTML documents. In the wake of touching base at the objective PC, it engenders in an indistinguishable route utilizing from focuses on the email tends to establish the casualty's email address book.

Endeavors towards viruses spread demonstrating have expanded altogether finished the previous couple of years, for the most part after a progression of virus outbreaks, for example, CodeRed [15] worm, Nimda [3] worm, Slammer worm [11], Sobig [4], W32/Bagle and W32/Novarg [2], Sober. X, Netsky. P and Mytob. ED [13].

Additionally, as of late, it has been watched that viruses misuse another, social-related, prominent specialized strategy, for example, Instant Messengers (IM) or Peer-to-Peer (P2P) document sharing networks [6]. IM networks give the capacity to exchange instant messages, as well as records supporting distributed document sharing, prompting the quick spread of records that are tainted. Viruses utilize "social designing" techniques keeping in mind the end goal to induce individuals to run noxious projects [5].

With IM, viruses can engender substantially quicker, since attacking potential victims does not include filter operations to obscure or unused IP addresses (something that could likewise prompt catch of the virus). What is just required is an on queue clients' contact list. Much more, there are some IM viruses that endeavor PC vulnerabilities, for example, the ones portrayed in [10], to permit programmed code execution. Such propagation implies are more unsafe and quicker since propagation does not require client mediation. In addition, since a consistently expanding number of individuals utilize IM administrations, new viruses show up the engender by formulating distinctive propagation strategies.

Despite the fact that a developing number of specialists concentrate their endeavors on conceiving new networks for distinguishing and dispensing with viruses, there is by all accounts less exceptional action towards the improvement and assessment of hypothetical models ready to record of how viruses abuse vulnerabilities of PC arranges and proliferate, as needs be.

In [14] Wang et al. propose and break down an viruses engendering model focused at bunched and a tree-like layered system designs. As per this model, viruses deliver duplicates that imitate in the system at a consistent rate without requiring client intercession.

Zou et al. considered the Code Red worm spread conduct utilizing the traditional pandemic Kermack-Mckendrick demonstrate [15]. Newman et al. landed at a diagnostic answer for the permeation limit for "little world" system topologies (see [7, 14]).

 ISSN: 2454-4248
253 – 257

Albert et al. were the first to propose a model for the vulnerabilities of energy law networks with respect to viruses spread [11]. The creators infer that the power law topology is helpless under consider attacks.

Mannan and van Oorschot [9] audit chose IM viruses and abridge their primary attributes, rousing a concise out queue of the system shaped by IM contact records, and a discourse of hypothetical outcomes of viruses in such networks.

II. Intrusion Propagation or Elimination Model

We display a computer arrange as an open Jackson system of interconnected administration focuses (queues) with approaching/active associations with the outside world. Each hub of the system is demonstrated as an M/M/1 queue with boundless size, i.e. no blocking (parcel dismissal) happens when another bundle is chosen to be sent to this node.

The service times of the queue take after the exponential dispersion and the entries the Poisson distribution. At each queue, it is expected that the service time of a bundle is autonomous from the administration times at alternate queues. It is additionally accepted that the bundle transmission time to a system queue is the same for all queues and around, rise to, to the opposite of the transmission speed of the connection prompting the queue.

This is for the most part valid in all parcel exchanged networks and it is likewise valid on the off chance that we accept that the bundle length is little and, along these queues, can be considered as consistent. The administration times for a parcel as it experiences the diverse system queues towards the sink node are autonomous of each other (Kleinrock's Independence Assumption). At whatever point a bundle is adjusted at queue picks the following hub to visit with likelihood or ways out the system with a specific likelihood (Markov directing). The model likewise permits deterministic directing, where the decision for the following not is foreordained. The system is available to entries all things considered, at specific hubs of the system. At every hub there is approaching activity displayed with a Poisson distribution.

The model parameters are the accompanying:

- N: the quantity of queues (organize nodes) in the system.
- λ_i: this is the parameter of the Poisson dispersion utilized to display the entry of specialists in the system (both antivirus or virus operators are viewed as undefined when they land at the system and, along these queues, are considered to frame a solitary Poisson entry process with a solitary parameter).
- μ_i: the parameter of the exponential appropriation accepted for the administration time of the i^{th} queue.
- ρi: the use of the i^{th} queue, which is equivalent to $\frac{\lambda i}{\mu i}$
- (ai; vi; di): number of antivirus and viruses specialists in addition to the quantity of viruses antivirus experiences (destructions) at the i^{th} queue, at the enduring (balance) framework state.
- Pr[a]: the likelihood that a queued assignment conveys an antivirus specialist.
- Pr[v]: the likelihood that a queued errand conveys a virus's operator.
- l_{ij}: the rate at which employments leave queue I and enter queue j.
- q_{ij}: the likelihood that work leaves queue I entering queue j.

III. Literature Survey

In this segment, we survey the existing literature on Distributed Denial of Service attacks.

S. Yu, et al. [16], proposed a dynamic resource allocation method for securing singular clients of cloud amid DDoS attack guaranteeing quality of service during attack. The cloud condition is fit for controlling the resource allotment since it has vast number of resources to dispense to individual client. The resource allocation system utilized as a part of mists assumes key part in relieving the effect of attack by offering access to resources.

V. A. Foroushani, et al. [17], proposed protection against DDoS attacks containing attack packets with spoofed IP addresses called Trace back based safe defense against DDoS loading attacks. The component is executed shut to attack source, rate-constraining measure of movement sent towards casualty.

B. Liu, et al. [18], proposed shared departure filtering for giving insurance against IP spoofing based flooding attacks. They have utilized genuine web dataset for acquiring reenactment comes about. The instrument utilizes the entrance control rundown of autonomous (AS) that contains rundown of tenets for applying entrance/departure separating and unicast reserve path forwarding.

In [19], A. Compagno, et al. introduced barrier against interest flooding conveyed dissent of administration attacks in Named Data organizing. Interest flooding requires restricted resources to dispatch attack. Pending interest table is kept up at switches for maintaining a strategic distance from copy interests. Poseidon structure is presented for identification and relief of interest flooding attacks.

C. Chung, et al. [20], proposed distributed intrusion recognition and countermeasure choice component in cloud frameworks. The NICE framework utilizes interruption recognition conspire at each cloud server for distinguishing and dissecting approaching traffic. The strategy works for virtual cloud framework and makes situation attack diagram for ascertaining helplessness to communitarian attacks.

In [21], S. Rastegari, et al. displayed a quantitative structure for understanding DDoS attack systems and gave defense answers for these attacks. The collaboration amongst

 ISSN: 2454-4248
253 – 257

aggressor and safe defense is exhibited utilizing Red group Blue group practice where Red group speaks to adversaries and Blue group recognizes conceivable vulnerabilities endeavoring to shield them.

IV. Methodology

In this section the proposed system architecture with detailed explanation are discussed. Fig. 2. Shows the proposed system architecture.

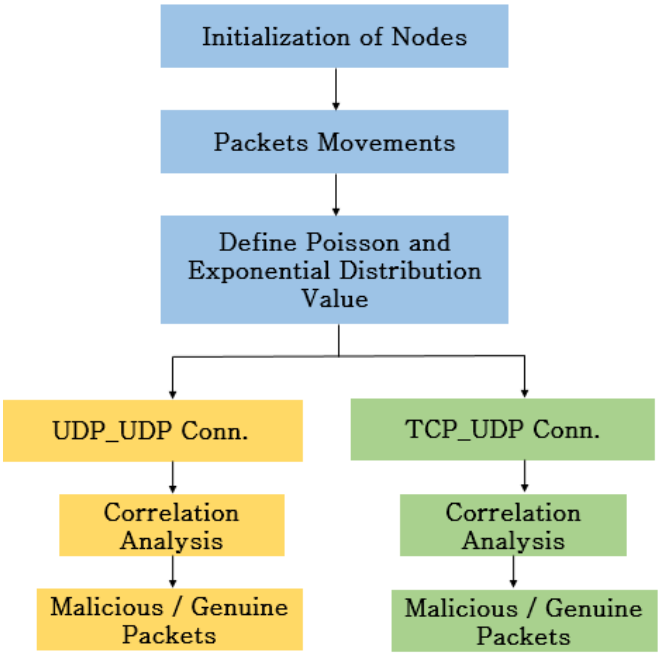

Fig. 1. Proposed system work flow

There are various modules which are responsible for detecting malicious packets. The main algorithm is correlation analysis which is presented in fig. 3. The modules description are:

A. Initialization of Nodes and Packet Movements

The nodes with various configurations are created. There are 4 nodes. In which the client and hacker are one who prepare and send messages to server.

B. Poisson and Exponential Distribution

The Poisson distribution is used to control and manage the arrival rate of the packets over networks. The exponential distribution are used to define the service time of the packets in the network.

The calculation of packet arrival and departure rate are calculated via:

$$P(k \text{ events in interval}) = e^{-\lambda}\frac{\lambda^k}{k!}$$

Where, λ average number of intervals.
And k = 0, 1…

C. UPD-UDP and UDP-TCP Connection Setup

The connection is established for both TCP and UDP. The user can send message via UDP protocol and server responds via UDP. In another scenario, the user sends message from UDP protocol and server response via TCP protocol.

D. Correlation Analysis

When packets arrived at server end, the server checks the packet constantly for any viruses or malicious packets. It calculates the malicious packets via correlation analysis shown in fig. 2.

Algorithm: Correlation Analysis
Input: NS Simulator Configuration and Nodes Description
Output: Malicious and Genuine Packets

Step-01: Locate suspicious flows on an upstream router.

Step 02: Sample the number of packets of suspicious flows per time unit T for a short time, get the value sequence for each flow.

Step 03: Submit sequences to a detection center, which will divide flows into pairs and calculate coefficients for each pair according to Spearman's Coefficient.

Step 04: Compare coefficients for suspicious flows and make decision by using some conditions.
return 0-> no relationship and **1** -> strong relationship and **-1** -> strong negative relationship

Step 05: If confirmed, then discard these flows on the routers

Fig. 2. Shows the Correlation Analysis Algorithm

E. Blocking of Malicious Packets

After analyzing the packets with correlation analysis, proposed algorithm blocks the packets using some measures as shown in correlation analysis algorithm. After that the system performances are measures which are discussed in result section.

V. Result

In this section, result of proposed algorithm and simulation are presented. Basically we worked on two protocols,

a. UDP attack over UDP client
b. UDP attack over TCP client

 ISSN: 2454-4248
253 – 257

A. Initialize Simulator

We have used NS2 simulator, which is responsible for creating and destroying of packets using correlation analysis.

Various parameters which are defined by simulator are:

a. Packet Color: The blue color indicated good and red indicated bad packets.
b. Packet Size: Packet size are randomly chosen by the simulator using passion and exponential distribution.
c. Nodes: There are total 6 nodes participating in transferring packets to each other.
d. Link speed: Bandwidth of the link is 50 Mbps
e. Delay of Link: 100ms
f. Queue Length: 10
g. Simulation time: 100ms

B. Define NAM

It is a TCL programming language based animator. It supports packet level animation. We have used this process to simulate the process of our proposed method.

Network simulator 2 is used for performing simulation. Fig. 3-6 shows the drop rate of packets without and with presence of attacker with UDP and TCP protocol.

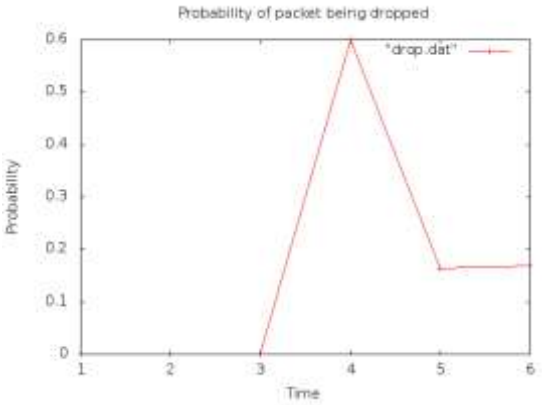

Fig. 3. Packet drop probability, without attacker using UDP to TCP protocol.

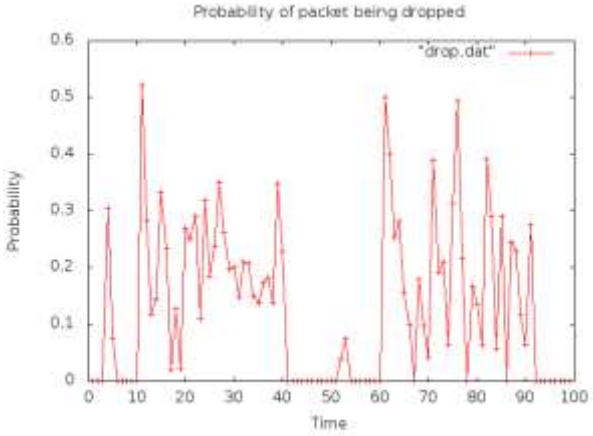

Fig. 4. Packet drop probability, with attacker using UDP to TCP protocol.

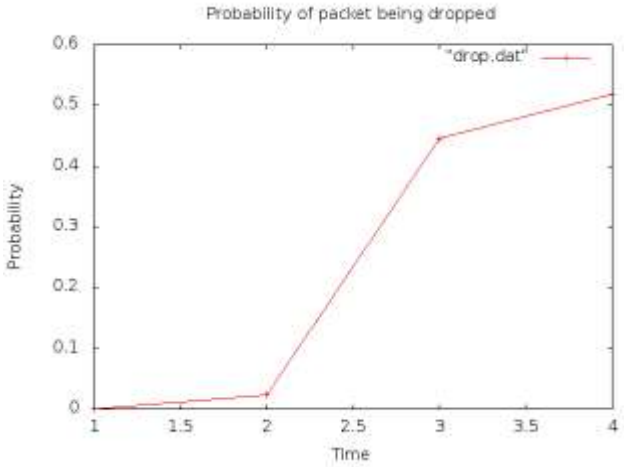

Fig. 5. Packet drop probability, without attacker using UDP to UDP protocol.

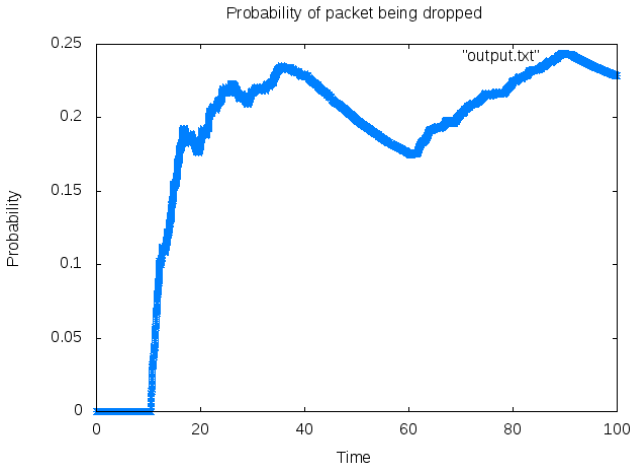

Fig. 6. Packet drop probability, with attacker using UDP to UDP protocol.

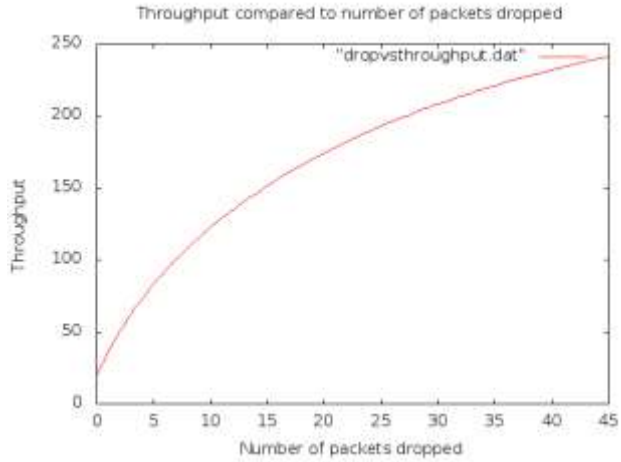

Fig. 7. Throughput of system, without attacker using UDP to TCP protocol.

 ISSN: 2454-4248
253 – 257

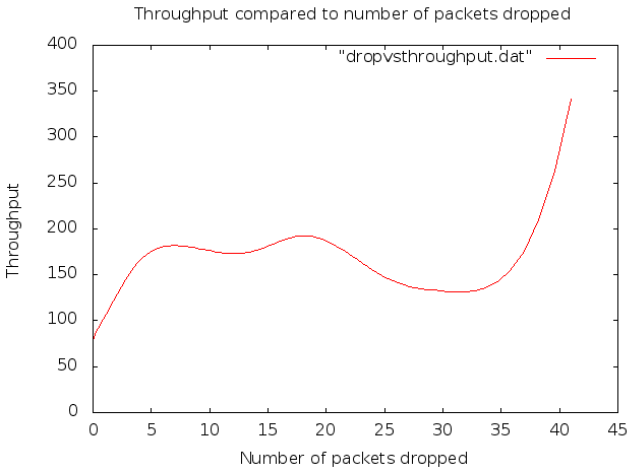

Fig. 8. Throughput of system, with attacker using UDP to TCP protocol.

With proposed algorithm, the system throughput increases, as compared to normal packet drops. We have reached at the normal stage at some point. The algorithm performs wells for attacker using DDoS attacks as shown in fig 8.

If number of packets flowing through the system increases, system throughput increases due to more and more utilization. Higher the link utilization, higher the number of packets dropped. System throughput is almost 2 times in presence of attacker compared to the absence of attacker.

VI. Conclusion

In this paper, we present a novel mechanism in which we have utilized correlation analysis for similar packets detection. The algorithm performs well with the malicious packets generated by the NS2 simulator. It tries to minimize the throughput of the system and also waiting time of genuine packets in the queue.

.

References

[1] D. Bundy, Basic Queuing Theory, Edward Arnold (Publishers) Ltd., 1986.
[2] CERT advisory CA-2004-02.
[3] CERT advisory CA-2001-26 Nimda Worm.
[4] CERT incident note IN-2003-03.
[5] A. Gostev, "Malware Evolution: January – March 2005," Kaspersky Lab Report 4.
[6] IMlogic Threat Center, Symantec Corporation. http://www.imlogic.com/im_threat_center/index.asp
[7] J.O. Kephart and S.R. White, "Measuring and Modeling Computer Virus Prevalence," in Proc. 1993 IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, California, 1993.
[8] L. Kleinrock, On the Modeling and Analysis of Computer Networks, in Proc. of the IEEE, Vol. 81, No. 8, August 1993.
[9] M. Mannan and P. Oorschot, "On Instant Messaging Worms, Analysis and Countermeasures," in Proc. of the 2005 ACM workshop on Rapid malcode (WORM'05).
[10] Microsoft, "How to update your computer with the JPEG processing (GDI+) security update".http://www.microsoft.com/athome/security/ update/bulletins/200409_jpeg_tool.mspx
[11] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver, "Inside the slammer worm," IEEE security and privacy, 1(4), 33–39, July 2003.
[12] J.D. Murray, Mathematical Biology: I. an Introduction, Springer, 3rd edition, 2nd Printing, 2007.
[13] Symantec Internet Security Threat Report Trends for January 05-December 05, Volume VIII and IX, 2005.
[14] C. Wang, J. Knight, and M. Elder, "On computer viral infection and the effect of immunization," in Proc. of the 16th annual computer security applications conference (ACSAC 00) , New Orleans, LA, Dec. 2000.
[15] C.C Zou, W. Gong, and D. Towsley,"Code-red worm propagation modeling and analysis.," in Proc. of the 9th ACM conference on Computer and Communications Security, ACM Press, pp. 138–147, 2002.
[16] S. Yu, Y. Tian, S. Guo, D. Wu, "Can We Beat DDoS Attacks in Clouds?", *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 9, pp. 2245-2254, Sept. 2014.
[17] V. A. Foroushani, A. N. Zincir-Heywood, "TDFA: Trace back based Defense against DDoS Flooding Attacks", *IEEE 28th International Conference on Advanced Information Networking and Applications*, pp. 597-604, May 2014.
[18] B. Liu, J. Bi, A. V. Vasilakos, "Toward Incentivizing Anti Spoofing Deployment", *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 3, pp. 436-450, March 2014.
[19] A. Compagno, M. Conti, P. Gasti, G. Tsudik, "Poseidon: Mitigating Interest Flooding DDoS Attacks in Named Data Networking", *IEEE 38th Conference on Local Computer Networks*, pp. 630-638, Oct. 2013.
[20] C. Chung, P. Khatkar, T. Xing, J. Lee, D. Huang, "NICE: Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems", *IEEE Transactions on Dependable and Secure Computing*, vol. 10, no. 4, pp. 198-211, July/Aug. 2013.
[21] S. Rastegari, P. Hingston, C. Lam, M. Brand, "Testing A Distributed Denial of Service Defense Mechanism Using Red Teaming", *IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA)*, pp. 23-29, April 2013.