# Network Security–Detection of Distributed Denial of Service Attacks

M. Venkata Krishna Reddy, L. Raghavender Raju, D. Jamuna, M.Gayathri

**Abstract -** **Security involving communications and networks is not as simple as it might first appear to the novice. Current intrusion detection and prevention systems seek to detect a wide class of network intrusions (e.g., DoS attacks, worms, port scans) at network vantage points. Unfortunately, even today, many IDS systems we know of keep per-connection or per-flow state to detect malicious TCP flows. Thus, it is hardly surprising that these IDS systems have not scaled to multi-gigabit speeds. By contrast, both router lookups and fair queuing have scaled to high speeds using aggregation. This paper proposes a system which is a novel data structure called Partial Completion Filter(PCF), that which detects a wide variety of DoS and scanning attacks that belongs to several categories (bandwidth based, claim-and-hold, port-scanning).This system can also detect bandwidth attacks that are scalable in the network**.

**Keywords -** Intrusion Detection System, Distributed Denial of Service, PCF, PPD, SBD

## INTRODUCTION I

Bandwidth attacks are a form of denial-of-service attack that aim to disrupt a network service by consuming large amounts of network or server capacity [2]. These attacks usually involve traffic from a large number sources that use fake source IP addresses[16]. Current intrusion detection and prevention systems seek to detect a wide class of network intrusions (e.g., DoS attacks, worms, port scans) at network vantage points [4]. Unfortunately, even today, many IDS systems we know of keep per-connection or per-flow state to detect malicious TCP flows [6]. The motive is to develop Partial Completion Filters (PCFs) *that* can detect both bandwidth attacks and partial completion attacks even when they correspond to small traffic volumes. Partial Completion Filters identify even flows with high imbalance between two types of control packets that are usually balanced. For example, TCP connections consist of equal number of SYN and FIN packets [5]. PCFs can be used to detect bandwidth attacks as they floods a network with large volume of bogus packets in order to overload the network bandwidth. The aim is to consume network bandwidth of the targeted network to such an extent that it starts dropping packets. The packets that get dropped also include legitimate traffic, causing denial of service to valid users.

PCF data structure consists of parallel stages each containing a set of counters. Packets are hashed based on the header fields using multiple independent hash functions and counters indexed by these hash functions are incremented/decremented for the two types of control packets [1]. If all the counters indexed by the hashes of a packet are above a particular threshold (exhibiting high imbalance), the flow is output. At the end of a measurement interval, these counters are all reset. PCFs are used to detect Partial Completion and Bandwidth Attacks. The proposed new methodology aggregates similar kind of packets to fall into one category. And this system provides an easy way to modify the logics (PCFs) at any instance of time. The main aim of PCFs is to operate over large time periods along with a general characterization of SYN floods. This system detects bandwidth based, partial completion DoS attacks, and also scan-based attacks.

## SECTION II

### 2.1 EXISTING SYSTEM

The existing systems like Netscreen, Frontier, etc are the well known Denial of Service attack detection systems [11]. These systems use hard-coded programs for detecting each DoS attack [12]. All the programs should be executed to detect the attacks at the same time, which consumes more CPU time and cost [2]. Improving the performance of detection is a challenging task [13]. Because of all these Intrusion Detection Systems (IDS) uses hard coded programs, and are placed in the embedded device which will be in binary format, there by users cannot modify the logics of the existing programs, once the product has been released [16]. All these IDS work on Per Packet basis Detection or Per Session Basis Detection [3]. These two approaches fail in the case of DoS and DDoS attacks.

### 2.2 PROPOSED SYSTEM

This paper proposes a new methodology to aggregate similar kind of packets to fall into one category, there by CPU time and cost can be reduced. This system also provides an easy way to modify the logics (PCFs) at any point of time and it can also detect the attacks that do scanning and the attacks that cause the server to crash.

The Proposed System detects Distributed Denial of Service attacks, Denial of service attacks, and works on multi-gigabit networks. And this is a system which works on simple logic called Partial Completion Filters (PCF). In the mentioned IDS/IPS devices, they are using a separate detection program for detecting DoS attacks. Because of these logics the systems fails in the case of DDoS attacks. DDoS attacks easily bypass these security systems.

In our proposed system the Implementation and maintenance of PCFs are very easy and friendly in nature. Because of this simple logic our system can work on multi-gigabit networks (PCF logic takes very less memory for maintaining the each system statistics).

Most of the today's IDS/IPS Systems are designed or scaled to detect attacks on per packet basis or per session basis [3]. Because of these approaches IPS/IDS fails to detect most of the DoS or DDoS attacks [9]. If the IPS/IDS is capable to detect small packets, then this kind of systems fails to protect Multi-Gigabit networks [15]. The main aim of this project is to design and implement an IPS which can work on independent of bandwidth or on the capacity of the network by using novel partial completion filters.

## SECTION III

## 3. IMPLEMENTATION

### 3.1. Working Principle of PCF

The working nature of Partial Completion Filter [1] is shown by the following figure.

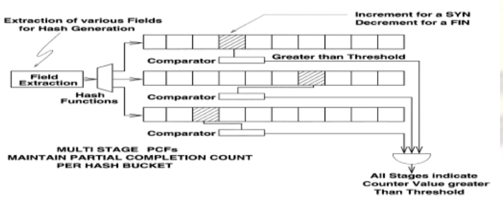
Extraction of various Fields for Hash Generation
Increment for a SYN Decrement for a FIN
Field Extraction
Hash Functions
Comparator
Greater than Threshold
Comparator
Comparator
MULTI STAGE PCFs MAINTAIN PARTIAL COMPLETION COUNT PER HASH BUCKET
All Stages indicate Counter Value greater Than Threshold

**Figure: Partial Completion Filters (PCF) Model Diagram**

### 3.2. Field Extraction

In this model Field extractor extracts the recordable values of each flowing packet and stores them in the database.

For example, if a packet is flowing from Ext-Sys1 to Int-Sys1 then Field extractor extracts the Ext-Sys1 IP-Address, Port number and Int-Sys IP-Address and Port number and the important field values, and submits them to the database of Sensor.

### 3.3. Hash Function

Based on the database values Hash function generates a unique value based on the filter specified [3]. For example if the hash function is
" <Same Destination IP><Same Destination Port> ",. Then hash function gives similar kind of packets which falls under the specified filter.

### 3.4. Filter Threshold

Filter threshold is a reconfigurable value, which is used to indicate the maximum allowable value for the specified filter [10]. For example, For above mentioned filter, the threshold is configured to 256, then comparator checks for the maximum of 256 filtered values, if exists then immediately log will be generated to the admin of the IDS.

### 3.5. Comparator

Comparator maintains a counter for each filter. If detection rate reaches or exceeds the threshold specified to the filter, then log is generated and counter will be reset to the zero [1].

### 3.6. Applying PCFs for Attack Detection

PCF Application is implemented to detect both Portscan attacks and Synflood attacks.

### 3.7. Bandwidth attack :

***Filter Used:***

<any source ip><any port><broadcast ip><any port>
Or
<icmp no destination found msg packet>

Bandwidth attacks consumes the bandwidth of the network and packet may or may not be destined to the internal machine. If more number of icmp no destination message packets found in the network then this kind of situation can be treated as smurf attack. Or any SYN or icmp packet is destined towards broadcast / network address and the source ip is internal network ip then this kind of packet can be detected with the threshold value 1 and with the above filter.

## SECTION IV

**4. Empirical Results:** The implementation can be shown in a stand alone system ( OS : Windows XP ) where VMware is used to create virtual environment with two systems. The two systems are linux installed, created with the help of VMware.

The stand alone system and other two linux installed systems are differentiated by their IP addresses. System 1( linux installed ) acts as web server where my application resides. System 2 ( linux installed ) is used to send attacks by different IP addresses, acts as a attacker. PCF logic is applied to detect various attacks. The attack information can be viewed in stand alone system (system 3) by valid login.

## CONCLUSIONS V

In this paper we have presented a novel system based on the flow balance heuristic to detect and filter DoS bandwidth Attacks. It appears to be widely perceived that detecting intrusions scalably within the network is a bad idea. Unfortunately, that causes security devices to choose between performance (which requires low memory) and completeness (which appears to require per-flow state). This Proposed System is a gentle first step towards suggesting that this tradeoff may not be as Draconian as is commonly thought. We believe that aggregated solutions cannot work without causing unacceptably high false positives, my paper shows some progress for bandwidth based and partial completion DoS attacks. The efficiency and accuracy of the proposed logic makes it highly suited for implementation in routers. This is fortunate because market researchers have already begun to warn that increases in total ownership costs for end node and edge solutions require the network to play a proportionately larger share in detecting and combating network intrusions. This System explores this possibility in the specific context of DoS attacks and scan attacks.

## ACKNOWLEDGEMENT

The authors express their deep gratitude to the Principal and the Management members of JPNCE for their encouragement and extensive support in preparing and publishing of this paper.

## REFERENCES

[1] Ramana Rao Kompella, Sumeet Singh, and George Varghese, “Onscalable Attack Detection in the Network,” ACM Transactions on Networking, Vol. 15, No. 1, February 2007.

[2] R. Chang. “Defending against flooding-based distributed denial-of-service attacks: a tutorial.” In *IEEE Communications Magazine*, Vol. 40 No. 10, Oct 2002, pp. 42-51.

[3] P. Ferguson and D. Senie. “Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing.” RFC2827, May 2000, http://www.ietf.org/rfc/rfc2827.txt.

[4] L. Garber. “Denial-of-service attacks rip the internet .”In *IEEE Computer*, Vol. 33 No. 4, April 2000, pp. 12-17.

[5] T. Gil and M. Poletto. “MULTOPS: a data-structure for bandwidth attack detection.” In *Proceedings of the 10th USENIX Security Symposium*, August 2001, Washington D.C., USA.

[6] J. Ioannidis and S. Bellovin. “Implementing Pushback: Router-Based Defense Against DDoS Attacks.” In *Proceedings of the Network and Distributed System Security Symposium (NDSS 2002)*, February 2002.

[7] K. Kendall. “A Database of Computer Attacks for the Evaluation of Intrusion Detection Systems.” Master’s Thesis, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, 1998.

[8] R. Lippmann, et al. “Analysis and Results of the 1999 DARPA Off-Line Intrusion Detection Evaluation.” In *Proceedings of the Third International Workshop on Recent Advances in Intrusion Detection (RAID 2000)*, pp. 162-182.

[9] K. Park and H. Lee. “On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack.” In *Proceedings of IEEE INFOCOM 2001*, April 2001, Anchorage, Alaska, USA, Vol. 1, pp. 338-347.

[10] T. Peng, C. Leckie and R. Kotagiri. “Adjusted Probabilistic Packet Marking for IP Traceback.” In *Proceedings of the Second IFIP Networking Conference (Networking 2002)*,19-24 May 2002, Pisa, Italy.

[11] Mazu Publishing. [Online]. Available: http://www.mazu.com

[12] Arbor Networks. [Online]. Available: http://www.arbornetworks.com

[13] H.Wang, D. Zhang, and K. Shin, “Detecting SYN flooding attacks,” in *Proc. IEEE INFOCOM*, 2002, pp. 1530–1539.

[14] V. Paxson, “Bro: A system for detecting network intruders in realtime,” *Computer Networks*, vol. 31, no. 23–24, pp. 2435–2463, 1999.KOMPELLA *et al.*: ON SCALABLE ATTACK DETECTION IN THE NETWORK 25

[15] K. Levchenko, R. Paturi, and G.Varghese, "On the difficulty of scalably detecting network attacks," in *Proc. 11th ACM Conf. Computer and Communications Security*, 2004, pp. 12–20.

[16] R. Keyes, "The Naptha DoS vulnerabilities," [Online]. Available: http://www.cert.org/advisories/CA-2000-21.html.

**M. Venkata Krishna** Reddy, Working as Assoc. Professor in CSE Dept. Jayaprakash Narayan College of Engineering, Mahabubnagar, M.Tech(CSE) from Vidya Vikas Institute of Technology, Hyderabad. B.Tech(CSE) from Sri Kottam Tulasi Reddy Memorial College of Engineering, Gadwal. His areas of Interest are in Mobile Adhoc Networks, Data Mining, Networking and guided M. Tech and B. Tech Students IEEE Projects.

**L. Raghavendar** Raju Working as Assoc. Professor in CSE Dept. Jayaprakash Narayan College of Engineering, Mahabubnagar, M.Tech(CSE) from Sree Datta Institute of Engineering, Hyderabad B.Tech(CSE) from Jayaprakash Narayan College of Engineering, Mahabubnagar His areas of Interest are in Networking, Data Mining, Wireless Sensor Networks and guided M. Tech and B. Tech Students IEEE Projects.

**Prof.D.Jamuna**, Working as Professor & Head of CSE Dept. Jayaprakash Narayan College of Engineering, Mahabubnagar, M.Tech(SE) from School of Information Technology, JNTUH, Hyderabad. BE(CSE) from Vijayanagara Engineering College, Bellary. Experience 15 Years in Teaching Profession. Her areas of Interest are in Wireless Sensor Networks, Data Mining, Networking and guided M. Tech and B. Tech Students IEEE Projects. She is a Member of CSI.

**M. Gayathri**, Working as Asst. Professor in CSE Dept. Jayaprakash Narayan Group of Educational Institutions, Mahabubnagar, M.Tech(CSE) from Vidya Vikas Institute of Technology, Hyderabad. B.Tech(ECE) from Sri Kottam Tulasi Reddy Memorial College of Engineering, Gadwal. Her Areas of Interest are in Computer Networks, Data Mining.