Sixth Annual IEEE International Conference on Pervasive Computing and Communications

PerCom 2008

17-21 March 2008, Hong Kong

PerCom 2008 Papers Workshop Papers

Search Getting Started

Copyright Information Trademarks Publisher Information

IEEE COMPUTER SOCIETY

IEEE

Proceedings of the

Sixth Annual IEEE International Conference on Pervasive Computing and Communications

PerCom 2008

Proceedings of the

Sixth Annual IEEE International Conference on Pervasive Computing and Communications

17-21 March 2008, Hong Kong

Los Alamitos, California

Washington • Tokyo

IEEE Computer Society Order Number E3113
ISBN 0-7695-3113-X
ISBN 978-0-7695-3113-7
Library of Congress Number 2007941925

Additional copies may be ordered from:

IEEE Computer Society
Customer Service Center
10662 Los Vaqueros Circle
P.O. Box 3014
Los Alamitos, CA 90720-1314
Tel: + 1 800 272 6657
Fax: + 1 714 821 4641
http://computer.org/cspress
csbooks@computer.org

IEEE Service Center
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
Tel: + 1 732 981 0060
Fax: + 1 732 981 9667
http://shop.ieee.org/store/
customer-service@ieee.org

IEEE Computer Society
Asia/Pacific Office
Watanabe Bldg., 1-4-2
Minami-Aoyama
Minato-ku, Tokyo 107-0062
JAPAN
Tel: + 81 3 3408 3118
Fax: + 81 3 3408 3553
tokyo.ofc@computer.org

Individual paper REPRINTS may be ordered at: <reprints@computer.org>

Editorial production by Bob Werner

IEEE Computer Society
***Conference Publishing Services* (CPS)**
http://www.computer.org/cps

Table of Contents

Sixth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom 2008)

Session: Application of Pervasive Systems

Session: Software Engineering, Security, and Privacy

Session: Data Management and Wireless Networks

Session: Context Aware Pervasive Systems

PerCom 2008 Workshops
Table of Contents

Sixth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom 2008)

PWN 2008: The Fourth IEEE PerCom Workshop on Pervasive Wireless Networking

PerEL 2008: The Fourth IEEE International Workshop on Pervasive Learning

CoMoRea 2008: The Fifth Workshop on Context Modeling and Reasoning

MP2P 2008: The Fifth IEEE International Workshop on Mobile Peer-to-Peer Computing

PerWare 2008: IEEE Middleware Support for Pervasive Computing Workshop

WPS 2008: The Second International Workshop on Web and Pervasive Security

ATPC 2008: The First IEEE Workshop on Agent Technologies for Pervasive Communities

PerDev 2008: The First International Workshop on Power-Aware Pervasive Devices

PerCare 2008: First International Workshop on Pervasive Digital Healthcare

Message from the General Chairs

On behalf of the Steering and Organization committees, we are delighted to welcome you to PerCom2008: The Sixth International Conference on Pervasive Computing and Communications. PerCom is an annual conference providing a forum for researchers and practitioners to exchange the new achievements and discuss future development in pervasive computing and communication research and technologies. Following the success of previous conferences, PerCom2008 will be held in Hong Kong. This is the first time that PerCom is held in Asia. We are privileged to serve as the General Chairs of PerCom2008.

This year, we have high quality paper submissions from all over the world. PerCom2008 offers a rich program to its audience spread over five days. Besides the main conference with 25 high quality research papers, the conference program includes the best paper session, keynote speeches, poster papers, 10 workshops, a Ph.D forum, and one panel. The excellent program is a result of the hard work and collective effort of many people and organizations. First, we would like to express our appreciation to the steering and organization committees for their sincere help, dedication, and deep commitment. The strong research component of PerCom2008 is due to the effort of the technical program committee chair and members, the workshop chairs, and the Ph.D forum chair.

First, our special thanks go to Matt Mutka the Program Chair and his team of Vice Chairs and Program Committee members who have done an outstanding job in carrying out the paper review tasks. Second, we would like express our appreciation of the contributions of the Workshop Chairs, Jadwiga Indulska and Cho Li, and PhD forum chair, Joseph Ng. We also would like to thank the keynote chair, Sajal Das. Our special thanks go to Mohan Kumar—the steering committee chair, Cathy Jiao, Daniela Nicklas, and Yuanchun Shi—the publicity chairs, and Gergely Zaruba—the finance and registration chair. We would like to thank Allan Wong, the Local Arrangement Chair, for carefully planning the events, and Miaomiao Wang, the conference web master, for designing and maintaining the web site. We also would like to extend our appreciation to the local organizing committee and all the student helpers for their great efforts in making the local arrangements and organizing an attractive social program. Without their dedicated help and diligent work the conference would not be such a success.

We would like to thank all the sponsors of the conference, including The IEEE Computer Society, The Hong Kong University of Science and Technology, the Hong Kong Polytechnic University, University of Texas at Arlington, The Croucher Foundation, K.C. Wong Education Foundation, IBM Research, Google and Elsevier Publications.

Fianally, we would like to take this opportunity to thank all the authors and audience of PerCom, many of whom have traveled great distances to participate in this workshop and make their valuable contributions.

Lionel Ni
Hong Kong University of Science and Technology

Jiannong Cao
Hong Kong Polytechnic University

Message from the Program Chair and Vice Chairs

We are pleased to announce an excellent technical program for the 6th International Conference on Pervasive Computing and Communications. The program covers a broad cross section of topics in pervasive computing and communications. This year, 160 papers were submitted for consideration to the program committee. As a result, the selection process was highly competitive, and the result is a program of high-quality papers.

The review process was carried out in two phases. Each paper was assigned to three members of the program committee. In the first phase of the review process, program committee members were asked to nominate papers for full review; approximately 5 percent of the papers were rejected in this phase due to violations of the submission guidelines, relevance to the conference scope, or because they were not deemed to be competitive with the remaining papers given the expected low acceptance rate. The remaining papers received between 3-6 full reviews each, either by program committee members or by carefully selected external reviewers.

The program committee meeting took place in East Lansing, MI on October 27. At this meeting 19 papers were accepted as full papers, resulting in a 12 percent acceptance rate. In addition, 6 papers were accepted as concise contributions and 10 papers were accepted for poster presentation. At the TPC meeting, and in further email discussion, several papers were nominated for the best paper award. A small committee has been formed to select the best paper.

This year's program is organized into nine sessions: best papers, RFID in pervasive computing, pervasive networking, localization and its applications, application of pervasive systems, software engineering, security and privacy, data management, context aware pervasive systems, and the poster session. With such a broad program, we hope that every attendee will benefit listening to several presentations of interest.

We thank the members of the program committee and the external reviewers for their work in preparing the reviews. We thank Lionel Ni (General Chair) and Jiannong Cao, (General Vice-Chair) for their support.

We hope that you enjoy the program at Percom 2008!

Matt Mutka (Chair)
Christian Becker, Anind Dey, Francis Lau, and Gergely Záruba (Vice-Chairs)

Technical Program Committee

Sheikh Iqbal Ahamed	Marquette University
Giuseppe Anastasi	University of Pisa
Stefano Basagni	Northeastern University
Claudio Bettini	University of Milano
Roksana Boreli	National ICT Australia Ltd
Guohong Cao	Pennsylvania State University
Roy Campbell	University of Illinois at Urbana-Champaign
Hojung Cha	Yonsei University
Alvin T.S. Chan	Hong Kong Polytechnic University
Mun Choon Chan	National University of Singapore
Mainak Chatterjee	University of Central Florida
Yuh-Shyan Chen	National Chung Cheng University
Hao-Hua Chu	National Taiwan University
Xiaowen Chu	Hong Kong Baptist University
Marco Conti	Italian Research Council
Diane Cook	Washington State University
John Davis	IBM TJ Watson
Nigel Davies	Lancaster University
Jonathan Englesma	Motorola Research
Alois Ferscha	University Linz
Vinny Cahill	Trinity College Dublin
Silvia Giordano	SUPSI, Switzerland
Tao Gu	Institute for Infocomm Research, Singapore
Jonna Hakkila	Nokia
Robert Harle	Cambridge University
Seongsoo Hong	Seoul National University
Jadwiga Indulska	University Queensland
Cathy (Yu) Jiao	Oak Ridge National Lab
Yuh-Jzer Joung	National Taiwan University
Sneha Kasera	University of Utah
Chung-Ta King	National Tsing Hua University
Mohan Kumar	University of Texas at Arlington
Rodger Lea	Univ. of British Columbia
Dongman Lee	Information and Communications University, Korea
David Levine	University of Texas at Arlington
Yunhao Liu	Hong Kong University of Science and Technology
Qiong (Joan) Luo	Hong Kong University of Science and Technology
Cecilia Mascolo	University College of London
Scott Midkiff	Virginia Tech
Jalal Al Muhtadi	King Saud University
Tamer Nadeem	Siemens Research
Klara Nahrstedt	University of Illinois at Urbana-Champaign
Daniela Nicklas	Univesitaet Stuttgart
Max Ott	NICTA
Jong Hyuk Park	Kyungnam University, Korea
Chiara Petrioli Rome	University La Sapienza
Kay Romer	ETH Zürich
Marcel Rosu	IBM TJ Watson
Kurt Rothermel	University of Stuttgart
Ichiro Satoh	National Institute of Informatics
Gregor Schiel	University of Mannheim
Steve Shafer	Microsoft Research

Albrecht Schmidt	University Bonn, University Munich
Young-Joo Suh	Pohang University of Science and Technology
Xueyan Tang	Nanyang Technological University
Yong-Meng Teo	National University of Singapore
Anand Tripathi	University of Minnesota
Xin Wang	SUNY Stony Brook
Steve Ward	MIT
Li Xiao	Michigan State University
Jingling Xue	University of New South Wales
Zhiwen Yu	Kyoto University
Daqing Zhang	GET/INT France
Frank Zhu	Microsoft

Sixth Annual IEEE International Conference on Pervasive Computing and Communications

Detecting and Tracing DDoS attacks by Intelligent Decision Prototype

Ashley Chonka, Wanlei Zhou, Jaipal Singh
School of Engineering & Information Technology
Deakin University
Geelong, 3220, Australia
{ashley, wanlei, jaipal}@deakin.edu.au

Yang Xiang
School of Management and Information Systems
Central Queensland University
Rockhampton, 4702, Australia
y.xiang@cqu.edu.au

Abstract

Over the last couple of months a large number of Distributed Denial of Service (DDoS) attacks have occurred across the world, especially targeting those who provide web services. IP traceback, a counter measure against DDoS, is the ability to trace IP packets back to the true source/s of the attack. In this paper, an IP traceback scheme using a machine learning technique called Intelligent Decision Prototype (IDP), is proposed. IDP can be used on both Probabilistic Packet Marking (PPM) and Deterministic Packet Marking (DPM) traceback schemes to identify DDoS attacks. This will greatly reduce the packets that are marked and in effect make the system more efficient and effective at tracing the source of an attack compared with other methods. IDP can be applied to many security systems such as Data Mining, Forensic Analysis, Intrusion Detection Systems (IDS) and DDoS defense systems.

Index Terms— IP Traceback, Machine Learning, Decision trees, Distributed Denial of Service, Intelligent Decision Prototype

1. Introduction

Businesses over the last decade have invested heavily in web technologies to provide better services to their clients and customers. With such heavy investment, any form of disruptions to these services can cost a business not just loss of profit but also the high cost of repairs to fix the problems. One of the most deadly forms of disruption is Distributed Denial of Service (DDoS) attacks. According to the Prolexic Zombie Report 2007, over 4000 DDoS attacks happen daily [29]. A DDoS attack is an explicit attack to prevent legitimate users from using their desired resources [4][5].

In a 'general' DDoS attack, the attacker usually disguises or 'spoofs' the IP address section of a packet header in order to hide their identity from their victim. This makes it extremely difficult to track the source of the attack. IP traceback [1][2] is a scheme that has been researched for at least ten years and provides an effective way to trace the source of DDoS attacks to its point of origin.

In this paper, we are applying machine learning principals to a packet marking system that has the characteristics of Probability Packet Marking (PPM) [6] and Deterministic Packet Marking (DPM) [7]. This machine learning mechanism, called Intelligent Decision Prototype (IDP), provides a more flexible and efficient way of marking packets compared with other IP traceback mechanisms, such as logging, messaging, PPM, DPM, Link testing and hop-counting.

IDP works by marking only packets that have the "appearance" or attributes of known and unknown DDoS attacks. The DPM systems marks every packet, while PPM systems mark every 1/20000 packet. This targeted marking is an advantage for IDP compared with other systems like DPM and PPM. IDP minimises the need to modify the IP protocol, since it only marks selected packets identified as an attack packet.

The rest of the paper is organized as follows: Section 2 covers related work that has been covered on IP traceback and machine learning. In section 3, the details of IDP are introduced, which include system design and implemented. Section 4 shows how IDP improves the traceback mechanism. Finally, the challenges and conclusion are discussed.

2. Related Work

Current IP traceback schemes can be categorized into two main areas, proactive and reactive [2]. Reactive traceback systems are responses to an ongoing attack, thereby must remain active during the

0-7695-3113-X/08 $25.00 © 2008 IEEE
DOI 10.1109/PERCOM.2008.76

attack, otherwise they cannot react to a DDoS attack. This makes reactive systems, like Control flooding [10] and Input debugging [11], unsuitable for the internet but is best suited for controlled networks.

One of the problems with reactive schemas is that they require ISP co-operation, which usually is not usually forthcoming due to a loss of competitive advantage.

In contrast, proactive schemas actively record tracing information as packets transgress the network, in which the victim can reconstruct the path taken by the attack packets and subsequently identify the source of the attack. Some examples of proactive schemas include messaging [12][13], logging [14][15] and packet marking [16][17]. Intelligent Decision Prototype (IDP) can be used in most of these areas but the main focus of this paper is the packet marking area.

2.1. Reactive methods

Link testing methods fall into the reactive category, which includes input debugging [10] and controlled flooding methods [11]. The main idea of Link testing is to begin at the victim end and find where the attack came from upstream links. This is accomplished by testing all possible routes to see where the attack packet might have come from.

Link testing has a number of advantages, such as, changes to the network infrastructure or to the internet protocols are kept to a minimum. Link testing also keeps traffic overheads to a minimum.

Link testing has a number of limitations. Firstly, it takes time and computer resources to establish a trace on the route taken by the attack packets. Secondly, if the attack packets transgress through the backbone network, then reconstructing the path is not possible. Thirdly, Link testing methods will not work unless it has enough attack packets to be able to trace back to the source. Lastly, Link testing is not suited to handle DDoS attacks, since DDoS incorporates multiple sources for the attack. Thereby, the resources and time that Link testing would have to invest in would be so high that itself could be called a denial of service (DoS) [2].

2.2. Proactive methods

The most well known proactive method for IP traceback is called messaging. In the paper by Bellovin et al., they proposed an ICMP message to find the source of spoofed attack packets [12]. The paper by Mankin et al. modified Bellovin's work by proposing an intension-driven ICMP traceback [13]. These methods run into trouble if there is a small amount of attack packets embedded into the attack traffic, thereby rebuilding the real path from such attack traffic is extremely difficult. The main problem with messaging schemes is that ICMP packets are often dropped by routers since false ICMP messages could be easily used and implanted by attackers.

Another proactive method for IP traceback is logging [14][15]. The logging method goal is to store traffic data for analysis at a later time. A hash-based logging method is one example of the logging method goals [24]. Baba et al. [15] proposed a system using tracing agents (tracers), which are deployed throughout the network to log attack packets and manage the agents. The main advantage of a logging system is that it can find the source of an attack based on a single packet. The problem with a logging system is that it needs large amounts of processing and storage requirements. This makes the logging system difficult to deploy on a wide scale.

A packet marking system is the last of the proactive methods. The two best known systems are Probabilistic Packet Marking (PPM) and Deterministic Packet Marking (DPM). Probabilistic Packet Marking, proposed by Savage, et al. [6], holds the assumption that attacking packets are much more frequent than normal packets that come into the router or host. Once the 20,000th packet enters the router, the PPM system marks this packet with probabilistic information, which will then allow the victim to reconstruct the path to the packet source.

Peng et al. [19] proposed an adjustment to the PPM system, in order to reduce the number of packets needed to reconstruct the attack path, thereby making it a more efficient system. Inside the packet header, PPM uses the fields that are rarely used within the IP header to mark the packets. The advantage of PPM is that it needs less attack traffic than an ICMP traceback system to be able to reconstruct the path back to the source, but has difficulties if multiple attacks sources increase.

Unfortunately, PPM suffers from mark spoofing, where an attacker spoofs the source address of the attack packet. This causes PPM to trace the attack to the wrong source [7]. PPM also reveals all the paths taken by the attack packets (full-path traceback system). This type of information is unnecessary since the goal of any traceback system is to find the source of attack, not every path taken by the attack packet to reach the victim.

Deterministic Packet Marking [7] was introduced in order to overcome the shortcomings of PPM. This method has many advantages over the other traceback systems, since it is simple to implement, has no bandwidth requirements, uses less overheads, and is free from false marking. The problem with DPM is in

order to perform a successful traceback you need enough packets to be collected so you can reconstruct the attack path [2].

Other proactive packet marking systems include Path Identifier [20], Authenticated Marking Scheme [21], polynomial path reconstruction and Flexible Deterministic Packet Marking (FDPM) [22].

2.3. Machine Learning

Machine Learning is a field that is divided into a broad range of categories, ranging from supervised learning, unsupervised learning, analytical learning, active learning, reinforcement learning and semi-supervised learning.

Supervised learning involves learning functions from labeled data sets [23][24]. Unsupervised learning involves algorithms that form grouping clusters to learn patterns and associations with data sets that have no attached labels [24]. Analytical learning uses data sets that are not labeled, but instead have background knowledge [25]. Reinforcement learning uses algorithms to learn control polices through a reinforcement environment [26]. Active learning [28] uses unlabeled data sets that can be labeled in sequential process. Lastly, Semi- Supervised learning [25] deals with data sets that are combination of labeled and unlabeled examples.

3. Intelligent Decision Prototype

3.1. Introduction

Intelligent Decision Prototype (IDP) is a supervised machine learning application that is employed into two parts. The first part, called Pre-Marked Decision (PMD), is located at the edge of the routers, like DPM. Figure 1 shows how the PMD is setup. The packet comes into the router, and is then analysed by PMD for attributes that make up a DDoS attack. If the traffic is legitimate, the packet is forwarded onto the next router or host. If PMD decides that the packet shows signs that it is not legitimate, it sends it for packet marking.

IDP uses the Deterministic Packet Marking (DPM) method to only mark packets it deems to be illegitimate. We call our packet marker the Intelligent Decision Prototype Marker (IDPM). This makes PMD a more efficient and effective packet marker than DPM, since it does not burden the router to mark every packet regardless whether the packet is legitimate or illegitimate.

The second part of IDP is made up of two sections. One section is to deal with reconstructing the path back to the source of the attack, which will be discussed down below. The second section uses another machine learning method, called Reconstruct And Drop (RAD), to deal with the actual attack packet.

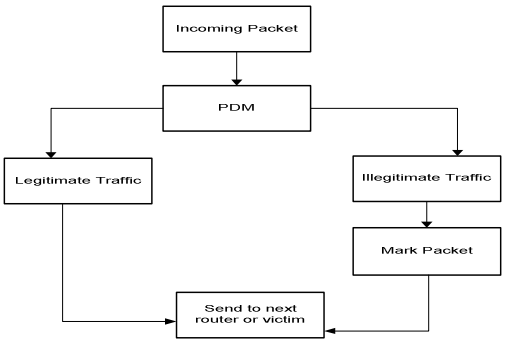

Figure 1. Example of PDM

3.2. Description of IDP

IDP is distributed on the edge routers, as seen in figure 2. As the packet comes into the router, IDP will send the packet for analysis by the PMD, to determine if the packet is legitimate or illegitimate. PMD, as seen in figure 3, is a decision tree that looks for attributes of known/unknown DDoS attacks.

Known DDoS attacks like Trinoo, TFN2K, etc. have certain attributes that can be tested against. Attackers, knowing these attributes, could attempt to modify these known attacks to get around the PMD. These new or unknown attacks are handled by PMD with a new technique called Alternative Decision Making (ADM).

Alternative decision builds upon the assumption that attackers have to employ the same communication channels to accomplish their attacks. These channels can be analysed to see if any new or modified attacks are in progress.

Once an attack has been identified by PMD, it is sent for marking. IDP, in regard to packet marking, is a hybrid method of DPM, PPM and Logging methods.

IDP incorporates a logging technique which allows for reconstruction of the source path using only one marked packet, even though many marked packets are sent to the victim. This is accomplished by using a unique ID mark for each of the edge routers that use IDP, as shown in figure 2.

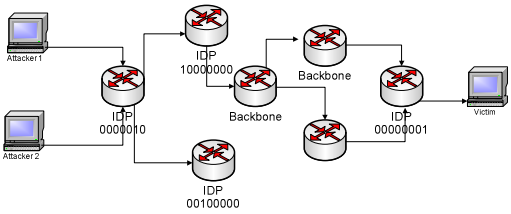

Figure 2. IDP diagram

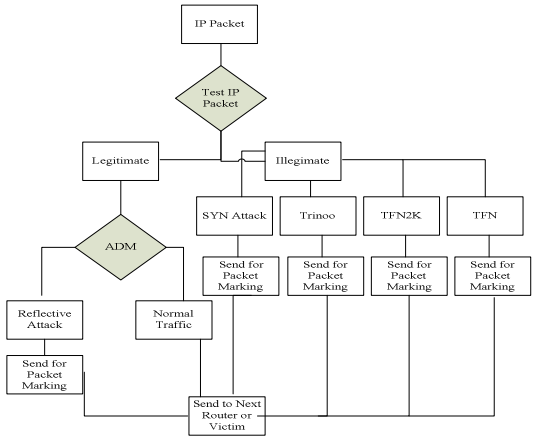

Figure 3. PDM decision tree

Once the packet has been through PMD, it is then forwarded to the next router or to the victim. Once the packet reaches the victim, the victim can reconstruct the source using the unique mark placed within the packet to determine the source location of the received packet.

3.3. Packet Marking

The packet marking algorithm of IDPM, follows the packet marking algorithm of DPM. DPM uses the 16-bit ID field and the reserved 1-bit flag. These fields are rarely used within the packet, so packet fragmentation is kept to a minimum. IDPM will mark each packet with its own unique ID that will remain unchanged for as long as the packet traverses the network. A router in the defence network will have a unique ID marker that is made up of 8bits, such as 0000001 (refer to figure 2).

A DDos victim will be able to identify the ingress router once it reconstructs the unique ID marker from a marked packet. The difference between IDP and DPM is that IDP does not mark packets deterministically, that is it does not mark every packet that enters the router. It only marks the packets that come from the PMD procedure. If the packet is spoofed, IDP will detect such spoof mark and send it to the packet marking procedure to include the correct mark.

Thus, IDPM solves the problem of tracing the wrong path due to spoofed packets, as well as keeping any changes to the IP packet to a minimum since it only marks packets it deems to be illegitimate. IDPM improves the ability to traceback since it only requires one packet to find the source of the attack.

4. Performance Evaluation

Simulations were conducted to evaluate the effectiveness of the PMD section of IDP, particularly the IP traceback procedure to see if it could detect known and unknown DDoS attack packets. The second goal was to see if IDP could successfully be used to trace back the source of the DDoS attack. The following metrics were used for this evaluation:

$$a = \frac{n}{m} \qquad (1)$$

Where a is the average legitimate packets detected by PMD (n) over the total packets (m) that passed through the router each day of the test data.

$$b = \frac{p}{q} \qquad (2)$$

Where b is the average of detected attack packets by PMD (p) over the total attacks packets (q) that were introduced into the data set.

For IDPM traceback we used the following calculations:

$$c = \frac{d}{e} \qquad (3)$$

Where c is equal to the average traceback success (d) over the total packets (e) that the victim received

$$f = \frac{g}{h} \qquad (4)$$

Where f is the average false positives (g) over the total packets that it received.

We also wanted to compare PMD over DPM performance, in which PMD only marks packets that it determines to be DDoS attack packets. We accomplished this by allowing IDP to run without PMD and just let IDPM mark the packets the way DPM does. Then we used the reconstruction data to check the performance against PMD.

4.1. Simulation Setup

To test out IDP and its traceback procedure, we needed a controlled group data set. The reason for this is to be able to determine if PMD and its traceback procedure works. We got this data group from the week 2 data set, 1998 DARPA intrusion detection evaluation data set at Lincoln Laboratory, MIT [28]. The data sets from MIT come in TCP dump format, so we extracted the features we needed and insert them into a MySQL database. These features included SrcIP, DestIP, SrcPort, DestPort and the length of time. We added two extra fields to the table. The first field added was for the PMD decision (0 for legitimate, 1 for

illegitimate). The second field added was to indicate whether the traceback procedure was successful (0 for success and 1 for failure).

4.2. Evaluation

Using the MIT data set, we set out to test to if PMD could detect the DDoS attack packets that we inserted into the data. Figure 4 show's that PMD successfully detected 75-79% of the legitimate traffic in the data set. This means that only 21-25% of the total legitimate traffic was attack traffic. PMD was able to detect 76-81% of the attack traffic. Figure 4 and Figure 5 results show that only a small number of attack traffic were misidentified, thereby we can conclude PMD can classify what is and is not attack traffic to around 75% accuracy.

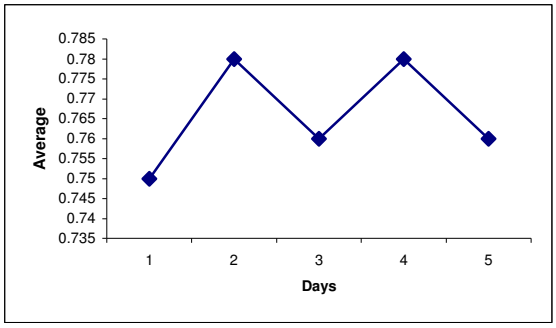

Figure 4. Average legitimate traffic detected by PDM

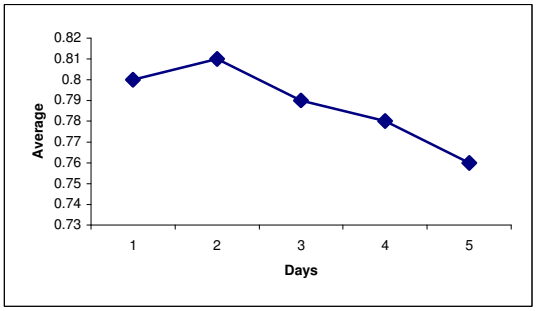

Figure 5. Average attack traffic detected by PDM

Figure 6 shows that IDPM was able to traceback 75-80% of marked packets back to the source. As seen in figure 7, 75-80% of the trace backed packets are DDoS attack packets (true positive).

Lastly, the comparison of IDP and DPM can be seen in figure 8, which shows a legitimate IP address (192.123.0.1). We than ran the IDP program, in which PPM took about 5sec to make a decision whether the packet was legitimate, therefore not requiring any packet marking. DPM on the other hand marked the packet as it came in. Figure 8 demonstrates that IDP is far more efficient than DPM in regard to packet marking.

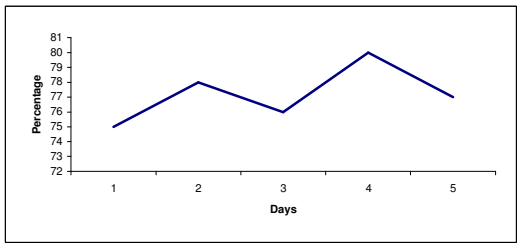

Figure 6. Average traceback by IDPM

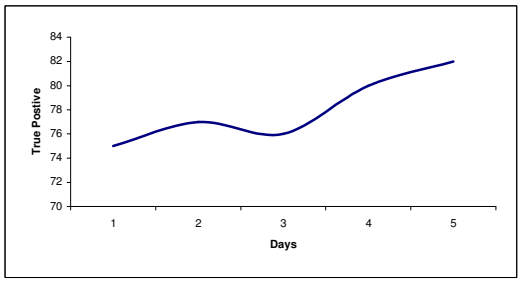

Figure 7. True positives traceback by IDPM

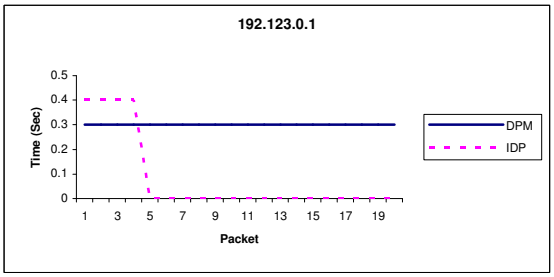

Figure 8. Comparison of PDM and DPM

5. Conclusion and Future Work

In this paper Intelligent Decision Prototype (IDP) was presented. It provides a Pre-Marking Decision (PMD) mechanism to evaluate a packet before the packet is marked for traceback purposes. This makes IDP more efficient and effective than other packet marking schemas (PPM and DPM), since it can't be marked spoofed like PPM and it doesn't have to mark every packet that comes into the router to be able to traceback to the source. We also show that IDP can successfully traceback 75-80% of packets from just one marked packet. In the future, we will be setting up IDP at the Sunet Corporation ISP to begin real-time data gathering and testing of IDP. This will allow us to fine tune IDP to better detect and filter DDoS attacks.

6. Acknowledgements

This research was supported by the ARC Linkage grant (Project number LP0562156).

References

[1] Bhaskaran, M., Natarajan, A.M. and Sivanandam, S.N., (2007), '*Tracebacking the Spoofed IP Packets in Multi ISP Domains with Secured Communication*' IEEE - ICSCN 2007, MIT Campus, Anna University, Chennai, India. Feb. 22-24, 2007. pp.579-584.

[2] Aljifri, M., (2003), '*IP Traceback: A NewDenial-of-Service Deterrent?*' Published By The Ieee Computer Society 1540-7993/03 2003

[3] Kim, Y, Cheong Lau, W., Choo Chuah, M., Jonthan Chao, H., (2006), '*PacketScore: A Statistics-Based Packet Filtering Scheme against Distributed Denial-of-Service Attacks*' IEEE transactions on dependable and secure computing, vol. 3, no. 2, April-June 2006

[4] Bouzida, Y.; Cuppens, F.; Gombault, S., (2006), '*Detecting and Reacting against Distributed Denial of Service Attacks*' Communications, 2006 IEEE International Conference on Volume 5, June 2006

[5] Trostle, J, (2006), '*Protecting Against Distributed Denial of Service (DDoS) Attacks Using Distributed Filtering*', Securecomm and Workshops, 2006 Aug. 28 2006-Sept. 1 2006 Page(s):1 - 11

[6] Savage, S., Wetherall, D., Karlin, A., and Anderson, T., (2001), '*Practical Network Support for IP Traceback*', SIGCOMM'00, Stockholm, Sweden, 2000

[7] Belenky, A.,and Ansari, N., '*Tracing Multiple Attackers with Deterministic Packet Marking (DPM)'*, Proc. of IEEE Pacific Rim Conference on Communications, Computers and Signal Processing

[8] Stefanidis, K.; Serpanos, D.N, (2005), 'Countermeasures Against Distributed Denial of 2005 IEEE Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Proceedings of Sept. 2005 Page(s):439 – 442

[9] Ho-Yu Lam; Chi-Pan Li; Chanson, S.T.; Dit-Yan Yeung, (2006), 'A Coordinated Detection and Response Scheme for Distributed Denial-of-Service Attacks' Approach to IP Communications, 2006 IEEE International Conference on Volume 5, June 2006

[10] Stone, R, (2000) "CenterTrack: An IP Overlay Network for Tracking DoS Floods," *Proc. 9th Usenix Security Symp.*,Usenix Assoc., 2000

[11] Burch, H., and Cheswick, B., "Tracing Anonymous Packets to Their Approximate Source," *Proc. 14th Conf.Systems Administration*, Usenix Assoc., 2000, pp.313–322.

[12] Bellovin, S., Leech, M., and Taylor, T., (2003), 'ICMP Traceback Messages,' Internet Draft, Internet Eng. Task Force, 2003; work in progress.

[13] Mankin, A., Massey, D., Wu, C.L., Wu S.F and Zhang, L., (2001), "On Design and Evaluation of 'Intention-Driven' ICMP Traceback," *Proc. IEEE Int'l Conf. Computer Comm. and Networks*, IEEE CS Press, 2001. pp. 159–165.

[14] Snoeren, A.C., et al., (2002), "Single-Packet IP Traceback," *IEEE/ACM Trans. Networking*, vol. 10, no. 6, 2002, pp. 721–734.

[15] Baba, T., and Matsuda, S., (2002). "Tracing Network Attacks to Their Sources," *IEEE Internet Computing*, vol. 6, no. 3, 2002

[16] Adler, M, (2002),'Tradeoffs in Probabilistic Packet Marking for IP Traceback,' *Proc. 34th ACM Symp. Theory of Computing*, ACM Press, 2002, pp. 407–418.

[17] Peng,T., Leckie, C., and Kotagiri, R., (2002), 'Adjusted Probabilistic Packet Marking for IP Traceback', Networking 2002.

[18] Snoeren, A.C., Partridge, C., Sanchez, L.A., Jones, C.E., Tchakountio, F., Schwartz, B., Kent, S.T., and Strayer, W.T., (2002) 'Single-Packet IP Traceback', IEEE/ACM Transactions on Networking, December, 2002,pp.721-734

[19] Peng,T., Leckie, C., and Kotagiri, R., (2002), 'Adjusted Probabilistic Packet Marking for IP Traceback', Networking 2002.

[20] Yaar, A., Perrig, A., and Song, D., (2003), 'Pi: A Path Identification Mechanism to Defend against DDoS Attacks', 2003 IEEE Symposium on Security and Privacy.

[21] Dean,D., Franklin, M., and Stubblefield, A., 'An Algebraic Traceback', Proc. of Network and Distributed System Security Symposium (NDSS 2001), pp.3-12.

[22] Xiang, Y., and Zhou, W., (2004), 'Trace IP packets by flexible deterministic packet marking (FDPM)', IP Operations and Management, 2004. Proceedings IEEE Workshop on 11-13 Oct. 2004

[23] Ribeiro, J.H.B.; Hashimoto, R.F., (2006), 'A New Machine Learning Technique Based on Straight Line Segments', Machine Learning and Applications, 2006. ICMLA '06. 5th International Conference on Dec. 2006 Page(s): 10-16

[24] Duda, R. O., Hart, P.E., and Stork. D.G, (2001), '*Pattern Classification*. JohnWiley and Sons, 2001.

[25] Mitchell, T.M, (1997), *Machine Learning*. McGraw-Hill, New York, 1997.

[26] Sutton, R.S and Barto. A.G, (1998), '*Reinforcement Learning: An Introduction'*. MIT Press, Cambridge, MA, 1998

[27] MIT 1998 DARPA Intrusion Detection Evaluation Data Set,

[28] Zhu. X., (2005), 'Semi-Supervised Learning Literature Survey'. Technical Report 1530, Computer Sciences, University of Wisconsin-Madison, 2005

[29] Prolexic Technologies, 'Prolexic Technology Report,(2007),
http://www.prolexic.com/zr/zombie_july_2007.pdf