International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Design and Implementation of ADFM in Network Processor

Gayatri Ratilal Mali[1], N. P. Karlekar[2]

[1]ME Student Dept. computer, Sinhgad Institute of Technology, Pune, India

[2]Project Guide, Department of Computer, Sinhgad Institute of Technology, Pune, India

Abstract: ***Denial of service attack denies services given by resources to the legitimate clients. DOS Attacker uses IP spoofing technique to hide their own identity, so first step to defend against DoS Attack is to find out IP address of the attacker to take further action. This paper represents a novel and practical IP trace back system, Flexible Deterministic Packet Marking (ADFM) to get IP address of the attacker when IP spoofing technique is used by attacker. ADFM belongs to the packet marking family of IP trace back systems. The novel characteristics of ADFM are in its flexibility: first, it can adjust the length of marking field according to the network protocols deployed (flexible mark length strategy); second, it can also adaptively change its marking rate according to the load of the participating router by a flexible flow-based marking scheme. This paper focuses on implementation of ADFM on network processor.***

Keywords: ADFM; network processor; IP traceback; packet marking; DDoS; PPM; DPM.

1. Introduction

With the boost in use of Internet, Internet crime is also increased. Due to use of automatic attack tools, attacks against Internet-connected systems are now so common place that Internet crime has become a ubiquitous phenomenon. Number of counter-measures were proposed and implemented but still internet crime is on rise. Due to vibrant, stateless, and anonymous nature of the Internet it is extremely difficult to mark out the sources of attack. In computing, a denial-of-service (DoS**)** or distributed denial-of-service (DDoS) attack is a try to make a system or network resource unavailable to its legitimate users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of efforts to temporarily or indefinitely disrupt or suspend services of hosts connected to the Internet. As clarification, DDoS (Distributed Denial of Service) attacks are sent by two or more persons, or bots. (DoS (Denial of Service) attacks are sent by one person or system [1]. Counter measure for DoS is to extract IP address of attacker from attacking packet header. But attacker has ability to forge IP address in packet header to hide their own IP address is called as IP spoofing [2]. To find the real source of net attacks, we tend to should possess the capability of discovering the origin of IP packets while not relying on the supply IP address field. This capability is called IP traceback. IP traceback systems offer a method to identify true sources of IP packets while not wishing on the source IP address field of the packet header, and are the major technique to seek out the real attack sources [3], [4]. Although presently there are several publications on IP traceback, some key problems that are essential to create associate IP traceback theme into a very usable traceback system were not solved, like how many sources can be traced in one traceback method, however large is that the false positive rate, how many packets are required to trace one supply, and how to lighten the load of participating routers.

Network Processor (NP) is helpful for its design is meant and enforced to satisfy the requirement. The Intel IXP2400 network processor could be a member of Intel's second-generation network processor family. It is a completely programmable network processor that implements a high-performance process design on one chip. It consists of nine programmable processors: one Intel XScale core and 8 micro-engines on identical die. The Intel XScale core is that's compliant with ARM architecture. The micro-engines are risc processors optimized for fast-path packet process. because of its intelligence and flexibility,IXP2400 network processors enable their customers expeditiously manage their network resource and information measure. ADFM encoding method has been enforced on Intel(R) IXP2400 network processor and that we shall introduce the performance of the ADFM on IXP2400.

2. Related Work

Current IP trace back schemes can be classified into five categories: link testing, messaging, logging, packet marking, and hybrid scheme [5] [6] [7] [8] [9]. Here we have considered packet marking scheme. Packet marking schemes insert trace back data into an IP packet header to mark the packet on its way through the various routers from the attack source to the destination; then the marks in the packets can be used to deduce the sources of packets or the paths of the trace. As this method overwrites some rarely used fields in IP header, it does not require modification of the current Internet infrastructure. This property makes it a promising trace back scheme to be part of DDoS defense systems. However, the space in IP header that can be utilized is limited. Thus, the information that one packet can carry is also limited. Therefore, many challenges for this category of trace back schemes are raised. For example, the number of sources that can be traced could be limited, the number of packets required to find one source could be large, and the load of the trace back router could be heavy. Probabilistic Packet Marking (PPM)[10] and Deterministic Packet Marking[11] Schemes are the two streams of the packet marking methods. The assumption of PPM is that the attacking packets are much more frequent than the Normal packets. It marks the packets with path information in a

probabilistic manner and enables the victim to reconstruct the attack path by using the marked packets. PPM encodes the information in rarely used 16-bit Fragment ID field in the IP header. To reduce the data that is to be stored in 16 bits, the compressed edge fragment sampling algorithm is used.DPM [12] stores the source address in the marking field. ADFM, the DPM scheme was modified to reduce false positive rates by adding redundant information into the marking fields. Unlike PPM, deterministic approaches only keep the first ingress edge router's information in the marks (but not the whole path). Moreover, they record marks in a deterministic manner (but not a probabilistic manner as in PPM).

3. Probabilistic Packet Marking Schemes

Probabilistic Packet Marking (PPM) [6] is one stream of the packet marking methods. The assumption of PPM is that the attacking packets are much more frequent than the normal packets. It marks the packets with path information in a probabilistic manner and enables the victim to reconstruct the attack path by using the marked packets. PPM encodes the information in rarely used 16-bit Fragment ID field in the IP header. To reduce the data that is to be stored in 16 bits, the compressed edge fragment sampling algorithm is used. Although PPM is simple and can support incremental deployment, it has many shortcomings that can seriously prevent it from being widely used. First, the path reconstruction process requires high computational work, especially when there are many sources. For example, a 25-source path reconstruction will take days, and thousands of false positives could happen [7]. Second, when there are a large number of attack sources, the possible rebuilt path branches are actually useless to the victim because of the high false positives. Therefore, the routers that are far away from the victim have a very low chance of passing their identification to the victim because the information has been lost due to overwriting by the intermediate routers. Many approaches were proposed to overcome the above deficiencies. For example, Song and Perrig proposed an advanced and authenticated PPM based on the assumption that the victim knows the mapping of the upstream routers. It not only reinforces the capability to trace more sources at one time but also solves the problem of spoofed marking. Another method to reduce the overhead of reconstruction was proposed in. It uses counters to complement the loss of marking information from upstream routers, in order to save computation time and reduce false positives. Adler analyzed the tradeoff between mark bits required in the IP header and the number of packets required to reconstruct the paths.

4. Deterministic Packet Marking Schemes

Another stream of packet marking methods, which does not use the above probabilistic assumption and stores the source address in the marking field, is in the category known as the deterministic approaches, such as Deterministic Packet Marking (DPM) [8], [9], our FDPM (the first version of FDPM was published in [10]), and Deterministic Bit Marking. Recently, in [11], the DPM scheme was modified to reduce false positive rates by adding redundant information into the marking fields. Unlike PPM, deterministic approaches only keep the first ingress edge router's information in the marks (but not the whole path). Moreover, they record marks in a deterministic manner (but not a probabilistic manner as in PPM). This category of schemes has many advantages over others, including simple implementation, no additional bandwidth requirement, and less computation overhead. However, enough packets must be collected to reconstruct the attack path (e.g., in the best case, at least two packets are required to trace one IP source with any of the above schemes). Importantly, all previous works neither perform well in terms of, nor have addressed the problems of, the maximum number of sources that the trace back system can trace in a single trace back process, the number of packets needed to trace one source, and the overload prevention on participating routers.

5. System Architecture

Flexible Deterministic Packet Marking scheme is novel packet marking IP traceback scheme. It contains two main parts one is encoding scheme another is reconstruction scheme. System architecture of proposed scheme is shown in figure no. It contains sender, Network, Destination machines. In network there is no. of routers. Ingress router is the closest router from sender. Each packet send by sender is passes through ingress router. Each Ingress router is deployed with encoding scheme and each router is deployed with reconstruction scheme. As shown in figure 1, each packet send from sender is marked with marking information at ingress router.

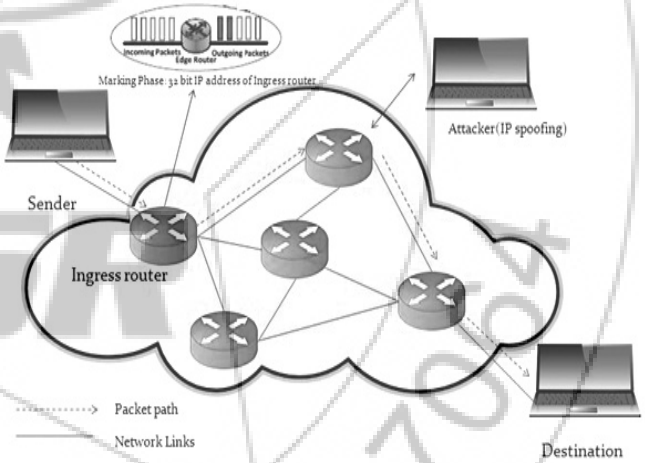

Figure 1: ADFM Architecture

As packets are marked with encoding scheme system can reconstruct IP address of the source at any router in path in the network using reconstruction scheme.

(A) Header Utilization for Marking Purpose:

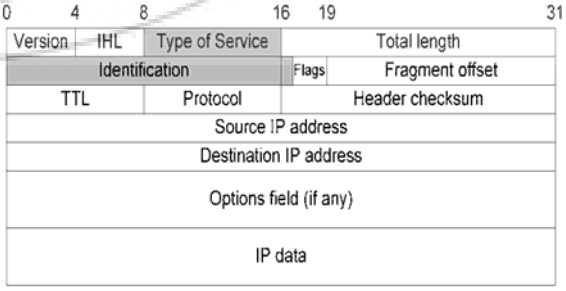

Figure 2: Header Utilization

In our scheme we have to mark IP address of the source machine from where packets are originated. System needs space to store mark (IP address) in packet header. Proposed scheme will use rarely used fields in the packet header by current network framework. Refer above figure no 2.Type of service is the 8 bit field which denotes what quality of service should be given to the packet. Details of Type of service are discussed in [13]. Support for Type of service is still under work, so we can use Type of service field for marking purpose. Less than 0.25 percent of all Internet traffic is fragments [14], Fragment ID can be safely overwrite without causing severe compatibility troubles. Dealing with the fragmentation problems has been discussed in [15].System can get space of 25 bits (8 +16+ 1) for marking purpose. Reserved bit will be used as flag to show weather system is using Type of Service field or not.

(B) Mark

This scheme is deployed on the ingress router in network. In this scheme, IP address of the source is marked in the packet header of packets. We get maximum space for marking for single packet is 25 bits, so minimum two packets are required to mark 32 bits of IP address. When 32 bit IP address is marked on the two different packets there is need to sequence them for reconstruction, so system will use sequence ID for that purpose. At the time of reconstruction on any router in the network, reconstruction router needs to know which packets are from which router, so each packet must contain such a field which identifies that on which router marking is done. Our system will use, digest for such purpose. Digest is calculated by applying hash function on IP address of the marking router. Our mark for single packet contains sequence number +Digest+ part of IP address of the source.

(C) Encoding Scheme

As per name of the scheme marking information encoded and marked on packet header of each packet at ingress router in this scheme. First system decides the mark length, if network is not using TOS field then system can use TOS field for marking then total marking length will be 24 bits and 1 bit to flag that system is using TOS field for marking. If System is not using TOS field i.e. network is using TOS then mark length would be 16 bits. If system is using TOS then flag would be marked as 0 otherwise marked as 1.If network is using TOS field partially (precedence field using but priority fields not using and vice versa) then mark length would be 19 bits. 2 Bits of the TOS field would be marked as 10 or 01 when TOS is used partially by system and 11 when complete TOS field is used by system. When length decision is executing par alley, digest is calculated using hash function where input is IP address of the marking router. Each packet is marked with sequence number, digest of marking router and part of IP address of the source as shown in figure no 3 and then send randomly using randomly selector.

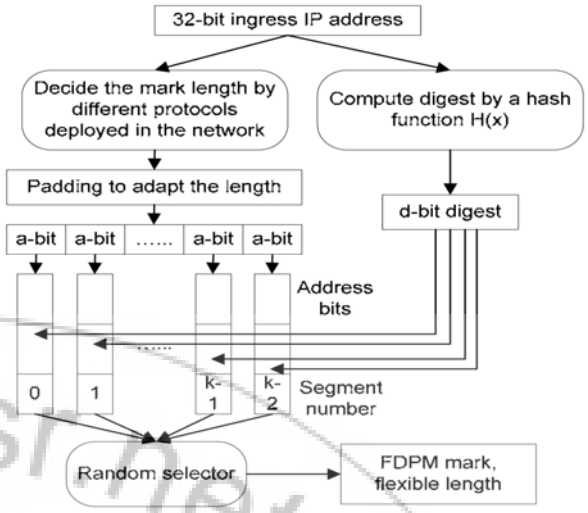

Figure 3: Encoding Scheme

(D) Reconstruction scheme

Reconstruction scheme is exact opposite of the encoding scheme, where IP address of the source reconstructed using marks in the packet header. Refer figure no 4.Incoming packets are stored in cache because rate of incoming packets is more than reconstruction speed. First step is recognizing length of the mark. Reconstruction scheme first see RF bit in the header if it is 1 then mark is of length 24 bits. If it is zero then, then system checks 7th and 8th bits of the TOS field, if they are 01 or 10 then mark length is 19 bits and if they are 11 then mark length is 16 bits. Packets of same digest number would be taken in single data structure and after that all packets with same digest number are sorted according to sequence number. Finally IP address of the source is extracted from packets. IF there is double segment number for same digest then they are put in new data structure.

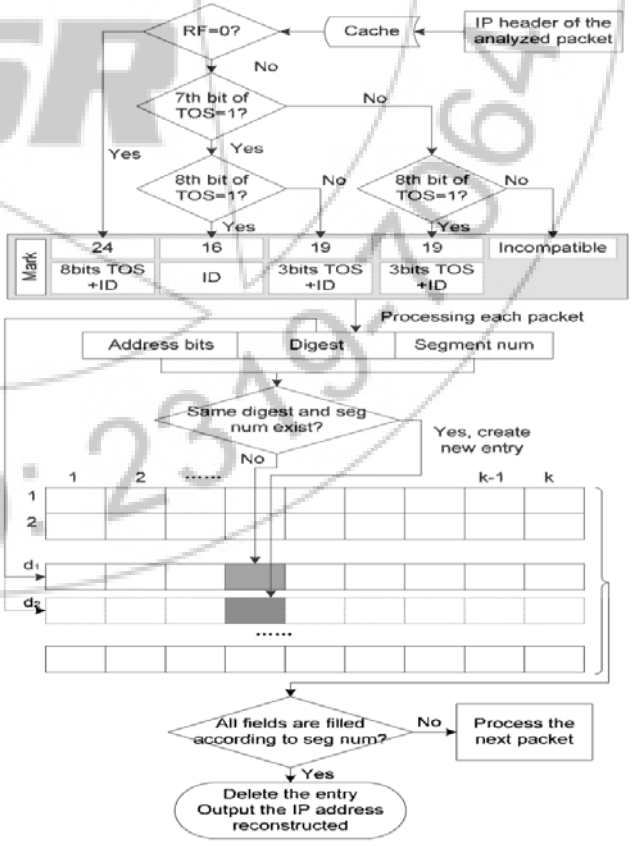

Figure 4: Reconstruction Scheme

6. Modules

(A) File Transfer module
In this module, we will design basic experiment set up. Our basic experiment set up contains one sender machine, destination machine, 2-3 machines acting as router. In this module we will implement scenario in which, sender sends file to destination by using socket programming. In this module sender selects file to send, and clicks send button on the panel then, packet formation of file takes place, and we can access fields in the packet header. Packets generated are sent along the socket to destination machine. Destination Machine gets file by receiving all packets sent by sender and can get sender machine's IP address by accessing IP header fields of the received packets.

(B) Encoding-Decoding Module:
In this module, Packet marking and decoding IP from marked packets will be covered. IP address of the sender machine will be marked to the packets at the ingress router by using Encoding Scheme. IP address of the sender machine can be retrieved by using Decoding scheme. Marking of the packets will be either 16-bit or32 bit or 19 bit depends on the network. In this module, there is no hacker in to the picture. Normal sender sends file but behind the screen when packets are form marking of IP address of the sender will be mark into the marking fields of the packets. When packets are received at the destination machine IP address of the sender is retrieved by using marks in marking fields in the packet header.

(C) Hacker module
In this module we will implement attack; how attacker will capture the packets on the path, after capturing the packets how attacker will manipulate those packets. Attacker will capture packets and form file from it then he may modify data in the file, delete data in the file, or only reads file and forwards to the destination and spoofs own IP address with Senders IP address.

(D) Final ADFM:
In this module, we will integrate all previous modules and develop final GUI for demo purpose. This module does all necessary remaining work. When we will develop this module, attacker maybe active or maybe not, ADFM system will find out IP address of the real sender of the packets without depending on the source IP address fields in the IP header of the packet.

7. Result

	APPM	DPM	ADFM
Computational Overhead	Moderate	Low	Very Low
Adaptability According to Network	No	No	Yes
Flow Marking	No	No	Yes
Minimum Packets required to Trace IP	More than DPM	More than ADFM	Minimum 4

8. Application

a) Our work is motivated with for enhancing security of current network system by utilizing rarely used field in the packet header, so our proposed system can be applied to current network system on large scale. This application requires more research and more experimental work before deploy it to the real system
b) To deploy proposed scheme to small private network for any private bank network.

9. Conclusion

In our work, we studied DDoS attack, IP spoofing technique and different available countermeasures for the same. We studied packet marking IP traceback scheme, like Probabilistic Packet Marking, Deterministic Packet Marking scheme. Then we proposed and designed new Flexible Deterministic packet marking scheme which has flexibility of changing mark length as per network protocol deployed.

10. Future Work

In our proposed system, we trace IP address of the attacker which uses IP spoofing for Dos attack; in future our system can get enhanced with block IP address functionality. We proposed our system on IPV4, in future system can enhanced with support for IPv6. In our project work, we will implement system on small scale, future work will be to implement

References

[1] en.wikipedia.org/wiki/Denial-of-service attack
[2] TCP/IP spoofing fundamentals, Hastings, N.E. Dept. of Electr. Eng. & Comput. Eng., Iowa State Univ., Ames, IA, USA McLean, P.A.1995
[3] H. Farhat, "Protecting TCP Services from Denial of Service Attacks," Proc. ACM SIGCOMM Workshop Large-Scale Attack Defense (LSAD '06), pp. 155-160, 2006
[4] H. Wang, C. Jin, and K.G. Shin, "Defense against Spoofed IP Traffic Using Hop-Count Filtering," IEEE/ACM Trans. Networking, vol. 15, no. 1, pp. 40-53, 2007
[5] H. Aljifri, "IP Traceback: A New Denial-of-Service Deterrent," IEEE Security and Privacy, vol. 1, no. 3, pp. 24-31, 2003
[6] Belenky and N. Ansari, "On IP Traceback," IEEE Comm., vol. 41, no. 7, pp. 142-153, 2003.
[7] S.M. Bellovin, ICMP Traceback Messages—Internet Draft, Network Working Group, 2000
[8] A.C. Snoeren, C. Partridge, L.A. Sanchez et al., "Single-Packet IP Traceback," IEEE/ACM Trans. Networking, vol. 10, no. 6, pp. 721-734, 2002.
[9] C. Gong and K. Sarac, "IP Traceback Based on Packet Marking and Logging," Proc. IEEE Int'l Conf. Comm. (ICC), 2005
[10] S. Savage, D. Wetherall, A. Karlin et al., "Network Support for IP Traceback," ACM/IEEE Trans. Networking, vol. 9, no. 3, pp. 226-237, 2006
[11] Belenky and N. Ansari, "P Traceback with Deterministic Packet Marking," IEEE Comm. Letters, vol. 7, no. 4, pp. 162-164, 2003
[12] Belenky and N. Ansari, "On Deterministic Packet Marking," Computer Networks, vol. 51, no. 10, pp. 2677-2700, 2007
[13] Type of Service in the Internet Protocol Suite, RFC1349, Network Working Group, 1992.
[14] Stoica and H. Zhang, "Providing Guaranteed Services without Per Flow Management," Proc. ACM SIGCOMM '99, pp. 81-94, 1999
[15] Belenky and N. Ansari, "On Deterministic Packet Marking," Computer Networks, vol. 51, no. 10, pp. 2677-2700,2007