Journal of Theoretical and Applied Information Technology
10th April 2014. Vol. 62 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DETECTION OF DDOS ATTACKS USING IP TRACEBACK AND NETWORK CODING TECHNIQUE

J.SATHYA PRIYA[1], M.RAMAKRISHNAN[2], S.P.RAJAGOPALAN[3]
[1]Research Scholar, Anna University, Chennai, India
2Professor,Velammal Engineering College,Chennai,India
[3]Professor,GKM Engineering College,Chennai,India

E-mail: sathyapriya.m.e@gmail.com

ABSTRACT

Distributed denial-of-service attacks can collapse even the well-structured networks. Nowadays with ever-more-powerful tools in a hacker's armoury, DDoS attacks are easier to launch. Typical types of DDoS attacks include bandwidth attacks and application attacks. In a bandwidth attack, network resources or equipment are exhausted by a bulk volume of packets. In application attack, TCP or HTTP resources are prevented from processing transactions. We concentrated in bandwidth attacks by using network coding concept along with the alternate path selection by using IP trace back one hop concept. Router acts as a intermediate to transfer packets across networks. Normally DDoS attackers try to paralyze the router to inject attack. So threshold value should be maintained to identify normal traffic from abnormal traffic to detect DDoS attacks. This type of approach will be more efficient for securing sensitive, secure and important information rather than heavy volume of data sent over router for the commercial business.
Keywords:- *Ddos Attack, Threshold Value, Network Coding, Alternate Path, Trace Back.*

1. INTRODUCTION

DDoS attacks can prevent intend user from receiving intend message at correct time. This type of attack can be made over two types of data resource one is on the heavy volume of data sent over the network for the commercial business process, thus shut down the server for some particular amount of time another one on the sensitive data like military application and so on. So this paper focuses more on sensitive data transmission rather than the attack which makes the business server shutdown for some period of time and makes huge revenue loss. In DDoS attacks, maliciously attackers inject bulk of different packets into the network, or the attacker's forward the same packet to many of the nodes as possible. We can generally classify these attacks as two types one is packet flood attack and another is DDoS attack. These attacks consume the bandwidth and buffer space, and thus prevent intent packets from reaching the target and thus thwart the network performance and services. Our aim is to divide and send the sensitive data and retrieve those data by network coding concept. Network coding concept can be implemented to retrieve the divide and sent original data across the network. Subsequently, two key techniques are there, random coding and linear coding. The random coding makes network coding more practical and the linear coding is proven efficient for network coding. Network coding has been widely recognized as friendly approach for improving network performance. Primary applications of network coding include the file distribution and multimedia streaming on P2P overlay networks, data transmission in sensor networks, tactical communications in military networks, etc. Compared with conventional packet forwarding technologies, network coding allows and encourages intermediate forwarders. Several significant advantages such as the potential throughput improvement, transmission energy minimization, and delay minimization are considered.

Network coding is used to retrieve the data sent over different nodes. In this paper the data has been split and sent over different router, then DDOS attacks are identified by matching with

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the threshold already set. Once attack has been identified, the router performs logging and marking over the routing table and shows an alternate path to forward the remaining data to the next neighbour router. As a future work we can concentrate in retrieving lost data by using data mining techniques.

2. PREVIOUS WORK

[1] Imad Aad etal-IEEE 2008 "Transactions on Networking"-paper, "Impact of denial of service attacks on Adhoc networks", proposed the Reputation based mechanism to detect Jelly fish and Black hole attack focusing on Multipath routing and DoS Resilience.[2] Y-C. Hu et al-Mobile Communication 2002,pp:12-33, "A Secure on Demand Routing protocol" proposed SEAD (Secure adhoc destination vector routing protocol) makes use of Hash chains and merkle hash tree. These structures is used to authenticate the metric (distance to the target) and sequence numbers. It adopts path weight to yield good put. It implements a technique called Route-request flooding attack. In this every node has a rate limit to route request even it is asked to relay. But it posses drawbacks such as rate limiting can also delay a victim's ability to respond to an attack, and consequently reduce the throughput of victims.[3] Minda Xiang et al-IEEE 2011 – "Mitigating DDoS attacks using protection nodes in Mobile Adhoc Networks". It makes use of two types of nodes in two different levels such as local protection node and remote protection node. It makes use of messages such as ANM & AIM to communicate between two different levels of nodes, If proper acknowledgement is received then transfer of messages takes place. It faces drawbacks such as False positive alert, Different setting of LPN updating period, Assignment of LPN in multi-level network.[4] Yi et al – "A Security Aware routing protocol for wireless adhoc networks"-2002 ACM proposed SAODV.In this during routing only nodes in the same level are selected, Compares level, then node will be included or RREQ packets are flooded continuously. [5] A. Hussain, J. Heidemann, and C. Papadopoulos, "A framework for classifying denial of service attacks," in Proc. ACM SIGCOMM '03, Karlsruhe, Germany, Aug. 2003, pp. 99–110.Adopted a hybrid trace back approach in which packet marking and packet logging are integrated in a novel manner, so as to achieve the best of both worlds, that is, to achieve small number of attack packets to conduct the trace back process and small amount of resources to be allocated at intermediate routers for packet logging purposes. But it posses challenges such as avoiding the use of large amount of attack packets to construct the attack path or attack tree. Leads to low processing and storage overhead at intermediate routers.[6] C. Gong and K. Sarac, "A more practical approach for single-packet IP trace back using packet logging and marking," IEEE Trans. Parallel Distributed Syst., vol. 19, no. 10, pp. 1310–1324, Oct. 2008.In this paper, we study the effectiveness of log-based IP trace back in tracing a single packet under the environment where not every AS (Autonomous Systems) supports log-based IP trace back. It posses drawbacks as most existing trace back techniques start from the router closest to the victim and interactively test its upstream links until they determine which one is used to carry the attacker's traffic. [7]Wei-Shen Lai et al-2008-"ACM Transactions" titled "Using Adaptive bandwidth a location approach to defend DDoS attacks". It monitors traffic pattern provides high priority to normal users and vice-versa. Its advantage is it decreases flow of malicious packets due to DDoS attacks. Its Posses challenges such as legitimate users need to maintain constant flow at all time. It also leads to increases packet drop rate. [8]A. Hussain, J. Heidemann, and C. Papadopoulos, "A framework for classifying denial of service attacks," in Proc. ACM SIGCOMM '03, Karlsruhe, Germany, Aug. 2003, pp. 99–110. In a multi-source attack, a master typically activates a large number of zombies by sending a trigger message that either activates the zombies immediately or at some later time. When observed near the victim, this distributed activation of zombie's results in a ramp-up of the attack intensity due to the variation in path latency between the master and the zombies and weak synchronization of local clocks at the zombies.[9] B.Al-Duwari and M. Govindarasu, "Novel hybrid schemes employing packet marking and logging for IP traceback," IEEE Trans. Parallel Distributed Syst., vol. 17, no. 5, pp. 403–418, May 2006. Tracing DoS attacks that employ source address spoofing is an important and challenging problem. Adopted a hybrid trace back approach in which packet marking and packet logging are integrated in a novel manner to conduct the trace back process

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

and small amount of resources to be allocated at intermediate routers for packet logging purposes. [10] C. Gong and K. Sarac, "A more practical approach for single-packet IP traceback using packet logging and marking," IEEE Trans. Parallel Distributed Syst., vol. 19, no. 10, pp. 1310–1324, Oct. 2008. Tracing IP packets to their sources, known as IP traceback, is an important task in defending against IP spoofing and DoS attacks. Log-based IP traceback technique is to log packets at routers in the network and then determine the network paths which packets traversed using data extraction techniques. The biggest advantage of log-based IP traceback is the potential to trace a single packet. Tracing a single packet in the Internet using log-based IP traceback involves cooperation among all Autonomous Systems (AS) traversed by the packet. The single packet traceback process may not reach the packet origin if some AS on the forwarding path does not support IP traceback. IP traceback mechanisms are deployed within each AS independently. [11]H. Burch and B. Cheswick, "Tracing anonymous packets to their approximate source," in Proc. USENIX LISA 2000, New Orleans, LA, Dec. 2000, pp. 319–327.In this paper outlined a technique for tracing spoofed packets back to their actual source host without relying on the cooperation of intervening ISPs. First, we map the paths from the victim to all possible networks. These observations often allow us to eliminate all but a handful of networks that could be the source of the attacking packet stream.

3.SCOPE OF THE RESEARCH

Although the means, motives and targets of a DDoS attack may vary, it generally aims preventing an Internet site or service from functioning efficiently. DDoS attacks can be classified into flooding attacks and software exploits. Flooding attacks work by flooding a victim with large amounts of packets leading to heavy traffic in the network and finally resulting in unavailability of resources. Software exploits attack a victim by sending as few as a single packet aiming to create bugs in system OS or software. Attackers send packets with arbitrary source address leading to IP spoofing. Tracing the paths of IP packets back to their origin, is termed as IP trace back. It is an important step in defending against DoS attacks employing IP spoofing.

If entire data is sent through the single router, then DDoS can exhaust the entire data well effectively. So better means and ways is to split the original data in to blocks and send the data through different router. Threshold value should be maintained at each router. Beyond the threshold limit. the router drops the packet and performs one hop to the neighbor node to find the alternate path. In the receiver side the receiver has to use network coding to receive the data.

The main scope of the research is even though hackers tries to induce DDoS attack at a router, they can exhaust only part of the data from the entire one and we hope remaining data can be received at the receiver side safely.

Further we have explored the idea IP trace back and one hop scheme to trace back the IP address of blocked router and can implement one hop to divert the path to the next neighbor router to retransmit the data from the attacked router. Defending against DDoS attacks means not only overcoming from its effect but also to identify the attack router/ node. This process is called IP trace back. In this paper we make use of the concept of trace back involving both packet marking and packet logging. During the process, if any attack is found, then the positive feedback cannot be returned. We use active routing method and OSPF(open source shortest path first) routing algorithm to identify an alternate path to continue the communication.

4.PROPOSED WORK

The proposed research focus on three things: First, is using Threshold Matching. Secondly slice the sensitive data fairly using RC4 algorithm to route over different routers. The reason to use the RC4 algorithm is to slice the entire data in to many numbers of blocks as possible. The concept of decryption on the receiver side and to retrieve the lost data from the retrieved data will be focussed on the future work. Thirdly, implements the concept of organizing the data sent over different routers using the concept of network coding. The entire data is divided into number of blocks through different routers in parallel. On receiving side it makes use of the concept of network coding to organize the data collected

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

over different routers. Finally focus on alternate path selection by IP based scheme by using one hop path to resend the data from the attacked router.

Threshold Matching:

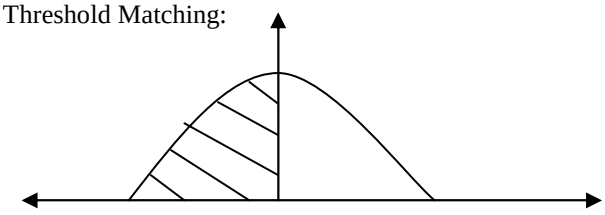

Figure 1. Matching Threshold

The router should perform anomaly detection strategy. This enables us to identify normal user from attacks. Various research work says identification of DDoS attack is performed at different levels of boundary. That is , the traffic would be monitored by remote nodes before the actual message reaches the local nearer nodes. In turn, there are papers explaining about P-Claim and T-Claim to identify the traffic limit. In this paper, we focus on the same thing but make use of the concept IP trace back to continue the normal communication as before . For the more effiency this type of approach can work well with the TCP oriented communication. In threshold matching approach, certain limit has been fixed, and this has been compared with the incoming bandwidth. This comparison helps to identify normal user from the abnormal user. Threshold limit is computed based on the factors such as data speed, frequency of data sent, and bandwidth. If data rate falls under the programmed limit then data will be forwarded else discards data. At the moment, the server informed about the DDoS attack from the router, then it enables the router to perform alternate path selection strategy. Alternate path selection is performed by using the concept one hop next strategy. Considering false positive and false negative in mind, the least value and the highest value are omitted. Here the router maintains not the single value but the average of threshold value of some packets of data received at short period of cycles . For example we consider the data sent and received over the period of 10ms. The values obtained can be maintained along with the routing information. If the obtained value matches with the mean value maintained in the router table, then the data packets can be sent/ received else discards the data.

If (obtainedvalue<=thresholdvalue)

Forwards

Else

Discards and call alternate path selection

Threshold Value=Th=$_{n=2}\sum^{n-1}$ n * 10ms/ N,

Where n is the data value computed for the every 10ms and N is the total number of data sent/ received. The values are maintained in the routing table. If it exceeds the limit then it is discarded and the same is noted in the server system. This extra maintenance of information may cause overhead to the buffer, even though it is negligible compared with its approach to detect attack.

RC4 algorithm:

In this step, the original data is divided in to blocks of data and sent through the different routers. For splitting the data into small slices we can make use of RC4 algorithm, which helps to split the data into many small blocks. Depending upon the size of the data and importance of data to be sent, we can make use of different algorithms to slice the data.

Key Scheduling Algorithm -KSA(K)

Initialization:

For i=0…N-1

S[i]=i

j =0

Scrambling:

For i=0…N-1

j=j+S[i]+K[i mod l]

Swap(S[i + 1],S[j])

Journal of Theoretical and Applied Information Technology
10th April 2014. Vol. 62 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Pseudo Random Generation Algorithm-PRGA(K)

Initialization:

i=0

j=0

Generation Loop:

i=i+1

j=j+S[i]

Swap(S[i],S[j + 1])

Output z=S[S[i]+S[j]]

Instead of sending the data through a single router, the data can be divided into blocks and sent to the different router from the sender side. In the same way from the receiver side the data can be fetched from different routers and combined to retrieve the original data. It does not take much time because it follows parallel processing of data transmission.

If suppose DDoS attackers tries to induce flooding attack on one router, they can make resource vanish only for the part of the data from the original one. Moreover, the router which comes under attack can also provide alternate path in order to enable continuation of communication without any delay.In this step, instead of sending the packet one by one to the same router, the split packet is sent through the different routers at the same time. Here synchronization of data should be considered. The divided portion of data reaches the different routers and tries to reach the destination through the neighbouring nodes. Instead of sending the data through a single router, the data can be divided into blocks and sent to the different router from the sender side. In the same way from the receiver side the data can be fetched from different routers and combined to retrieve the original data. It does not take much time because it follows parallel processing of data transmission.

If suppose DDoS attackers tries to eject flooding attack on one router, they can make resource vanish only for the part of the data from the original one. On the other side remaining portion of the data can be received by the receiver. For the missing packets, one can do either of one among proposed idea. One is when sending the data itself we can compute threshold value for each fragment of data. This threshold value is computed based on the size of the data, the speed of data, time to reach destination, original data and the fragment number. These computed values are stored randomly among different fragments of data sent over the different routers. On the receiver side one may miss one or two fragments due to DDoS but can retrieve the lost data from the data packets received.

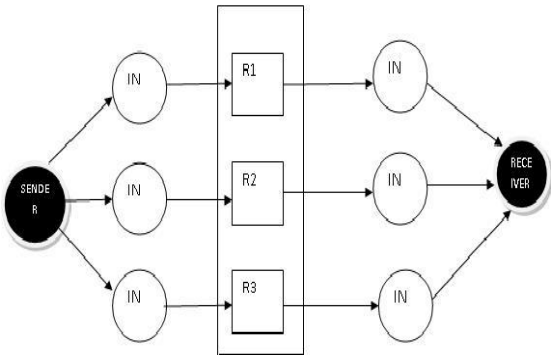

Figure 2. Transfer Of Data From Source To Destination By Divide And Send

Network Coding:

Network coding enables us to combine the data received from different neighbor nodes via different router and organize the original data sent by the receiver. Because of DDoS attack we may miss one or two fragments, but we can organize the remaining data. In DDoS normally there won't be corruption of data takes place but what it will do is calmly suspend the resource from reaching the destination for some time or make that particular node shut down. So later we can get the data from the shut down node. But waiting leads performance loss, business loss and so on. So when router is suspected under DDoS attack, it could diver or shows an alternate path through the neighboring routers. Alternate path selection can be discussed in the fore coming approach.

Alternate Path Selection:

Each router maintains a router interface table which contains numbers of the upstream routers [17]. IP headers identification field, Flag and fragment offset field is used as a 32-bit marking field. When a border router receives a packet from the local network it forwards the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

packet by setting the marking field as zero. When a core router receives a packet it computes new mark value [17]. Until the mark value does not overflow it is forwarded to next router with the new mark value as computed. When the mark value overflows the packet's mark value is logged onto the router. Hash table is maintained for efficient storage and access of the logged mark values. The corresponding index in the hash table is used for further mark value computation. The packet is now transferred with the new mark value. This process continues until the packet reaches the destination.

When the victim is under attack it sends the upstream router a request for path reconstruction with the received attack packet's mark value [17]. The attack packets upstream router is found iteratively until the source is reached. Hash table containing the mark value is referred while the obtained upstream interface is negative. When the attack source is reached during this process path reconstruction is done. This process proposed by Ming-Hour Yang and Ming-Chien Yang [17] is enumerated with the algorithm and a routing example. If any router in the routing path goes down during the path reconstruction process positive feedback could not be received. In this case another alternate path to continue with the traceback scheme should be discovered.

The main idea behind packet marking is to record network path information in packets. In mark based IP trace back, routers write their identification information (e.g., IP addresses) into a header field of forwarded packets. The destination node then obtains the marking and finds the network path.

The basic idea in packet logging is to record the path information at routers. In the log-based trace back, packets are being logged by the routers at the path to the destination. Then the network path is determined based on the information logged at the routers. Now the lost data can be retransmitted from the neighbor router.

Begin
1. If router does not support the trace back process then
2. Discover the router one hop next in the routing path
3. mark $_{intermediate}$= mark $_{req}$ / (D(R) +1)
4. check in the hash table of failed router
5. if mark $_{intermediate}$ is a valid index entry then
6. Make its corresponding mark value from HT as mark $_{req}$
7. mark $_{req}$=mark value in HT
8. obtain UI from the same HT row
9. else
10. mark $_{req}$=mark $_{intermediate}$
11. endif
12. send reconstruction request with mark $_{req}$
13. endif

End

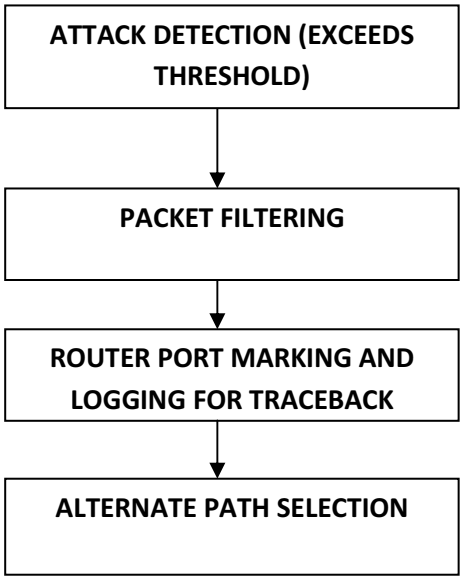

Figure 3. Proposed Approach

During the traceback, if any router goes down its impossible to continue with the traceback. For example, if the router $R_{2\ fails}$, the path reconstruction could not continue further with the mark value 32. Through OSPF routing the hash table, interface table of each router is established to the other routers in the network. Hence R1, R3, R4, R5, R6, R7 has all the information regarding R2. Two ways are possible now. One is to find the nearest adjacent router of R2 to continue or the second way is to continue with the next router (one hop away) in the routing path pre-established.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

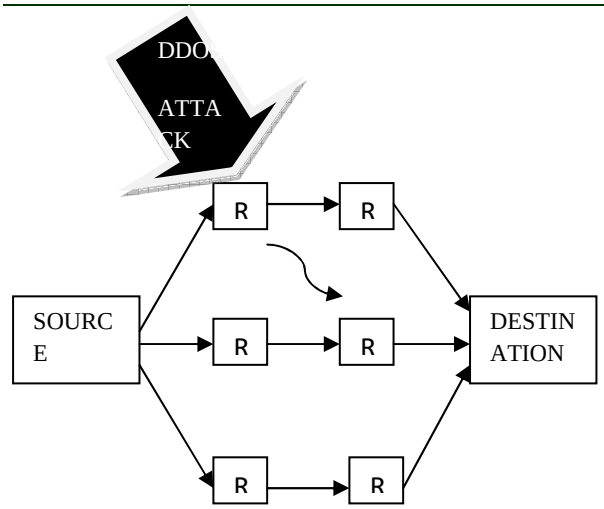

Figure 4. Alternate Path Selection

The trace back scheme in our paper continues with the second approach which is explained with R2.

1. When R2 fails, the reconstruction scheme now continues with R1 which is one hop away from the failed router R2 on the network path in existence prior.
2. When the mark value 32 reaches R1 it is first divided by the total number interfaces plus one of the failed router R2. i.e. mark $_{intermediate}$= mark req/ total number of interfaces + 1 of failed router.
3. Now the mark $_{intermediate}$=32/4=8.
4. Now the hash table of R2 is checked for any valid mark entry with corresponding to index 8.
5. If no valid entry, this mark $_{intermediate}$ is made as mark$_{req}$.
6. If there is a valid mark entry for the index value 8, the corresponding mark value entry is made the mark$_{req}$.
7. The upstream interface of R1 is calculated.
8. This newly obtained mark value is R1.
9. Now R1 continues with the trace back process until it reaches the source.

5. COMPARISON ANALYSIS

From the recent research it is observed IP trace back by one hop concept yield good throughput in detecting and protecting resource against DDoS attacks. By enhancing the concept further shows better throughput than the before to send the sensitive data fairly by RC4 algorithm.

6. CONCLUSION

In this paper DDoS attack is identified by matching with the threshold value, if it exceeds that is identified as attack, and then this information is updated in server and do the alternate path selection. Using RC4 algorithm, we can split and send the data, so only partial loss of data exist then precede the trace back when the router proves negative to support, is continued by selecting an alternate path with help of OSPF routing. QoS of this routing is checked with parameters like bandwidth and delay. Also, time required to trace back to the attack source when no router fails and the when the router fails leading to alternate path selection is compared. By selecting the alternate path delay caused due to router failure is avoided to an extent. As the data is sent parallel to different routers at same time, it would not be time consuming. Moreover this type of approach we can use for the sensitive data transmission rather than all types of data. As a future extension to this paper alternate path through shortest path algorithm could be constructed and its efficiency could be analyzed with the path constructed one hop away from the failed router.

Further work will be focused on retrieving the lost data from the retrieved data using data mining techniques.

ACKNOWLEDGMENT

I would like to express my sincere thanks to my Supervisor Professor Dr.S.P.Rajagopalan and Joint supervisor Professor Dr.M.Ramakrishnan, for their full cooperation for my research work. With out their guidance I could not finish this research project. I would like to thank them for their useful comments and remarks through out the implementation of this work. I would like to thank each and everyone, who have supported me throughout entire process.

REFERENCES:

[1] Imad Aad etal, "Transactions on Networking", "Impact of denial of service attacks on Adhoc networks",.

[2] Y-C. Hu et al, "A Secure on Demend Routing protocol", Mobile Communication 2002,pp:12-33.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[3] Minda Xiang et al, "Mitigating DDoS attacks using protection nodes in Mobile Adhoc Networks",IEEE 2011.
[4] Yi et al , "A Security Aware routing protocol for wireless adhoc networks", ACM 2002.
[5] A. Hussain, J. Heidemann, and C. Papadopoulos, "A framework for classifying denial of service attacks," in Proc. ACM SIGCOMM '03, Karlsruhe, Germany, Aug. 2003, pp. 99–110.
[6] C. Gong and K. Sarac, "A more practical approach for single-packet IP traceback using packet logging and marking," IEEE Trans. Parallel Distributed Syst., vol. 19, no. 10, pp. 1310–1324, Oct. 2008.
[7] Wei-Shen Lai et al, "Using Adaptive bandwidth a location approach to defend DDoS attacks",ACM 2008.
[8] A. Hussain, J. Heidemann, and C. Papadopoulos, "A framework for classifying denial of service attacks," in Proc. ACM SIGCOMM '03, Karlsruhe, Germany, Aug. 2003, pp. 99–110.
[9] B.Al-Duwari andM. Govindarasu, "Novel hybrid schemes employing packet marking and logging for IP traceback," IEEE Trans. Parallel Distributed Syst., vol. 17, no. 5, pp. 403–418, May 2006.
[10] C. Gong and K. Sarac, "A more practical approach for single-packet IP traceback using packet logging and marking," IEEE Trans. Parallel Distributed Syst., vol. 19, no. 10, pp. 1310–1324, Oct. 2008.
[11] H. Burch and B. Cheswick, "Tracing anonymous packets to their approximate source," in Proc. USENIX LISA 2000, New Orleans, LA, Dec. 2000, pp. 319–327.
[12] S. Acedanski, S. Deb, M. Medard, and R. Koetter, "How Good Is Random Linear Coding Based Distributed Networked Storage," Proc. Workshop Network Coding, Theory and Applications, Apr. 2005.
[13] P.A. Chou, Y. Wu, and K. Jain, "Practical Network Coding," Proc. Allerton Conf. Comm., Control, and Computing, Oct. 2003.
[14] C. Gkantsidis and P.R. Rodriguez, "Network Coding for Large Scale Content Distribution," Proc. IEEE INFOCOM, pp. 2235-2245, 2005.
[15] S.Vincent and J.I.Raja, "A Survey of IP Traceback to overcome Denial of service attacks" in Proc. Recent Advances in Networking,VLSI and Signal Processing.
[16] M.Hour Yang and M.Chein Yang, "RIHT- A Novel Hybrid IP Traceback scheme" in Proc. IEEE Trans on Information Forensics and Security, April 2012, vol. 7,no. 2, pg. 789-797
[17] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Practical network support for IP traceback," in Proc. ACM SIGCOMM2000, Stockholm, Sweden, Aug. 2000, pp. 295–306.
[18] A. C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio, B. Schwartz, S. T. Kent, and W. T. Strayer, "Single-packet IP traceback," IEEE/ACM Trans. Networking, vol. 10, no. 6, pp. 721–734, Dec. 2002.
[19] A. Belenky and N. Ansari, "IP traceback with deterministic packet marking," *IEEE Commun. ett.*, vol. 7, no. 4, pp. 162–164, Apr. 2003.
[20] A. Belenky and N. Ansari, "Tracing multiple attackers with deterministic packetmarking (DPM)," in *Proc. IEEE PACRIM'03*, Victoria, BC, Canada, Aug. 2003, pp. 49–52.
[21] H. Badis et al "Optimal Path Selection in a Link State QoS Routing Protocol".
[22] T. Killalea, "Recommended Internet Service Provider Security Services and Procedures"in Network Working Group,BCP: 46, Nov 2000.
[22]Gong and K. Sarac, "A more practical approach for single-packet IP traceback using packet logging and marking," IEEE Trans. Parallel Distributed Syst., vol. 19, no. 10, pp. 1310–1324, Oct. 2008.