Volume 6, Issue 9, September 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Review on Distributed Network Attack

Sneh Lata, Er. Rupinder Kaur
Bhai Gurdas Institute of Engineering and Technology,
Punjab, India

***Abstract**— Distributed denial-of-service attacks can collapse even the well-structured networks. Nowadays with evermore-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**— LPN, MAC, OSPF, LMAC*

I. INTRODUCTION

Mobile ad-hoc network is one of the most emerging fields in research and development of wireless network. As the popularity of mobile device and wireless networks increased significantly over the past years, it hasnow become one of the most vibrant and active field of communication in wireless technology.[1]

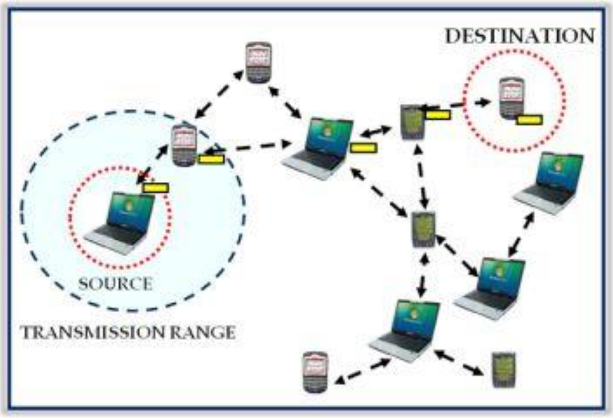

Fig 1: Mobile Ad hoc Network (MANET)

MANET is a self-configuring and infrastructure- less network. Each device or node is free to move independently, and will therefore change its links with other devices frequently in any direction. The primary challenge in creating a MANET environment is to continuously maintain the information required to route the traffic properly. Such networks can operate by themselves or by connecting itself to the larger Internet. They may contain one or more transceivers. This results in a highly dynamic and autonomous topology.[1]

II. NETWORK ROUTING

Routing is the process of selecting best paths in a network.Routing is the process of exchange of information from one host to the other host in a network. It is the process of forwarding packets towards its destination using most efficient path. Routing is performed for many kinds of networks, including the telephone network (circuit switching), electronic data networks (such as the Internet), and transportation networks. This article is concerned primarily with routing in electronic data networks using packet switching technology. In packet switching networks, routing directs packet forwarding through intermediate nodes. Intermediate nodes are typically network hardware devices such as routers, bridges, gateways, firewalls, or switches. The routing process usually directs forwarding on the basis of routing tables which maintain a record of the routes to various network destinations. Thus, constructing routing tables, which are held in the router's memory, is very important for efficient routing. In case of overlapping/equal routes, the following elements are considered in order to decide which routes get installed into the routing table:[2]

- Prefix-Length: where longer subnet masks are preferred (independent of whether it is within a routing protocol or over different routing protocol)
- Metric: where a lower metric/cost is preferred (only valid within one and the same routing protocol)

Administrative distance: where a lower distance is preferred (only valid between different routing protocols)[2]

III. BACKGROUND

Imad Aad etal-IEEE 2008 "Transactions on Networking"-paper, "Impact of denial of service attacks on Adhoc networks", projected the Reputation primarily based mechanism to discover Jelly fish and part attack that specialize in Multipath routing and DoS Resilience.[2] Y-C. Hu et alMobile Communication 2002,pp:12-33, "A Secure on Demand Routing protocol" projected SEAD (Secure adhoc destination vector routing protocol) makes use of Hash chains and merkle hash tree. These structures is employed to evidence the metric (distance to the target) and sequence numbers. It adopts path weight to yield sensible place.

It implements a method referred to as Route-request flooding attack. during this each node features a rate limit to route request even it's asked to relay. But it posses drawbacks like rate limiting may delay a victim's ability to retort to associate attack, and consequently scale back the outturn of victims.[3] Minda Xiang et al-IEEE 2011 – "Mitigating DDoS attacks exploitation protection nodes in Mobile Adhoc Networks". It makes use of 2 types of nodes in 2 completely different levels like local protection node and remote protection node.

It makes use of messages like ANM &amp; AIM to communicate between 2 completely different levels of nodes, If correct acknowledgement is received then transfer of messages takes place. It faces drawbacks like False positive alert, Different setting of LPN change amount, Assignment of

LPN in multi-level network.[4] Lolo et al – "A Security Aware routing protocol for wireless adhoc networks"-2002 ACM projected SAODV. In this throughout routing solely nodes within the same level are elect, Compares level, then node are enclosed or RREQ packets are flooded unendingly. [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 within which packet marking and packet logging are integrated in a very novel manner, so as to achieve the simplest of each worlds, that is, to achieve small range of attack packets to conduct the trace back method and tiny quantity of resources to be allotted at intermediate routers for packet logging functions. however it posses challenges like avoiding the employment of huge quantity of attack packets to construct the attack path or attack tree. Leads to low process and storage overhead at intermediate routers.[6] C. Gong and K. Sarac, "A more sensible approach for single-packet information processing trace back exploitation packet work 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 information processing trace back in tracing one packet below the setting where not each AS (Autonomous Systems) supports log-based information processing trace back. It posses drawbacks as most existing trace back techniques start from the router highest to the victim and interactively check its upstream links till they determine that one is employed to hold the attacker's traffic. [7]Wei-Shen Lai et al-2008- "ACM Transactions" titled "Using accommodative bandwidth a location approach to defend DDoS attacks". It monitors approach pattern provides high priority to traditional users and vice-versa. Its advantage is it decreases flow of malicious packets owing to DDoS attacks. Its Posses challenges like legitimate users have to be compelled to maintain constant flow the least bit time. It additionally results in 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 very multi-source attack, a master generally activates an outsized range of zombies by causing a trigger message that either activates the zombies straightaway or at some later time. once determined close to the victim, this distributed activation of zombie's ends up in a ramp-up of the attack intensity owing to the variation in path latency between the master and the zombies and weak synchronization of native clocks at the zombies.[9] B.Al-Duwari and M. Govindarasu, "Novel hybrid schemes using packet marking and work for information processing traceback," IEEE Trans. Parallel Distributed Syst., vol. 17, no. 5, pp. 403–418, May 2006. Tracing DoS attacks that use supply address spoofing is associate important and difficult drawback. Adopted a hybrid trace back approach within which packet marking and packet work are integrated in a very novel manner to conduct the trace back method and tiny quantity of resources to be allotted at intermediate routers for packet work functions. [10] C. Gong and K. Sarac, "A a lot of sensible approach for single-packet information processing traceback exploitation packet work and marking," IEEE Trans. Parallel Distributed Syst., vol. 19, no. 10, pp. 1310–1324, Oct. 2008. Tracing information processing packets to their sources, called information processing traceback, is a very important task in defensive against information processing spoofing and DoS attacks. Log-based information processing traceback technique is to log packets at routers within the network and so determine the network methods that packets traversed exploitation information extraction techniques. The biggest advantage of log-based information processing traceback is that the potential to trace one packet. Tracing one packet within the net exploitation log-based information processing traceback involves cooperation among all Autonomous Systems (AS) traversed by the packet. the one packet traceback method could not reach the packet origin if some AS on the forwarding path doesn't support information processing traceback. IP traceback mechanisms are deployed inside every AS severally. [11]H. Burch and B. Cheswick, "Tracing anonymous packets to their approximate supply," in Proc. USENIX LISA 2000, port of entry, LA, Dec. 2000, pp. 319– 327.In this paper printed a method for tracing spoofed packets back to their actual supply host without hoping on the cooperation of intervening ISPs. First, we tend to map the methods from the victim to all doable networks. These observations typically allow U.S. to eliminate nearly a couple of networks that could be the supply of the assaultive packet stream.

IV. RELATED STUDY

A. Monitor Nodes Technique Monitor nodes supervise whether there occurs any jamming or misrouting of information through other remaining nodes. Manju V.c and Sasi Kumar M [2] has proposed a technique for identifying jamming attack in the wireless sensor networks. Based on residual energy of nodes some of the existing nodes are marked as monitor nodes. These nodes collect the Receiver Signal Strength Indicator and packet delivery ratio from all the other nodes. Based on this metric, they compute a weight value of each node. The computed weight value is compared against the threshold value. When the estimated weight value goes beyond the threshold value, the corresponding node is marked as jammer and it is isolated from data transmission. This technique significantly improves system performance.

B. Gateway MAC Technique G-MAC is an energy efficient sensor medium access control technique designed to coordinate transmission within a cluster. Michael Brownfield, et al., [1] has described the energy resource vulnerabilities of Wireless Sensor Networks. They also proposed a new MAC protocol which mitigates many of the effects of denial of sleep attacks. G-MAC has several energy-saving features. It shows guarantee in extending the network existence and also the centralized architecture makes the network more resistant to denial of sleep attacks.

C. Evasion Technique Wenyuan Xu, et al., [4] has proposed two different but complementary approaches. First approach is to simply retreat from the interferer, which may be accomplished by either spectral evasion (channel surfing) or spatial evasion (spatial retreats). The second approach aims to compete more actively with the interferer by adjusting resources, such as power levels and communication coding, for achieve communication in the presence of the jammer. These techniques are important areas for studying and classifying the scenarios where one defense strategy is advantageous over another. Mingyan Li, et al., [3] have derived solutions to the optimization problems, optimal attack and network defense strategies. They also found alternatives for modeling lack of knowledge for the attacker and the network.

D. Multi Dataflow Technique Multi dataflow is a topologies scheme that can effectively defend the mobile jamming attack. Hung-Min Sun, et al., [5] have multi dataflow topologies scheme to reduce the affected area caused by the mobile jamming attack. Mobile jamming attack not only causes the energy consumption but also breaks the routing on WSN and also shows that the existing defense mechanism is unable to withstand this attack.

E. WCL Technique The low complexity, the fast calculation and the minimal resource requirements recommend WCL as localization algorithm in wireless technique. Jan Blumenthal, et al., [6] has introduced Weighted Centroid Localization technique to make it fast and easy for the algorithm to locate devices in wireless sensor networks.WCL algorithm is derived from a centroid determination which calculates the position of devices by averaging the coordinates of known reference points. They summarized the basic theoretical and practical facts concerning the analysis of RSSI measurements.

F. LMAC Technique LMAC has proven to be the most resistant protocol against energy efficient attack. LMAC is a good representative of the TDMA category. In LMAC time is divided into frames, which are further divided into time slots. David R. Raymond and Randy C [7] have classified the Lightweight Medium Access Control (LMAC) technique. Initially, it classified denial-of-sleep attacks on WSN medium access control protocols based on an attacker"s knowledge of the MAC protocol and ability to penetrate the network. Next, it explored potential attacks from each attack classification. The impacts on sensor networks running for leading WSN MAC protocols and analyzing the efficiency of implementations of these attacks. Finally, it proposed a framework to defend against denial of- sleep attacks and provides specific techniques that can be used against each denial-of-sleep vulnerability. Ahmed R. Mahmood, et al., [8] has proposed and evaluated two modifications to the Lightweight Medium Access Control (LMAC) [3] protocol. The first is Data Packet Separation Slot Size Randomization (DSSSR) and the second is Round Robin (RR) slot size assignment. Enhancing the attack and applying it to other types of protocols is also a potential future work because the war between the attacker and defender never ends. Saman Taghavi Zargar and James Joshi [9] in their work have explore the scope of the DoS flooding attack problem and attempts to combat it and categorize the DoS flooding attacks and classify existing countermeasures based on where and when they prevent, detect, and respond to the DoS flooding attacks.

V. PROBLEM DEFINITION & SOLUTION

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.

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. 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.

VI. METHODOLOGY

In the very first step of research proposal as defined in the flowchart, nodes of MANET will be deployed in the creation of node step:

a) **Creation of Nodes:** With the advances in software and hardware architecture, mobile nodes can be created according to the requirements. Each node is equipped with a transmitter and receiver and they are said to be purpose specific, autonomous and dynamic. The packets in this network contain a single field associated with the destination address in it.

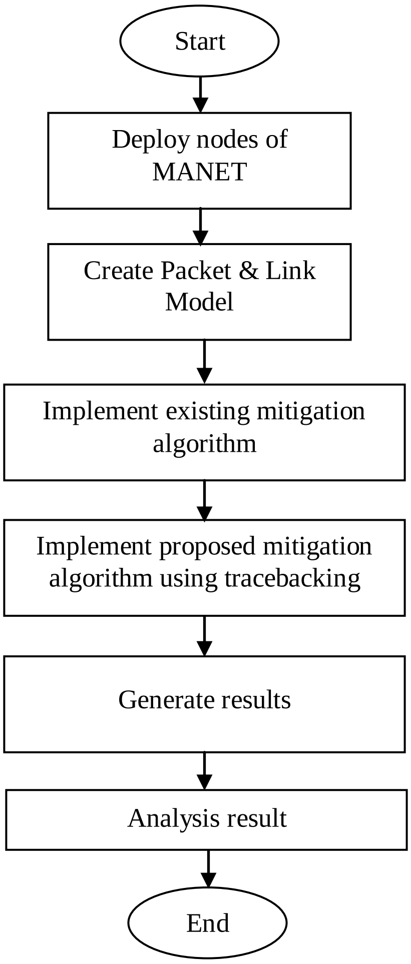
Start
Deploy nodes of MANET
Create Packet & Link Model
Implement existing mitigation algorithm
Implement proposed mitigation algorithm using tracebacking
Generate results
Analysis result
End

Fig 2: Flow Chart of protocol enhancement

After the creation of the nodes of network the packet modeling, link modeling and hub modeling are defined below:

b) **Defining Packet Model and Link Model:** After the packet format has been created, it is specified as an attribute in a generator so that it can beformatted accordingly. The packet contains attributes such as name, type, size. Also, the set at creationattribute is changed to unset which may ensure that the field will not be assigned a default value when thepacket is created.

c) **Creation of Hub Model:** The hub model consists of point-to-point transceivers for each peripheral node, and a processmodel to relay packets from receiver to the appropriate transmitter. The packet streams have a unique indexwhich is an easiest method to set up a direct association, between the hub processes which indices outgoing packet stream and the peripheral destination address values.

Creation of Peripheral Node Model: The peripheral node model generates packet, assigns destination address, and processes receivedpackets. It uses a user-defined process model to assign destination addresses to the generated packet andtransmit them to the node's point-to-point transmitter. This process model retrieves the packet arriving fromthe point-to-point receiver and processes it to calculate the packet's end-to-end delay and the value iswritten to a global statistic so that it is accessible to multiple processes throughout the system.

VII. RESULTS AND DISCUSSION

In this research study the effect on various QoS parameters such as Load, Average End-to-End Delay, Throughput, Average Energy Consumption have been seen by varying the no. of nodes i.e. 20,40,60,80 and 100 nodes at the constant speed of 100m/s after implementing the proposed and existing approach.

1) Performance Metrics

1. Average End-to-end Delay: The second metric is average end-to-end delay, it is the average between a packet being created and being delivered to the sink. The average delay in a TDMA multihop based protocol depends greatly on the order of the allocated time slots of the forwarding nodes. The best case scenario is that the forwarding nodes are in sequence.

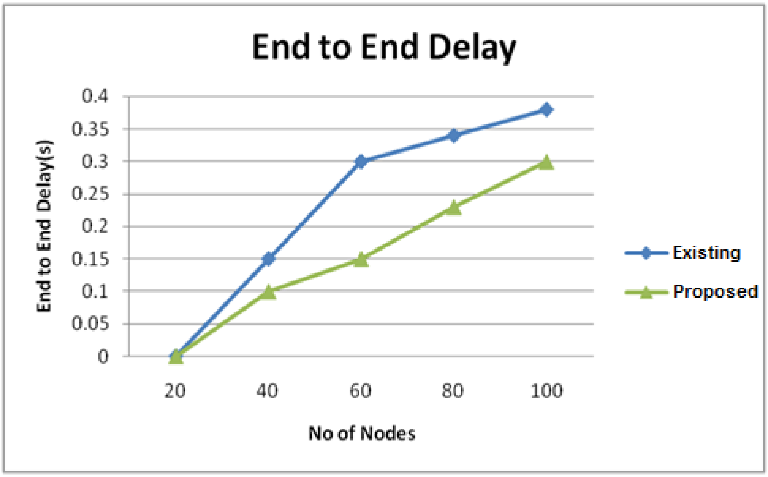

Fig 3: Comparison of Average End-to-end delay

Figure 3 shows the better results of average end- to-end delay in EVGDRA. As the path is deviated load is less so the packets will reach to destination in time without any delay as the result of which end to end delay in the proposed is less as compare to Existing.

2. Load:

Overhead is a major factor in designing routing protocols for mobile sensor networks since more no. of packets can cause congestion, which will limit the throughput of data. There are generally two types of overhead; packet overhead and control overhead. Packet overhead is the ratio of non-data bits to data bits in a data packet. Control overhead is the ratio of bits in control packets to bits in data packets. Control packets are often used to negotiate channel access, discover routes or share topology information.

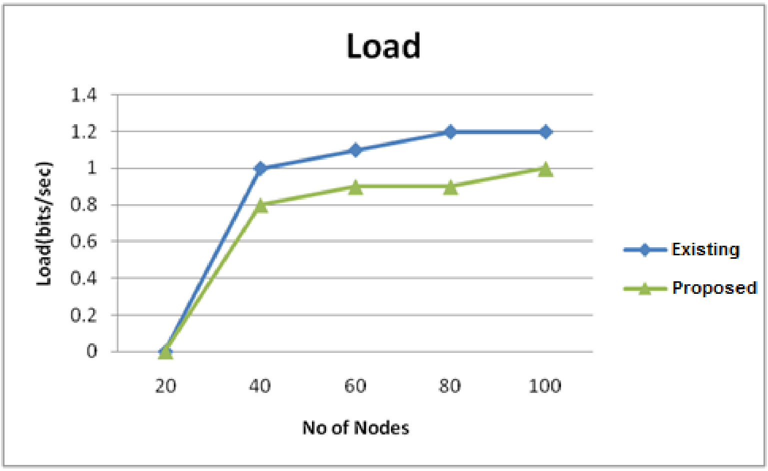

Fig 4: Comparison of load

Figure 4 shows low overhead result shown by proposed as compare to existing. As the packet drop is reduced the packet delivery ratio is improved so all the packets are delivered in time so overhead is reduced in proposed scenario.

3. Throughput:

Throughput, is defined as the number of data bits successfully delivered to the sink, per second, over the entire simulation time.

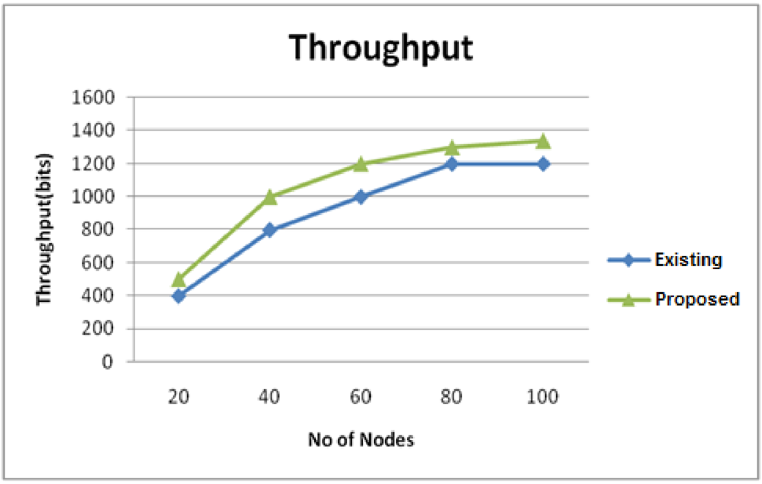

Fig 5: Throughput comparison

Figure 5 shows that Proposed algorithm shows better results as shown in graph. As the packets will take the reciprocal path more no. of packets will reach to the destination without any loss so as a result of which throughput of Proposed is improved.

VIII. CONCLUSION

The evolution in intruder tools is a long- standing trend and it will continue. And, DoS attacks by their very nature are difficult to defend against and will continue to be an attractive and effective form of attack. To investigate the issue of distributed denial of service by means of the proposed architecture and mechanism for detection and control of DDOS attacks over reputation and score based MANET. To studied a novel DoS attack perpetrated by Jel- lyFish: relay nodes that stealthily misorder, delay, or periodically drop packets that they are expected to forward, in a way that leads astray end-to-end congestion control protocols. This attack is proto- colcompliant and yet has a devastating impact on the throughput of closed-loop flows, such as TCP flows and congestion-controlled UDP flows. For completeness, we have also considered a well- known attack, the Black Hole attack, as its impact on open-loop flows is similar to the effect of JellyFish on closed-loop flows. We studied these attacks in a variety of settings and have provided a quantification of the damage they can inflict. We showed that, perhaps surprisingly, such attacks can actually increase the capacity of ad hoc networks as they will starve all multihop flows and provide all resources to one-hop flows that cannot be intercepted by JellyFish or Black Holes. As such a partitioned system is clearly undesirable; we also consider fairness measures and the mean num- ber of hops for a received packet, as critical performance measures for a system under attack.

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.

[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.