I.J. Modern Education and Computer Science, **2014, 1, 65-71**
Published Online January 2014 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijmecs.2014.01.07

Distributed Denial of Service Attacks: A Review

Sonali Swetapadma Sahu
School of Computer Engineering, Kalinga Institute of Industrial Technology (KIIT), India
Email: sonali90sahu@gmail.com

Manjusha Pandey
School of Computer Engineering, Kalinga Institute of Industrial Technology (KIIT), India
Email: manjushapandey82@gmail.com

Abstract **—** A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to monitor physical or environmental conditions.WSN is a fluorishing network that has numerous applications and could be used in diverse scenarios. DDoS (Distributed Denial of Service) is an attack where a number of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users.Not much research work has been done in DDoS in WSN.We are conducting a review on DDoS attack to show its impact on networks and to present various defensive, detection and preventive measures adopted by researchers till now.

Index Terms **—** Distributed Denial of Service attack, Wireless Sensor Network, Networks, Detection, Prevention, Defense.

I. INTRODUCTION

A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to monitor physical or environmental conditions. A WSN system incorporates a gateway that provides wireless connectivity back to the wired world and distributed nodes. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting .The main characteristics of a WSN includes:

- Power consumption constraints for nodes using batteries or energy harvesting
- Ability to cope with node failures
- Mobility of nodes
- Communication failures
- Heterogeneity of nodes
- Scalability to large scale of deployment
- Ability to withstand harsh environmental conditions
- Ease of use

A DDOS attack (better known as a Distributed Denial of Service attack) is a type of web attack that seeks to disrupt the normal function of the targeted computer network. This is any type of attack that attempts to make this computer resource unavailable to its users.A DDOS attack is simply a combined effort to prevent computer systems from working as well as they should, typically from a remote location over the internet. A number of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users. The most common method of attack is to send a mass saturation of incessant requests for external communication to the target. These systems are flooded with requests for information from non-users, and often non-visitors to the website. The goal of this attack is to create a large enough presence of false traffic such that legitimate web traffic intended for actual web users is slowed down and delayed. If this type of service becomes too slow, time sensitive information such as live video footage may be rendered entirely useless to legitimate end users.

WSN has several issues like energy, computation, communication capabilities, deployment, storage, power consumption, longevity etc that makes it prone to various attacks. DDoS is one of them.

The rest of the paper is structured as follows. Section II describes about the defense and detection techniques based on filtering. Section III deals with mechanisms to detect, prevent and defend DDoS attack based on flooding. Section IV discusses an approach to build a defense infrastructure. Section V discusses mechanisms to counter application layer DDoS attack. Section VI discusses about broadcast authentication and safe routing in WSN against DDoS. Section VII discusses mechanisms involving distributed defense approaches. Section VIII discusses about the fast traceback technique. Section IX discusses mechanism regarding anti spoofing and mitigation of DDoS attack.

II. DEFENSE AND DETECTION OF DDOS ATTACK BASED ON FILTERING

Mechanisms are discussed below regarding defense against and detection of DDoS attacks with regard to IP spoofing, a two tier scheme, packet marking and users' feature monitoring.

A. Detection and Defense against DDoS Attack with Spoofing

An HCF (Hop Count Filtering) technique is used to detect the attack and to drop the spoofed IP packet [1] [18].

```
1. For each packet:
2. Extract the final TTL Tf;
3. Extract source IP address S;
4. Find Initial TTL Ti;
5. Find Hc (Hop Count) =Hi-Hf;
6. Use S to extract stored Hs (Hop count)
from IP2HC mapping table;
7. If (Hc! = Hs)
8. The packet is spoofed;
9. Else
10. The Packet is legitimate;
```

HCF can be efficiently implemented inside the Linux kernel. It is a simple and effective solution in protecting Internet servers against spoofed IP packets. HCF is readily deployable in end systems Moderate amount of storage is required. There are 0% false positives. Considerable false negatives collateral damage can occur.

Since hop-count values have a limited range, 1 and 30, multiple IP addresses may have the same hop-count values. If attacker unfortunately is having same number of hops as that of spoofed IP address then IP2HC (IP to Hop Count) mapping table cannot classify that packet as spoofed. TTL (Time To Live) is an extra field in the IP header.Its tranmission will consume more energy. On demand routing is not possible.Suppose routing path is changed then Hc! =Hs. The packet may be legitimate but it will be considered as spoofed. If rerouting happens then when every time Hs is updated, the table also needs to be updated.Updating of IP2HC mapping table after a fix time span can be an overhead. Use of 8 bit prefix can save more memory space.

B. A Two-Tier Coordinated Defense Scheme against DDoS Attacks

A two-tier coordination approach for detecting and mitigating DDoS attacks is used. The first tier traffic filter (lst-TF) filters suspicious traffic for possible flooding. This is achieved by using proactive tests to identify and isolate the malicious traffic. The second tier traffic filter (2nd-TF), which is deployed on network routers, performs online monitoring on queue length status with RED (Random Early Detection)/Droptail mechanism for any incoming traffic [2].

The system is scalable due to the distribution of processing workload. Computation of arrival rate and queue length is simple. Detection of high-rate as well as potential low rate attack is possible. Workload of routers is reduced.

The FPR (False Positive Rate) and FNR (False Negative Rate) for 2nd-TF RED has the worst performance. The reason is that the arrival rate of a flow may not depend only on the drops at the router, but also on the demand from application, and the drops elsewhere along the path. Therefore, legal packet can be easily identified as illegal one, and vice-versa. If the discarded packet is legal, then the sending rate will be reduced based on TCP protocol .On the other hand the attack traffic maintains its sending rate.

RED is used to overcome the shortcomings of Droptail mechanism i.e. low throughput and high delay. RED can be solely used to tackle low rate traffic. Droptail method can be eliminated from the proposed mechanism.

C. An Active DDoS Defense Model Based on Packet Marking

The model is composed of the subsystem of the tracking of the attacks and the subsystem of filtering of the attack flows. The function of the former is to reconstruct the attack paths using the information from the marked packets while the function of the later is to filter the attacking packets according to the information obtained from the former. In addition, flow detection and neural network are also used in the model so that the model is more powerful in the functions of identification and filtering of attack packets and protection of the legitimate flows [3] [17].

The model has a higher efficiency in reconstructing the attack path. It is simple to realize with reduced cost. As the scheme can improve the efficiency of tracking and recognize the attack packet, the information in the database is much more reliable and the filtering module can filter the attack flow with a much higher credibility. The basic probability packet marking scheme does not need the topology information of the network and has improved a lot on the false alarm rate, computational complexity, convergence and security. No additional storage is needed. ISP cooperation is not required. False alarm rate is low.

The model requires marking of every packet that comes into the router so as to be able to traceback to the source. But this incurs overhead. The decision making module can be eliminated as the functionalities that are accomplished by this module can also be achieved using the filter module.

D. Defending Systems against Tilt DDoS Attacks

This paper proposes an effective defense system to resist against Tilt-DDoS attacks, denoted as DAT. DAT monitors a user's features (e.g. request volume, instant and long-term behavior) throughout a connection session to determine whether he is malicious user or not. For users behaving differently, DAT provides differentiated services to them. Therefore, DAT guarantees a certain level of services to legitimate users even under attacking. In addition, this paper also designs counter-attack mechanisms such as filter, rate-limiter and scheduler to downgrade services to malicious users. The observed

Copyright © 2014 MECS

users' behaviors also pass to scheduler as scheduling parameters. A new scheduling strategy is also proposed for the scheduler in DAT to further improve the service throughput of legitimate users [4].

The DAT is capable of effectively suppressing DDoS attacks, so that the protected server cluster is able to operate normally even under attack. It concentrates to serve legitimate users instead of wasting resources on malicious users. There is significant improvement in system's throughput. Robustness is high. DAT outperforms in terms of response time and detection accuracy.

For LDF (Lowest DbD First) scheduling, a high threshold may lead to many users with higher DbDs (Degree of Behavior Deviation) receive low (even zero) service throughput and cause starvation. In this mechanism a threshold of maximum request rate is set. But the issue is selection of threshold value so that neither false positive nor false negative is unreasonably magnified. So considering this aspect analysis is required to be done.

III. DETECTION, PREVENTION AND DEFENSE AGAINST DDOS ATTACK BASED ON FLOODING

Mechanisms are stated below based on flooding to detect, prevent and defend against DDoS attack.

A. A Real-Time DDoS Attack Detection and Prevention System Based on per-IP Traffic Behavioral Analysis

Based on per-IP behavioral analysis, a new DDoS detection system is realized. For each IP user, our system will create records for every single IP user's sending and receiving traffic and judge whether its behavior meets the normal principles. A specific packet identification technique is utilized to reach real-time flooding attack detection goal. A non-parameter CUSUM (Cumulative Sum) algorithm is applied to detect the abnormal behavior of each IP. Based on a decision algorithm, each IP user will be classified as attacker, victim or normal user. After differentiating the attacker, the system will block its traffic and forward the normal user packets [5].

Based on per-IP traffic behavior analyses, it is easier to differentiate the attackers from the normal users. As the approach needs less computation and memory, the system could be deployed for on-line DDoS detection and prevention.By applying the non-parameter CUSUM algorithm and decision algorithm, this system can detect attacks accurately at the earlier attack stage. The system can quickly filter the attack traffics and forward the normal traffics simultaneously by means of the fast identification technology. The system has high DDoS detection accuracy and short detection time. For DNS flooding attack and Smurf attack, the system can find out the attacks by checking the mismatch between the request packets and response packets.

The system does not immediately take defensive measures to stop the attack, but keep observing the suspected IP record. After the alarming of attacks counts more than three, the system starts to filter the traffic from the attackers. As most attackers spoof the source IP to unreachable addresses, the server cannot receive their ACK (Acknowledgement) packets to complete the TCP connection. Therefore, in the records, the number of transmitted ACK packets from attackers could not be updated.

At the application layer stage, the data unload module can be eliminated. A flexible mechanism should be adopted in which from the suspicious IP, segregation of attackers and victims could be done instead of waiting for the counter value to reach 3.

B. A Distributed Defense Framework for Flooding-Based DDoS Attacks

A distributed framework is proposed to defend against DDoS attacks. It has three major components: detection, traceback, and traffic control. A detection component of a victim-end defense system detects unusual changes of incoming traffic to identify hidden attacks. The traceback component mainly focuses on analyzing incoming traffic to identify the addresses of routers at the source end of the attack. When an attack is found to be in progress, the traceback component of the defense system at the victim end first identifies the edge routers at the source end using the Fast Internet Traceback (FIT) technique. The defense system at the victim end then sends alert messages to source-end nodes. When an alert message from a victim end is received at the source end, the traffic control component of the source end defense system is triggered to set up rate limits on the edge router of the source end to reduce the attack traffic that is forwarded towards the victim end [6].

The rate limit mechanism efficiently reduces attack traffic from being forwarded to the victim that is efficiently drops the attack packets at the source end while maintains QoS for the legitimate traffic at the victim end. Average latency and failure rate of HTTP transactions with the distance-based framework are less. Collateral damage is less.

After an attack the recovery process in the framework is slow. During an attack, the framework does not perform well to decide whether an attack has ended. This might lead to trigger the recovery mechanism even when an attack is under progress. It would be better if the recovery process is executed at the source end.

C. Global Detection of Flooding-Based DDoS Attacks Using a Cooperative Overlay Network

In this paper, a distributed defense infrastructure is proposed to detect DDoS attacks globally using a cooperative overlay network and a gossip-based information exchange protocol. The overall approach is outlined below:

1) Each node makes an independent, local measurement of the victim bitrate.
2) All nodes participate in distributed averaging algorithm whereby they arrive at the average of their local measurements – ideally they would all

arrive at the same value.

3) Since the distributed averaging algorithm takes some time to complete, each node locally adjusts the resulting average by combining it with its latest local measurement.
4) The adjusted average is then multiplied by the number of overlay nodes and the result is taken to be the total victim traffic that originates from distance ≥ d to the victim. This is further corrected to account for victim traffic that cannot be measured, i.e. traffic that originates
from distance< d to the victim, to obtain the total victim bit rate.
5) Each node then locally tests whether the victim bit rate exceeds the victim’s capacity. If at least 50% of a node’s local tests are positive within a given time window then the node flags that an attack is happening at that time [7].

The proposed solution can detect attacks with a detection rate as high as 0.99 with false alarms below 0.01. As a decentralized approach is adopted, there is no single point of failure.

There may be not enough time for all packets to be communicated between all defense nodes in each round of the gossiping, i.e. the round time may be less than the required communication time. In this case, packets which arrive after the round are discarded. This leads to errors in the averaging process. Increasing the number of rounds, either by increasing the phase time or by decreasing the round time, leads to wastage of various network resources and increase of detection latency. The overlay does not measure packets that come from inside the overlay, i.e. traffic that comes from nodes at a distance less than the overlay distance from the victim. Increasing the round time and increasing the number of rounds generally increases the False Positive rate.

Attack packets may be sent within the overlay. In order to block these packets from reaching the victim some lightweight alert node should be deployed within the overlay. For early detection of attacks number of rounds should be less. Instead of discarding packets that arrive after the round, they can be put in a waiting queue where in the next round they can be picked up. This may not create error in the averaging process.

IV. INTEGRATED DDoS ATTACK DEFENSE INFRASTRUCTURE FOR EFFECTIVE ATTACK PREVENTION

A general purpose DDoS defense technology is developed where the attack phases are analysed alongwith the general characteristics of attacks. For each phase DDoS attack prevention requirements are proposed and the integrated DDoS attack defense infrastructure is suggested [8].

Focus is on general characteristics and infrastructure not on specific characteristics. Novel attacks can be detected.If the suggested requirements are developed and applied to current DDoS attack defense systems, then DDoS attack could be effectively blocked.

For Attack agent development phase prevention, the mechanism is dependent only on degree of law against hacking and DDoS attack. The C&C (Command & Control) server connection detection is not a majestic agent detection method. If very high amount of network traffic occurs, then software based analysis methods could not handle the situation and the analysis results can show high rate of false negatives. Source IP address could be spoofed.It is impossible to identify the exact IP address of attack systems. Therefore, access control list based packet blocking is impossible.

For preventing the attack agent's development simply relying on the execution of the law will not bear fruit rather a protocol or a sensing device could be installed that might hinder the development of the attack agent. For agent control mechanism detection, additional analysis is inevitable. With the analysis, connection initiation mechanism should be identified first.IP spoofing could be detected by observing the massive traffic flow.

V. APPLICATION LAYER BASED DDoS DETECTION

Counter and detection measures are discussed for application layer DDoS attacks.

A. An Effective Approach to Counter Application Layer DDoS Attacks

This paper proposes a scheme to counter application layer DDoS attack and to schedule the flash crowd during DDoS attacks. In this scheme, an Access Matrix is defined to capture the access patterns of the legitimate clients and the normal flash crowd. Dimensionality reduction schemes are applied to reduce the multidimensional Access Matrix. A counter-mechanism consisting of a suspicion assignment mechanism and a scheduler is deployed. The suspicion mechanism assigns a score to each client session, and the scheduler decides whether to forward the session's requests or to drop the request based on the suspicion score [9].

Using the suspicion score, legitimate users can be differentiated from illegitimate users and served even during the flash crowds. It schedules the traffic even on attack based on the system workload and scheduling policy. As the DDoS counter mechanism is integrated into the reverse proxy, the attack request is intercepted from reaching the web server.

Calculation of suspicion score will be computationally expensive and resource constraint issue arises. An algorithm is needed to be designed in such a manner that it will be resource efficient and incur less computation overhead.

B. Application layer DDoS detection using clustering analysis

This paper introduces clustering analysis method to model users' browsing behavior and to detect the App-DDoS attacks. The main idea of this method is to cluster users' sessions. To detect App-DDoS, deviation between sessions and normal clusters is calculated. We extract four features from session to cluster user's sessions– average size of objects requested in the session, request rate, average popularity of all objects in the session, average transition probability. By clustering users' sessions, user's browsing behavior can be grouped. When App-DDoS takes place, attack sessions can be separated from the normal ones [10].

The simulation result shows that the method is effective to detect App-DDoS attacks. The system adopts hierarchical clustering in which it is not required to determine the number of clusters in advance. Thus provides flexibility. As normalization is used, the effect of difference between scales of the features is eliminated.

The consideration of the fact that bots are unaware of the object's popularity of the website may not hold true. This may lead to wrong analysis of the measures that could have the potential for detection of the DDoS attack. Other efficient clustering methods need to be explored. More features should be extracted from the user's sessions to describe web user's browsing behavior more exactly.

VI. BROADCAST AUTHENTICATION PROTOCOL SCHEME BASED ON DBP-MSP AND SAFE ROUTING IN WSN AGAINST DDOS ATTACKS

In order to help WSN achieve better performance against DDoS attacks in broadcast authentication, a new strategy based on DBP-MSP (Dynamic Bit Pattern-Message Specific Pattern) and safe routing is proposed in this paper. Puzzle mechanism is used with difficulty level k decided by the base station in DBP-MSP. By introducing a broadcast state table, which is updated by the base station according to messages from nodes, the receiver can verify the puzzle solution by the message the base station returns by searching the table. A key chain distribution scheme is introduced where the base station passes the one way key chains to the sender every time interval [11] [19].

DBP-MSP improves the performance of broadcast authentication against DDoS attacks. This approach reduces the energy and memory consumption of the sender thus extending the lifetime of WSN. The storage and computation burden on the sender can be reduced. Because of the use of dynamic bit pattern, an attacker can not pre-compute the answer, and hence can not arouse efficient DDoS attacks. Replay attack is prevented. Because of the use of safe routing strategy, one-way key chains are unique for each sender so that the security of broadcast authentication is strengthened. So disclosure of one of the chains will not help an attacker to compromise another one.

Because of the use of hash function, the sender has to search through all possible solutions to solve the puzzle. This incurs overhead in terms of searching time. An optimized secure hash function can be built or any other mathematical function can be used that does not incur space and computation overhead.

VII. DISTRIBUTED DEFENSE AGAINST DDOS ATTACKS

Distributed defense mechanisms are discussed.

A. A Novel DDoS Attack Defending Framework with Minimized Bilateral Damages

This paper proposes Heimdall, a novel traffic verification based framework to protect legitimate traffic from bilateral damages. Heimdall architecture consists of three distinct function units: a puzzle/identifier generator, a puzzle solution verifier, and a puzzle resolver. A CAT (Change Aggregation Tree) is constructed after a DDoS attack is detected and the victim is recognized [12] [18].

The mechanism protects established connections. The system can validate new initial request for communication. It opens valid channels between users and the protected server. It filters out malicious flows with very high accuracy. The UPI (Unique Puzzle Identifier) prevents attackers from using the same solution to launch replay attacks.

The edge routers may themselves become targets of a coordinated DDoS attack. If the path to such a router does not include any other hardened routers it may not be able to cope with the attack. It does not closely correspond to real world scenario. If multiple ISPs adopt Heimdall, the spread of Heimdall routers would make such attacks targeted on individual routers even more difficult.

B. A Collaborative Peer-to-Peer Architecture to Defend Against DDoS Attacks

In this paper, an efficient and distributed collaborative architecture is proposed that allows the placement and the cooperation of the defense entities to better address DDoS attack. The use of content based DHT (Distributed Hash Table) algorithm permits also to improve the scalability and the load balancing of the whole system. This modular architecture has been implemented on IDS (Intrusion Detection System) entities with the DHT Pastry protocol [13].

Due to the use of peer to peer model, the possibility of storage overload at some points is reduced. No single point of failure occurs. In addition to this robustness, high scalability and fast resource lookup are achieved. As HMAC function is used, hash function can be used without any modification. The integration of the HMAC function adds a robust access control with the sharing of a key in association with the original hash function. The Security Level can implement any IDS module that can provide data information and alerts on possible attacks. For the P2P (Peer to Peer) Level, it can be based on any DHT algorithm that permits the efficient distribution and exchange of data among the different nodes of the architecture. The load balancing is ensured by the consistent hashing of the DHT.

Replication of information may lead to consumption of additional memory space. In the developed program a threshold is fixed that must be reached to decide that the traffic is probably malicious. An issue is that fixing a threshold is not enough to decide if a flow is an attack because each of distributed flows can be under this limit and present a danger to the victim when they are aggregated. The Management Network in the proposed system can present some complexity because of the dynamic aspect of the DHT nodes.

Use of distributed approach ensures no single point of failure. So the replication process need not be used. A judicious approach should be adopted in fixing a limit so that neither false positivites nor false negatives occur.

C. RateGuard: A Robust Distributed Denial of Service (DDoS) Defense System

In this paper, a Leaky-Bucket (LB) based highly robust DDoS defense system, called RateGuard is proposed. It can react to FAAs (Fast Adaptive Attack) and LRAs (Low Rate TCP Attack) by rate-limiting excessive traffic in real-time according to the victim's nominal traffic profile. Moreover, by associating an LB with each joint attribute value, the huge space required for possible joint attribute values makes it almost impossible for attackers to scan the victim's nominal traffic profiles and, thus, makes it highly robust to cope with AAS (Adaptive Attacks with statistical filtering rules Scanning) and other sophisticated attacks [14].

Because of the simple operation of LB based rate control, it can quickly rate limit any excessive traffic beyond the predetermined rate set according to the nominal traffic profile without the need for complex processing. The response time of RateGuard, a LB-based dynamic rate-limiting system, can be much smaller than RTT (Round Trip Time). Thus it can avoid the FOFA (Fail Once Fail Anytime) problem and react to FAA in real-time. RateGuard can effectively mitigate LRA by rate-limiting the attacking traffic at the ingress line cards. Low false positive and low false negatives result.

The huge space required by possible joint attribute values makes the defense system very costly as it has to store the large nominal traffic profile and keep track of the large number of LBs.

VIII. FAST TRACEBACK AGAINST LARGE-SCALE DDOS ATTACK IN HIGH-SPEED INTERNET

This paper describes a novel DDoS traceback scheme. The proposed scheme maps k hash digests of the router's IP into an m-bit Bloom Filter array. Then the m-bit Bloom Filter array is probabilistically written into the IP header of the passing packet or deterministically accumulated with the marking information in the IP header of the marked packet. If the Bloom Filter array in the marking information is full, the marking information is probabilistically written into another packet with the same source address and same destination address [15] [17].

The scheme has low false positive rate. Fewer packets are required to reconstruct the attack path. There are low computation overhead and storage overhead at the router. False negative rate does not exist. There is no extra network communication overhead. The space for marking in the IP header is limited. It depends on the size of the spare space in the IP header.

IX. MANTLET TRILOGY: DDOS DEFENSE DEPLOYABLE WITH INNOVATIVE ANTI-SPOOFING, ATTACK DETECTION AND MITIGATION

In this paper Mantlet, an overlay-based approach to detect and mitigate DDoS attacks, is proposed. Mantlet combines three innovative mechanisms for anti-spoofing, attack detection and mitigation, respectively. To circumvent IP spoofing [18], a probing mechanism named Bypass Check is proposed to authenticate the clients of TCP or UDP services. Then, Cumulative Sum (CUSUM) is adopted to detect DDoS attacks based on the abrupt change of sequential packet symmetry, the ratio of received to transmitted packets of a service. After detection, the suspicious flows that contribute to asymmetry are segregated and experience preferential dropping test (PDT). A suspicious flow is confirmed as malicious if it is unresponsive to packet drops [16].

Mantlet is not a service-specific solution. It does not require changes on the client-side so that it can be developed readily with an overlay network and current path migration techniques. Both MLGs (Mantlet Gateways) and BFs (Bypass Firewalls) maintain no state at this stage so that malicious flows do not occupy any memory at MLGs and BFs.Bypass Check authenticates a TCP client by checking only its first connection request so that Bypass Check has little side-effect on the following communication.UDP is a connectionless protocol so that we cannot validate the source IP address during connection establishment. The limitation of the Bypass Check for UDP source authentication is that it relies on the echo of UDP probing packet from the clients. It takes a long detection delay to detect an attack. To achieve a tradeoff between the security and availability, an alternative way is to rate-limit unauthenticated clients.

X. CONCLUSION

The mechanisms proposed by the authors are mostly regarding the detection of and defense against DDoS attack.Some are also proposed on prevention but they contain loopholes for which desired result has not been accomplished.Very few works have been done on WSN platform to tackle DDoS attack.

DDoS attacks are complex and serious problem affecting not only a victim but the victim's legitimate clients.DDoS defense approaches are numerous so need to learn how to combine the approaches to completely solve the problem.Internet community must cooperate to counter threat global deployment of defense mechanisms.

WSN designs could be made resistant to DoS attacks by answering some of the questions like Who will be the attackers? What are their capabilities? What could be the target? What are the vulnerabilities? What could be the result of the attack? We need to have a solution that will attempt to prevent multiple DoS attacks i.e. DDoS attacks.The security vs. energy efficiency trade-off needs to be considered.

So our target will be to address the problems lying in the existing systems and build a prevention system and implement it so that the attack can be get ridden of to the maximum extent.

REFERENCES

[1] Mr. I. B. Mopari, Prof S. G. Pukale, Prof M. L. Dhore,” Detection and Defense against DDoS Attack with IP Spoofing”, International Conference on Computing, Communication and Networking, IEEE, 2008.

[2] Chin-Ling Chen, Chih-Yu Chang,” A Two-Tier Coordinated Defense Scheme against DDoS Attacks”, IEEE, 2011.

[3] Yongping Zhang, Zhuqing Wan, Mingming Wu,” An Active DDoS Defense Model Based on Packet Marking”, Second International Workshop on Computer Science and Engineering, IEEE, 2009.

[4] Huey-Ing Liu, Kuo-Chao Chang,” Defending Systems against Tilt DDoS Attacks”, The 6th International Conference on Telecommunication Systems, Services, and Applications, IEEE, 2011.

[5] YiZhang, QiangLiu, Guofeng Zhao,” A Real-Time DDoS Attack Detection and Prevention System Based on per-IP Traffic Behavioral Analysis”, IEEE, 2010.

[6] Yonghua You, Mohammad Zulkernine, Anwar Haque,” A Distributed Defense Framework for Flooding-Based DDoS Attacks”, The Third International Conference on Availability, Reliability and Security, IEEE, 2008.

[7] Thaneswaran Velauthapillai, Aaron Harwood and Shanika Karunasekera," Global Detection of Flooding-Based DDoS Attacks Using a Cooperative Overlay Network", Fourth International Conference on Network and System Security, IEEE, 2010.

[8] Yang-Seo Choi, Jin-Tae Oh, Jong-Soo Jang, Jae-Cheol Ryou,” Integrated DDoS Attack Defense Infrastructure for Effective Attack Prevention.

[9] S. Renuka Devi, P. Yogesh," An Effective Approach to Counter Application Layer DDoS Attacks", IEEE, ICCCNT'12.

[10] Chengxu Ye, Kesong Zheng, Chuyu She,” Application layer DDoS detection using clustering analysis”,2nd International Conference on Computer Science and Network Technology, IEEE, 2012.

[11] Jiawei Chen,” Broadcast Authentication Protocol Scheme Based on DBP-MSP and Safe Routing in WSN against DDoS Attacks”, Second International Conference on Networking and Distributed Computing, IEEE, 2011.

[12] Yu Chen, Wei-Shinn Ku, Kazuya Sakai, Christopher DeCruze,”A Novel DDoS Attack Defending Framework with Minimized Bilateral Damages”, IEEE CCNC, 2010.

[13] Radwane Saad, Farid Nait-Abdesselam, Ahmed Serhrouchni,” A Collaborative Peer-to-Peer Architecture to Defend Against DDoS Attacks”, IEEE, 2008.

[14] Huizhong Sun, Wingchiu Ngan, H. Jonathan Chao,” RateGuard: A Robust Distributed Denial of Service (DDoS) Defense System”, IEEE, 2009.

[15] Zaihong Zhou, Biwei Qian, Xiaomei Tian, Dongqing Xie," Fast Traceback against Large-Scale DDoS Attack in High-speed Internet", IEEE, 2009.

[16] Ping Du, Akihiro Nakao,” Mantlet Trilogy: DDoS Defense Deployable with Innovative Anti-Spoofing, Attack Detection and Mitigation”, IEEE, 2010.

[17] Feng Liang, Xinjian Zhao, David Yau, “Real Time IP Traceback with Adaptive Probabilistic Packet Marking”. Journal of Software, 2003.14(5).pp.1005-1010.

[18] Cheng Jin and Kang G.Shin, "Defense against Spoofed IP Traffic Using Hop-Count Filtering", IEEE/ACM Trans. Networking, vol.15 No. I, Feb 2007.

[19] X. Du, M. Guizani, Y. Xiao, H. Chen, "Defending Dos Attack on Broadcast Authentication in Wireless Sensor Networks," In Proceeding of IEEE Communication Society subject matter experts for publication in the ICC 2008.

Sonali Swetapadma Sahu is currently pursuing M.Tech from Kalinga Institute of Industrial Technology in the School of Computer Engineering, Bhubaneswar. She has completed her B.Tech from Koustuv Institute of Self Domain, Biju Patnaik University of Technology, and Bhubaneswar. Her research interest areas include Wireless Sensor Network, Security and Privacy in Wireless Sensor Network and Computer Networks.

Manjusha Pandey is presently working as an Assistant Professor in the School of Computer Engineering, Kalinga Institute of Industrial Technology, and Bhubaneswar. She is pursuing her PhD from Indian Institute of Information Technology, Allahabad. She has more than 10 research publications to her credit in journals and conferences of repute. Her research interest areas include Wireless Sensor Network, Security and Privacy in Wireless Sensor Network, Human Computer Interaction and Computer Networks.