Survey of Detection Techniques for DDoS Attacks

1st Kavita S. Kumavat   
Ph.D. Scholar, Computer Engineering Dept.,  
*St. Francis Institute of Technology,*Mumbai, India  
Assistant Professor at Vishwakarma University, Pune

kavitakumavat26@gmail.com

2rd Joanne Gomes  
 *Head of Dept., Information Technology Dept.,*  
*St. Francis Institute of Technology,*Mumbai, India  
jgomes@sfitengg.org

*Abstract*— The internet has become a vital part of every person’s life today. The world is becoming smarter with applications. Many systems use distributed environment for working. Threads, attacks, and vulnerabilities are the major security concerns of any distributed system. The distributed system is vulnerable to DDoS attacks at different layers of the network. The most harmful attack on the distributed system is Distributed Denial of Service Attack (DDoS) in which an attacker can simply halt the working of all other users connected to the network. To secure distributed systems against DDOS attacks, various intrusion detection mechanisms and tree-based approaches have been proposed for information security. Most of these proposed mechanisms mention in this paper only concentrate on a single type of DDoS attack at any given time. Hence, developing a system that will support detecting and preventing various DDoS attacks is necessary. This paper provides a survey of DDoS attack detection and prevention using traditional techniques and tree-based techniques. Also, this paper will give an introduction to the proposed methodology Network Analysis Tree (NAT) which will be working on the detection and prevention of different DDoS attacks like flooding, DNS amplification, ICMP Smurf, Collision, Jamming, and Tampering.

Keywords— attack, DDoS, detection, prevention, security.

# Introduction

A global structure for data or information society that enables interconnections of advanced services (physical and virtual) is based on interoperable communication and information technologies. It connects different objects, things, and devices that emerged with RFID-based technology. Basic security issues are related to confidentiality, authentication, integrity, and availability [1].To maintain security in the system, it is required to study detailed architecture. The application layer supports middleware security, platform security, cloud security [2]. As the distributed system is supported by a wireless sensor network (WSN), there are more chances of DDoS attacks. DDoS-based attacks on WSN can be broadly divided into two categories an attack against security mechanism and an attack against routing mechanism [3]. DDoS is a very harmful attack on distributed and IoT-based systems. DDoS attack impacts the access of legitimate user. The author categorizes the flooding attacks and organizes previous countermeasures based on when and where that attack was detected, responded to, and prevented the flooding attacks. Also, mentioned the essentiality of collaborative defense and a comprehensive distributed approach [5].

This paper describes the security aspects of a distributed system. Different authentication mechanisms and percentage observations of different DDoS attacks are presented here. Mainly the paper gives an overview of multiple attacks that take place on the distributed system. As DoS and DDoS attacks are more harmful and there are multiple ways through which they affect the system, this paper provides few details about them. This paper basically focuses on the survey of different DDoS attacks detection and prevention mechanisms. Surveys on DDoS detection and prevention concentrate on traditional and tree-based approaches. This paper introduced the proposed mechanism NAT for the detection and prevention of different DDoS attacks.

The paper is arranged in the following manner:

Section II contains a details literature survey, Section III exclusively introduces different threats (DDoS attacks) in the system and details different traditional methods available for detection and prevention of those attacks and Section IV explains different Tree-based approaches, Section V contains a proposed methodology and Section VI concludes the paper.

# Literature Survey

This paper focuses on a survey of different DDoS attacks including TCP SYN flood, ICMP Smurf, DNS Amplification, Jamming, Collision, and tampering attack.

FireCol is an adaptable answer for the initial identification of flooding DDoS attacks. The investigation of FireCol illustrated its light computational and additionally correspondence overhead [6]. TCP SYN flood easily exploits 3-way handshake-based communication. To avoid TCP SYN flood attacks anomaly detection mechanism is used which detects SYN flood attacks in the network using unused regions in HTTP and payload. This anomaly detection mechanism contains a packet filtering and monitoring system. This detection mechanism is faster for attack detection and is effective [7]. Also, an adaptive thresholding algorithm is used to detect and prevent TCP SYN attacks. This algorithm will overcome the constraint of the static thresholding method [24].

M. Robbie proposed an article on computer network security which is used to detect ARP (Address resolution protocol) poisoning, SYN Flooding and ICMP redirect attacks [8]. To protect kernel integrity a trustworthy method is proposed in paper [9] which is used for monitoring a hardware-based system. The authors here present the structure and usage of Address Translation Redirection Attack (ATRA) that empowers total avoidance of the equipment or hardware-based outside monitors that anchor its trust on different processors. If received the ping request is carrying a 1000 bytes payload, then it shows an abnormal ping packet. Hence after getting the ping packet immediate action should be essential [10].

Authors take note of rate-constraining DNSSEC reactions when repeatedly queried by a single source [11]. Amplification attacks utilize the bandwidth of attacking agents effectively, so that, generally, each packet a zombie sends causes compromised machines to send larger or multiple packets to the victim address. The fact of a DNS amplification attack is that the DNS responses are greater than DNS requests [12]. M. Ismail, et. al, proposed a flexible flow (sFlow) method in which all flow data is collected and from that data malicious DNS responses are found to detect DNS amplification attacks. In this method, the attack detection logic categorizes between abnormal and normal traffic by using a particular value of flexible flow, wherein the absence of transaction ID of DNS query would indicate an attack [27]. To detect and prevent collision attacks, (Carrier sense Multiple Access / Collision Notification) CSMA/CN approach is used. CSMA/CN is used to abort unsuccessful transmission with collision notification [13]. The stochastic collision attack is introduced from the concept of the optimal distinguisher, which increases the success when the model is identified [14].

Transmitting adaptive camouflage traffic (TACT) is used to combat jamming attacks. By generating additional traffic called camouflage message delay is minimized by TACT. Experiments demonstrate that TACT can reduce the chance that a message is not delivered on time in order of magnitude [15]. TJC (Threshold-based Jamming Countermeasure) is used to countermeasure which illustrates fine performance in contrast to reactive jamming attacks with changing traffic intervals and several suspicious nodes. The simulation of the algorithm by mobility illustrates TJC adaptability by moving the position of nodes in the system [16]. JAMMY algorithm is provided a solution for a selective jamming attack on the TDMA (Time Division Multiple Access) based WSN (Wireless Sensor Networks) system. JAMMY makes variations in the slot consumption outline at each superframe, thus creating it random to the adversary. JAMMY is decentralized in nature, as sensor nodes control the next slot use design in an autonomous and distributed way. JAMMY results from performance analysis show negligible overhead and allow many nodes to communicate with the network [25].

Against tampering attacks, the authors introduced a TamperProof approach in which parameter tampering is avoided. TamperProof is an efficient and effective mechanism, which doesn’t require any changes on the server-side. TamperProof is an online defense mechanism applied in a trusted environment for client and server communication [17]. In the existing method 2 phases are included, the data transfer phase, and the initial seed sharing phase. In the seed sharing phase, the time-hopping key setup is done with random numbers generated by PDC and PMU. In the data transfer phase, the secret seed is used to produce a random time hopping sequence [18]. In WSN, a Tamper-aware authentication framework is used for authentication of different sensor nodes as well as packets and mitigation of tampering attacks [26].

Our fundamental commitments incorporate a novel enhanced Very Fast Decision Tree (EVFDT) characterization system and it contrasts with the existing system as far as assault characterization exactness furthermore, tree measure. The execution of the EVFDT algorithm is assessed on the manufactured dataset produced by executing a LEACH convention. Attack code is composed to produce a DDoS attack. The trial result demonstrates that the proposed algorithm can distinguish an assault with high arrangement exactness (96.5%) and low false caution rate (1.1%) with less memory overhead [19]. Another tree-based technique ATIDS can be part into two sections: the examination of the progressed attack tree and the exploration of the interruption identification. ADtT is the primary realized attack tree demonstrating procedure particular for interruption identification reasons, while ATIDS is the main realized IDS dependent on demonstrated assault tree guide and gives discovery vulnerability evaluation [20]. Augmented Attack Tree provides a bottom-up detection algorithm for the detection of DDoS based on three attacks UPD flood, ICMP flood, and TCP SYN flood attack. This algorithm provides logic to observe the network traffic between the victim server and the internet [21]. An attribute tree is invented to measure different aspects of attack filtered from attack traffic to improve detection accuracy. The legitimacy of the packet is detected by the attribute tree. But attribute tree is not able to complete prevention from attack [22]. Change Aggregation Tree (CAT) is an aggregation scheme invented from Distributed Change-point Detection (DCD) Architecture. In real-time anomaly is detected by the CAT tree. CAT tree efficiently works for less than 180 nodes [23]. The Lightweight Decision-Tree model [28] based on the C4.5 Algorithm works for detecting flooding-based DDoS attacks in three steps. First is a pre-processing step in which feature extraction of DDoS attacks is done. In the second step training of the algorithm C4.5 is done and in the last step testing and justification of the Decision-Tree algorithm is takes place.

# Threats in Distributed System

This section presents details of TCP SYN flood, ICMP Smurf, DNS Amplification, Jamming, Collision, and Tampering attacks that are relevant to distributed systems. Also, this section will give details of existing techniques available for the detection and prevention of attacks.

## TCP SYN Flood Attack

TCP SYN flood is a DDoS attack in which the attacker uses a three-way handshake mechanism for communication to exploit the server. In this attack, the attacker sends multiple TCP/IP requests to exploit the server and keeps the half-open connection to attack the system as shown in Figure 1. Thus, when an attacker uses the half-open connection to exhaust the server and all its resources, the system may crash and though the server is free, the legitimate user will not be able to access it.

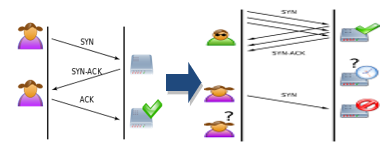


Fig. 1. TCP SYN Flood attack

J. Francois, I. Aib, and R. Boutaba [6] have introduced a “Firecol” approach for providing collaborative protection against flooding-based DDoS attacks. The authors introduced the architecture and algorithm of Firecol which provide a composed intrusion prevention system. Firecol provides low overhead with incremental deployment support. Firecol architecture contains a selection manager (for checking and rule selection), score manager (for updating the score list and looking for abnormal scores), and detection manager (Update/Compute the bandwidth of the examined rule and control if the attack or not).

***High potential attack = horizontal communication (Compute the packet rates)***

But, the limitation of the Firecol approach is that it does not support Intrusion Prevention. Different rule structures, CUSUM, and adaptive threshold algorithms [7] are only used to detect SYN flood attacks but they do not provide prevention.

Also, one of the effective algorithms for TCP SYN flood detection and prevention is the Adaptive threshold [24] which will reduce the false-positive ratio compared to the static thresholding method. This algorithm will alert users of any change in threshold calculation.

In future works, the adaptive threshold algorithm is extended for the detection and prevention of ICMP flooding, HTTP flooding, etc. attacks.

## ICMP Smurf Attack

ICMP smurf attack is one type of DDoS flooding-based attack in which the attacker uses a spoofed IP address to broadcast requests. It uses ICMP echo request and ICMP echo response. Smurf attackers use the whole network of computers to redirect an overwhelming amount of traffic to a victim's machine and its network as shown in Figure 2.

Step 1. The attacker identifies a victim’s IP address.

Step 2. The attacker sends an ICMP ECHO REQUEST at the broadcast address of the network. The packet has the source IP address spoofed to the point toward the target.

Step 3. The host’s ICMP ECHO RESPONSE on the network will be focused to the target’s IP address.

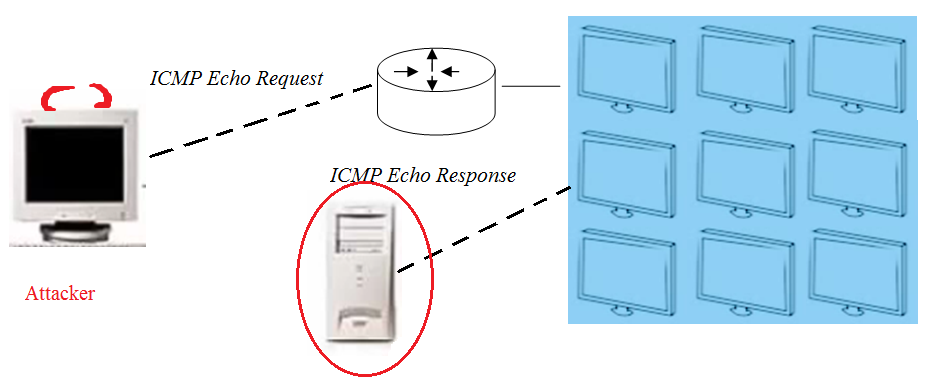


Fig. 2. ICMP Smurf Attack

In the existing study, under DDA (Distributed Defense Approach) [10] traffic on the router is measured and then compared with the threshold to check whether it is greater than the normal size of the ping packet.

The existing system only provides survey-based techniques as a solution for detecting ICMP-based attacks. Hence it is required that in the future the mechanism will be able to find different parameters under ICMP surf attack and effectively detects and prevents the attack.

## DNS Amplification Attack

Reflection-based DDoS attack is also known as a DNS amplification attack. In this attack, the attacker turns a mini request into a maximum amount of payload and points towards the network.

In this attack, the attacker directly attacks the DNS server by sending a DNS query using a spoofed IP address. Then DNS server sends many replies to the end-user or attacker and hence the legitimate user cannot get access to the DNS server as shown in figure 3.

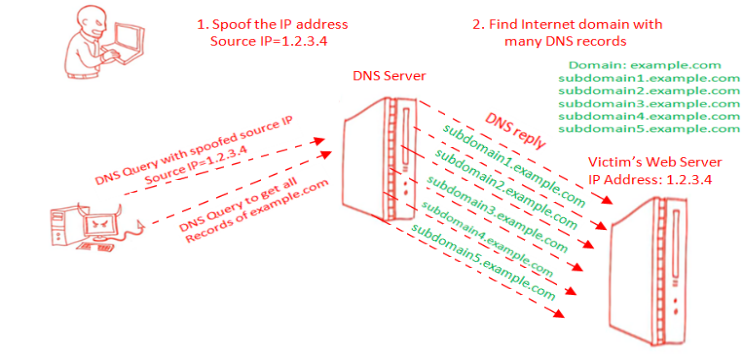


Fig. 3. DNS Amplification attack

D. C. MacFarland et. al. [11] measure and characterize the potential of attack which is associated with DNS server, with different countermeasures adoption. The strategy allows the poorly provisioned group to mitigate massive DNS amplification attacks by considering negligible performance overheads. As existing methods provide effective mechanisms but it has a minor performance overhead. To remove performance overhead it is necessary to do future work which provides a high-performance rate.

Also, the existing method flexible flow (sFlow) [27] is used to detect DNS amplification attacks on the emulated network and it only focuses on detecting malicious DNS responses. Further refinement in this technique will focus on detecting and preventing DNS amplification with the authentic dataset, which involves some aspects and measurement of accuracy, recall, precision, false positive, and false negative.

## Collision Attack

Collision is a type of DDoS attack which occurs when more than one node of a partially duplex communication mode network tries to transmit at a similar time.

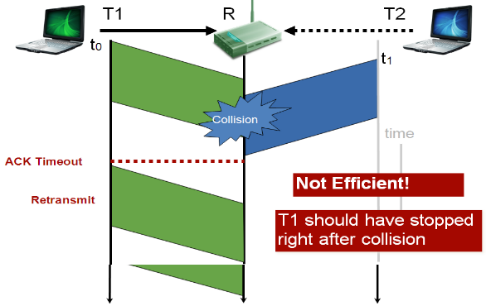


Fig. 4. Collision attack

A collision attack occurs when two users try to access resources at the same time as shown in figure 4.

S. Sen, R. Choudhary, and S. Nelakuditi [13] provided collision notifications for detecting collision-based DDoS attacks. In CSMA/ CN, the receiver customs physical layer information for detecting collision attacks. Collision notification contains a unique signature transmitted on a similar medium as data. But CSMA/CN only focuses on the wireless network.

## Jamming Attack

The jamming attack is a subset of DDoS attacks in which the attacker prevents other nodes to use the channel.

****

**(A)**

****

**(B)**

Fig. 5. Jamming attack

In normal communication, the sender sends a request and the receiver gives a response to that request then the communication is successful, as shown in figure 5(A). But, in jamming attacker can jam the intermediate device or router so that the jamming device blocks the signal, and hence receiver does not get any reply from the sender as shown in 5(B).

JAMMY algorithm [25] is available for jamming attack detection and prevention. In this algorithm, authors use the different methods for finding a secure slot for communication then it will use a slot acquisition algorithm. After the acquisition of the appropriate slot node will join for communication in WSN. The JAMMY attack only focuses on limited channel WSNs. The existing method threshold-based jamming countermeasure (TJC) [16] for jamming attack detection and prevention provides low accuracy and is only appropriate for detecting and preventing collision attacks. So, future research will concentrate on high accuracy and finding a more efficient method for detecting and preventing all kinds of jamming attacks.

## Tampering Attack

A tampering attack is a web-based attack in which some parameters of a form field or URL (Uniform Resource Locator) are changed by an attacker without the permission of a valid user.

In a URL tampering attack, an attacker may be a normal user where he can log in to his account, and just by changing the parameter of URL, he can access the other user account without permission as shown in figure 6.



Fig. 6. Explanation: Tampering attack

TamperProof [17] is online protection organized in a reliable environment among the server and client and needs no knowledge of or access to, the server-side codebase, creating it active for legacy and new applications.

In the Existing system study, the Tamper-aware authentication framework [26] is designed for WSN which is used to ensure authentication for sensor nodes and mitigation of tampering attacks. This framework provides an energy-efficient mechanism for nodes authentication at a low cost and also recovers nodes from tampering before major harm.

TamperProof and Tamper-aware authentication framework are only used to detect URL tampering. Both these techniques are unable to find the effect of parameter tampering.

1. Traditional Approaches Details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sr. No.** | **Method** | **Parameter** | **Attacks Covered** | **Efficiency** |
| 1. | FireCol: Collaborative Protection Network [6] | Compute and update the analyzed rule bandwidth | Flooding attack | TPR (true positive rate)>0.7 |
| 2. | Adaptive Thresholding Method [24] | Check adaptive threshold value, Check for packet protocol | TCP SYN Flood | CPU load valued  -during attack 96-100  -before attack 7-13 |
| 3. | Distributive defence approach (DDA) [10] | Captured packets (ICMP echo request), Packet analysis using Wireshark | Ping & ICMP smurf attack | processing time, the buffer size is less |
| 4. | BW based DDoS defense mech. [12] | The bandwidth available, attack size | DNS Amplification | Attack detection rate is >90% |
| 5. | Flexible Flow (sFlow) [27] | Check packet header predefined flow values to see whether traffic originated from DNS servers | DNS Amplification | 100% Attack detection rate |
| 6. | CSMA/ CN [13] | Collision notification, Packet Resumption, and Acknowledgment | Collision attack | Collision probability 0.1 |
| 7. | Stochastic Collision Distinguisher for masking Gaussian noise with EM approach[14] | -a compare two variants of collision-correlation power analysis  -average value of the leakage | collision attacks | (very) low SNR |
| 8. | Anti-jamming strategy [15] | Coordinated mode related Worst-case delay, Optimal load, and traffic load | jamming | Delay<0.9 |
| 9. | TamperProof [17] | Analyze request, analyze user, the processing time | Tampering | Incurred at most 4.8% overhead in round trip times |
| 10. | Tamper-aware authentication framework for WSN [26] | Hash function selection, Energy-efficiency analysis | Tampering | Efficiency >90% |

# Tree-Based Approaches

There are different tree-based approaches are available to analyze DDoS attacks as follows-

## Enhanced Very Fast Decision Tree (EVFDT)

EVFDT [19] is used for DDoS attack detection cloud-assisted WBAN (wireless body area networks). EVDFT efficiently detect DDoS attack by using the adaptive tie-breaking approach with node splitting threshold. Also, the lightweight iterative pruning method is used for resolving the expansion of tree size under extreme noise. EVDFT provides high accuracy in detection by lower false alarms.

The proposed system provides two phases. The first phase shows the detection system architecture for a DDoS attack. In which data collection is used for capturing incoming streams for preprocessing and feature extraction. In the initial stage of processing data is divided into a number of packets for feature extraction. Real-time packets are distinguished from network traffic for defining quality of service, which is help for attack classification.

In the second phase, EVFDT works like a decision tree for classifying malicious behaviors of traffic.

But the limitation of EVDFT is not suitable for a real WBAN testbed for performance evaluation.

## Attack Tree-based Intrusion Detection System (ATIDS)

ATIDS [20] is used as an intrusion detection system-based attack tree, introduced for the detection of multistep attacks. ATIDS contain aggregation (metrics value computations) and attack tree-based algorithm (ADtT) for achieving quality of delectability, detection uncertainty assessment, and providing tree framework. But the drawback of ATIDS is it is not able to generate low-level alerts from different intrusions.

## Augmented Attack Tree (AAT)

The author proposed a methodology that contains a packer sniffer for filtering network traffic. Sniffer output is forwarded to Packet Header Information DB (PHIDB) for storing detailed information. PHIDB provides data for AAT analyzer for detecting malicious traffic. AAT [21] is used for detecting three types of flooding-based attacks i.e. UDP flood, SYN flood, and ICMP flood.

## Attribute Tree (AT)

In [22] authors provide a defense system that contains 2 main phases as training (exercise) phase and the detection phase. The training phase is a preprocessor for the detection phase. Attack traffic packets and normal traffic packets are transmitted first to the packet Elicitor for generating attributes. Then attributes are given to the attribute tree populator for finding tree attributes by differentiating attack traffic from normal traffic using a traffic classifier.

## Change Aggregation Tree (CAT)

CAT [23] is used to detect DDoS attacks on DETER testbed. Attacks with packet size 128 bytes are detected by CAT like UDP flood, ICMP flood, TCP Syn flood, etc. Real-time anomaly-based detection is provided by CAT on the router. But the drawback of CAT is only suitable for up to 180 nodes. When we apply CAT to more than 180 nodes then the result is not as per expectation. CAT working is unsuccessful for in excess of 180 nodes. CAT provides a 98 % detection rate and less than 1% false alarm.

## Lightweight Decision-Tree Algorithm

C4.5 is used to detect different types of DDoS flooding attacks. The lightweight decision tree model is based on the C4.5 algorithm **[28]** for network monitoring uses feature selection for the detection of DDoS attacks which is deployable on different network devices like routers and switches over port mirroring techniques. In this, various monitoring or examining nodes can be allocated to various network parts. Lightweight decision tree algorithms provide subsequent mitigation and additional monitoring to different strategic network fundamentals. The main advantage of this algorithm is if any node in the network fails then also other nodes are working effectively.

In the future, the system will focus on higher line rate and full network traffic which improve the system efficiency to monitor nodes distributed across the 381 networks.

1. Tree-based Approaches Details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sr. No.** | **Tree Specification** | **Parameter** | **Attacks Covered** | **Efficiency** |
| 1. | Adaptive tie-breaking threshold,  lightweight iterative pruning [19]. | Tree size, memory, classification accuracy, and time | DDoS attack on the network  Traffic | classification accuracy of about 96.5% with 0% noise |
| 2. | Attack Tree-based IDS monitors N/W  [20] | Traffic analysis on edge devices | -ICMP Redirect  -Smurf Attack | 100% detection rate and 0% false rate |
| 3. | Change Aggregation Tree (CAT) is used to find DDoS attacks on the DETER testbed [23]. | Packet Size | -TCP SYN /UDP/ICMP flooding | On DETER testbed a 98%detection rate with less than 1% false alarms |
| 4. | Lightweight decision tree (DT) model [28] | Packet rate | Flooding based attack | Detection accuracy of over 99.9% |

# Proposed Methodology: Network Analysis Tree (NAT)

Distributed Denial of Service (DDoS) attacks are not only affected the quality of service but also the consumption of resources. To overcome system deficiencies, it would be better to use a tree-based approach because it would do useful work for the detection, prevention, and analysis of DDOS attacks detected in the system. Tree-based approach to DDoS attacks detection is as shown in Figure 7, which works step by step manner. When a web application is infected by some malicious activity and stops its work, the above method will work efficiently to find the effect of the attack. Based on the attack effect, active components at that time will be detected from the infected web. An active component includes different standards, tree-based methods work to identify which standard is active during the attack. And then the actual cause of the attack will be investigated by detecting the responsible attributes of the attack. Multiple attacks can be analyzed on a distributed system using a tree-based system.

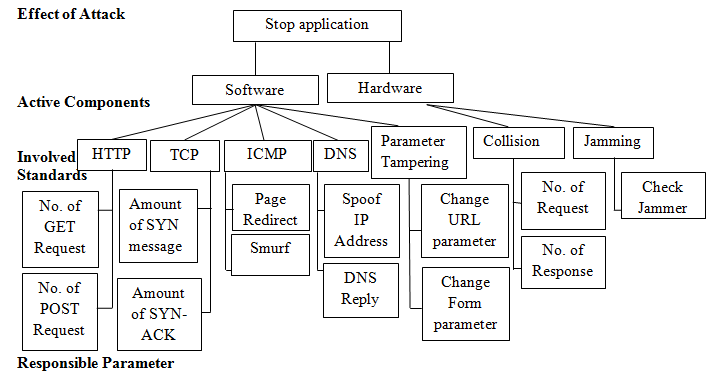


Fig. 7: Network Analysis Tree approach

# Conclusion

Distributed applications are designed to provide comfort to users. Along with the comfort, they provide some side effects such as different vulnerabilities, attacks, and threats that break the confidentiality of user information. It is a very critical task to preserve the privacy of data in a distributed system. Some attacks on a distributed system, such as DDoS not only affect the working of a system but also affect all connected systems in the network. There are multiple prevention techniques available to prevent DDoS attacks, but they do not guarantee to remove all the different causes of this attack efficiently. This paper introduced a survey of different traditional and tree-based mechanisms to detect and prevent multiple types of DDoS attacks such as Flooding attacks (TCP Syn flood), ICMP-based attacks, Amplification attacks, Collision, Jamming, and Tampering. This paper gives details of different methods used in traditional and tree-based approaches for the analysis of DDoS attacks.

In the future, the authors will work on the proposed method NAT mentioned in this paper for developing a system that will detect and prevent different types of DDoS attacks.

##### References

1. P. Fremantle and P. Scott, “A security survey of middleware for an Internet of Things,” *Peerj CC-BY 4.0 Open Access*, Aug 2015.
2. Q. Jing et al., “Security of the Internet of Things: perspectives and challenges,” *Springer Wireless Netw* DOI 10.1007/s11276-014-0761-7, 2014.
3. S. Alam `and D. De, “Analysis of Security Threats in Wireless Sensor Network,” *International Journal of Wireless & Mobile Networks (IJWMN)*, Vol. 6, No. 2, April 2014.
4. Idris et. al., “HTTP Flood Mitigation Using Gateway Inspection and Second Chance Approach Analysis”, *International Journal of Cyber-Security and Digital Forensics (IJCSDF),* *The Society of Digital Information and Wireless Communications (SDIWC),* Vol. 6, No. 1, Jan. 2017, pp. 14-22.
5. S. T. Zargar, J. Joshi, D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks", IEEE Commun. Surveys & Tutorials, vol. 15, no. 4, pp. 2046-69, Feb. 2013.
6. J. Francois, I. Aib, and R. Boutaba, “FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks”, *IEEE/ACM Transactions on Networking, IEEE/ACM*, Sept. 2012, 20 (6), pp.1828-1841.
7. S.H.C. Haris., et. al., "TCP SYN flood detection based on payload analysis", Proc. of 2010 IEEE Student Conference on Research and Development (SCOReD 2010), Putrajaya, Malaysia, Dec 2010, pp. 149-153
8. Myers, Robbie. “Attacks on TCP/IP Protocols.” Last accessed Jan 4, 2016.http://www.utc.edu/center-information-security-assurance/pdfs/course-paper-5620-attacktcpip.pdf.
9. Daehee Jang et.al., “ATRA: Address Translation Redirection Attack against Hardware-based External Monitors”, ACM, Scottsdale, Arizona, USA, CCS’14, November 3–7, 2014.
10. V. K. Yadav et. al., “DDA: An Approach to Handle DDoS (Ping Flood) Attack”,in*Proc. of International Conference on ICT for Sustainable Development, Advances in Intelligent Systems and Computing, Springer, Singapore*, Vol.10, Issue No. 2, Sept. 2016.
11. D. C. MacFarland et. al., “Characterizing Optimal DNS Amplification Attacks and Effective Mitigation”, *Springer*, Vol. 8, No. 2, Mar. 2015.
12. M. Geva, A. Herzberg, and Y. Gev, “Bandwidth Distributed Denial of Service: Attacks and Defenses”, Article in IEEE Security and Privacy Magazine, Jan. 2013.
13. S. Sen, R. Choudhary and S. Nelakuditi, “CSMA/CN: Carrier Sense Multiple Access with Collision Notification”, *proc. In MobiCom’10, ACM*, Sept. 2010.
14. Nicolas Bruneau et. Al., “Stochastic Collision Attack”, *International IEEE Transactions On Information Forensics And Security,* Vol. 12, No. 9, Sept. 2017.
15. Lu, Zhuo, W. Wang, and C. Wang. "Camouflage Traffic: Minimizing Message Delay for Smart Grid Applications under Jamming." *IEEE Transactions on Dependable & Secure Computing*, Vol. 12, No.1, Feb. 2015, pp. 31-44.
16. Sachin D. Babar, Neeli R. Prasad, and Ramjee Prasad, “Activity Modelling and Countermeasures on Jamming Attack”, Journal of Cyber Security and Mobility, River Publisher, Vol. 2, No. 1, Apr. 2013.
17. Nazari Skrupsky et. al., “TamperProof: A Server-Agnostic Defense for parameter Tampering Attacks on Web Applications”, Proc. of the Third ACM Conference on Data and Application Security and Privacy (CODASPY’13), San Antonio, Texas, USA, Vol. 7, No. 2, Feb. 18–20, 2013.
18. M. N. Aman et. al., “Detecting data tampering attacks in synchrophasor network using time hopping”, *2016 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), Ljubljana*, 2016, pp. 1-6.
19. R. Latif et al., “EVFDT: An Enhanced Very Fast Decision Tree Algorithm for Detecting Distributed Denial of Service Attack in Cloud-Assisted Wireless Body Area Network”, *Pub. Hindawi Corporation, Mobile Information Systems (HCMIS)*, Vol. 2015, Issue 5, Aug. 2015.
20. J. Wang., “Advanced Attack Tree-Based Intrusion Detection”, *Pub. In Lough borough University Institutional Repository (LUIR),* Leicestershire, UK,Feb 2012.
21. J. Wang et. al., “Augmented Attack Tree Modeling of Distributed Denial of Services and Tree-Based Attack Detection Method”, *Proc. in 10th IEEE International Conference on Computer and Information Technology (CIT 2010)*, Oct. 2010.
22. P. Jayashree and Dr. K. S. Easwarakumar, “An Effective Defense Cum Prevention Of DDoS Attacks In Active Networks Using Attribute Trees”, *Ubiquitous Computing and Communication Journal (UCCJ)*, Jun. 2008.
23. Yu. Chen et. al., “Distributed Change-Point Detection of DDoS Attacks: Experimen-tal Results on DETER Testbed”, *Pres. in DETER Community Workshop on Cyber Security Experimentation and Test (DCWCSET),* Jul. 2007.
24. Ramkumar B., Subbulakshmi, T, “Tcp Syn Flood Attack Detection and Prevention System using Adaptive Thresholding Method”, Pres. in ITM Web of Conferences, Vol. 37, No. 10 Jan. 2021.
25. M. Tiloca, D. De Guglielmo, G. Dini, G. Anastasi, and S. K. Das, “Jammy: A distributed and dynamic solution to selective jamming attack in tdma wsns,” *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 4, pp. 392–405, 2017.
26. H. Mensah, K. Boateng, and J. Gadze, “Tamper-aware authentication framework forwireless sensor networks”, *IET Wireless Sensor Systems,* Vol. 7 Iss. 3, pp. 73-81, Jan. 2017.
27. A. Atan, N. Noor, M. Ismail, “DNS Amplification Attack Detection via Flexible Flow (sFlow)”, *Sindh University Research Journal (Science Series),* Vol. 48, Apr. 2016.
28. G. Lucky, F. Jijunju and A. Marshall, “ A Lightweight Decision-Tree Algorithm for detecting DDoS flooding attacks”, *Pres. in 2020 IEEE 20th International Conference on Software Quality, Reliability and Security Companion,* Vol.10, Jun. 2020.