ANALYSING DUPES - ALGORITHM TO DETECT AND PREVENT DOS ATTACK

Er. Sandeep Singh Khehra[1], Ms.Rimpi Rani[2]
[1,2]Guru Kashi University, Talwandi Sabo

Abstract

In the last three decades, the number of people using the Internet has exploded, and e-commerce sites, search engines, and online banking have all become indispensable components of today's world. The key issues that plague the Internet are application security and availability. DoS attacks are a serious attack when it comes to availability. It prevents the intended user from accessing resources or services. The DoS attack has extremely hazardous consequences. A denial of service attack occurs when attackers send a high number of spam or copy solicitations to a server, delivering it inaccessible to other people or real clients. The Computer Emergency Response Team arranges refusal of administration assaults into three sorts. The main class was worried about asset usage, like organization data transfer capacity or CPU utilisation.. In this paper, the DUPES algorithm is introduced and developed to improve the security of MAC spoof DoS assaults. To protect against start frame and logoff frame DoS attacks, four alternative approaches were established. To test DUPES' performance, the number of clients is increased. When the number of clients grows, the most dangerous attack is the start frame attack. However, the packet delivery ratio, throughput, and packet drop measurement all show a decrease in performance.

Keywords: Dupes, Algorithm, Detect, Prevent, Dos Attack, Etc

1. INTRODUCTION

In the last three decades, the number of people using the Internet has exploded, and e-commerce sites, search engines, and online banking have all become indispensable components of today's world. The key issues that plague the Internet are application security and availability. DoS attacks are a serious attack when it comes to availability. It prevents the intended user from accessing resources or services. The DoS attack has extremely hazardous consequences. Small and mid-sized businesses, as well as government websites, have recently been subjected to denial-of-service attacks, which have had a huge social impact. DoS have become a problem for software and financial organisations. Dos attacks have hit Microsoft, eBay, Amazon, Buy.com, Capital One Bank, SunTrust Bank, and other financial institutions online artificial jewellery sites, for example. According to a recent poll, attackers in the United States targeted Capital One and SunTrust banks on October 8, 2012. An eight-hour attack was launched on these sites. As a result, the Capital One website is frequently unavailable for up to eight hours at a time. On July 3, 2013, a DoS attack was launched against an online artificial jewellery store.

1.1 Examining accounting models for detecting duplicate web service requests

A denial of service attack occurs when attackers send a high number of spam or copy solicitations to a server, delivering it inaccessible to other people or genuine clients. The Computer Emergency Response Team orders disavowal of administration assaults into three sorts. The main classification was worried about asset usage, like organization data transmission or CPU use. The subsequent classification incorporates the actual obliteration or control of organization parts. The third classification incorporates the cancellation or change of setup the executives. The primary sort of assault is the least difficult for aggressors to complete with negligible exertion. This assault will be helped out either through convention abuse (TCP SYN flood: sending just TCP SYN questions without answering TCP/ACK, or through a blend of the two). UDP flooding is the method involved with sending countless UDP bundles to a server's port. Smurf assault: broadcasting a ping demand with the casualty's source address, and the reaction will arrive at the casualty from all machines. Ping flood: sending an enormous number of pings ping demands) or through countless app downloads. A DoS attack on a wireless infrastructure network is more likely. The number of user's increases as the wireless network is set up quickly and easily.

As the number of users grows, so does the number of security issues. One of the most serious security issues is a denial-of-service attack. 802.11i, WiFi Protected Access (WPA), 802.11b, 802.1x, 802.1w, 802.11, and Wired Equivalent Privacy (WEP) are some of the security protocols that exist and are applied over WLAN to detect DoS attacks. WEP is the first attempt at a DoS attack to degrade security. WEP's RC4 algorithm contains a number of severe flaws. The solution to this problem is to obtain enhanced network security via rapid requisition. IEEE 802.11i was finally ratified in 2004, and it is the most crucial phase of wireless security. Despite the fact that WEP has numerous security weaknesses, many businesses continue to use it due to the early adoption of wireless technologies.

2. REVIEW OF THE LITERATURE

Ahmed Al-Ani, Mohammed Anbar, Selvakumar Manickam, (2018) Duplicate Address Detection (DAD) is a key operation of Web Protocol variant 6. (IPv6). It permits all hubs on a similar connection to impart and join to the organization with a solitary IP address. Father, then again, is inclined to security defects. To guarantee that the conditional IP address is conveyed to all current hosts by means of a NS message, the DAD method utilizes two Neighbor Discovery (ND) messages, specifically Neighbor Solicitation (NS) and Neighbor Advertisement (NA). Therefore, DAD permits any pernicious hub on a similar connection to get the NS message and afterward send a farce answer to forestall the objective hub's location arrangement, bringing about a DoS assault. The reason for this study is to safeguard the DAD strategy by camouflaging the speculative IP address during the interaction, keeping an antagonistic hub from intruding with the objective hub's IP setup. The proposed DAD-match security procedure grows the SHA-3 hash work by presenting another choice called DADmatch, which keeps up with the hash worth of a provisional IP address and connects it to NS and NA messages, bringing about NS-match and NA-match messages. We accept that the DAD-match method will give less difficult lightweight security and will totally deny DoS assaults during DAD activities in an IPv6 connect neighborhood organization.

Bharathi Balasubramanian & Gm Manivasagam & R. Gunasundari (2018) IPv6 is the most recent version of the Internet Protocol (IP), which assigns a unique identity to machines on networks and addresses them while also routing traffic across the Internet. This protocol was designed to address the addressing issues that plagued the previous version. It also includes new services and features, such as host auto-configuration. This capability allows the host to configure itself without the need for any other tools. Some security vulnerabilities have arisen as a result of IPv6's architectural features. The most serious is a DAD (Duplicate Address Detection) denial of service attack, which prevents the auto-configuration feature from working. To solve these issues, techniques such as SeND (Secure Neighbor Discovery) and SSAS have been developed (Simple Secure Addressing Scheme) have been created. The complexity of these processes, as well as the decrease of their effectiveness, is side consequences. This study examines the mechanisms' moral flaws and suggests a new approach, Safe Addressing Scheme (SAS), to overcome them.

Shafiq Rehman and Selvakumar Manickam (2016) Most IPv6 security challenges are the same as IPv4; but, IPv6 has its own unique design characteristics that have extra implications for system and network security, as well as policy and process implications. Address autoconfiguration is a significant element of the IPv6 protocol stack that allows hosts to generate their own addresses based on information from other hosts as well as information from router advertisements. DAD (Duplicate Address Detection) is a procedure used in address autoconfiguration to see if the addresses generated have already been specified. Nonetheless, the DAD process's design makes it vulnerable to DoS attacks, leaving hosts unconfigured. Any host, for example, can respond to Neighbor Solicitations (NS) for a temporary address, prompting the other host to treat it as a duplicate and finally reject it. Various systems, such as SeND and SAVI, have been devised to combat such attacks; however these strategies have proven ineffective because DoS attacks are still possible. As a result, a new technique is required to better prevent DoS assaults on the DAD process. We provide a detailed design and development of a novel mechanism that can overcome the shortcomings of current preventative strategies in this research.

Shafiq Rehman and Selvakumar Manickam (2015) IPv6 (Internet Protocol version 6) is quickly becoming the de facto IP communication standard around the world. Nonetheless, the nature of IPv6's protocol design has given rise to a variety of security vulnerabilities. One of the security flaws involves exploiting a weakness in the implementation of the Duplicate Address Detection (DAD) method, which can lead to Denial of Service (DoS) attacks. Such assaults have the potential to render the entire network inoperable. To detect this attack, several measures have been implemented. These systems did, however, have some flaws. We present a novel mechanism in this research that employs a rule-based approach to overcome the drawbacks of previous mechanisms while also improving accuracy and performance.

3. OBJECTIVES

- ✓ To examining accounting models for detecting duplicate web service requests.
- ✓ To analyze attack during and after applying ThreV.

4. RESEARCH METHODOLOGY

4.1 Detect and prevent DoS attack Methodology

Various security approaches have been implemented to prevent DoS attacks; nevertheless, there is currently no powerful answer for recognizing and forestalling MAC parody DoS assaults, which must be addressed. Multiple strategies are provided in this thesis to solve the shortcomings of existing solutions. This paper provides a useful a tool for preventing DoS assaults in a network infrastructure, which is created by combining various detection and prevention strategies to create a safe network. DUPES is a suggested detection technique that combines four algorithms: ThreV (Threshold Value), ANM (Alternative Numbering Mechanism), ThreVANM (ThresholdValue and Alternative Numbering Mechanism), and TPatLetEn (ThresholdValue and Alternative Numbering Scheme) (Traffic Pattern Filtering and Letter Envelop Protocol).

- ✓ **DUPES**

ThreV, ANM, ThreVANM, and TPatLetEn are four detection algorithms that are combined in DUPES A DUPE. It keeps an Intruder Table (InT) with intruders' MAC addresses and a The MAC addresses of WLAN users are stored in a Basic Identity Check (BIC) table.

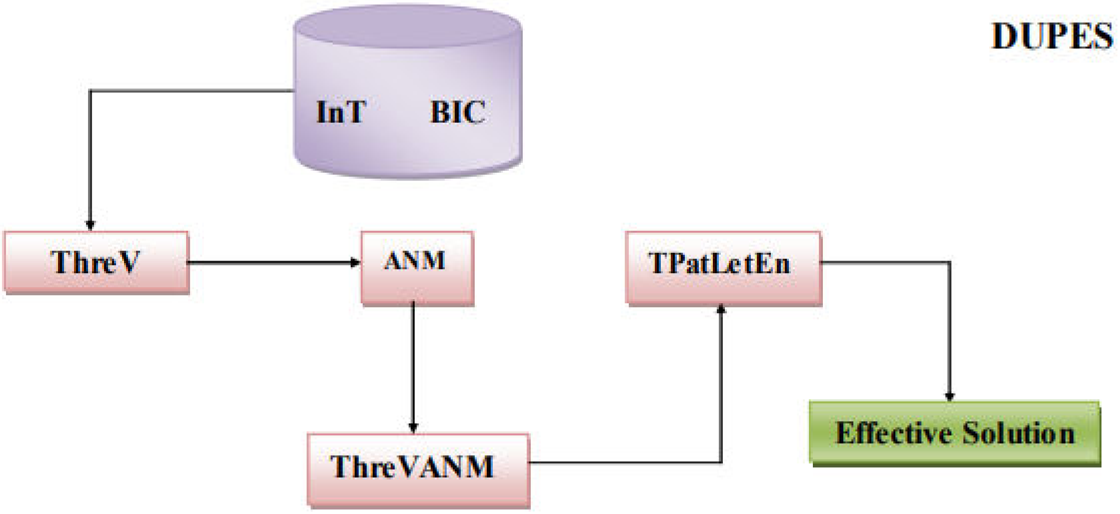


Figure 1: Operations of DUPES

- ✓ **Threshold Value (ThreV):**

When AP receives a login request from a client, it sends a message in response In this scenario, the threshold value is set at 4 milliseconds. The AP must respond to the client in less than 4 milliseconds. If the AP receives many requests in a short period of time, these requests will be regarded spoofing frames (SF). If a client obtains a response message from the AP before the threshold stage, the message is designated as a Spoofed Frame response.

4.2 Threshold Value (ThreV)

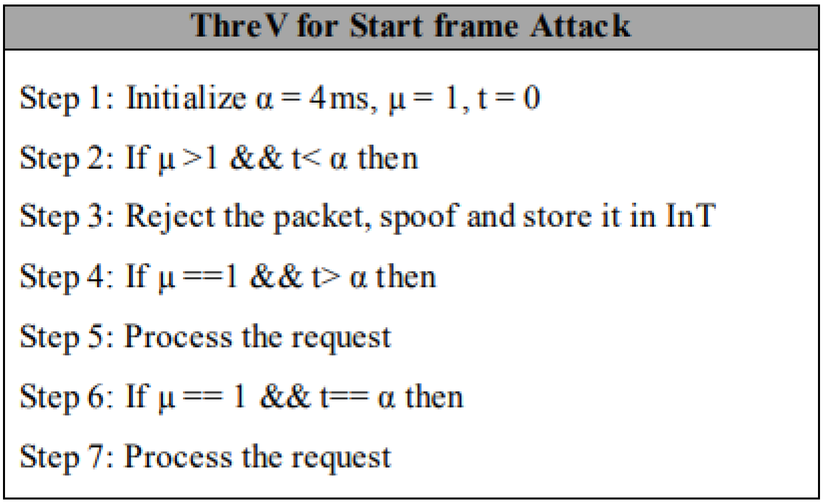
When AP gets a client login request, it sends a response message. The threshold in this case is set at 4 milliseconds. The AP must respond to the client in less than 4 milliseconds. If the AP receives more than one request in a certain period of time, these requests will be regarded spoofing frames (SF). If a client receives a response message from the AP prior to the threshold stage, the message is reserved as a Spoofed Frame response.

5. DISCUSSION AND RESULT

5.1 Attack Experimentation in ThreV

Experimentation is emulated on NS2 with three nodes: client, intruder, and access point. To analyse the performance of the ThreV algorithm, start and logoff frames through AP/Client are used. The usefulness The effectiveness of the suggested technique is demonstrated by analysing network performance in a simulated attack scenario. To validate the algorithm's performance, values for packet delivery ratio, control overhead, normalised routing overhead, latency, throughput, and packet drop are recorded.

Algorithm: ThreV for start frame attack over AP and Client



```
ThreV for Start frame Attack
Step 1: Initialize $\alpha = 4ms, \mu = 1, t = 0$
Step 2: If $\mu > 1$ && $t < \alpha$ then
Step 3: Reject the packet, spoof and store it in InT
Step 4: If $\mu == 1$ && $t > \alpha$ then
Step 5: Process the request
Step 6: If $\mu == 1$ && $t == \alpha$ then
Step 7: Process the request
```

5.2 Start Frame and Logoff Frame Attack over AP/Client

The start frame attack is launched in the WLAN, and the network's performance is monitored throughout the attack. After deploying ThreV, the network performance is measured, and the findings are promising.

Table 1 Result of start frame attack during and after applying ThreV

Parameter	**Over AP**		**Over Client**	
	Attack Scenario	**ThreV**	**Attack Scenario**	**ThreV**
Packet delivery ratio	61.52	97.55	73.02	93.74

- ✓ **Packet Delivery Ratio**

In start frame attack experiments, the packet delivery ratio is higher in attack over AP than in attack over client. The initial frame over AP is the most lethal when compared to a client-attack attack. When ThreV was used in a start frame attack over AP, the packet delivery ratio increased substantially. In the event of a logoff frame assault over client /AP, the result obtained via ThreV is the inverse of the start frame attack. As illustrated in Figure 2, ThreV's performance in The start frame assault over AP exceeds the start frame assault over the client. The start frame attack on the AP/client packet delivery ratio and the logoff frame attack on the AP/client packet delivery ratio have both been seen. increased considerably.

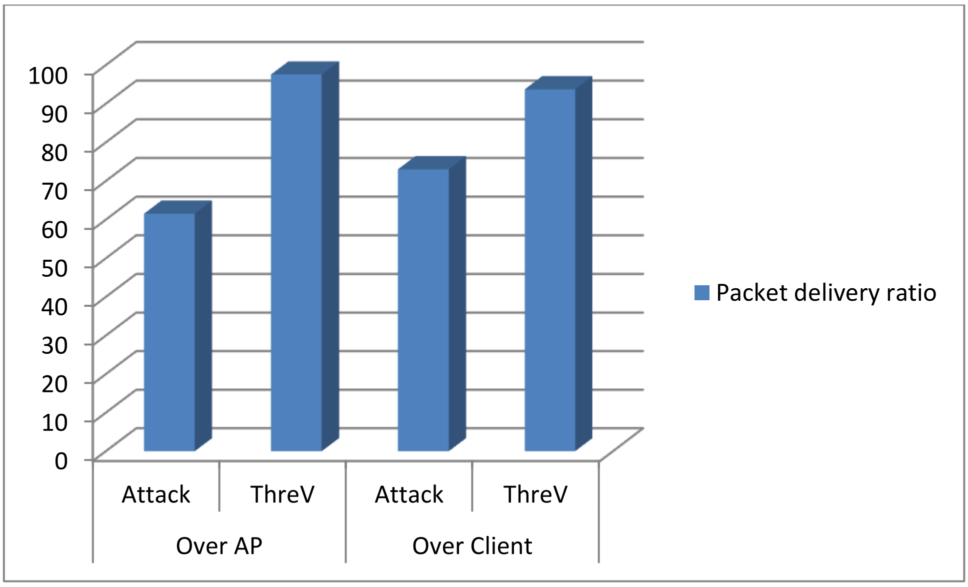


Figure 2: Result of start frame attack during and after applying ThreV Packet Delivery Ratio

In the start frame attack, 81 CBR packets were seized, while in the logoff frame attack, 90 CBR packets were taken. ThreV's performance is evaluated as the suggested technique detects and avoids DoS attacks. Table 1 shows the Below are the experimental findings of the attack before and after applying ThreV in the start frame attack. The metrics packet delivery ratio, control overhead, Normalized routing overhead, latency, throughput, and packet drop are used to assess ThreV's performance.. ThreV is a suggested algorithm. is discussed, as well as its impact on the AP/Client attack's Start frame and Logoff frame attacks. ThreV's framework was presented, as well as the testing of attacks and remedies. Finally, the ThreV results were analysed using six parameters in an attack scenario. The suggested ThreV algorithm has a substantially higher performance in terms of packet drop and delay time, according to the results. Throughput, packet delivery ratio, normalised routhing overhead, and control overhead all showed promising results.

6. CONCLUSION

In this paper, the DUPES algorithm is introduced and developed to improve the security of MAC spoof DoS assaults. To protect against start frame and logoff frame DoS attacks, four alternative approaches were established. To test DUPES' performance, the number of clients is increased. When the number of clients grows, the most dangerous attack is the start frame attack. However, the packet delivery ratio, throughput, and packet drop measurement all show a decrease in performance. DUPES have been proposed to improve security measures against infrastructure DoS attacks. Despite the enhanced efficiency, some security issues were discovered, including false positives, in which a normal user is mistaken for a hacker. When the qualifications for a genuine client are met, hackers are treated as legal clients in this scenario. To address this problem, a hybrid technique is developed that can efficiently detect and thwart DoS attacks.

REFERENCES

1. Al-Ani, Ahmed & Anbar, Mohammed & Manickam, Selvakumar & Al-Ani, Ayman. (2018). DAD-Match: Technique to Prevent DoS Attack on Duplicate Address Detection Process in IPv6 Link-local Network. Journal of Communications. 13. 317-324. 10.12720/jcm.13.6.317-324.

2. Balasubramanian, Bharathi & Gm, Manivasagam & R., Gunasundari. (2018). A-Novel-Approach-For-Preventing-Dos-Attack-In-Duplicate-Address-Detection-Of-IPV6.

3. Rehman, Shafiq & Manickam, Selvakumar. (2016). Novel Mechanism to Prevent Denial of Service (DoS) Attacks in IPv6 Duplicate Address Detection Process.

International Journal of Security and its Applications. Vol.10. pp. 143-154. 10.14257/ijsia.2016.10.4.15.

4. Rehman, Shafiq & Manickam, Selvakumar. (2015). Rule-Based Mechanism to Detect Denial of Service (DoS) Attacks on Duplicate Address Detection Process in IPv6 Link Local Communication. 10.1109/ICRITO.2015.7359243.

5. Wright, J, How 802.11w will improve wireless security, http://www. networkworld.com/columnists/2006/052906-wireless-security.html (Browsed on 04.10.2012).

6. Bicakci, Kemal, and Bulent Tavli, "Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks ", Computer Standards & Interfaces, Vol. 31(5), 931-941, 2009.

7. Bulbul, Halil Ibrahim, Ihsan Batmaz, and Mesut Ozel, "Wireless network security: Comparison of WEP (wired equivalent privacy) mechanism, WPA (wi-fi protected access) and RSN (robust security network) security protocols", In Proceedings of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop, ICST (Institute for Computer Sciences, SocialInformatics and Telecommunications Engineering), pp 1-6, 2008.

8. Sherif Khattab, "A Defense framework against Denial-of-Service in computer Networks", Doctoral Thesis, University of Pittsburgh, 2008.

9. Elleithy, K. M, Blagovic, D, Cheng, W, & Sideleau, P, "Denial of Service Attack Techniques: Analysis, Implementation and Comparison", Journal of Systemics, Cybernetics and Informatics, Vol. 3(1), 66-71, 2006.

10. Mitchell, Changhua He John C, "Security Analysis and Improvements for IEEE 802.11 i", In The 12th Annual Network and Distributed System Security Symposium (NDSS'05) Stanford University, Stanford, pp. 90-110. 2005.