Digital Innovations & Contemporary Research in SCIENCE, ENGINEERING & TECHNOLOGY
Vol. 12. No. 2, 2024 Series

Article Citation Format
Jimoh, H.O. & Ahmed, M.O. (2024): Analyzing Network Time Protocol (NTP) Based Amplification DDoS Attack and its Mitigation Techniques. Journal of Digital Innovations & Contemporary Research in Science, Engineering & Technology. Vol. 12, No. 2. Pp 17-24. www.isteams.net/digitaljournal. dx.doi.org/10.22624/AIMS/DIGITAL/V11N2P2x

Article Progress Time Stamps
Article Type: Research Article
Manuscript Received: 12st January, 2024
Review Type: Blind Peer
Final Acceptance:1 1th April, 2024

Analyzing Network Time Protocol (NTP) Based Amplification DDoS Attack and its Mitigation Techniques

[1]Jimoh, Hammed. O. & [2]Ahmed, Mubarak .O ·
[1] Department of Cybersecurity
The Federal Polytechnic, Offa, Kwara State, Nigeria
[2] Cisco Systems, Nigeria, Lagos, Nigeria.
E-mails: hamid.jimoh@gmail.com; mublamouchi@gmail.com

ABSTRACT

Network Time Protocol amplification attack is a form of distributed denial-of-service (DDoS) attack in which an attacker exploits or sends a request to a vulnerable NTP server by using their IP address to flood a targeted network or server with an overwhelming volume of User Datagram Protocol (UDP) traffic. In the past, the techniques that involved reflecting traffic off NTP servers to the victim, with the attacker hiding their identity by spoofing the source IP address were carried out using mainly Domain Name Server (DNS) servers but the use of vulnerable NTP servers as reflectors in DDoS attacks has gain lot of popularity since 2014, and this is as a result of the realization of high amplification scale that NTP servers can provide. This type of reflector attack maximized the use of the amplification factor of NTP servers to magnify the attack bandwidth, making it particularly disruptive and difficult to mitigate. Since NTP amplification is not a popularly known attack and there has not been much thorough research on it, this paper explores a holistic overview of NTP amplification attacks, how NTP is used for DDoS attacks, and the overall method that can be used to mitigate such attacks.

Keywords: Distributed Denial-of-Service (DDoS) attack, DNS servers, NTP servers

1. INTRODUCTION

Cyber attacks have become a prevalent issue in the global world and now becoming part of our everyday lives. Various critical infrastructures over the networks have been subjected to one form of attack or the other. Some of these attacks are extremely damaging and great threats to personal life or organization. A Network Time Protocol (NTP) based amplification DDoS attack is one of the most common and dangerous attacks perpetrated by threat actors to spoof into various networks and servers to cause severe damages, leading to service disruptions, downtime, and potential financial and reputational damage. Thus, it is imperative to understand the attack vector and modus operandi used by the adversaries and its possible mitigation techniques.

Generally, denial-of-service (DoS) attacks are one of the main security issues that have become visible in recent years. “When the frequency of Internet traffic to a source increases, it can cause the system to not function efficiently. Malicious attacks using thousands of packets can be used to shut down services on a server or use up bandwidth” [1]. This attack adopts a method of increasing the volume of network traffic and then occupying all the bandwidth to deny authorized users of accessing their network or system. In a DoS attack, a single system targets the victim system. However, a distributed denial-of-service (DDoS) attack is a malicious attack launched from multiple or numerous compromised devices, in an attempt to make an online service unavailable to users by temporarily interrupting or suspending the services of its hosting server. The group of compromised systems is called a botnet.

“When the attacker intends to perform a DDoS attack, the DDoS master is sent a command, telling it to notify the zombie computers to attack the victim” [2]. When a DDoS attack happens, it's usually a difficult issue to resolve because you can hardly differentiate between legitimate user traffic and malicious traffic. The features of DDoS attacks were keenly observed and since then, there have been increasing incidents of attacks exploiting the Network Time Protocol (NTP). A Network Time Protocol (NTP) is a networking protocol designed and used by a computer system connected to the internet for time synchronization. “DDoS attacks using NTP servers gained popularity in late 2013 and have been a factor in several major attacks in the first half of 2014” [3]. Since then, the root cause of these attacks and their effective techniques have been widely studied and recognized and have thus gained popularity. Although there has been widespread awareness on the internet on how this attack can be mitigated, till this moment, there are no tangible measures or techniques on how to tackle this issue.

This paper summarizes how NTP is used to amplify DDoS attacks, its modus operandi, and preventive measures to mitigate such attacks within an organization and internet service provider (ISP).

2. RELATED WORKS

NTP DDoS attacks were analyzed on a global scale by looking at the rise of NTP amplification attacks, how many amplifiers there are, and their amplification scale. The victims of the attacks were found by looking at the source port of the original attack packet. It was found that most of the victims were game-related, with victims including Minecraft, Runescape, and Microsoft Xbox Live. The most popular source port found was port 80/UDP, which they said may have been used to target games using this port or websites. When classifying the number of attacks that occurred throughout 15 weeks of monitoring several amplifiers, a simplification was used but classifying each unique targeted IP in a week-long sample as one attack. This simplification does not take account of attacks targeting network blocks or a single IP hosting multiple sites.[4]

Using Network Time Protocol (NTP) based Amplification for Distributed Denial of Service (DDoS) attack.
“An NTP amplification attack is a reflection-based volumetric distributed denial-of-service (DDoS) attack in which an attacker exploits a Network Time Protocol (NTP) server functionality to overwhelm a targeted network or server with an amplified amount of User Datagram Protocol (UDP) traffic, rendering the target and its surrounding infrastructure inaccessible to regular traffic” [5]. NTP amplification attacks include some key characteristics, some of which include; **reflection, amplification, and UDP protocol**. Reflection is one of the main characteristics because it is a method that requires reflecting traffic off the NTP servers to the victim. During this process, the attacker's identity is hidden by spoofing the source IP address.

Also, amplification as a characteristic occurs when attackers amplify the volume of data sent to the victim, thus, overwhelming their network. This is executed by exploiting commands that generate large responses from the NTP servers. Spoofing IP addresses is quite very easy with the use of user datagram protocol (UDP) because a handshake isn't required in UDP to establish connections before data transfer.

This makes UDP protocol a key characteristic in NTP amplification attacks. “One particularly damaging variant of the NTP attack uses the MONLIST command, supported in older NTP implementation, that returns the last 600 clients that an NTP server has talked to, hence resulting in responses with an amplification factor of 10-200x with just a single NTP server. Accordingly, large-scale attacks that simultaneously solicit thousands of NTP servers can produce incredible damages while requiring a very limited number of resources on the attacker’s side. For example, on February 10, 2014, about 1300 NTP servers on different networks were involved in an unprecedented cyber attack, where each server generated at peak hours approximately 90 Mb/s of traffic towards particular targets located on the Internet”.[6]

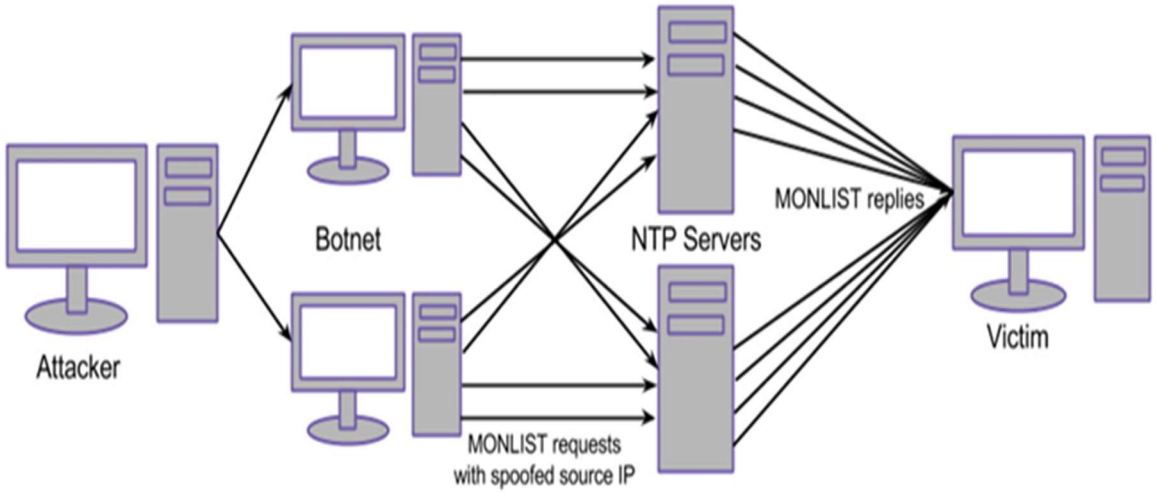

Figure 1: Distributed Denial of Service attack using NTP servers as reflectors [3]

From Figure 1 above, it can be observed that the attacker successfully executed the DDoS amplified attack by sending a UDP/123 MONLIST request with a specific spoofed source address of the intended victim of the attack to a vulnerable NTP server. In return, the server then forwarded the reply to the spoofed IP address (the victim) and it was then flooded with large packets.

Aside from the NTP amplification attack that occurred in February 2014 as stated above, the number of such attacks had considerably increased with one of these attacks reaching just below 400 Gbps. This was reported as one of the largest recorded attacks using NTP. “By April 2014, Arbor Networks released data that showed that 85% of DDoS attacks above 100 Gbps were using NTP amplification [7]. In early 2014 there were more than 430,000 vulnerable NTP servers” [7]. “However, by June 2014, this number decreased to around 17,647 vulnerable servers largely due to the application of patches and configuration changes by network administrators” [8]. “A report released by Arbor Networks in October 2014 showed that NTP amplification-based attacks are decreasing, compared to April’s data with a little over 50% of incidents over 100Gbps using this protocol” [9].

Analysis of How NTP-based Amplification DDoS Attack Work

A detailed description and corresponding examples of NTP amplification attacks have been discussed above. In this section, an analysis of the DDoS attack mechanism and how the source address of the UDP packets can be spoofed will be discussed here to give a better understanding of how the attack is propagated. Firstly, let's analyze how NTP amplification is prone to attacks because of its response to a packet with a spoofed source IP address. With this attack, this makes at least one of its in-built commands send a long reply to a short request, which makes it ideal as a DDoS tool. This will be briefly explained below.

DDoS attack by spoofing the source address of a UDP packet: The UDP (User Datagram Protocol) is widely used over the internet as it is "a simple transport protocol that extends the host-to-host delivery of packets of the underlying network into a process-to-process communication. Since many processes are running on a given host (e.g. multiple Internet browsers), UDP needs to add a level of demultiplexing, allowing multiple application processes on each host to share the network. Therefore, the only interesting issue in UDP is the form of address used to identify a process" [10]. Since UDP is a connectionless protocol, it is particularly vulnerable to source spoofing except extra precautions are put into consideration. If any of these precautions are not taken, the threat actors exploit this vulnerability and send a service request packet based on UDP with a forgotten address, i.e., the victim's, with a forged address to some server (springboard, reflector) thus, using the spoofed address of the target as the source address as shown in figure 2 below

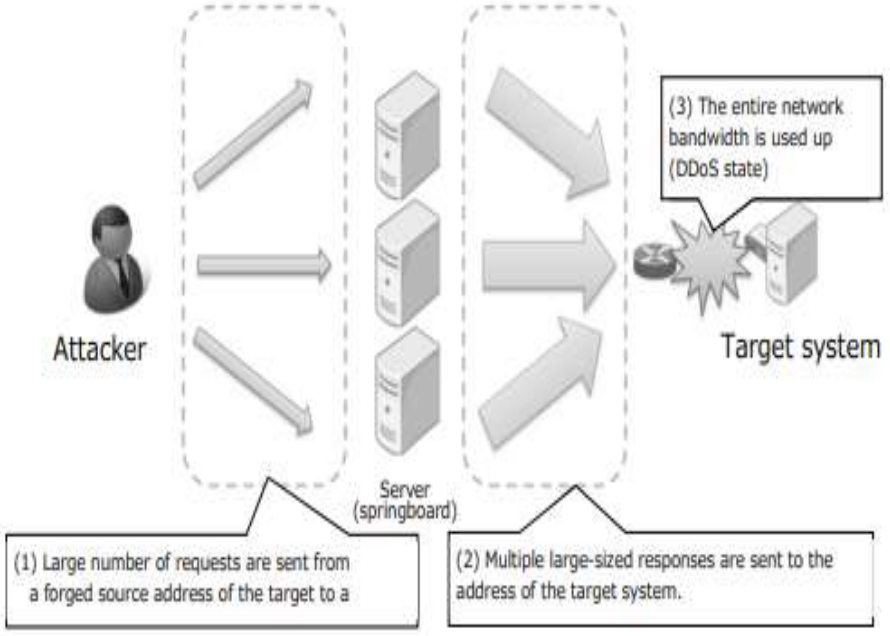

Figure 2: DDoS attack in which the source address of a UDP packet is spoofed [11]

From the above figure, the unsuspected target server replies and sends data to the victim almost immediately, because the source address has been forged. "In such cases, when a forged packet elicits a large, overwhelming response, it can cause a massive traffic load to hit the victim's network bandwidth. This is how the DDoS attack, in which the source address of a UDP packet (UDP-based Amplification Attacks) is spoofed, essentially functions". [11]

Our second analysis will be based on **time synchronization**. Time synchronization isn't only available in the network or server devices connected to the internet, but also in numerous devices like network scanners, network cameras, network printers, and other systems using NTP. This makes them a vulnerable and easier method for threat actors to pull off exploits and launch a full-scale attack as shown in Figure 3 below;

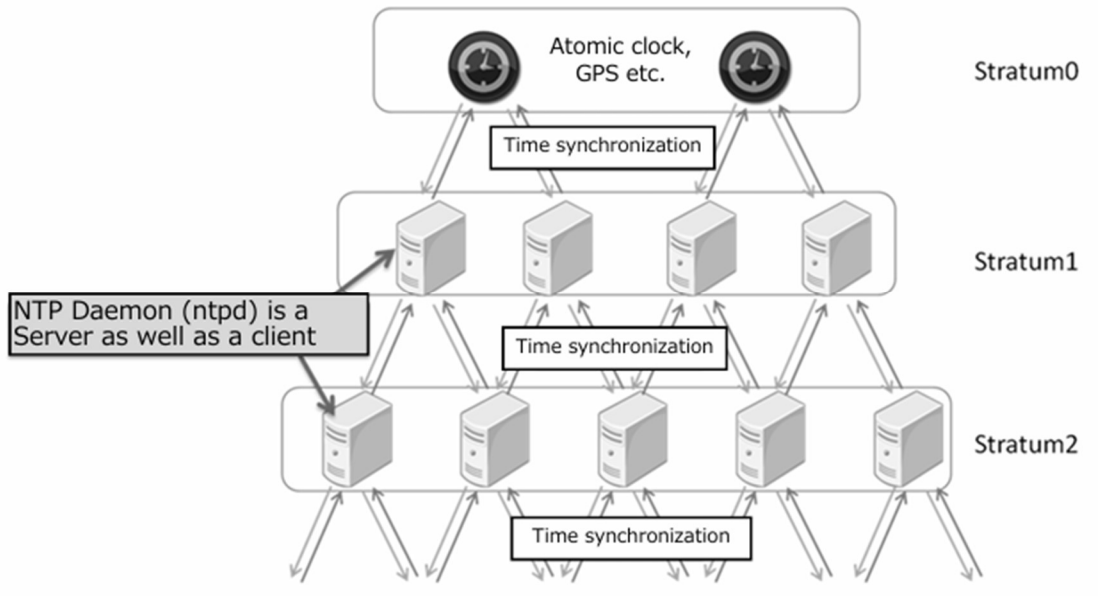

Figure 3: Hierarchal Configuration of NTP based on Time Synchronization [13]

The time synchronization attack is closely related to the configuration based on the NTP specification. "NTP is a hierarchal protocol that uses a high-precision NTP server called Stratum0 as its apex (as shown in Figure 3 above). What is more, the NTP daemon acts as a client for NTP services running on other devices, it also operates as a Server providing NTP services to other devices simultaneously. Therefore, unless appropriate restrictions are set for each NTP daemon, the services may eventually be provided to an unspecified number of devices. Amongst these, it is the **monlist** command that is exploited in a DDoS attack and is a service that does not need to be provided to most devices. However, due to factors such as an unusual configuration, lack of knowledge on the system administrators' part or an incorrect default configuration, and so on, there are still a large number of devices present that are vulnerable to these attacks" [13].

3. MITIGATING DDOS NTP AMPLIFIED ATTACK

"One of the biggest problems of cyber-defense, in general, is represented by anonymity and the resulting non-imputability that cyberspace can offer to the authors of a cyber attack, as it becomes difficult, if not impossible, to identify them". [12]. A multidimensional solution can be proposed to mitigate the effect of DDoS NTP amplified attacks. The solution is composed by the analysis of the two aspects of the problem: **the technical and strategic one** as discussed in our analysis above. Although, for an individual or company running a website or service, mitigation options are limited. This comes from the fact that the individual's server, while it might be the target, is not where the main effect of a volumetric attack is felt.

Due to the high amount of traffic generated, the infrastructure surrounding the server feels the impact. The **technical perspective** is to analyze the specific tool that attackers have to use and can prevent the attacks. First of all, is to configure client systems and use antivirus protection so that the attacker cannot recruit his botnet arm, and finally configure name servers to reduce the attacker's ability to corrupt a zone file with the amplification record. Another important action is to disable open recursion on name servers and accept only recursive DNS from trusted sources. However, since the botnet host is unable to generate DNS request messages that pose as a targeted name server, a new proposed mitigation called **Honeypot** can be adopted. In modern warfare, it is imperative to know your enemy, to nullify the chances of future attacks.

"Honeypots are one of the techniques aimed at collecting information about the attacker by entrapping him in such a way that he doesn't know about it" [14]. Most of the data from the honeypot are recorded and later analyzed to understand the attack vectors and the software tools the threat actor is using, which pose a threat to critical infrastructure. "The goal of this type of honeypot is to lure an attacker to install either handler or agent code within the honeypot, thereby allowing the honeypot's owner to track the handler or agent behavior and better understand how to defend against future DDoS installation attacks. Honeypots are also helpful because they can store event logfiles during a DDoS attack" [6].

The **strategic perspective** is that since DDoS is an attack that overloads a service by consuming resources or generating a flood of traffic to overwhelm a target, the bottlenecks need to be identified, and measures should be taken to enhance the resilience of the server in light of such attacks. In most cases, the entry point is the Internet connection making it the most critical bottleneck, but other factors need to be looked at to address this issue. Some of the strategic methods that should be adopted are discussed below: [13]

Internet service line/ internal Network Bandwidth: Though this method does not address the root cause of the problem, it is largely believed that by having a network with more scalable bandwidth, one can become more prepared to handle the attack. Today, high-speed internet connections of 1 Gbps or 10 Gbps are available at much more affordable prices than before, and so it is advisable to upgrade to such services to enhance the resilience of the system. Further, it is necessary to review the network within the information system. Of late, it is not uncommon to see servers or network devices with interfaces of 1 Gbps or above, but until a few years ago, there was a greater number of devices with much less capacity. There have been cases where 100 Mbps or less could be accommodated in cables comprising the network. The bandwidth could be enhanced, but there could be instances where the internal network could become a fresh bottleneck, so it is recommended that the bandwidth of the connections within the local network systems also be checked and enhanced as one of the measures to mitigate this issue

Filtering in Gateways and ISP routers: One method considered for preventing the inflow of malicious traffic to local networks is the blocking of NTP traffic from non-NTP servers being used for time synchronization at the Internet gateway. More specifically, this would mean filtering the traffic destined for UDP port 123, but it is necessary to check if this will affect communication with remote NTP servers over the Internet, and interfere with the ability to provide outbound NTP services. Another effective method would be to adopt filtering at the ISP router (Egress Filtering) and make a request to the ISP to restrict massive amounts of NTP traffic over the Internet connection itself. Whether this method can be implemented will differ depending on the service policy or the services menu of the ISP.

However, in addition to being a pre-emptive measure, it can serve as a mitigation to counter an actual DDoS attack. Therefore, it is recommended that you build a favorable arrangement by discussing with the concerned ISP manager in advance

Implementation of DDoS (Mitigation) service: There are instances where the ISP that you are contracted to could provide services for deploying a specialized set of techniques to resist a DDoS by detecting and mitigating DDoS traffic. Since these issues are addressed in the backbone of the ISP where there is greater bandwidth before entering the clients' Internet connection, the expectation is that the malicious traffic over the Internet connection can be addressed as well. However, there could be a considerable gap from the time of the DDoS mitigation service subscription until the start of the actual service. It is necessary to implement the service beforehand to be able to distinguish the DDoS traffic based on the regular traffic patterns that one is generally aware of.

4. CONCLUSION AND FUTURE WORK

Most attackers conveniently use DNS and NTP to attack a system or network, because, sending small query packets can get a response 200x bigger. When this response is combined with IP spoofing, can easily lead to the realization of an amplified DDoS attack. However, countering amplification of DDoS attacks is an important security issue to be faced with in this present-day network-empowered organization. In this paper, we have identified and analyzed an alternative defense strategy like a honeypot that can be used to mitigate any amplified DDoS attack, as well as the implementation of strategic techniques to effectively protect and prevent any individual or organization from such attacks. In the future, we intend to deeply analyze this approach by trying to find a holistic set of indicators that can foster a complete and effective prevention methodology and also to further characterize NTP DDoS attacks by using IP datagram and UDP datagram.

REFERENCE

[1] Chen, Yu, Hwang, Kai, & Ku, Wei-Shinn. 2007. Collaborative detection of DDoS attacks over multiple network domains. Parallel and Distributed Systems, IEEE Transactions on, 18(12), 16491662.

[2] Jun, Jae-Hyun, Lee, Dongjoon, Ahn, Cheol-Woong, & Kim, Sung-Ho. 2014. DDoS Attack Detection Using Flow Entropy and Packet Sampling on Huge Networks. Pages 185190 of: ICN 2014, The Thirteenth International Conference on Networks.

[3] Rudman, L., & Irwin, B. (2015, August). Characterization and analysis of NTP amplification-based DDoS attacks. In 2015 Information Security for South Africa (ISSA) (pp. 1-5). IEEE.

[4] Czyz, Jakub, Michael Kallitsis, Manaf Gharaibeh, Christos Papadopoulos, Michael Bailey, and Manish Karir "Taming the 800 Pound Gorilla: The Rise and Decline of NTP DDoS Attacks." Proceedings of the 2014 Conference on Internet Measurement Conference. ACM, 2014.

[5] CloudFlare, “Technical Details Behind a 400Gbps NTP Amplification DDoS Attack,” 2013. [Online]. Available: http://blog.cloudflare.com/technical-details-behind-a 400gbps-ntp-amplification-ddos-attack.

[6] Colella, A., & Colombini, C. M. (2014). Amplification DDoS attacks: Emerging threats and defense strategies. In Availability, Reliability, and Security in Information Systems: IFIP WG 8.4, 8.9, TC 5 International Cross-Domain Conference, CD-ARES 2014 and 4th International Workshop on Security and Cognitive Informatics for Homeland Defense, SeCIHD 2014, Fribourg, Switzerland, September 8-12, 2014. Proceedings 9 (pp. 298-310). Springer International Publishing.

[7] Mimoso, M. "Dramatic drop in vulnerable NTP servers used in DDoS attacks. News Article." (2014)
[8] NSFOCUS. (2014, February). NTP amplification attacks are one the rise? (Part 1) [Online] Available: http://nsfocusblog.com/2014/02/04/ntp-amplification-attacks-are-on-the rise-part-1
[9] Networks, A. (2014, October). Arbor Networks' ATLAS Data Shows Reflection DDoS Attacks Continue to be Significant in Q3 2014. [Online] Available: http://www.arbornetworks.com/news -and events/press-releases/recent-press-releases/5283-arbor-networks-atlas data-shows-reflection-ddos-attacks-continue-to-be-significant-in-q3 2014
[10] Mneimneh, S. (2008). Computer Networks UDP and TCP. Hunter College of CUNY. New York.
[11] US-CERT, "Alert (TA14-017A) UDP-based Amplification Attacks," 2013. [Online]. Available: http://www.us-cert.gov/ncas/alerts/TA14-017A.
[12] Schreier, F.: On Cyberwarfare, DCAF Horizon 2015 Working Paper Series (7) (2012), http://www.dcaf.ch/Publications/On-Cyberwarfare.
[13] NTP Reflection DDoS Attack Explanatory Document, [online]. Available https://www.janog.gr.jp/wg/doc/ntp-wg-en.pdf 3/13/2015 Edition 1
[14] Adeel, M., Chaudhry, A. A., Ahmed, E., Samad, K., & Shaikh, N. M. (2005, August). Honeynets: An Architectural Overview. In *2005 Student Conference on Engineering Sciences and Technology* (pp. 1-6). IEEE.