International Journal of Information & Network Security (IJINS)
Vol.3, No.3, June 2014, pp. 212~224
ISSN: 2089-3299

DDoS Attack Defense in Next Generation Networks using Private Security Policy

Dac-Nhuong Le
Faculty of Information Technology, Haiphong University, Haiphong, Vietnam

Article Info

Article history:

Received March 5th, 2014
Revised April 10th, 2014
Accepted April 20th, 2014

Keyword:

Next Generation Network
Distributed Denial of Service
Quality of Service
NS-2

ABSTRACT

The Distributed Denial of Service (DDoS) attacks have not been around with any significance for very long over the history of ICT. However, this problem is evolving quickly, and it is becoming increasingly hard to grasp a global view of the problem. Particularly for Next Generation Network (NGN), that will provide advanced services, such as Quality of Service (QoS) guarantees to users and their applications. In this paper, we focus to analysis challenges DDoS prevention in NGN and propose a defense method using private security policy. The efficiency of our proposed method was also proved in the experiment with NS2. DDoS attack is controlled effectively by the private security policy the bandwidth of the regular traffic would be maintained.

Corresponding Author:

Dac-Nhuong Le,
Faculty of Information Technology, Haiphong University, Vietnam
171 Phan Dang Luu, Kien An, Haiphong, Vietnam.
Email: nhuongld@hus.edu.vn

1. INTRODUCTION

In Next Generation Network (NGN), the backbone of the overall network architecture will be IP network, supporting different access network technologies such as WLAN, UMTS Terrestrial Radio Access Network (UTRAN), and WiMax. Moreover, this integrated wireless system, will have to handle diverse types of traffics: data traffics (*e.g. web browsing, e-mail, ftp*), voice traffic (*e.g. VoIP*), and multimedia traffics (*e.g. video conferencing, online TV, online games*), etc. NGN will provide advanced services, such as Quality of Service (QoS) guarantees, to users and their applications [1]. The Internet Protocol Multimedia Subsystem (IMS) is such a standardized NGN for worldwide use. It is still under active development from a worldwide alliance, called the 3rd Generation Partnership Project (3GPP). The key features of IMS are multimedia session management, guaranteed QoS, secure network access and service control. IMS is based on core IP protocols, with the fundament on SIP (*Support Session Initial protocol*) for session control. Other important protocols in IMS are Diameter for AAA (*Authentication, Authorization, and Accounting*) service, or RTP for media transport. IMS defines many different roles, with the most prominent ones are: CSCF (*Call Session Control Function*), HSS (*Home Subscription Server*), AS (*Application Server*), MRF (*Media Resource Function*), GF (*Gateway Function*). TISPAN (*Telecommunication and Internet converged Services and Protocols for Advanced Networking*) is based on the IMS specification, and extends it among other to DSL access, non SIP-based applications and IPTV services [2, 3, 4].

The DDoS field is evolving quickly, and it is becoming increasingly hard to grasp a global view of the problem. Since 2013, attackers have been abusing communication protocols such as Character Generator, Network Time Protocol (NTP) and Domain Name System (DNS). These are all based on the User Datagram Protocol (UDP) which indirectly allows attackers to conceal their identities via address spoofing so they are not immediately identified as the source of an attack. Attackers send small request packets to intermediary

victim servers, and those servers in turn respond to the attacker's intended target. The availability of these vulnerable protocols, which are often enabled by default in server software, make the Internet a ready-to-use botnet of potential victim devices that can be exploited by malicious actors to launch huge attacks. In "*Prolexic Quarterly Global DDoS Attack Report Q1 2014*" [5] of Prolexic Technologies found that in just three months since the Quarter 4 of 2013 there had been a 18% increase in the total number of DDoS attacks, 39% increase in average attack bandwidth, 35% increase in infrastructure (Layer 3 & Layer 4) attacks had occurred, 36% decrease in application (Layer 7) attacks, 24% decrease in average attack duration: 23 vs. 17 hours, 114% increase in average peak bandwidth. The attack, which exceeded 10 hours in length, peaked at more than 200 Gbps and 53.5 million packets per second are shown in Fig.1.

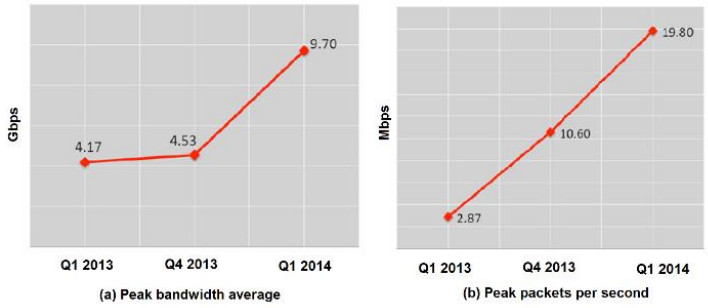

Fig 1. Comparison of peak bandwidth average and packets per second in Q1 2013, Q4 2013 and Q1 2014

In this paper, we focus on analysis challenges DDoS prevention of NGN. We have suggested an approach for guaranteed QoS to normal users under DDoS flood attack based on bandwidth dynamic assignment in order to sustain the server. The rest of this paper is organized as follows: Section 2, we focus on analyzing the advantages and disadvantages of the X805-ITU-T security architecture for NGN. Section 3 introduces DDoS attacks and DDoS defense machanise classification. Section 4 presents our method suggested to bandwidth dynamic controlled for guaranteed QoS to normal users under DDoS flood attack. Section 5 analysis experiment results in NS-2. Finally, Section 6 concludes the paper.

2. NGN SECURITY ARCHITECTURE

2.1 ITU-T X805 Security Architecture

ITU-T has suggested the X.805 framework for NGN architecture for achieving End-to-End (E2E) security in distributed applications. They provide a comprehensive, multi-layered, E2E network security framework across eight security dimensions in order to combat network security threats [6]. The NGN Security Dimensions include access control, authentication, non-repudiation, data confidentiality, communication security, data integrity, availability, and privacy. The NGN Security Layers are a hierarchy of equipment and facilities organized as three layers: infrastructure security layer, service security layer, and application security layer. Each layer relates to unique vulnerabilities, threats and mitigation measures. The NGN Security Planes comprises the types of security related activities that are typically deployed on a network. They are management security plane, control security plane, end-user security plane. Each security plane has to be interconnected with each security layer, so resulting in nine security perspectives. Each security perspective corresponds to unique vulnerabilities and threats. ISO/IEC has defined the information technology security requirements and objectives for NGNs [6]. The main objective is controlling the security risks to an acceptable level for all stakeholders of NGNs. Attacks are becoming more sophisticated, unpredictable, frequent and from a wider range of sources. On the other hand, the existing standards, solutions or methodologies do not appear to sufficiently support the required security assessments. Standardization has a very important role in the achievement of security objectives. However, technologies are developing very fast and the research and standardization organizations do not have enough time to analysis all possible vulnerabilities and threats before technologies are deployed.

2.2 An vulnerability, threat, risk analysis

In this section, we present these several reasons for the insufficiency of the current methods for analyzing vulnerabilities, threat and risks as reference studies to reach security objectives and standardization of NGNs. Each new NGN service can include different compositions of many new technological equipment and software solutions, and these compositions entail different complex threats and risks. The composition of services does not necessarily imply that the upper services inherit the security attributes of its components.

Each new composition adds and amplifies vulnerabilities and threats, and therefore each new service would require a specific security analysis. For instance, the traditional communication network PSTN, its protocols and the Internet infrastructure are used together for VoIP. Vulnerabilities derive from errors or oversights in the design of SIP protocols in 802.11b [7]. SIP as an IP based signaling protocol, which is used by global Voice over Internet providers and plays major role NGN based telecommunication networks [8]. As a matter of fact, protocols are deployed without a complete and unquestionable proof of their security properties. During their lifetime, protocols change, incorporating patching and evolving with the addition of new features. Each new version is vulnerable in some ways not totally known when being deployed, and differing from its previous versions. The current vulnerability, threat and risk analysis methodologies such as e-TVRA for NGNs [9] typically focus on known threats and vulnerabilities because this is the available information. All threats, vulnerability and risk analysis methods continuously need to update their knowledge of new weaknesses of the assets being studied, to identify how these weaknesses can be exploited, for then evaluating the security risk, and defining and implementing the needed countermeasures. As the information basis for those analyses is incomplete, new evaluations will be needed in time. The set of security data is never complete, and assessments should be redone with each series of new data. In addition, it is known that information on attacks is not promptly disclosed due to their sensitivity. When disclosed, it should be taken into consideration for remaking the security assessment of the systems for which it is relevant. Therefore the improvement of NGN security systems via vulnerability, threat and risk analysis tool is a time consuming and always incomplete process.

The risk as any unwanted event that might have negative consequences defined in [10]. Different methodologies for risk and threat assessment define risk with regard to the threats and threat agents known to the users. Today, total threat assessments are rarely possible due to the complexity of systems and networks: threat scenarios can affect many components, generate intricate and multifaceted failure mechanisms, and propagate within the systems in complicated ways. So, NGN risk models cannot ignore this situation. In [11], the author defined another required feature is security measurement. However, there are no security measurement definitions and tool has proven it's logical and mathematically validity. Therefore the security of NGN systems cannot be determined in absolute terms, although there is the need to measure in some way the fulfillment of the security requirements. From this the need for appropriate security measurements and metrics. This is fundamental for evaluating whether new security scenarios or solutions have positive or negative effects upon the NGN network and its services. An important attribute of any security evaluation is uncertainty which depends on time and the chosen reference values. As security is a function of time, evaluations should provide a proper answer about its evolution, and its dependency upon the changes in different factors. In addition, as NGN systems put together many actors, security might have different quantitative values for each one of them. The measurement of security should be a continuous activity, dynamically evolving according to the changes in the NGN architecture and service, and to the points of view various stakeholders.

3. CHALLENGES FOR DDOS ATTACK DEFENSE IN NGN

3.1 Distributed denial of service (DDoS)

Denial-of-Service (DoS) attacks are a class of network attacks performed to interrupt or terminate applications, servers, or even whole networks, with the aim of disrupting legitimate users' communication. Disruption targets are web browsing, listening to online radio, or even interrupting essential communication. DoS attacks are commonly performed intentionally and in most cases difficult to counter. In many cases it is only possible to mitigate, but not to completely prevent the attack. DoS attacks can have different forms, and they can also be differently motivated. There are two common strategies to launch a DoS attack, by either exploiting a software vulnerability or by depleting resources at the target host. The first of DoS attack is to exploit vulnerabilities in a software component on the target machine. This includes vulnerabilities in application servers, network stacks, or general operating system vulnerabilities. Vulnerabilities in huge projects are a common case, as it is impossible to predict every situation where software is deployed. To exploit the vulnerability, an attacker sends a messages crafted in a specific way that takes advantage of that given vulnerability. The second common DoS attack is to overwhelm a resource at the target. The attack tries to overwhelm resources at the target by generating more requests than the target can handle. There are three common resources an attacker can exploit: memory, CPU power and bandwidth. The exploitation is possible because all these three resources are finite. DoS attacks can be launched against both services and networks with many types of DoS attack, such as TCP Syn Flood, UDP flood, Ping of death, Teardrop attack, etc [7].

Over the time DoS attacking strategies have become more elaborate with one of the most severe forms being Distributed DoS (DDoS) attacks. DDoS attack is a technique that uses client/server model, combines lots of computers as an attack platform and launches at one or more victims (machines or

networks). Traditional DDoS attacks involve two steps. The first is breaking into a large number of computers using techniques such as virus, Trojan, buffer overflow, etc. and gaining a zombie network. The second is sending a great deal of traffic to victims using zombie network and preventing them from offering service to their legitimate users. In most cases, the first step is the key to restrict the scale and performance of DDoS attack as more and more Internet users recognize the security of computer system and network [8, 9]. DDoS attacks can be realised using different topologies shown in Fig 2.

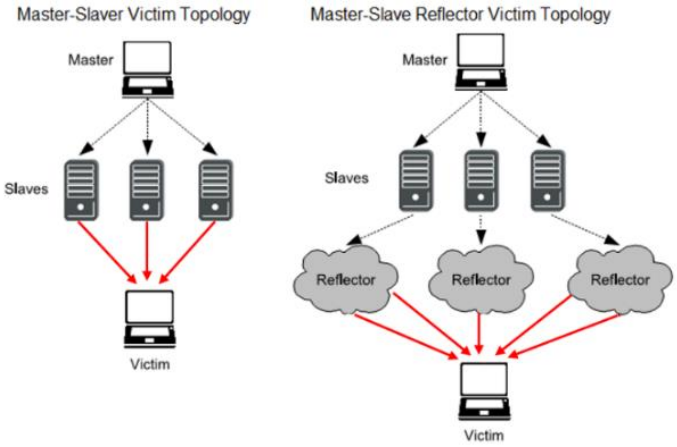

Fig 2. DDoS Attack topologies

In Master-Slave-Victim topology, the master either directly represents the attacker or is controlled by the attacker while slaves represent terminals being controlled by the master system. Thus each slave terminal attempts to flood the victim with a massive amount of packets using forged source addresses so that the victim is unable to detect the real source of the flood. In Master-Slave-Reflector-Victim topology (DRDoS), the attacker commands each slave to send spoofed echo request packets to the broadcast address of an amplifying network. The source address is spoofed and equal to the address of the victim. Every host of the amplifying network will reply to the victim. Note that with this topology the source address of actual attacking traffic arriving at the victim is not spoofed, because reflectors send with their real source address, assuming that they received an echo request from the victim.

3.2 DDoS Attacks classification

According to the classification of the CERT Coordination Center (CERT/CC), attackers launch attacks using different techniques including HTTP, ICMP, SYN Floods, UDP Floods, DNS Request Floods, TCP RESET and others. The attack components are often used in combination, and range in size from a few hundred megabits per second to several gigabits per second. There can be several classifications of DDoS attacks based on various criteria in [10]. DDoS Attacks are divided into four classification is shown in Fig.3.

3.3 DDoS Attack tools

DDoS attack can be performed by using various available tools. Even one can exploit the systems using their own attacking tool/tools. Easy availability of DDOS tools is one of the reasons for conducting DDoS attack. Some attacking tools are agents based in which agents and handlers know each other's identity while in IRC based attacking tools, communication is done indirectly in which they do not know each other identity. Using these tools, attackers conceal their identity by the eal source of the attackers to stop the attack at the point spoofing the source IP address and launch an attack. The first tools developed to perpetrate the DDoS attack were Trin00 and TFN. TFN then bring forth the next generation of tools called TFN2K. These DDoS attack tools are designed to bring one or more sites down by flooding the victim with large amounts of network traffic originating at multiple locations and remotely controlled by a single client. Table I gives a comparison among various popular DDoS tools [11, 12].

3.4 DDoS Defense Classification and Filtering Techniques

The seriousness of the DDoS problem and the increased frequency of DDoS attacks have led to the advent of numerous DDoS defense mechanisms. Some of these mechanisms address a specific kind of DDoS attack such as attacks on Web servers or authentication servers. Other approaches attempt to solve the entire

generic DDoS problem. Most of the proposed approaches require certain features to achieve their peak performance, and will perform quite differently if deployed in an environment where these requirements are not met. As is frequently pointed out, there is no "*silver bullet*" against DDoS attacks. Therefore we need to understand not only each existing DDoS defense and filtering techniques approach, but also how those approaches might be combined together to effectively and completely solve the problem shown in Fig.4 and Table II [13, 14].

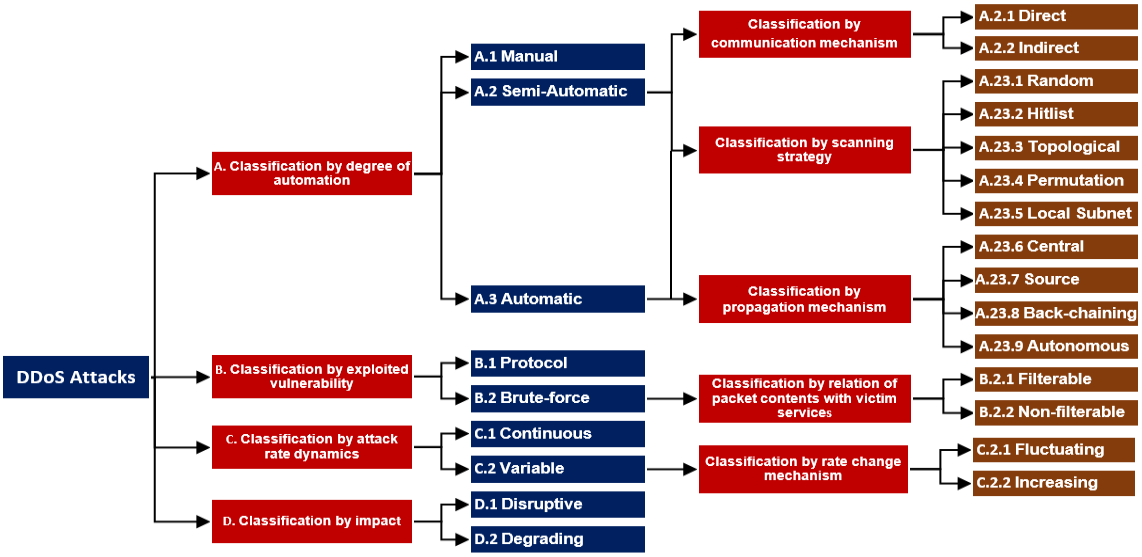

Fig 3. Classification of DDoS attacks

TABLE I. DDoS ATTACK TOOLS

Ord	Tool name	Year	Possible Attacks	Packet Format and Type Attacks
1.	**Stacheldraht**	06/1999	Bandwidth and Resource Depletion	Udp, Tcp-Syn, Icmp, Directed Broad Cast
2.	**Trinity**	08/1999	Bandwidth and Resource Depletion	Udp, Tcp-Syn, Tcp-Ack, Tcp-Rst
3.	**Shaft**	11/1999	Bandwidth and Resource Depletion	Udp, Tcp, Icmp
4.	**Trinoo**	02/2000	Bandwidth Depletion	UDP
5.	**Tfn (Tribe Flood Network)**	04/2000	Bandwidth and Resource Depletion	Udp, Tcp-Syn ,Icmp Echo Rst, Directed Broadcast
6.	**Mstream**	04/2000	Bandwidth Depletion	Tcp-Ack, Icmp, Tcp-Rst
7.	**Tribe Floodnet (Tfn2k)**	06/2000	Targa And Mix Attack	Udp, Tcp-Syn, Icmp
8.	**Knight**	07/2001	Bandwidth and Resource Depletion	Syn, Udp
9.	**Kaiten**	08/2001	Bandwidth and Resource Depletion	Udp, Tcp-Syn, Tcp-Push+Ack
10.	**Owasp Http Post Tool**	12/2010	Resource Depletion, Slow Post, Slow Get	http
11.	**Davoset**	07/2010	Resource Depletion	XSS
12.	**Ufonet**	2013	Resource Depletion	Web Abuse

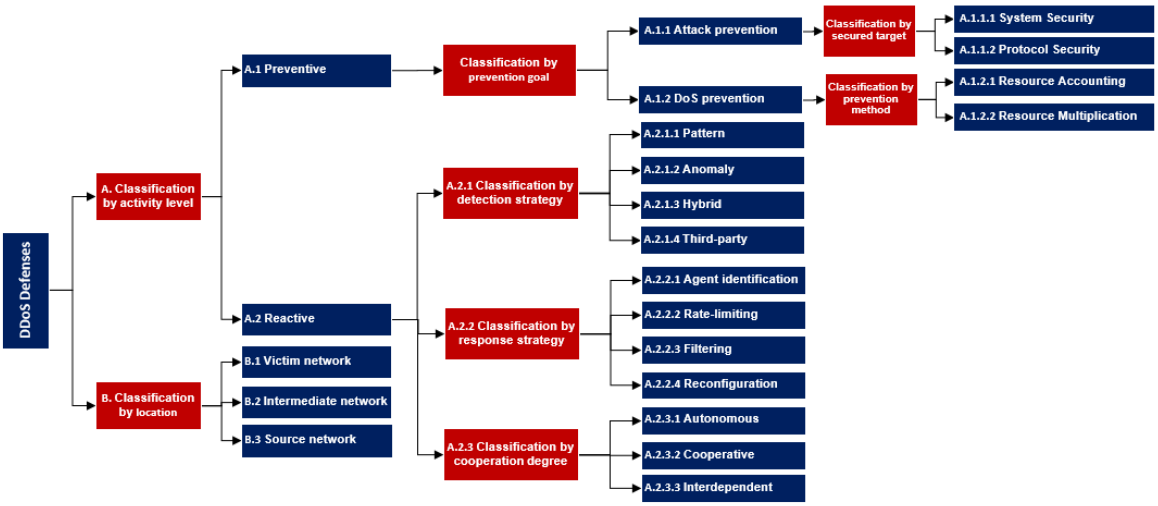

Fig 4. Classification of DDoS Defenses

TABLE II. FILTERING DDOS ATTACK TECHNIQUES

Ord	Filtering techniques	Benefits	Limitations
1.	Ingress/ Egress	- Prevents IP Spoofing	- Need global development - Attacks with real IP addresses can not be prevented
2.	Route based Packet Filtering (RPF)	- Work well with static routing	- Problem when dynamic routing is used - Need wide implementation to be effective
3.	History based	- Does not require cooperation of whole Internet Community. - Gives priority to the frequent packets in case of congestion or attack	- Ineffective when the attacks come from real IP addresses - Requires an offline database to keep track of IP addresses - Depend on information collected
4.	Capability based	- Provides destination a way to control the traffic it desires - Incremental deployment	- Attacks against the request packets can not prevented (e.g. ROC attack) - High computational complexity and space requiremen
5.	Secure overlay Service (SOS)	- Works well for communication of predefined source nodes	- Solution has limited scope e.g. not applicable to web servers - Require introduction of a new routing protocol that itself another security issue
6.	Source Address Validity Enforcement (SAVE)	- Filtering improperly addressed packets is worthwhile - Incremental deployment	- During the transient period valid packets can be dropped

3.5 DDoS Defences Challenges and goals

The main problem that permits effective DDoS handling is the problem of large scale. DDoS is a distributed threat that requires a myriad of overlapping "*solutions*" for various aspects of the DDoS problem, which must be spread across the Internet because attacking machines may be spread all over the Internet. The following is a list of challenges for DDoS defence [15, 16]:

- *Uncertainty of defence placement*: Ideally, a defence solution should be located close to the attacker, to allow fast reaction to the attack. Unfortunately, it is seldom known where the attacker is located. Also, network closely to the attacker might not be under control of the target, so it is mostly not even possible to locate defences there. Hence, most defences are placed close to the target, with the main drawback that there the defence mechanisms also can be overwhelmed by large scale DDoS traffic. Ideally, the defence should be located a different places.
- *Lack of detailed attack information:* It is widely believed that reporting occurrences of attacks damages the business reputation of the victim network. Therefore, very limited information exists about various attacks, and incidents are reported only to government organisations under obligation to keep them secret.
- *Lack of defence system benchmarks:* Many vendors make bold claims that their solution completely handles the DDoS problem. There is currently no standardised approach for testing DDoS defence systems that would enable their comparison and characterisation.
- *Difficulty of large-scale testing.* DDoS defences need to be tested in a realistic environment. This is currently impossible due to the lack of large-scale test beds, safe ways to perform live

distributed experiments across the Internet, or detailed and realistic simulation tools that can support several thousand nodes.

It is an impossible task to devise a solution targeting the listed challenges. The sheer size of the Internet renders any complete solution ineffective. The goal should therefore be to devise protection methods compromise between completeness and effectiveness [17, 18, 19]. Whether the DDoS defence strategy is preventive, reactive, or a combination of both, there are some basic goals it wants to achieve:

- *Effectiveness*: A good DDoS defence should actually defend. It should provide either effective prevention that really makes attacks impossible or effective reaction ensuring that the DoS effect goes away.
- *Completeness*: A good DDoS defence should handle all possible attacks. If that degree of perfection is impossible, it should at least handle a large number of them.
- *Provide service to all legitimate traffic*. As mentioned earlier, the core goal of DDoS defence is not to stop DDoS attack packets, but to ensure that the legitimate users can continue to perform their normal activities despite the presence of a DDoS attack.
- *Minimum false-positive rates.* Good DDoS defence mechanisms should target only true DDoS attacks. Preventive mechanisms should not have the effect of hurting other forms of network traffic.
- *Low deployment and operational costs.* DDoS defences are meant to allow systems to continue operations during DDoS attacks, which, despite being very harmful, occur relatively rarely. The costs associated with the defence system must be compensated with the benefits provided by it. Other operational costs relate to overheads imposed by the defence system.

4. DEFENDING UDP FLOODING ATTACK BASED ON PRIVATE SECURITY POLICY

4.1 Our approach

In this section, we considers flood attacking. Taking into account the experiments we shall discuss, the term bandwidth attacking used in the paper is equivalent to flood attacking without confusion causing. Flood packets may be generated by hundreds or thousands of machines distributed all over the world. Note that a flood attacker's goal is not to break into the target site (target for short) but to overwhelm it by bombarding flood packets on it or to considerably degrade its performances for serving its legitimate traffic. We assumes that, the target network is the NGN (best-effort class communication is assumed). Internet service providers (ISP) provide their services over the NGN which is a private extension. Edge routers in the NGN can be controlled. NGN topology has two types of Edge routers are Entrance-Side Edge Routers and Exit-Slide Edge Router. The carrier and ISP side detect abnormal IP packets. Individual information is used and identified by a private security policy that a user registered beforehand so normal IP packets are never discarded as a result of being false-recognized.

Due to the problems of existing countermeasures shown in the previous section, their countermeasures decrease the damage caused by a DDoS attack that consumes server resources. On the other hand, a DDoS attack using UDP (user datagram protocol) accelerates the load on the network, is hard to counter because UDP packets sent from network are limited by the LAN, and enough countermeasures have not been developed. Therefore, our method targets DDoS attacks using UDP. DDoS attack using UDP is detected by judging whether it exceeds a certain number of UDP packets (available bandwidth) in the unit-time output from the NGN side. The number is determined according to the private security policy on the LAN side and registered in the private security policy before the DDoS attack detection starts. A UDP-based DDoS attack can be controlled down to the minimum bandwidth available for forwarding UDP packets from the NGN to a LAN, which is registered similarly. Here, the DDoS attack is controlled by delaying UDP packets judged to be DoS attack packets. The process of DDoS prevention based on private policy has four phases is shown in Fig.5.

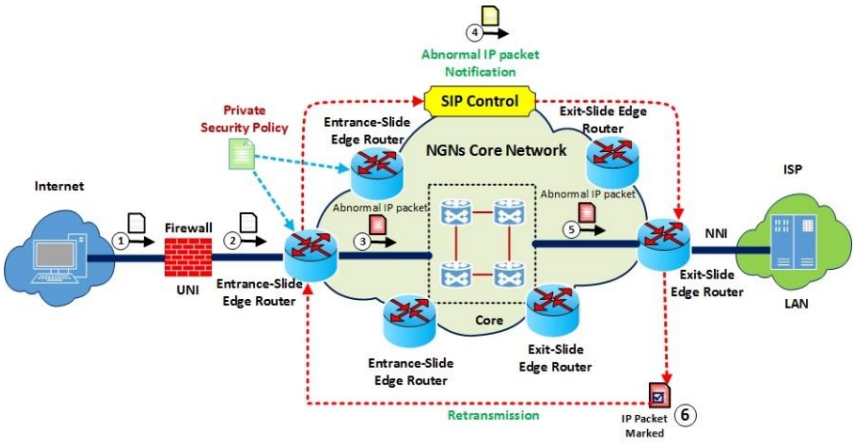

Fig 5. UDP Flooding DDoS Attack Defense method using private policy

Phase 1: *Private security policy initialization at Entrance-Side Edge Routers.* The bandwidth in a time unit that a server can use for UDP packets is set as a parameter for controlling a DDoS attack by using the number of UDP packets available bandwidth in time unit (seconds). It is registered in the private security policy as a parameter for detecting a UDP-based DDoS attack. The private security policy includes destination IP address, DoS attack detection threshold and UDP communication bandwidth.

Phase 2: *Abnormal IP packet detection at Entrance-Side Edge Routers*. The number of UDP packets arriving at a server is always observed at NGN exit-side Edge Routers. A DDoS attack is judged to occur when the number of UDP packets (for one second) exceeds the values registered in the private security policy. The packet type (UDP), destination IP address, and destination port number are examined. When the measured number of UDP packets in time unit equals to the number registered in the private security policy or more are detected, they are recognized as abnormal packets. So, those packets are judged to be DDoS attack packets. Destination IP address "*IP*", destination port number "*Port*", and average packet size are read from packets judged to be DDoS attack packets (bytes). The bandwidth of UDP packets must be controlled and limited. We can calculated the packet delay time. After a DDoS attack is detected at an NGN Exit-side Edge Router, all NGN Entrance-side Edge Routers are notified of the attack by SIP control. This SIP is assumed to be our private extension. The SIP-based notification contains information about the type of DDoS attack packets and their destination IP address and destination port number and the required delay. This information is used for marking IP packets. The delay time is used by the path control, which imposes this delay.

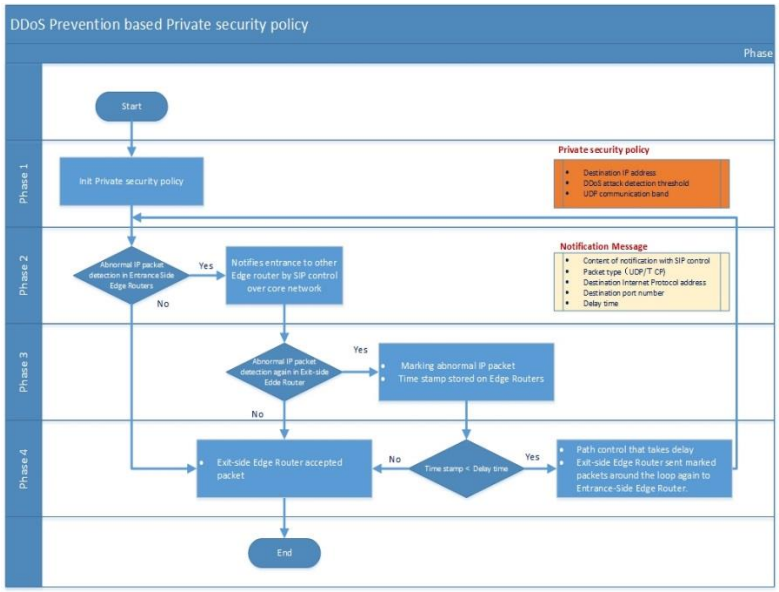

Fig 6. DDoS Prevention based on private security policy

Phase 3: *Abnormal IP packets Marked*. The NGN Entrance-side Edge Router checks all IP packets as they pass through. It checks for IP packet information corresponding to the packet type, destination IP address, and destination port number of DDoS attack packets reported by the NGN Exit-side Edge Router by SIP control and writes the extraction time (as a timestamp) in the extension header field of the IP packet (Note that at present SIP does not have this function. So it is assumed that the proposed SIP have such a function). If IP packet being MTU size, the fragmentation of IP packets will be done before the timestamp is written in these IP packets. All IP packet are examined and they having destination port number "*Port*" and packet type "*UDP*" and destination IP address "*IP*" are regarded as DDoS attack packets. The information extraction time is written into the IP packets in order to mark them.

Phase 4: *Abnormal IP packets control at Exit-side Edge Router takes delay time.* All marked IP packets are forwarded by the NGN Entrance-side Edge Router around a loop so that they return later. When an IP packet is received, the marked timestamp is compared with the current time to ensure that the required delay had been added. The path control for delaying IP packets marked at an NGN Entrance-side Edge Router by retransmitted along a route (with a loop added) that returns to the Entrance-side Edge Router. When a marked IP packet is received at an NGN Entrance-side Edge Router, the Edge Router judges whether the current time minus the marking time is greater than the required delay time. Then, IP packets that have been delayed long enough are transmitted to the destination IP address through the NGN core router, while ones with insufficient delay are sent around the loop again. So, IP packets transmitted from the NGN Exit-side Edge Router to the destination IP address "*IP*" and destination port number "*Port*" are transmitted at a reduced bitrates.

Thus, our method decreases the number of IP packets per time unit by applying a path control that imposes a delay. In this way, DDoS attacks can be controlled. Note that the point here is to delay them. Packets that are clearly malicious are discarded. However, genuine or borderline packets are delayed so that the user can decide. As a result, the influence of DDoS packets on other packets user traffic becomes extremely small.

5. EXPERIMENTS AND RESULTS

5.1 Network Topology for simulation

Fig.7 shows our network topology for the simulation. Network architecture consists HTTP Server DNS1 Server, DNS2 Server, NTF Server, regular Users, DDoS Attack connected by NGN network. In NGN network, the routers are divided into 3 categories Core Router, Entrance-side Edge Routers, Exit-side Edge Routers. We assumed both of them send UDP, TCP packets via NGN from the Internet to the servers. The bandwidth of the access line between NGN and servers was 10 Mbps, and that of both the Internet and NGN was much broader 10Mbps.

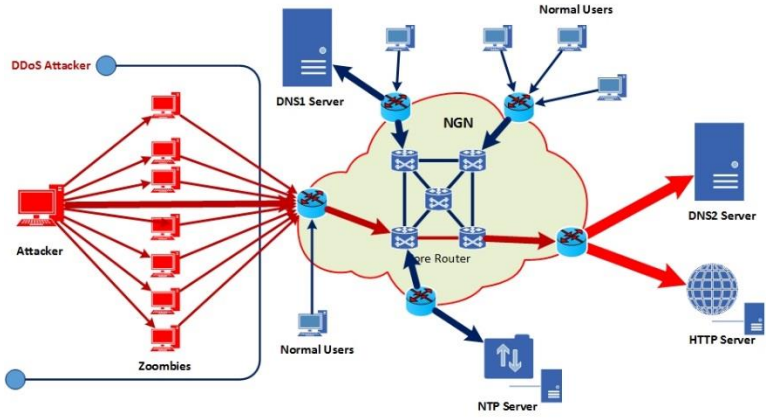

Fig 7. Network Topology for simulation

5.3 NS-2 Implementation for simulation

We evaluated the effect of our defense technique using Network Simulator version 2.3.3 (NS-2) [20]. The network topology implemented in NS-2 include 20 nodes (n0, n1,…,n19) are shown in Fig 8.

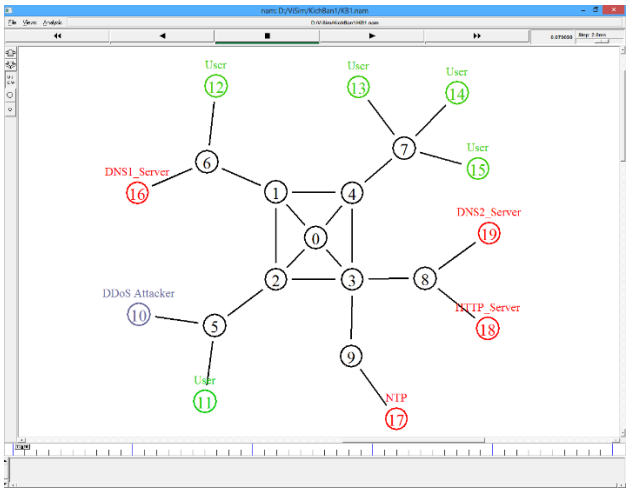

Fig 8. Network structure in NS-2

Table II shows simulation detail conditions and Table III shows a private security policy to control the DDoS attacks using our method. The assumed threshold of the DDoS attack is 10% of bandwidth maximum. So, we caculate to bandwidth of the control is 1 Mbps here.

TABLE III. OBJECT'S PARAMETER DETAIL FOR SIMULATION

Classification	NS-2 Object	Parameter	Values
Core Router	n0, n1, n2, n3, n4		
Entrance-side Edge Routers	node 5, node 6, node 7, node 9		
Exit-side Edge Router	node 8		
DDoS Attacker	node 10	Protocol	UDP
		Size of Packet	64 Byte
		Transmission Pattern	Constant Bit Rate
		Transmission bandwidth	10 Mbps
		Port	53
Users	node 11, node 12	Protocol	TCP
		Size of Packet	64/512/1024/1500 Bytes
		Transmission Pattern	Constant Bit Rate
		Transmission bandwidth	5 Mbps
		Port	80
Users	node 13, node 14, node 15	Protocol	TCP
		Size of Packet	64/512/1024/1500 Bytes
		Transmission Pattern	Constant Bit Rate
		Transmission bandwidth	5 Mbps
		Port	80
DNS1 Server	node 16	Protocol	UDP
		Bandwidth Maximum	10 Mbps
		Port UDP	53
		Transmission Pattern	Constant Bit Rate
		Transmission bandwidth	5 Mbps
NTP Server	node 17	Protocol	UDP
		Bandwidth Maximum	10 Mbps
		Port UDP	123
		Transmission Pattern	Constant Bit Rate
		Transmission bandwidth	5 Mbps
HTTP Server	node 18	Protocol	UDP/TCP
		Bandwidth Maximum	10 Mbps
		Port TCP	80
		Port UDP	123
		Normal UDP Bandwidth use	0.175 Mbps
		DDoS attack detection threshold	10% = 1 Mbps
DNS2 Server	node 19	Protocol	UDP

Classification	NS-2 Object	Parameter	Values
		Bandwidth Maximum	10 Mbps
		Port UDP	53
		Normal UDP Bandwidth use	0.35 Mbps
		Port UDP	123
		Normal UDP Bandwidth use	0.175 Mbps
		DDoS attack detection threshold	10% = 1 Mbps

5.4 Simulation and results

In the simulation, NS-2 made the UDP packets of the regular users and DDoS attacker and sent the UDP packets respectively to the NGN. The simulation was done with some scenarios in terms of combination of regular traffic and DDoS traffic.

Case study 1: After 5 seconds, the attacker starts sending UPD packets to HTTP Server during 30 seconds. The HTTP Server is congested temporarily caused by the DDoS attack. Therefore, all requests from user send to the server will be rejected. We started set up our private security policy in the Entrance-side Edge Routers and Exit-side Edge Routers. When our control method had been executed, the communication bandwidth of regular users was secured and these users could communicate without any influence of the DDoS attack. It is also confirmed that traffic does flow into the internal NGN, because the DDoS attack is controlled effectively by the entrance-side edge router is illustrated in Fig.10.

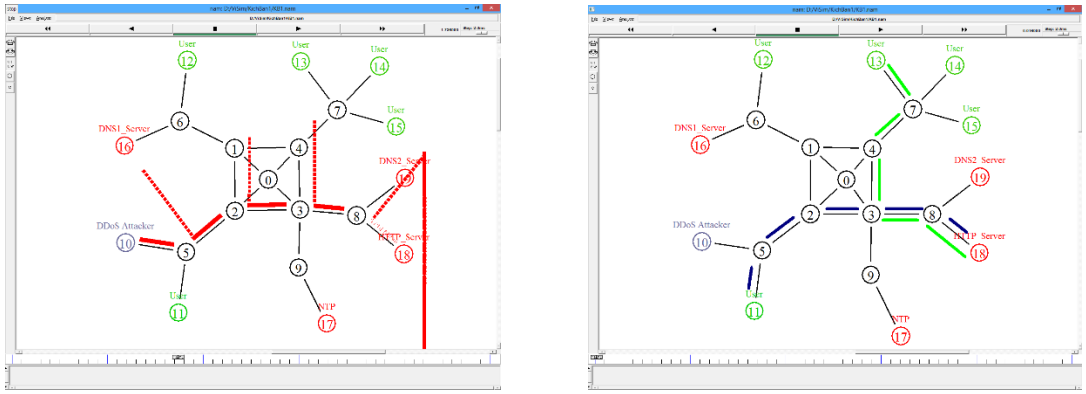

Fig 10. Congestion was temporarily caused by the DDoS attack in HTTP Server and DDoS attack is controlled effectively by the private security policy in Case study 1.

Case study 2: Similar case stuty 1, after 5 seconds, the attacker starts sending UPD packets to HTTP Server and DNS2 Server during 30 seconds. Both HTTP Server and DNS2 Server are congested temporarily caused by the DDoS attack. We had been executed our proposed method and the DDoS attack is controlled effectively is illustrated in Fig.11.

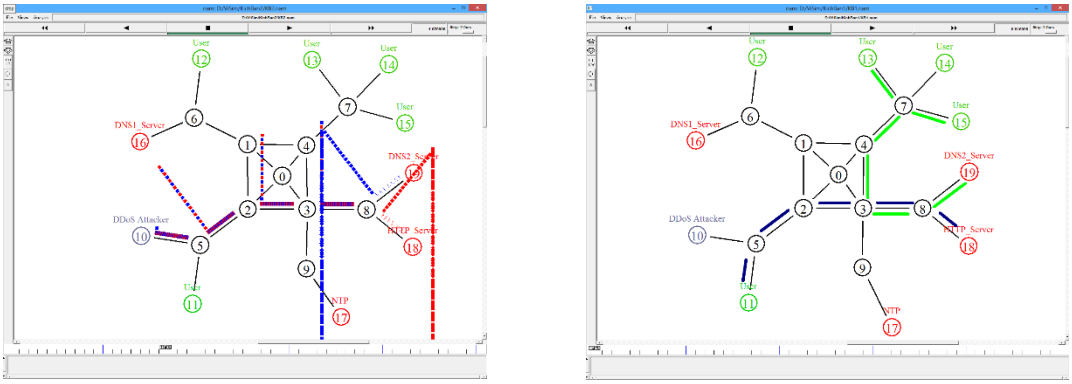

Fig 11. Congestion was temporarily caused by the DDoS attack in HTTP Server and DDoS attack is controlled effectively by the private security policy in Case study 2.

To evaluate the effectiveness of the proposed method, we compared the UDP bandwidth of servers. In Fig.12, from 0 second to 5 second, traffic ratio of both users and DDoS traffic were less than 5Mbps around and no bandwidth degradation occurred on the regular traffic. Starting at 5th seconds, the DDoS attack occupying almost full bandwidth of the access link (~10Mb/s) and our private security policy had been

executed. After 5 seconds the DoS attack started, our countermeasures worked effectively, the bandwidth of the DDoS traffic was decrease by the proposed countermeasures so that the bandwidth of the regular traffic would be maintained.

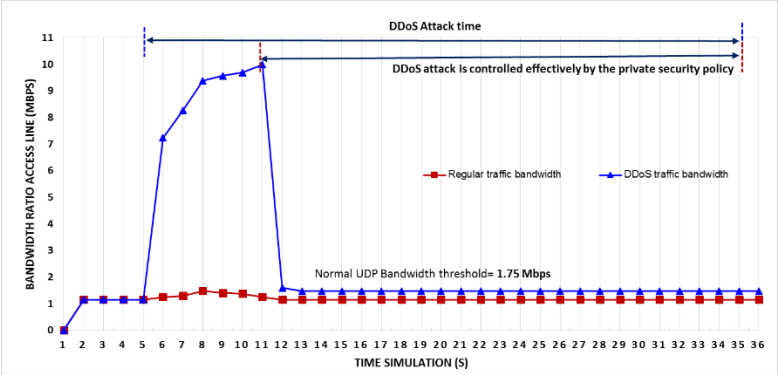

Fig 11. DDoS attack is controlled effectively by the private security policy in Case study 1

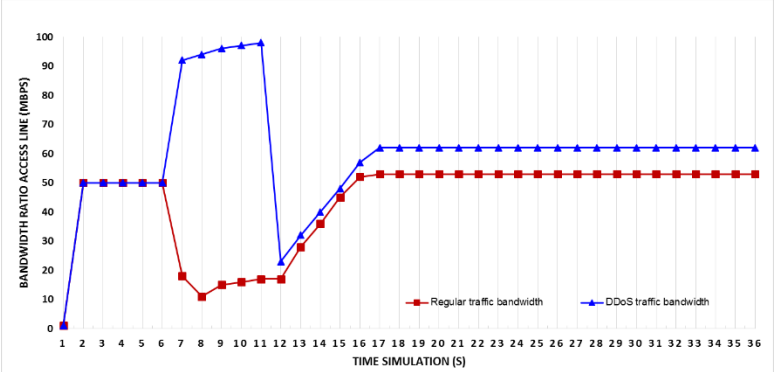

Fig 12. DDoS attack is controlled effectively by the private security policy in Case study 2

6. CONCLUSIONS

In this paper, **w**e focus to analysis challenges DDoS prevention in NGN and propose a defense method using private security policy. The efficiency of our proposed method was also proved in the experiment with NS2. DDoS attack is controlled effectively by the private security policy the bandwidth of the regular traffic would be maintained. Our next goal is guaranteed QoS to normal users under DDoS flood attack in NGNs and suggest an intelligent Intrusion Detection System (IDS) using SNORT.

REFERENCES

[1] ITU-T, Technology Watch Briefing Report Series, *Next-Generation Networks and Energy Efficiency*, No. 7, 8/2008.
[2] ITU-T Y-2001, *General overview of NGNs*, 2004.
[3] ITU-T Y-2011, *General principles and general reference model for Next Generation Networks*, October 2004.
[4] ITU-T Y-2012, *Functional requirements and architecture of the NGN. Release 1*, September 2006.
[5] Prolexic Quarterly Global DDoS Attack Report Q1 2014, USA. www.prolexic.com
[6] Cho Y, Won Y, Cho B. 'ITU-T X.805 *based vulnerability analysis method for security framework of end-to-end network services*. In Proceeding of the 4th WSEAS, Tenerife, Spain, pp.288-292, 2005
[7] J. Mirkovic, S. Dietrich, D. Dittrich, and P. Reiher. *Internet Denial of Service: Attack and Defense Mechanisms*, Prentice Hall PTR, 2004.
[8] D. Dittrich. *Distributed Denial of Service (DDoS) Attacks/tools.* Reference page about DoS attacks, tool and events. Last updated Aug. 2008. http://staff.washington.edu/dittrich/misc/ddos,
[9] Cisco, *Strategies to protect against Distributed Denial of Service Attacks.*
[10] CERT Coordination Center, *Denial of Service Attacks*, http://www.cert.org/tech_tips/denial_of_service.html.
[11] Arun Raj Kumar, P. , S. Selvakumar, *Distributed Denial-of-Service (DDoS) Threat in Collaborative Environment A Survey on DDoS Attack Tools and Traceback Mechanisms*, IEEE International Advance Computing Conference (IACC 2009) Patiala, India, 6 -7 March 2009.
[12] T. Anderson, T. Roscoe, D. Wetherall, *Preventing Internet Denial-of-Service with Capabilities*, In ACM SIGCOMM Computer Communication Review, Vol.34(1), January 2004, pp. 39-44
[13] J. Li, J. Mirkovic, M. Wang, and P. Reither, *Save: Source address validity enforcement protocol*, in proceedings of IEEE INFOCOM, 2002, pp. 1557-1566.
[14] J. Mirkovic, P. Reiher, *A Taxonomy of DDoS Attack and DDoS defense Mechanisms*, ACM SIGCOMM Computer Communications Review, Volume 34, Issue 2, pp. 39-53, April 2004
[15] Swain B.R., Sahoo B.S., *Mitigating DDos attack and Savin Computational Time using s Probabilistic approach and HCF method*, Department of Computer Science and Engineering, National Institute of Technology, Rourkela, Orissa.2009 IEEE International Advance Computing Conference(IACC 2009)
[16] Khazan Golriz, Azgomi M.A., *A Distributed Attack Simulation for Quantitative Security Evaluation using SimEvents*, IEEE 2009 Iran university of Science and technology,Tehran.
[17] He Li, Tang Binhua, *Available Bandwidth Estimation and its Application in Detection of DDoS Attacks*, ICCS 2008.
[18] A.Sardana and R.Joshi. *An auto-responsive honeypot architecture for dynamic resource allocation and QoS adaptation In DDoS attacked network*, Computer Communication on Heterogeneous Networking for Quality, Reliability, Security, and Robustness – Part II Elsevier, vol. 32, Issue 12, pp. 1384- 1399.
[19] Deepika Mahajan and Monika Sachdeva. *DDoS Attack Prevention and Mitigation Techniques- A Review*. International Journal of Computer Applications 67(19):21-24, April 2013. Published by Foundation of Computer Science, New York, USA.
[20] The Network Simulator NS-2", http://www.isi.edu/nsnam/ns

BIBLIOGRAPHY OF AUTHOR

Dac-Nhuong Le
He received the BSc degree in computer science and the MSc degree in information technology from College of Technology, Vietnam National University, Vietnam, in 2005 and 2009, respectively. He is a lecturer at the Faculty of information technology in Haiphong University, Vietnam. He is currently a Ph.D student at Hanoi University of Science, Vietnam National University.
His research interests include algorithm theory, computer network and networks security.