International Journal of Grid and Distributed Computing
Vol. 11, No. 3 (2018), pp.23-32
http://dx.doi.org/10.14257/ijgdc.2018.11.3.03

Multi-Phase Detection of Spoofed SYN Flooding Attacks

Namkyun Baik[1] and Namhi Kang[2*]

[1]*Korea Advanced Agency of Convergence Technology, Korea*
[2]*Duksung Womens' University, Korea*
[1]*white-knight@naver.com,* [2]*kang@duksung.ac.kr*

Abstract

This paper proposes a method of establishing an effective network-based countermeasure against distributed denial-of-service (DDoS) attacks utilizing spoofed SYN flooding. In the proposed method, determination of forged traffics involved in an attack is considered as the most important factor, and forged packets are detected through the comparison with normal packets. To eliminate the limitation of conventional countermeasures that normal SYN packets are blocked indiscriminately, comparison of traffic load with sessions was set to be the first step in detection function. To lighten the burden of controlling network nodes and the entire internet, the function of identifying and removing abnormal traffics was proposed based on the investigation of sequence number redundancy and the comparison of time-to-live (TTL) field values, which may be easily realized using a single network-based security device. The multi-phase detection method proposed and tested in the present study greatly increased the web service availability experienced by normal users. Therefore, the method proposed in this paper may significantly contribute to the detection and handling of spoofed SYN Flooding DDoS attacks.

Keywords*: Distributed Denial of Service, SYN flooding, rate limit, Sequence Number, Time To Live*

1. Introduction

Various internet-based services and technologies have been developed, and their variety and rate of advancement are increasing and accelerating. In particular, IoT (Internet of Things) technology has been drawing attention as a new growth engine technology to establish a hyper-connectivity society through mutual connection between all daily life objects. In addition, the IoT technology enables virtual objects that do not exist physically to become subjects of connection and to function intelligently [1]. However, the increase in the number of objects that can be connected to the internet may mean the increase of the targets of cyber-attack and extend the range of threats to cyber security. Further, since the IoT technology is applied to various fields of converged services, including vehicles, homes, appliances, and healthcare, the threat to cyber security is directly linked with not only economic loss due to the exposure of information but also the life of users; therefore, security must be provided to the IoT technology [2, 3].

Distributed Denial of Service (DDoS) attack refers to an attack to disturb the normal operation of a victim's system by causing overload on the network and system through the transfer of massive traffics [4]. Since DDoS attack first appeared in 1996 as a method of exhausting network resources, the scale of DDoS attack and the damage caused by the attack have increased with the development of the internet environment. In particular, the DDoS attack to web servers providing services to unspecified masses is one of the highest

Received (November 26, 2017), Review Result (January 22, 2018), Accepted (January 24, 2018)
* Corresponding Author

ISSN: 2005-4262 IJGDC

threats in terms of information security and invasion effects because of the high performance of internet users' personal computers, the increase of infected botnets, and the expansion of bandwidth and the increased difficulties in chasing liability due to the establishment of giga-lines. However, an effective method of detecting DDoS attacks has not yet been applied successfully.

According to the statistical data for 2017, the share of SYN flooding among the types of DDoS attack was increased from 48% in the first quarter to 53% in the second quarter, and 60% in the third quarter, accounting for about half of the total attacks. SYN flooding attacks where overload is given to channels using spoofed IP addresses without amplification are performed continuously and commonly, rather than server amplification attacks (DNS, *etc.*) where an attacker transmits a large amount of responses to a server for simple request packet transmission [5]. For the detection, network-based security instruments, such as firewall, intrusion detection system, intrusion prevention system, and DDoS equipment, are used. The detection method employed is the TCP/IP (protocol 3/4 layer) abnormal behavior-based statistical 'rate-limit' method. However, statistical methods have limitations as they do not distinguish slow DDoS attacks by multiple spoofed botnets from normal users.

To provide fundamental data that are necessary to establish an effective network-based countermeasure to spoofed SYN flooding DDoS attacks, this study proposes a method of detecting forged packets through the comparison with normal packets, considering that determination of forged traffics involved in an attack is the most important factor.

This study includes five chapters. Chapter 2 describes the conventional representative countermeasures to spoofed SYN flooding DDoS attacks and their limitations. Chapter 3 proposes a multi-phase detection method that may detect spoofed SYN flooding DDoS attacks more accurately, wherein the method includes comparison of traffic load with sessions, investigation of sequence number redundancy, and comparison of time-to-live (TTL) field values. Chapter 4 describes a test where forged packet detection is compared and analyzed between the rate-limit method, the representative method currently commonly employed, and the multi-phase detection method. Chapter 5 presents the conclusion of the present article.

2. Relevant Studies on Spoofed SYN Flooding DDoS Attacks

In the Internet, Internet Protocol (IP) addresses may be privately and dynamically assigned by Point-to-Point Protocol/Serial Line Internet Protocol (PPP/SLIP), Dynamic Host Configuration Protocol (DHCP), and Classless Internet Domain Routing (CIDR). Firewall, Proxy Socket Server, and Network Address Translator (NAT) also enable different hosts to have a same IP address or different IP addresses to be used by a same host. In addition, although a protocol header may not be modified in a general TCP/IP stack of an operating system, any field values can be modified using a network raw socket (pcap library) [6]. Since an IP address is therefore no longer the only identification information, the authenticity of a host may not be determined only by the IP address, which may be easily camouflaged by an attacker without any specific constraints. However, appropriate countermeasures have not been provided against forged IP.

Representative studies on spoofed SYN flooding DDoS attacks and their limitations are described below.

- Ingress/Egress Filtering

This method basically blocks traffic from a source IP address that is out of the network bandwidth assigned by an internet service provider (ISP) [7]. The limitation of this method is that the increase of the processing load on all Ingress/Egress routers slows down the overall transmission speed.

- TCP Intercept

This method connects two terminals through transparent forwarding by intercepting a TCP SYN packet transmitted to a destination, transmitting a TCP SYB+ACK packet to the source, and then considering the connection as normal if an ACK packet is received from the source [8]. However, this method requires connection session management at individual routers, which may exhaust the processing capacity of the routers and decrease the transmission speed due to numerous connections.

- Unicast Reverse Path Forwarding

This method can block the attacks based on the spoofing of source IP addresses, wherein a router receiving a packet confirms the reliability of the source IP address by checking the source IP address and verifying the existence of a reverse path to the IP address [9]. However, the application and realization of this method are limited if the network has an asymmetric network structure with multiple routing paths, but not a single network structure.

The countermeasures to SYN flooding DDoS attacks generally employed by all existing network-based security instruments are based on the rate-limit method that is a statistical method. The rate-limit method limits the number of packets having a specific service or a pattern per unit time, blocking the excessive packets over a certain limit. However, this method has a limitation as it indiscriminately blocks not only abnormal, spoofed packets but also normal packets.

3. Method of Detecting Spoofed SYN Flooding DDoS Attacks

The countermeasure to spoofed SYN flooding DDoS attacks described above is to control all network nodes and the entire internet. However, the method is not employed appropriately because of the insufficient theoretical basis, limitations in each node capacity and processing rate, the need for policy cooperation between ISP enterprises, and other technical constraints that limit the actual application.

Therefore, Chapter 3 proposes a multi-phase detection method that detects spoofed SYN flooding DDoS attacks more accurately in a single network-based security instrument, wherein the method includes comparison of traffic load with sessions, investigation of sequence number redundancy, and comparison of TTL field values.

3.1. Comparison of Traffic Load with Sessions

Since the purpose of a spoofed SYN flooding DDoS attack is to exhaust the communication resources of a web server, sessions are not required by the attacker. Therefore, if the traffic load increases several times more than the increase of the sessions, this can be indicated as an abnormal state with overloads. Assuming that the ratios of traffic load values to sessions, measured over a considerably long period of time, are normally distributed, the range of probability of normal or abnormal traffic values can be expected, based on the mean (a) and the standard deviation (σ) of the traffic load values relative to the sessions, as shown in the table below. For example, if 3% of the values (separated in the '+' direction from the mean) are set to be abnormal ratio values, the overload corresponding to the values (x) is set to be '$a + 1.83\sigma$'.

The overload threshold based on the ratio of traffic to sessions can be used to accurately determine the starting point of an attack by deciding whether a network overload state is caused by a DDoS attack or by a normal flooding of traffic. This reduces the false-positive rate of a security instrument, increasing the product safety and reliability.

Table 1. Normal Probability Values Depending on Distribution Ranges

Distribution range	Normal probability values
≤+0.5σ	0.6915
≤+1σ	0.8413
≤+1.5σ	0.9332
≤+1.83σ	0.97
≤+2σ	0.9772
≤+2.5σ	0.9938
≤+3σ	0.9987

3.2. Investigation of Sequence Number Redundancy

TCP that functions at a level higher than IP, a disconnected service, provides sequence numbers of four bytes to identify the packets with respect to the only connection and secure the sequential transmission of application layers. In other words, to establish a connection for each terminal, an initial sequence number selected for own SYN packet is transmitted, and the value is randomly assigned each time when the system (operating system) or the connection is initialized through the pseudo random number generation (PRNG) function [10]. Therefore, the probability that the initial sequence number is redundant for all the connections is extremely low at 1/232, and there should be no initial sequence number redundancy in the same system. However, the automation tool for spoofed SYN flooding DDoS attacks uses the same initial sequence number in order to improve the packet generation rate.

Hence, redundancy of a same initial sequence number for each connection for more than N times, as set up by the administrator, within an appropriately short time period (The period of attack should be determined by the administrator.) may be detected as a spoofed SYN flooding DDoS attack.

3.3. Comparison of TTL Field Values

A TCP/IP header has filed values designated by the protocol. Almost all operating systems that are generally used conform to the protocol, and the field values having a range generate packets that are defined independently within the range. Therefore, the TTL field values of packets have the initial default values such as 32, 64, 128, and 256 according to the TCP/IP stack of individual operating systems. The table below shows the default TTL values of individual operating systems.

Table 2. The Default TTL Values of Individual Operating Systems

Operating System	Default TTL	Operating System	Default TTL
linux kernel 2.0	64	HP-UX	255
linux kernel 2.2	255	Window 95	32
linux kernel 2.6	64	Window 98	128
Ubuntu	128	Window NT	128
FreeBSD	255	Window Server 2012	128
Solaris	255	Window 10	64

Since a TTL value is reduced by 1 each time a router is passed through, the total hops which a packet has passed through may be calculated by deducting the TTL value at the destination from the default TTL value. In most cases, a TTL field value is not reduced over 30 [7].

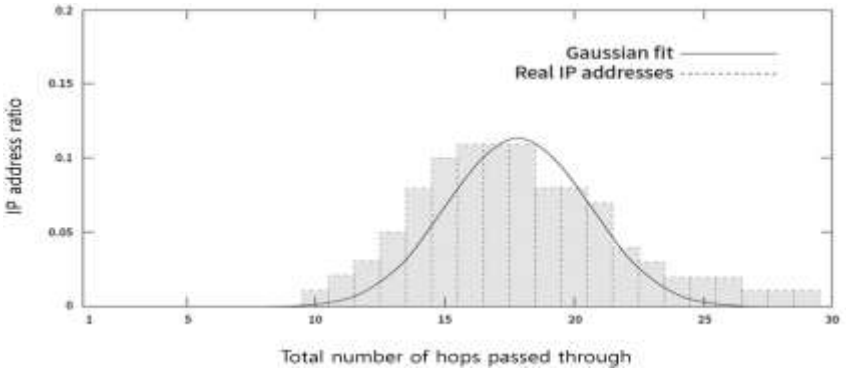

Figure 1. Statistical Data for the Total Number of Hops Passed through as Calculated using Traceroute

The statistical data from the internet show that the total number of hops passed through has a Gaussian distribution as shown in Figure 1, and thus the data can be displayed in a standard normal distribution. Similar to comparing the traffic load with sessions, the ranges of probability values of normal or abnormal traffic can be expected based on the mean (a) and the standard deviation (σ) of the total number of hops passed through, as shown in Table 1. For abnormal TTL field values, threshold values corresponding to an abnormal range may be established. In other words, a TTL field value of a SYN packet out of the range permitted by the TCP/IP stack of the operating system is considered as a spoofed SYN flooding DDoS attack.

3.4. Algorithm of Multi-Phase Detection of Spoofed SYN Flooding DDoS Attack

The multi-phase method for detecting spoofed SYN flooding DDoS attacks is based on the algorithm shown in the figure below.

First, with respect to the input traffic, the traffic load is compared with the sessions, and if the traffic load is abnormal, the detection of spoofed SYN flooding DDoS attacks is initiated. Subsequently, the redundancy of the sequence number is investigated. If the redundancy of the default sequence number is over N times, as set up in advance, and if the TTL field value is greater than a predetermined threshold value for an abnormal range, the packets are removed. Otherwise, the packets are transmitted as normal ones.

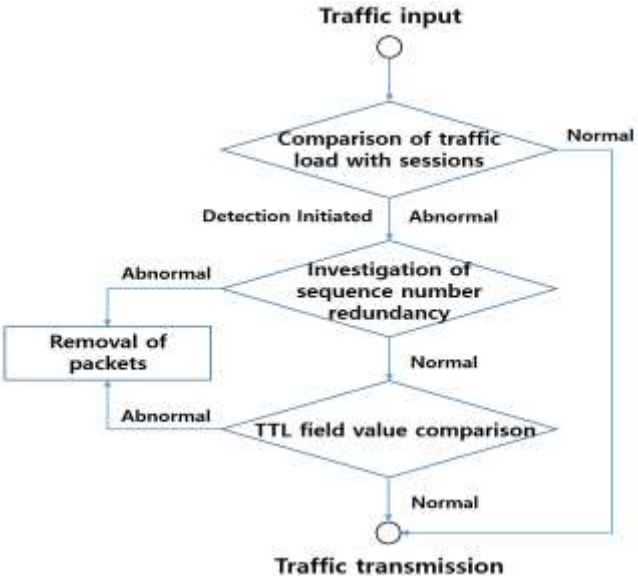

Figure 2. Algorithm of Multi-Phase Detection of DDoS Attacks

4. Evaluation and Review

Referring to the internet attack sources and relevant documents, a SYN flooding DDos tool having the following characteristics was designed and prepared for a test.

Table 3. Syn_Flooding_DDoS.c

Item	Setting
Packet size	54 bytes
Transmission rate	10,000/sec
Source IP address	getrandom (0, 255)
Default sequence number	Fixed (50%), Variable (50%, PRNG)
TTL field values	Normal distributions for 32, 64, 128, and 256

The figure below shows the environment of the simulation and the setting values. A hundred normal users per hour access the web server, and an attacker continuously transmit the SYN flooding DDoS attack packets shown in Table 3. The network-based security instrument selectively uses the rate-limit method and the algorithm proposed in Section 3.4 to compare and monitor the performance of the two methods. The web server, the victimized system, has 10,000 backlog queues, and a web page has five static contents and five dynamic contents to open 10 sessions for one user. The network bandwidth is assumed to be large enough to transmit the packets of normal users and SYN flooding DDoS attacks.

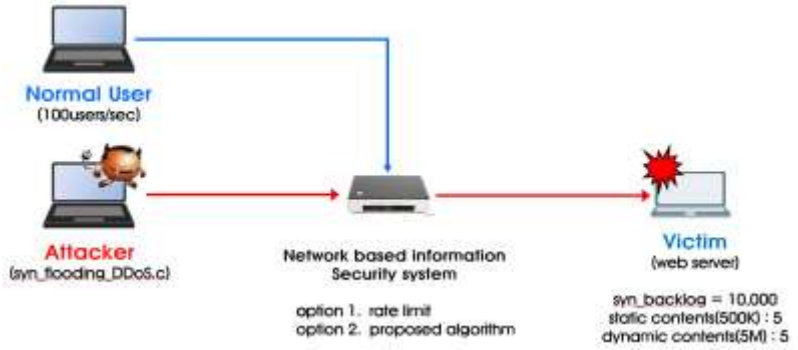

Figure 3. Test Environment

The rate-limit method compared has the SYN flooding DDoS attack setting value of 5,000 SYN packets per second. For the proposed algorithm, the abnormal range threshold for about 30% of traffic load relative to the sessions is set up as 'a + 0.5 σ ,' and the threshold for 10 times redundancy of an default sequence number and TTL field values is also set up as 'a + 0.5σ .'

4.1. Web Service Characteristics-Based Performance Evaluation Index

To provide the evidence that the multi-phase method proposed in this paper for detecting spoofed SYN flooding DDoS attacks is superior in the performance to the rate-limit method that is currently employed by all network-based security instruments, this study applied an web server-centered availability evaluation index that reflects the characteristics of the HTTP protocol; this evaluation index is objective, quantitative, easy to measure, and can be actually experienced by web users. Since a service for a web server includes multiple sessions, if only one of the sessions is omitted, or if a load is generated by the request for retransmission for an omitted session, the web user satisfaction for the quality of the service is significantly decreased. Therefore, the possibility of viewing all documents by being normally connected to a web server at a

desired time is the availability that is actually experienced by web users, and the availability can be evaluated using the evaluation indices [12].

$$\cdot \text{ Service Access Ratio (\%)} = \frac{\text{Number of responded services}}{\text{Total number of serviced requested}} \times 100 \quad (1)$$

$$\cdot \text{ Contents Completeness Ratio (\%)} = \frac{\text{Number of completed contents}}{\text{Total number of contents required by allowed services}} \times 100 \quad (2)$$

※ *Service : A web page requested by a web user to a server. At least one content is required.*
Content : One static or dynamic content (information) in SIP, DIP, Sport, Dport, Protocol ID-based TCP/IP access

The service access ratio in Equation (1) is the ratio of the number of services responded to the number of information provision services requested by a user to a web server. The contents completeness ratio in Equation (2) is the ratio of the completely provided contents to the number of web paged requested by the service.

4.2. Service Access Ratio

The figure below shows the service assess ratio and the content completion ratio of the rate-limit method and the proposed multi-phase method for detecting spoofed SYN flooding DDoS attacks with regard to normal users in the test environment and for the setting values described above.

The rate-limit method allowed service access in the beginning, but the service access ratio was significantly decreased as not only abnormally spoofed packets but also normal SYN packets were blocked indiscriminately from the time when the number of SYN packets per second became over 5,000. On the contrary, the proposed method removed about 50% of the attacking packets through the investigation of the sequence number redundancy and then additionally removed about 30% of the packets through the comparison of the TTL field values, significantly increasing the possibility for the SYN packets of normal users to reach the web server.

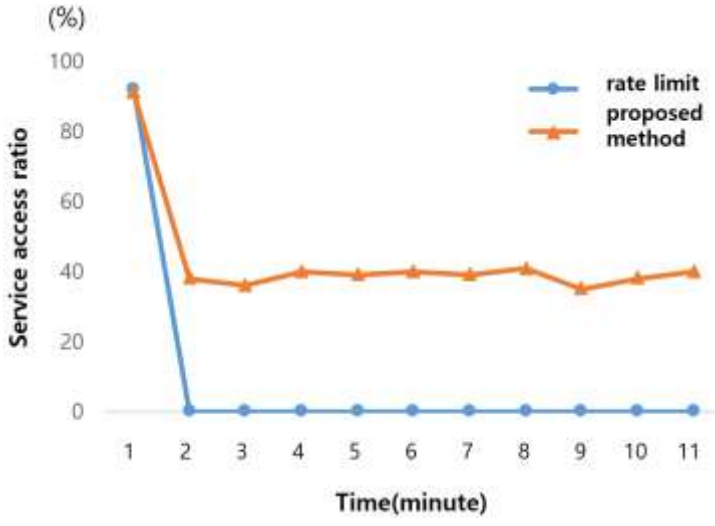

Figure 4. Service Access Ratio over Time

4.3. Contents Completion Ratio

For normal users, both the rate-limit method and the proposed method showed good performance with regard to the contents completion ratio, because the number of sessions downloaded to normal users or the network capacity does not matter significantly once

the packets pass through the filtering of each method. The contents completion ratio was high also because additional SYN packet requests are made continuously until the contents were completed through the retransmission of the TCP/IP stack. However, the contents completion is not very important to the rate-limit method, because the service access ratio was extremely low, as tested before. On the contrary, the proposed method completely provided almost all static or dynamic contents through the access of about 40% and later retransmission, which increased the web service availability experienced by normal users. Therefore, the proposed method may be applied to network-based security instruments to greatly improve the quality of the internet service experienced by users.

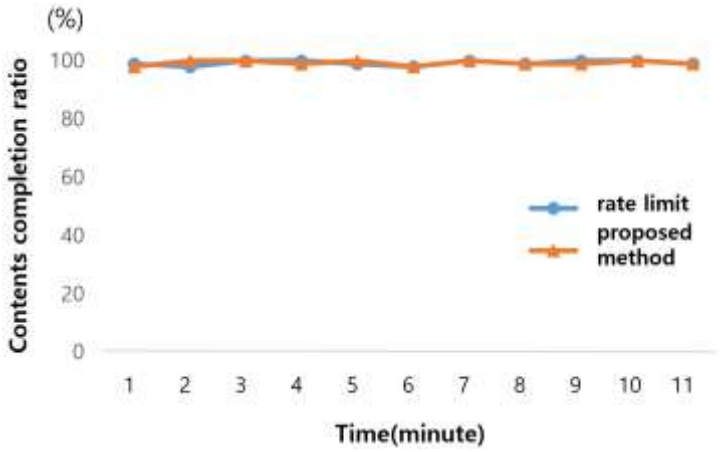

Figure 5. Contents Completion Ratio over Time

5. Conclusions

This study proposed a multi-phase method for detecting spoofed SYN flooding DDos attacks to increase the detection accuracy and improve the web service availability for normal users. To eliminate the limitation of the conventional countermeasures that even normal SYN packets are blocked indiscriminately, the detection function was designed to begin with the comparison of traffic load with sessions. The proposed method includes the investigation of sequence number redundancy, which is easily performed in a single network-based security instrument, to remove the burden of controlling network nodes and the entire internet. In addition, the proposed method includes the comparison of TTL field values to selectively remove abnormal traffic. To show the better performance of the proposed method than the conventional rate-limit method, the performance was tested using service access ratio and contents completion ratio, which are web service characteristics-based performance evaluation indices. The result of the test showed that the proposed multi-phase detection method provided almost all static or dynamic contents through the access and later retransmission, significantly increasing the web service availability experienced by normal users.

Therefore, the result of this study may greatly contribute to the identification and handling of spoofed SYN flooding DDoS attacks. Further studies are currently conducted on a multi-phase detection method at an application level, which is the highest network level.

References

[1] S. Li, L. D. Xu Email and S. Zhao, "The internet of things: a survey", Information Systems Frontiers, Springer, vol. 17, no. 2, **(2015)**, pp. 243-259.
[2] K. Sye Loong, S. S. Kumar and H. Tshofenig, "Securing the Internet of Things: A standardization perspective", Internet of Things Journal, IEEE, vol. 1, no. 3, **(2014)**, pp. 265-275.
[3] J. Park, H. Kwon and N. Kang, "IoT–Cloud collaboration to establish a secure connection for lightweight devices", Wireless Networks, vol. 23, no. 3, **(2016)**, pp. 681-692
[4] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms", ACM SIGCOMM Computer Communication Review, vol. 34, issue 2, **(2004)**, pp. 39-53
[5] "Kaspersky DDOS attacks in Q1 2017 May 11", https://securelist.com/ddos-attacks-in-q1-2017/78285/, **(2017)**.
[6] "Raw Socket", http://msdn.microsoft.com/en-us/library/windows/desktop/ms740463(v=vs.85).aspx/, **(2017)**.
[7] Tao Peng, Christopher Leckie and Kotagiri Ramamohanarao, "Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems", ACM Computing Surveys, vol. 39, **(2007)**.
[8] "Configuring TCP Intercept (Preventing Denial-of-Service Attacks)", https://www.cisco.com/c/en/us/td/ docs/ios/12_2/security/configuration/guide/fsecur_c/scfdenl.html?dtid=osscdc000283/, **(2014)**.
[9] "Unicast Reverse Path Forwarding (uRPF) Enhancements for the ISP-ISP Edge" https://www.cisco.com/ c/dam/en_us/about/security/intelligence/urpf.pdf/, **(2005)**.
[10] "RFC 1948 : Defending Against Sequence Number Attacks", http://www.ietf.org/rfc/rfc1948.txt?number=1948/, **(1996)**.
[11] W. Hainging, J. Cheng and S. Kang, "Defense against spoofed IP traffic using hop-count filtering", IEEE/ACM Transactions on Networking, vol. 15, **(2007)**.
[12] N. Baik and S. Jung, "Operation Policy for Enhancing Availability of a Web Server against DoS Attacks", The Journal of Korea Information and Communications Society, vol.33 no.8, **(2008)**, pp. 735-744.

