DoS Attack Prevention Using Rule-Based Sniffing Technique and Firewall in Cloud Computing

Kagiraneza Alexis Fidele[1,2*], and *Agus* Hartanto[2]

[1] Data Entry and Update Taxpayer's Registry in Rwanda Revenue Authority (RRA) Kigali-Rwanda
[2] Master of Information System, School of Postgraduate Studies Diponegoro University, Semarang – Indonesia

Abstract. Nowadays, we are entering an era where the internet has become a necessary infrastructure and support that can be applied as a means of regular communication and data service. In these services, cloud-based on servers has an essential role as it can serve numerous types of devices that are interconnected with several protocols. Unfortunately, internet cloud servers become the main target of attacks such as Denial of Service (DoS), Distributed Denial of Service (DDoS). These attacks have illegal access that could interfere in service functions. Sniffing techniques are typically practiced by hackers and crackers to tap data that passes through the internet network. In this paper, sniffing technique aims to identify packets that are moving across the network. This technique will distinguish packet on the routers or bridges through a sniffer tool known as snort connected to a database containing the attack pattern. If the sniffing system encounters strange patterns and recognizes them as attacks, it will notify to the firewall to separate the attacker's original Internet Protocol (IP) address. Then, communication from the attacker's host to the target will be discontinued. Consequently, the identified attack activity will stop working, and the service will proceed to run.

Keywords: **Security; Sniffing and Firewall; Denial of Service attack prevention.**

1 Introduction

In the latest technology, cloud computing performs a significant function in administering access to information resources instantly as desired by end-users. If users wish to communicate or obtain information resources, they necessitate the internet; here, the cloud enables its customers to use widely distributed resources on the internet to do computations. Nevertheless, the big hurdle is that security usually becomes a problem in the development of cloud computing [1].

In order to improve reliability and mitigate information system security risks, various techniques must be implemented immediately [2]. The objective of advancing the security of cloud computing is to preserve data confidentiality, integrated integrity, availability of information resources, and data accountability. Security is all needed in cloud computing, but availability is the most important thing because the primary function of cloud computing is to give services. Cloud customers demand to process information, store, and share data. Herewith, the user will suspend disbelief if the service in clouding system is inaccessible [3, 4].

At present, many people depend on information sources and communication activities in data-based environments. Clouding systems are advantageous as they can connect technology that accommodates the data and services. Because of the service's capabilities, the cloud has long been a target by trespassers in overworking information and causing cloud computing systems unavailable to users. There are numerous types of attacks in cloud computing, and most of the attacks that cause network failures are Denial of Service (DoS) attacks and Distributed Denial of service (DDoS) [1, 5, 6, 7]. The leading disturbing cause for data availability is DDoS attacks [8].

These attacks intend to reduce network performance reasonably, through circumstances where the intended user cannot access the network. The primary purpose of DDoS is to make resources unavailable for use [9, 10]. DoS attacks accomplish this by flooding the target with traffic or sending it information that triggers a crash [11]. As a result, DoS attacks lessen network performance by targeting network bandwidth or connectivity as the victims of attacks [12].

The main target of DDoS attacks in the cloud computing environment varies, such as the types of TCP/IP services (such as web servers and FTP servers), CPU storage, and other network resources [13, 14]. Attackers can entirely reduce network performance at the expense of victims from different hosts. Attackers use techniques to scan networks, then locate machines that have the potential to have vulnerabilities. Then, the attacker uses this machine as an agent.

* Corresponding author: alexkagiraneza@gmail.com

Various protection techniques can be done to avoid DoS attacks. In this paper, we propose a system using a packet sniffer (SNORT). This system will help distinguish the characters of DoS attacks. SNORT identifies the type of attack, then captures it and transfers the packet to the firewall system. The firewall system will discard packets across the network.

1.1 Related work

1.1.1 Sniffing

Sniffer is a program that can read and analyse any data packet and protocol that passes through the machine where the application is installed. By default, a computer on a network (workstation) only listens and responds to packets that already sent. However, a sniffer with such designs will be capable of monitoring and capturing all the network traffic that passes without considering the package's recipients. This method is designated as sniffing [15].

In order to be able to read and analyse each protocol that passes through the machine, a program needs to transfer the packet back to the attacker's computer. An attack conducted by a computer is called a spoofing attack. The attacker will act as a Man-In-the-Middle Attack [16].

1.1.2 IP spoofing

The basis of IP spoofing is to hide or forge the source IP address of packets, so that the source of the network package cannot be traced, thus tricking the destination computer. People who send out DoS (Denial of Service) attacks habitually disguise the targeted PC by covering the IP header and supplanting it with the different IP header. Some common models of attack are Ping of Death, Syn Flood, Land Attack, and Teardrop [17].

1.1.3 Type of DoS attacks

In general, there are various types of DoS attacks [18]:

a. Volume Based Attack
   This type of attack includes UDP floods, ICMP floods, and other fake flood packets. This type of DDoS attack is targeting the bandwidth of the site attacked. The number of attacks is volume-based and usually measured in Bits per second.
b. Attack Protocol
   This type of DDoS attack consumes resources on its server, or intermediate communication equipment, such as routers, load balancers, and even some firewalls. Some examples of protocol attacks include SYN floods, fragmented packet attacks, Ping of Death, Smurf DDoS, and many more. Protocol attacks are usually measured in Packages per second.
c. Application Layer Attack
   It is probably the most dangerous type in a DDoS attack. Application layer attacks consist of requests that resemble to be genuine and reliable. This attack aims to destroy the webserver. Examples of attacks on some application-layer attacks are Slowloris, Zero-day DDoS attacks, DDoS attacks that target Apache, and operating system vulnerabilities. The type of attack is measured in Requests per second.

1.1.4 Example of DoS

Examples of DoS attacks are as follows [19, 20]:

a. SYN Flooding, TCP is sending SYN data with a fake address;
b. Teardrop Attack sends IP packets with confusing offset values;
c. Smurf Attack sends a large volume ICMP packet with another host address;
d. Ping of Death uses a ping utility that found on a computer operating system;
e. Remote Controlled Attack controls several other networks to attack the target;
f. UDP Flooding utilizes the UDP protocol, which is connectionless to attack the target; and
g. ICMP Flooding.

There are various types of methods proposed by various researchers to anticipate security problems in cloud computing, especially in DDOS [21, 22].

Moreover, there are various types of Distributed Denial of Service attacks and Denial of service attacks in different layers' protocols of sensor networks [23]. Different mechanisms are designed for improving security for network routing protocol sensors, botnets that contain a system of different types of tools and thorough installation that can be controlled based on systems Internet Relay Chat (IRC) [24, 25].

According to Patil, a designed immune system for DoS attack on wireless sensor networks, the Co-FAIS immune system improved learning parameters in the fuzzy system. An improved capability of learning also improves the accuracy rate of detection. In this system, six modules proposed: Sniffer Module (SM): it captures the packets that pass across the network and pre-process to Fuzzy detection. Fuzzy Misuse Detector Module (FMDM): it plays a role to identify packets, the incoming packets, and standard packets. Danger Detector Module (DDM): when the attack fails (defended or detected), the module calculates the difference between parameters of malicious packets and normal packets. Fuzzy Q-learning Vaccination Module (FQVM): it is an algorithm used to defend an attack; it consists of a Fuzzy controller which converts the continuous inputs into the fuzzy set. Cooperative Decision-Making Module (Co-DMM): the module combines the output from FMDM and FQVM detector; analysis the source of the attack and gives sharp results. Response Module (RM): this module modifies the hosts in a network or updates database. It produces an attack signature and eliminates it from the safe list to make a detection faster [26].

The above mentioned are modules of the immune system for DoS on WSN. However, the mechanism of cloud computing will not be safe if they only use these modules considering DoS security is challenging to disclose. Therefore, we proposed the SNORT packet

sniffer. By utilizing this package, the system will instantly identify the type of attack and swiftly provide information to the firewall to discard attacks.

2 System design and method

We designed a system that can combine packet sniffing and firewalls so that all packet forms will be transported into the network system [27]. If a package appears, the network goes down, and online services cannot be accessible to users. In this system, we designed packet sniffing. The system can identify packets that move across the network layer from the Transmission/Internet Protocol (TCP/IP) Control Protocol. As in Fig. 1 below, a service failure occurs when a packet befalls.

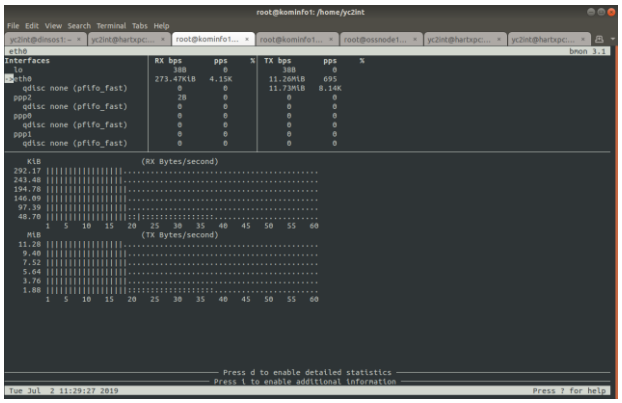

Fig.1. Bandwidth monitoring

As explained in Fig. 1 earlier, there appears to be an abnormal surge in bandwidth traffic. It also shows that DoS attacks have successfully caused the network busy, so accessing the server through the network will be extremely slow, and requests from users will be inaccessible.

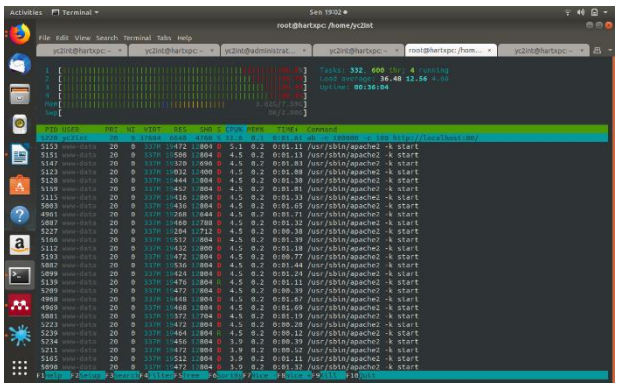

Fig.2. System resource monitoring

In Fig. 2, the output from htop shows that there is an abnormal surge in processor and RAM usage. It indicates that a DoS attack is occurring on server services and causes the Apache webserver to be very hectic toiling requests from attackers. As a result of a very busy server, requests from real clients cannot be completed.

The system sniffing package captures all incoming traffic and captures packets within the allotted time. After a suspected packet is transported to the firewall for the detection process, problems continue to occur in the package. There is an order to attack the services requested by the client; this results in a disruption to online service sources. Following, we will explain how firewall system security works.

2.1 Intrusion detection system (IDS) using SNORT

SNORT is an open-source network intrusion detection system (NIDS) and intrusion prevention system (IPS) [28]. Snort was developed for the first time in 1998 by Martin Roesch, who could analyze real-time traffic and package logging on Internet Protocol (IP) networks.

The role of Intrusion Detection System is to recognize that a computer system is under attack. Intrusion Detection System is not only used to detect seizures but also can contribute with forensic information that allows identifying the source of the attack. SNORT has the characteristics, as follows:

a. Portable for many operating systems, has been ported to Linux, Windows, OSX, Solaris, and BSD;
b. Small size and light;
c. Fast-Snort can detect attacks on the 100 Mbps network;
d. Can make our own rules to detect new attacks;
e. Snort is an open-source and under GPL license.

Snort is software used to detect and analyze intruders and various types of traffic attacks in real-time. Snort is not limited to protocol analysis or intrusion detection systems (Intrusion IDS Detection System, but a combination between these two is beneficial in response to incidents of attacks on the host network host. The Snort feature can be a helper system administrator and network; it can advise us of intruders who have inherent dangers.)

These features present Snort a network detection and attack detection system; this is undoubtedly very useful for incident response teams. Snort can now operate with four (4) fruit modes:

a. Package sniffer: Practical reading packages from the network and show us inside the form of unbroken flow on the screen;
b. Packet logger: to record all packages that are pass on the disk;
c. Network Intrusion Detection System (NIDS): detection of intruders on the network: in this mode, Snort will perform to detect attacks done through computer networks;
d. Inline Mode, take packages from iptable and command the iptable to continue the package based on the type of rule from Snort used.

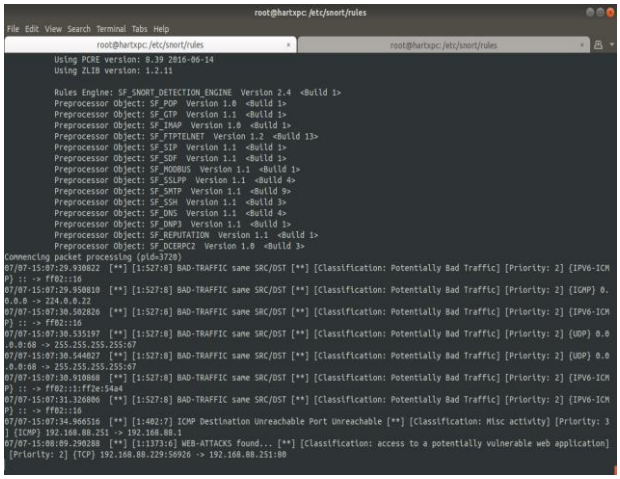

Fig.3. Snort system

2.2 Firewall mechanism using Linux

Networks play a critical role in the digital world. With networks, users can communicate and share data. Because of this serviceableness, networks became the main target of attacks. For maintaining network security from attacks, special techniques must be applied so that attacks and other dangerous threats can be prevented. A firewall is a tool designed to prevent illegal access from private networks [29].

An attacker can practice various ways to access classified information, and a firewall is a solution to specific attacks [30]. The implementation of a firewall can ensure network security in the same way; the firewall will not allow malicious packages to access through protected networks [31].

The primary function of the firewall is to block various types of interference originating from the internet. In Fig. 4 below, we use Linux as a firewall that can filter the Internet Protocol and IP 2 as routing, illustrated as follows:

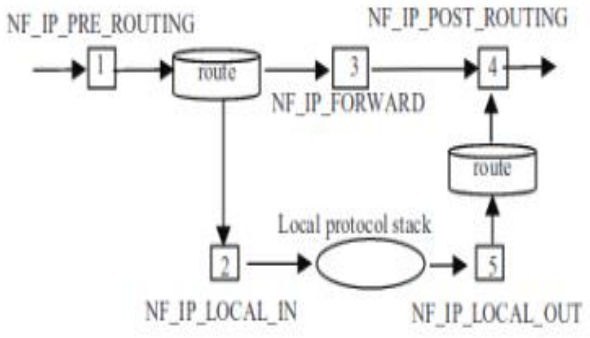

Fig.4. Firewall Mechanism

Packages go through the pre-routing-forwarding and post routing processes. The package goes to Linux IP (NF-IP-LOCAL-IN), and the packet exits from Linux IP (NF-IP-LOCAL-OUT) will then be processed after the routing process. In this case, the firewall system enhances security on the network and proceeds to carry out operations.

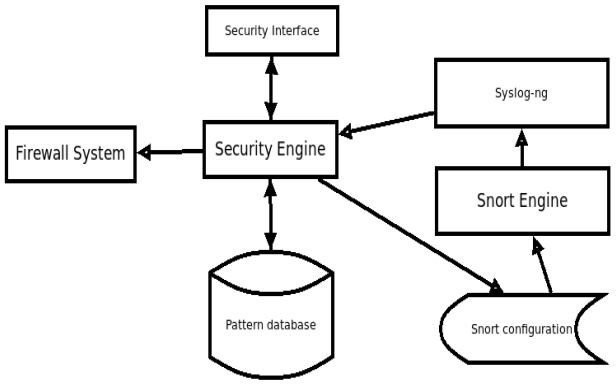

Fig.5. Proposed System

The Security Engine is the central controller of the system we propose. This security engine will handle the Security Interface, firewall system, pattern database, and snort engine. Security Interface is an interface that is serviceable for interacting with network system administrators, configuration adjustments, and monitoring processes. The security engine will translate the execution ordered by the system administrator through the security interface.

The administration system will also monitor through a security interface, the result of processing data, and information from the security engine. On the other hand, the pattern database will be saved into the database engine, for example, MySQL, and MongoDB.

Later, the Security engine will produce a snort configuration based on the patterns stored in the database. After the snort configuration is made, the snorting engine will read and run the sniffing and matching patterns. The output from snort is log alerts, then sent to Syslog-ng. The security engine reads the output of Syslog-ng, which must be translated and then gives instructions to the firewall system to reject or drop all packets originating from the source IP address indicated as an attacker. For more detail can be seen in the rule-based diagram in Fig.6.

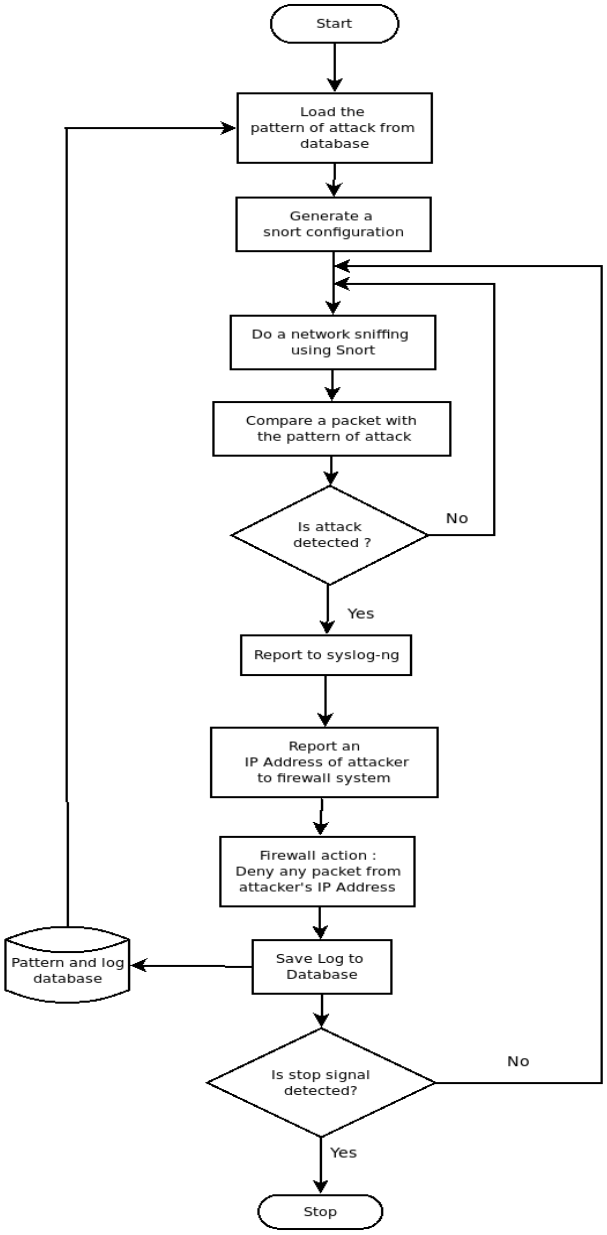

Fig.6. Diagram of rule-based system flow

3 Results and discussions

Security in the digital world for people is paramount — especially nowadays, with cloud computing, which allows users to access resources easily. The internet is the main target of attacks, so various schemes of services become unavailable to customers. Special techniques are needed to deal with and prevent Denial of Service or DoS attacks. As shown in Fig. 2, the system resource monitoring shows how the service runs abnormally when a DoS attack occurs on network services and makes it very busy serving attacker requests. In Fig. 3 shows how the SNORT system technique identifies DoS attacks in real-time.

When an attacker sends a malicious packet into the system, Packet sniffing (SNORT) will understand the type of attack. Then when the packet sniffer has captured the dangerous package, it transfers the package to the Detection firewall system. As a result, like a firewall system in Fig. 4, the security engine will act as a central system controller that controls other parts of the system and makes each activity rerun.

Communication continues between the Security Interface, pattern database, and snort engine. The output comes from snort is log alerts, then sent to Syslog-ng. The security engine gets information from Syslog-ng, later the data information must be identified. The results of the identification are in the form of instructions. The instructions are then forwarded to the firewall to prevent all attacks. Then finally, the availability of secure network services can be accessed by users.

4 Conclusion

Cloud internet, with excellent service for its users, is a technology facility that is very valuable for people's daily lives. Cloud allows its customers to use widely distributed resources through the internet to perform computation. Various types of attacks will be a big problem when services on cloud computing unavailable to users. On the other hand, security is an essential feature so that the cloud internet can provide services effectively and efficiently. In this study, the Sniffing technique was proposed to identify the types of DoS attacks.

The packet sniffer (SNORT) successfully identifies the attack, then captures the malicious packet and then transfers it to the firewall system so that the attack can be controlled immediately. Sniffing (SNORT) techniques and firewall systems can enhance service availability. This research is expected to motivate researchers in the future. Better and stronger security mechanisms hopefully can make the internet network system more trustworthy.

References

1. Y, Qiao, Yu, F. Richard, *Distributed Denial of Service Attacks in Software-Defined Networking with Cloud Computing*, IEEE Communications Magazine **53**(4), 52-59 (2015)
2. A.H. Paul, *Industrial-Strength Firewall Topologies*, Information Systems Security **14**(2), 20–26 (2005)
3. Z. Xiao, Y. Xiao, *Security and Privacy in Cloud Computing*, IEEE Commun. Surveys & Tutorials **15**(2), 843–59 (2013)
4. S.T. Zargar, J. Joshi, D. Tipper, *A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks*, IEEE Communications Surveys & Tutorials **15**(4), 2046-2069 (2013)
5. R.V. Deshmukh, K.K. Devadkar, *Understanding DDoS Attack & Its Effect in Cloud Environment*, Procedia Comput. Sci **49**(1), 202–210 (2015)
6. Radware Ltd, *DDOs Attack Survival Handbook, Chicago: Radware*, CSUSB (2013)
7. X. Geng, Y. Huang, A.B. Whinston, *Defending Wireless Infrastructure Against the Challenge of DDoS Attacks*, Mobile Networks and Applications **7**(3), 213-223 (2002)

8. R. Mehta, *Distributed Denial of service Attacks on Cloud Environment*, Int. J. Adv. Res. Comput. Sci. **8**(5), 2204–2206 (2017)
9. B. Santhi, G.J. Bharathi, *Study on Distributed Denial-of-Service Attack,* Research Journal of Applied Sciences **4**(10), 1366- 1370 (2012)
10. Y. Xie, S.Z. Yu, *Monitoring the Application-layer DDoS Attacks for Popular Websites*, IEEE/ACM Transactions on Networking **17**(1), 15-25 (2009)
11. S.T. Zargar, J. Joshi, D. Tipper, *A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks*, IEEE Communications Surveys & Tutorials **15**(4), 2046-2069 (2013)
12. S. Patil, S. Chaudhari, *DoS Attack Prevention Technique in Wireless Sensor Networks*, Procedia Computer Science **79**, 715–721 (2016)
13. J. Arzamendia, F. Lopez-Pires, *Distributed Denial of Service Attacks in Cloud Computing: A Literature Review,* Int. J. Enhanc. Res. Manag. Comput. Appl. (2016)
14. K.H. Alotaibi, *Threat in Cloud- Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attack , and Security Measures*, J. Emerg. Trends Comput. Inf. Sci. **6**(5), 241–244 (2015)
15. S. Ansari, S.G. Rajeev, H.S. Chandrashekar, *Tips on How to Get the Network Interface*, Internetworking Res. Exp., 17–19 (2003)
16. S. Schuckers, *Spoofing and Anti-Spoofing Measures*, Information Security technical report **7**(4), 56-62 (2002)
17. M. Darwish, A. Ouda; L.F. Capretz, *Cloud-based DDoS Attacks and Defenses*, International Conference on Information Society (i-Society 2013) IEEE, 67-71 (2013)
18. M. Monika, Y. Singh, *A Review: DoS and DDoS Attacks*, International Journal of Computer Science and Mobile Computing **4**(6), 260-265 (2015)
19. M. Darwish, A. Ouda; L.F. Capretz, *Cloud-based DDoS Attacks and Defenses*, International Conference on Information Society (i-Society 2013) IEEE, 67-71 (2013)
20. E. Alomari, et al., *Botnet-Based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art*, arXiv preprint arXiv:1208.0403 (2012)
21. G.J. Han, W. Shen, Q.D. Trung, et al., *A Proposed Security Scheme Against Denial of Service Attacks in Cluster-Based Wireless Sensor Networks*, Security and Communication Networks (2011)
22. D. Raymond, S.F. Midkiff, *Denial-of-service in Wireless Sensor Networks: Attacks and Defenses*, IEEE Pervasive Computing **7**(1), 74-81 (2008)
23. M. Li, I. Koutsopoulos, Network *Defense Policies in Wireless Sensor Networks,* Network **9**(8), 1307–1315 (2010)
24. Z. Cao, X. Zhou, M. Xu X, et al., *Enhancing base station security against DoS attacks in wireless sensor networks*, IEEE Wireless Communications Networking and Mobile Computing. 1-4 (2007)
25. C. Douligeris, A. Mitrokotsa. *DDoS attacks and defense mechanisms: classification and state-of-the-art*. Computer Networks **44**(5), 643–666 (2004)
26. S. Patil, S. Chaudhari, *DoS Attack Prevention Technique in Wireless Sensor Networks*, Procedia Computer Science **79**, 715–721 (2016)
27. N.P. Patel, R.G. Patel, D.R. Patel, *Packet Sniffing : Network Wiretapping Packet Sniffing : Network Wiretapping*, Researchgate (2014)
28. J. Carr, *Snort: Open source network intrusion prevention*, Esecurity Planet (2007)
29. Y, Yu, Y. Li, Y. Deng, *Study on Linkage Mechanism of IDS and Firewall Based on SNMP Protocol*, Procedia Engineering **29**, 3424–3428 (2012)
30. M. Imran, A.A. Alghamdi, B. Ahmad, *Role of firewall Technology in Network Security*; IJIACS **4**, 3–6, (2015)
31. Q.-X. Wu, *The Research and Application of Firewall based on Netfilter,* Phys. Procedia **25**, 1231–1235 (2012)