An Adaptive SYN Flooding attack Mitigation in DDOS Environment

Khalid Hussain, Syed Jawad Hussain, Veena Dillshad, Muhammad Nafees, Muhammad Awais Azeem
Computer Science & Engineering Department HITEC University Taxila, Pakistan

Abstract
A honeypot being an information security server attract the hackers towards it by showing open ports and services and monitor network traffic closely by playing some key feature roles: divert malicious traffic from valuable network machines, do in depth analyses of malicious traffic by generating early warning about new attacking techniques. This research has been done to mitigate SYN Flooding attack in DDOS environment. Most of the previous research has been conducted to mitigate DDOS attack, specifically for SYN Flooding attack there is still a room to enhance with respect to latest techniques. In this research a three way counter algorithm has been presented to mitigate SYN flooding attack. This algorithm is based on windows advance firewall rules. This work is enhancement of the firewall capabilities to identify SYN flooding attack. The proposed work evaluate in DDOS environment, result show the 97.5% identification, detection and mitigation of SYN Flood attack in DDOS environment.

Keywords
DDOS, SYN flooding, malicious traffic, honeypot

1. Introduction

From past to up till now security is a very big issue for each individual organization because hackers can hack information using different techniques due to which organizations will lose their important data. By using honeypot intruder will be determine and block to hack information. This technique will help organizations to safeguard their valuable information from intruders.
With the increased connectivity of computer systems, the emergence of the Internet and the high sense of security, there is no doubt about the need for security measures for protecting organization's systems and information.
Honeypot is a device that can maintain log and monitor each and every malicious activity performed by the intruder by designing it in a way that it seems ordinary to the intruder. Honeypot is an exclusive device that can allow a security specialist to examine activities performed on compromised machine by an intruder without notifying or affirming attacker that they are being examined. Due to this nonappearance, valuable information can be gained about actual planning of a hacker.

Honeypot is designed in a simplistic way that it becomes beneficial for the user. One point of preference is the way that a honeypot gathers little arrangements of information. Like other security devices, honeypots maintain record of everything that it interacts with. The genuine point of interest of honeypots however is that they are intended to just have connection with malicious users. Thusly, honeypots gather littler data sets of information with high esteem. Likewise, by catching anything they interact with, honeypots can distinguish any new instruments or advances utilized by hackers. The most essential and valuable point of preference is its effortlessness. With this, the assets required are negligible. This reductions cost in deploying a honeypot in light of the fact that a costly, effective PC is not much required. Honeypots are additionally less inclined to commit errors or be misconfigured.

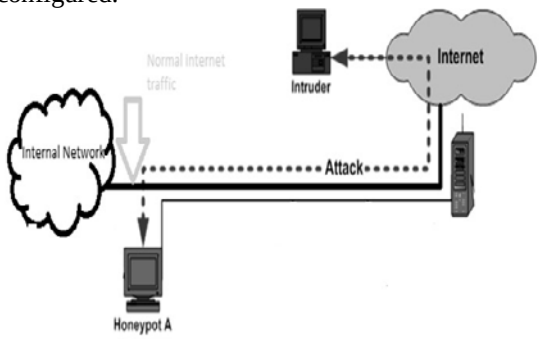

Figure 1 Framework of Honeypot

This diagram will basically represent general framework of our honeypot. If some intruder will intrude through internet into local area network it will be redirected towards honeypot where useful forensics will be done against each attack and understand behavior of attacker whereas normal traffic will be directed towards LAN.

The main idea for deploying the honey pot is to look for the attacks which are done for compromising the network for gaining confidential information. Previously work done on honey pot, but there are some gaps which may require to high lightened for improvement. Up till now all Honey pots are made generally for all type of attacks due to which they didn't give accurate results. To overcome this problem specific attack related Honeypot is to be designed to get more efficient results. This honeypot is

Manuscript received July 5, 2016
Manuscript revised July 20, 2016

specially designed to detect and mitigate SYN Flooding attack in DDOS environment. The main focus will be to make sure that the implementation of honey pot should completely result in detecting the attack by the intruders in an effective manner.

At the point when an intruder endeavors to break a Honeypot, assault related data, for example, the IP location of the intruder, will be acquired. This movement done by the aggressor gives profitable data and examination on assaulting procedures, permitting framework to back track the association and to search for the interlopers.

Honey pots could add to the accompanying three key parts of security:

- **Prevention**: Honeypots are used to intact with intruders and give them a feel that they can attack organization through honeypot. Once the intruder is completely engaged then honeypot will use different methods to prevent organization from their intrusions.
- **Detection**: honey pots can play major rule in this area; it supplements the identification capacities of existing IDS. Honeypots don't have these lacks since all inbound movement are for certain scans, while outbound activity shows a compromised machine; in addition, there is no compelling reason to overhaul attack signature database since honeypots identify interruption by checking exercises versus depending on an attack signature database.
- **Reaction**: honey pots can also play major rule in this area, at the point when a machine is attacked, methodology can be utilized for valuable legal sciences data in light of the fact that either the information is as of now intensely contaminated, or the machine can't be ceased, or both. Be that as it may, a honeypot has been embedded into a system of web servers, which is presently traded off; the occurrence reaction group could simply expel honeypot logged off, and by taking a gander at the harms in the honeypot.

2. Related Work

'SYN-FIN' pair behavior is used for SYN flood attack detection which can stable under different approach models [1].This paper presented a simple and robust SYN flooding detection to be installed at leaf routers that connect end machines to the internet. Simplicity of this mechanism is statelessness and low computation overhead.

Bloomed Filter based approach is used for detection of SYN flood attack [2]. This paper presented a novel detection method against DDOS attack. Proposed technique will give accurate results for little storage. Detection mechanism is not tested in real environment.

Three Counters Algorithm is used for SYN flood attack detection [3]. In this work detection scheme uses valid SYN-FIN pair's behavior for detecting various SYN flood attacks. Proposed work is not tested in real environment and not catering legitimate users under this algorithm.

Review various SYN flooding attack detection schemes [4]. In this work advantages and disadvantages of each scheme is analyzed and critically examined. Detection schemes base on Router data structure; statistical analysis of packets flow, artificial intelligence can be deeply analyzed.

OPNET modeler simulation environment is used for SYN flooding attack analyses [5]. In this paper

Adaptive threshold and CUSUM algorithm is used for detection of SYN flood attack and for mitigation LINUX firewall is used. Dramatically deteriorated results are obtained while simulation of SYN flood attack is conducted.

Python script is used for SYN flooding attack generation and for detection Wire shark is used [6]. In this work firewall script are written using command line tool IP Tables in Linux for prevention of attack.

Linear prediction analyzes technique is used for detection of SYN flooding attack [7]. This methodology is applied at leaf routers and firewalls to discover the attacking methodology. Linear prediction makes use of exponential back off property of TCP used during timeouts. This approach can be used to detect only low intensity base attacks.

Non parametric CUSUM cumulative sum algorithm is used for SYN flooding attack detection [8]. By using this algorithm less false alarm and high detection ratio is achieved. DARPA SYN flooding attack data set is used which represents Tcpdump and audit data generated over five weeks of simulated network traffic in a hypothetical military LAN.

Learning Automata algorithm is used for detection of SYN flooding attack [9]. This paper proposes a self-managing approach, in which host defends by dynamically tuning its two parameters that is m (maximum no of half open connections) and h (hold time of each open connection). Simple queuing model is used to show network metrics under attack. By merging Packet filtering technique with this algorithm will give perfect results for future.

Transparency protocol is used for solving problem of high speed traffic in DDOS attack [10]. Transparency protocol works on the originality of data in this way source and destination address could be used as unique labels for the end system.

C language script is used for attack generation and Wire shark is used for attack detection [11]. In this work

experiment is done to generate SYN flood attack and estimate packet rate per second at victim server.

Plan inspects TCP fragments to discover no less than one of numerous ACK sections originating from the server [12]. In this paper author propose an accurate sampling scheme for detecting SYN flooding attack as well as TCP port scanning activity. Proposed methodology depends only on sampling rate regardless on the sampling method.

Fuzzy logic based system is used to detect SYN flooding attack [13]. Performance of the proposed system is compared with Cumulative Sum algorithm. Simulation base work is done which shows performance of Fuzzy logic algorithm better than CUSUM algorithm.

Intentional dropping based filtering technique is used for mitigating SYN flooding attack [14]. In this work main technique is to drop first SYN packet against each connection request. Rests of the SYN packets are transmitted only if they match TCP's timeout mechanism. Proposed technique will in connection establishment latency due to effective reducing attackers attack rate.

Ad hoc flooding attacks are analyzed [15]. In this work an FAP (Flooding attack prevention) mechanism is used for defense against Ad hoc flooding attacks. At the point when the attacker sends numerous assaulting DATA bundles to the victim machine, the machine may remove the way and does not set up a way with the gatecrasher any more. Mobile ad hoc networks can prevent ad hoc flooding attack by FAP with minimal overhead.

3. Attack Generation Using Tool Base Approach

During tool base testing following tools and OS will be used:

- Ettercap
- Hping3
- Wireshark

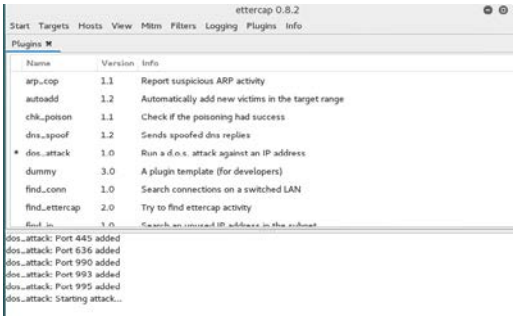

Figure 2 Attack Generation Using Ettercap

SYN flooding attack is generated using Ettercap tool on a victim machine in LAN. This attack is done on specific ports of victim machine and analyzes behavior of attack using Wire shark.

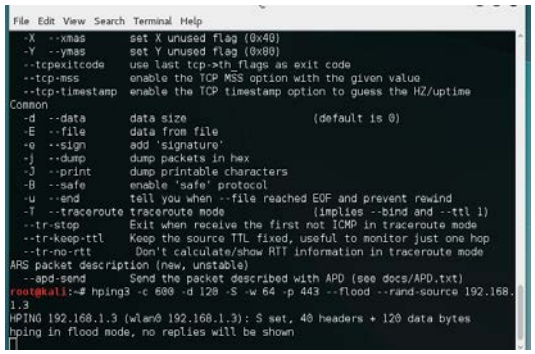

Figure 3 Attack Generation Using HPING3

Another tool HPING3 is used to generate SYN flooding attack on victim machine on a LAN to analyze which tool is better to flood more SYN packets on victim machine. Detection of attack is done through Wireshark and analyze that HPING3 will generate more no of SYN packets on victim machine.

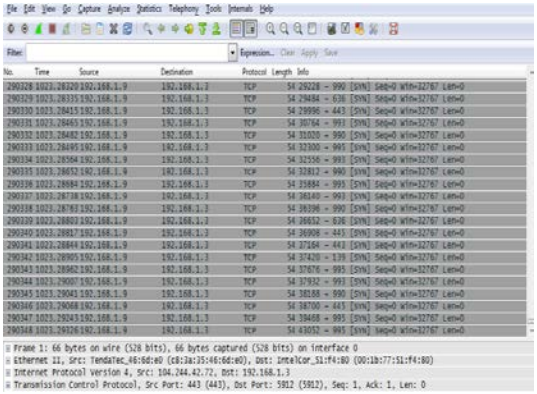

Figure 4 Attack Detection through Wireshark

After generating SYN flooding attack from both Ettercap and HPING3 tool, behavior of attack is analyzed through Wire shark. Wire shark will show source and destination IP addresses from which attack is generated and detected and also show ports being attacked.

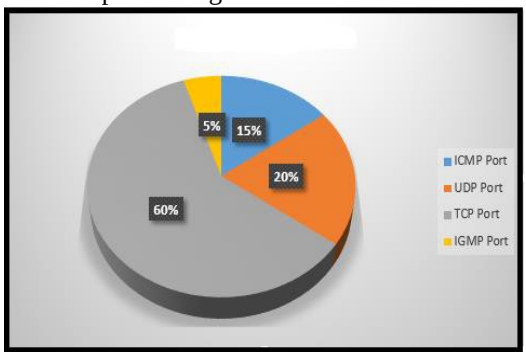

Figure 5 Attack Detection Results

4. Proposed Methodology

This research has been done to mitigate SYN Flooding attack in DDOS environment. Most of the previous research has been conducted to mitigate DDOS attack, specifically for SYN Flooding attack there is still a room to enhance with respect to latest techniques. In this research a three way counter algorithm has been presented to mitigate SYN flooding attack. This algorithm is based on windows advance firewall rules. This work is enhancement of the firewall capabilities to identify SYN flooding attack.

4.1 SYN Flooding Attack

The SYN Flooding attack is also known as "half open attack" because in this attack a complete 3 way handshake is not completed towards by the client. In a normal 3 way handshake the client should return the ACK(acknowledgement) packet to the server for secure communication whereas in SYN flooding attack the client first send the information to the server for starting a communication between each other, in respond to which server will send the ACK packet back to the client and wait for the client that the client must send him ACK packet to start a communication but the client would not sent the ACK packet towards the server and hence a communication barrier occurs. While server is waiting for the client ACK packet a bunch of fake IP addresses are generated by the client to busy the server so that it could make his job done, whereas it is impossible for the server to close down the requests by sending RST (reset) packets back to the client until or unless the connection time was not out. Under these circumstances the server will completely busy and communication with the legitimate client is difficult or impossible. SYN flooding attack basic purpose is to find open ports over the network and hack more information as many as possible. Up till now we have covered the attack generation and detection phase.

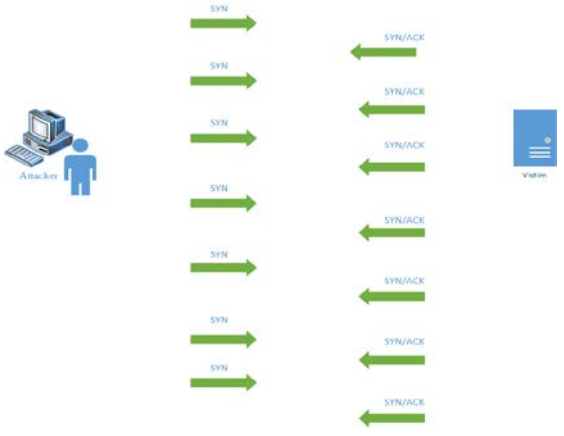

Figure 6 SYN Flood Attack Mechanism

4.2 SYN Flooding Attack Generation

For attack generation code will be written in c language because it support both windows and Linux. To create TCP and IP header <netinet/tcp.h> and <netinet/ip.h> header files are used which will provide declarations for TCP and IP headers. IP and TCP header will contain almost all basic information about packet that is to be transmitted. Calculate the checksum of the packet and then to send packet tell socket, the buffer containing headers and data, total length of our datagram, routing flags and socket address. To flood attack simple while loop is used that will run until condition is true.

4.3 Three Way Counter Algorithm for Attack Detection

Here the algorithm that is used to handle the attack is 3way counter algorithm in which it will check the complete ACK (acknowledgement) packets that will meet the 3 way handshake procedure successfully and also check other packets that will not meet 3 way handshakes. This algorithm states the following steps

- We have created three tables in its database.
- In theTable-1 we have stored only those IP addresses that are uniquely come over the network.
- In the Table-2 we have stored all those IP addresses that can come across the network more than one time and individually increment their values by using counter.
- In the Table-3 only those packets are stored that have completed their 3 way handshake procedure successfully and increment those IP addresses values that can achieve 3 way handshake procedure more than one time.
- Now we can define such rule that will check whether the packet is valid or it is an attack, so for this we can define a threshold value 3 and then calculate the counter values of Table-2 and Table-3 if the result after subtraction of both the counter values is less than 3 then we called that packet as safe packet otherwise state that packet as an attack.
- In this algorithm we can also define rule for such packets that are invalid packets although they have provide some ACK (acknowledgement) but actually these
- Packets cannot meet the 3 way handshake procedure because these packets do not have synchronization response with the server.

4.4 Windows Advance Firewall Rules

- First of all identify the protocol which you want

to filter; in current scenario it is going to be TCP.

- Point out the source and destination IP address and port number – traffic coming from web pages will be from any port no and IP address, coming on this server, on port 80.
- Windows Firewall must be open with MMC Advance Security
- Insert the new rule – to bring up new Inbound Rule Wizard Click on the New Rule button in Windows Firewall with Advance Security MMC.

5. Working of Application

Our application is basically divided into two modules:

5.1 Device Capturing

Our main goal is to capture any network traffic for analysis to check whether it is malicious or not for that we have to first select network device. Our program will listen all active network devices and show them in windows list box. User will select device of interest and program will start capturing packets of that network traffic. User may cancel its selection by pressing on Cancel Button.

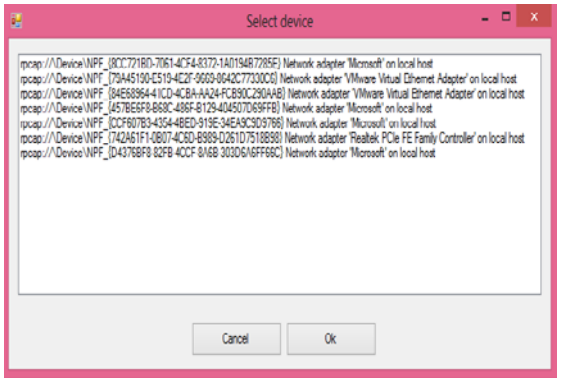

Figure 7 Device Capturing Window

The first interface that will occur during the start of our application is look like this in the above diagram. In this window we have some adapters through which we will connect with the network that will be selected to generate attack.

5.2 Packet Sniffing

After selecting network device our main target is to sniff packets of that network. Our program will use Winpcap library to sniff packets. Each packet coming is shown in data grid view and will show basic information like time interval and length. Detailed information of each packet is shown in rich textbox which will show following information of each packet as follows:

- Source IP
- Destination IP
- Header Length
- Protocol
- Time to live
- Header Checksum

On the information analysis will be done whether it is malicious traffic or not if it is malicious traffic it is moved towards database where further analysis will be done.

Figure 8 Packet Sniffing Form

This is basically the packet capture form application design in our module which will only occur if the adapter is selected in the previous “Select Device” window. This window can have 3 Data Grid Views (DGV). In the first DGV top of the left window, an incoming traffic with specific attributes like Count (total number of packets that arrive), Time Val (Time interval to reach the packet from source to destination), Link Layer Type (connection basically through we are connection with the network either through Wi-Fi or Ethernet) and Length (total length of the packet) have shown. At the bottom of first DGV now in second DGV complete information has shown of the packet having attributes like Source IP address, Destination IP address, Source MAC address and Destination IP address etc. In the third DGV top of the right window, SYN Flooding attacks are detected and are shown like this e-g IP: 169.254.58.7 is invalid ACK Packet.

5.3 Attack Mitigation

For mitigation of Sync Flooding Attack advance rule base approach of windows firewall is used. Set of rules are defined for inbound traffic which is malicious to mitigate it. Our program will access windows firewall and pass set of rules for particular IP address which is malicious to block all traffic from that particular address. Some of rules which are defined for particular IP address are as follows:

- Set inbound rules.

- New rule should be selected under Inbound Rules
- Custom rule should be selected.
- Select rule for all program
- Fetch IP address from IP address from database which has more sync requests
- TCP traffic from that IP address should be block on any port no.

6. Platform Used

6.1. Net Framework

Net Framework is used for development of application. C# language will used for packet sniffing and to define set of rules called (Signatures) for attack detection and mitigation.
Net Framework is used because it has many built in libraries support for packet capturing and socket programming. .NET is a programming framework created by Microsoft that developers can use to create applications more easily.

6.2. C# Internal Database

C# internal database will be used to store Sync packets and to perform analysis on them. For developers new version of SQL Server Express named as Local DB is best because it has a much lower memory footprint. When visual studio 13 is installed Local DB will be automatically installed. Local DB is used in place of the SQL Server Express for developing light switch project. SQL Server Express is now deprecated.

6.3. Major Libraries

WinPcap is the basic library which can be used for packet sniffing. WinPcap supports windows platform. For packet capturing and network analysis WinPcap library is used which is open source for Win32 platforms.
Most systems administration applications get to the system through broadly utilized working framework primitives, for example, sockets. It is easiest way to get to information on the system with this methodology since the working framework adapts to the low level points of interest (protocol management of, packet reassembly, and so on.) and gives a natural interface that is like the one used to peruse and compose records.
Most of the time, may be, the 'easy way' is not up to the assignment, since a few applications require direct access to bundles on the system. That is, they require access to the "crude" information on the system without the mediation of convention preparing by the working framework.

The motivation behind WinPcap is to give this sort of access to Win32 applications; it gives features to:

- detect raw bundles, both the ones bound to the machine where it's running and the ones traded by different hosts
- filter the parcels as indicated by client determined rules before dispatching them to the application
- transmit raw packets to the system
- gather factual data on the system activity

7. Acknowledgment

This research is supported by the National Engineering and Scientific Commission (NESCOM) was conducted in collaboration with the Computer Science and Engineering Department HITEC University Taxila Cantt under the contract No. NESCOM/Proj/RAC/HITEC(56)/2016 .

8. Conclusion

Detecting DOS attack three way counter technique is appropriate. In this study we implement the same technique to mitigate SYN flooding attack in DDOS environment. Result shows that through this technique we become able to detect and mitigate SYN flooding attack successfully. As now days every application is shifting towards the cloud because of increase in flexibility, rapid development and cost reduction, we are also looking to shift this application on the cloud in the future that can help to increase security and minimize organizational loss. Whenever a client want to access the information from the cloud a strong authentication process is created which can enhance the security by maintaining the log file of his/her movements and provide efficient, better and fast results. When the honeypot is deployed on the
cloud it will attract the hacker and detect its movements on the cloud and store that information in a particular log file from where he/she can easily detected and further more he/she will be properly banned to login from the cloud so that instead of losing the data and organization capital loss it will be saved in the future.
On shifting towards the cloud some important features are take place which are as follows

- Security and Privacy
- Storage and Scalability
- Backup and Disaster recovery
- Mobility
- Cost Efficiency
- Enable IT innovation

References

[1] Wang, H., D. Zhang, and K.G. Shin. Detecting SYN flooding attacks. in INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE. 2002: IEEE.

[2] He, Y., W. Chen, and B. Xiao. Detecting SYN flooding attacks near innocent side. in International Conference on Mobile Ad-Hoc and Sensor Networks. 2005: Springer.

[3] Gavaskar, S., R. Surendiran, and D.E. Ramaraj, Three counter defense mechanism for TCP SYN flooding attacks. International Journal of Computer Applications, 2010. 6(6): p. 0975-8887.

[4] Manna, M.E. and A. Amphawan, Review of syn-flooding attack detection mechanism. arXiv preprint arXiv:1202.1761, 2012.

[5] Bogdanoski, M., T. Shuminoski, and A. Risteski, Analysis of the SYN flood DoS attack. International Journal of Computer Network and Information Security, 2013. 5(8): p. 1.

[6] Rani, D.D., et al., TCP Syn Flood Attack Detection And Prevention. International Journal of Computer Trends and Technology (IJCTT), 2013. 4(10): p. 3412.

[7] Divakaran, D.M., H.A. Murthy, and T.A. Gonsalves. Detection of SYN flooding attacks using linear prediction analysis. in 2006 14th IEEE International Conference on Networks. 2006: IEEE.

[8] Zhang, T., Cumulative Sum Algorithm for Detecting SYN Flooding Attacks. arXiv preprint arXiv:1212.5129, 2012.

[9] Bekravi, M., S. Jamali, and G. Shaker, Defense against SYN-Flood denial of service attacks based on learning automata. arXiv preprint arXiv:1208.5037, 2012.

[10] Chawla, R. and G. Kaur, Improved framework for DDoS attack prevention in clustered environment. International Journal in IT & Engineering, 2015. 3(3): p. 314-320.

[11] Rana, D.S., N. Garg, and S.K. Chamoli, A Study and Detection of TCP SYN Flood Attacks with IP spoofing and its Mitigations. International Journal of Computer Technology and Applications, 2012. 3(4).

[12] Korczynski, M., L. Janowski, and A. Duda. An accurate sampling scheme for detecting SYN flooding attacks and portscans. in 2011 IEEE International Conference on Communications (ICC). 2011: IEEE.

[13] Tuncer, T. and Y. Tatar. Detection SYN flooding attacks using fuzzy logic. in Information Security and Assurance, 2008. ISA 2008. International Conference on. 2008: IEEE.

[14] Al-Duwairi, B. and G. Manimaran. Intentional dropping: a novel scheme for SYN flooding mitigation. In Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies. 2005: IEEE.

[15] Yi, P., et al. resisting flooding attacks in ad hoc networks. in International Conference on Information Technology: Coding and Computing (ITCC'05)-Volume II. 2005: IEEE.