A Dynamic Ddos Protection Mechanism for WLAN based on SDS Architecture

Zhenyu Wang[1, 2], Heng He[1, 2], Yan Hu[1, 2], Ji Zhang[1, 2], Wei Xia[1, 2]
[1]School of Computer Science and Technology, Wuhan University of Science and Technology, Wuhan, Hubei 430065, China
[2] Hubei Province Key Laboratory of Intelligent Information Processing and Real-time Industrial System, Wuhan University of Science and Technology, Wuhan, Hubei 430065, China
374487006@qq.com, heheng@wust.edu.cn, 1540823670@qq.com, 1143828107@qq.com, xiawei137hao@sina.com

Keywords: Distributed Denial of Service, Software Defined Networking, Protection Mechanism, Wireless Local Area Network.

Abstract: The impact of distributed denial of service (DDoS) attacks has become more and more serious and widespread in wireless local area network (WLAN). Traditional DDoS protection mechanisms become less reliable and cannot easily adapt to the diverse types of DDoS attacks. Meanwhile, the emergence of software defined networking (SDN) has provided a new solution to solve the security problem in WLAN. In this paper, we propose a dynamic DDoS protection mechanism for WLAN based on software defined security, which is a branch of SDN architecture in the network security. When outer-net data flow streams into the network, the mechanism can judge the credibility of the flow by its self-detection function, and then it will deploy different security strategies to handle the data flow according to the credibility before server responds to it. The analysis and experiment show that compared with traditional DDoS protection mechanisms, the proposed mechanism is a priori detection method, and is more flexible and efficient.

1 INTRODUCTION

With the rapid technological development of the Wireless Local Area Network (WLAN), the user requirements for security and trust of WLAN are also increasing significantly. Because WLAN has its own unique security threats, for instance, the IEEE 802.11 series standards and WEP/WPA encryption protocol have obvious defects, the WLAN security issues have become increasingly prominent. Distributed Denial of Service (DDoS) attack is a kind of typical attack in WLAN and the DDoS protection mechanism of WLAN has become a hot topic in the research field of network security (Yu et al., 2011), (Tupakula et al., 2011).

DDoS attack is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, the motives for, and the targets of a DDoS attack vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. DDoS attack in WLAN is mainly divided into the following types: bandwidth consumption attacks, resource consumption attacks, identity fraud attacks, interference type attacks, etc. Bandwidth consumption attacks include ICMP flooding, UDP flooding, etc. Resource consumption attacks include SYN flooding, auth flooding, etc. Identity fraud attacks include deauth flooding, association flooding, disassociation flooding, etc. Interference type attacks include teardrop, RF Jamming, etc. Based on these attacking types, there are lots of protection solutions proposed in recent years, such as route-based filtering (Park, 2003), packets analysis (Zhang et al., 2009) anomaly detection (Thatte et al., 2011), etc. However, most of the solutions are efficient for certain type of attack, but work little to other types of attacks, while DDoS attacks are presenting more diverse and complicated trend in WLAN. Therefore, it’s necessary to propose a dynamic solution by integrating the previous ones, which is flexible to deal with most of the types of attacks.

Nowadays, network technology becomes more mature and gradually develops into a new network architecture, Software Defined Networking (SDN) (Thomas and Ken, 2014). It is an emerging

He H., Xia W., Hu Y., Wang Z. and Zhang J.
A Dynamic DDoS Protection Mechanism for WLAN based on SDS Architecture.
DOI: 10.5220/0006443400410047
In *ISME 2016 - Information Science and Management Engineering IV (ISME 2016)*, pages 41-47
ISBN: 978-989-758-208-0

architecture purporting to be dynamic, manageable, cost-effective, adaptable, and seeking to be suitable for the high-bandwidth, dynamic nature of today's applications. The SDN architecture decouples network control and forwarding functions, enabling network control to be directly programmable and the underlying infrastructure to be abstracted from applications and network services. OpenFlow (OF) (Lei, 2013) protocol is a foundational element for building SDN solutions. OF separates the control plane and data plane of network equipment, so as to realize the flexible control of network traffic and provide a good platform for the core network and innovative applications. As a result, SDN offers more new possibilities to solve network security problems, including DDoS attacks. Software Defined Security (SDS) is a branch of SDN architecture in the network security, and it achieves the separation and reconstruction of the data surface and control surface, realizing modularity, servitization and reusability.

In this paper, based on SDS architecture and existing approaches, we propose a Dynamic DDoS Protection Mechanism for WLAN, namely DDPM, to solve the problem of diverse and complicated DDoS attacks in WLAN effectively. According to the types of DDoS attacks, DDPM deploys different security strategies for the underlying network. When outer-net data flow streams into the SDN network, the system can judge the credibility of the flow by its self-detection function, and then it will make decision to handle the data flow according to the credibility before server responds to it. Compared with traditional DDoS protection mechanisms, DDPM is a priori detection method, which is more flexible and efficient.

2 DYNAMIC PROTECTION MECHANISM BASED ON SDS

2.1 Architecture

DDPM inherits three main features of SDN framework: centralized control, open interface and virtualized network (Lei, 2013). The separation of the data plane and the control plane atomizes the functions and divides the system into five service modules, which provide northern interface for the invocation by higher layer. Meanwhile the virtualized network shields the realization of devices and thus reduces the difficulty of deployment. Figure 1 shows the architecture of DDPM.

In Figure 1, DDPM is divided into five function modules: Threat Detection module (TD), Credit Evaluation module (CE), State Table module (ST), Core Strategy module (CS) and Traffic Identification module (TI).

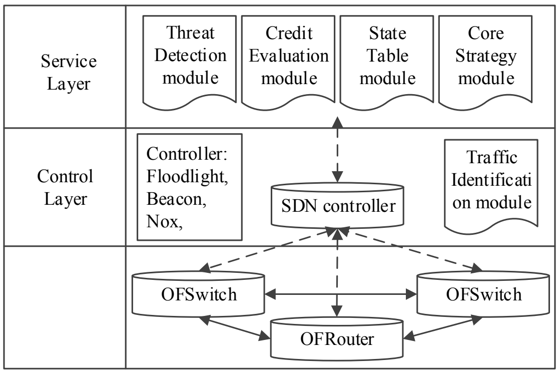

Figure 1: Architecture of DDPM.

On the Infrastructure Layer, OFSwitch and OFRouter, which are deployed in the SDN network, maintain flow tables, device status and other important information. When data flow streams into the SDN network, these devices will specify its action to forward or to discard.

On the Control Layer, SDN controller maintains the underlying network topology, manages network information, issues forwarding strategy and provides northern interface to the higher layer. More specifically, TI, which is deployed in the SDN controller, processes the data flow that Infrastructure Layer could not identify and then delivers the underlying network information to Service Layer. After receiving the developed strategy from Service Layer, SDN controller transfers the strategy into flow tables that specify data flow’s action and status tables that maintain devices’ status.

Service Layer contains concrete implement of DDPM. Firstly, TD detects the current status of network according to the underlying network information. Secondly, CE evaluates the credit level of the data flow and preserves the values in the ST. Actually, these three modules associated with each other. Finally, CS will develop the newest strategy according to the information from previous modules if the system has detected the change of current network status, and issue this strategy to the Control Layer. Figure 2 shows the execution flow of DDPM.

2.2 Implement of the Modules

TI, as the function module of Control Layer, provides intermediate hub for the Service Layer and

A Dynamic DDoS Protection Mechanism for WLAN based on SDS Architecture

Infrastructure Layer. Data flow will be matched to the flow tables, when it streams into the access layer switch. After failing to match any flow tables, the access layer switch will package this flow into a Packet_In message and send it to the SDN controller. Then, the controller will send the message to TI for processing. First, TI will cluster data flows' information (Ramos et al., 2008), (Lee et al., 2008) such as MAC, IP, data packet type and port and so on. Figure 3 (1) shows the discrete model of flows, with each record as a tuple. Figure 3 (2) shows the aggregation model of the flows. It clusters source IP and integrates the same network segment into one record. Compared to the discrete model, aggregation model can greatly reduce the number of records and the scale of flow table, which greatly reduces the load between controller and switch.

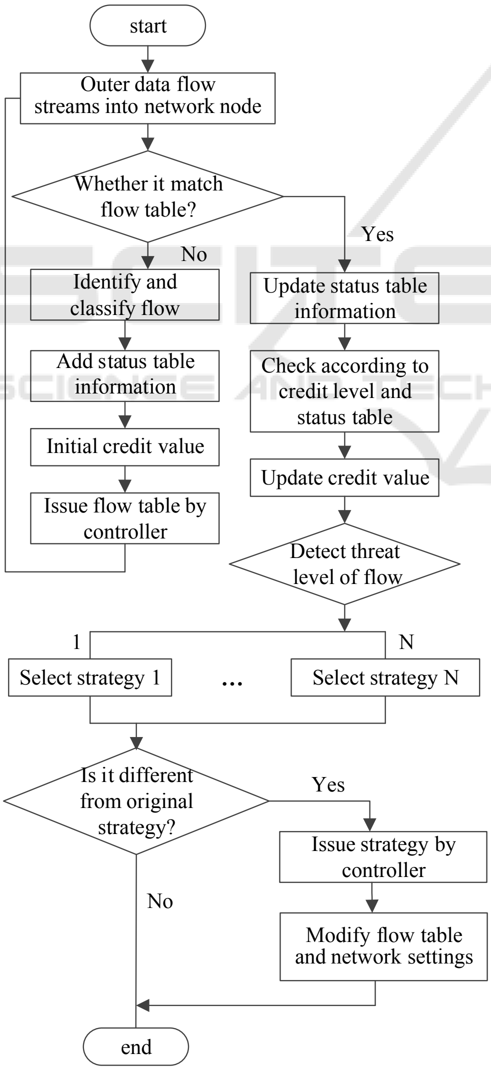
start
Outer data flow streams into network node
Whether it match flow table?
No
Yes
Identify and classify flow
Add status table information
Initial credit value
Issue flow table by controller
Update status table information
Check according to credit level and status table
Update credit value
Detect threat level of flow
1
N
Select strategy 1
...
Select strategy N
Is it different from original strategy?
Yes
No
Issue strategy by controller
Modify flow table and network settings
end

Figure 2: Execution flow of DDPM.

After TI identifies the unrecorded flows, ST will store each result in the library as one record. Once the records are set up, ST will update the records according to the information of the flow tables and OFSwitch's status which is obtained by SDN controller as the same type of flows stream into the switch. Every time ST updates its records, TD will do once self-similarity detection (Xiang, 2004), which aims to detect the change rate of information including bandwidth, sending rate of packet, amounts of flow tables and other important indexes. First, detection of bandwidth change rate can monitor the SDN network loads, so it can detect the bandwidth consumption attack effectively. Second, aggregating the flow tables based on source network segment and calculating its matching frequency can reflect DDoS attacks' strength effectively, because most cases of the sources of attacks come from a handful of network even the forged sources. However, given the trend of diverse attacks, TD also detects the change rate of the amounts of flow tables. When attacks come from many sources, the scale of flow tables will increase dramatically.

CE, based on the results of TD's detection, evaluates each data flow's credit. It divides the credit into five levels: safety, alert, emergency, danger and destruction, by which CS develops five different strategies. Every time the certain flow is over each level's threshold, SDN controller will send the packaged raw data flow to TD which will analyze the data flow and separate the flow into two parts. One part is the same with previous flow, while another is the definite one over the threshold.

More specifically, after TI identifies the new data flow, CE will mark the data flow as the default value: safety. And then CS develops and issues a forwarding strategy that the data flow selects the optimal path to forward according to Dijkstra algorithm. With the increasing sending rate of certain flow over the alert-credit threshold, CE marks it for "alert" and then CS changes this flow's forwarding strategy to select another lighter-load forwarding path. By this way, it can reduce the load of certain link and best utilize available bandwidth. Furthermore, if the certain data flow is over the emergency-credit threshold, CE will mark it for "emergency" and then changes the strategy to drop the certain packet type of the flow. This flow is actually based on series of flows which comes from different source MAC/ IP but same network segment. As a result, which flow the system is going to drop is the flow with definitized source MAC/IP and packet type, while other flows within the same flow cluster will not be limited. Once certain flow is over

43

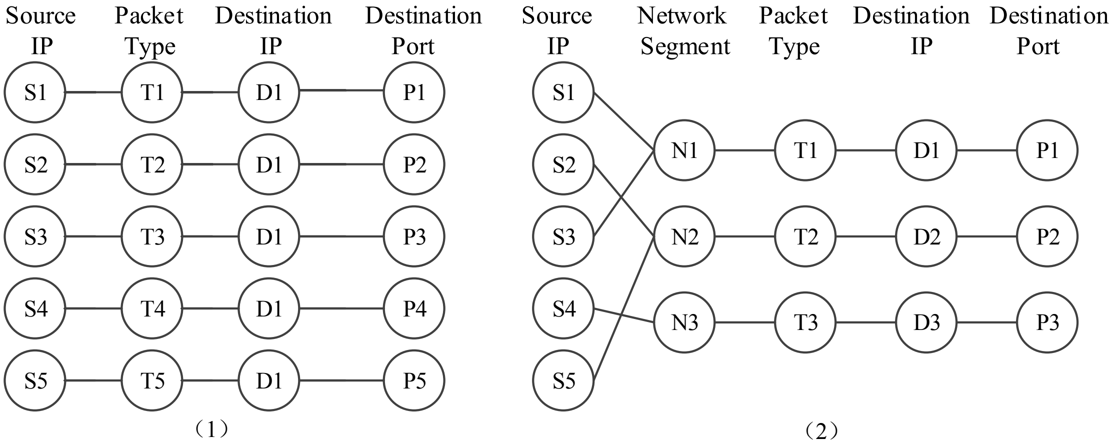

Figure 3: Discrete and aggregation model of data flows.

danger-credit threshold, CS will change the strategy to drop all this source-based flows. The communication between server and normal users will not be affected until any flows exceed the destruction-credit threshold. At the time, CE marks the flow for "destruction" and informs CS to change the strategy to limit the receive rate of certain port that this data flow streams into through issuing the status-change command to the OFSwitch. There is no doubt that all flows from this port will be affected by limiting the import of the OFSwitch.

The process of DDPM's protection is dynamic. It offers several different strategies to handle different intensities of data forwarding. Once certain flow recovers to lower credit level, CS also needs to change the strategy to temperate one. In addition, with higher level of the flows' credit, there are larger scale of flow tables and higher frequency of data receiving. As a result, it's an elastic, real-time and reliable mechanism but also has much higher requirements of the performance of hardware.

3 ANALYSIS AND EVALUATION

It's SDN network that makes this elastic and dynamic mechanism possible. The characteristic of service atomization makes DDPM easy to extend new function modules to improve its reliability. Compared to single and static traditional solutions, DDPM is more like a set containing different solutions. Based on different detection indexes, it provides several detection results. Therefore, it's more reliable for DDPM because while one index might be not relative to certain type of attack, another index could be correlative to it.

On the way of protection, DDPM provides five-level strategies, which means that all situations have been divided into five different intensities of attacks. With the increasing intensity of data transmission rate, the system develops the stricter strategy. More importantly, the data flow sending to server will be detected as long as it streams into the SDN network. In order words, DDPM can resist the potential DDoS attack before server is under attack. Apparently, it's more efficient and safer to protect server from DDoS attack than the traditional solutions which are based on analysis of packets that server has received.

To build a SDN network requires only OFSwitch, OFRouter and SDN controller because DDPM is accomplished primarily in software and does not need any other expensive protective equipments. On the other hand, it also requires the higher performance of these network equipments. Under the enormous amounts of data flows, forwarding devices need to match quantities of flow tables simultaneously and SDN controller needs to process large numbers of unrecognized data flows. Moreover, it is difficult to ensure the reliability of single controller within a large scale network. However, the SDN technique is developing rapidly and the collaboration among multiple controllers will be well achieved in the near future. Above all, the comprehensive comparison is shown in Table 1.

Table 1: Comprehensive comparison.

Solutions	Traditional mechanism	DDPM
Scalability	Low	High
Reliability	Low	High
Flexibility	Low	High
Protective method	Single	Multiple

A Dynamic DDoS Protection Mechanism for WLAN based on SDS Architecture

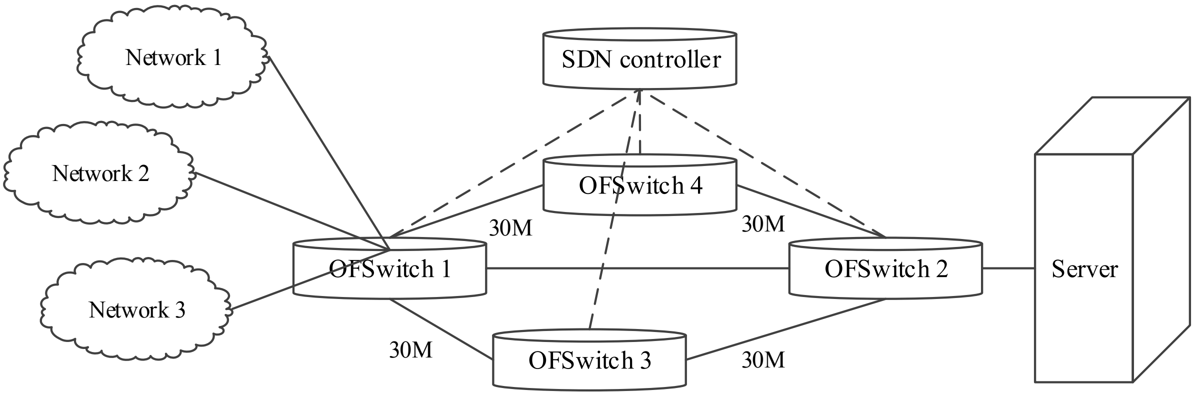

Figure 4: Experimental structure.

4 EXPERIMENTAL EXAMPLE

In order to illustrate the feasibility and effectiveness of DDPM, we construct an experimental example in which we simulate common ICMP flooding and SYN flooding as two types of DDoS attacks. ICMP flooding is a type of attack that consumes the bandwidth of victim's network, while SYN flooding is aiming to exhaust the resources of victim. The experimental structure is shown as Figure 4.

In Figure 4, SDN network consists of OFSwitch 1~4, SDN controller and server. Firstly, OFSwitch 1 is used to connect with outer network 1~3. Secondly, OFSwitch 2 connects with OFSwitch 1 by a 15M link. Thirdly, OFSwitch 3 and OFSwitch 4 are both linked between OFSwitch 1 and OFSwitch 2 and the bandwidth of the links are all set for 30M. Finally, SDN controller controls the underlying network by southern interface. In addition, the link between OFSwitch 1 and OFSwitch 2 is the shortest path but not always the optimal path, which is determined by the actual loads of each link. Data flows from network 1 act as the normal data request, while data flows from network 2~3 act as the abnormal ones. Detail steps are given:

Step1: Outer network sends data flows to server. (Network 1 sends few steady data flows, network 2 sends quantities of TCP requests accompanied with few ICMP requests and network 3 sends quantities of ICMP requests with few TCP requests.)

Step2: All varieties of data flows stream into SDN network. If OFSwitch 1 cannot process the data flows, it will deliver them to SDN controller by Packet_In messages. And then turn to Step3. Otherwise, turn to Step6.

Step3: SDN controller delivers the messages to TI to analyse them. The results of analysis are submitted to Service Layer by SDN controller.

Step4: Each module of Service Layer works coordinately. CS develops the newest strategy for the data flows and issues to SDN controller.

Step5: SDN controller issues the flow tables and OFSwitch's status tables to the relative OFSwitch according to the strategy.

Step6: Data flows match the flow tables and OFSwitchs set their status. Data flows' action will be specified to be forwarded, limited or dropped according to the records. Then the information of network will be updated. Turn to Step1.

The experimental process is shown as follows:

As can be seen from Figure 5, data from network 2~3 increase dramatically in different time points respectively, while data from network 1 stay steady throughout the experiment. When data sending rate is over the first threshold (20Mbits/ 3s, in Figure 5 and Figure 6), the system chooses to drop the packets with the type that leads to exceed the threshold (at 30s from network 2 and 69s from network 3, in Figure 6). When data sending rate is over the second threshold (30Mbits/ 3s, in Figure 5 and Figure 6), the system drops the packets with source ip from certain network (at 63s from network 2 and 84s from network 3, in Figure 6). Moreover, at the beginning, the data flows are forwarding on the link: s1 to s2. With the increasing loads of the link, the system splits the flows (data from network 1 transmitted on link: s1 to s2; data from network 2 transmitted on link: s1 to s3; data from network 3 transmitted on link: s1 to s4) when the loads of each link are over its threshold (s1 to s2: 10Mbits, s1 to s3: 20Mbits, s1 to s4: 20Mbits, in Figure 7). It can be seen that DDPM is feasible and efficient.

45

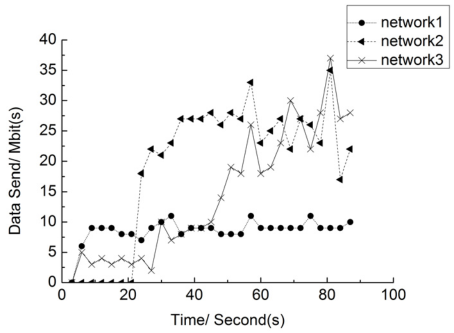

Figure 5: Data sent by outer network.

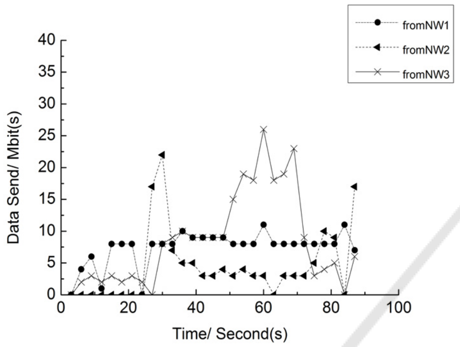

Figure 6: Data received by server.

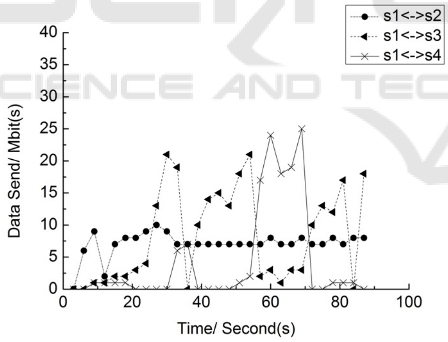

Figure 7: Loads of each link.

5 CONCLUSIONS

DDPM achieves a new dynamic protection mechanism to prevent DDoS attacks flexibly according to the intensity of attacks in WLAN. The characteristic of service atomization makes DDPM easy to extend new function modules to improve its reliability. Moreover, DDPM can resist the potential DDoS attacks before the server is under attack. Therefore, DDPM can deal with the diverse and complicated types of DDoS attacks efficiently. In future work, we will focus on the design of security protection mechanism based on multiple controllers in large scale network.

ACKNOWLEDGEMENTS

This work was supported by the National Natural Science Foundation of China under Grant No. 61602351, No. 61502359, No. 61602349 and No. 61303117, the Young Scientist Foundation of Wuhan University of Science and Technology under Grant No. 2015XG005, the Open Foundation of Hubei Province Key Laboratory of Intelligent Information Processing and Real-time Industrial System under Grant No. 2016znss10B, and the College Student Innovation Foundation of Wuhan University of Science and Technology under Grant No. 15ZRA096. Heng He is the corresponding author of the article.

REFERENCES

Lee, K., Kim, J., Kwon, K., Han, Y., Kim, S., 2008. DDoS attack detection method using cluster analysis. *Expert Systems with Applications*, 34(3), pp. 1659-1665.

Lei, B., 2013. *Deciphering SDN: Core Techniques and Practical Guide*. Publishing House of Electronics Industry. Beijing.

Park, K., 2003. Scalable DDoS protection using route-based filtering. In *Proceedings of DARPA Information Survivability Conference and Exposition*, pp. 97-97. IEEE Computer Society: Washington, DC.

Pelechrinis, K., Iliofotou, M., Krishnamurthy, S., V., 2011. Denial of service attacks in wireless networks: The case of jammers. *Communications Surveys & Tutorials*, 13(2), pp. 245-257. IEEE.

Ramos, E., Chae, S., Kim, M., Choi, M., 2008. The optimistic schemes of cluster analysis and k-NN classifier method in detecting and counteracting learned DDoS attack. In *Proceedings of New Technologies, Mobility and Security*, pp. 1-5. IEEE Computer Society: Tangier.

Thatte, G., Mitra, U., Heidemann, J., 2011. Parametric methods for anomaly detection in aggregate traffic. *IEEE/ACM Transactions on Networking*, 19(2), pp.512-525.

Thomas, D., Ken, G., 2014. *SDN: Software Defined Networks*. People's Posts and Telecommunications Press. Beijing.

Tupakula, U., Varadharajan, V., Vuppala, S., K., 2011. Counteracting DDoS attacks in WLAN. In *Proceedings of the 4th International Conference on Security of Information and Networks*, pp. 119-126. ACM.

A Dynamic DDoS Protection Mechanism for WLAN based on SDS Architecture

Xiang, Y., Lin, Y., Lei, W., Huang, S., 2004. Detecting DDoS attack based on network self-similarity. *IEE Proceeding on Communications*, 151(3), pp. 292-295.

Zhang, Y., Wan, Z., Wu, M., 2009. An active DDoS defence model based on packet marking. In *Proceedings of the 2nd International Workshop on Computer Science and Engineering*, pp. 435-438. IEEE Computer Society.

47