Research on Detection Method of Malicious Node Based on Flood Attack in VANET

Yizhen Xie[1], Yuan Li[2(✉)], and Yongjian Wang[3]

[1] Beijing University of Posts and Telecommunications, Beijing 100876, China
[2] Southwest University of Science and Technology, Mianyang 621010, Sichuan, China
Liyuan_3033@163.com
[3] National Internet Emergency Center, Beijing 100029, China

Abstract. For the reason of the variability and mobility of VANET's topology, it is easy to be attacked by attackers. This paper proposes two detection methods for TCP Synchronize Sequence Numbers (SYN) flood attacks and UDP traffic flood attacks in combination with the requirements of the rapid and real-time detection for malicious nodes in the security of the 5G VANET, and to enhance the ability to identify and detect malicious nodes. For the TCP SYN flood attack, the number of access requests with the same node ID is limited, and the number of semi-connections in Road Side Unit (RSU) is adjusted. For the UDP traffic flood attack, the RSU is used to monitor and analyze the data traffic of each node in VANET. Through the feasibility analysis, the above two detection methods can effectively detect flood attacks in VANET, thus assisting the network defense mechanism to ensure network security. Thereby providing guarantee for the security of VANET in the 5G communication environment.

Keywords: VANET security · 5G · Flood attack · TCP SYN flood · UDP traffic flood

1 Introduction

As an intelligent system for the application of the Internet of Things in transportation systems, VANET is an integrated application and extension of related technologies such as computers, Internet, mobile communication networks, and Internet of Things [1]. VANET plays an important role in easing urban traffic pressure, reducing traffic accident rates, improving road utilization, and unmanned driving. 5G VANET uses 5G network-based C-V2X technology, which mainly includes four major communication scenarios: vehicle-Cloud communication: vehicle and VANET service platform interaction information through 5G network; vehicle-vehicle communication: vehicle to vehicle via LTE/5G-V2X technology interaction information; vehicle-road communication: vehicle and road infrastructure facilities use LTE/5G-V2X technology to interaction information; vehicle-people communication: vehicle and user intelligent terminals interaction information through 5G networks. The emergence of 5G communication technology has helped the development of VANET. The characteristics of low latency

X. Wang et al. (Eds.): 6GN 2020, LNICST 337, pp. 373–383, 2020.
https://doi.org/10.1007/978-3-030-63941-9_28

and high speed will improve the performance and reliability of VANET. However, due to the open network environment of the VANET, the mobility of nodes, and the dynamic structure of the topology, it is vulnerable to be attacked by attackers and causes serious security problems. Therefore, VANET security is an important part of the research field of VANET.

The security threats of wireless communication in the 5G VANET scenario can be divided into three categories: traffic attacks cause network overload, identity forgery causes information leakage or misjudgment, and malicious interference causes system errors. Flood attacks are the main aspect in traffic attacks. Through the research on the flood attack problem faced by VANET, this paper mainly detects the two attack modes of TCP SYN flood attack and UDP traffic flood attack. The main research contents are as follows:

For the architecture of VANET adopting the TCP protocol, when the vehicle node initiates a connection request to the RSU and initializes, the RSU uses the SYN header to perform a "Triple handshake" connection with the vehicle nodes, The attacker can quickly initiate a large number of connections in a short time. The requests cause the RSU to fail to respond, thus consuming a large amount of RSU computation processing resources until the service is denied. For this TCP SYN flood attack, the node's ID restriction method is used for detection and defense. When the node sends a access request, the RSU records the node's ID. When the same ID sends the access request multiple times in a short time, the node's requests should be restricted. For the node's ID that has already existed in the network, its request packet will no longer be accepted. At the same time, the RSU shortens the TCP handshake half-connection suspension timeout period and closes the request connection initiated by the duplicate ID.

For the architecture of VANET using the UDP protocol, when a normal node in the network is hacked into a malicious node and initiates a traffic attack, the RSU will be targeted. A malicious node will frequently broadcast data packets to other nodes. The destination address of the data packet is the RSU, and a large number of data packets occupy network bandwidth resources and RSU's computing processing capability in a short time. For such flood attacks, RSU is used to monitor the data traffic of nodes in the network in real time. RSU counts the data traffic of each node, calculates the traffic average value according to the time period, and records the source address of the received data packet. If the node data traffic average value is higher than the normal value and the data packet source address frequency is too high in a certain period of time, the node may be determined to initiate a flood attack and isolate it. In addition, UDP packet verification is added to analyze the availability of the data packet and improve the detection accuracy.

5G technology protects the safety of connected cars. With its powerful mobile bandwidth, 5G communication technology can reach a peak rate of 20 Gbit/s, support lower latency ($\leq$10 ms), higher reliability ($>$99.99%), and more terminal connections (1 million terminals can be connected per square kilometer) [2], which can meet the safety communication needs of VANET In the detection of SYN TCP flood attacks, the high reliability of 5G can improve the detection performance; in the detection of UDP flood attacks, 5G can guarantee the real-time nature of traffic detection with low latency characteristics.

The second section of this paper introduces the current research status of VANET security and flooding attack detection. The third section introduces TCP SYN flood and UDP traffic flood attack methods and corresponding detection methods; the feasibility analysis is carried out in the fourth section; finally, summarize the full text.

2 Related Work

VANET is defined by the China IoT School-Enterprise Alliance. VANET is a network that integrates information such as vehicle location, vehicle speed, and vehicle travel path. It can collect the environment and status information of the vehicles and their surroundings through wireless devices such as GPS, radio frequency, sensors and cameras [3]. Then the related information is transmitted through the Internet technology, and finally the relevant analysis technology is used to process the information, thereby more effectively realizing the traffic of the vehicles and improving the overall traffic efficiency of the city. Since the rise of VANET in recent years, relevant security defense measures have not been improved in time. At present, there are still many security problems in VANET, which have occurred from malicious attacks by attackers, with serious consequences.

In 2010, researchers at Rutgers University in Southern Carolina demonstrated how to crack the car's internal network and counterfeit the tire pressure sensors' information of some car brands. Even destroyed the TPMS system over 40 meters away through wirelessly interfering. At the Las Vegas hacking conference in 2013, two hackers demonstrated how to attack the Toyota Prius and Ford Mavericks control systems to achieve a series of operations such as sudden braking, including high-speed driving, brake failure, and steering of the steering wheel [4]. In 2015, two security researchers demonstrated a vulnerability in the car's "Uconnect" feature of Chrysler's Jeep Cherokee, remotely invading and controlling the target vehicle, and freely controlling the entertainment system, wipers, steering wheel, engine, etc. At the beginning of 2017, the safety weather van of VANET had been urgently transferred to the data security and privacy of customers. In June, a database of dealers in the United States was attacked, involving sales data leaks from more than 10 million vehicles. In December, Nissan Motor officially announced that its financial company database data information was stolen by hackers, customers' personal information and loan information were all stolen [5]. MegamosCrypto protection systems from Audi, Porsche, Bentley and other Volkswagen brands were also breached.

At present, many scholars have conducted research on the detection of malicious nodes in VANET. How to meet the requirements of low-latency, high reliability, high speed, large capacity, and high security in high-density vehicle scenarios is the challenge faced by 5G VANET and the focus of related research. However, most of the existing literature research on flood attack detection is based on traditional wired networks and wireless sensor networks, and few researchers have studied the flood attacks in VANET. The current research status of flood attack detection is as follows:

In [6], for SYN Flood attack on the target computer, the detection function is set on the target computer. If it finds that receives SYN packets for the local machine without responding, it is considered to be subjected to a SYN flood attack and refuses to connect

with it. However, this method is not suitable for the scenario where vehicle nodes in VANET frequently access the network and is likely to cause misjudgment.

The most obvious feature of UDP traffic flood attack is that the traffic is greatly increased. It is also a common method based on traffic changing detection. The real-time defense mechanism (DDM) of DHCP flooding attack is proposed in [7]. The dynamic peak estimation model is established by using two key parameters of real-time DHCP traffic average speed and IP pool margin to evaluate whether the port is attacked. If it is attacked, the mitigation model starts defense. In the mitigation model, the IP pool cleaning is performed by using the response feature of the Address Resolution Protocol (ARP). The intra-period interception mechanism is designed to intercept the attack source, which can reduce the blocking and minimize the interception to the user. The impact of normal use. The shortcoming of this method is that the computational processing capability of the node and the RSU is relatively high, otherwise the real-time performance of the defense cannot be met.

Literature [8] proposed a method for constructing a new SYN-agent that uses the TCP header reservation flag to inform the server of a complete the triple TCP handshake. If it is a SYN-attack, there should be no further ACK after this. After a short period of time, the half-open TCP connection is removed from the proxy. Therefore, the TCP SYN flood attack is avoided to make a large number of TCP semi-connections occupy resources. This method is applicable to a scenario where the nodes are relatively fixed. In VANET, the vehicle enters and exits the network at any time, and the detection is difficult.

Literature [9] proposed a SYN Flood attack mitigation method based on supervised learning classification method, which identifies and blocks SYN Floods before they reach their targets, thus preventing resource consumption and performance loss. This method selected a classifier and adjusts parameters according to the policy and change characteristics of the SYN Flood attack, but the learning attack strategy occupies a large amount of computing resources of the RSU.

Literature [10] proposed an effective method to detect and defend against UDP flood attacks under IP spoofing types. This method utilizes a Bloom filter-based storage efficient data structure and an IP Wedge Reference Detection Method. It achieves higher detection rate while defending against UDP flood attacks with IP spoofing, and has lower storage and computational costs. However, this method does not consider the availability of attack packets.

The detection method for traditional network flood attacks is not applicable to VANET. Considering the actual network environment of VANET, combined with the low-latency and high-reliability characteristics of 5G communication, this paper proposes a detection method for TCP SYN and UDP traffic flood attacks in VANET. 5G communication technology can meet the needs of single-vehicle uplink and downlink data rates greater than 10 Mbit/s, 50 Mbit/s in some scenarios, latency of 3-50 ms, and reliability greater than 99.99%. At the same time, it can meet the real-time interactive data of vehicles, roads and pedestrians, and the high data transmission demand of up to TB-level per day [11]. The application of 5G communication technology in the low-latency and high-mobility VANET scenario solves many problems and challenges faced

by the current VANET, and enables the VANET to obtain better performance under high-speed movement [12].

3 Principles and Methods of Flood Attacks

3.1 TCP SYN Flood

In the process of establishing a connection with TCP, a "Triple handshake" is required. As shown in the figure, first handshake: When the TCP network establishes a connection, the client sends a SYN packet to the server and enters the SYN_SENT state, waiting for the server to confirm. The second handshake: After receiving the SYN packet, the server confirms the SYN of the client and sends a SYN+ACK packet to the client. The server enters the SYN_RECV state, which is the half-connected state [13]. The third handshake: After receiving the SYN+ACK packet of the server, the client feeds back the ACK response packet to the server. After receiving the response packet, the server completes the successful TCP connection, as shown in Fig. 1.

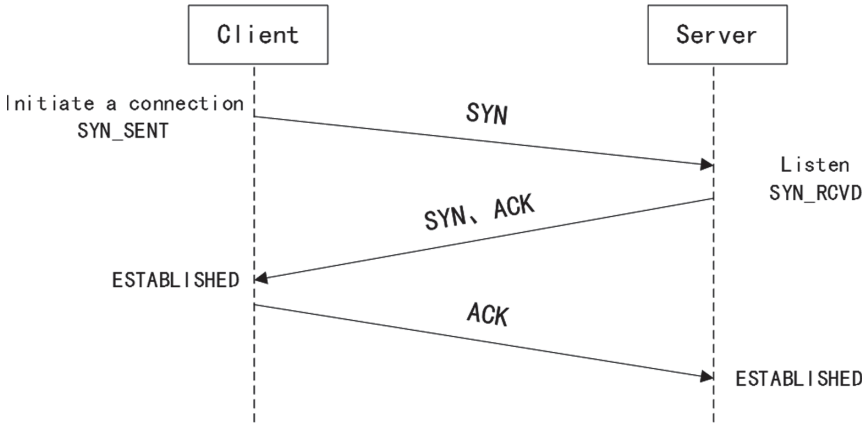

Fig. 1. Triple handshake.

The attacker uses the defect of the TCP "Triple handshake" connection mechanism to initiate a SYN attack. The attacker controls malicious node to initiate a connection and attempts to access VANET. The malicious node masquerades as a normal node to initiate a connection request to the RSU as a client. After receiving the SYN+ACK packet of the server in the second handshake phase, the malicious node does not continue to complete the third handshake, and does not return the ACK response packet to the server, so that the server remains half-connected. After the attacker initiates multiple connection requests, the server will suspend the corresponding number of half-connected states. As a VANET relay server, the RSU will gradually be exhausted by a large number of useless half-connected state processing resources, rejecting other connection services, resulting in normal legal vehicle nodes unable to access VANET, as shown in Fig. 2. The attack

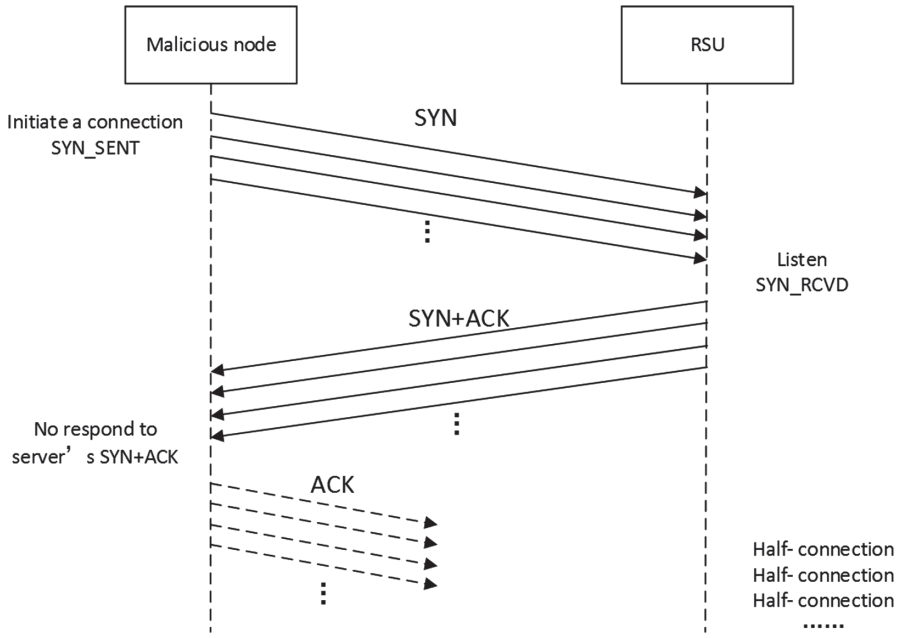

Fig. 2. TCP SYN flood attack.

motivation of the TCP SYN flood attack is to exhaust the computing resources of the RSU.

The rapid mobility of the vehicle nodes and the multilateral nature of the network topology are essential characteristics. It also determines that the network access request is more frequent in this network environment, and the harm caused by the SYN flood attack is more serious.

3.2 UDP Traffic Flood Attack

UDP is a connectionless protocol and does not require any connection to be made to transmit data. The attacker sends a large number of UDP packets to the RSU [14]. The RSU is busy processing the UDP packets and cannot process normal packet requests or responses. A large number of useless UDP packets carry a large amount of network traffic quickly occupying network bandwidth resources, causing network congestion to reject other normal services, as shown in Fig. 3.

In addition, in the UDP flood attack, the attacker sends a large number of UDP packets or malformed UDP packets with fake IP addresses. These fake IP addresses do not exist in current VANET, and the destination IP address of the packets will never be available. So these packets will always be forwarded within the network, resulting in continuous attack traffic, and the target node does not get back information to cause system resources to run out or even crash. The malformed UDP packet will not be parsed after the node receives it. Therefore, after the node receives the packet, it detects whether it is normal. The incomplete abnormal packet will be discarded, but the detection and

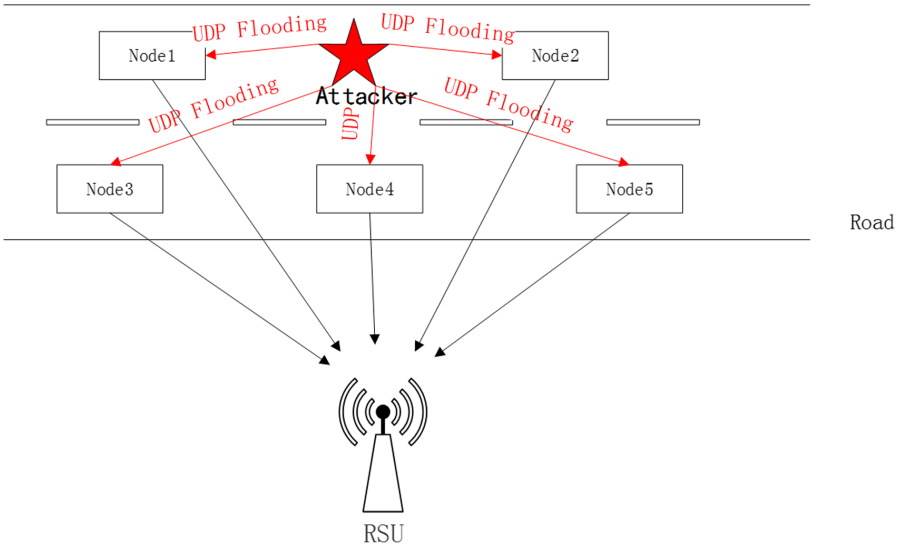

Fig. 3. UDP traffic flood attack.

discarding of the packet requires the node to calculate the processing resource. Many malformed data packets will occupy large detection computing resources of the node until the computing power of the node is exhausted, causing the target node to denial of service.

The attacking mode is that the attacker places the malicious node in VANET in advance, or attacks normal nodes in the network and capture control to become malicious nodes. Since UDP is based on a connectionless protocol, the node and the RSU do not continuously maintain a connection, and the member nodes of VANET change constantly. So it is difficult to detect the malicious node causing the UDP flood attack in VANET.

4 Detection Method

4.1 Detection for TCP SYN Flood Attack

Because the TCP SYN flood attack utilizes the TCP "Triple handshake" process, the server will suspend the half-connection and wait for the client to acknowledge the ACK packet. Therefore, one of the keys to detecting the SYN flood attack is to detect the authenticity and availability of the client's SYN packet. If a client continuously sends a SYN packet request to the network, but does not respond to the ACK packet to the server, causing the server to suspend a large number of half-connected states, it can detect that the client initiates a TCP SYN flood attack. Secondly, limiting the number of server-side TCP half-connections and the timeout period can alleviate the SYN flood attacks sent by attackers.

In the practical application environment of VANET based on 5G technology, the IP of the vehicle node requesting to access the network is detected, and the IP of the node

that has entered the network is recorded in the RSU. The IP that has entered the network cannot be requested to enter the network again; the IP address of the node that has not entered the network limits the number of network access requests per unit time. When the node requests to access the network, it sends a SYN packet to the RSU. The RSU detects the source node IP of the packet. If there is too many access requests from duplicate IPs in a short period of time, the RSU can identify the node of the IP as a malicious node. The RSU adopts a policy that restricts the IP packet, and the SYN packet that discards the IP does not respond. The detection of flood attacks on the RSU side is mainly to monitor the number and time of TCP half-connected states. When the RSU suspends many vehicle nodes access requests, significantly exceeding the normal mean, it can be assumed that the RSU may be under TCP SYN flood. At this point, the RSU needs to shorten the TCP handshake half-connection suspension timeout period and close the duplicate IP-initiated request connection, as shown in Fig. 4. Under the low-latency conditions of 5G technology, the timeout needs to be further reduced to accommodate fast connections. In this way, the flood attack can be effectively dealt with, the computational pressure of the RSU to handle the half-connected state is alleviated, and the normal legal node requesting the network access is not greatly affected, and the normal access of the vehicle nodes in VANET is guaranteed.

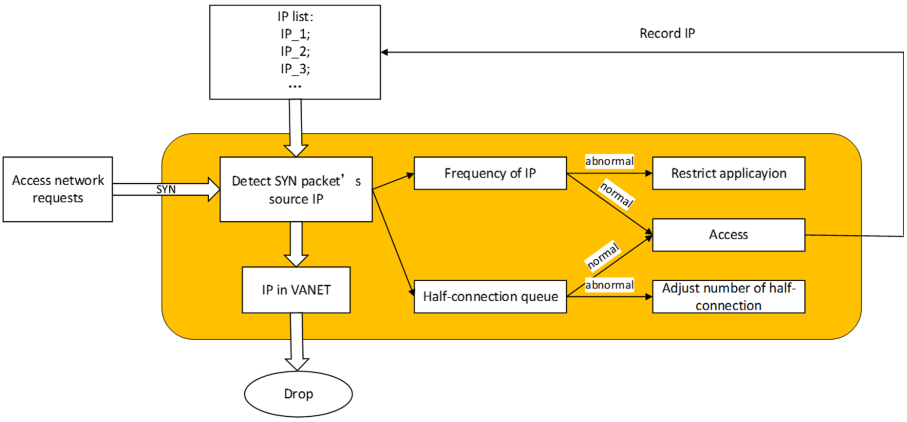

Fig. 4. TCP SYN flood detection method.

4.2 Detection for UDP Traffic Flood Attack

Due to the variability of the composition of the vehicle network node, the identity of the node is difficult to authenticate. Before the vehicle node sends the UDP data packet, the legality of the node cannot be known. Therefore, in the case of UDP traffic flood attacks, it is better to monitor node's traffic. The RSU monitors the data traffic of each node in the network to analyze whether the traffic is abnormal. There are also two ways to monitor traffic: First, the RSU directly monitors the data traffic sent and received by each node in the network, and performs traffic change statistics. However, in this way, each time the

node sends and receives data, the RSU must monitor and sample it, which will occupy a large amount of computing resources of the RSU and occupy much network bandwidth. Second, the vehicle node counts the source IP address of the data packet when receiving the data packet, and generates a traffic statistics data packet, where the packet includes the data source IP address, the destination IP address, and the data packet size. Each node performs traffic statistics packets and uploads them to the RSU. The RSU collates and counts the traffic statistics of each node. Because the UDP packet of the node is sent to multiple nodes, the traffic condition of the source node is counted by multiple nodes, thus avoiding the contingency difference of the individual nodes and improving the credibility. After the RSU counts the traffic changes of each node according to the time interval, it can be compared with the normal ones. The difference is due to the increase in the amount of data reported by the vehicle or the surge in data traffic caused by the flooding attack. Due to the high-bandwidth and low-latency characteristics of 5G, the average value of traffic needs to be adjusted in real time according to the different states of ordinary VANET communication and 5G communication to adapt to different network conditions. Therefore, the RSU can detect a malicious node that initiates a UDP flood attack inside VANET. The detection method is shown in Fig. 5.

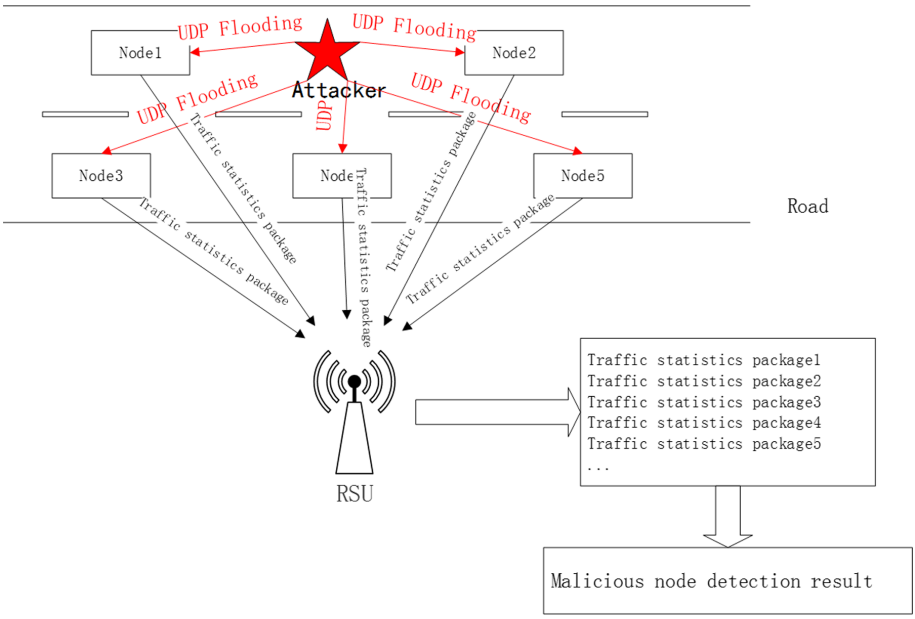

Fig. 5. UDP traffic attack detection mode.

In addition, an attacker may send many UDP packets with a fake destination IP address. At this condition, the destination IP address connectivity of the UDP packet in the network is detected and analyzed. If the destination IP does not exist in the RSU routing list or is not connectable, the forwarding of the packet is stopped. It is also necessary to detect the integrity and availability of UDP packets to avoid the large

amount of malformed data packets occupying the computing power of the vehicle nodes or RSUs.

5 Experimental Analysis

5.1 Detection Method for TCP SYN Flood Attack

In the VANET application environment, once the RSU is attacked by the TCP SYN flood, other legitimate vehicles cannot enter the network normally. The road conditions and vehicle emergency information on this road cannot be accepted in time. The RSU analyzes all the captured SYN packets, and obtains the statistics of the SYN packets sent by each node. The RSU detects the suspended half-connection status in real time, and detecting the number of these TCP half-connections can effectively determine whether it has been attacked by SYN flood. RSU reduces the half-connection waiting time can alleviate the calculation and buffering pressure, and effectively prevent the same vehicle ID from launching a network access request multiple times to maliciously attack the RSU to occupy network access request resources. While detecting and mitigating TCP SYN flood attacks, this method can also ensure that other legitimate vehicle nodes can access the network normally.

5.2 Detection Method for UDP Traffic Flood Attacks

When VANET is attacked by UDP traffic flood attack, it will lead to denial of service. The most important feature of UDP traffic flood attack is traffic changes. By monitoring the characteristics of traffic changes, traffic flooding in VANET can be effectively detected, and current limiting measures can be taken in time. The UDP flood detection method in this paper enables the RSU to collect the traffic statistics of each node in VANET in time, so that multiple nodes can be statistically analyzed. Combined with UDP packet verification detection, the legality of UDP packets in network traffic is analyzed, and the analysis capability of traffic in the VANET is further enhanced, and the detection accuracy is improved. This method can not only detect abnormal changes in traffic in time, but also accurately detect the flooding node.

6 Conclusion

In this paper, by analyzing the attack principle of TCP SYN flood attack and UDP traffic flood attack in detail, combined with the special network application environment of the 5G VANET, the detection methods for the above two flood attacks are proposed. For the TCP SYN flood attack, the method of restricting the repeated network access request and adjusting the number and time of TCP half-connections is adopted, which effectively alleviates the flooding of the SYN packet and ensures that the legal vehicle node normally enters the network; for the UDP traffic flood attack, the whole network node is adopted. The method of traffic monitoring and UDP packet check validity effectively mitigates UDP traffic flood and improves detection accuracy.

The two types of flood attacks in this article also have limitations. The detection method for the TCP SYN flood attack will be affected by the network changes. The average traffic in the detection method for UDP flood attacks will be affected by 5G network conditions, and the detection performance of both will be affected by mobility of the vehicles. When multiple nodes attack at the same time, the detection effect may not be ideal.

References

1. Zhou, H.: Research on traffic information collection and processing methods in the Internet of Vehicles. Jilin University (2013)
2. Xu, C.: Impact of 5G connected vehicles on the development of autonomous driving technology. Inf. Commun. 46–47 (2018)
3. Lin, T.: Research on multi-path TCP transmission and control in vehicle networking. Dalian University of Technology (2017)
4. Nan, Y., Rongbao, K.: Analysis and protection of vehicle network security threats. Commun. Technol. **48**(12), 1421–1426 (2015)
5. Chen, L.: Security threats and research status of Internet of Vehicles. http://wemedia.ifeng.com/73941858/wemedia.shtml. Accessed 16 Aug 2018
6. Huang, Y., Wan, L., Li, X.: SYN flooding attack based on IP spoofing. Comput. Technol. Dev. **18**(12), 159–161,165 (2008)
7. Zou, C., Liu, P., Tang, X.: Real-time defense of DHCP flood attack in SDN network. Comput. Appl. http://knsCnki.net/kcms/detail/51.1307.TP.20181203.1628.008.html. Accessed 16 Aug 2018
8. Liu, P., Sheng, Z.: Defending against TCP SYN flooding with a new kind of SYN-agent. In: 2008 International Conference on Machine Learning and Cybernetics, Kunming, pp. 1218–1221 (2008)
9. Degirmencioglu, A., Erdogan, H.T., Mizani, M.A., Yılmaz, O.: A classification approach for adaptive mitigation of SYN flood attacks: preventing performance loss due to SYN flood attacks. In: NOMS 2016–2016 IEEE/IFIP Network Operations and Management Symposium, Istanbul, pp. 1109-1112. IEEE (2016)
10. Verma, K., Hasbullah, H., Kumar, A.: An efficient defense method against UDP spoofed flooding traffic of denial of service (DoS) attacks in VANET. In: 2013 3rd IEEE International Advance Computing Conference (IACC), Ghaziabad, pp. 550–555. IEEE (2013)
11. Chen, W., Li, Y., Liu, W.: Analysis of the progress and key technologies of the connected car industry ZTE. http://kns.cnki.net/kcms/detail/34.1228.TN.20200217.1748.004.html. Accessed 21 Feb 2020
12. Liangmin, W., Xiaolong, L., Chunxiao, L., Jing, Y., Weidong, Y.: Prospects of 5G telematics. J. Netw. Inf. Secur. **2**(06), 1–12 (2016)
13. Tang, H., Zeng, Y.: Detection of SYN flood attack based on semi-join list. Comput. Eng. **37**(19), 135–137,144 (2011)
14. Houmer, M., Hasnaoui, M.L., Elfergougui, A.: Security analysis of vehicular ad-hoc networks based on attack tree. In: 2018 International Conference on Selected Topics in Mobile and Wireless Networking (MoWNeT), Tangier, pp. 21–26. IEEE (2018)