Turkish Journal of Science & Technology
17(2), 233-239, 2022

Research Paper
https://doi.org/10.55525/tjst.1054070

A Defense Mechanism Against DoS Attacks on Unmanned Aerial Vehicle Communication

Vedat TÜMEN[1]*, Kubilay DEMİR[2]
[1]Department of Computer Engineering, Faculty of Engineering
[2]Architecture, Bitlis Eren University, Bitlis, Turkey
*[1]vtumen@beu.edu.tr, [2]kdemir@beu.edu.tr

(Geliş/Received: 06/01/2022 Kabul/Accepted: 04/06/2022)

Abstract: The use of Unmanned Aerial Vehicles (UAV) in every field is increasing rapidly. In order for UAVs to perform their duties correctly, they must be able to maintain continuous communication with ground stations. The use of WiFi wireless communication protocol has increased due to its high bandwidth. One of the most important threats that can threaten this type of communication is Denial of Service (DoS) attacks. In the event of such an attack, the UAV becomes inaccessible and may crash. Especially when the open port number is known, it becomes much easier to perform attacks that consume the resources of the drone. In this study, a mechanism is proposed to eliminate or at least mitigate the attack risk. This mechanism enables UAVs using wireless communication (WiFi) to communicate using TCP over UDP using middleware. In addition, by periodically changing the UDP open ports with a secret port number sequence known to both parties, it prevents the attacker from using the open port for a long time and renders the attack ineffective. In this study, the effects of the port hopping method on UAVs are evaluated. Test results on real systems shows that the proposed system makes the communication system of UAVs more resistant to DoS attacks by 91.2%.

Key words: Unmanned aerial vehicle, DoS, Defense mechanism.

İnsansız Hava Araçların Haberleşmesine Yönelik Saldırılara Yönelik bir Savunma Mekanizması

Öz: İnsansız Hava Araçlarının (İHA) her alanda kullanımı hızlı bir şekilde artmaktadır. İHA'ların doğru bir şekilde görevlerini yerine getirebilmeleri için yer istasyonları ile devamlı olarak haberleşmelerini sürdürebilmeleri gerekir. WiFi kablosuz haberleşme metodu yüksek bant genişliği nedeni ile kullanımı artmıştır. Bu haberleşme tipini tehdit edebilecek en önemli tehditlerden biri Hizmet Reddi (DoS) saldırılarıdır. Bu tip bir saldırı durumunda İHA ulaşılmaz olur ve düşebilir. Özellikle açık port numarasının bilinme surumun da dronun kaynaklarını tüketecek ataklar gerçekleştirmek çok daha kolay hale gelir. Bu tehlikeyi gidermek veya en azından hafifletmek amacıyla bu çalışmada bir mekanizma önerilmiştir. Bu mekanizma kablosuz haberleşme (WiFi) kullanan İHA'ların TCP kullanarak gerçekleştiği haberleşmeyi arabir yazılım (middleware) kullanılarak UDP üzerinden yapmasını sağlar. Ayrıca UDP açık portlarını iki tarafın bildiği gizli bir port numarası dizilimi ile periyodik olarak değiştirerek saldırganın açık portu bulması durmda uzun süre kullanımını engeller ve saldırıyı etkisiz kılar. Bu çalışmada port atlatma (port hopping) metodunun İHA'lar üzerine uygulamasını ve etkileri incelenecektir. Gerçek sistemler üzerinde yapılan testler önerilen sistemin İHA'ların haberleşme sistemini %91.2'ye kadar daha fazla DoS ataklarına dayanıklı kıldığını göstermiştir.

Anahtar kelimeler: İnsansız hava aracı, DoS, Savunma mekanizması.

1. Introduction

The usage area of Unmanned Aerial Vehicles (UAV) has expanded to many areas from personal use to flying base stations. As examples of recently popular usage areas; agriculture, mapping, security, search and rescue, filming, etc. In addition, we witness the introduction of a new usage area every day [1].

Commercial mini and micro UAVs use WiFi communication protocol due to video transmission requirements [2]. WiFi protocol is a promising protocol whose features are being developed day by day. Supporting a communication distance of around one hundred meters, WiFi supports data transfer up to seven hundred bits per second. Due to these superior features, it is widely used in commercial UAVs [3]. The widespread use of the WiFi protocol in UAVs creates opportunities in many ways, as well as opportunities for attackers.

Such an attack on UAVs will be a common problem, since a Denial of Service (DoS) attack does not require a high level of specialized knowledge and hardware. When a DoS attack is made, the UAV is inaccessible to the

[1] Corresponding author: vtumen@beu.edu.tr. ORCID Number of authors:[1]0000-0003-0271-216X, [2]0000-0001-5355-2472

ground station. There are many types of DoS attacks [4]. Someone can make the device inaccessible by filling the entire communication channel with malicious packets, or can make the system inaccessible by consuming the system's resources with much less malicious packets. A powerful hardware is required to generate a large enough number of packets to fill the entire channel. These attacks can rarely be performed on UAVs. Attacks performed at higher Open Systems Interconnection (OSI) layers, such as Transmission Control Protocol (TCP) SYN attack, can be performed more easily with lower packet count [5].

In this study, a study was carried out to prevent attacks at the upper levels of OSI layers. The proposed defense approach prevents attacks on the 4th layer and above with a method applied in the 3rd layer (network layer). For this purpose, one of the most effective methods proposed in the literature is the port hopping method. This method is not suitable for use in all communication networks as it requires mutual secret sharing and can only be applied on the User Datagram Protocol (UDP) protocol [6-8]. For this reason, there are some applications in the literature for areas where high-level security is required in local networks or private wide area networks [9-11]. In this study, the application and evaluation of the port hopping mechanism on UAVs are performed. Although there are studies mentioning that port hopping mechanisms can be applied on UAVs, its application and evaluation has not been fulfilled [12].

The proposed model does not require changes in the software of commercial UAVs. It is assumed to allow commercial UAVs to install middleware on flight computers. On the ground station side, there are usually mobile phones. A separate middleware is also installed on this mobile phone side. These middlewares on both sides catch and forward TCP based messages to UDP. In addition, open UDP port numbers change in a known order only between the UAV and the mobile phone. The security provided by the proposed method has been tested with a test system. In the comprehensive evaluations, it has been observed that the system can withstand up to 91.2% more attacks when the proposed method is applied.

In the remainder of this article, the relevant studies in the literature in Section 2 and the model proposed in Section 3 are explained. In Section 4, the tests of the system were carried out, and finally, in Section 5, the results were given.

2. Related Works

With the widespread use of the Internet, DoS and (Distributed Denial of Service: DDoS) attacks seriously damage both the end users and the servers these users are connected to. Many different studies have been developed in the literature to prevent these damages.

Lee et al. proposed a new practical technique called port hopping to detect and block DoS/DDoS attacks. According to the method he proposed, based on the fact that the port numbers of the server change dynamically according to time and a cryptographic key shared between the server and the client, authorized clients stated that they could determine the valid port number used by the server, while malicious users stated that they could not find the valid port number [6]. The server can then easily filter out illegitimate packets by examining the port number found in the UDP/TCP headers. In the real-time experiment conducted on two computers, a port hopping mechanism was applied between client and server. With this mechanism, it sends UDP packets from client to server. The attacker fills the server with different rates of UDP packets at different rates. The filling speed of UDP packets to the server was determined and measures were taken. In this study, successful results were obtained depending on the traffic density in the network.

For a structure where cloud storage technology is used for smart electrical networks, both a hierarchical cloud structure and a port-hopping-based defense mechanism have been developed to prevent DoS attacks [7,8]. It also provides a structure for distinguishing aggressive and non-aggressive clients by using the port hopping structure.

Shi et al., using port and address skipping methods in network systems, suggested different methods aiming to establish a healthy communication under DoS/DDoS attacks and eavesdropping on the network in sending confidential information between departments and agents [9]. In this method, the client replicator performs data transfer via the data module and aims to provide secure information transfer by creating a jump address list between the server and the trusted client. When the results of this work he proposed were examined, he determined that the system he developed with the jump tactic had difficulties in getting the information from the audience and that he had to receive and analyze all the information. In this case, it has developed a system that examines much more and repetitive redundant data and causes great delays or difficulties in finding the useful data packet.

Shoufan et al. stated that the address hopping method can be used in the transmission of information packets in communication between UAV vehicles. In this study, different encryption methods have been developed and a more secure communication protocol has been tried to be made. As a result of the proposed study, it has been shown that DoS/DDoS attacks can have serious effects on UAV vehicles, therefore a secure communication protocol can be developed [12].

3. Proposed Method

In this study, a defense method is proposed to mitigate DoS attacks that can target vital communication systems for UAVs, the use of which is increasing rapidly today. In this method, the main goal is to block malicious connection requests at the network layer before they reach the upper layers. In order to achieve this, the open port numbers in the UAV and the end-user computer (smartphone, tablet, etc.) are changed periodically, according to a hidden secret. Thus, when an attacker who does not know the open port sends packets with the wrong port number, these packets are dropped at the network interface card. The proposed method for the realization of the scenario is presented in two stages, the attack and defense model.

3.1. Attack model

In this study, it is aimed to protect against DoS attacks targeting the layers above the network layer. As it is known, OSI layers consists of 7 layers, as denoted in Figure 1.

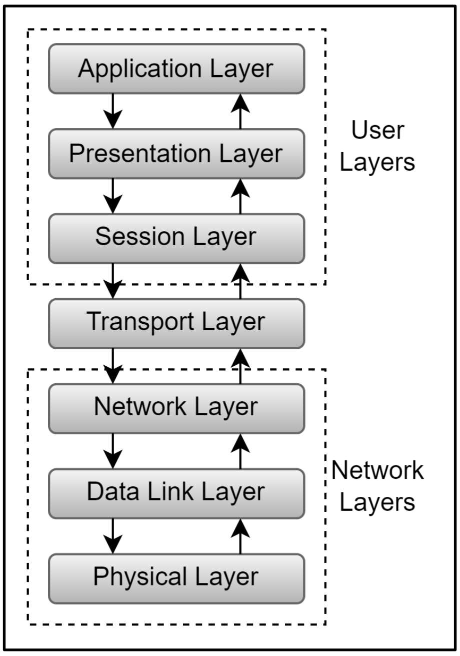

Figure 1. OSI network layers

With the low number of data packets, it is possible to completely consume computer resources (RAM, CPU, Eran Card, etc.) in the layers above the network layer. For this reason, it seems very risky for malicious packets to reach layers above Layer 3.

For example, the most well-known of these types of attacks are TCP SYN attacks. This type attack(TCP syn flood, 2021) can be expressed as: "In a TCP SYN attack, the attacker sends repeated SYN packets using a fake IP address to open a TCP connection on the targeted computer. The attacked computer receives a connection request, which it sees as bona fide, to communicate. It responds with a SYN-ACK packet for each connection request. But the malicious computer does not send the expected ACK. The attacked server waits for a while for the SYN-ACK packet to be acknowledged. During this time, the server cannot close the connection by sending an RST packet and the connection remains open. Before the connection times out, the attacker sends another SYN packet. This leaves more and more connections half-open. Eventually, as the server's connection tables fill up, legitimate clients are denied service and the server may even fail or crash" [13].

3.2. Proposed defence model

The proposed method suggests changing the open port number over time. However, in the basic system, due to the TCP connection structure, communication must be made over the same IP address and port during the session established. This makes port switching impossible on TCP. The proposed method to overcome this problem carries the communication over TCP over UDP with the help of a middleware (Middleware) installed on both the UAV side and the computer that acts as the remote controller. The proposed approach is illustrated visually in Figure 2.

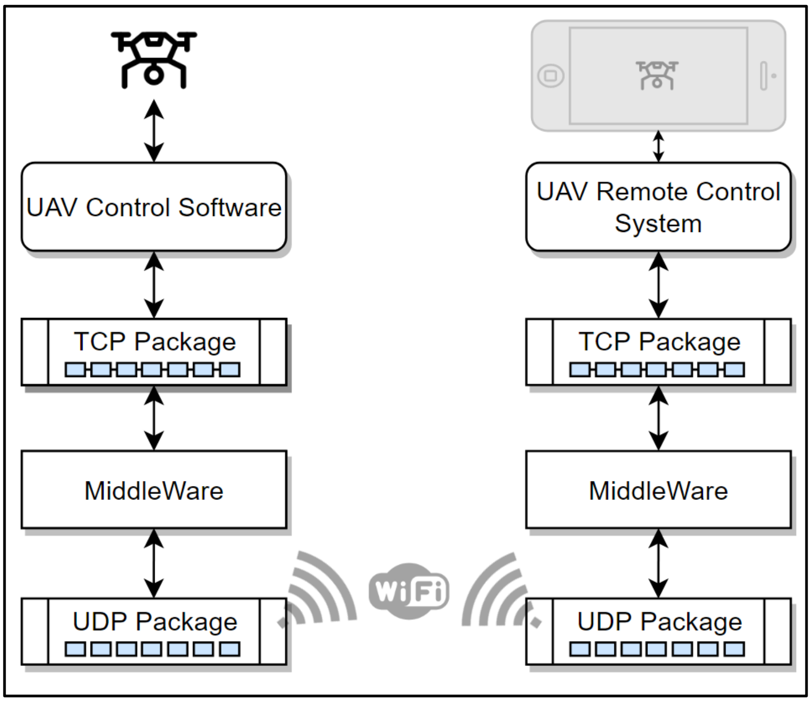

Figure 2. Proposed model.

As it can be seen in Figure 1, TCP packets coming out of the UAV control software on the remote controller are picked up by the developed middleware. This packet is sent to the known open UDP port of the other party over the currently open UDP port. On the UAV side, the middleware reads the open UDP port and receives these packets, then converts them to TCP format and delivers them to the control software. In this way, the proposed defence mechanism runs without the need for any changes in the UAV software.

It is an extremely demanding task for two parties to open and close the same ports at the same time. To achieve this, the middleware first periodically sends synchronized packets for clock synchronization. After the clock is synchronized, the port number is generated in the random number generator using a secret key password placed between the two parties during the setup. Since the same numbers are generated at the same time on both sides, the same ports are open at the same time. Therefore, both sides know which port to send the data to, but the attacker does not know this. Thus, the attacker's packets are dropped at the network layer. Figure 3 shows a DoS attack on a UAV in a field.

Figure 3. Image of the DoS attack on the UAV

4. System Test and Evaluation Results

In order to test the proposed method, the system is tested from several aspects: 1) the effect of the proposed system on the maximum communication capacity, 2) the resistance of the defense system against attacks. Figure 4 shows the effect of the proposed model on the maximum communication performance of the system

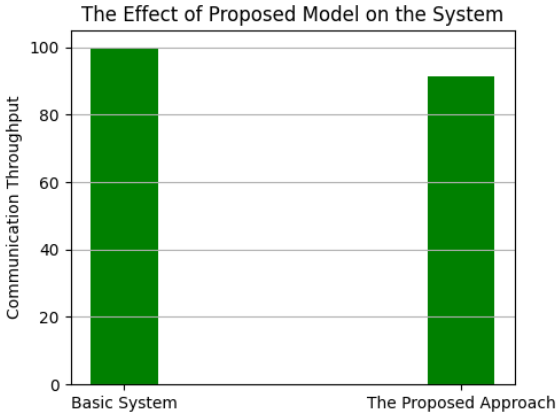

Figure 4. The effect of the proposed model on the maximum communication performance of the system

4.1. Communication throughput test

The burden of a proposed defense methodology on the current system should not exceed an acceptable level. Therefore, the system was tested without installing the developed software and then the maximum communication capacity (throughput) was measured. Afterwards, once the developed software is installed, how much decrease in the maximum communication capacity occurs is tested. As can be seen in Figure 5, a negligible (2%) performance drop was detected. This result shows that the proposed system can provide defense without a high overhead.

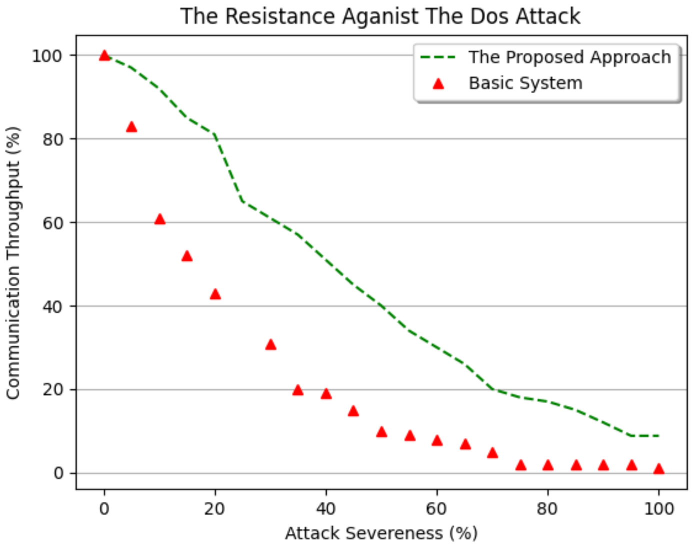

Figure 5. The resilience of the basic system and the system protected by the proposed model against attacks

4.2. System performance test

Secondly, we examined the effects of attacks on UAVs and on the UAV communication system for two cases: 1) Not using the proposed defense system and 2) Using the proposed defense system. In the event of an attack, it is compared how many malicious packets the UAV communication system can withstand. As it can be seen from Figure 4, 10% of the number of malicious packages that make the system with the proposed defense mechanism inaccessible becomes inaccessible when the proposed system is not used. This shows that if the proposed method is used, the system can withstand 91.2% stronger attacks.

5. Results

In this study, a defense system is presented against DoS attacks targeting the communication systems of UAVs. This defense system can be installed using a middleware without changing the software on the UAVs and on the controller. This middleware receives incoming packets over TCP and converts them to UDP format and sends the packets to the other party over the open port determined according to a secret between the UAV and the Remote Controller, the other party converts the packets back to TCP format and delivers them to the software. Open ports are changed over time according to the secret between the two parties. Thus, the open port is closed in the time required for the attacker to find the open port. It has been seen in the tests of the system that the proposed model provides an extra protection of 91.2% and brings a reasonable overhead for the system. As a future work, we plan to develop a mitigation method to address physical layer attacks such as jamming, interference vb.

References

[1] Savkin, A. V., & Huang, H. (2018). “Deployment of unmanned aerial vehicle base stations for optimal quality of coverage,” *IEEE Wireless Communications Letters*, *8*(1), 321-324.

[2] Bernal, S. A. S. (2016). “*Detection solution analysis for simplistic spoofing attacks in commercial mini and micro UAVs”* (Doctoral dissertation, MS thesis, University Of Tartu).

[3] Lin, H. Y., Tu, K. C., & Li, C. Y. (2020). “VAID: An aerial image dataset for vehicle detection and classification,” *IEEE Access*, *8*, 212209-212219.

[4] Huseinović, A., Mrdović, S., Bicakci, K., & Uludag, S. (2020). “A survey of denial-of-service attacks and solutions in the smart grid”. *IEEE Access*, *8*, 177447-177470.

[5] Zeebaree, S. R., Jacksi, K., & Zebari, R. R. (2020). “Impact analysis of SYN flood DDoS attack on HAProxy and NLB cluster-based web servers”. *Indones. J. Electr. Eng. Comput. Sci*, *19*(1), 510-517.

[6] Lee, H. C., & Thing, V. L. “Port hopping for resilient networks”. In IEEE 60th Vehicular Technology Conference, 2004. VTC2004-Fall. 2004: Vol. 5, pp. 3291-3295.

[7] Demir, K., “A Secure and Reliable Communication Platform for the Smart Grid”. Ph.D. Thesis, Darmstadt, Technische Universität, 2017.

[8] Demir, K., Ismail, H., Vateva-Gurova, T., & Suri, N. “Securing the cloud-assisted smart grid”. International Journal of Critical Infrastructure Protection, 2018; 23, 100-111.

[9] Shi, L., Cui, Y., Liu, X., Sun, H., Xue, Z., & Zhang, S. “A covert communication scheme based on DNA microdots for port hopping”. International Journal of Performability Engineering, 2017; 13(5), 598.

[10] Luo, Y. B., Wang, B. S., & Cai, G. L. “Analysis of port hopping for proactive cyber defence.” International Journal of Security and Its Applications, 2015; 9(2), 123-134.

[11] Luo, Y. B., Wang, B. S., Wang, X. F., Hu, X. F., Cai, G. L., & Sun, H. “RPAH: Random Port and Address Hopping for Thwarting Internal and External Adversaries”. IEEE Trustcom/BigDataSE/ISPA, 2015; Helsinki, Finland, Vol. 1, pp. 263-270.

[12] Shoufan, A., Yeob Yeun, C., & Taha, B. “eSIM-Based Authentication Protocol for UAV Remote Identification”. Security and Privacy in the Internet of Things: Architectures, Techniques, and Applications, 2021; 91-122.

[13] TCP syn flood: Ddos attack glossary: Imperva. Learning Center. Retrieved December 24, 2021, from https://www.imperva.com/learn/ddos/syn-flood/