

Detecting man-in-the-middle attacks via hybrid quantum-classical protocol in software-defined networks

Thakwan A. Jawad, Awan Nahel Mahmood, Abdulhameed N. Hameed

Department of Systems and Control Engineering, College of Electronics Engineering, Ninevah University, Mosul, Iraq

Article Info

Article history:

Received Sep 2, 2022

Revised Feb 11, 2023

Accepted Feb 18, 2023

Keywords:

BB84 protocol

Diffie-Hellman

Man-in-the-middle attack

Quantum key distribution

Software-defined networking

ABSTRACT

Man-in-the-middle (MitM) attacks became one of the most risk attacks on OpenFlow communication channel in software-defined networking, its detection is a very hard task due there is no authentication in OpenFlow protocol. This channel is the most important in the network and is responsible for sending the control commands from the controller to the switches, so once the OpenFlow channel is hacked, the entire network is controlled by the attacker. Therefore, we propose a complementary solution to transport layer security protocol to detect man-in-the-middle attacks based on hybrid quantum-classical protocol. Based on the hybrid protocol, an easy-to-implement authentication between controller and switches depends on quantum and classical security layers. Also, detect eavesdropping on channel depending on quantum parameters. In this paper, we implement a simulation of hybrid protocol using a software-defined networking emulator for monitoring the OpenFlow channel to detect attacks, and the results showed the ease of detecting the eavesdrop and verifying the authentication of the other party with a hybrid method to get a high level of authentication.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Awan Nahel Mahmood

Department of Systems and Control Engineering, College of Electronics Engineering, Ninevah University

Mosul, Iraq

email: awan.mahmood@uoninevah.edu.iq

1. INTRODUCTION

Over the last decade, researchers have focused on transforming networks into a more open, programmable, reliable, secure, and manageable infrastructure. Software-defined networks (SDNs) are the main result of this effort and the basic concept is to separate network control from a data plane. So led need to the communication channel between these two planes to send commands, requests, and statistics. this channel is called OpenFlow [1], [2]. The basic role of the OpenFlow protocol is to define the communication protocol that manages the interaction between the SDN controller and the network forwarding devices like switches and routers, so it becomes easier to change the configuration according to the business requirements. So, protecting this channel is important to protect the entire network [3]–[5]. The man-in-the-middle (MitM) attack is one of the most dangerous attacks on SDN, where the attacker becomes a malicious third party in the communication process of the victims without their knowledge. MitM attackers can copy, modify and replace victims' traffic, causing significant damage to victims and posing a real risk on communication channel [6]–[8].

The MitM attack has different types, but the kind that threat of OpenFlow protocol security is its attempt to access the encryption key because once get the key to encrypt the communication channel between the controller and the switch. Then, it is very easy for the attacker to modify the OpenFlow messages such as changing the flows by modifying the switch forwarding table and gathering information.

There are many traditional methods used to provide authentication between two parties to avoid attacks that are efficient on a certain level of classic attacks. In the process of protecting the OpenFlow communication channel which used the traditional ways of detecting down the MitM attack such as using authentication in transport layer security (TLS) protocol [9], [10] but have many weaknesses [11]. So, many researches are focused on the security protocols to protect against MitM attacks. Nisar *et al.* [12] proposed the use of the TLS protocol to protect the OpenFlow communication channel against the MitM attack but in 2017 both Agborubere and Sanchez-Velazquez [11] proved that the TLS protocol has contained security holes of such attacks, so they proposed adding messages between the two parties to verify authentication to protect against MitM attacks. While in 2018, Zhang and Qiu [13] proposed a proactive detection mechanism CMD to detect MitM attacks in SDN based on connection characteristics of network traffic, without the analysis of packet contents. On other hand, Hugues-Salas *et al.* [14] proposed using the parameters of quantum key distribution protocols to detect the attacks of DDoS and MitM. This provides a high level of authentication and detection of eavesdropping based on the physical properties of quantum mechanics. The first quantum key distribution protocol was proposed in 1984 by Bennet and Brassard, it was later called BB84 [15]. It utilized the uncertainty concept and no-cloning theorem [16] to guarantee that the transmission of the key has not been eavesdropped on or changed, so considered an important cryptography method aimed to solve several network security problems [17]–[19]. This protocol uses two bases rectilinear and diagonal to prepare photon states. In this paper, we propose a system to detect MitM attacks based on a hybrid quantum-classical protocol to achieve authentication between two endpoints. On the other hand, monitoring the parameters of quantum key distribution (QKD) protocol to predict any attempt to eavesdrop to secure the communication channel. In our proposal, the hybrid protocol was implemented to achieve adequate security for the communication channel between the controller and switches in software-defined networks so the proposed protocol could be considered as complementary to TLS security protocol to achieve adequate security for OpenFlow messages.

This paper is organized as section 2 explains quantum key distribution and BB84 protocol while in section 3 we present the hybrid quantum-classical protocol. In section 4, we show the proposed model to detect and prevent MitM attacks in software-defined networking. In section 5 presents the main results and simulation and section 6 shows the security analysis and finally in section 7 provides the concluding remarks.

2. QUANTUM KEY DISTRIBUTION PROTOCOL

The progress in quantum physics has led to thinking of new ways to ensure security in communication. Designers of encryption systems had to think about a new encryption system and solve distribute the key securely in symmetric encryption systems. In the distribution of the quantum key, a single or entangled quantum is transferred between two parties [20]. Each of the parties has two channels: the quantum channel for the exchange of quantum and the classic public channel to check for eavesdropping. If a third party makes measurements of the transferred quantum, both of party will discover an eavesdropper presence on the public media. Depending on the rules of the mechanics of quantum, the measurement performed by the eavesdropper will modify the quantum state [20], and also cannot clone an arbitrary quantum state. In 1984, Charles H. Bennet” and “Gilles Brassard” proposed the first QKD protocol, and therefore called “BB84” [15]. The BB84 protocol uses quantum and classical channels. Uses a quantum channel such as optical fiber to send pulses of polarized light, where each pulse contains one photon. And a classical public channel, such as a telephone line or internet connection for an established authentication between the parties. In general, the main idea of the security of QKD protocols and BB84 protocol depends on the exploitation of the no-cloning theorem and the superposition principle [16], [21]–[23].

3. HYBRID QUANTUM-CLASSICAL PROTOCOL

The hybrid protocol was proposed to be complementary to the TLS protocol and thus aims to achieve full security for OpenFlow messages. In the hybrid protocol [24], [25], the classic Diffie-Hellman protocol was integrated with the QKD-BB84 protocol to achieve two levels of authentication. The first is through the physical properties of quantum bits and the second level is achieved by the classical authentication channel. To explain the protocol more clearly, the protocol function will be presented in two stages The first stage uses a quantum channel: the polarized photons are prepared based on random bases and random bits. The polarized photons are transmitted through a quantum channel to the other side. These photons, based on the theory of non-cloning, any attempt to eavesdrop on the state of the photon is detected by both parties. While, in the second stage, the process of authentication between the parties through a classic channel is performed. Where the random bases and the parameters of Diffie-Hellman and time-stamp are sent with hashing code to achieve authentication, then both parties calculate their keys by combining the classic and quantum key using XOR operation as shown in Figure 1.

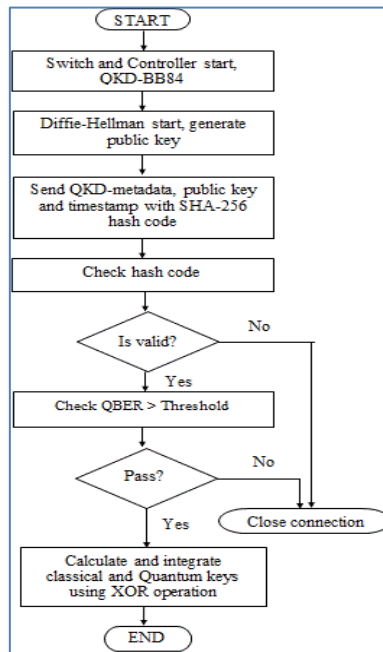


Figure 1. Hybrid quantum-classical protocol

4. PROPOSED WORK

In this work, we focus on how to detect MitM attacks in less time and more accurately. Also, we do a simple procedure to prevent the risk of attack on the network by closing the connection and port. So we suggest a hybrid protocol to achieve authentication and detect MitM attacks on the OpenFlow channel depending on quantum parameters such as quantum bit error rate (QBER) and secret key rate (SKR). Achieving authentication will be based on the rules of quantum mechanics and the hash code of the traditional method. The proposed action aims to detect MitM attack begins with the operation of hybrid protocol and agreement on threshold max-error between switch and controller, this threshold determined based on channel noise without an attack.

On the other hand, basic parameters are exchanged for measuring photons and calculating the key. The controller then checks the authentication code sent over the classic channel to make sure that the switch is intended for it, then calculates the error rate of the generated key and compares it with an agreed threshold. If the error rate is greater than the minimum, this indicates that the MitM attacker has modified the status of the transfer photon. Depending on the characteristics of the quantum mechanics [11], the parties will know that a third party has modified the status of the photon transmitted through their communication channel. Algorithm 1 explains the overall process of authentication and detection of MitM attacks by the controller as shown in Figure 2, while Algorithm 2 explains the authentication achievements between the controller and the switch. When the controller detects a MitM attack on the OpenFlow channel, this will perform a precaution like closing the connection and deleting the port. The algorithm code is shown in Figure 3.

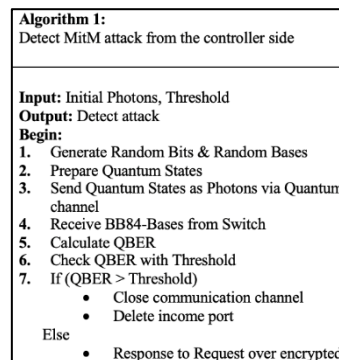


Figure 2. Authentication process code of MitM attacks

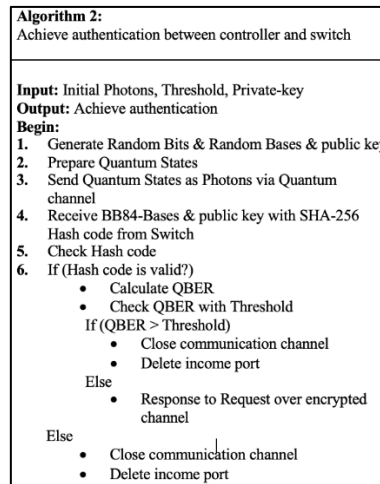


Figure 3. Authentication achievements code of MitM attacks

5. SIMULATION RESULTS

To prove the efficiency of the proposed work, we implement this work on a software-defined network (SDN) with and without the existence of MitM attack and then monitor the results of QBER. The simulation of the SDN environment has been developed by using a mininet emulator with ryu controller and python programming language. So in the first, hybrid protocol was operated between the switch and the controller without an attack for more than one time and with different entries for the number of initial photons to determine the limit of the threshold to be used later:

$$QBER = \frac{N_{wrong}}{N_{wrong} + N_{right}} \quad (1)$$

where (N wrong) is the number of photons that are not detected, and (N right) is the number of photons that are right detected. Table 1 shows the length of the final key and QBER. Also, we are calculating QBER depending on (1) [20].

Based on the above results, the threshold limit is set to 49%. After this, the hybrid protocol was run again between the switch and the controller in the presence of the MitM attack more than once and with different entries for the initial number of photons. The results show that the QBER is more than the minimum, meaning that the attacker has modified the status of the photons as shown in Table 2.

Table 1. The final key length and QBER in case of MitM attack

No. Try	Initial Qbits=256		Initial Qbits=512		Initial Qbits=1024		Initial Qbits=2048	
	Len. Key	QBER	Len. Key	QBER	Len. Key	QBER	Len. Key	QBER
Try 1	132	48%	252	50%	523	48%	981	52%
Try 2	136	46%	245	52%	502	50%	1,005	50%
Try 3	126	50%	259	49%	514	49%	1,070	47%
Try 4	128	50%	271	47%	553	45%	1,028	49%
Try 5	134	47%	246	51%	530	48%	1,013	50%
Mean	131	48%	254	49%	524	48%	1,019	49%

Table 2. The final key length and QBER with the presence of MitM attack

No. Try	Initial Qbits=256		Initial Qbits=512		Initial Qbits=1024		Initial Qbits=2048	
	Len. Key	QBER	Len. Key	QBER	Len. Key	QBER	Len. Key	QBER
Try 1	63	75%	125	75%	253	75%	511	75%
Try 2	58	77%	126	75%	254	75%	492	75%
Try 3	69	73%	122	76%	234	77%	523	74%
Try 4	60	76%	133	74%	270	73%	508	74%
Try 5	68	73%	142	72%	279	72%	527	74%
Mean	63	74%	129	74%	258	74%	512	74%

The difference of QBER in the case with and without absence MitM attacker has been displayed in Figure 4. Obtained results show that the QBER is more than the threshold, so the attacker can be detected simply. Figure 5 shows the running of MitM attack on mininet emulator to measure the sending keys as a quantum again to switch. Figure 6 shows the quantum IDs sent between controller and switch using the Wireshark tool.

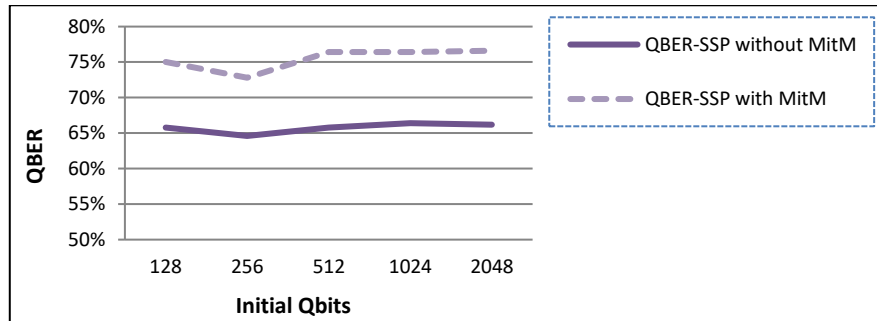


Figure 4. QBER comparison

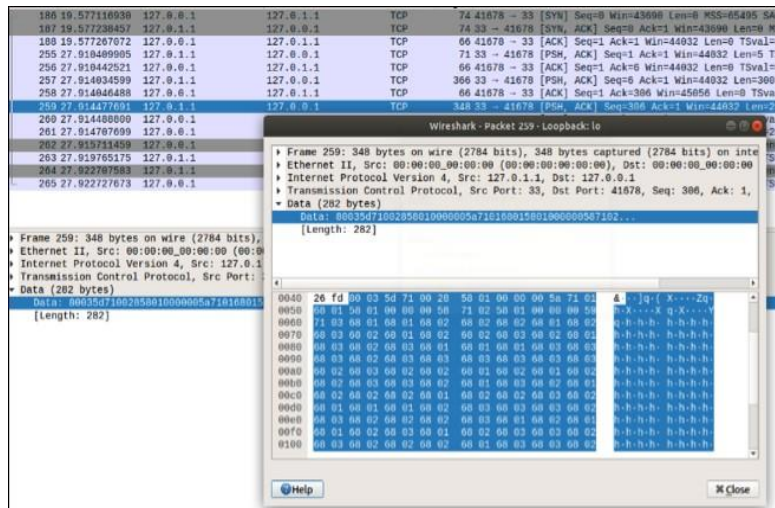


Figure 5. MitM attacker

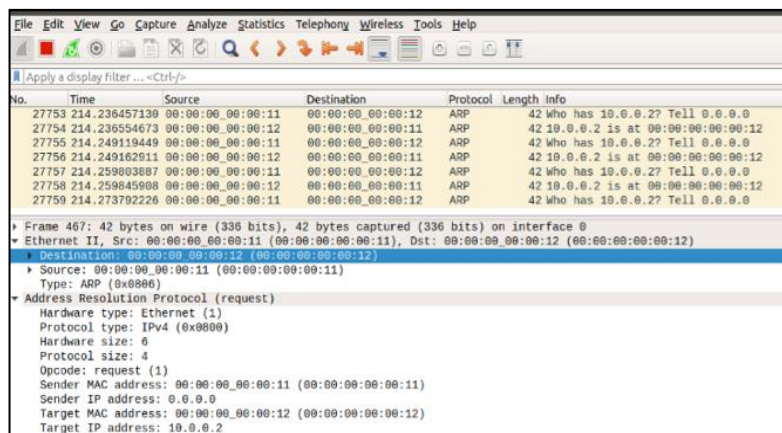


Figure 6. The communication between controller and switch

6. SECURITY ANALYSES

We are offering some analysis of the hybrid protocol as in: i) QKD-BB84 is controlled by SDN-controller in the result, only the legitimate switches can get quantum key which permits only these switches to connect to the controller, ii) in the proposed protocol the classical channel achieved authentication by using the SHA-256 hash function as well as the freshness of hash code by adding a timestamp, and iii) based on quantum properties that are protected from eavesdroppers, all this can bring authentication between controller and switches.

So, a MitM attack on the OpenFlow channel can be detected and mitigated through these measures. Mitigating the risk of a MitM attack on the OpenFlow channel requires a combination of preventive and detective measures. Implementing security best practices, such as using strong authentication mechanisms as in our proposed idea, regularly updating software and firmware, and using encryption, can help prevent MitM attacks.

7. CONCLUSION

A result of the rapid development and trend towards more manageable and programming networks, this led to the emergence of software-defined networks. On the other hand, the problem of MitM attack on the OpenFlow channel that connects the controller to the data plane threatens the entire network security. Therefore, we suggest a way to detect MitM attacks by relying on the quantum-classical protocol. This method can detect the attack in real-time and with high accuracy and authentication because we rely on QKD parameters and properties of quantum mechanics to detect this type of attack, as well as classical ways to achieve authentication. This work was performed on the mininet emulator by using the Python programming language. Obtained results show the difference in QBER rate in the case of the presence and absence of MitM attacker. So it is easy to detect the attacker and take the necessary action by the SDN-controller.




REFERENCES

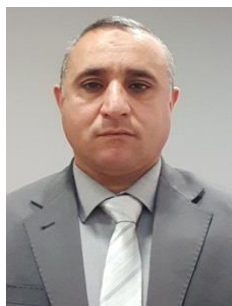
- [1] K. Benzekki, A. El-Fergougui, and A. E. Elaloui, "Software-defined networking (SDN): a survey," *Security and Communication Networks*, vol. 9, no. 18, pp. 5803–5833, Dec. 2016, doi: 10.1002/sec.1737.
- [2] M. K. Jaiswal, "Introduction to OpenFlow," in *Innovations in Software-Defined Networking and Network Functions Virtualization*, 2018, pp. 52–71.
- [3] D. Kreutz, J. Yu, F. M. V. Ramos, and P. Esteves-Verissimo, "Anchor: Logically centralized security for software-defined networks," *ACM Transactions on Privacy and Security*, vol. 22, no. 2, pp. 1–36, May 2019, doi: 10.1145/3301305.
- [4] H. M. Fadhil and A. A. Abdullah, "Enhancement datagram transport layer security protocol based on BB84 protocol in the internet of things," *AIP Conference Proceedings 2547, 060005*, vol. 2547, no. 1, pp. 060005-1–060005-12, Dec. 2022, doi: 10.1063/5.0112138.
- [5] J. Lam, S. G. Lee, H. J. Lee, and Y. E. Oktian, "Securing SDN southbound and data plane communication with IBC," *Mobile Information Systems*, vol. 2016, pp. 1–12, 2016, doi: 10.1155/2016/1708970.
- [6] S. Kaur, K. Kumar, and N. Aggarwal, "A review of security threats in software-defined networking," *Intelligent Computing and Communication Systems*, pp. 123–131, 2021.
- [7] A. Sebbar, K. Zkik, Y. Baddi, M. Boulmalf, and M. D. E. C. El-Kettani, "MitM detection and defense mechanism CBNA-RF based on machine learning for large-scale SDN context," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 12, pp. 5875–5894, Dec. 2020, doi: 10.1007/s12652-020-02099-4.
- [8] S. B. Sadkhan, M. S. Abbas, S. S. Mahdi, and S. A. Hussein, "Software-defined network security - status, challenges, and future trends," in *Al-Muthanna 2nd International Conference on Engineering Science and Technology, MICEST 2022 - Proceedings*, Mar. 2022, pp. 10–15, doi: 10.1109/MICEST54286.2022.9790219.
- [9] B. Dowling, M. Fischlin, F. Günther, and D. Stebila, "A cryptographic analysis of the TLS 1.3 handshake protocol," *Journal of Cryptology*, vol. 34, no. 4, p. 37, Oct. 2021, doi: 10.1007/s00145-021-09384-1.
- [10] R. Oppliger, *SSL and TLS: Theory and practice*. Artech House Publishers, 2009.
- [11] B. Yigit, G. Gur, B. Tellenbach, and F. Alagoz, "Secured communication channels in software-defined networks (double)," *IEEE Communications Magazine*, vol. 57, no. 10, pp. 63–69, Oct. 2019, doi: 10.1109/MCOM.001.1900060.
- [12] K. Nisar et al., "A survey on the architecture, application, and security of software defined networking: Challenges and open issues," *Internet of Things (Netherlands)*, vol. 12, p. 100289, Dec. 2020, doi: 10.1016/j.iot.2020.100289.
- [13] K. Zhang and X. Qiu, "CMD: A convincing mechanism for MITM detection in SDN," in *2018 IEEE International Conference on Consumer Electronics, ICCE 2018*, Jan. 2018, vol. 2018-January, pp. 1–6, doi: 10.1109/ICCE.2018.8326334.
- [14] E. Hugues-Salas et al., "Experimental demonstration of DDoS mitigation over a Quantum key distribution (QKD) network using Software Defined Networking (SDN)," in *Optics InfoBase Conference Papers*, 2018, vol. Part F84-OFC 2018, p. M2A.6, doi: 10.1364/OFC.2018.M2A.6.
- [15] D. Alvarez and Y. Kim, "Survey of the development of quantum cryptography and its applications," in *2021 IEEE 11th Annual Computing and Communication Workshop and Conference, CCWC 2021*, Jan. 2021, pp. 1074–1080, doi: 10.1109/CCWC51732.2021.9375995.
- [16] Y. C. Chen, M. Gong, P. Xue, H. D. Yuan, and C. J. Zhang, "Quantum deleting and cloning in a pseudo-unitary system," *Frontiers of Physics*, vol. 16, no. 5, p. 53601, Oct. 2021, doi: 10.1007/s11467-021-1063-z.
- [17] O. Amer, V. Garg, and W. O. Krawec, "An introduction to practical quantum key distribution," *IEEE Aerospace and Electronic Systems Magazine*, vol. 36, no. 3, pp. 30–55, Mar. 2021, doi: 10.1109/MAES.2020.3015571.
- [18] A. A. Abdullah, R. Z. Khalaf, and H. B. Habib, "Modified BB84 quantum key distribution protocol using legendre symbol," in *SCCS 2019 - 2019 2nd Scientific Conference of Computer Sciences*, Mar. 2019, pp. 154–157, doi: 10.1109/SCCS.2019.8852619.




- [19] A. A. Abdullah and Y. H. Jassem, "Enhancement of quantum key distribution protocol BB84," *Journal of Computational and Theoretical Nanoscience*, vol. 16, no. 3, pp. 1138–1154, Mar. 2019, doi: 10.1166/jctn.2019.8009.
- [20] S. Pirandola *et al.*, "Advances in quantum cryptography," *Advances in Optics and Photonics*, vol. 12, no. 4, p. 1012, Dec. 2020, doi: 10.1364/aop.361502.
- [21] M. S. Zubairy, *Quantum mechanics for beginners: with applications to quantum communication and quantum computing*. New York: Oxford: Oxford University Press, 2020.
- [22] G. Popescu, *Principles of biophotonics, volume 1: linear systems and the fourier transform in optics*. IOP Publishing, 2019.
- [23] M. A. Nielsen, I. Chuang, and L. K. Grover, "Quantum computation and quantum information," *American Journal of Physics*, vol. 70, no. 5, pp. 558–559, May 2002, doi: 10.1119/1.1463744.
- [24] A. A. Abdullah and S. S. Mahdi, "Hybrid quantum-classical key distribution," *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 12, pp. 4786–4791, Oct. 2019, doi: 10.35940/ijitee.L3682.1081219.
- [25] S. S. Mahdi and A. A. Abdullah, "Improved security of SDN based on hybrid quantum Key distribution protocol," in *Proceedings of the 2nd 2022 International Conference on Computer Science and Software Engineering, CSASE 2022*, Mar. 2022, pp. 36–40, doi: 10.1109/CSASE51777.2022.9759635.

BIOGRAPHIES OF AUTHORS






Thakwan A. Jawad    received a B.Sc. degree from the technical computer engineering collage at the Technical University of Technical North, Iraq, in 2004. M.Sc. degree in computer engineering/computer security from the Eastern Mediterranean University (EMU), Cyprus, 2014. He is working as an assistant lecturer in the electronic engineering department at Ninevah University, systems and control engineering department. He is computer literate in the OPNET program, which he used in the field of networks. He can be contacted at email: thakwan.jawad@uoninevah.edu.iq.



Awan Nahel Mahmood    received a B.Sc. degree from the technical computer engineering collage at the Technical University of Technical North, Iraq, in 2005. M.Sc. degree in computer engineering/computer network from the Eastern Mediterranean University (EMU), Cyprus 2014. respectively. Previously he worked in the electronic engineering department at Mosul University and in systems and control department at Ninevah University, as an assistant lecturer at Ninevah University. He is computer literate in the MATLAB and OPNET programs, which he used in the field of networks. The experiment in the classroom: In 2019, I will be directing a graduation project titled design of a Wi-Fi network using OPNET modeler for senior students in the fourth class-electronic section. He can be contacted at email: awan.mahmood@uoninevah.edu.iq.



Abdulhameed N. Hameed    received the B.Sc. degree in communication engineering from the University of Mosul, Mosul, Iraq, in 2006, and the master's degree in communication engineering from the University of Mosul, Mosul, Iraq, in 2013. He is working as a lecturer with the college of electronics engineering, Ninevah University (2013-present). He is an instructor in electronics engineering college CISCO Networking Academy (2009-present). His current research interests include computer networking, wireless ad hoc networks, mobile ad hoc networks, wireless communications, vehicular communication technology, network security, and IoT. He can be contacted at email: abdulhamed.hameed@uoninevah.edu.iq.