Indonesian Journal of Electrical Engineering and Computer Science
Vol. 19, No. 2, August 2020, pp. 940~948
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v19.i2.pp940-948

Multi-level cyber security system for VANET

Muntadher Naeem Yasir[1], Muayad Sadik Croock[2]
[1]Department of Computer Science Iraqi Commission for Computers and Informatics (ICCI), Iraq
[2]Computer Engineering Department, University of Technology, Iraq

Article Info

Article history:

Received Dec 4, 2019
Revised Feb 6, 2020
Accepted Feb 19, 2020

Keywords:

C2C
C2I
Cyber security
DoS attack
VANET

ABSTRACT

Recently, the cyber security of vehicular ad-hoc network (VANET) including two practicable: car-to-car and car-to-infrastructure has been considered due to importance. It has become possible to keep pace with the development in the world, where the safety of people is a priority in the development of technology in general and in particular in the field of VANET. In this paper, a cyber security system for VANET has been proposed to tackle the DOS attacks. The proposed system includes three security levels. Firstly, the registeration level that ask vehicles to be registered in the system, in which the network exclude the unrigestered ones. Secondly, the authentication level that checks the vehicles before joining the network. This is done by applying a proposed algorithm that considers the hash function and factory number. Thirdly, the proposed system ables to detect the DOS attack by any involved vehicle using the monitoring algorithm that allocate such vehicle to be excluded from the network. The obtained results show the efficient performance of the proposed system in managing the security of the VANET network. The multi-level system increases the security of the network, in which the attacks can be eliminated.

Corresponding Author:

Muntadher Naeem Yasir,
Department of Computer Science,
Iraqi Commission for Computers and Informatics (ICCI),
Informatic Institute for Postgraduate Studies, Iraq.
Email: muntadher.naeem@yahoo.com

1. INTRODUCTION

Road transport focuses on people because the safety of them is the one of concerns in building a VANET network. In many countries, licensing requirements and safety regulations guarantee the separation of these two sectors. Road traffic is made by car or truck that can be targeted by DoS attackers as a prevalent in VANET. These attacks lead to damage of the safety of stirrups, and made them take a path that may lead to harm them and enter the maze of traffic congestion [1, 2].

Different studies and research work in the field of security in VANET had been presented to tackle the araised problems in terms of communication, data transmission and people safety. In [3, 4], the authors focused on Service Denial (SD) attacks that prevents end-users receiving the right data at the right moment. They analyzed SD attacks, behavior and effects on the network using various analytical models to detect an efficient answerusing different steps. Step one was building the simulator of VANET that analyzed the behavior of the network under this attack. Step two compared the proposed network with a normal network without attack to grasp the network's behavior under this type of attacks. Step three used many mathematical methods to predict if a car was under an attack or not. Authors have observed that logistic regression and neural network are better than Mean Squared Error (MSE), Root Mean Square (RMS) and Means Absolute Value (MAV) to analyze information and to predict attacks. Each parameter from the simulation was studied using the logistic regression to read the effects in details. In [5, 6], VANET turned any shared node into a wireless router network or car to cover a range of 100 to 300 meters as a base for establishing a network

with a wide group. The authors presented an absolute overview and discussion in VANET to give a rich survy. In [7], a malicious and irrelevant packet detection algorithm were proposed, used to analyze and find the Denial of Service attack. It also lessened the overhead delay in the information analysis and processing, which increased the connect in coming times. The authors of [8, 9] suggested a reaction technique against Denial-of-Service attacks in VANET. They believed that these contributions were very useful for determining the Denial-of-Service attack reaction issue on VANETs. In [10], the authors classified the VANET system based on its capability, following attackers can be responsible for the Denial of Service (DOS) attack. In [11], authors presented a set of possible denial-of-service attacks. The first level talked about attacks that occur between Vehicles to Vehicles (V2V). It pointed out that the attacker sends false messages to the victim to be occupied and separated from the service in the network. On the other side, the intruder sends messages to the RSU running busy without contacting other Vehicles to Infrastructure (V2I).

As a result, the literary study of some researchers regarding DoS attacks leads to considerd a lightweight protocol based on Vasudev work. The proposed system differs in terms of construction, phases, and handling of DoS attacks, unlike what Vasudev did. The proposed system supports two different types of communication, Car-to-Car (C2C) and Car-to-Infrastructure (C2I).

2. PROPOSAL SYSTEM

As mentioned earlier, the proposed system considers the security at cyber level for VANET. The proposed sysem can be divided into different sub-sections as follows.

2.1. Proposal system structure

Figure 1, Shows the the proposed schema that uses the lightweight protocol due to limitation of storage memory employing the technology of time difference. This schema explains the three security levels of the proposed system: registeration, authentication and DOS attack detector for four cars as a prototype. At the first level, each car (A, B, C, D) request individual keys from the server as a registeration process. The server responds requests by generated keys. The lightweight authentication protocol is implemented in the second level by exhchanging keys with nighbour vehicles. If the system detects unauthenticated vehicle, it is excluded from the network. The third level explains the detection of DOS attack by one of included vehicle. The detected attacked vehicle is excluded from the network.

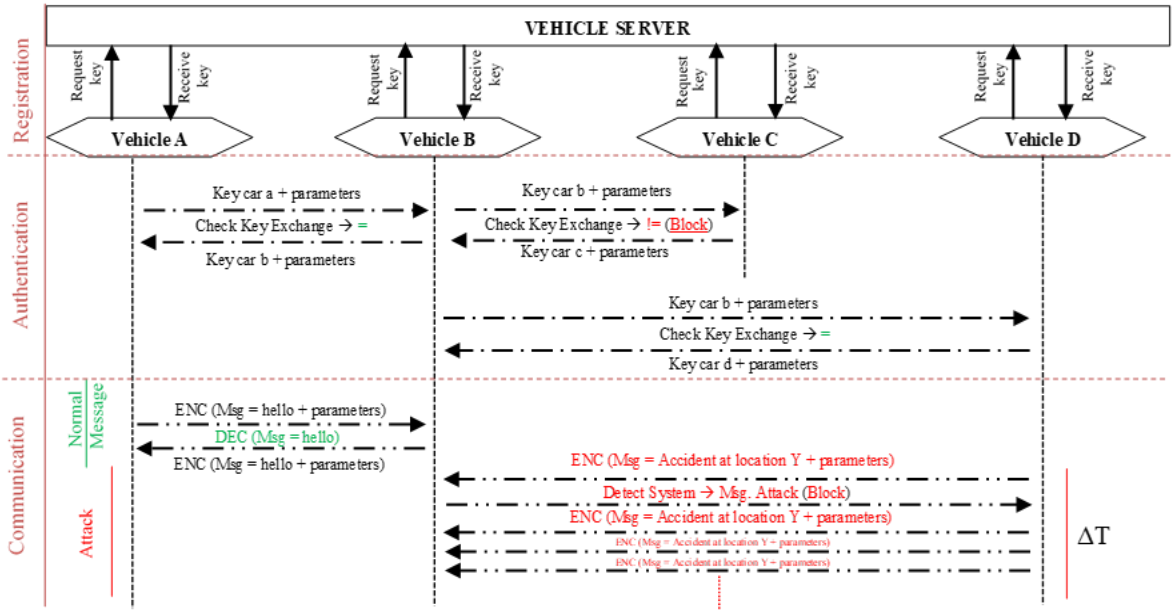

Figure 1. Proposal system structure

2.2. Levels of the proposed system

As mentioned earlier, three levels are considered in the proposed cyber security system. These levels can be explaining in the next sub-sections.

2.2.1. Level One: registration

In the registration phase, each vehicle sends the key request to the server to be registered within the system through the manufacturers or traffic. At the other hand, the server stores all information, sent from the vehicles, within the TAMPER-PROOF DEVICE (TPD) [12-15]. After that, each vehicle works to store its key also within its own TPD. This is done through a safe path that is the result of applying the proposed protocol works to secure it as hown in Figures 2. The working steps of the proposed registeration algorithm is shown as:

a) Every car: (car_a ,car_b ,car_c ,car_d) selects and Identification (ID): (ID_car_a , ID_car_b ,ID_car_c ,ID_car_d) and PassWords (PW): (PW_car_a ,PW_car_b ,PW_car_c ,PW_car_d) and they generate values: (R_car_a ,R_car_b ,R_car_c ,R_car_d). For ensuring security, all cars compute the following:

Car_a :
$A_a = h [ID\_car\_a \| PW\_car\_a] \oplus R\_car\_a$
$B_a = h [ID\_car\_a \| A_a] \oplus R\_car\_a$
$C_a = h [PW\_car\_a \| B_a] \oplus R\_car\_a$
$Req.id = B_a \oplus C_a$

Car_b :
$A_b = h [ID\_car\_b \| PW\_car\_b] \oplus R\_car\_b$
$B_b = h [ID\_car\_b \| A_b] \oplus R\_car\_b$
$C_b = h [PW\_car\_b \| B_b] \oplus R\_car\_b$
$Req.id = B_b \oplus C_b$

Car_c :
$A_c = h [ID\_car\_c \| PW\_car\_c] \oplus R\_car\_c$
$B_c = h [ID\_car\_c \| A_c] \oplus R\_car\_c$
$C_c = h [PW\_car\_c \| B_c] \oplus R\_car\_c$
$Req.id = B_c \oplus C_c$

Car_d :
$A_d = h [ID\_car\_d \| PW\_car\_d] \oplus R\_car\_d$
$B_d = h [ID\_car\_d \| A_d] \oplus R\_car\_d$
$C_d = h [PW\_car\_d \| B_d] \oplus R\_car\_d$
$Req.id = B_d \oplus C_d$

Then encryption of Req.id, which is the requested key, is sent to Car_Server through insecure path.

b) After receiving the Car-Server the requests, it selects the ID, PW and time response (T_S): (ID_S, PW_S, T_S) and generate values (R_S). For ensuring security, the Car_Server computes:
$Ns = h [ID\_car\_S \| T\_S] \oplus R\_car\_S$
$Key\_car\_i = h [ID\_car\_S \| Req.i \| Ns] \oplus R\_car\_S$
Then, the TPD_Server Stores the result as [Key_car_i]. The encrypted Key_car_i is sent to all cars (Car_a , Car_b , Car_c , Car_d) through insecure path.

c) After receiving the keys of cars (Car_a , Car_b , Car_c , Car_d), the decryption process is done for Key_car_i. Then TPD_Car Stores its own key (Key_car_a , Key_car_b , Key_car_c , Key_car_d).

Figure 2, Explain the algorithm of registeration process for car A as example. The other cars follows the same steps.

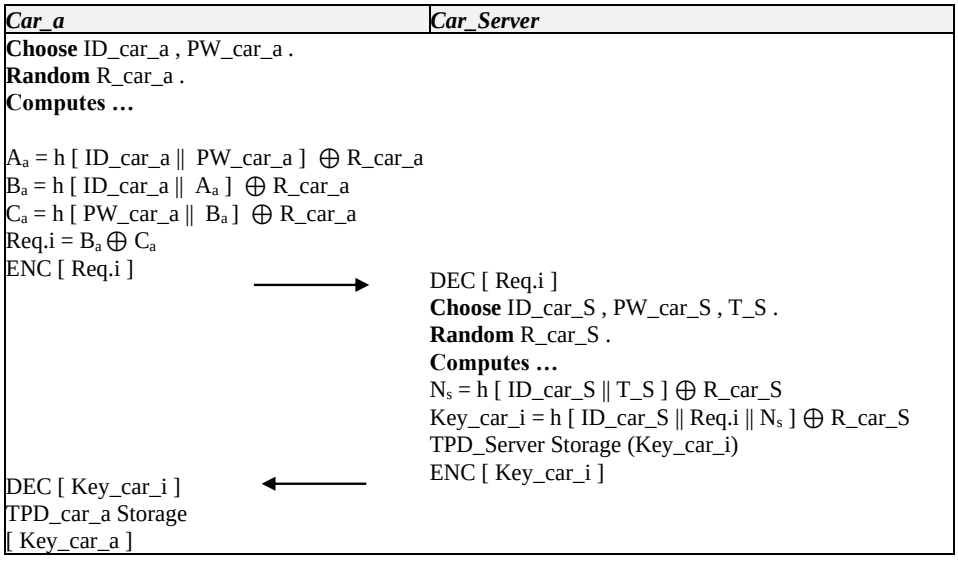

Figure 2. Vehicle registration A

2.2.2. Level two: authentication

During the authentication phase, any vehicle inside the network can communicate with another vehicle in specific range using the technique of Dedicated Short Range Communication (DSRC) [16-20]. The authentication process gives the licence for cars to communicate. For example, when the vehicle A is authenticated with vehicle B, vehicle A can send its key to vehicle B. While, vehicle B can send its key to vehicle A and thus both cars now have the other vehicle key (Car_a = {Key_car_b} and Car_b = {Key_car_a}). Vehicle A sends the key of vehicle B to the Server_Car and vehicle B is doing the same for A. Now, the presence of the A and B vehicles is checked if the key for each vehicle registered within the TPD server. If the result is positive, then such car is treated as a licensed vehicle. At this stage, it cannot be confirmed that the vehicle is harmful or not, only, the key is checked in the server after which the vehicle is communicated. Figure 3, Explains the procedure of authentication between car A and B as an algorithm.

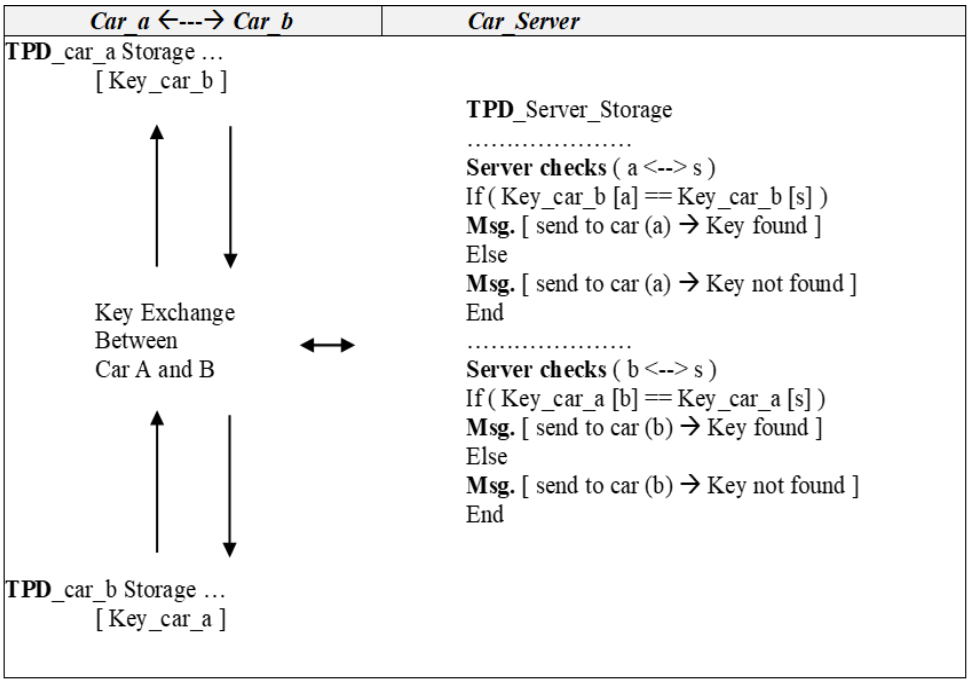

Figure 3. Authentication between Car A & B

2.2.3. Level three: communication and DOS attack detection

In this level, the proposed protocol works to secure data, discover the attack [21-26]. Know the harmful vehicle after it has passed through the registration and authentication stages. The communication and data transfer process is performed between vehicle A and as shown in Figure 4, That viewed the diagrammatic of the Car-to-Car.

a) Car_a , selects: (Welcome , Key_car_a , Sending time T_a) and generates value of (U_car_a), then for ensuring security , the car computes:

Car_a :

$X_a = h [Key\_car\_a \| T\_a] \oplus U\_car\_a$

$Y_a = h [X_a \| Key\_car\_a] \oplus U\_car\_a$

$Z_a = IN \oplus Key\_car\_a \oplus X_a \oplus Y_a \oplus T\_a$

The encryption of Req and is sent to Car_b through insecure path in the following form:

$T\_a , Req = ENC\ H_a (Z_a)$, where ENC is stand for encryption.

b) After receiving the Car_b the request, it performes the decryption for Req ($Req = DEC\ H_b (Z_a)$), where DEC is stand for decryption. The time difference verification is computed depending on ($\Delta T_b \leq T\_b –$

T_a). The car selects: (Welcome , Key_car_b , Sending time T_b) and generates value of (U_car_b), then for ensuring security , the Car computes:

Car_b :
$X_b = h [Key\_car\_b \| T\_b] \oplus U\_car\_b$
$Y_b = h [X_b \| Key\_car\_b] \oplus U\_car\_b$
$Z_b = IN \oplus Key\_car\_b \oplus X_b \oplus Y_b \oplus \Delta T_b$

The encryption of Rep and sent to Car_a through insecure path in the following form:

$Rep = ENC\ H_b (Z_b)$, Sending time : T_b'

c) In the Car_a side and after receiving the request, the decryption is done for Rep ($Rep = DEC\ H_a (Z_b)$). The time difference verification is evaluated depending on ($\Delta T_a \leq T_a' - T_b'$), after that the communication process is performed.

Car_a	***Car_b***
Choose IN = Welcome , Key_car_a , Sending time T_a . **Generate** U_car_a . **Computes …** $X_a = h [Key\_car\_a \| T\_a] \oplus U\_car\_a$ $Y_a = h [X_a \| Key\_car\_a] \oplus U\_car\_a$ $Z_a = IN \oplus Key\_car\_a \oplus X_a \oplus Y_a \oplus T\_a$ $Req = ENC\ H_a (Z_a)$	
→	If ($\Delta T_b \leq T\_b - T\_a$) T_a , $Req = DEC\ H_b(Z_a)$ **Choose** IN = Welcome , Key_car_b , Receiving time T_b . **Generate** U_car_b . **Computes …** $X_b = h [Key\_car\_b \| T\_b] \oplus U\_car\_b$ $Y_b = h [X_b \| Key\_car\_b] \oplus U\_car\_b$ $Z_b = IN \oplus Key\_car\_b \oplus X_b \oplus Y_b \oplus \Delta T_b$
←	$Rep = ENC\ H_b (Z_b)$, Sending time : T_b' Else Attack
Receiving time : T_a' If ($\Delta T_a \leq T_a' - T_b'$ **)** $Rep = DEC\ H_a (Z_b)$ Else Attack	

Figure 4. Communication and attack detection

2.3. GUI of the proposed system

This section discusses the graphical user interface shown in Figure 5, Which represents the practical aspect in this paper. The language C# is used in the construction of the network as well as the security aspect, which represents the security of data transmission between vehicles. The server is built from the following parts: First part is the environment that contains a group of the vehicles (A, B, C, D) where A and B are normal vehicles while D represents the attack of DoS and C has malfunction of its system during the authentication phase. The second part represents the network infrastructure and is the presence of the server that contains the information about vehicles of the network. The third part is the tools through which the three security levels are implemented: registration, authentication, as well as the communication and attack detection. The last part is a window of events in which the results of the communication phases appear in the proposed protocol.

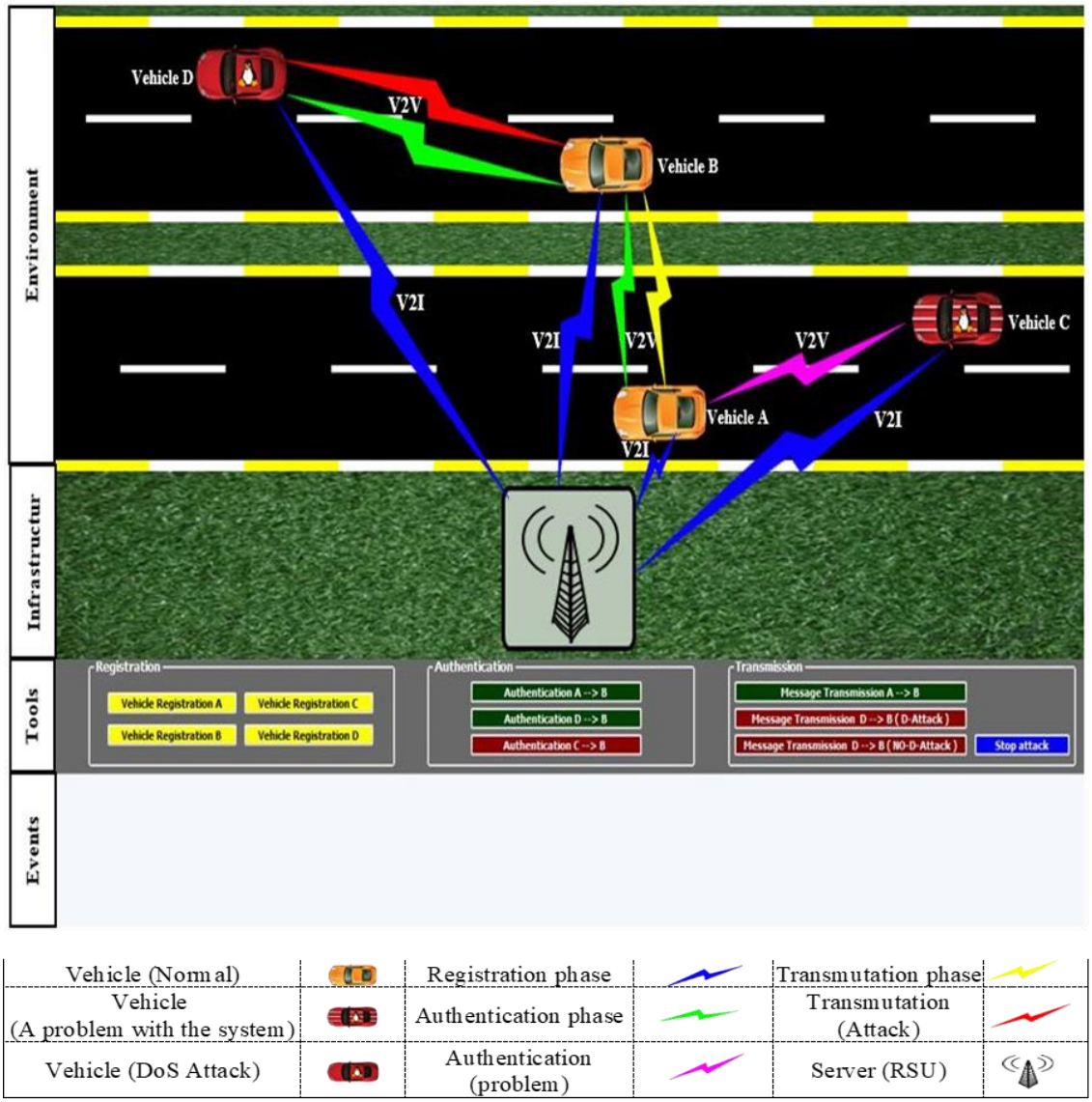

Figure 5. GUI of the proposed sytsem

3. RESULTS

It is well known now that the considered prototype includes four cars. In order to test the performance of the proposed security system, three case studies has been considered.

3.1. Case study one

In the registration level of vehicles (A, B, C, D), they send their information, which represents a request for a key for each vehicle in the network to the server. After accepting the registration request of vehicles, the server works to send a key to each vehicle that its information is registered by the server (See Figures of 6-9). Note that there is no vehicle can access the network before registration.

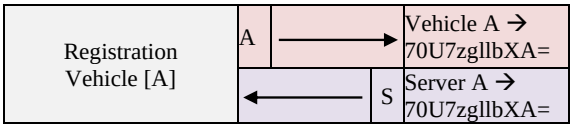

Figure 6. Vehicle registration A

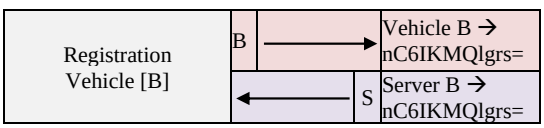

Figure 7. Vehicle registration B

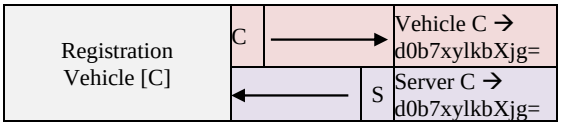

Figure 8. Vehicle registration C

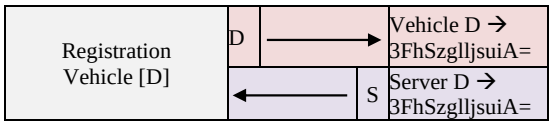

Figure 9. Vehicle registration D

3.2. Case study two

After the registration phase, the authentication phase is performed where the vehicles are authenticated with each other and the server according to the mechanism of the proposed authentication algorithm. Authentication process between vehicles A and B as well as D and B is normal and successed without problems as shown in Figures 10 and 11. With regard to vehicle authentication of vehicles C and B are unsuccessful due to a malfunction of the vehicle C or a change in vehicle information after the registration process. Therefore, the communication between car C and B has not been authenticated, and the vehicle C is blocked and banned from the grid as shown in Figure 12.

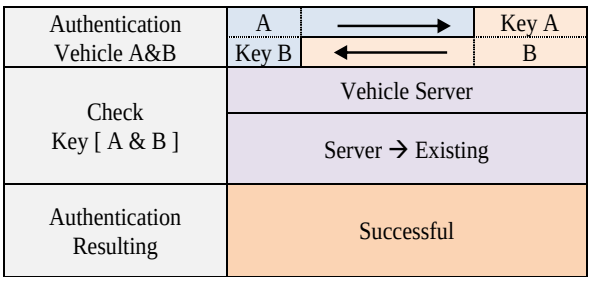

Figure 10. Authenticaton between vehicle A & B

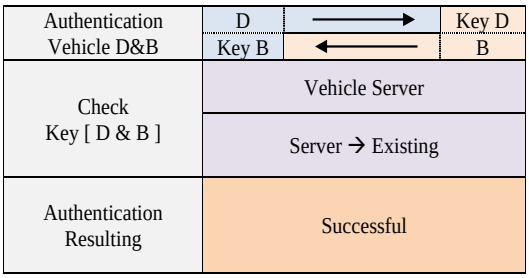

Figure 11. Authenticaton between vehicle D & B

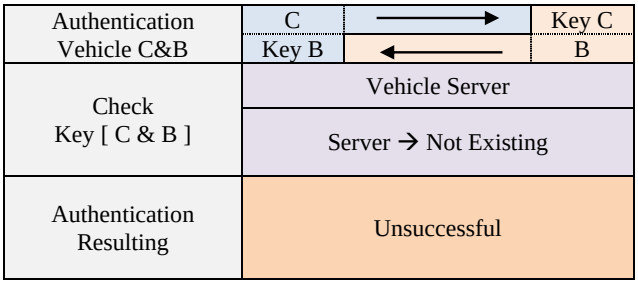

Figure 12. Authenticaton between Vehicle C & B

3.3. Case study three

Here we address two cases. The first case is a normal transmission process where a welcome message (hello) is sent from the vehicle A after encrypted by hash function to vehicle B. Thus, the vehicle works to calculate the time difference of the number of messages received and make sure their integrity and decoding. The message is sent back to the vehicle A also calculates the time difference of the received messages to verify the integrity of the message to be a successful picture transmission without malfunction or attack during the transmission process. Thus it indicates the strength and durability of the protocol in force as shown in Figure 13.

The second case is the process of detecting an attack by sending an unspecified large set of messages built by the DoS attack in vehicle D. It represents the role of the DoS attack by sending a number of messages that indicate (accident at location Y) to the victim vehicle B and making it takes another road that might be congested traffic. This attack is discovered by calculating the time difference of the number of messages, sent from vehicle D inside vehicle B, and thus identify the attacking vehicle. The proposed system blockes vehicle D information inside the server for disconnecting it from the network. The proposed system does not allow the attacker to enter the network again as shown in Figure 14.

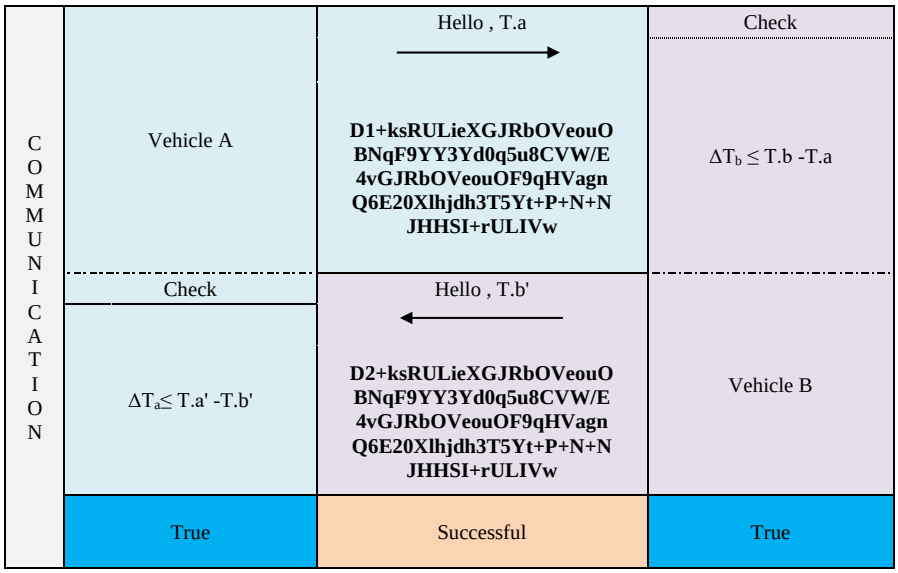

Figure 13. Communication from vehicle A to vehicle B (NORMAL)

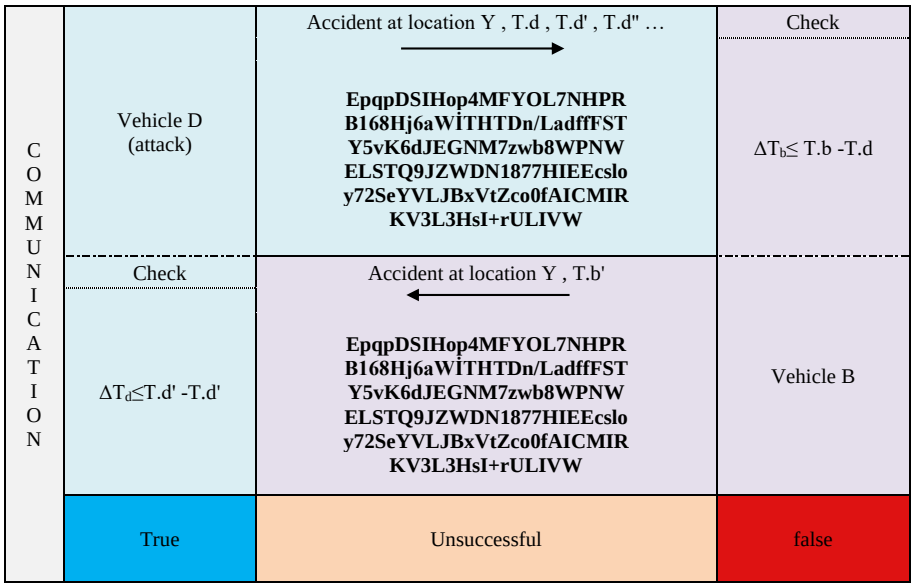

Figure 14. Communication from vehicle D (DoS attack) to vehicle B (ATTACK)

4. CONCLUSION

In this paper, we have proposed a lightweight protocol for multi-level cyber security in VANET. The proposed protocol consisted of three levels, each of which works to maintain network security, from attacks that are related to DoS attacks to reach the required safety. These levels were registeration, authentication as well as communication and attach detetction. The proposed levels worked as obstacles to prevent the DoS attaches. Even if the the attached vehicle passes the registeration and authentication levels, the third level can detect it from its behaivour inside the VANET. The obtained results showed the efficiency in performance of the peoposed system in detecting the attckes. This was concluded by considering different case studies.

REFERENCES

[1] M. Arif, G. Wang, M. Z. A. Bhuiyan, T. Wang, and J. Chen, "A survey on security attacks in VANETs: Communication, applications and challenges," *Veh. Commun.*, p. 100179, 2019.

[2] M. S. Sheikh, J. Liang, and W. Wang, "A Survey of Security Services, Attacks, and Applications for Vehicular Ad Hoc Networks (VANETs)," *Sensors*, vol. 19, no. 16, p. 3589, 2019.
[3] Y. Lahrouni, C. Pereira, B. A. Bensaber, and I. Biskri, "Using Mathematical Methods against Denial of Service (DoS) attacks in VANET," in *Proceedings of the 15th ACM International Symposium on Mobility Management and Wireless Access*, pp. 17–22, 2017.
[4] M. N. Javed, H. Shafiq, K. A. Alam, A. Jamil, and M. U. Sattar, "VANET's Security Concerns and Solutions: A Systematic Literature Review," in *Proceedings of the 3rd International Conference on Future Networks and Distributed Systems*, pp. 40, 2019.
[5] R. S. Raw, M. Kumar, and N. Singh, "Security challenges, issues and their solutions for VANET," *Int. J. Netw. Secur. its Appl.*, vol. 5, no. 5, p. 95, 2013.
[6] W. Ben Jaballah, M. Conti, and C. Lal, "A Survey on Software-Defined VANETs: Benefits, Challenges, and Future Directions," *arXiv Prepr. arXiv1904.04577*, 2019.
[7] A. Quyoom, R. Ali, D. N. Gouttam, and H. Sharma, "A novel mechanism of detection of denial of service attack (DoS) in VANET using Malicious and Irrelevant Packet Detection Algorithm (MIPDA)," in *International Conference on Computing, Communication & Automation*, pp. 414–419, 2015.
[8] M. N. Mejri, N. Achir, and M. Hamdi, "A new security games based reaction algorithm against DOS attacks in VANETs," in *2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, pp. 837–840, 2016.
[9] S. Ahmed, M. U. Rehman, A. Ishtiaq, S. Khan, A. Ali, and S. Begum, "VANSec: Attack-resistant VANET security algorithm in terms of trust computation error and normalized routing overhead," *J. Sensors*, vol. 2018, 2018.
[10] V. H. La and A. R. Cavalli, "Security attacks and solutions in vehicular ad hoc networks: a survey," 2014.
[11] A. Pathre, "Identification of malicious vehicle in vanet environment from ddos attack," *J. Glob. Res. Comput. Sci.*, vol. 4, no. 6, pp. 30–34, 2013.
[12] H. Vasudev and D. Das, "A lightweight Authentication protocol for V2V communication in VANETs," in *2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, pp. 1237–1242, 2018.
[13] H. Liu, Y. Sun, Y. Xu, R. Xu, and Z. Wei, "A secure lattice-based anonymous authentication scheme for VANETs," *J. Chinese Inst. Eng.*, vol. 42, no. 1, pp. 66–73, 2019.
[14] K. S. Eunice and I. Juvanna, "Secured Multi-Hop Clustering Protocol for Location-based Routing in VANETs," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, pp. 121–126, 2019.
[15] B. Wang, Y. Wang, and R. Chen, "A Practical Authentication Framework for VANETs," *Secur. Commun. Networks*, vol. 2019, 2019.
[16] Q. Xu, T. Mak, J. Ko, and R. Sengupta, "Vehicle-to-vehicle safety messaging in DSRC," in *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, pp. 19–28, 2004.
[17] V. D. Kumar, V. V. Kumar, D. Kandar, "Data Transmission Between Dedicated Short Range Communication and WiMAX for Efficient Vehicular Communication," *J. Comput. Theor. Nanosci.*, vol. 15, no. 8, pp. 2649–2654, 2018.
[18] B. Jia, Z. Wei, B. Liu, and Z. Feng, "Performance Analysis for the Coexistence of Radar and Communication in VANETs," in *2019 IEEE/CIC International Conference on Communications in China (ICCC)*, pp. 979–983, 2019.
[19] M. S. Gurmani and D. P. F. Möller, "Mechanism Protecting Vehicle-to-Vehicle Communication," in *Smart Technologies*, Springer, pp. 335–343, 2020.
[20] U. Shaikh and N. Thalkar, "Vehicle Communication Systems: Technology and Review," in *Conference on Technologies for Future Cities (CTFC)*, 2019.
[21] S. Kumar and K. S. Mann, "Prevention of DoS Attacks by Detection of Multiple Malicious Nodes in VANETs," in *2019 International Conference on Automation, Computational and Technology Management (ICACTM)*, pp. 89–94, 2019.
[22] A. N. Upadhyaya and J. S. Shah, "Attacks on vanet security," *Int J Comp Eng Tech*, vol. 9, no. 1, pp. 8–19, 2018.
[23] A. Durrani, S. Latif, R. Latif, and H. Abbas, "Detection of Denial of Service (DoS) Attack in Vehicular Ad Hoc Networks: A Systematic Literature Review.," *Adhoc Sens. Wirel. Networks*, vol. 42, 2018.
[24] Y. Gao, H. Wu, B. Song, Y. Jin, X. Luo, and X. Zeng, "A Distributed Network Intrusion Detection System for Distributed Denial of Service Attacks in Vehicular Ad Hoc Network," *IEEE Access*, vol. 7, pp. 154560–154571, 2019.
[25] W. Ahmed and M. Elhadef, "DoS Attacks and Countermeasures in VANETs," in *Advanced Multimedia and Ubiquitous Engineering*, Springer, pp. 333–341, 2018.
[26] M. A. Fadhel, O. Al-Shamaa, and B. H. Taher, "Real-Time detection and tracking moving vehicles for video surveillance systems using FPGA," *Int. J. Eng. Technol.*, vol. 7, no. 2.31, pp. 117–121, 2018.