

Cyber DoS attack-based security simulator for VANET

Muntadher Naeem Yasir¹, Muayad Sadik Croock²

¹Department of Computer Science, Iraqi Commission for Computers and Informatics (ICCI),
Informatic Institute for Postgraduate Studies, Iraq

²Department of Computer Engineering, University of Technology, Iraq

Article Info

Article history:

Received Feb 2, 2020

Revised May 4, 2020

Accepted May 15, 2020

Keywords:

Cyber security

DoS attack

Lightweight protocol

V2V

VANET

ABSTRACT

At the late years, researches focused on the cyber denial of service (DoS) attacks in the vehicle ad hoc networks (VANETS). This is due to high importance of ensuring the safe receiving of information in terms of vehicle to vehicle (V2V), vehicle to infrastructure (V2I) and Vehicle to Road side unit (V2R). In this paper, a cyber-security system is proposed to detect and block the DoS attacks in VANET. In addition, a simulator for VANET based on lightweight authentication and key exchange is presented to simulate the network performance and attacks. The proposed system consists of three phases: registration, authentication as well as communications and DoS attack detection. These phases improve the system ability to detect the attacks in efficient way. Each phase working is based in a proposed related algorithm under the guidance of lightweight protocol. In order to test the proposed system, a prototype is considered includes six cars and we adopt police cars due to high importance of exchanged information. Different case studies have been considered to evaluate the proposed system and the obtained results show a high efficiency of performance in terms of information exchange and attack detection.

Copyright © 2020 Institute of Advanced Engineering and Science.
All rights reserved.

Corresponding Author:

Muntadher Naeem Yasir,

Department of Computer Science,

Iraqi Commission for Computers and Informatics (ICCI),

Informatic Institute for Postgraduate Studies,

Al-nidal Street, Baghdad, Iraq.

Email: muntadher.naeem@yahoo.com; 120102@uotechnology.edu.iq

1. INTRODUCTION

The VANETs as a branch of the MANETs, shows the ability of communications to exchange data between vehicles (V2V) about the security and safety of data. This leads to the safety of vehicles those within the network. VANETs working is usually categorized into the use of Dedicated Short-range Communication (DSRC) technology that includes coverage of 1000 m, data rate of 27 Mbps, bandwidth of 75MHz and general security issues are availability and authentication [1, 2].

It is important to note that we focused in this paper on the police car network because of the high sensitivity to security services. The exchange of information between vehicles requires a system with high durability in terms of maintaining the confidentiality of data within the system from the attacks on the VANETS for police Vehicle. After our study of a set of researches, it becomes clear that the most prominent and widespread attacks within the scope of availability are Denial of Service (DoS) that separate the service from the target vehicle [3-7]. So, we suggested a general protocol that includes building a network design, information transfer system, and data storage for all vehicles that detects DoS attacks through the proposed algorithm in the communication phase.

Different research studies and works in the field of security in VANET had been presented to tackle the raised problems in terms of communication, data transmission and people safety. In [8], The researchers

proposed a distributed mechanism to protect against harmful compounds. This mechanism of action was performed through the behavior of prediction of malicious vehicles within the network. It used Kalman filters to divide the vehicles into three sections: white, gray and black based on working factors within the network range. Their goal was to prevent or detect DoS attacks. They have used NS3 simulations to complete their work within this specific environment, which result to predict malicious vehicles and this decreases as the number of nodes increases, giving results of 80%. While if the number of compounds increases, the percentage is gradually decreased. But it can still detect harmful attacks with high intensity and the ratio is also high when delivering packets between vehicles. In [9], a mechanism to prevent DoS attack on the physical layer, MAC and IEEE 802.16P was suggested. Packet delivery ratio values are used to identify the harmful vehicles. The mechanism of work was based on the percentage of beam delivery. A list was created to save IP all harmful vehicles. MATLAB and NS2 are used for simulations. The results have compared in the event that there were harmful vehicles or not. A specific number of vehicles have used only 10. The contract was discovered in seconds and added to the list.

In [10], the PSO algorithm was used in VANET to detect DoS attacks. The PSO algorithm was based on behavior simulations. In [11], authors discussed a mechanism to combat jamming messages that could cause a DoS attack. Naturally, there were multiple paths in the network, the path may be long or it may be short to be considered by the vehicles. Long paths are alternative in the event of congestion or traffic blocks. Harmful vehicles send jamming messages to the long and short paths and this causes a DoS attack. A DoS attack separated service from vehicles on VANET to an increase traffic jams and accidents. The researchers suggested a mechanism that worked to stop attacks by using the following parameters (Packet Send Ratio and Segregation). This mechanism does not prevent or detect harmful vehicles from attacking in the future on the VANET.

In [12], The authors suggested an algorithm based on the detection of an enhanced attack package to identify DoS. The mechanism of operation of this algorithm was to verify harmful compounds as well as to improve the performance of the system as quickly as possible. The role of road side unit (RSU) here is to quickly check with each vehicle that works with server registration to store all the information in the database. The algorithm taked the path of early detection of DoS attacks through the channel the vehicle is communicating with RSU. In [13], the researchers suggested DJVAN algorithm to detect jamming in the VANET. The algorithm was based on the packet delivery rate (PDR). When jamming was effective, the attacker launched attacks on the two connected vehicles. Therefore, the contact could not obtain a contact link to send the information. Even if there was a communication process, the data packets did not arrive completely. Thus, if the value of the PDR was small, the system cloud judge whether it was DoS attacks or not.

As a result, the literary studies of some researchers regarding DoS attacks leads to considered a lightweight protocol based on researchers work. The proposed system differs in terms of construction, phases, and handling of DoS attacks. The proposed system supports two different types of communication, vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (C2I).

2. PROPOSED SYSTEM

As mentioned earlier, the proposed system takes into account the online security of VANET. The proposed system can be divided into different sub-sections as follows.

2.1. Proposed system schema

A number of the attacks have appeared recently in the VANET network, the most famous of which are DoS that separates the vehicle from other vehicles. This leads to serious problems that may cause material or physical damage. Figure 1 shows the proposed scheme that is based on the use of a lightweight protocol which consists of three levels. The proposed protocol is characterized by exploiting a very small storage space within the system, as well as a currency mainly focused on discovering DoS attacks that separate the victim's vehicle from the service. This is done by sending number unlimited of messages which leads to the vehicle's delusions with false information providing to take another path which can cause an overlap in sending of correct information between police vehicles.

The proposed protocol works to determine the identity of the attacking vehicle, whether it is in the process of sending or receiving through the time difference or the number of messages sent from the attacker. The scheme clarifies the work of the protocol with three levels of registration, authentication, communication and detection of the attack. The first level is the registration, between the vehicles and the server (V2S) by sending each vehicle of request a key to the server. Then, the server returns the request accompanied with a key for each vehicle. The second level is authentication where each vehicle works to exchange keys with each other. Each vehicle sends the key received to the server to check the presence of the keys in the server. The three level represents communication and attack detection through the mechanism of the number of messages received and the time difference of messages to identify the vehicle. This level

works to store its information within the system and disconnects the car from the network and prevents any further trying in future.

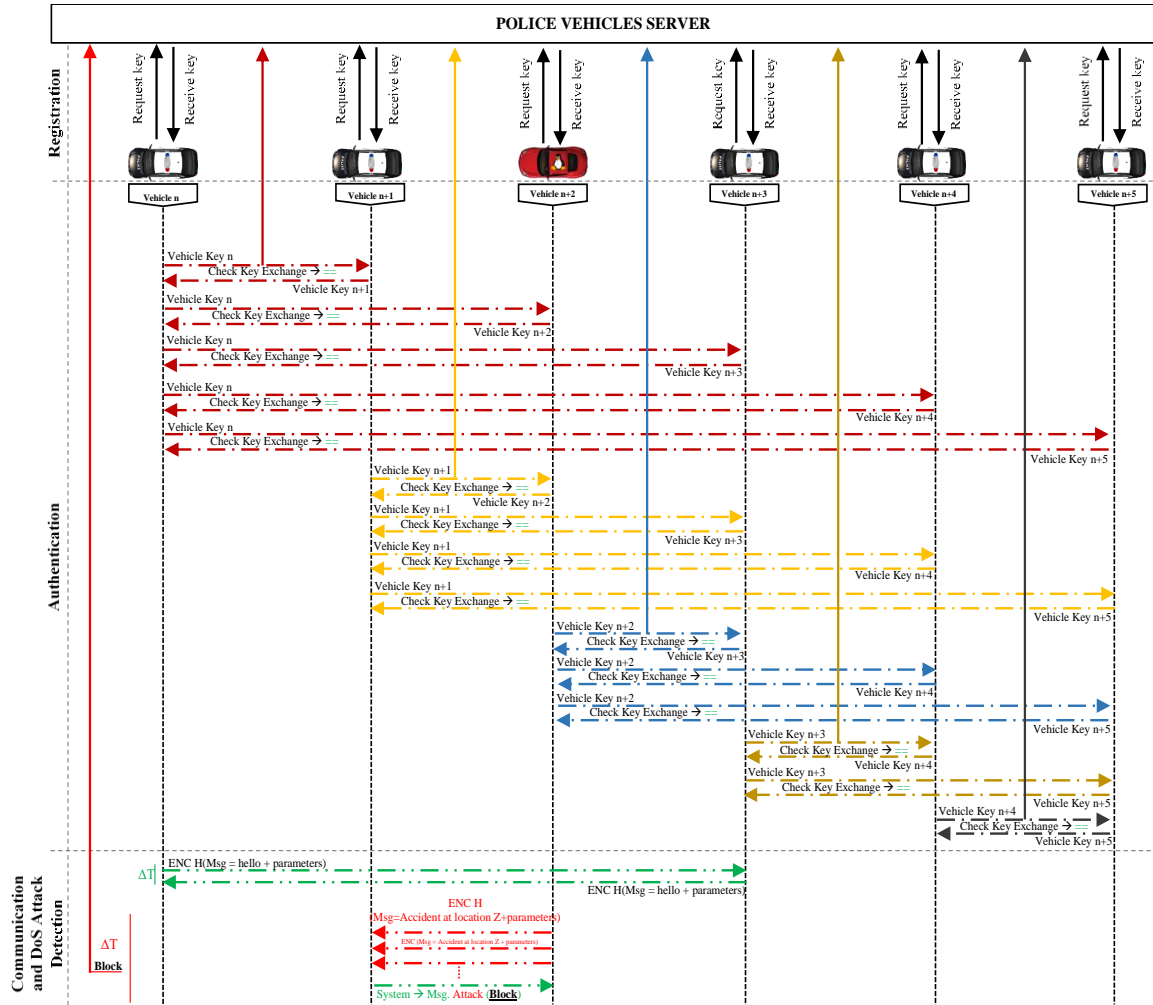


Figure 1. Proposed system schema

2.2. Levels of the proposed system

Three levels are considered in the proposed cyber security system. These levels can be explained in the next sub-sections.

2.2.1. Level one: registration algorithm

In the registration phase, the process between the police vehicles and the server is carried out by sending a key request from the vehicle to the server to request a key. Figure 2 shows the work of the proposed algorithm at the level of registration, through a number of steps outlined below:

Step 1 : Start

Step 2 : Vehicle_n selects and Identification (ID_{V_n}), PassWords (PW_{V_n}) and they generate values (R_{V_n}). For ensuring security, all Vehicles computes the following:

Vehicle_n:

$$A_n = h[ID_{V_n} || PW_{V_n}] \oplus R_{V_n} \tag{1}$$

$$B_n = h[ID_{V_n} || A_n] \oplus R_{V_n} \tag{2}$$

$$C_n = h[PW_{V_n} || B_n] \oplus R_{V_n} \tag{3}$$

$$Req_n = B_n \oplus C_n \tag{4}$$

- Step 3 : Encryption of Req_n using hash function MD5, which is the requested key, is sent to Vehicle_Server through insecure path.
- Step 4 : After receiving the Vehicle_Server the requests, it Checking whether the vehicle registered its information inside the server beforehand, or not sent to Step 9.
As well as checking whether the vehicle is registered as an Attacker vehicle that was discovered during the communication process, or not sent to Step 9.
- Step 5 : Server selects the ID_s, PW_s and time response (ID_{V_s}, PW_{V_s}, T_s) and generate values (R_{V_s}). For ensuring security, the Vehicle_Server computes:

$$N_s = h[ID_{V_s} || T_s] \oplus R_{V_s} \tag{5}$$

$$Key_{V_i} = h[ID_{V_s} || Req_i || N_s] \oplus R_{V_s} \tag{6}$$

Then, the TPD_Server Stores the result as (Key_{V_i}).

Step 6 : Prior to the process of sending the key, it is tested through NIST using three types of frequency, block and runs test it to make sure that the key is strong in terms of randomness [14-16], except that return to step 5.

Step 7 : Encrypted of Key_{V_i} using hash function MD5, then sent to Vehicle n through insecure path.

Step 8 : After receiving the keys of Vehicle n, TPD_Vehicle Stores its own key (Key_{V_n}).

Step 9 : End.

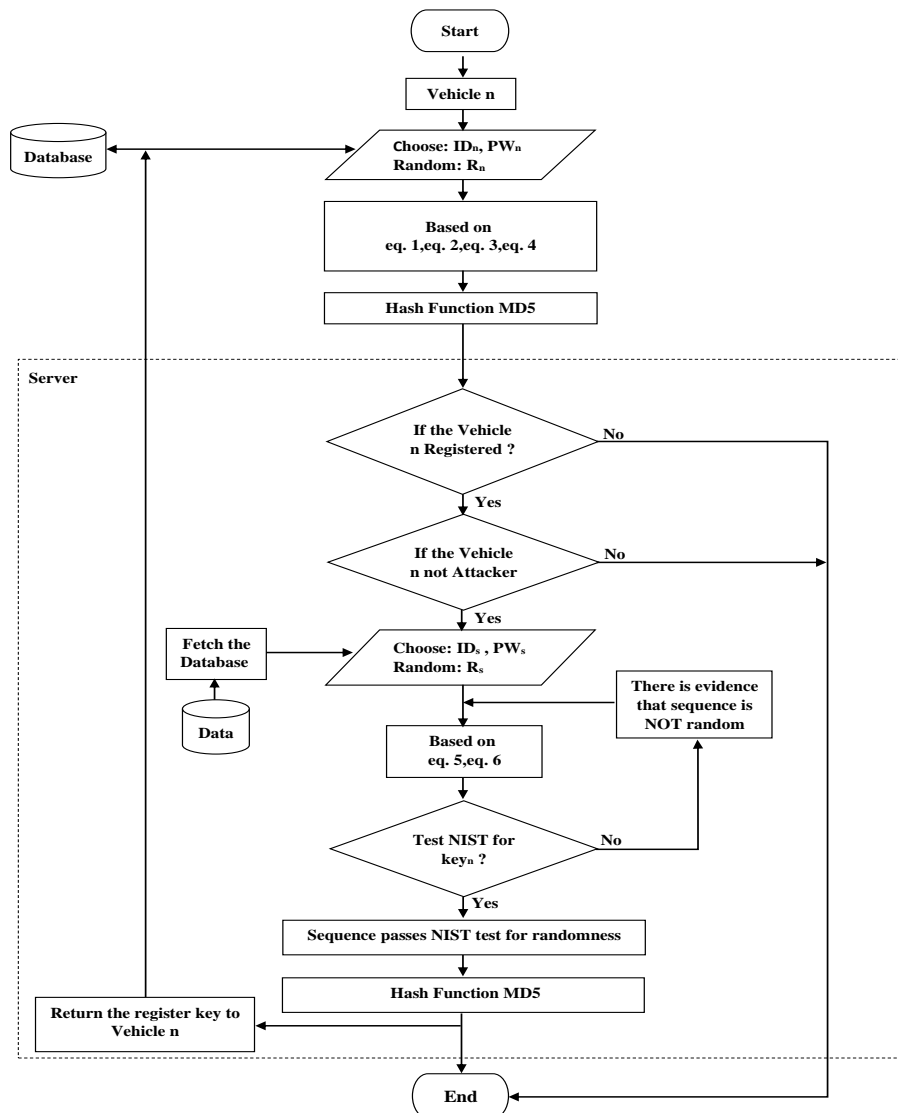


Figure 2. Vehicle n registration algorithm

2.2.2. Level two: authentication algorithm

In the Authentication phase, the authentication process takes place between a vehicle and a neighbor vehicle (V2V) or between the vehicle and the road side units or infrastructure (V2I). After the process of checking the vehicle registration, authentication phase begins. The authentication process is carried out by exchanging the keys of the two vehicles with each other. Each vehicle sends its key to the server to verify the presence of the key that was previously stored in the registration phase. Figure 3 shows the work of the proposed algorithm for authentication, and the next steps are illustrated:

Step 1 : Start.

Step 2 : Check the Vehicle registration is it registration valid or not previously registered in the network to be registered before the authentication phase.

Step 3 : Send vehicle n key to another vehicle $n+1$ (V_n2V_{n+1}) or infrastructure (V_n2I_s).

Step 4 : After receiving the keys of Vehicle n , Vehicle $n+1$ or infrastructure send their keys to a vehicle n .

Step 5 : After receiving the keys, the server checks the validity of the keys and makes sure they are inside its database.

Step 6 : After checking if the vehicle and vehicle key to be authenticated with is present, the authentication process is successfully completed, otherwise, the authentication currency is not done.

Step 7 : End.

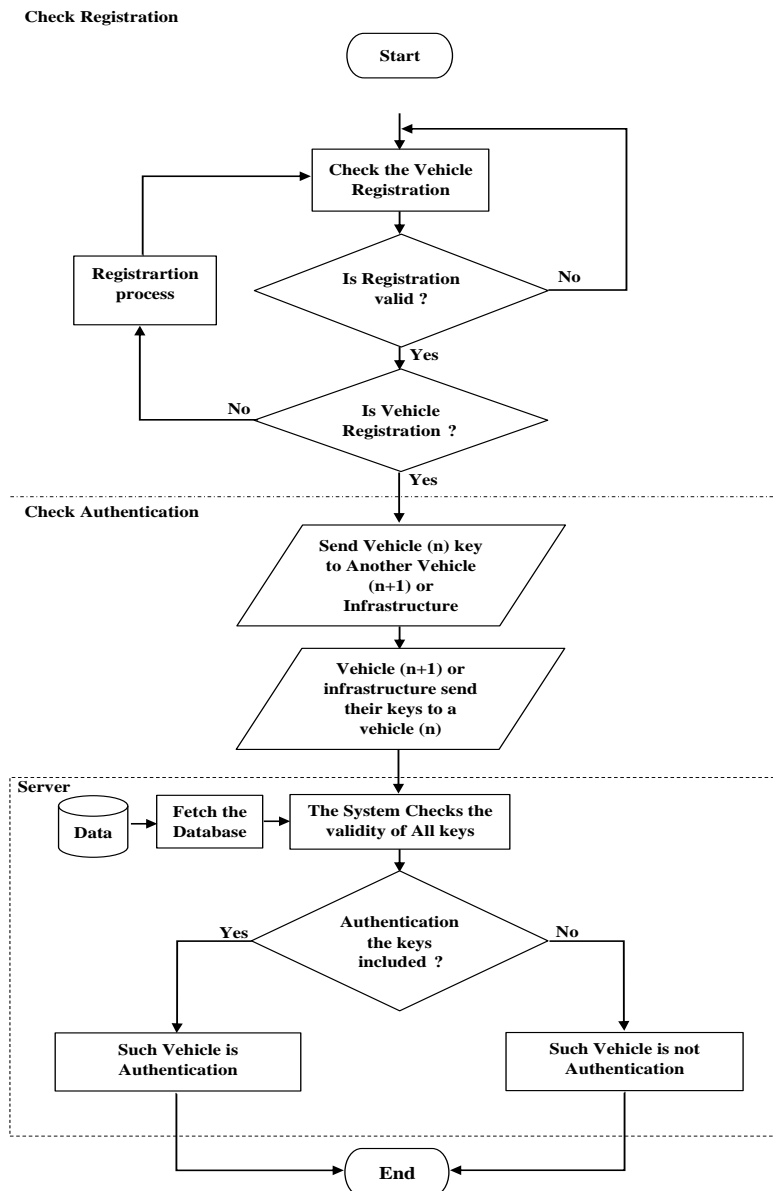


Figure 3. Authentication algorithm between vehicles n and $n+1$

2.2.3. Level three: communication and DoS attack detection algorithm

During the communication phase and detection of DoS attacks, data transmission between two adjacent or non-adjacent vehicles is carried out. This is done by sending a message from the vehicle n to the vehicle $n+1$ for informing of an accident at the location W or requesting help or otherwise. This requires accurate information between vehicles due to the sensitivity of the networks within the scope of maintaining security. The proposed protocol determines the identity of the attacking vehicle through the number of messages or the time difference that occurs during the transmission process between the sent received messages by vehicles. The verification process of the message is done by following it inside the receiving and sending vehicles after receiving the response message from the vehicle. Figure 4 illustrates the work of the proposed algorithm for the communication process and the detection of DoS attacks.

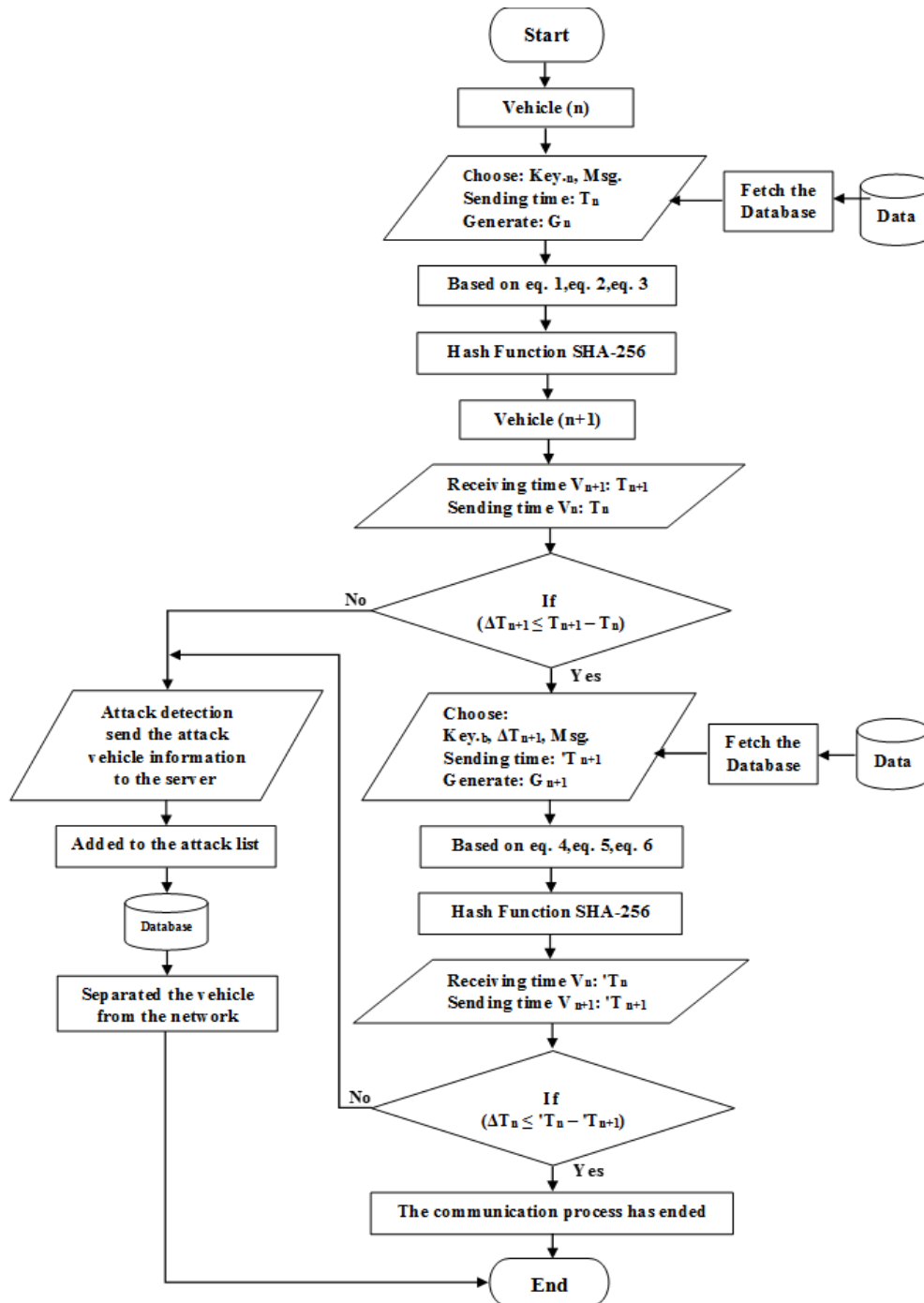


Figure 4. Communication and attack detection algorithm

The following steps illustrate the work of the algorithm.

Step 1 : Start.

Step 2 : Vehicle_n , selects: (Msg:Accident at the location W , Key_V_n , Sending time T_n) and generates value of (U_V_n) ,then for ensuring security , the Vehicle computes:

Vehicle_n :

$$XX_n = h[\text{Key_V}_n || T_n] \oplus U_{V_n} \quad (7)$$

$$YY_n = h[XX_n || \text{Key_V}_n] \oplus U_{V_n} \quad (8)$$

$$\text{REQ}_n = (\text{INPUT-Msg}) \oplus \text{Key_V}_n \oplus XX_n \oplus YY_n \oplus T_n \quad (9)$$

Step 3 : Encryption of REQ_n using hash function SHA-256 and is sent to Vehicle_{n+1} through insecure path.

Step 4 : After receiving the Vehicle_{n+1} the request, it on ($\Delta T_{n+1} \leq T_{n+1} - T_n$).

Step 5 : If the equation condition is fulfilled, the communication process is completed. If the equation condition is not fulfilled, this means that the sending vehicle is considered as a DoS attack. The system works to reserve the vehicle information after confirming that it is a DoS attack. It is added to the attack list inside the server to be prevented when you try to enter the network in the registration phase again, so it works to disconnect it from the network.

Step 6 : The car selects: (Msg: ok, Key_V_{n+1} , Sending time T_{n+1}) and generates value of (U_V_{n+1}) ,then for ensuring security , the Vehicle computes:

Vehicle_{n+1}:

$$\text{CC}_{n+1} = h[\text{Key_V}_{n+1} || T_{n+1}] \oplus U_{V_{n+1}} \quad (10)$$

$$\text{NN}_{n+1} = h[\text{CC}_{n+1} || \text{Key_V}_{n+1}] \oplus U_{V_{n+1}} \quad (11)$$

$$\text{REP}_{n+1} = (\text{INPUT-Msg}) \oplus \text{Key_V}_{n+1} \oplus \text{CC}_{n+1} \oplus \text{NN}_{n+1} \oplus \Delta T_{n+1} \quad (12)$$

Step 7 : Encryption of REP_{n+1} using hash function SHA-256 and is sent to Vehicle_n through insecure path.

Step 8 : Next receiving the Vehicle_n the reply, it computed depending on ($\Delta T_n \leq T_n - T_{n+1}$).

Step 9 : If the equation condition is fulfilled, the communication process is finished. If the equation condition is not fulfilled, Step5.

Step 9 : End.

2.3. GUI of the proposed system

In this side, we deal with the details of the designed VANET's simulator in terms of the Graphical User Interface (GUI). To build this simulator, we rely on a set of software of Microsoft Visual Studio 2013, SQL Server 2014, and Photoshop. The C# language was used in programming of the proposed protocol at all three levels: registration, authentication, communication and detection of DoS attacks. For the data transfer process in V2S, the vehicle traffic mechanism is coordinated within the environment used and the encryption used within the protocol's work. The use of a flexible programming language that deals with Network work like C# language. As for the SQL server 2014 is required, to store the information of each vehicle, as well as storing vehicles information on the server, it requires us to create a database for each vehicle and also to the server. For the design of the interface, we used Photoshop.

Figure 5 shows the GUI design that is divided into four sections. The first section is the environment that represents the vehicles and the mechanism for signal transmission between them and the server. The second section is the infrastructure that consists of RSU connected to the server. The third section shows the tools used for each case whether it is in the stage of registration, authentication, communication and detection of DoS attacks. As for the last section, it represents the results interface for each stage and shows how the protocol works.

3. RESULTS

Now, it is well known that the considered prototype includes six vehicles as a prototype. In order to test the performance of the proposed security system, three case studies have been considered.

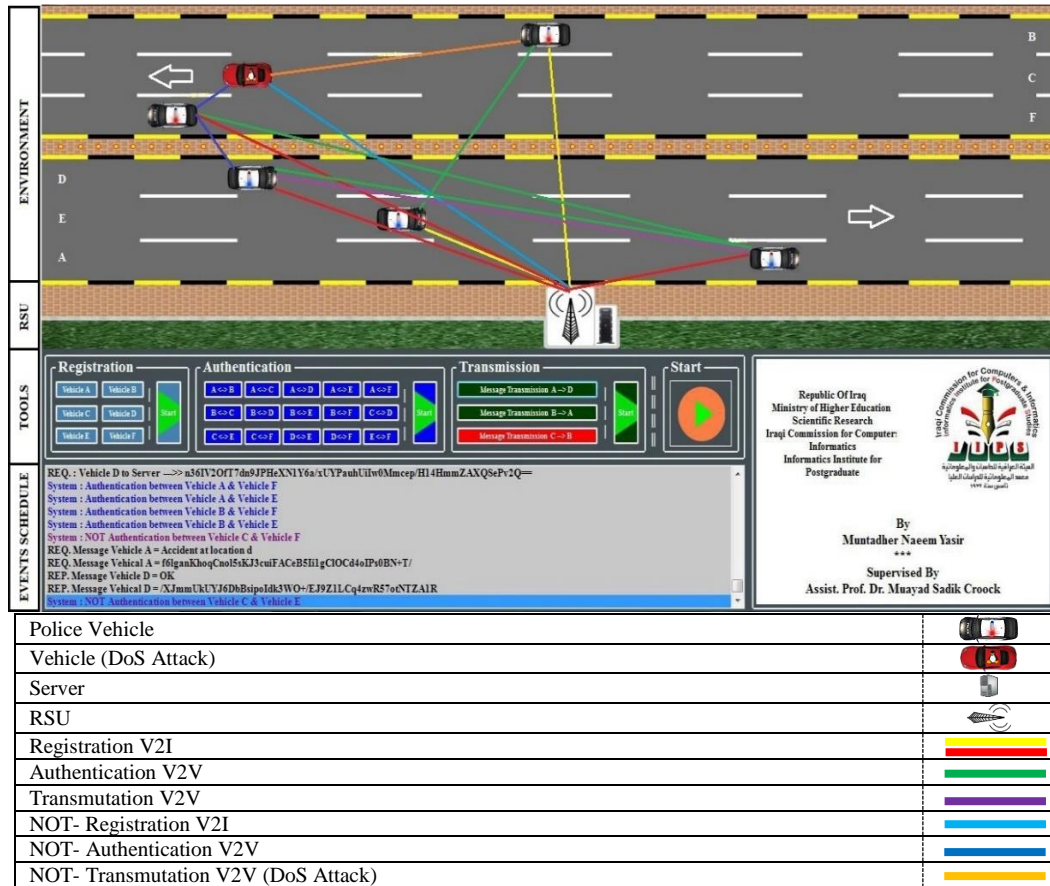


Figure 5. Graphical user interface of the proposed system

3.1. Case Studies of registration results

In this section, we address the study of registration for a number of cases that may occur during the registration process. Also, we address the statement of the results of our proposed protocol. Note, that the data used in the sent and received processes has been encrypted at this phase using Hash function MD5 [17-19].

3.1.1. First one

Figure 6 shows the case that considers a successful registration process between the vehicle (A) and the server. Starting the registration phase by sending the vehicle n a request that carries vehicle information to the server, which must be stored previously on the server. After the server receives the request, it checks the vehicle information in the server. If the vehicle information is present on the server, the server sends a response carrying a key to the vehicle as shown in Figure 7.

$ID_{n(A)}$	65785	ID_{n-S}	65785
$PW_{n(A)}$	8934567887904	PW_{n-S}	8934567887904
REQ.	$h[ID_n + PW_n] MD5$	IF $(ID_n = ID_{n-S}) \& \& (PW_n = PW_{n-S})$	
REP.	$h[Key_n] MD5$	Successful	

Figure 6. Communication between V2S (Successful)

REQ : Vehicle A to Server -->> UC66fO9ibMsSX60KrPcxo63ZGi8dH7zUjBYgMJ+gGLddxFRsSik=
 REP : Server to Vehicle A -->> GLnjwqUkCKwPx5vh9yYL0/DqMzW+JNr.AvoYIPMfcf2sZDTP62QbtaYDGo.A==

Figure 7. Communication result between V2S (Successful)

3.1.2. Second one

The second case adopts an unsuccessful registration process between the vehicle (A) and the server as shown in Figure 8. Starting the registration phase by sending the vehicle n a request that carries vehicle information to the server. After the server receives the request, it checks the vehicle information in the server. If the vehicle information is not present on the server, the server sends a response carrying a message (Cannot register or not registration) to the vehicle as shown in Figure 9.


			
$ID_{n(A)}$	65785	ID_{n-S}	65785
$PW_{n(A)}$	7855346789856	PW_{n-S}	8934567887904
REQ.	$h[ID_n+ PW_n] MD5$	IF ($ID_n = ID_{n-S}$) & ($PW_n \neq PW_{n-S}$)	
REP.	NOT-Registration	Unsuccessful	

Figure 8. Communication between V2S (Unsuccessful)

```
REQ. : Vehicle A to Server ----> A7IDeJZAgUv9eDFqHUDPNYjiUX/4m5J2HLdLQAi6mprW79UA=
System : Car A --> NOT Registration
```

Figure 9. Communication result between V2S (Unsuccessful)

3.1.3. Third one

Figure 10 shows the third case of an unsuccessful registration process between the vehicle (C) and the server. Starting the registration phase by sending the vehicle n a request that carries vehicle information to the server. After the server receives the request, it checks the vehicle information in it. If the vehicle n, is already registered in the list of vehicles that pose a threat to the network after its discovery at the communication stage. The server sends a response carrying a message (Cannot register or not registration <<Attacker>>) to the vehicle as shown in Figure 11.



			
$ID_{n(C)}$	87785	Attacker list-S	Vehicle (Attack)
$PW_{n(C)}$	4995346743756	If (Vehicle = Attack)	
REQ.	$h[ID_n+ PW_n] MD5$	Unsuccessful	
REP.	NOT-Registration	Unsuccessful	

Figure 10. Communication between V_{Attack}2S (Unsuccessful)

```
REQ. : Vehicle B to Server ----> JKROwrOhWEVwqqh4IEJLCUbG+x1w3/4FqfCPDren7ao0oMFXXEnFGNk=
REQ. : Vehicle C to Server ----> HMzEzSamOJVQId3t7Fm4nITt/RMVGPRV/BPs4mx3Ef5o/6Jy6pw=
REP. : Server to Vehicle B ----> 1chvPqdiHxPR7pudxGT0W5Z2/rj8x9SfzUtbaDtZEjgufn1CTZFqLGYI
System : Car C ----> NOT Registration << Attacker >>
System : NOT Authentication between Vehicle B & Vehicle C
```

Figure 11. Communication result between V_{Attack}2S (Unsuccessful)

3.2. Case studies of authentication results

In the authentication section, we explain a study of two cases, namely: the success of authentication and the lack of success of authentication and what is the role of the proposed protocol at this stage in particular. Note that authentication occurs between V2V or V2I during the registration phase.

3.2.1. First one

In this case, the authentication process takes place between the vehicle (A) and the vehicle (B) as shown in Figure 12. The vehicle n sends its key to the vehicle n+1. Likewise, the vehicle n+1 send its key to the vehicle n, in order to the keys exchange. After this step, each vehicle (V_n, V_{n+1}) sends its key to the server. The server, checks for the presence of the key of each vehicle. If the keys are presented for both vehicles, authentication is successful. The result is shown in Figure 13.

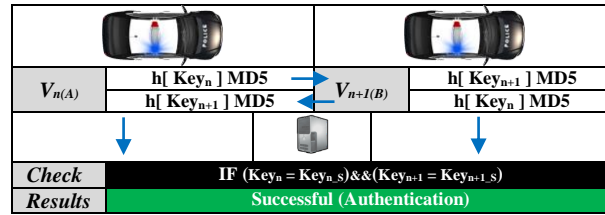


Figure 12. Authentication between V2V (Successful)

```
REQ. : Vehicle B to Server ----> 1xO3eX7iaOIKfswsAouEe68C7TPbUSHlonTKILRcE7rOFFWXwWcp
REQ. : Vehicle A to Server ----> igTsW8goiSpFOkgrMQgqrM/M+dj3Jf51vSUu97SVWb5uJU3hCX/Rlus=
REP. : Server to Vehicle B ----> 0AHHriXmc9aRCzW78y7TO1jSB/Q3k+ffLX05h/fsmYdWbXPfFu5qbmTWOFuL
REP. : Server to Vehicle A ----> LbykDxdsnU+PMNTCV86DgmKGZK3/75o7RoiO6X4gr3rRTK01Wpnk+XRcg6U=
System : Authentication between Vehicle A & Vehicle B
```

Figure 13. Authentication result between V2V (Successful)

3.2.2. Second one

In the second case, the authentication process between Vehicle (A) and Vehicle (B) is performed as shown in Figure 14. After the key exchange process between both vehicles, each vehicle (V_n, V_{n+1}) sends its key to the server. The server checks the key for each vehicle stored on it. In the event that the vehicle $n + 1$ keys exist, but the vehicle n key does not exist, which means the vehicle n is not passing the registration phase. Therefore, the authentication process is failed as shown in Figure 15.

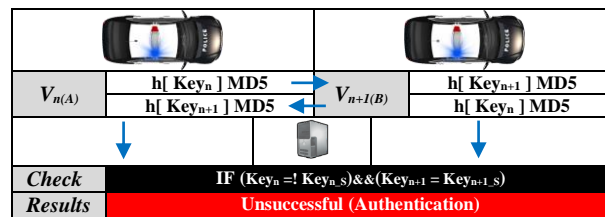


Figure 14. Authentication between V2V (Unsuccessful)

```
REQ. : Vehicle B to Server ----> hZ4u13yeMXL2EzbbzBAVidcRNbVT9CU0CwAQbySUXsfOQSufWG3XoJg==
REQ. : Vehicle A to Server ----> gP1DfmKkIB0YClCRtjAOLaFPQCEjLH0gilUvfyvtBRRik51+9Ujd
REP. : Server to Vehicle B ----> JSShaGHMbRNWfkc1yeVzCFd/XRyRTzLpby/z7hMhAZWsqnlXwWP++ra
System : Car A ----> NOT Registration
System : NOT Authentication between Vehicle A & Vehicle B
```

Figure 15. Authentication result between V2V (Unsuccessful)

3.3. Case studies of communication and dos attack detection results

After studying the results of the registration and authentication cases, we discuss the results of the communication case and the detection of DoS attacks, through two cases. The first case represents a normal connection between two vehicles. The second case shows how the DoS attack is discovered during the communication phase. Note that the data used in the transmission and reception process has been encrypted at this stage by using Hash function SHA-256 [20-26].

3.3.1. First one

Figure 16 shows a successful communication process between the first vehicle V_n (A) and the second vehicle V_{n+1} (D). Vehicle n sends a message to the vehicle $n+1$ holding the following text (accident at the location Y) to inform it of an accident at the location Y . After verifying the integrity of the message, the vehicle $n+1$ sends a response bearing the following text (OK) to the vehicle n , which also checks the received message and finds whether it is harmful to the network system or not. Figure 17 shows the results of the communication process between both vehicles.

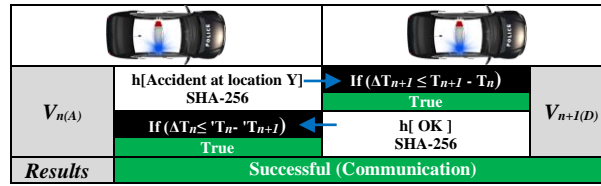


Figure 16. Communication from vehicle A to vehicle D (Normal)

```

REQ. : Vehicle D to Server ----> 99iCaBrgRw3ZVDvASD78OWz2kdrj4MoPalnHC6gEILCHgtqciQ==
REQ. : Vehicle A to Server ----> Qmzb3ohLn+LEruG6mzUHP/EM+njo4cLA47TLgOs8pYF75PGE
REP. : Server to Vehicle D ----> U0/WyLozRVCY6qMyUfsfYMyO91ARLU3MYGbpA737dPd3j0F8Q9U7A==
REP. : Server to Vehicle A ----> gTYU8A42iSdlvCxRuUESs/XGQbiVhwahvW8PcmTv/pviv+3PW6/
System : Authentication between Vehicle A & Vehicle D
REQ. : Vehicle D to Server ----> JPWqwhDuAL4xv9voXIqWP+6V9vtXk0VLnoyWd+HNf8zlkj1T1Uw=
REQ. : Vehicle A to Server ----> rfQsPxsd0Qay60m6i9BGCJY+a5+8hlf22xnojjQTvPDRuDDooNWTIKOcnvFAwI=
REQ. Message Vehicle A = Accident at location Y
REQ. Message Vehical A = 7G2Jih0SmI5kvADdCU+dalO7fGMbRTQVpe5xek3TbDqBi0CGQOB422k0
REP. Message Vehicle D = OK
REP. Message Vehical D = BayCjTFj9oSrLY6lySHBlIoO7JpCyfbK6X6XAnJuVw0/6KjLW3nbx7KM
    
```

Figure 17. Communication result from vehicle A to vehicle D (Successful)

3.3.2. Second one

Figure 18 shows the process of identifying or detecting a DoS attack during communication between two vehicles (V_C2V_B) or (V_n2V_{n+1}). When the vehicle n sends a message to the vehicle $n+1$, it carries the following text (accident at site X) and in large quantities to report it to an accident at site X. This is to ensure that a vehicle takes another path or other location. After verifying the message, the type of attack is determined using the mechanism of our protocol by calculating the time difference for the transmission and to receive ($\Delta T_{n+1} \leq T_{n+1} - T_n$). The Vehicle $n+1$ sends a response with the following text (OK) to the server. In turn, it blocks the vehicle that posed a threat to the vehicle as well as adding it to the list of attacking vehicles. Figure 19 shows the results of the attack detection process in our proposed protocol.

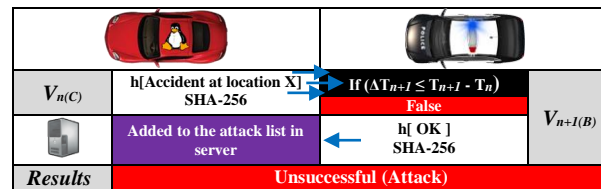


Figure 18. Communication and DoS attack detection from vehicle C to vehicle B (Attack)

```

REP. : Server to Vehicle B ----> HxbAlxGsmDxsQ2jIORzh2ShlvtVOEbc4qESsGMfbMkgefR2W640=
REP. : Server to Vehicle C ----> 36xclZ8Qvs7F5fgDDHxD7KraI6YiVonU5mRq6cNvvUZrJWS+EFsBeVykclBslug=
System : Authentication between Vehicle B & Vehicle C
REQ. : Vehicle B to Server ----> Tsf/TtoIBSZV4fqMeZ6Ege+bG9dn284lOh06B5AP7BO425wDrHIQ
REQ. : Vehicle C to Server ----> /lh019E+GPY9C7szdaGN6zrQ9Y6DxlEHiXfvCzHO4tp9pXv3FL8J9WSfvNpB
REQ. Message Vehicle C = Accident at location X
REQ. Message Vehical C = HzaCP0P76sJinQMIiJs2pETY2DWMIsdOlnu9DS1MddzwEnMfy42EZpHLnm5w
REQ. Message Vehicle B = OK
REQ. Message Vehical B = iE7K0Do/cYCHkewY9zIINNsLumGApP1w6NRmfiRheTDpe2X8yi/uzCE+fsGL
System : Vehicle C ----> Attacker
    
```

Figure 19. Communication results and DoS attack detection from vehicle C to vehicle B (Attack)

4. CONCLUSION

In this paper, we have proposed a lightweight protocol of cyber security system to detect and block of DoS attacks in VANET. A simulator for VANET was presented based on lightweight authentication and key exchange protocol. The proposed protocol includes three levels, each of which works to maintain

network cyber security from attacks that are related to DoS attacks to reach the required safety. These levels were registration, authentication as well as communication and attack detection. The proposed levels worked as obstacles to prevent the DoS attacks. Even if the attacked vehicle passes the registration and authentication levels, the third level can detect it from its behavior inside the VANET. The obtained results showed the efficiency in performance of the proposed system in detecting the attacks. This was concluded by considering different case studies.

REFERENCES

- [1] Q. Xu, et al., "Vehicle-to-vehicle safety messaging in DSRC," in *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, pp. 19-28, 2004.
- [2] K. B. Kelarestaghi, et al., "Survey on Vehicular Ad Hoc Networks and Its Access Technologies Security Vulnerabilities and Countermeasures," *arXiv Prepr. arXiv1903.01541*, pp. 1-22, 2019.
- [3] U. Parmar and S. Singh, "Overview of various attacks in VANET," *International Journal of Engineering Research and General Science*, vol. 3, no. 3, pp. 120-125, 2015.
- [4] J. M. De Fuentes, et al., "Overview of security issues in vehicular ad-hoc networks," in *Handbook of research on mobility and computing: Evolving technologies and ubiquitous impacts*, IGI global, pp. 894-911, 2011.
- [5] K. Verma, et al., "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)*, pp. 550-555, 2013.
- [6] P. Sirola, et al., "An analytical study of routing attacks in vehicular ad-hoc networks (VANETs)," *International Journal of Computer Science Engineering*, vol. 3, no. 4, pp. 210-218, 2014.
- [7] A. Pathre, "Identification of malicious vehicle in vanet environment from ddos attack," *Journal of Global Research in Computer Science*, vol. 4, no. 6, pp. 30-34, 2013.
- [8] T. Bouali, et al., "A distributed prevention scheme from malicious nodes in VANETs' routing protocols," in *2016 IEEE Wireless Communications and Networking Conference*, pp. 1-6, 2016.
- [9] K. Jeffane and K. Ibrahim, "Detection and identification of attacks in Vehicular Ad-Hoc Network," in *2016 International Conference on Wireless Networks and Mobile Communications (WINCOM)*, pp. 58-62, 2016.
- [10] S. M. Nyabuga, et al., "Using particle swarm optimization (PSO) algorithm to protect vehicular ad hoc networks (VANETS) from denial of service (DOS) attack," *International Journal of Advanced Research in Computer Engineering and Technology*, vol. 5, no. 3, pp. 628-631, 2016.
- [11] I. K. Azogu, et al., "A new anti-jamming strategy for VANET metrics-directed security defense," in *2013 IEEE Globecom Workshops (GC Wkshps)*, pp. 1344-1349, 2013.
- [12] A. Singh and P. Sharma, "A novel mechanism for detecting DOS attack in VANET using Enhanced Attacked Packet Detection Algorithm (EAPDA)," in *2015 2nd international conference on recent advances in engineering & computational sciences (RAECS)*, pp. 1-5, 2015.
- [13] L. Mokdad, et al., "DJAVAN: Detecting jamming attacks in Vehicle Ad hoc Networks," *Performance Evaluation*, vol. 87, pp. 47-59, 2015.
- [14] V. B. Suresh, et al., "On-chip lightweight implementation of reduced NIST randomness test suite," in *2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, pp. 93-98, 2013.
- [15] A. Kaminsky, "Testing the Randomness of Cryptographic Function Mappings," *IACR Cryptology ePrint Archive, Report 2019/078*, 2019.
- [16] B. Kang, et al., "Nonce-Based Key Agreement Protocol Against Bad Randomness," *International Journal of Foundations of Computer Science*, vol. 30, no. 04, pp. 619-633, 2019.
- [17] M. Erritali, et al., "A Contribution to Secure the Routing Protocol "Greedy Perimeter Stateless Routing" Using a Symmetric Signature-Based AES and MD5 Hash," *International Journal of Distributed and Parallel Systems*, vol. 2, no. 5, pp. 95-103, 2011.
- [18] R. Shaikh and D. Deotale, "A survey on VANET security using ECC, RSA & MD5," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 4, no. 6, pp. 167-172, 2015.
- [19] X. Wang and H. Yu, "How to break MD5 and other hash functions," in *Annual international conference on the theory and applications of cryptographic techniques*, pp. 19-35, 2005.
- [20] J. Petit, "Analysis of ecDSA authentication processing in vanets," in *2009 3rd International Conference on New Technologies, Mobility and Security*, pp. 1-5, 2009.
- [21] J. J. Haas, et al., "Real-world VANET security protocol performance," in *GLOBECOM 2009-2009 IEEE Global Telecommunications Conference*, pp. 1-7, 2009.
- [22] B. Pooja, et al., "Mitigation of insider and outsider DoS attack against signature based authentication in VANETs," in *2014 Asia-Pacific Conference on Computer Aided System Engineering (APCASE)*, pp. 152-157, 2014.
- [23] J. Molina-Gil, et al., "Aggregation and probabilistic verification for data authentication in VANETs," *Information Science*, vol. 262, pp. 172-189, 2014.
- [24] A. Smitha, et al., "An optimized adaptive algorithm for authentication of safety critical messages in VANET," *2013 8th International Conference on Communications and Networking in China (CHINACOM)*, pp. 149-154, 2013.
- [25] K. Mershad and H. Artail, "REACT: Secure and efficient data acquisition in VANETs," *IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pp. 149-156, 2011.
- [26] S. A. Shah, et al., "A Dynamic Privacy Preserving Authentication Protocol in VANET Using Social Network," in *International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing*, pp. 53-65, 2019.