SE-GPSR: Secured and Enhanced Greedy Perimeter Stateless Routing Protocol for Vehicular Ad hoc Networks

https://doi.org/10.3991/ijim.v14i13.14537

Meriem Houmer, Mariya Ouaissa (✉), Mariyam Ouaissa,
Moulay Lahcen Hasnaoui
Moulay Ismail University, Meknes, Morocco
mariya.ouaissa@edu.umi.ac.ma

Abstract—In Intelligent Transport Systems (ITS), Vehicular Ad-hoc Networks (VANET) play an essential role in improving road safety and traffic efficiency. Nevertheless, due to its special characteristics like high mobility, large size of the network and dynamic topology make routing of data in the vehicular ad hoc network more challenging. The problem in these networks is to determine the routing protocol best suited to this environment, and then secure it to provide optimal and secure routing for the data. Recently, position-based routing protocol has been developed by researchers to be a very interesting routing technique for communication between vehicles. In this paper, we propose an secured and enhanced version of the Greedy Perimeter Stateless Routing (GPSR) protocol. This protocol consists of two modules: (i) To implement an improvement of GPSR routing protocol which minimizes transfer delays and control messages. (ii) To deal with security issues, we have proposed a solution that combines between an improved Diffie-Hellman algorithm for reliable key exchange and the hash function based Message Authentication Code (MAC) for the verification of the authentication and integrity of GPSR packet. The proposed solution was checked by the security protocol verification tool, Automated Validation of Internet Security Protocols and Applications (AVISPA), which indicated that it is a very secure level. Simulation results showed that our proposed compared to the original GPSR offers better performances.

Keywords—VANET, Position-based routing, Security, GPSR, Diffie-Hellman, H-MAC.

1 Introduction

The technological development that the world has seen today has affected all areas, particularly the communications sector, which is undergoing considerable change with the advent of wireless technology. Vehicular Ad hoc Networks (VANETs) are a new form of mobile ad hoc networks for establishing communications between vehicles or with infrastructure located at roadside. These networks are used to meet the

communication needs applied to transport networks to improve driving and road safety for road users [1].

Routing plays a very important role in VANET since all services are supported, unicast or multicast, based on multi-hop communications for routing of data [2]. In order to achieve the packet transfers, the routing protocols use local information of their neighborhoods in the network to decide the relay nodes that will be used in the data routing. In VANET, vehicles will probably face many obstacles like road junctions, buildings, traffic lights, trees, etc resulting in insufficient channel quality and connectivity. Hence, it is necessary to use an efficient and reliable routing protocol to have effective communication without losing data.

The traditional routing protocols designed for mobile ad hoc network cannot be used directly in VANETs, because it does not provide reliability, low latency, and high throughput performance [3]. Therefore, researches have proposed different routing protocols adapted to the vehicular networks, according to the popularity and the success of the Global Positioning System (GPS) that used in the VANET routing protocol has become a hot research spot. In fact, the most promising routing protocol category in VANETs that use this system is the position-based routing protocol.

Given the importance of the information exchanged between vehicles and the opening of the VANET environment, an attacker can send alert messages whose content is falsified or prevent the delivery of a legitimate message in order to cause accidents [4]. Since routing is a fundamental service in any communication system, it can be an ideal target for attacks. Unfortunately, the constraints brought about by the high mobility of the nodes in these networks and their decentralized aspect makes routing security more problematic than any other type of network. In this context, we are interested in routing security issues in vehicle communications. The main objective is to provide security mechanisms adapted to the characteristics of VANETs networks and their applications [5].

The objective of this work, is firstly propose an improvement to the Greedy Perimeter Stateless Routing (GPSR) protocol, which we have redesigned to increases the time to live of the packet to prevent the loss of data, also to decrease the number of hops that minimize the end-to-end delay. The second step is to secure this improved GPSR protocol, where each vehicle want to communicate with a destination vehicle should have a shared secret key which is obtained by executing an improved Diffie-Hellman Algorithm for reliable key exchange, this key will be used by the Keyed-Hash Message Authentication Code (HMAC) to verify the authentication and the integrity of GPSR packet.

The rest of the paper is organized as follows: In section 2 we present the background includes system architecture and security in VANET routing. Section 3 introduces the Greedy Perimeter Stateless Routing Protocol. Section 4 describes several preliminaries used in our solution. In section 5, we propose our secured and enhanced version of GPSR. The security of the designed protocol and the performance evaluation are analyzed in section 6. Finally, we conclude in section 7.

2 Background

In this section, we describe the system architecture of VANET communication and we present the fundamentals of routing and security in VANET.

2.1 System architecture

The VANET network is a subcategory of the Mobile Ad-Hoc Network (MANET) [6], where the nodes are replaced by vehicles, which can communicate with each other thanks to the On-Board Unit (OBU) and with other entities in the network such as the Road Side Unit (RSU) (Figure 1) [7].

In vehicular networks, two modes of communication can be distinguished, Vehicle-to-Vehicle (V2V) communications and Vehicle-to-Infrastructure (V2I) communications. Vehicles can use one of these two modes or combine them if they cannot communicate directly with road infrastructure. Vehicle networks are made up of several entities, which communicate with each other via radio waves.

RSU (Road-Side Unit): is an infrastructure located near roads. It plays the role of the router, which provides connectivity between OBU-OBU (V2V) or between an OBU and another infrastructure (V2I). Its main functions are broadening the communication range, providing connectivity to the OBU and other entities, and running security applications.

OBU (On-Board-Unit): is a wireless device, embedded in smart vehicles. It allows the transmission of information between cars or between a car and another infrastructure thanks to Dedicated Short Range Communications (DSRC). It is connected to one or more Application Units (AU). The OBU is based on IEEE 802.11p radio technology for sending short-range safety data. Among other things, it provides wireless radio access, ad hoc geographic routing, reliable and secure data transfer, as well as support for IP mobility.

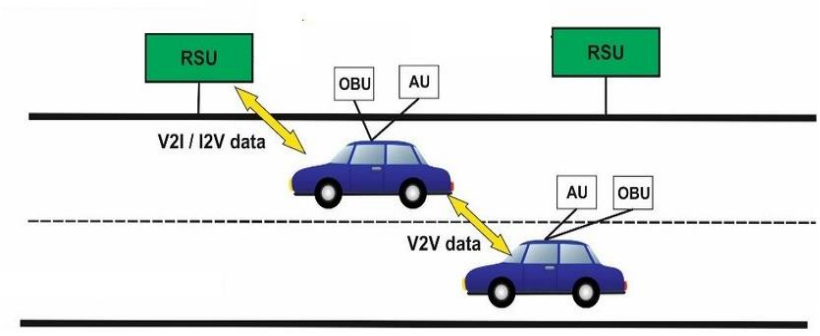

Fig. 1. VANET Architecture

2.2 Security aspects of routing in VANET

The design of routing protocols in VANETs is an important and necessary problem to support ITS. The main difference between VANETs and MANETs is the special mobility model and the rapidly modifiable topology. It is not actually practical to apply existing MANET routing protocols for vehicular networks. Routing is based on multi-hop communications; this makes communication between two or more nodes possible even if they are not in the same radio transmission range. The routing strategy must take into account the different characteristics of VANETs networks (changes in topology, high mobility, limited capacity of radio links, etc.) to ensure a strategy that guarantees permanent network connectivity. In the ad hoc context, it is possible that the destination node is outside the radio transmission range of the source node, which requires the use of the relaying technique where the intermediate nodes can serve as a relay to route the packets to the good destination [8]. Generally, routing protocols can be classified into two main families:

Routing protocols based on topology: Routing protocols based on topology use information on the links between nodes for packet forwarding. This family of protocols can be divided into three categories: proactive, reactive and hybrid protocols. In the literature, there are several topological protocols such as AODV, DSR and TORA as reactive protocols; OLSR and DSDV as proactive protocols and ZRP as hybrid protocol.

Geographic routing protocols: Geographic (or position-based) routing protocols use geographic coordinates (for example, provided by GPS) to find a route to the destination. To achieve this objective, the geographic coordinates of the nodes are included in the routing tables. The major advantage of these protocols compared to previous protocols is that they considerably reduce signaling (control packets), especially in large and dynamic networks. In the literature, there are several geographic routing protocols. The best known are: LAR, DREAM, GPSR.

In fact, if the routing protocol rules used were not well designed, the malicious entity can manipulate them in order to interrupt the routing of a security-related message; therefore, these VANET networks will have a negative impact on road safety in the presence of attackers. In ad hoc networks, an attack is just a specific combination of a few attack mechanisms aimed at achieving one or more objectives. Attackers can replay and modify data packets, but these manipulations are not typically considered as a routing security issue, and must be detected using cryptographic tools at the upper layer level (the verification model of end to end) or lower layers (the hop-by-hop verification model). However, the elimination of data packets is considered an action aimed at routing functionality [9].

3 Greedy Perimeter Stateless Routing (GPSR)

Greedy Perimeter Stateless Routing is a Unicast and reactive Position Based routing protocol. Its operating model assumes that all the nodes are on the same plane. Actually, because of the mobility of the nodes, certain routing algorithms which are based on the network topology, or launch a phase of discovery of routes to convey data are not

suitable for GPSR. Therefore, it uses the geographical position of the nodes for the routing of data or control packets [10].

In VANET, the nodes are likely to move. Accordingly, we need a mechanism allowing each node to know the position of its neighbors. In order to signal their presence and their location, the nodes flood the network by sending a signaling packet (beacon messages) containing their position and their identifier. It uses the control messages "beacon" to inform the neighboring nodes about the directions that a node can assume, also to construct their position table.

Alternatively, the GPSR protocol allows the node to encapsulate in a few bits their position in the header of the packets that sends. In this case, all the interfaces of the nodes must be in promiscuous mode in order to receive the packets if they are in the coverage area of the transmitter. GPSR uses two mechanisms to transmit a packet to its recipient: Greedy Forwarding and Perimeter Forwarding.

3.1 Greedy forwarding

The fundamental aspect of this technique is the concept that the source node knows the geographical location of the destination node. This location information is included in the route request packet, and it can be recognized through the exchange of beacons messages. The greedy forwarding mode consists of choosing the nearest neighbor to the destination, in its geographical area, as the next hop to forward the packet. This mechanism is repeated recursively until the destination is reached. Figure 2 shows an example of this routing mode in which a source S sends a packet of data to the node D, The packet is transmitted and relayed jump-by-jump by proceeding at each step the selection of the nearest neighbor of the destination [11].

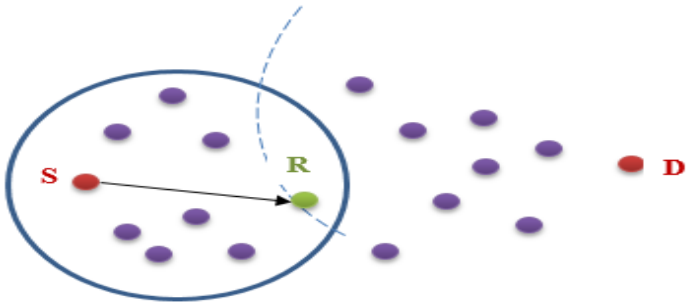

Fig. 2. Greedy Forwarding

3.2 Perimeter forwarding

Perimeter forwarding is used when the Greedy Forwarding algorithm could not find a neighboring node closer to the destination except itself. This mechanism uses the right-hand rule. This algorithm uses the right-hand rule which is defined as follows: When a packet arrives at node x from the node y, the path to follow is the next one

which is in an anticlockwise direction when leaving of x and with respect to the segment [xy] while avoiding "crossing links" (road already traveled). Figure 3 shows a more specific example of this mode [12].

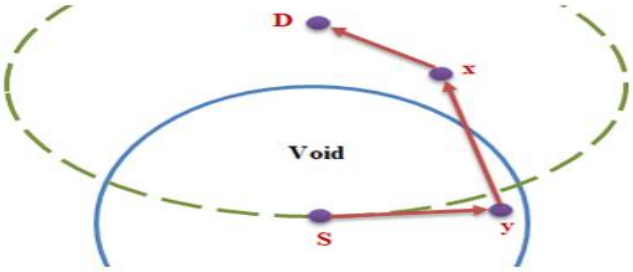

Fig. 3. Right-hand Rule

3.3 Drawbacks of GPSR

The GPSR can face a link failure in the VANET due to the high mobility of nodes and frequent topology changes. Since GPSR is a geographical strategy, it can lead packets toward dead ends. Moreover, due to the routing loop between the greedy forwarding and the perimeter forwarding transmission strategies, the Time-To-Life (TTL) of a packet can decreases which increases the packet loss, and a timeout may occur because of the number of hops necessary to reach the destination. This number of hops increases in the perimeter forwarding mode which increases the end-to-end delay. Also in the side of security, the GPSR protocol does not specify any security measures. However, it is the main target for attacks which aim to route road safety alerts in the VANET network in order to disrupt road traffic or cause accidents. That is why we propose a Secured and Enhanced GPSR (named ES-GPSR) that minimizes these weak points.

4 Preliminaries

In this section, we describe and analyze the cryptographic methods and algorithms used in our solution namely Diffie-Hellman Protocol, Message Authentication Code, and AES encryption.

4.1 Diffie-Hellman key exchange protocol

Diffie-Hellman (DH) Key Exchange is the commonest public-key algorithm that allows a secret key sharing between two entities while only plaintext messages can be exchanged on unsecured networks. Indeed, any encryption of a large amount of data can only be done with secret key encryption, especially if this exchange takes place in real time, due to the relative slowness of public key encryption. For exchanging between two interlocutors a secret key K of size t bytes, node 1 and node 2 have a finite

cyclic group G and g is a generator of this group. Take for example for G the multiplicative group (Z/pZ) where p is a large prime number [13]. Figure 4 shows the Diffie Hellman key exchange process.

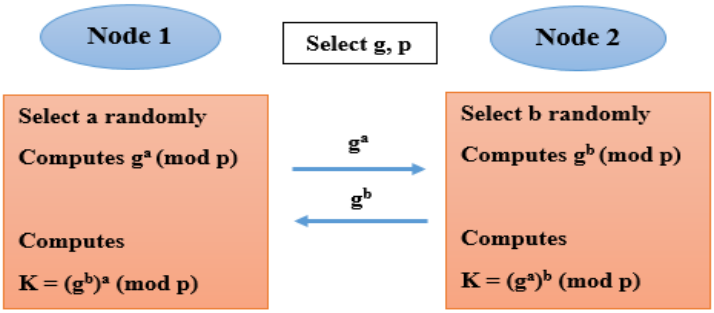

Fig. 4. Diffie-Hellman Key Exchange Protocol

4.2 Message Authentication Code (MAC)

The concept of MAC is relatively similar to hash functions. These are also algorithms that create a small, authenticating block of fixed size. The big difference is that this authenticator block is no longer based only on the message, but also on a secret key. Like hash functions, MACs do not need to be reversible. In fact, the receiver will perform the same calculation on the message and compare it with the received MAC. The MAC ensures that the message is unchanged (integrity) and comes from the sender (authentication, by using the secret key). It can also be used as additional encryption and can be calculated before or after the main encryption, although it is generally advised to do it before [14].

Many algorithms for calculating MAC exist in modern cryptography. The most popular are based on hashing algorithms, like HMAC (Hash-based MAC, e.g. HMAC-SHA256) and KMAC (Keccak-based MAC). Others are based on symmetric ciphers, like CMAC (Cipher-based MAC), GMAC (Galois MAC) and Poly1305 (Bernstein's one-time authenticator). Other MAC algorithms include UMAC (based on universal hashing), VMAC (high-performance block cipher-based MAC).

Table 1 contains the execution time for some of the most commonly used MAC algorithms. All were implemented in Crypto++ Library [15], coded in C++ language and ran on Intel Core 2 1.83 GHz Processor under Windows environment.

Table 1. Execution Time of MAC Algorithms

Symmetric Algorithms	HMAC	CMAC	VMAC
Execution Time (µs)	0.509	0.600	3.738

It is desirable to create MACs from hash functions rather than from block encryption. Several reasons are advanced such as the speed of the hash functions, and the lack of

export controls. The major difference between MAC and Hash being the management of a secret key, it is necessary to integrate this key into the hashing algorithm. The principle was to directly concatenate the message to the key.

4.3 Advanced Encryption Standard (AES)

The AES encryption standard was adopted in 2000 by NIST to replace DES [16]. This symmetric encryption is made up of substitutions, offsets, "or excludes-sif" and multiplications in a finite field of fixed polynomials; these operations are elementary, simple and quick to calculate. It allows encrypting blocks of 128, 192 or 256 bits using symmetric keys of 128, 192 or 256 bits. The choice of the size of the key and the size of the blocks are independent, so there are in total 9 possible combinations. This leaves greater flexibility to the AES user depending on the security level and the calculation speed desired [17].

In this context, we measure and compare the execution time of the AES and other symmetric algorithms to prove that the AES is faster and more responsive to our needs for security in the context of vehicular ad hoc networks. We will use to measure the execution time of AES, DES and Blowfish encryption algorithms with 128 bits is a size of keys that we implemented in Crypto++ Library and coded in C++. Execution time values were obtained by measurements running on a Pentium 4 2.1 GHz processor under Windows (Table 2).

Table 2. Execution Time of Symmetric Algorithms

Symmetric Algorithms	AES	DES	Blowfish
Execution Time (µs)	2.196	5.998	3.976

5 Proposed Scheme

In this section, we propose our framework scheme named Secured and Enhanced GPSR (SE-GPSR) that contains two contributions, the first consist of the enhancement of GPSR routing protocol and the second phase includes a set of mechanisms to secure the improved protocol.

5.1 The enhanced version of GPSR

In our first contribution, the enhanced version of GPSR that we have proposed is currently designed only to urban scenarios, and it aims to reduce the drawbacks of GPSR. In our enhanced version, the Perimeter Forwarding method has been removed and a new next-hop selective mechanism has been introduced. This mechanism is based on the distance between the source node (or relay node) and the destination plus the distance between the source node (or the relay node) and the next hop. The next-hop is the neighbor that provides a minimum overall distance. Actually, the global distance of the node relay is represented by the distance between the source node and this relay plus the distance between this relay and the destination.

Our aim is to route a message as soon as possible to a relay node which is in the same way as the final destination. To achieve our goal, we need to change the method that discovers the next hop in the GPSR algorithm. In the proposed method, each relay node should add its identifier in the packet header to not return the packet to the previous node. Also, each node must temporarily save the identifier of all packets processed to compare them with the identifier of the succeeding packet in order to avoid routing loops. Figure 5 present the flowchart of the enhanced GPSR.

Basically, the enhanced accepts a datagram as a parameter. First of all, it recovers the geographical position of the destination, the identifier of the preceding node and the identifier of the datagram. If the identifier of the datagram does not exist in the list of datagrams already processed, it adds this datagram identifier in the list. After that, it selects a neighbor that has a minimum overall distance and different from the preceding node. As well, it inserts its identifier in the datagram header to not return this datagram to it. Finally, it sends the datagram to the next hop choosing.

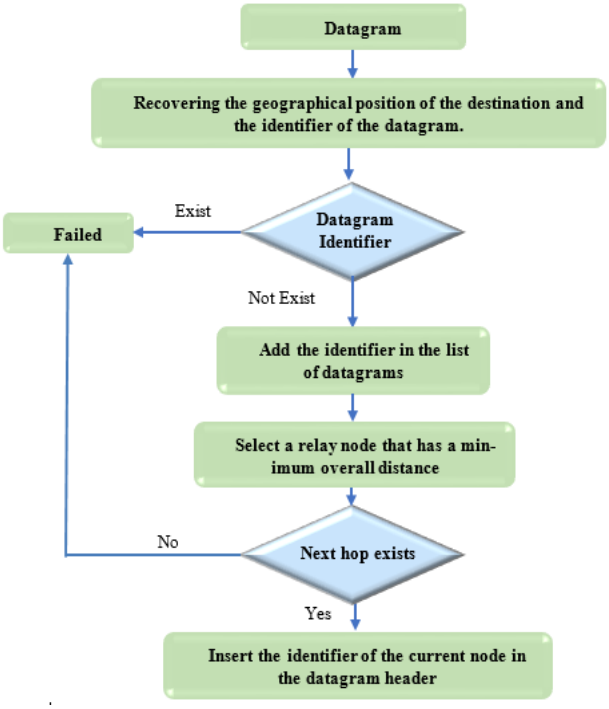

Fig. 5. Enhanced GPSR Diagram

5.2 Secure enhanced GPSR

To ensure the enhanced GPSR protocol presented in our first contribution, we will take into consideration the principle of improvement that we proposed, then we will secure the exchange of keys between the vehicles as well as the GPSR packets sent. We

will consider that the identifier of each vehicle is transmitted in clear, which will allow us to the relay node to verify the identities of source and destination as well as the optimal route of each transfer. Here are the main points of our solution:

- Generate a shared secret key between two vehicles using an enhanced and more secure Diffie-Hellman algorithm.
- Apply a hash function-based MAC using the generated secret key on the GPSR packet (Authentication and Integrity)
- Use the AES algorithm to encrypt the sent data.

5.3 Establish secret keys

Our first phase in this contribution is to establish secret keys between two vehicles (in a hop**),** no other cryptographic information is exchanged by the two entities, and trusted third parties are not available. The idea is to have secret key that will be used in symmetric encryption and hash function-based MAC. According to Figure 4 of the process of DH algorithm, it is understood that the attacker can change those DH parameters without being detected and break in communication. This attack is called Man in The Middle (MITM). For this reason, we consider an improved the Diffie-Hellman algorithm to the next level of security to reduce the probability of Diffie-Hellman attacks.

The enhanced Diffie-Hellman algorithm for reliable key exchange is based commitment scheme in order to resist attacks presented in the DH algorithm (Figure 6). A commitment scheme is considered as an important cryptographic primitive that permits to constitute blocks. This scheme allows an individual user to commit an allocated value or message with the capacity to eventually reveal the committed message or value while keeping the message invisible to other users. The two functions Commit and Open, describe a commitment scheme.

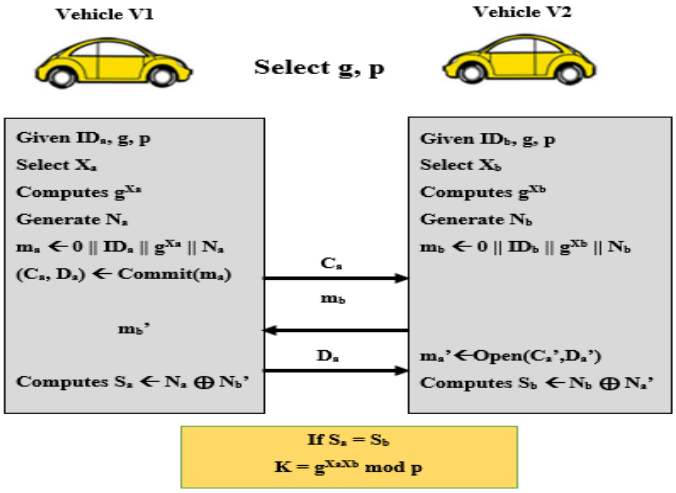

Fig. 6. Process of Key Exchange using an Enhanced Diffie-Hellman Protocol.

We supposed that two vehicles V1 and V2 agree upon G, g, p, where G is a finite cyclic group, g is a generator in G, and p is a large prime number.

Firstly, V1 and V2 select randomly their secret exponents X_a and X_b respectively and compute DH public parameters g^{Xa} and g^{Xb} respectively. After that, V1 and V2 respectively generate random values N_a and N_b. Thereafter, both vehicles prepare the messages m_a and m_b respectively where ID_a and ID_b are identifiers for nodes. Here, 0 and 1 are used to prevent a reflection attack. Then, V1 calculates the commitment/opening pair (C_a,D_a) of her message m_a and sends the commitment C_a to V2, which answers with her message m_b. Consecutively, V1 sends D_a, by which V2 opens the commitment C_a'. In the verification, both the vehicles generate verification strings S_a and S_b, If they are match, then both V1 and V2 accept each other's DH-parameters g^{Xa} and g^{Xb} as being authentic and unchanged. Then, they both generate shared key K.

5.4 Message authentication and encryption

In the regular procedure of MAC only message authentication from a source takes place and the message is sent in clear on the network. Indeed, in our proposition, we will consider the case where we are going to ensure the service of confidentiality in addition to authentication and integrity of the message. The idea is that, the MAC is concatenated to the message, and everything is encrypted and sent to the destination.

An extension to the MAC function to use the cryptographic hash function and the secret key in the message authentication code is the Keyed Hash Message Authentication code. In general, the HMAC value is determined using MD5 and SHA-1 cryptographic hash functions. The type of cryptographic hash used in creating the HMAC in our scheme is HMAC-SHA256. Several objectives had to be achieved such as the fact of using existing hash functions without modifications, of allowing an easy replacement of the hash function in case faster or safer functions are found or required, of preserving the initial performance of the hash function and use (and manipulate) the keys in a simple way. HMAC treats hash functions like 'black boxes'. The hash function becomes a module. It then becomes simple to replace it if we develop a new faster or safer hash function, which provides a better guarantee of security. Due to this modularity, there will be no modification to be made to the algorithm.

In VANETs the hash function MAC will be the mechanism to ensure the integrity and the authentication of packets exchanged between vehicles in GPSR. In fact, routing packet from the source to the destination requires minimum time for mobile Nodes, so we suggest using the AES encryption algorithm to crypt message sent in clear over the network (Figure 7).

The vehicle recipient incorporates the same packet with the same secret key locally in HMAC. The recipient compares this to the HMAC of the transmitter. The sender is authenticated if the two HMACs matches and the completeness of the message is guaranteed.

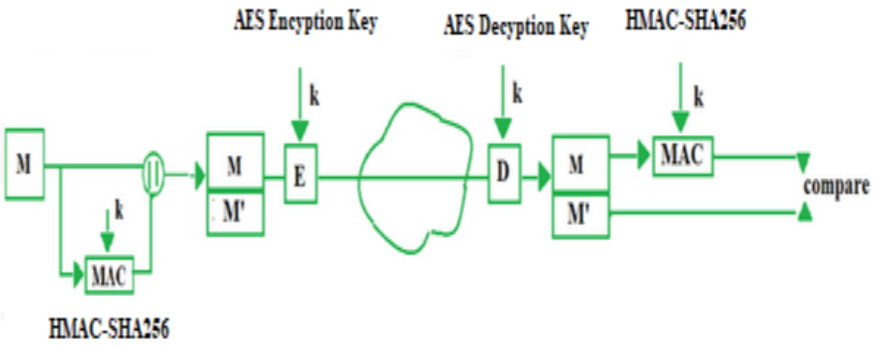

Fig. 7. Process for Creating and Checking Hash based-MAC and Encryption

6 Results and Discussion

In this section, we present the security analysis of our proposed scheme by the formal verification and we evaluate the results of simulation of the original GPSR and SE-GPSR using Network Simulator 2 (NS2) in terms of several metrics.

6.1 Security analysis

This solution was checked by the security protocol verification tool, Automated Validation of Internet Security Protocols and Applications (AVISPA) [18], which indicated that it is a very secure level. The main advantage of this tool is the ability to use different verification techniques on the same protocol specification. The protocol designer interacts with the tool by specifying a security problem in the High Level Protocol Specification Language (HLPSL) [19]. The primary goal of our proposed scheme is to verify that it can provide a reliable key exchange between two vehicles In order to secure the data transferred. We need to verify that the proposed scheme can ensure a successful authentication and integrity between the entities by using back-end servers. In Figures 8 and 9, we present the roles of vehicles 1 and 2.

```
role Vehicle1 (V1,V2:agent, G:text, Snd,Rcv:channel(dy),HMAC: hash_func)
played_by V1 def=
local State:nat, Pa,Nbb,Na,Naa,IDa,Xa,Nsecret,Xb:text, Sa,Ma,Mb,Ca,Da,X,K:message
const r1, r2 : protocol_id
init State := 1
transition
1. State=1 /\ Rcv(start) =|>
State':=2   /\ Xa' := new() /\ G' := new()
/\ X' := exp(G',Xa')
/\ Mb' := new()
/\ Ca' := new()
/\ Ma' := (0.IDa.X.Na)
/\ Snd (Ca')
/\ Rcv (Mb')
2. State=2 /\ Snd(Da') =|>
State' :=3 /\ Na' := new() /\ Nbb' := new() /\ Sa' := xor(Na',Nbb')
           /\ X' := new() /\ Xb' := new() /\ K':=exp(X',Xb') /\ Nsecret':= new() /\ Snd(HMAC(Nsecret'.K'),r1)
end role
```

Fig. 8. Role of Vehicle 1

```
role Vehicle2 (V2,V1: agent, G:text, Snd,Rcv:channel(dy),HMAC: hash_func)
played_by V2 def=
local State : nat, Nb,Nbb,Naa,IDb,Xb,Nsecret,Xa:text, Sa,Da,Sb,Mb,Caa,Daa,Y,K: message
const r1, r2 : protocol_id
init State := 0
transition
1. State=0 /\ Snd(start) =|>
State':=1
/\ Xb' := new() /\ G' := new()
/\ Y' :=exp(G,Xb') /\ Nb' :=new() /\ IDb' := new() /\ Mb' :=(0.IDb'.Y'.Nb') /\ Snd(Mb')
2. State =1 /\ Rcv(Da') =|>
State' :=2 /\ Naa':=new() /\ Nb':=new() /\ Sa' := xor(Nb',Naa')
          /\ Xa':=new() /\ Y' := new() /\ K':=exp(Y',Xa') /\ Nsecret':= new() /\ Rcv(HMAC(Nsecret'.K'),r2)
end role
```

Fig. 9. Role of Vehicle 2

After running this specification with OFMC and CLAtSe backends, we can conclude that the proposed scheme can accomplish our goal and can resist those malicious attacks, such as MITM attacks and secrecy attacks under the test of AVISPA. The outputs of the model checking results are shown in Figures 10 and 11.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/SE-GPSR.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.06s
  visitedNodes: 10 nodes
  depth: 4 plies
```

Fig. 10. Results Reported by the OFMC Back-End

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/span/span/testsuite/results/SE-GPSR.if

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed   : 0 states
  Reachable  : 0 states
  Translation: 0.02 seconds
  Computation: 0.00 seconds
```

Fig. 11. Results Reported by the CL-AtSe Back-End

6.2 Simulation results

The SE-GPSR protocol is simulated using NS2 [20] to emulate selective attacks such as Sink hole, Grey hole, Selfish, On-off and Modification attacks in the vehicular ad-hoc network. The network animator output for 200 nodes and the number of malicious nodes is varied between 5 and 20. In this simulation, we compare original GPSR to our secured and enhanced version ES-GPSR in terms of Packet Delivery Ratio and End-to-End Delay. The parameters used in the simulation are listed in Table 3.

Table 3. Simulation Parameters

Parameter	Value
Simulation time	100 seconds
Number of nodes	200
Mobility model	Random Way Point
Speed	70 Km/h
Protocol MAC	802.11p
Package size	128 bytes
Transmission interval	1 pack / second
Simulation area	1000 x 1000 m

Packet Delivery Fraction It is the ratio between the number of packets sent by the source and the number of packets received by the destination. Figure 12 shows the packet delivery ratio of the original and the secured and enhanced greedy perimeter stateless routing protocols against the number of malicious nodes. It is clearly observed that the new version of GPSR performs better than the original version. This is explained by the increase in the time to live of the packet, which is due to the suppression of the perimeter transfer in the SE-GPSR. Furthermore, short routes are preferred to transfer packets in SE-GPSR from source to destination. In addition, based on its degree of confidence, SE-GPSR selects or unselects routing nodes.

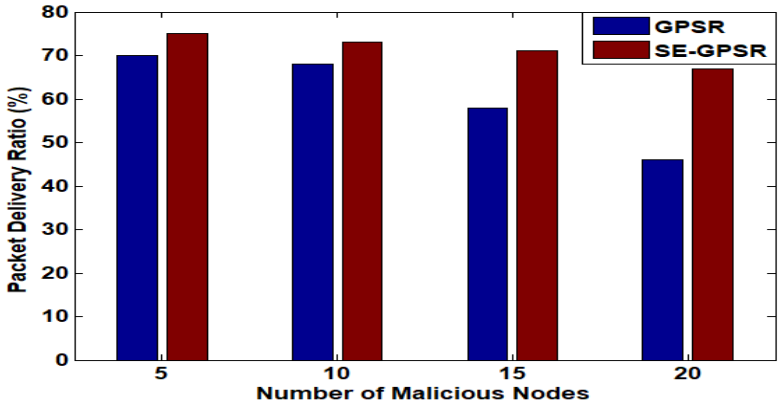

Fig. 12. Packet Delivery Ratio vs. Number of Malicious Nodes

End-to-end delay: Represents the time interval between the date that the package is sent by the source and the date that the package is received by the destination. In SE-GPSR, the packets are transmitted to their destination in a brief time. This is due to the fact that, unlike GPSR, SE-GPSR does not get in a routing loop between the greedy forwarding and the perimeter forwarding transmission modes. The typical end-to-end delay allows nodes to choose optimal paths for data transmission and that will improve the quality of services of the network. However, according to the simulation results of the end to end delay against the number of malicious nodes illustrates in Figure 13, the delay of SE-GPSR protocol is higher slightly than that of GPSR protocol. This is due to the additional processing time used in hash operations and different cryptographic methods. This additional end to end delay in our proposal is introduced to make the protocol more secure against attacks on the network and to find the non-malicious node before forwarding the packet.

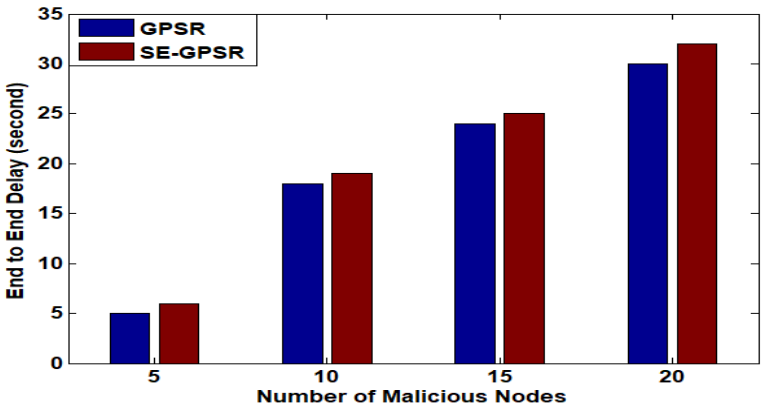

Fig. 13. End to End Delay vs. Number of Malicious Nodes

7 Conclusion

The problem of communication in vehicular ad hoc networks attracts more and more attention from research groups. In this type of network, routing and security are two major concerns. In this paper, we have proposed a secured and enhanced version of the greedy perimeter stateless routing protocol that improves the performance of the traditional GPSR. We have at first improved GPSR by removed the perimeter forwarding technique and add a new function based on the minimum overall distance to select the next hop. However, this modification prolongs the time-to-life of the packet and then increases the packet delivery ratio. In addition, it decreases the number of hops and the end-to-end delay. Secondly, we have secured this improvement by an enhanced DH for key exchange and hash function based MAC to ensure the authentication, integrity and confidentiality services. Formal verification and security analysis show that the proposed protocol can provide robust security and fulfill its design goals. In addition, it is clearly shown in our simulation results that the SE-GPSR outperforms GPSR

significantly in the terms of packet delivery ratio and provides a higher slightly end-to-end delay because of the additional processing time used in different security mechanisms in order to make our proposed more secure.

8 References

[1] M. Houmer and M.L. Hasnaoui, "A Qualitative Assessment of VANET Routing Protocols under different Mobility Models," *Journal of Computer Science*, vol. 15, no. 2, pp. 161-170, 2019. https://doi.org/10.3844/jcssp.2019.161.170

[2] S. Cloudin and P. Mohan Kumar, "Challenges on Mobility Models Suitable to Vanet," *Journal of software*, vol. 12, no. 2, pp. 91-100, 2017.

[3] R. Dutta and R. Thalore, "A Review of Various Routing Protocols in VANET," *International Journal of Advanced Engineering Research and Science*, vol. 4, no.4, pp. 221-224, 2017. https://doi.org/10.22161/ijaers.4.4.34

[4] R.G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys." *Computer Communications*, vol. 44pp. 1-13, 2014. https://doi.org/10.1016/j.comcom.2014.02.020

[5] L.R. Raghavendar and C.R. Reddy, "A Key Exchange Approach for Proficient and Secure Routing in Mobile Adhoc Networks," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 11, no. 4, pp. 43-54, 2017. https://doi.org/10.3991/ijim.v11i4.6440

[6] J. Kumar and A. Kathirvel, "Analysis and Ideas for Improved Routing in MANET," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 13, no. 4, pp. 164-177, 2019. https://doi.org/10.3991/ijim.v13i04.9928

[7] 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. https://doi.org/10.3390/s19163589

[8] B. Paul, Md. Ibrahim, and Md. Abu Naser Bikas, "VANET Routing Protocols: Pros and Cons," *International Journal of Computer Applications*, vol. 20, no.3, pp. 28-34, 2012. https://doi.org/10.5120/2413-3224

[9] J. Kakarla, S. Sathya, G. Laxmi, and R. Babu, "A Survey on Routing Protocols and its Issues in VANET," *International Journal of Computer Applications*, vol. 28, no. 4, pp.38-44, 2011. https://doi.org/10.5120/3373-4663

[10] B. Karp and H.T. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks," In Proceedings of the 6th annual international conference on Mobile Computing and Networking, 2000, pp. 243-254. ACM. https://doi.org/10.1145/345910.345953

[11] Z. Jiang, J. Ma, W. Lou, and W. Jie, "An information model for geographic greedy forwarding in wireless ad-hoc sensor networks." In IEEE INFOCOM 2008-The 27th Conference on Computer Communications, 2008, pp. 825-833. IEEE. https://doi.org/10.1109/infocom.2008.134

[12] G.M. Tang, Y. Xie, J.Y. Tang, and W.D. Xiao, "Regional perimeter routing for GPSR based on left & right-hand rules," *Jisuanji Yingyong Yanjiu*, vol. 28, no. 3, pp. 1099-1101, 2011. https://doi.org/10.1109/iccsnt.2011.6182067

[13] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. 22, pp. 644–654, 1976. https://doi.org/10.1109/tit.1976.1055638

[14] B. Preneel and P.C. Van Oorschot "On the security of iterated message authentication codes," *IEEE Transactions on Information theory*, vol. 45n no. 1, pp. 188-199, 1999 https://doi.org/10.1109/18.746787

[15] Crypto++ Library: http://www.cryptopp.com/.

[16] S. Heron, "Advanced encryption standard (AES)," *Network Security*, vol. 2009, no. 12, pp. 8-12, 2009. https://doi.org/10.1016/s1353-4858(10)70006-4
[17] W.S. Wardhono, N.D. Priandani, M.T. Ananta, K.C. Brata, and H. Tolle, "End-to-end privacy protection for facebook mobile chat based on aes with multi-layered md5," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 12, no. 1, pp. 160-167. 2018 https://doi.org/10.3991/ijim.v12i1.7472
[18] AVISPA Project : http://www.avispa-project.org/
[19] M. Ouaissa, M. Ouaissa, and A. Rhattoy, "An Efficient and Secure Authentication and Key Agreement Protocol of LTE Mobile Network for an IoT System," *International Journal of Intelligent Engineering and Systems (IJIES)*, vol. 12, no. 4, pp.212-222, 2019. https://doi.org/10.22266/ijies2019.0831.20
[20] N. Singh, R.L. Dua, and V. Mathur, "Network Simulator NS2-2.35*," International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 2, no. 5, pp.224-227, 2012.

9 Authors

Meriem houmer is a PhD Student at Research Team ISIC, Laboratory of Modelisation of Mathematics and Computer Science from ENSAM, Moulay Ismail University, Meknes Morocco. Her research interests routing protocols and security in vehicular ad hoc network.

Mariya Ouaissa is a PhD graduated in 2019 in Computer Science and Networks, at the Laboratory of Modelisation of Mathematics and Computer Science from ENSAM, Moulay Ismail University, Meknes, Morocco. Her main research topics are IoT, M2M, WSN, Ad Hoc Networks, Cellular Networks and Security.

Mariyam Ouaissa is a PhD graduated in 2019 in Computer Science and Networks, at the Laboratory of Modelisation of Mathematics and Computer Science from ENSAM, Moulay Ismail University, Meknes, Morocco. Her main research topics are M2M, WSN, Ad Hoc Networks and Cellular Networks.

Moulay Lahcen Hasnaoui is an Associate Professor in Department of Computer Science at High School of Technology, Moulay Ismail University, Meknes, Morocco. Also, in a member of Research Team ISIC at High School of Technology. His research interests include Information Systems and Communications.

Article submitted 2020-04-01. Resubmitted 2020-05-20. Final acceptance 2020-05-20. Final version published as submitted by the authors.