International Journal of Electronics Communication and Computer Engineering
Volume 5, Issue 6, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

Efficient Privacy and Revocation in VANETs by Measuring the Level of Trustiness

Reham Abdellatif Abouhogail
Electrical Quantities Metrology Department,
National Institute of Standards, Cairo, Egypt

Heba K. Aslan
Informatics Department,
Electronics Research Institute, Cairo, Egypt

***Abstract* – In the near future, Vehicular Ad-Hoc-Networks are going to change the way people drive and can help to improve the traffic management and roadside safety. Unfortunately, a VANET faced a set of challenges in security, privacy and detection of misbehaving nodes. In this paper, we propose a new protocol which we named Symmetric Key Based Privacy System (SKBPS) for VANET system. The system consists of three units: The Certificate Authority (CA), The Road Side Unit (RSU) and node units. CA is a trusted party to take charge of the network's security and privacy issues. RSU acts as the key distributor for the group of vehicles in its region, and judge whether a vehicle is a trust node or not. Nodes are ordinary vehicles on the road. CA is able to estimate whether a vehicle is a legitimate node or not. SKBPS for VANET presents a new technique which facilitates the revocation of malicious vehicles and guarantees efficient privacy. SKBPS found solutions for most types of attacks in VANET like: traffic analysis attack, malicious vehicle attack and Sybil attack. The proposed protocol is analyzed using both BAN logic and Strand Spaces model. The analysis shows that the proposed protocol achieves its goals without bugs or redundancies, and it isn't vulnerable to data desynchronization.**

***Keywords* – Security, Ad-Hoc Networks, Key Management, VANETs, Privacy.**

I. INTRODUCTION

Vehicular Ad-Hoc Networks (VANET) will help to improve traffic safety and efficiency. Vehicular networks have become a hot emerging research subject. Advances in VANETs have triggered the development of new attractive applications such as payment systems that satisfy additional requirements associated with VANET. There are two modes of vehicle communication in a VANET: Vehicle-to-Vehicle (V2V) and Vehicle–to-Infrastructure (V2I). The main application of VANET is the distribution of information about local traffic or road conditions. By making an analysis to the VANET system, we found that VANET system is considered a type of MANET system but it differs from MANET in many points:

1. The backward secrecy is not important in VANET system in some situations, because the history information for some applications is not important, like information about past traffic.
2. The vehicles have more capabilities than the mobiles. Therefore, we can add more features.
3. The main application of VANET, which require to be secured, is the distribution of information about local traffic or road conditions.
4. Lack of security in VANET is more dangerous, and may affects life.
5. The very high speed of real-time constraints is an important characteristic in VANETs. So all the security services should meet strict time constraints [1]. The security infrastructure of VANETs is very important. The system should guarantee that life critical information cannot be modified by an attacker. Also, the privacy of the drivers and passengers is a highly important object. Preserving the authenticity of messages exchanged contradicts with maintaining the privacy of the vehicles. In the present paper, we propose a new protocol to satisfy these two goals: security and privacy. The proposed protocol is characterized by low communication and computation overheads to revoke the malicious vehicles. In contrast to most presented schemes, which are based on public key cryptography, our proposed scheme is based on symmetric key cryptography. This leads to a lower computation overhead and a higher performance. In addition, the proposed protocol overcomes several types of attacks in VANET like: traffic analysis attack, malicious vehicle attack and Sybil attack. The proposed protocol facilitates the revocation of malicious vehicles and guarantees efficient privacy. The proposed protocol is analyzed using both BAN logic and Strand Spaces model. The analysis shows that the proposed protocol achieves its goals without bugs or redundancies, and it isn't vulnerable to data desynchronization. The remainder of the paper is organized as follows: the related work over VANET is summarized in Section 2. In Section 3, a description of the new protocol is detailed. In Section 4, a verification of the proposed protocol is described. In Section 5, Comparison of the new protocol with other protocols is presented. Finally, Section 6 concludes the paper.

II. RELATED WORK

VANET security and privacy is an interesting topic for both industry and academic research. The highly dynamic topology, the shared wireless medium, and the lack of any centralized network management make VANETs susceptible to eavesdropping, intrusion, penetration and so on. Security in VANETs is more difficult because there's no fixed infrastructure. Most of the security solutions are based on public key cryptography as in IEEE1609.2 standard [2]. Each vehicle has a pair of keys: a private signing key and a public verification key. The verification key is certified by a Certificate Authority (CA). Each sent message will be signed to provide message authentication, which could prevent the outsider attackers from injecting false messages [3]. To prevent Sybil attack, Yan et al. [4] proposed a novel solution that is based on seeing of believing. They used on-board radar as the virtual eye. For more trustiness, the vehicle can see surrounding vehicles.

By comparing, what is seen with what has been heard, a vehicle can detect the real position of the intended vehicle, and determine the malicious ones. Some researchers work on prevention of traffic analysis attack. Cencioni et al. [5] proposed VIPER: a Vehicle- to- Infrastructure communication Privacy Enforcement Protocol. VIPER is resilient to three major traffic analysis attacks: coding attack, message volume attack and timing attack. Privacy requires getting a method to authenticate the vehicles while preserving their anonymity. Vehicle identification number (IN) can be used to identify vehicles in VANETs; this number is unique for each vehicle. VIPER uses a public key algorithm to reach its goal. Langley et al.'s in [6] proposed generating some large random value and concatenate this value to the vehicle's IN. The resulting value is then hashed using some hash algorithm. The hashed value is then used as a unique identifier. The appending of a random value provides some security against brute force attacks to determine the vehicle's identity. In [7], a new system architecture called the Plausibility Validation Network (PVN) was proposed to check the raw data from sensors and further evaluate whether the incoming or generated message is valid or not. The PVN system provides security against illusion attack. The presented protocols try to solve the problem of false message injection from outsider attacker by assign to each vehicle a private signing key and a public verification key. The verification key is certified by a certificate authority (CA). The signature is used to provide message authentication. In [8], E. Ramaya proposed cooperative message authentication protocol for VANET to prevent compromised RSUs and malicious vehicle. E. Ramaya uses public encryption technique. His system solved the problem of uncompromised RSU's by regular broadcasting the compromised RSUs' identities. E. Ramaya's system allows sending accusation message from the vehicles to the CA, which may facilitate the denial of service attack by sending many false accusation messages. In [1], Neng et al. proposed a protocol for VANET using symmetric encryption for exchange of messages. In their protocol, all group members share the same group key. This makes the system susceptible to many types of attacks, like: Sybil attack and malicious vehicle attack. The description for all of these types of attacks, and the proposed solutions are declared in Table.1. In the next section, a description of the proposed protocol is detailed.

III. Symmetric Key Based Privacy System (SKBPS)

Vehicular networks have become an emerging research area. Because of its nature, it is vulnerable to different attacks like: eavesdropping, intrusion, and penetration. Most of the security solutions are based on public key cryptography which leads to a high computation overhead and also degrades the system's performance. In the present paper, we propose a solution which is based on symmetric key cryptography which leads to a low computation overhead and enhances the system's performance. In the next subsections, a description of the SKBPS protocol is detailed.

A. Network Structure

In this paper, we consider infrastructure which is based on VANET, where entities can be classified into three categories: the certificate authority, road side infrastructure and nodes as shown in Fig.1. The certificate authority is responsible of giving the service to the vehicle's owner. Road side infrastructure consists of RSUs deployed at the road sides which are responsible for key distribution. Road signs or Traffic lights can be used as RSUs after reformation [8]. RSU's have powerful firewalls and other security protection mechanisms. RSU's is more secure than nodes. Nodes are ordinary vehicles on the road that can communicate with each other and with RSU's by radio. We assume that each vehicle is equipped with an On Board Unit (OBU) and a Global Positioning System (GPS). The OBU is installed in the vehicles for transferring messages between the vehicles and RSU. The GPS receiver will provide position and a clock to the vehicle. Each region is divided into clusters. Each cluster has its own RSU. Each car has an Identification number I_N representing its identity.

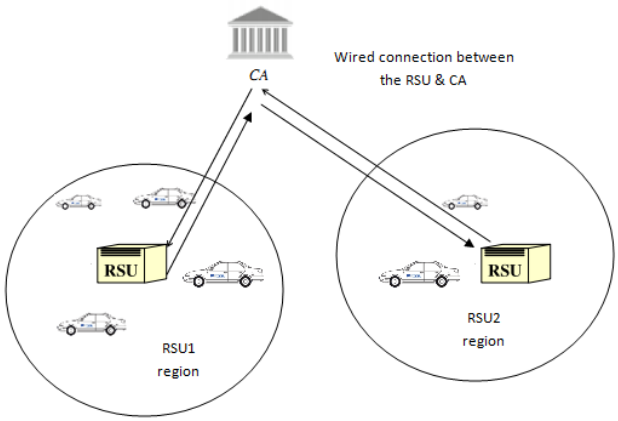

Fig.1. The Network Structure of the Proposed System

B. Security Protocol Model

A new and simple protocol is applied between the vehicles and the corresponding RSU that exists in their region. SKBPS protocol requires time synchronization between the vehicle and the RSU. The system is composed of six main phases:

1. Registration phase: when a vehicle j demands the service, the CA generates a random number Rj to this vehicle. The vehicle's owner generates public and private keys.
2. In order to eliminate the brute force attack, the vehicle's identification number IN is concatenated with Rj and hashed using a certain hash function; Sj= H(IN|| Rj). Then, the public key of the vehicle j Kvj, Sj and Rj are stored in the database of the CA. At the end of this phase the vehicle's owner will have a smart card which contains Rj, Sj, Kvj and Kvj-1. Sj is the secret number of each vehicle; it will be used to check the authenticity of the vehicle in the authentication phase.
3. Login phase: when the vehicle enters a new RSU region, it sends through a secure channel its secret number Sj, and its public key signed by its secret key then

encrypted by the public key of the RSU Kr (Kr is obtained from a periodical broadcast sent by the RSU). This is shown in Fig.2.

4. Authentication phase: when the RSU receives the login message from a new vehicle, the RSU checks from the CA the authenticity of this vehicle. The CA uses its database to compare the stored Kvj and Sj with the sent Kvj and Sj. If this holds, the CA informs the RSU that this vehicle is registered and the CA sends to the RSU the public key of this vehicle Kvj. The RSU stores the time of the first received vehicle's message Tj0, and makes the following three steps.

First step: the RSU checks if the vehicle is a new one by comparing the vehicle's Kvj with the stored Kvj's in its database. If this holds, the RSU gives the vehicle a number j, and goes to the second step.

Second step: the RSU calculates the vehicle's initial key Kj0; where Kj0= H(Rj||Tj0). Kj0 is used as an initial key for the first T period of this vehicle.

Third step: the RSU sends Tj0, the group key KG and the vehicle's number j encrypted by the vehicle's public key Kvj and signed using the private key of the RSU Kr-1. This is shown in Fig.2.

The RSU can calculate a new Kj1 after a specific time period T using the one-way function F: Kj1 = F(Kj0). The remainder of the chain is computed recursively using Kj(i+1) = F(Kji). Note that this gives us Kji = FN−i(KjN), so we can compute any value in the key chain from Kj0 even if we do not have an intermediate values. Each key Kji will be active for certain period then expired. This last step is used to prevent replay attack. The RSU stores for each vehicle: the vehicle number j, the initial time when the vehicle joins the RSU's region Tj0, the initial key Kj0, and the vehicle's secret number Sj. The steps of the SKBPS protocol are presented in Fig.2. Because of the high mobility of the vehicles, sometimes a vehicle can leave from the area served by an RSU to another area served by another RSU. So every RSU periodically broadcasts its public key. A unique region group key KG is used for each region.

5. Message Exchange Phase: when a vehicle sends a message to the RSU the message will be encrypted by the symmetric key Kji of this period of time Tji. Also, the vehicle appends its number j with each message. The RSU uses the number j to determine the identity of the sender. The RSU decrypts the message with the corresponding key of this period of time. Then, the RSU sends the message encrypted with KG to the rest members in the same RSU region. The KG is known to all the vehicles in the same region.

6. Sign out Phase: when the vehicle detects that the RSU is changed, the vehicle can detect that from the change of the broadcasting public key. When a vehicle leaves one RSU region to another RSU region, it makes a sign out. The sign out message must contain the signature of the vehicle to preserve the non_repudiation property.

7. Revocation Phase: the revocation happens in two cases: the first case: when the CA detects a misbehaving node. The second case: when the vehicle stops the service. In both cases, the RSU must change the group key KG and sends the new one to the rest members in its region. In VANET the members in the RSU region change quickly. So the RSU can keep the old KG for certain time and give the new login vehicles the new KG. Also, the CA sends to other RSU's the Sj of the revoked vehicle. In case of detecting any misbehaving nodes, the KG must be updated. The keys used in our protocol are defined below:

1. Kr: the public key of the RSU. It is used when the vehicle sends the initial message; which contains its Sj.
2. Kr-1: it's the private key of the RSU. It is used for making a digital signature when the RSU distributes the new group key. It's used also in the authentication phase to help the vehicle authenticate the RSU.
3. KG: the group key used for sending messages between the RSU and all group members in its region.
4. Kji: the symmetric key of vehicle j. It's used to send messages between the vehicle number j (nodej) and the RSU in its region through the time period i.
5. Kvj: the public key of the vehicle j. it's used in the login phase.
6. Kvj-1: the private key of the vehicle j. it's used in the login phase.

According to Wang et al analysis [1], the AES (Advanced Encryption Standard) is the most suitable choice for VANETs. They make a simulation in NIST (National Institute of Standards and Technology, USA) on two PCs. They select PCs which have certain capabilities comparable to the VANET system. The result of this experiment shows that the AES is more suitable for VANET than both DES and 3DES.

C. The Packet Format

Once the vehicle has an initial key Kj0, it begins the communication with the RSU. The vehicle sends packet which contains the following:

1. The message encrypted by Kji: (m)Kji.
2. The number of the vehicle: j.

Also, The RSU is responsible of making an update to KG after certain time period, and distributes the new group key to the current members in the region.

D. Measurement of the Level of Trustiness

CA can divide the vehicles in each RSU region into three levels of trustiness according to the level of trust on this vehicle. This level is determined according to the following procedures:

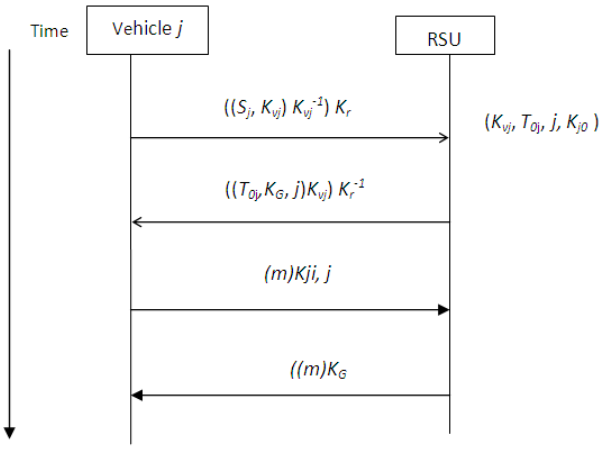

Fig.2. The Proposed SKBPS Protocol

1. The RSU builds a database which contains each node secret number S_j, the vehicle number j, the vehicle's random number R_j, the vehicle's initial time T_{j0}.
2. The RSU stores some received packets from the nodes at different time periods T_{ji}.
   The RSU calculates the expected K_{ji} for the selected time periods T_{ji}; $K_{j(i+1)} = F(K_{ji})$.
3. The RSU can from steps 2 and 3 restores the sent messages in this time periods, and determine if these messages are reasonable or not.
4. When the RSU completes the previous three steps, it will have a list that contains three different classifications for the vehicles in its region. Each RSU sends this list to the CA.

The CA can classify the vehicles into three levels:

1. Level 1: trusted vehicles.
2. Level 2: undetermined vehicle.
3. Level 3: entrusted vehicles.

The vehicles in level3 will be revoked. The vehicles in level1 can be used for distributing messages from the RSU to other nodes. This way is considered a simple way to revoke members than sending a revocation list. The revocation method proposed in IEEE P1609.2/D2 [2] is based on the distribution of CRLs (Certificate Revocation Lists) that contains the most recently revoked certificates. There are several drawbacks in this approach. The first drawback is that CRLs can be very long due to the huge number of vehicles and their high mobility (meaning that a vehicle can encounter a high number of vehicles when traveling, especially over long distances). Second, the short lifetime of certificates still creates a vulnerability window. Also, the infrastructure will not be available, especially in the first years of use [9]. The CA informs other RSU's about the malicious vehicles.

So the proposed system can catch the malicious vehicles, even if they are members in the group.

E. Security Parameters

Some parameters are the main reasons for the robustness of our system:

1. Each vehicle can't take many initial key numbers, because the initial key is given after checking the identity of the vehicle $H(I_N || R_j)$, which is a unique number; which prevents the Sybil attack. A more classification of each type of attack and the proposed solutions are given in Table 1.
2. When the vehicle leaves the RSU region to a new one (the vehicle remarks that from the new RSU's public key), it logs out and the RSU deletes the vehicle's information from the database. Thus, if the vehicle enters the region again, it will not appear as a malicious one.
3. In each specific time period Tji, Kji is changed, and the old Kji is expired, which prevent replay attack.
4. Protection against RSU Compromise: the compromised RSU can broadcast their public key but it can't build a connection with the participating vehicles. The compromised RSU can't get the secret numbers Sj of the vehicles or the random numbers Rj, which is necessary for computing the keys used for data exchange. In the following section, an analysis of SKBPS protocol is presented.

Table 1: Description of a number of attacks and their solutions in our scheme

Attack	**Description**	**Solution**
DOS attack	This attack means prevention of the network services by jamming for example.	The solution is based on using an OBU that is installed in vehicles. In case of DOS attack the OBU will switch the channel, or change the frequency, or make any suitable solution.
Brute force attack	In this type of attack, the attacker operates through all possible vehicle's identification numbers (I_N) in order to determine the identity of a vehicle.	Using a credit number for each vehicle concatenated with large and random number, then hashed using any suitable hash algorithm.
Replay attack	This attack happens when the attacker resent the previously sent messages.	This attack becomes impossible, because there's a different key for each time period.
Sybil attack	This attack means that a vehicle appears as a several vehicles either at the same time or in succession. It refers as an attack where the vehicle's identity masquerades as multiple simultaneous identities.	To prevent this attack, past keys don't be used. Keys are refreshed after certain time period.
Traffic analysis Attack	The attacker compromises certain parts of the VANET to match a message sender with the recipient. For example: The attacker uses the packet which contains location of vehicle ID.	The scheme is resilient to masquerading, because each vehicle has its own secret keys (K_{ji}'s), and each K_{ji} expired after its time period T_{ji} terminates.
Malicious vehicle	This attack occurs when a malicious vehicle can easily change its identity to another vehicle without punished.	The two secret parameters I_N, T_{0j} for each new vehicles prevents this type of attack.
False injection from outsider attacker	This attack is one of the major security threats. An outsider attacker injects false messages.	SKBPS protocol uses a group key K_G for the group members only which prevents this type of attack.

False injection from intsider attacker	This attack is like the previous attack but happens from one of the group members.	SKBPS makes an analysis for the sent messages randomly. The analysis checks the message in this period was reasonable or not. The misbehaving nodes are detected and classified as level 3 as declared in Section 3.4
Illusion attack	Is a new security threat in VANET; where the adversary intentionally deceives sensors on her/his own vehicle to produce wrong sensor readings [7].	Our system doesn't provide security against this type of attack.

IV. VERIFICATION OF SKBPS PROTOCOL

The analysis of SKBPS proposed protocol is carried out using two tools of verification. The first selected one is Burrows, Abadi; and Needham (BAN) logic [10], and the second selected one is Strand Spaces [11]. BAN is more suitable for verification of authentication. It allows the assumptions and goals of a protocol to be stated abstractly in belief logic. On the other hand, Strand spaces are more suitable for checking many types of attacks; like: data desynchronization attack.

A. Verification of the System by BAN logic

BAN logic is a set of rules for defining and analyzing information exchange protocols. Specifically, BAN logic helps its users determine whether exchanged information is trustworthy, secured against eavesdropping, or both. For a successful verification of the protocol, the belief state of communicating parties should satisfy the protocol goals. The goal of SKBPS is that the node and the RSU believe that they share a common secret K_{j0} and also each participant should believe that the other participant also believes in the same key. Therefore, we will consider the authentication is completed between the RSU (*B*) and vehicle (*A*) if there is a data packet "*X*" which the receiver *B* believes that it is sent by the sender *A*. Thus authentication between *A* and *B* will be completed if: $B \mid\equiv A \mid\equiv S_j$ and $B \mid\equiv S_j$. The basic rules of BAN logic are:

- The interpretation rule
$$\frac{P \mid\equiv (Q \mid\sim (X,Y))}{P \mid\equiv (Q \mid\sim X), P \mid\equiv (Q \mid\sim Y)}$$
- Message Meaning Rule
$$\frac{P \equiv P \xleftrightarrow{K} Q, P \lhd [X]_K}{P \mid\equiv Q \mid\sim X}, P \neq Q$$
- Nonce Verification Rule
$$\frac{P \mid\equiv \#(X), P \mid\equiv Q \sim X}{P \mid\equiv Q \mid\equiv X}$$
- Jurisdiction Rule
$$\frac{P \mid\equiv Q \Rightarrow X, P \mid\equiv Q \mid\equiv X}{P \mid\equiv X}$$
- Freshness Rule
$$\frac{P \mid\equiv \#(X)}{P \mid\equiv \#(X,Y)}$$
- Synthetic Rule
$$P \mid\equiv (Q \mid\sim X) \rightarrow P \mid\equiv (Q \mid\sim (X,Y))$$

We can represent the operation of authentication of the protocol by the following formula:

$$A \rightarrow B: \{((S_j, K_{vj}) K_{vj}^{-1}) K_r\} \quad (1)$$

Where:
A: vehicle *j*.
B: Road Side Unit.
K_r: public key of *B*.
K_{vj}: public key of vehicle *j* (node *A*).
K_{vj}^{-1}: private key of vehicle *j*.
S_j: indicates the secret number.

Thus authentication between *A* and *B* will be completed if: $B \mid\equiv A \mid\equiv S_j$ and $B \mid\equiv S_j$; where the symbol $\mid\equiv$ means believes. Now, we transform the message sent from the vehicle to the RSU as the following:

$$A \rightarrow B: \{((S_j, \#K_{vj})_{K_{vj}^{-1}})_{K_r}\} \quad (2)$$

The initial assumptions are given by:

$$A \mid\equiv \xrightarrow{K_r} B \quad (3)$$

$$B \mid\equiv \xrightarrow{K_r} B \quad (4)$$

$$A \mid\equiv \xrightarrow{K_{vj}} A \quad (5)$$

$$B \mid\equiv \xrightarrow{K_{vj}} A \quad (6)$$

$$B \mid\equiv A \mid\Longrightarrow K_{vj} \quad (7)$$

$$B \mid\equiv \#K_{vj} \quad (8)$$

- Equation (3) indicates that *A* believes that K_r is the public key of *B*.
- Equation (4) indicates that *B* believes that K_r is the public key of *B*.
- Equation (5) indicates that *A* believes that K_{vj} is the public key of *A*.
- Equation (6) indicates that *B* believes that K_{vj} is the public key of *A*.
- Equation (7) indicates that *B* believes that *A* has jurisdiction over K_{vj}.
- Equation (8) indicates that *B* believes that K_{vj} is fresh. It means that K_{vj} is belonging to a new vehicle which does not exist in the data base of the RSU.

Using Equations (3) and (2), and by applying the message meaning rule, we obtain:

$$B \mid\equiv A \mid\sim (S_j, K_{vj})_{K_{vj}^{-1}} \quad (8)$$

From Equations (8) and (6) and by applying the message meaning rule we obtain:

$$B \mid\equiv A \mid\sim (S_j, K_{vj}) \quad (9)$$

International Journal of Electronics Communication and Computer Engineering
Volume 5, Issue 6, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

From Equations (9) and (8), and by applying the freshness rule, we obtain:

$$B \mid\equiv \mathrm{A} \mid\sim \#(S_j, K_{vj}) \quad (10)$$

From Equations (9) and (10), and by applying the nonce-verification rule, we get:

$$B \mid\equiv \mathrm{A} \mid\equiv (S_j, K_{vj}) \quad (11)$$

From Equation (11) and by applying the Synthetic Rule, we obtain:

$$B \mid\equiv \mathrm{A} \mid\equiv S_j \quad (12)$$

From Equation (12) and by applying the Jurisdiction Rule, we get:

$$B \mid\equiv S_j \quad (13)$$

After authentication of the vehicle, the RSU sent to the vehicle a message contains the group key. The goals of this message are: $A \mid\equiv B \mid\equiv K_G$ and $A \mid\equiv K_G$. We can represent the message sent from the RSU to the vehicle as the following formula:

$$A \rightarrow B: \{((T_{j0}, K_G, j)K_{vj})K_r^{-1}\} \quad (14)$$

Now, we transform the message sent from the RSU to the vehicle as the following:

$$B \rightarrow A: \{((\#T_{j0}, K_G, j)_{K_{vj}})_{K_r^{-1}}\} \quad (15)$$

We need to add the following assumptions:

$$A \mid\equiv \mathrm{B} \mid\Rightarrow \mathrm{K_G} \quad (16)$$

$$A \mid\equiv \#\mathrm{T_{j0}} \quad (17)$$

Equation (16) indicates that *A* believes that *B* has jurisdiction over K_G.

- Equation (17) indicates that *B* believes that T_{j0} is fresh.

Using Equations (14) and (3), and by applying the message meaning rule, we obtain:

$$A \mid\equiv \mathrm{B} \mid\sim (T_{j0}, K_G, j)K_{vj} \quad (18)$$

Using Equations (18) and (5), and by applying the message meaning rule, we obtain:

$$A \mid\equiv \mathrm{B} \mid\sim (T_{j0}, K_G, j) \quad (19)$$

From Equations (19) and (17), and by applying the freshness rule, we obtain:

$$A \mid\equiv \mathrm{B} \mid\sim \#(T_{j0}, K_G, j) \quad (20)$$

From Equations (19) and (20), and by applying the nonce-verification rule, we get:

$$A \mid\equiv \mathrm{B} \mid\equiv (T_{j0}, K_G, j) \quad (21)$$

From Equation (21) and by applying the Synthetic Rule, we obtain:

$$A \mid\equiv \mathrm{B} \mid\equiv K_G \quad (22)$$

From Equation (22) and by applying the Jurisdiction Rule, we get:

$$A \mid\equiv K_G \quad (23)$$

From (12) & (13), and (22) & (23) we deduce that SKBPS is free from any bugs or redundancies, and it is free from any type of known attacks like: replay attacks, message modification, insertion, or deletion. In the next subsection, verification of the system by Strand Spaces is presented.

B. Verification of the System by Strand Spaces

Strand spaces proposed by Guttman et al in [11] is a mathematical technique for formal verification of security protocols. In strand spaces model, an execution of a protocol includes a set of actions. Send and receive actions are used to represent send message and receive message respectively. For simplicity, (send a) is denoted as (+a), and (receive a) is denoted as (–a). A strand is a sequence of transmission and reception events local to a particular run of a principal. If this principal is honest, it is a regular strand. If it is dishonest, it is a penetrator strand [12]. A bundle C is a causally well-founded collection of nodes and arrows of both kinds. In a bundle, when a strand receives a message *m*, there is a unique node transmitting *m* from which the message was immediately received. By contrast, when a strand transmits a message m, many strands (or none) may immediately receive m. the height of a strand in a bundle is the number of nodes on the strand that are in the bundle [13].

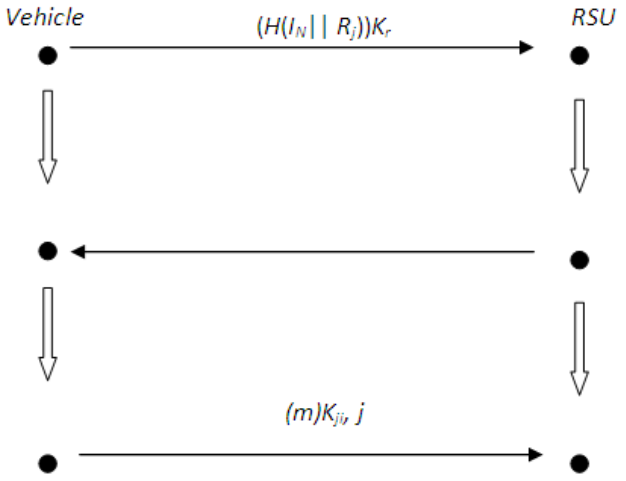

Fig.3. The bundle C_{SK} of the SKBPS Protocol

The penetrator can't destroy the synchronization of the *Kji* updating between the RSU and the vehicle. Both of the RSU and the vehicle refresh the key after a certain time period. As shown in Fig. 3, SKBPS has no data desynchronization attack. In the next section, comparison of SKBPS with other VANETs protocols is discussed.

V. COMPARISON OF SKBPS WITH CMAP, VIPER AND NENGET AL. PROTOCOLS

Although the presented scheme, SKBPS uses symmetric encryption function, the non-repudiation property is achieved. SKBPS satisfies non-repudiation by assigning a secret number S_j to each vehicle. Non-repudiation property is very important in VANET system. Drivers causing accidents should be reliably identified, which is available in our system. Some other schemes use public key cryptography to achieve this property. Public key encryption is based on mathematical functions, computationally intensive and is not very efficient for small mobile devices [14]. In SKBPS, each vehicle has its

own symmetric key K_{ji}. Although SKBPS needs two symmetric operations for each message (Each user sends its message to the RSU then the RSU resends it to the rest of the group members after making decryption using the user's key K_{ji}, and encryption with the group key K_G), it is considered more suitable in real time than making one asymmetric operations. Asymmetric encryption techniques are almost 1000 times slower than symmetric techniques, because they require more computational processing power [15]. There is no masquerading attack with satisfying privacy. We prevent the adversary to know the identities of all vehicles by encrypting the messages by the group key. Table 2 shows a comparison between our protocol with CAMP [8], VIPER and Neng et al. protocols. CMAP and VIPER use public key encryption function for message exchange, while Neng et al. protocol and SKPBS protocol use symmetric encryption function. Our proposed protocol assumes synchronization between the vehicle and the RSU. It's easy and available by the GPS system, which is part of our system. Also, the vehicle has more capabilities than other mobile systems, which can support this feature easily. SKBPS protocol has the following advantages over both CMAP and VIPER protocols:

- It has low computation overhead and low latency compared to these protocols, since it uses symmetric key encryption.
- Both CMAP and VIPER are susceptible to insider attack. Our protocol overcomes this attack as declared in Table.1
- SKBPS protocol has a simple revocation method. While in VIPER and CMAP, the revocation is not simple. In VIPER, the RSU periodically broadcasts a message containing the identities of the vehicles currently belonging to the group. In SKBPS, all message exchanges are through the RSU. Thus, any revoked message is ignored without sending to the rest of group members. CMAP protocol allows the vehicles to send accusation messages to the CA if a vehicle finds that other vehicles send false messages. This method may lead to Denial of Service attack by sending large number of false accusation messages.

In addition, SKBPS protocol, compared to Neng et al. protocol, overcomes the problem of insider attack and satisfies the vehicle's privacy. Since in Neng et al., each message must be signed. This leads to the easiness of tracing system's vehicles which threaten the vehicle's privacy.

Table 2: Comparison of SKBPS protocol with CMAP, VIPER and Neng et al. protocols

The Protocol	Method of Encryption	Possibility of Insider Attack	Detection of compromised RSU	Privacy	Revocation Process
CMAP	Public encryption	Yes	Yes	Satisfied.	By judging in the accusation messages
VIPER	Public encryption	Yes	Yes	Satisfied	Periodically broadcasts a message
Neng, et.al	Symmetric encryption	Possible	Yes	Didn't satisfy.	Simply, by cutting the channel
SKBPS	Symmetric encryption	Impossible	Yes	Satisfied	Simply, by cutting the channel

V. Conclusion

In this paper, we present a new protocol, which we named SKBPS protocol, for the security and privacy in vehicular ad hoc networks. The system should guarantee that life critical information cannot be modified by an attacker. Also, the privacy of the drivers and passengers is a highly important object. Preserving the authenticity of messages exchanged contradicts with maintaining the privacy of the vehicles. In the present paper, we propose a new protocol to satisfy these two goals: security and privacy. Our new protocol uses symmetric key encryption. The use of symmetric key encryption leads to low computation overhead and enhances the system's performance. For each new vehicle j, a new symmetric key kji is generated for each time period Tji. The system assumes time synchronization between the RSU and the vehicles, the system uses the GPS to satisfy this property.

The RSU uses another key KG to communicate with the rest of vehicles that exist in its region. The RSU measures the trustiness for each participating vehicle by certain analysis. This last analysis helps the RSU to decide whether to revoke the vehicle or not. SKBPS protocol is characterized by low communication and computation overheads to revoke the malicious vehicles. If the vehicle takes a high level of trustiness, it could be used for distributing data between vehicles which simplify the network. SKBPS protocol overcomes many types of attacks in VANET system. BAN logic is used to make a verification of the new system. The verification results show that it achieves its goals, free from redundancies and bugs. The mutual authentication is achieved between the RSU and the vehicle node. Also, it is analyzed using Strand Spaces model, the results shows that the new protocol isn't vulnerable to data desynchronization attacks.

References

[1] Neng-Wan.W, Yueh-Min.H, Wei-Ming C., "A Novel Secure Communication Scheme in Vehicular Ad Hoc Networks", Computer Communications, 31, 2008, pp.2827-2837.

[2] IEEE P1609.2/D2 – Draft Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Messages, November 2005.
[3] Suguo du, Xiaolong Li, Junbo Du, Haojin Zhu, "An attack-and defense game for security assessment in vehicular ad hoc networks", Peer-to-Peer Networking Applications, March 2012.
[4] YAN G., OLARIU S., WEIGLE M., 'Providing VANET security through active position detection', Comput. Commun., 2008, 31, (12), pp.2883-2897
[5] Paolo.C, Roberto.D, "A Mechanism to Enforce Privacy in Vehicle-to-Infrastructure Communication", Computer Communications, 31, 2008, pp.2790-2802.
[6] Langley C., Lucas R., FU H., "Key Management in Vehicular ad-hoc networks", IEEE int. Conf. on Electro/Information Technology, 2008, pp. 223-226.
[7] LO N., TSA H., "Illusion Attack on VANET Applications- A Message Plausibility Problem", IEEE Globecom Workshops, 2007, pp. 1-8.
[8] E. Ramya, "Distributed Key Management Techniques for Message Authentication in VANETs", ICCCE 2012, April 2012.
[9] Maxim R., Jean P., "Securing Vehicular Ad Hoc Networks", Journal of Computer Security, 15, 2007, pp.39-68.
[10] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication", ACM Transactions on Computer Systems , vol. 18, no. 1, pp. 18-36, Feb. 1990.
[11] Joshua Guttman and F. Javier Thayer Fabrega, "Authentication Tests", Proceedings of the 2000 IEEE Symposium on Security and Privacy, Oakland, CA, May 2000.
[12] Miaolei Deng, Weijun Zhu, "Desynchronization Attacks on RFID Security Protocols", Telkonika, vol.11, no.2, Feb 2013, pp.681-688.
[13] Joshua Guttman and F. Javier Thayer Fabrega, "*Authentication Tests and the Structure of Bundles*", Theoretical Computer Science, 2001.
[14] Diaa S., Hatem. M, Mohie M., "Performance Evaluation of Symmetric Encryption Algorithms", IJCSNS International Journal of Computer and Network Security, VOL.8 No.12, December 2008, pp.280-286.
[15] Ruangchaijatupon, P. Krishnamurthy, "Encryption and Power Consumption in Wireless LANs-N'', the Third IEEE Workshop on Wireless LANs, September 2001, Newton, Massachusetts, pp. 27-28.

AUTHOR'S PROFILE

Dr. Eng Reham Abdellatif Abouhogail graduated from Faculty of Engineering Ain Shams University, obtained MSc with a Master of Electronics and Communications from Cairo University, obtained Ph.D from Faculty of Engineering Ain Shams University. She is now an assistant professor in the National Institute for Standards, Giza, Egypt. She has 13 years of experience of research.

Her area of research includes VLSI Design, Network Security and Wireless Networks. She has published many research papers in International journals and conferences.

Dr. Heba K. Aslan is a Professor at the Electronics Research Institute, Cairo- Egypt. She received her B. Sc., M. Sc. And Ph. D. from Faculty of Engineering, cairo University in 1990, 1994 and 1998 respectively. Her research interests include: Key Distribution Protocols, Authentication Protocols, Logical Analysis of Protocols and Intrusion Detection Protocols.