IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 21, 2019, accepted October 9, 2019, date of publication October 11, 2019, date of current version October 24, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2946969

An Efficient and Secure Key Agreement Protocol for Sharing Emergency Events in VANET Systems

CHIN-LING CHEN[1,2,3], YUE-XUN CHEN[4], CHIN-FENG LEE[4], YONG-YUAN DENG[3], AND CHI-HUA CHEN[5], (Member, IEEE)

[1]School of Computer and Information Engineering, Xiamen University of Technology, Xiamen 361024, China
[2]School of Information Engineering, Changchun Sci-Tech University, Changchun 130022, China
[3]Department of Computer Science and Information Engineering, Chaoyang University of Technology, Taichung City 413, Taiwan
[4]Department of Information Management, Chaoyang University of Technology, Taichung City 413, Taiwan
[5]College of Mathematics and Computer Science, Fuzhou University, Fuzhou 350108, China

Corresponding author: Chi-Hua Chen (chihua0826@gmail.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61906043, Grant 61877010, Grant 11501114, and Grant 11901100, in part by the Fujian Natural Science Funds under Grant 2019J01243, and in part by Fuzhou University under Grant 510730/XRC-18075, Grant 510809/GXRC-19037, Grant 510649/XRC-18049, and Grant 510650/XRC-18050.

ABSTRACT With the recent rapid increase in the number of motor vehicles on roads, traffic accidents have increased, and emergency reporting processes have become essential. In this paper, a key agreement protocol for a real-time traffic sharing system is proposed for Vehicular Ad-Hoc Networks (VANETs), in which a broadcast center authenticates the legitimacy of a user when they report an emergency and issues a certificate of emergency to other users. This study uses a digital signatures mechanism, key agreement and authentication scheme to satisfy the security requirements for a VANET. Burrows-Abadi-Needham logic (BAN logic) is applied to prove that the proposed scheme achieves secure authentication. The proposed protocol ensures the privacy of the communication between fleets and provides a mechanism for immediate emergency reporting. The experiment results show that the proposed scheme is feasible and meets security requirements.

INDEX TERMS VANET, authentication, BAN logic, key agreement, signature.

I. INTRODUCTION

With the rapid development and popularization of motor vehicle transportation in various regions, people spend a significant amount of their time on such transportation, and traffic complexity is increasing due to the increased number of vehicles on the road. Mobile communication devices can be used to deal with this situation [1]. The continuously increasing number of motor vehicles has caused many problems, such as the increased likelihood of a series of traffic accidents [2]. The severity of such accidents depends on the situation. Traffic accidents usually occur very quickly, and the emergency response to the accident is very important [3]. Emergency response to traffic accidents is generally divided into three parts: rescuing injured people, traffic maintenance, and searching for on-site evidences. The treatment of injured people and maintenance of on-site traffic are both urgent matters and must be dealt with immediately [4]. Accordingly, it is indispensable to be able to relieve traffic by sharing information between vehicles and issuing relevant emergency information [5].

Due to the recent development of science and technology networks, people can communicate in a variety of environments [6]. The environment architecture of Vehicular Ad-Hoc Networks (VANETs) and their applications have, as a result, received a significant amount of interest from researchers [7]–[10]. In a VANET, vehicles can be organized into a communication network [11], in which vehicles can be regarded as a mobile communication facility capable of forwarding and obtaining messages in the VANET system. This technology allows vehicles to share traffic information directly with other vehicles, or to request and receive information from the broadcasting center through a Road Site Unit (RSU), thus being able to achieve the requirement of sharing instant road conditions based on the architecture [12], [13]. However, due to the fact that the vehicles are communicating in a high-speed environment, the unnecessary consumption of resources in communication leads to unnecessary waste, and related security requirements are also increasing [6]. Thus, this study proposes a secure authentication scheme to ensure

The associate editor coordinating the review of this manuscript and approving it for publication was Marco Martalo.

the security of information shared among vehicles, offering a secure vehicle-to-vehicle traffic sharing environment [14].

A number of recent studies have focused on VANETs. Lia et al. proposed a VANET scheme that achieved authentication and integrity but did not offer non-repudiation [15]. Chen et al. proposed a scheme that transferred information between vehicles, and required that each vehicle in the network be trustworthy [16]. Non-repudiation and message integrity are indispensable in preventing counterfeit emergency messages, Chim et al. also emphasized that vehicles should be able to verify whether a message is indeed sent and signed by another vehicle without being modified [17], thus preventing message tampering during transmission, and ensuring that received messages contain the original information [18]. Therefore, the integrity of the information must be guaranteed during the transmission process. Digital signatures can be used to achieve non-repudiation of information. VANETs can accommodate more complex calculations than mobile devices, but they often consume excessive resources. Therefore, the cost of inter-vehicle communication must be considered. Dhillon and Kalra achieved communication using lightweight technology and one-way hash function and exclusive-or to perform low-cost computations [19]. Moreover, in the light computation of Wu et al.'s method, timestamps can be used in messages, allowing receivers to check the validation of a timestamp to prevent replay attacks using old messages [20]. These technologies can also be applied to VANETs [21]–[23].

In order to reduce the computation cost and meet security requirements, this study focuses on the following issue. Users are divided into users who join a team, and general users. Users are able to share information with each other and report the information to the broadcasting center. However, the information between teams is usually complete and reliable. Therefore, it is important to ensure communication security and authentication certification among teams [24]. In addition, identity authentication, the protocol must guarantee immediate information transfer and negotiate a secure secret key for the team. The secret key is used for communication between teams to ensure that the source of the information is credible [25], [26]. To conclude, we list the cons and pros of the related works in Table 1.

The remainder of this paper is organized as follows. Literature reviews are described in Section II. The proposed method is described in Section III. Security analyses are conducted in Section IV. Finally, conclusions and future work are offered in Section V.

II. PRELIMINARY

This section describes and discusses the literature reviews of Burrows-Abadi-Needham logic (BAN logic), discrete logarithm problems, and security requirements.

A. BAN LOGIC

BAN logic proof was proposed by Burrows and Abadi in 1989 [27]. Authentication protocols are the basis of security in many distributed systems, and VANETs are no exception. In order to ensure the correctness of a proposed scheme, many studies offer the BAN logic model to prove that their authentication protocols are effective, using many logic symbols and formula rules in the proof process [28].

B. DISCRETE LOGARITHM PROBLEMS

The discrete logarithm problem states that, if Pisa based point on G, and if a generated point Q belongs to G, it is difficult to find k from $Q = kP$ [29].

C. SECURITY REQUIREMENTS

In this paper, a Certification Authority (CA) is a trusted third-party whose function is to distribute legitimate public-private key systems to all users. A Broadcasting Center (BC) integrates and verifies information from all users. For more urgent incidents, emergency credentials are issued to protect a user's legitimacy. However, a complete VANET must achieve the following requirements:

1) MUTUAL AUTHENTICATION

To ensure a secure communication processes between two parties, the object of communication is verified by the system, and its legality ensured. Thus, the scheme must offer identity authentication [9], [10], [13], [14], [16], [30].

2) NON-REPUDIATION

A VANET system must prevent the dissemination of altered or forged information by unauthorized parties. In order to ensure the reliability of the information transmitted, both parties must attach a private seal of a legitimate user as the basis for the information during the communication. At the same time, this also makes it impossible for a sender to deny that they had sent a message, achieving undeniable information [16], [24], [26], [33].

3) KEY AGREEMENT

To ensure the legitimacy of the communication object, a common session key must be established during the communication so as to prevent communication security forgery by a third party [16], [29], [31], [33].

4) CONFIDENTIALITY

Sensitive user information is vulnerable to interception during the communication process and can then be used to carry out illegal actions. Accordingly, the transmitted information must protect the privacy of the parties and ensure communication security between both parties [12], [16], [31]–[35].

5) INTEGRITY

Transmitted messages can also be forged or modified by a third party during transmission. If two parties cannot guarantee the integrity of their messages during communication, the messages sent to each other become meaningless. Thus, the proposed scheme must ensure that the received

TABLE 1. The comparison of security issue of the related vanet works.

Scheme	Cons issue (Insufficient)	Pros issue (Characteristic)
[15]	Ignore non-repudiation issue	Provide authentication and integrity
[16]	Vehicles communication needs to be trusted	Focus on mutual authentication and non-repudiation
[17-18]	Computational cost is heavy	Focus on whether message tamper
[19]	Ignore non- reputation, Integrity and Unforgeability issues	Use lightweight operations to solve known attacks
[20-22]	Ignore non- reputation, Integrity and Unforgeability issues	Use timestamp to prevent replay attacks
[24-26]	Computational cost is heavy	Solve the communication security and authentication among teams

information by both parties has not been tampered with [5], [6], [16], [30]–[33].

6) UNFORGEABILITY

Because of the frequent communication in a VANET, attackers may take the opportunity to intercept and forge messages, causing traffic chaos. It is also therefore crucial that sensitive information cannot be forged in the scheme [13], [24].

III. METHOD

The proposed scheme uses a vehicle network as the basic environmental framework. As shown in Figure 1, the environment is applied to a real-time traffic sharing system between fleets. The roles in the environment include CA, BC, RSU, User of Team, and general User. The structure of the proposed scheme is shown in Figure 1. The notations of this study are listed in Table 2.

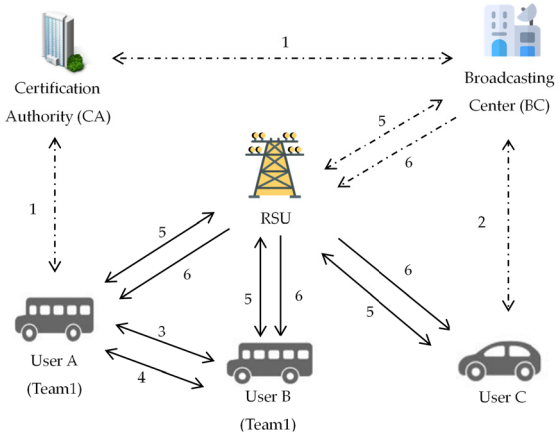


FIGURE 1. Structure of the proposed scheme.

A. CONSTRUCTION

Step 1: The CA distributes a public and private key to each user and BC via secure channel.
Step 2: Users register with BC via secure channel.
Step 3: Users generate a common session key between users in the same team.
Step 4: In the same team, users communicate using the negotiated session key.
Step 5: A user sends an emergency traffic event to the BC through the RSU, and the latter verifies the validity of the message. If it is legal, the BC issues an emergency certificate to the user.
Step 6: BC verifies the validity of the traffic event. If it is valid, BC broadcasts road conditions to all users through RSU.

B. INITIALIZATION PHASE

In order to issue the legality of public and private keys, the following processes must be followed in advance.

(1) CA distributes public and private keys to each user and BC.
(2) Users and BC share each other's public key.
(3) All users can report events to BC.
(4) A secure channel between RSU and BC.

C. REGISTRATION PHASE

In this phase, a user registers with BC and obtains the required parameters. The scenarios are shown in Figure 2.

Step 1: User generates r_i and sends (ID_U, r_i) to BC.
Step 2: After receiving the ID_U, BC generates n_i and makes a user's certificate as follows:

$$Cert_i = Sprk_{BC}(ID_{BC}, ID_U, n_i) \tag{1}$$

BC then stores $(ID_U, r_i, n_i, Cert_i)$ and sends $(ID_{BC}, ID_U, n_i, Cert_i)$ to the user.
Step 3: User uses the BC's public key to verify $Cert_i$:

$$Vpuk_{BC}(Cert_i) \stackrel{?}{=} (ID_{BC}, ID_U, n_i) \tag{2}$$

If it holds, user stores $(r_i, ID_{BC}, n_i, Cert_i)$.

D. KEY AGREEMENT PHASE

Identity authentication between User A and User B takes place in key agreement phase. Moreover, users must nego-

TABLE 2. Notations.

Notation	Description
ID_X	Identity of X
t_{Xi}	The i^{th} timestamps generated by X
r_X	The random number generated by X
r_i	The i^{th} random number generated by User
n_i	The i^{th} member number issued by BC
ΔT	The legal delay time interval
C_i	The i^{th} ciphertext
M_{Xi}	The i^{th} emergency message sent from X
$GF(p)$	The finite field
E	The elliptic curve defined on finite field $GF(p)$
G	*The generator point based on E*
R_X	*Large prime integer selected by X*
P_X	*R_X multiplied by G and based on E*
SK_{AB}	A session key of user A and user B
$ESK_{AB}(M)$	Encrypt message M by A and B's session key SK_{AB}
$DSK_{AB}(M)$	Decrypt message M by A and B's session key SK_{AB}
$Epuk_X(M)$	Encrypt message M by X's public key puk_X
$Dprk_X(M)$	Decrypt message M by X's private key prk_X
$Sprk_X(M)$	Sign message M by X's private key prk_X
$Vpuk_X(M)$	Verify message M by X's public key puk_X
Sig_X	A digital signature made by X
$Cert_i$	The i^{th} user's certificate which conforms to X.509 standard
$Cert_e$	The certificate of emergency issued by BC
$H()$	A hash function
$\oplus$	The exclusive-or computation
$A \stackrel{?}{=} B$	Verify if formula A is equal to formula B
------>	A secure channel
——>	An insecure channel

tiate the session keys between both parties. The session key generation between User A and User B is shown in Figure 3.

Step 1: User A generates r_A and chooses R_A, and then calculates P_A and makes a signature Sig_A:

$$P_A = R_A G \tag{3}$$

$$Sig_A = Sprk_A(ID_A, P_A, G, r_A), \tag{4}$$

calculates C_1

$$C_1 = Epuk_B(r_A) \tag{5}$$

and then sends $(C_1, Sig_A, ID_A, P_A, G)$ to User B.

Step 2: User B generates r_B and chooses R_B, then decrypts C_1:

$$r_A = Dprk_B(C_1) \tag{6}$$

and verifies Sig_A:

$$Vpuk_A(Sig_A) \stackrel{?}{=} (ID_A, P_A, G, r_A) \tag{7}$$

If it holds, User B generates P_B, C_2 and C_3:

$$P_B = R_B G \tag{8}$$

$$C_2 = r_B \oplus ID_B \oplus r_A \tag{9}$$

$$C_3 = H(ID_B, P_B, r_A, r_B), \tag{10}$$

then calculates SK_{AB} between User A and User B:

$$SK_{AB} = R_B P_A, \tag{11}$$

stores (ID_A, SK_{AB}), and sends (C_2, C_3, ID_B, P_B) to User A.

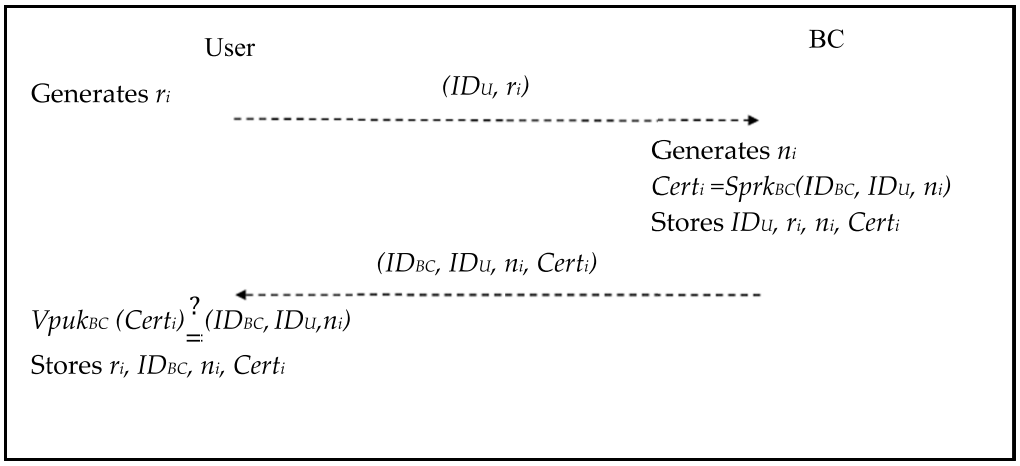


FIGURE 2. User registers with BC.

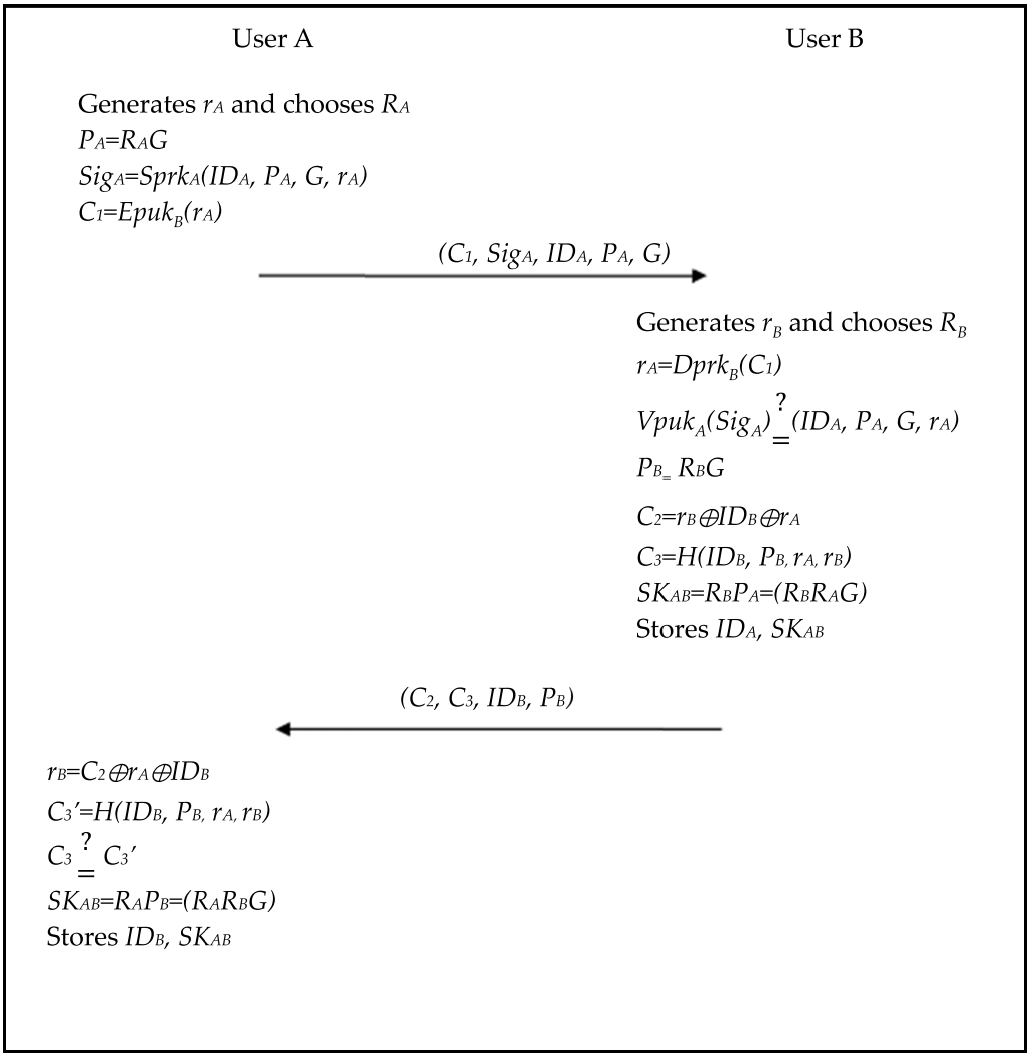


FIGURE 3. Generate the session key between User A and User B.

Step 3: User A decrypts C_2 by r_A and ID_B:

$$r_B = C_2 \oplus r_A \oplus ID_B, \tag{12}$$

calculates C_3':

$$C_3' = H(ID_B, P_B, r_A, r_B), \tag{13}$$

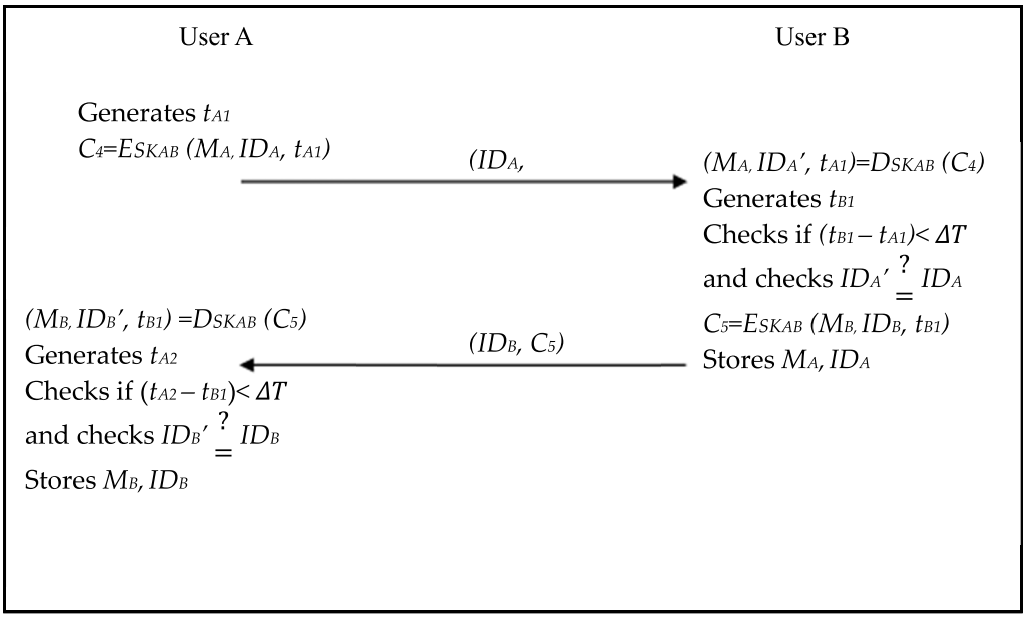


FIGURE 4. User A and user B sharing incidents in the same team.

and verifies C_3:

$$C_3 \stackrel{?}{=} C_3' \tag{14}$$

If it holds, User A calculates SK_{AB}:

$$SK_{AB} = R_A P_B, \tag{15}$$

and stores (ID_B, SK_{AB}).

E. THE SAME TEAM COMMUNICATION PHASE

In this phase, user A and user B are in the same team and communicate using the previously negotiated session key. Figure 4 shows User A and User B sharing incidents in the same team.

Step 1: User A generates t_{A1}, and uses session key SK_{AB} to generate C_4:

$$C_4 = ESK_{AB}(M_A, ID_A, t_A), \tag{16}$$

and then sends (ID_A, C_4, t_{A1}) to User B.

Step 2: User B find SK_{AB} by ID_A, and decrypts C_4 using SK_{AB}:

$$(M_A, ID_A', t_{A1}) = DSK_{AB}(C_4), \tag{17}$$

User B generates t_{B1} and verifies whether t_{A1} is within the legal time, checks if:

$$\text{If } (t_{B1} - t_{A1}) < \Delta T \tag{18}$$

and checks ID_A is true:

$$ID_A' \stackrel{?}{=} ID_A \tag{19}$$

If it is legal, User B receiving M_A, and encrypts C_5:

$$C_5 = ESK_{AB}(M_B, ID_B, t_{B1}), \tag{20}$$

stores (M_A, ID_A) and sends (ID_B, C_5) to User A.

Step 3: On receiving the message from User B, User A decrypts C_5:

$$(M_B, ID_B', t_{B1}) = DSK_{AB}(C_5) \tag{21}$$

User A generates t_{A2}, verifies if t_{B1} is within the legal time, checks if:

$$(t_{A2} - t_{B1}) < \Delta T \tag{22}$$

and checks ID_B is true:

$$ID_B' \stackrel{?}{=} ID_B \tag{23}$$

If it is legal, stores (M_B, ID_B)

F. COMMUNICATION PHASE BETWEEN USER AND BC

In this phase, the user sends emergency information to the BC via RSU. Once the BC confirms the message is legal, the emergency certificate is issued to the user. The user reports the incidents to BC as shown in Figure 5.

Step 1: User generates t_{U1} and makes a signature Sig_U as follows:

$$Sig_U = Sprk_U(ID_U, M_U, Cert_i) \tag{24}$$

The user then calculates C_6:

$$C_6 = H(n_i \oplus ID_U \oplus t_{U1}), \tag{25}$$

and sends $(t_{U1}, Sig_U, ID_U, M_U, C_6)$ to BC via RSU.

Step 2: BC uses ID_U to find n_i, r_i and $Cert_i$, calculates C_6':

$$C_6' = H(n_i \oplus ID_U \oplus t_{U1}), \tag{26}$$

then verifies C_6':

$$C_6' \stackrel{?}{=} C_6 \tag{27}$$

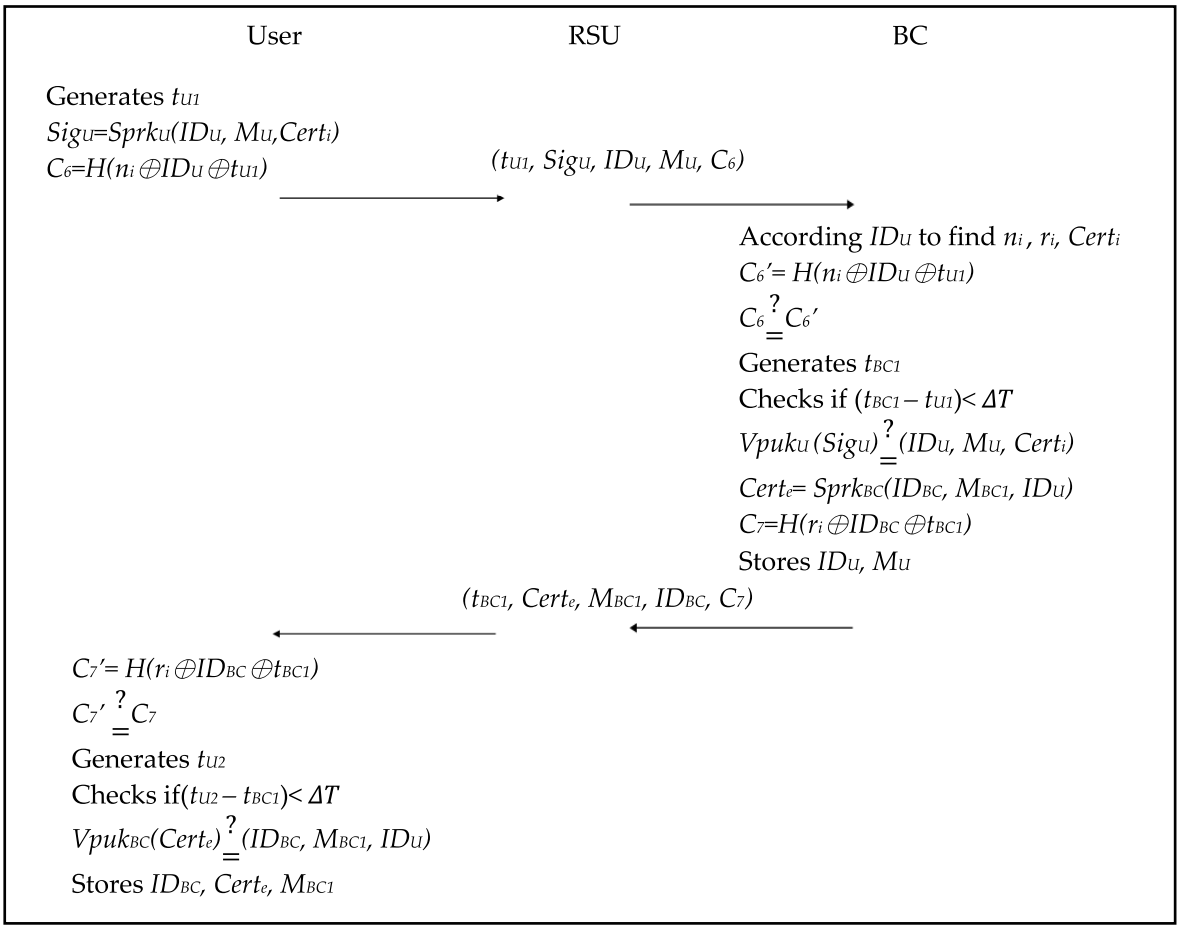


FIGURE 5. User reports an incident to the BC.

If it is true, BC generates t_{BC1} and verifies if t_{U1} is within the legal time or not by checking if:

$$(t_{BC1} - t_{U1}) < \Delta T \tag{28}$$

If it is legal, verifies Sig_U:

$$Vpuk_U(Sig_U) \stackrel{?}{=} (ID_U, M_U, Cert_i) \tag{29}$$

If it holds, BC makes a signature $Cert_e$:

$$Cert_e = Sprk_{BC}(ID_{BC}, M_{BC1}, ID_U) \tag{30}$$

and calculates:

$$C_7 = H(r_i \oplus ID_{BC}, t_{BC1}), \tag{31}$$

It then stores ID_U and M_U and sends (t_{BC1}, $Cert_e$, M_{BC1}, ID_{BC}, C_7) to the user via RSU.

Step 3: User calculates C_7':

$$C_7' = H(r_i \oplus ID_{BC}, t_{BC1}), \tag{32}$$

verifies C_7':

$$C_7 \stackrel{?}{=} C_7', \tag{33}$$

If it is true, user generates t_{U2} and verifies if t_{BC1} is within the legal time by checking if:

$$(t_{U2} - t_{BC1}) < \Delta T \tag{34}$$

If it is legal, verifies $Cert_e$:

$$Vpuk_{BC}(Cert_e) \stackrel{?}{=} (ID_{BC}, M_{BC1}ID_U) \tag{35}$$

If it holds, the user stores ID_{BC}, $Cert_e$ and M_{BC1}.

G. BROADCAST PHASE

The BC broadcasts the received emergency information to all users in this phase. The BC broadcasts real-time traffic information to all users, as shown in Figure 6.

Step 1: BC generates t_{BC} and makes a signature Sig_{BC}:

$$Sig_{BC} = Sprk_{BC}(M_{BC2}, ID_{BC}, t_{BC2}), \tag{36}$$

then sends (Sig_{BC}, M_{BC2}, ID_{BC}, t_{BC2}) to user via RSU.

Step 2: After receiving message from BC, the user then verifies Sig_{BC}:

$$Vpuk_{BC}(Sig_{BC}) \stackrel{?}{=} (M_{BC2}, ID_{BC}, t_{BC2}) \tag{37}$$

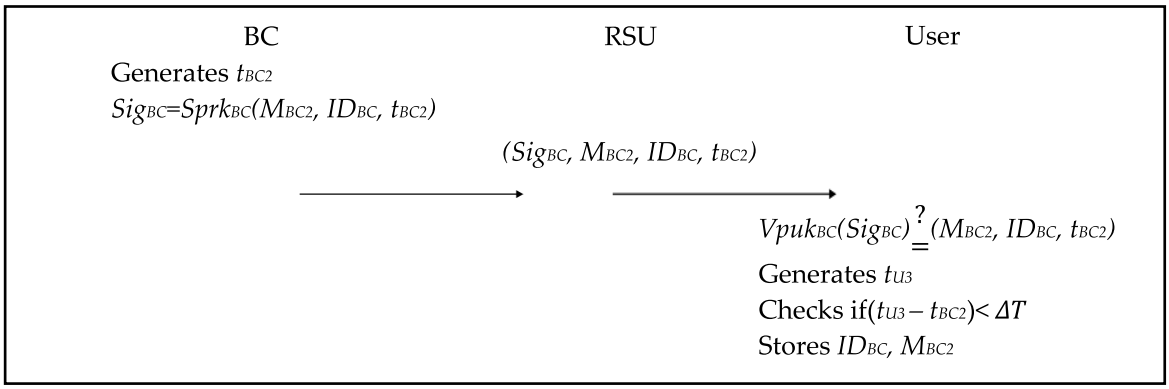


FIGURE 6. BC broadcasts real-time traffic information to all users.

If it holds, the user generates t_{U3} and verifies whether t_{BC2} is within the legal time by checking if:

$$(t_{U3} - t_{BC2}) < \Delta T \tag{38}$$

If it is legal, the user stores ID_{BC} and M_{BC2}.

IV. RESULTS AND DISCUSSIONS

A. RESULTS

1) MUTUAL AUTHENTICATION PROOF

The proposed scheme must be able to verify the legitimacy of both sender and receiver's identities. This study uses BAN logic to determine if both parties have achieved mutual authentication.

BAN logic notations and meanings are as follows.

- $P| \equiv X$: P believes formula X.
- $P \lhd X$: P sees formula X.
- $P| \sim X$: P once said formula X.
- $P| \Rightarrow X$: P may control formula X.
- $\#(X)$: The means that formula X is recent.
- $| \stackrel{Puk}{\longrightarrow} P$: P has a public key Pukcorresponding to a private key Prk.
- $P \stackrel{K}{\longleftrightarrow} Q$: P and Q may communicate by secret key K.
- $P \stackrel{S}{\Longleftrightarrow} Q$: The formula S is a secret known only to P and Q.
- $\{X\}_K$: The formula X encrypted by K.
- $\langle X \rangle_Y$: This represents X combined with formula Y.

Furthermore, the following are the main logical rules of the BAN logic process.

- *Seeing rule*: $\frac{P \lhd (X,Y)}{P \lhd X}$, $\frac{P| \equiv | \stackrel{K}{\longrightarrow} P, P \lhd \{X\}_K}{P \lhd X}$
- *Freshness rule*: $\frac{P| \equiv \#(X)}{P| \equiv \#(X,Y)}$

Message-meaning

- *rule*: $\frac{P| \equiv | \stackrel{K}{\longrightarrow} Q, P \lhd \{X\}_{K^{-1}}}{P| \equiv Q| \sim X}$, $\frac{P| \equiv P \stackrel{S}{\Longleftrightarrow} Q, P \lhd \langle X \rangle_S}{P| \equiv Q| \sim X}$
- *Nonce verification rule*: $\frac{P| \equiv Q| \Rightarrow X, P| \equiv Q| \sim X}{P| \equiv Q| \equiv X}$
- *Jurisdiction rule*: $\frac{P| \equiv Q| \Rightarrow X, P| \equiv Q| \equiv X}{P| \equiv X}$
- *Belief rule*: $\frac{P| \equiv (X,Y)}{P| \equiv X}$
- *Session key rule*: $\frac{P| \equiv \#(SK), P| \equiv Q| \equiv X}{P| \equiv P \stackrel{SK}{\longleftrightarrow} Q}$

The goal of this section is to authenticate the session key between users in the same team, and the goal of the formula should be reached as follows.

Goal 1. $A \mid \equiv A \stackrel{SK_{AB}}{\longleftrightarrow} B$
Goal 2. $A \mid \equiv B| \equiv A \stackrel{SK_{AB}}{\longleftrightarrow} B$
Goal 3. $B \mid \equiv A \stackrel{SK_{AB}}{\longleftrightarrow} B$
Goal 4. $B \mid \equiv A| \equiv A \stackrel{SK_{AB}}{\longleftrightarrow} B$
Goal 5. $A \mid \equiv ID_B$
Goal 6. $A \mid \equiv B| \equiv ID_B$
Goal 7. $B \mid \equiv ID_A$
Goal 8. $B \mid \equiv A| \equiv ID_A$

Notes: A: User A, B : User B

Idealize the protocol in the key agreement phase as follows.

$$Message\ 1\ \mathrm{A} \rightarrow \mathrm{B}(\{r_A\}_{Puk_B}, \{ID_A, P_A, G, r_A\}_{Prk_A})$$
$$Message\ 2\ \mathrm{B} \rightarrow \mathrm{B}(< ID_B, P_B, r_A, r_B >_{H(x)})$$

To analyze the proposed scheme, this study made the following assumptions.

A1 $A \mid \equiv \#(R_A)$
A2 $B| \equiv \#(R_B)$
A3 $B| \equiv | \stackrel{Puk_B}{\longrightarrow} B$
A4 $B| \equiv | \stackrel{Prk_A}{\longrightarrow} A$
A5 $A \mid \equiv \#(r_A)$
A6 $B| \equiv \#(r_A)$
A7 $B| \equiv \#(r_B)$
A8 $A| \equiv \#(r_B)$
A9 $A| \equiv A \stackrel{H(x)}{\Longleftrightarrow} B$
A10 $A| \equiv B| \Longrightarrow ID_B$
A11 $B| \equiv A| \Longrightarrow ID_A$

The proof of the proposed scheme is as follows.

(1) User B authenticates User A:
By *Message 1*, the following statement is obtained:

$$B \lhd (\{r_A\}_{Puk_B}, \{ID_A, P_A, G, r_A\}_{Prk_A}) \tag{S1}$$

By *(S1)*, *A3* and the *seeing rule*:

$$B \triangleleft (r_A, \{ID_A, P_A, G, r_A\}_{Prk_A}) \quad \text{(S2)}$$

Based on *(S2)*, and according to*A6* and the *freshness rule*:

$$B| \equiv \#(r_A, \{ID_A, P_A, G, r_A\}_{Prk_A}) \quad \text{(S3)}$$

By *(S2)*, *A4* and the *message-meaning rule*:

$$B| \equiv A| \sim (ID_A, P_A, G, r_A) \quad \text{(S4)}$$

By *(S3)*, *(S4)* and the *nonceverification rule*:

$$B| \equiv A| \equiv (ID_A, P_A, G, r_A) \quad \text{(S5)}$$

Based on *(S5)* and the *belief rule*:

$$B| \equiv A| \equiv ID_A(Goal\ 8) \quad \text{(S6)}$$

By *(S6)*, *A11* and the *jurisdiction rule*, the following equation can be gotten.

$$B| \equiv ID_A(Goal\ 7) \quad \text{(S7)}$$

Due to *(S3)* and *A2*, when $SK_{AB} = R_B P_A$ is calculated this study derives:

$$B| \equiv \#(SK_{AB}) \quad \text{(S8)}$$

According to *(S5)*, *(S8)* and the *session key rule*:

$$B| \equiv A \overset{SK_{AB}}{\longleftrightarrow} B(Goal\ 3) \quad \text{(S9)}$$

With *(S9)*, and based on the Elliptic Curve algorithm, it can be ensured that B believes that A is bound to calculate the same result:

$$B| \equiv A| \equiv A \overset{SK_{AB}}{\longleftrightarrow} B(Goal\ 4) \quad \text{(S10)}$$

(2) User A authenticates User B:
By *Message 2*, the following statement is obtained:

$$A \triangleleft (< ID_B, P_B, r_A, r_B >_{H(x)}) \quad \text{(S11)}$$

By *A8* and the *freshness rule*:

$$A| \equiv \#(< ID_B, P_B, r_A, r_B >_{H(x)}) \quad \text{(S12)}$$

By *(S11)*, *A9* and the *message-meaning rule*:

$$A| \equiv B| \sim (< ID_B, P_B, r_A, r_B >_{H(x)}) \quad \text{(S13)}$$

By *(S12)*, *(S13)* and the *nonceverification rule*:

$$A| \equiv B| \equiv (ID_B, P_B, r_A, r_B) \quad \text{(S14)}$$

Based on *(S14)* and the *belief rule*:

$$A| \equiv B| \equiv ID_B(Goal\ 6) \quad \text{(S15)}$$

By *(S15)*, *A10* and the *jurisdiction rule*:

$$A| \equiv ID_B(Goal\ 5) \quad \text{(S16)}$$

Due to *(S12)* and *A1*, when $SK_{AB} = R_A P_B$ is calculated, the following is derived:

$$A| \equiv \#(SK_{AB}) \quad \text{(S17)}$$

According to *(S14)*, *(S17)* and the *session key rule*:

$$A| \equiv A \overset{SK_{AB}}{\longleftrightarrow} B(Goal\ 1) \quad \text{(S18)}$$

With *(S18)*, and based on the Elliptic Curve algorithm, it can be determined that A believes that B is bound to calculate the same result:

$$A| \equiv B| \equiv A \overset{SK_{AB}}{\longleftrightarrow} B(Goal\ 2) \quad \text{(S19)}$$

Based on the above results, when *(S6)* satisfies *Goal 8*, *(S7)* satisfies *Goal 7*, *(S9)* satisfies *Goal 3*, *(S10)* satisfies *Goal 4*, *(S15)* satisfies *Goal 6*, *(S16)* satisfies *Goal 5*, *(S18)* satisfies *Goal 1* and *(S19)*satisfies *Goal 2*, it can be determined with certainty that User A and User B believe SK_{AB} and the ID of both parties. Thus, the proposed scheme can establish a session key and achieve mutual authentication between User A and User B.

2) NON-REPUDIATION ANALYSIS

In the proposed scheme, the information flow is signed, and the receiver can verify if that the signature is true or not. The formula for providing a verifiable signature is shown in Table II. According to Table 3, the messages achieve non-repudiation in the proposed scheme.

3) KEY AGREEMENT ANALYSIS

In the proposed scheme, users in the same team verify each other's identities and generate a common session key $SK_{AB} = R_A R_B G$ as follows:

$$SK_{AB} = R_B P_A = R_B(R_A G)$$
$$SK_{AB} = R_A P_B = R_A(R_B G)$$

By above formulae, P_A, P_B and Gare in the insecure channel, and an attacker can intercept these parameters. However, R_A and R_B are generated by User A and User B respectively. Attackers cannot calculate SK_{AB} by using P_A, P_B and G. Neither party's private key discloses the shared key in the case of an external channel. Thus, the proposed scheme achieves key agreement.

4) CONFIDENTIALITY ANALYSIS

In the proposed scheme, sensitive messages n_i and r_i are protected using hash function and exclusive-or as follows:

$$C_6 = H(n_i \oplus ID_U \oplus t_{U1}) \quad (25)$$
$$C_7 = H(r_i \oplus ID_{BC} \oplus t_{BC1}) \quad (31)$$

Therefore, third parties cannot tamper with the transmitted information.

5) INTEGRITY ANALYSIS

In order to ensure the integrity of the message during the communication process, the proposed scheme uses a signature mechanism to ensure that messages are not tampered with:

$$Sig_u = Sprk_u(ID_u, M_u, Cert_i) \quad (24)$$
$$Sig_{BC} = Sprk_{BC}(M_{BC2}, ID_{BC}, t_{BC2}) \quad (36)$$

TABLE 3. The verifiable proofs of non-repudiation.

Evidence	Issuer	Holder	Verification
Sig_A=$Sprk_A(ID_A, P_A, G, r_A)$	User A	User B	$Vpuk_A(Sig_A) \stackrel{?}{=} (ID_A, P_A, G, r_A)$
Sig_U=$Sprk_U(ID_U, M_U, Cert_i)$	User	BC	$Vpuk_U(Sig_U) \stackrel{?}{=} (ID_U, M_U, Cert_i)$
$Cert_e$=$Sprk_{BC}(ID_{BC}, M_{BC1}, ID_U)$	BC	User	$Vpuk_{BC}(Cert_e) \stackrel{?}{=} (ID_{BC}, M_{BC1}, ID_U)$
Sig_{BC}=$Sprk_{BC}(M_{BC2}, ID_{BC})$	BC	User	$Vpuk_{BC}(Sig_{BC}) \stackrel{?}{=} (M_{BC2}, ID_{BC})$

Based on the above formulae, M_U and M_{BC2} are protected by signatures, therefore ensuring that the message meets the integrity requirements by verified signature.

6) UNFORGEABILITY ANALYSIS

In the communication phase, after the user reports the emergency, BC authenticates if the user is legitimate or not. If it is legal, BC can issue a certificate of emergency $Cert_e$ to the user. In order to make sure that $Cert_e$ is not tampered with, BC will make a signature by BC's private key.

$$Cert_e = Sprk_{BC}(ID_{BC}, M_{BC1}, ID_u) \tag{30}$$

In accordance with above formula, BC's private key is protected; it means that attacker cannot forge the BC's signature. The attacker cannot forge a legal certificate of emergency to disrupt communication.

7) KNOWN ATTACKS ANALYSIS

In recent years, Abbasinezhad-Mood et. al. [36], [37] proposed an adversarial model to solve the man-in-the-middle and known-key attacks. In our scheme, we involve other mechanisms such as timestamp, random number, public-key cryptography system, session key and hash function to protect messages. The following descriptions illustrate our scheme regarding how to defend the known attacks.

(1) Replay attack

In the proposed scheme, the user and the BC generate a timestamp in each phase and send the timestamp to the other party. After receiving the message, the other party will first verify whether the timestamp is legal or not. If it holds, it means that that timestamp is legal. Before verifying the time stamp, the following formulas are used to confirm that the timestamp has not been modified by any attacker:

$$C_4 = ESK_{AB}(M_A, ID_A, t_{A1}) \tag{16}$$
$$C_5 = ESK_{AB}(M_B, ID_B, t_{B1}) \tag{20}$$
$$C_6 = H(n_i \oplus ID_u \oplus t_{u1}) \tag{25}$$
$$C_7 = H(r_i \oplus ID_{BC} \oplus t_{BC1}) \tag{31}$$
$$Sig_{BC} = Sprk_{BC}(M_{BC2}, ID_{BC}, t_{BC2}) \tag{36}$$

And the following verifications are used to check if the message is legal:

$$\text{Checks if}(t_{B1} - t_{A1}) < \Delta T \tag{18}$$
$$\text{Checks if}(t_{A2} - t_{B1}) < \Delta T \tag{22}$$
$$\text{Checks if}(t_{BC1} - t_{u1}) < \Delta T \tag{28}$$
$$\text{Checks if}(t_{u2} - t_{BC1}) < \Delta T \tag{34}$$
$$\text{Checks if}(t_{u3} - t_{BC2}) < \Delta T \tag{38}$$

If an attacker resends old information, it will be verified at this stage. Thus, replay attacks can be effectively detected.

(2) Man-in-the-middle attack

An attacker may intercept messages during the transmission process and impersonate a user to send illegal messages. The proposed scheme uses the public-key cryptography system, session key and hash function to protect messages:

$$C_1 = Epuk_B(r_A) \tag{5}$$
$$C_2 = r_B \oplus ID_B \oplus r_A \tag{9}$$
$$C_3 = H(ID_B, P_B, r_A, r_B) \tag{10}$$
$$C_4 = ESK_{AB}(M_A, ID_A, t_A) \tag{16}$$
$$C_5 = ESK_{AB}(M_B, ID_B, t_{B1}) \tag{20}$$
$$C_6 = H(n_i \oplus ID_u \oplus t_{U1}) \tag{25}$$
$$C_7 = H(r_i \oplus ID_{BC} \oplus t_{BC1}) \tag{31}$$

According to the above formulae C_1, only User B can decrypt C_2 and C_3; r_A is important information of User A, but is all protected and only User B can access it. Thus, attackers cannot intercept r_A. C_4 and C_5 are encrypted by SK_{AB}. C_6 and C_7 contain n_i and r_i, respectively; n_i and r_i, can be obtained by users from the BC in the registration phase, as they belong to non-public parameters. Thus, when attackers execute a man-in-the-middle attack, they cannot correctly intercept important information.

(3) Impersonation attack

Attackers may impersonate legitimate users and uses legal resources during transmission. In order to prevent this attack, the proposed scheme uses a signature and

TABLE 4. Comparison of calculation cost.

Phase	Proposed scheme	Chen et al. [16]	Wang and Yao [3]
Key agreement phase	$T_{Enc}+T_{Dec}+T_{Sig}+T_{Ver}+2T_H+4T_{Xor}$	NA	NA
Communication phase of the same team	$4T_{SK}$	$2T_{Sig}+2T_{Ver}+2T_{Enc}+2T_{Dec}+4T_H$	NA
Communication phase between user and BC	$2T_{Sig}+2T_{Ver}+4T_H+4T_{Xor}$	$2T_{Sig}+2T_{Ver}+2T_{Enc}+2T_{Dec}+4T_H$	$3T_{Sig}+4T_{Ver}+2T_{Enc}+2T_{Dec}+3T_H$
Broadcast phase	$T_{Sig}+T_{Ver}$	NA	$T_{BSig}+T_{BVer}$

TABLE 5. Communication cost of the proposed scheme.

Phase	Communication cost	Transmission time	
		3.5G 14 Mbps (ms)	4G 100 Mbps (ms)
Key agreement phase	$T_E+T_{Sig}+3T_{Xor}+T_H$ =2368 bits	0.1613	0.0225
Communication phase of the same team	$2T_{SK}$=512 bits	0.0349	0.0049
Communication phase between user and BC	$2T_{Sig}+2T_H+4T_{Xor}$ =2688 bits	0.1831	0.0256
Broadcast phase	T_{Sig}=1024 bits	0.0698	0.0098

hash function to protect sensitive messages:

$$Sig_u = Sprk_u(ID_u, M_u, Cert_i) \quad (24)$$

$$C_6 = H(n_i \oplus ID_u \oplus t_{U1}) \quad (25)$$

$$Cert_e = Sprk_{BC}(ID_{BC}, M_{BC1}, ID_u) \quad (30)$$

$$C_7 = H(r_i \oplus ID_{BC} \oplus t_{BC1}) \quad (31)$$

$$Sig_{BC} = Sprk_{BC}(M_{BC2}, ID_{BC}, t_{BC2}) \quad (36)$$

Based on the above formulae, as Sig_U, $Cert_e$ and Sig_{BC} include the user identity and the important message, attackers cannot impersonate that identity and message in the signature. C_6 and C_7 are protected by hash function, and n_i and r_i are not disclosed in the insecure channel. Therefore, the proposed scheme is secure against impersonation attacks.

B. DISCUSSIONS

In this section, the calculation cost, security comparison and communication cost of the proposed scheme will be discussed. The comparison of calculation cost is given in Table 4, the communication cost of the proposed scheme is shown in Table 5. And the security comparison of the proposed scheme and related works are shown in Table 6.

Table 4 compares the calculation costs of the proposed scheme and that of Chen et al.'s scheme. In the commutation phase between user and BC, the signature and signature authentication operations are compared. Both parties incur the same cost for a digital signature. However, Chen's scheme needs two encryption operations, two decryption operations and four hash functions, so the cost is much higher than that of the four hash functions and four exclusive-or operations in the proposed scheme. Thus, the calculation cost of the proposed scheme is lower than that of Chen et al.'s scheme.

By the way, we explore the scheme of Wang and Yao [3]. They used the Bilinear Pairing, Public Key Infrastructure and Certificate mechanism to implement their system. Due to they use the Certificate based mechanism, they need not key agreement phase; but the public key issue and the certificate management still need to be conducted. In this article, they do not explore the issue of the V2V in the same team. To conclude, they use the Bilinear pairing-based mechanism has high cost especially in VANET environment.

Table 5 shows the time(ms) required to transmit all messages in 3.5G and 4G environments. The key agreement phase is taken as an example, which requires 0.1613 ms to transmit a message in 3.5G, and 0.0225 ms to transmit a message in 4G.

In Table 6, the security of the proposed scheme and previous schemes are analyzed. The results show that the proposed scheme is secure against most known attacks and meets security requirements not met by previous related schemes.

TABLE 6. Security comparisons of related works.

	Our scheme	Chen et al.[16]	Isaac et al. [31]	Remyakrishnan and Tripti [30]	Zhang et al. [32]	Li and Zhang [33]
Prevent replay attack	Yes	Yes	Yes	Yes	No	No
Prevent man-in-the-middle attack	Yes	Yes	NA	Yes	NA	Yes
Prevent impersonation attack	Yes	Yes	NA	NA	NA	Yes
Mutual authentication	Yes	Yes	Yes	No	Yes	Yes
Non-repudiation	Yes	Yes	No	No	Yes	Yes
Key agreement	Yes	Yes	Yes	Yes	No	Yes
Confidentiality	Yes	Yes	Yes	Yes	Yes	Yes
Integrity	Yes	Yes	No	Yes	Yes	Yes
Unforgeability	Yes	NA	NA	NA	NA	NA

V. CONCLUSION AND FUTURE WORK

The scheme proposed in this study is applicable to sharing traffic system of vehicle fleets and can serve as a real-time reporting system for users and traffic broadcast centers. An emergency reporting system is proposed, with a secret key applied between teams to ensure the security of messages shared between teams, and a signature mechanism is included to ensure the non-repudiation and integrity of messages in the communication processes. The proposed scheme is therefore secure against known malicious attacks, and offers mutual authentication, non-repudiation, key agreement, confidentiality, integrity and unforgeability.

Table III shows that the proposed scheme incurs lower computational cost than previous studies, and Table IV shows that the security of the proposed scheme is more complete than previous schemes. Ban logic is used to prove that the proposed scheme achieves secure mutual authentication.

Future work will create more services, for example E-commerce and value-added services, applying the improved security and privacy for VANETs offered by the proposed scheme to more environments.

REFERENCES

[1] C.-L. Chen, T.-M. Kuo, and T.-F. Shih, "Design of a secure communication and handoff protocol for VANETs," *J. High Speed Netw.*, vol. 20, no. 3, pp. 179–192, 2014.

[2] C. Zhang, X. Lin, R. Lu, P. H. Ho, and X. Shen, "An efficient message authentication scheme for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 57, no. 6, pp. 3357–3368, Nov. 2008.

[3] S. Wang and N. Yao, "LIAP: A local identity-based anonymous message authentication protocol in VANETs," *Comput. Commun.*, vol. 112, pp. 154–164, Nov. 2017.

[4] H. Hartenstein and L. P. Laberteaux, "A tutorial survey on vehicular ad hoc networks," *IEEE Commun. Mag.*, vol. 46, no. 6, pp. 164–171, Jun. 2008.

[5] G. Marfia, M. Roccetti, A. Amoroso, and G. Pau, "Safe driving in LA: Report from the greatest intervehicular accident detection test ever," *IEEE Trans. Veh. Technol.*, vol. 62, no. 2, pp. 522–535, Oct. 2013.

[6] J.-L. Huang, L.-Y. Yeh, and H.-Y. Chien, "ABAKA: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 60, no. 1, pp. 248–262, Oct. 2011.

[7] A. Benslimane, S. Barghi, and C. Assi, "An efficient routing protocol for connecting vehicular networks to the Internet," *Pervasive Mobile Comput.*, vol. 7, no. 1, pp. 98–113, 2011.

[8] S. Sharma and A. Kaul, "A survey on intrusion detection systems and honeypot based proactive security mechanisms in VANETs and VANET Cloud," *Veh. Commun.*, vol. 12, pp. 138–164, Apr. 2018.

[9] R. Muthumeenakshi, T. R. Reshmi, and K. Murugan, "Extended 3PAKE authentication scheme for value-added services in VANETs," *Comput. Elect. Eng.*, vol. 59, pp. 27–38, Apr. 2017.

[10] S. S. Manvi and S. Tangade, "A survey on authentication schemes in VANETs for secured communication," *Veh. Commun.*, vol. 9, pp. 19–30, Jul. 2017.

[11] X. Yang, L. Liu, N. H. Vaidya, and F. Zhao, "A vehicle-to-vehicle communication protocol for cooperative collision warning," in mobile and ubiquitous systems: Networking and services," in *Proc. 1st Annu. Int. Conf. Mobile Ubiquitous Syst., Netw. Services*, Boston, MA, USA, Aug. 2004, pp. 1–10.

[12] D. Tian, J. Zhou, Y. Wang, H. Xia, Z. Yi, and H. Liu, "Optimal epidemic broadcasting for vehicular ad hoc networks," *Int. J. Commun. Syst.*, vol. 27, no. 9, pp. 1220–1242, 2014.

[13] M. Wazid, A. K. Das, N. Kumar, V. Odelu, A. G. Reddy, K. Park, and Y. Park, "Design of lightweight authentication and key agreement protocol for vehicular ad hoc networks," *IEEE Access*, vol. 5, pp. 14966–14980, 2017.

[14] C.-C. Yang, Y.-L. Tang, R.-C. Wang, and H.-W. Yang, "A secure and efficient authentication protocol for anonymous channel in wireless communications," *Appl. Math. Comput.*, vol. 169, no. 2, pp. 1431–1439, 2005.

[15] C.-T. Li, M.-S. Hwang, and Y.-P. Chu, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks," *Comput. Commun.*, vol. 31, no. 12, pp. 2803–2814, 2008.

[16] C.-L. Chen, M.-L. Chiang, C.-C. Peng, C.-H. Chang, and Q.-R. Sui, "A secure mutual authentication scheme with non-repudiation for vehicular ad hoc networks," *Int. J. Commun. Syst.*, vol. 30, no. 6, p. e3081, 2017.

[17] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "SPECS: Secure and privacy enhancing communications schemes for VANETs," *Ad Hoc Netw.*, vol. 9, no. 2, pp. 189–203, 2011.

[18] C.-L. Chen, W.-C. Tsai, Y.-Y. Chen, and W.-J. Tsaur, "Using a stored-value card to provide an added-value service of payment protocol in VANET," *Inf. Technol. Control*, vol. 42, no. 4, pp. 362–372, 2013.

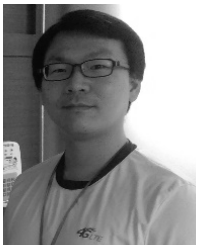
[19] P. K. Dhillon and S. Kalra, "A lightweight biometrics based remote user authentication scheme for IoT services," *J. Inf. Secur. Appl.*, vol. 34, pp. 255–270, Jun. 2017.
[20] F. Wu, X. Li, L. Xu, S. Kumari, M. Karuppiah, and J. Shen, "A lightweight and privacy-preserving mutual authentication scheme for wearable devices assisted by cloud server," *Comput. Elect. Eng.*, vol. 63, pp. 168–181, Oct. 2017.
[21] S. Bao, W. Hathal, H. Cruickshank, Z. Sun, P. Asuquo, and A. Lei, "A lightweight authentication and privacy-preserving scheme for VANETs using TESLA and Bloom filters," *ICT Express*, vol. 4, no. 4, pp. 221–227, Dec. 2018.
[22] J.-S. Cho, S.-S. Yeo, and S.-K. Kim, "Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value," *Comput. Commun.*, vol. 34, no. 3, pp. 391–397, 2011.
[23] Y. Tu and S. Piramuthu, "Lightweight non-distance-bounding means to address RFID relay attacks," *Decis. Support Syst.*, vol. 102, pp. 12–21, Oct. 2017.
[24] C. L. Chen and K. W. Cheng, "Design of a VANET privacy and non-repudiation accident reporting system," *Secur. Commun. Netw.*, vol. 9, no. 18, pp. 5187–5202, 2016.
[25] W. B. Jaballah, M. Conti, M. Mosbah, and C. E. Palazzi, "A secure alert messaging system for safe driving," *Comput. Commun.*, vol. 46, no. 15, pp. 29–42, 2014.
[26] J. Li, H. Lu, and M. Guizani, "ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 4, pp. 938–948, Apr. 2015.
[27] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, 1990.
[28] C.-L. Chen, Y.-Y. Deng, Y.-W. Tang, J.-H. Chen, and Y.-F. Lin, "An improvement on remote user authentication schemes using smart cards," *Computers*, vol. 7, no. 1, pp. 1–9, 2018.
[29] H. B. Yang, J. H. Chen, and Y. Y. Zhang, "A fresh two-party authentication key exchange protocol for mobile environment," in *Proc. Int. Conf. Ind. Technol. Manage. Sci.*, Tianjin, China, 2015, pp. 933–936.
[30] P. Remyakrishnan and C. Tripti, "A novel approach for enhancing the security of user authentication in VANET using biometrics," in *Proc. 49th Annu. Conv. Comput. Soc. India CSI Emerg. ICT Bridging Future*, Hyderabad, India, 2015, pp. 299–306.
[31] J. T. Isaac, S. Zeadally, and J. S. Cámara, "A lightweight secure mobile payment protocol for vehicular ad-hoc networks (VANETs)," *Electron. Commerce Res.*, vol. 12, no. 1, pp. 97–123, 2012.
[32] L. Zhang, Q. Wu, B. Qin, J. Domingo-Ferrer, and B. Liu, "Practical secure and privacy-preserving scheme for value-added applications in VANETs," *Comput. Commun.*, vol. 71, pp. 50–60, Nov. 2015.
[33] J. Li and L. Zhang, "Sender dynamic, non-repudiable, privacy-preserving and strong secure group communication protocol," *Inf. Sci.*, vol. 414, pp. 187–202, Nov. 2017.
[34] K. Gai, K.-K. R. Choo, M. Qiu, and L. Zhu, "Privacy-preserving content-oriented wireless communication in Internet-of-Things," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 3059–3067, Aug. 2018. doi: 10.1109/JIOT.2018.2830340.
[35] K. Gai, Y. Wu, L. Zhu, M. Qiu, and M. Shen, "Privacy-preserving energy trading using consortium blockchain in smart grid," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3548–3558, Jun. 2019. doi: 10.1109/TII.2019.2893433.
[36] D. Abbasinezhad-Mood, A. Ostad-Sharif, M. Nikooghadam, and S. M. Mazinani, "A secure and efficient key establishment scheme for communications of smart meters and service providers in smart grid," *IEEE Trans. Ind. Informat.*, to be published. doi: 10.1109/TII.2019.2927512.
[37] D. Abbasinezhad-Mood, A. Ostad-Sharif, and M. Nikooghadam, "Novel anonymous key establishment protocol for isolated smart meters," *IEEE Trans. Ind. Electron.*, to be published. doi: 10.1109/TIE.2019.2912789.

CHIN-LING CHEN received the Ph.D. degree from National Chung Hsing University, Taiwan, in 2005. From 1979 to 2005, he was a Senior Engineer with Chunghwa Telecom Company Ltd. He is currently a Professor. His research interests include cryptography, network security, and electronic commerce. He has published over 90 articles in SCI/SSCI international journals.

YUE-XUN CHEN received the B.S. and master's degrees in information management from the Chaoyang University of Technology, in 2017 and 2019, respectively. His research interests include computer security and network security.

CHIN-FENG LEE received the Ph.D. degree in computer science and information engineering from National Chung Cheng University, Taiwan. She is currently a Professor of information management with the Chaoyang University of Technology, Taichung, Taiwan. Her research interests include steganography, image processing, information retrieval, and data mining.

YONG-YUAN DENG received the Ph.D. degree with the Institute of Information Management, Chaoyang University of Technology, Taichung, Taiwan, in 2016, where he has been a Postdoctoral Researcher with the Institute of Information Engineering and Computer Science, since 2017. His research interests include cryptography, sensor networks, mobile commerce, and radio frequency identification systems.



CHI-HUA CHEN (M'07) received the Ph.D. degree from the Department of Information Management and Finance, National Chiao Tung University, in 2013. He currently serves as a Professor with the College of Mathematics and Computer Science, Fuzhou University, China. He has published over 270 journal articles, conference papers, and patents. His recent research interests are in the Internet of things, big data, deep learning, cellular networks, data mining, and intelligent transportation systems.