Blockchain-based Secure Ambulance-to-Everything Communications in Emergency Rescue Operations

Chakkaphong Suthaputchakun
School of Engineering
Bangkok University
Thailand
E-mail: chakkaphong.s@bu.ac.th

Yue Cao
School of Cyber Science and Engineering, Wuhan University
and Suzhou Research Institute of Wuhan University
China
E-mail: yue.cao@whu.edu.cn

***Abstract*— Rescue operations are extremely crucial and require high level of security both in terms of secure rescue operations and secure communications. Due to an emerging of vehicular communications, these communications can be utilized in rescue operations to provide smooth rescue routes. For example, an ambulance can communicate with traffic lights to turn a green light in advance before an arrival of the ambulance. However, security in such communications becomes an ultimate concern in this case. Even one forged communication could lead to a serious outcome during a rescue operation. For example, a vehicle may masquerade as an ambulance to gain a smooth route, while a real ambulance, on the other hand, could be blocked by such forged vehicle. To secure broadcast communications in vehicular networks, especially for rescue operations, Blockchain-based Secure Ambulance-to-Everything Communications or BSAX has been proposed in this paper. A priority-based certificate and Blockchain technology are proposed in BSAX to distinguish between certificates of ordinary vehicles and emergency vehicles, such as ambulances and firefighting buses. With these two technologies, vehicles could verify each emergency message and could securely as well as anonymously rebroadcast each message without compromising their privacy. This great achievement could securely enhance rescue missions and save many lives in the future.**

Keywords*— *Ambulance, Anonymous Vehicular Communications, Blockchain, Priority, Rescue Operation, Secure Vehicular Communications, Traffic Light

I. INTRODUCTION

Due to the higher number of vehicles and its tendency to increase every year, road traffic in many countries worldwide becomes more intensively congested. During rescue operations, one tiny delay could lead to a severe loss in terms of lives.

According to the statistics from US National Highway Traffic Safety Administration [1], in the past 20 years, there are 29 annual fatal crashes and 33 fatalities every year involving ambulances in US, which is illustrated in Figure 1. Such fatalities consist of 63% as occupants of normal vehicles, 12% as pedestrians, and 25% as occupants of ambulances, i.e. 4% as ambulance drivers and 21% as ambulance passengers. In summary, one-fourth of such fatalities are related to ambulances.

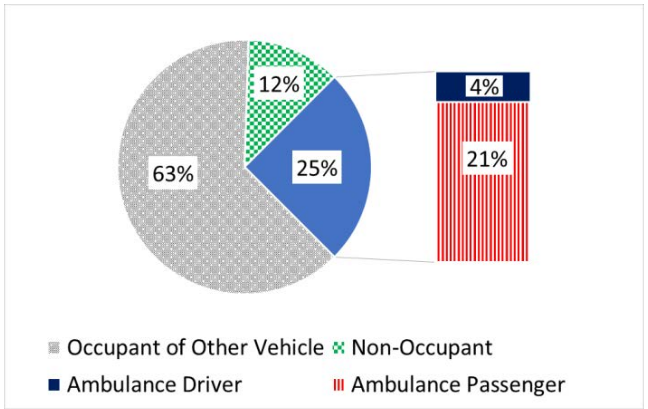


Fig. 1 Fatal Crashes in US in the Past 20 Years

Therefore, in [2, 3] ambulance-to-traffic light communications are proposed to manipulate traffic light schedules along rescue routes by allowing communications between ambulances and traffic lights. This communication makes sure that the traffic lights will turn on a green light to clear traffic at intersections in advance before the ambulances arrive, so that the ambulances can go through such intersections without stop or delay. As a result, the rescue operations become more responsive.

However, communication security is omitted in such protocols. It is noticed that rescue missions are considered very critical operations and require an extreme level of security. Communications without security become impractical in this case due to the fact that every vehicle can impersonate an ambulance to gain advantage in terms of a fast route and affect an authentic ambulance, who could get blocked in traffic by such masqueraded vehicle.

Therefore, in this paper, Blockchain-based Secure Ambulance-to-Everything Communications in Emergency Rescue Operations (BSAX) is proposed to utilizing Blockchain and priority-based certificate technologies to provide anonymous, secure, and prioritized broadcast communications between ambulances and everything along the rescue routes, including traffic lights and other vehicles. The major contributions of BSAX are summarized as follows;

978-1-6654-8550-0/22/$31.00 ©2022 IEEE

- BSAX allows secure broadcast communications from ambulances to traffic lights or Roadside Units (RSUs) via other vehicles as relays in a decentralized manner.
- BSAX supports anonymous communications through a distributed authentication using Blockchain concept.
- Priority-based certificate allows more critical or more urgent ambulances to go through intersections before other lower priority vehicles without revealing their true identities.

As a result, BSAX could provide security, privacy, efficiency, and robustness in the ambulance-to-everything communications. The organization of the paper is as follows. Section II summarizes security requirements and constraints in vehicular communication networks. The proposed BSAX is explained in Section III. Comprehensive discussion and analysis are conducted in Section IV. Finally, Section V provides a conclusion of the paper.

II. Literature Review: Security and Contraints in Vehicular Communication Networks

A. Unique Characteristics of Vehicular Communication Networks

It is very challenging to provide security in vehicular communication networks due to their unique characteristics [4, 5, 6, 7].

Number of Vehicles: The vehicular networks cover a variety of network densities. For example, in rural areas, networks normally are sparser than that in urban areas. During the rush hour, the higher number of vehicles and denser networks are expected.

Dynamic Topology: Apart from the diversity of the number of vehicles, members in the networks are also rapidly changed, i.e. joining and exiting the networks. This results in extremely dynamic network topologies.

Communication Constraints: One of key communications in vehicular networks is related to safety messaging, such as rescue-related information. There are several rigid constraints that the communications must achieve, such as time-sensitive message, high reliability, diverse message priorities, high level of security, and etc.

Therefore, these special characteristics make it very challenging to design a secure and anonymous communication protocol, especially during rescue missions.

B. Threats and Risks

In addition to the uniqueness of vehicular networks, the networks are also prone to several kinds of attacks as follows;

Jamming / Interference: Malicious vehicles could continuously send bogus messages to prevent other legitimate vehicles, including ambulances, from accessing the networks. Consequently, rescue missions could be delayed, interrupted, or blocked leading to higher number of loss of lives and serious injuries.

Message Forgery / Replay: Forged and replayed messages could be sent by any malicious vehicles to attain some benefits in terms of fast and smooth routes. However, this could make a direct impact to performance of rescue operations. For example, a traffic light could be misled by a forged or replayed message and block a rescue route requested by a legitimate ambulance.

Impersonation: By modifying and replaying messages, a malicious vehicle could impersonate an ambulance to gain advantages and potentially slow down an actual rescue mission.

Privacy: Due to nature of broadcast communications (one-to-all communications) a malicious vehicle could possibly keep tracking one particular vehicle. Therefore, privacy is the other serious concern not lesser than the security.

As a result, the designed broadcast communication protocol during rescue missions must be able to tackle all of these threats and risks.

C. Security Requirements

To achieve security in ambulance-to-everything communications, the following security aspects have to be achieved during communications.

Authentication: Only legitimate vehicles are allowed to join and send messages. To verify the vehicles, authentications become mandatory.

Message Integrity: Even though legitimate messages are sent by legitimate vehicles, the messages could be possibly altered or modified by other malicious vehicles. Thus, message integrity becomes a crucial security aspect in the ambulance-to-everything communications.

Non-repudiation: In case of law investigation, such as road accidents, all vehicles have to be responsible for all messages that they sent out. Non-repudiation, then, becomes one of the compulsory security aspects.

Message Freshness: To prevent any vehicles from replaying any stale or old messages aiming to gain illegal benefits, message freshness must be implemented. Message freshness is assuring only timely messages will be accepted in the ambulance-to-everything communications.

Anonymity: To protect all vehicles, including ambulances, from revealing their real identities, anonymity must be provided in parallel to the main communications. As a result, vehicles are still able to authenticate, while concealing their true identities from being tracked.

D. System Constraints

Generally, safety messaging in vehicular communication networks has very concrete constraints, since it could involve live, injury, and dead. Therefore, there are two main constraints needed to be taken into consideration as follows;

Time Constraint: Safety messages normally have short life time in milliseconds and require promptly transmissions. Therefore, security mechanisms added into ambulance-to-everything communications must not violate this time constraint.

Reliability Constraint: Every safety message in ambulance-to-everything communications is critical and need high reliability. One message loss may drastically affect performance of rescue operations.

These constraints, therefore, must be complied by all means in order to assure success in safety message transmissions.

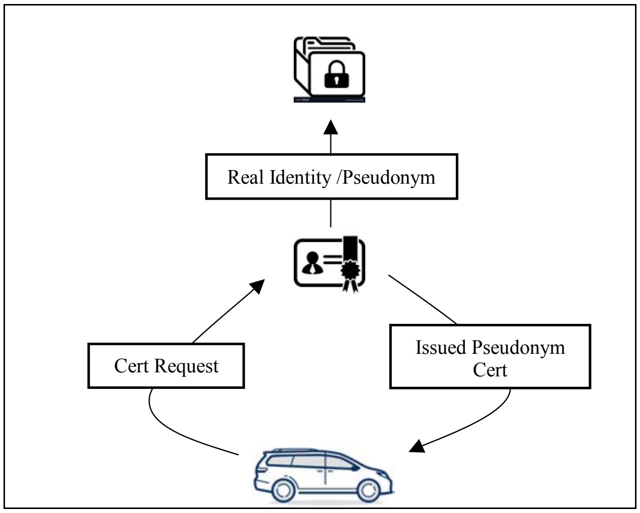


Fig. 2 Yearly Certificate Renewal

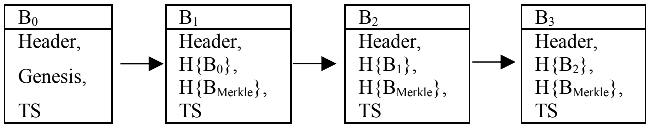
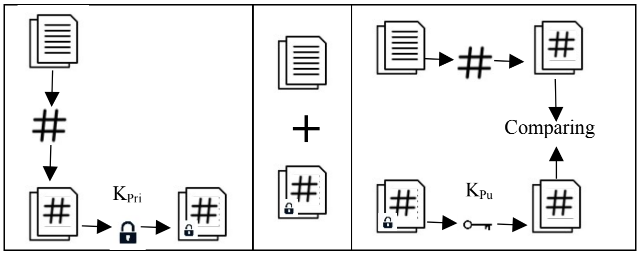


Fig. 3 Public Ledger in Blockchain



(a) Digital Signature Creation

(b) Sending Message

(c) Digital Signature Verification

Fig. 4 Digital Signature Creation and Verification

III. Blockchain-based Ambulance-to-Everything Communications

The proposed BSAX contributes to secure and anonymous multi-hop broadcast communications between any ambulances and other traffic lights along rescue routes in advance via relay vehicles. The proposed BSAX could work on top of many vehicular broadcast protocols in the literature, such as PATcom and A2T [2, 3]. Therefore, detail of broadcast communication concept, packet congestion control, and packet collision problems managed by the protocols in the literature is out of the scope of this paper. In addition, the paper make some assumptions as follows;

- A chain of priority-based Public Key Infrastructure (PKI) certificates is pre-issued by a trusted Certificate Authority (CA) and securely pre-loaded into a secure database, such as tamper-proof data storage, of all vehicles including ambulances during yearly checkup illustrated in Figure 2.
- Links between any certificates and real identities of vehicles are kept secretly and securely by a trusted CA shown in Figure 2. This links can only be revealed, when it is required for a law-related investigation.
- In order to achieve security in Blockchain, it is assumed that more than half of all parties, including ambulances, vehicles, traffic lights, and RSUs, are legitimate and are not compromised by any kinds of attacks.

A. Overview of Blockchain

Blockchain [8, 9, 10] is a linear link-list data structure that securely accumulates all transactions happened in a network in a chronological order. This linear list that holds all transaction records is called a public ledger. The ledger contains a hash value of its parent block, i.e. a predecessor block. A genesis or an original block is referred as the first block of each ledger, which has no parent block. A sample of a public ledger in Blockchain is demonstrated in Figure 3. Each block in a ledger normally consists of a block header, a hash value of a parent block, a hash value of all transactions in a network or a merkle tree, and finally a time stamp.

To securely store all transactions in a Blockchain ledger, asymmetric cryptography, i.e. a digital signature, is required in Blockchain. All members in a network have their own certificates, including pairs of a public key and a private key. Basically, a public key is known by everybody in the network, while a private key is known only by the owner. In order to create a digital signature, a message has to be hashed to make it smaller. Then, the hash value is signed or encrypted by using a private key. The result is called a digital signature. Therefore, the digital signature can be created by only the owner of such private key, i.e. no one else knows the private key. To verify a digital signature, the digital signature must be decrypted by using the public key, which is matched with the private key. Then, a hash of a message is compared with the result from the decryption. If both parts are identical, the digital signature is verified. The concept of digital signature and its verification is demonstrated in Figure 4. This digital signature and public ledger concept makes Blockchain secure and decentralized. Moreover, since the ledger accumulates all transactions in a network, all transactions are traceable. Therefore, Blockchain also provides an auditability aspect. Based on these secure, decentralized, and auditable abilities, Blockchain becomes one possible solution to provide secure ambulance-to-everything communications in vehicular networks, which is mostly decentralized and requires auditability in case of law investigations.

B. Overview of Priority-based PKI Certificate

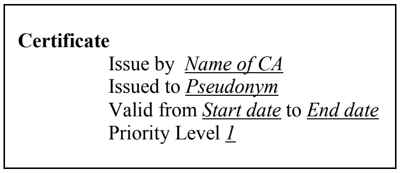
In this paper, three levels of priority are defined as follows;

The first priority (the highest priority) is defined and assigned to the most critical members in vehicular networks, which are emergency vehicles consisting of ambulances, firefighting buses, police cars, and etc.

The second priority is assigned to all road infrastructures, such as RSUs and traffic lights in order to gain lower priority in communications compared to the first priority, but still has higher priority than the last group.

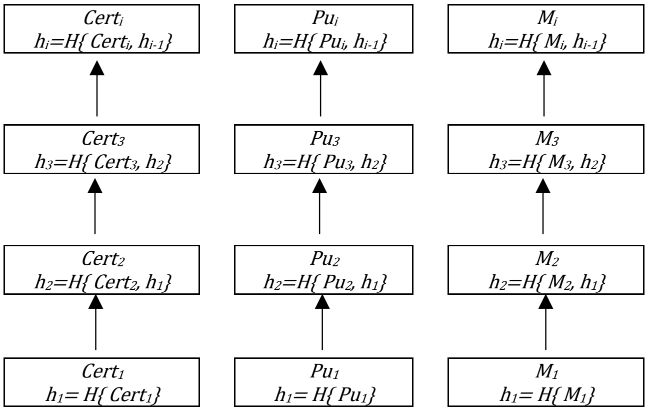
TABLE 1
SUMMARY OF DEFINED PRIORITY LEVELS

Priority	Entity	Samples
Pri(1)	Emergency Vehicles	Rescue related messages
Pri(2)	Road Infrastructures	Road and Traffic Warning message
Pri(3)	Normal Vehicles	Vehicle information message



Certificate
Issue by *Name of CA*
Issued to *Pseudonym*
Valid from *Start date* to *End date*
Priority Level *1*

Fig. 5 A Sample of Certificate



(a) CBC (b) RBC (c) MBC

Fig. 6 Certificate, Revoked Key, and Message Blockchains

The third priority, which is the lowest priority, is normally assigned to all other vehicles apart from the first two groups. Thus, vehicles in this group have lowest priority to access the communication channels.

The defined priority levels summarized in Table I are basically embedded in chains of PKI certificates, when they are issued by Certificate Authority (CA) during the yearly vehicle's maintenance. A sample of certificate is shown in Figure 5.

C. BSAX Ledgers

BSAX involves both vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. There are three key ledgers in BSAX, which are Certificate Blockchain, Revoked Key Blockchain, and Message Blockchain shown in Figure 6.

Certificate Blockchain (CBC): Certificate Blockchain or CBC is a public ledger accumulating all legitimated certificates ever used in the networks. It provides fast and efficient way to validate each received certificate, because the main validation operation is based on a hash function, which requires low computational resources.

Revoked Key Blockchain (RBC): Revoked Key Blockchain or RBC, on the other hand, is a public ledger accumulating all revoked keys used from the past to the present in the networks. This ledger is mainly used to disprove any revoked keys in the network.

Num	*Pri*	*Loc*	*SP*	*RoadID*	*LaneID*	*Dest*	*DMin*	*TTL*	*TS*

Fig. 7 WSM Format in BSAX

$A \rightarrow X$:
$$M_{Original} = WSM, \{H[WSM]\}_{Pr_A}, Cert_A$$

Fig. 8 Message Format Sent by Ambulance

Message Blockchain (MBC): MBC is the third public ledger accumulating all messages sent in the networks. This can be used for auditability in case of law-related investigation to track down each message and its creator.

D. BSAX Entities

In addition to three key ledgers in BSAX, there are the other three main paradigms in BSAX containing ambulances, normal vehicles, and traffic lights.

Ambulances: In rescue missions, ambulances are sources of WAVE Short Messages (WSMs). Messages are normally created by ambulances, which contains information as shown in Figure 7. The information consists of a sequence number of a message (Num), priority of a message (Pri), current location (Loc) and speed (SP) of an ambulance, current road (RoadID) and lane (LaneID) information, destination of a rescue operation (Dest), a relay distance (DMin), time to live of a message (TTL), and time stamp (TS). More detail of this WSM format can be seen in [3]. Only one modification has been made in this paper is by adding a time stamp (TS) into WSM messages to guarantee freshness and prevent a reply attack.

Each WSM message itself is for public, so there is no need to encrypt such message. Therefore, WSM can be sent in clear text shown as the first part of $M_{Original}$ in Figure 8. However, by broadcasting a message, other vehicles must assure that such message comes from a legitimate vehicle. Thus, the message must be anonymously signed by using a private key of an ambulance before being broadcasted shown in the second part of $M_{Original}$. The third part is an ambulance's certificate, which can be used to authenticate the ambulance. In addition, before accepting a message, vehicles will validate the received certificate and a public key embedded in the received message against CBC and RBC ledgers, respectively.

Normal Vehicles: A main role of normal vehicles in BSAX is to act as message relay entities. Since ambulances may not be in communication ranges of traffic lights, BSAX allows multi-hop broadcasting and uses vehicles on the road to relay messages to the target traffic lights. As long as the TTL value is still valid and the message has not reached the targeted destination, vehicles will relay such message to the next communication hop. Otherwise, the message will be discarded. A relayed message from a relay vehicle i (R_i) is shown in Figure 9. It is notice that WSM is still relayed in a clear text, since it is for a public use with an additional relay time stamp, TS_{R_i}. The second part of the message, M_{R_i}, on the other hand, is a digital signature of the relay vehicle R_i. This signature consists of a hash value of the signature of the original ambulance with a current relay time stamp, $H\{\{H[WSM]\}_{Pr_A},TS_{R_i}\}$, signed by a private key of R_i. The third and fourth parts of M_{R_i} are certificates of both the ambulance and the relay vehicle R_i.

$$\begin{gathered}Relay\ i \rightarrow X: \\ M_{R_i} = WSM, TS_{R_i}, \left\{H\left\{\{H[WSM]\}_{Pr_A}, TS_{R_i}\right\}\right\}_{Pr_{R_i}}, Cert_A, Cert_{R_i}\end{gathered}$$

Fig. 9 Message Format Replay by Vehicles

Basically, there are 2 cases of relaying messages.

1) Received Messages directly from Ambulances: Since the message may be sent for the first time (directly from an ambulance) shown in Figure 8, in this case, a vehicle firstly checks a validity of an ambulance's certificate and public key in the public ledgers CBC and RBC, respectively. If they are valid, the vehicle continue to verify an ambulance's digital signature by decrypting the signature, $\{H[WSM]\}_{Pr_A}$, using the validated ambulance public key, Pu_A, and comparing the result with a hash value of WSM, $\{H[WSM]\}$. The vehicle will relay the message to the next hop, only when both parts are perfectly matched. Otherwise, the message will be dropped. By relaying a message, a relay vehicle adds a relay time stamp, TS_{R_i}, into the message and creating a new signature by signing $H\{\{H[WSM]\}_{Pr_A}, TS_{R_i}\}$ with its own private key, Pr_{R_i}, as well as append the message with its certificate, $Cert_{R_i}$.

2) Received Messages from Relay Vehicles: In this case, the message is relayed by another relay vehicle shown in Figure 9. Firstly, the vehicle has to verity a digital signature of a relay vehicle by checking a validity of the relay vehicle's cerificate and its public key from both CBC and RBC as well as verifying the relay signature against a hash value of WSM and a relay time stamp, $H\{\{H[WSM]\}_{Pr_A}, TS_{R_i}\}$. If the digital signature of a relay vehicle is valid, a verification of the ambulance's signature must be additionally conducted as similar as in the first case. Only if both signatures are valid, the vehicle will relay the message to the next hop by inserting an updated relay time stamp, TS_{R_i}, and creating a new digital signatue.

Traffic Lights: Traffic lights are generally the main destinations of messages. Once a traffic light receives a message, it firstly verifies the relay vehicle's certificate and public key from CBC and RBC public ledgers followed by a verification of a digital signature of the relay vehicle. If the digital signature of the relay vehicle is valid, the traffic light will continue to verify the ambulance's signature. If both signatures are valid, the traffic light will accept the message. Otherwise, the message will be discarded. The traffic light will gather validated messages and determine an optimal traffic light schedule, so that any approaching ambulances can go through any intersections without stops.

IV. Discussion and Analysis

According to uniqueness, threats and risks, security requirements, and system constraints of vehicular communication networks, especially during rescue missions, it becomes very challenging to decide a broadcast communication protocol to cope with all these aspects. BSAX is comprehensively analyzed in this section in order to evaluate its performance against all required aspects in the secure vehicular communication networks.

A. Uniqueness Analysis

Due to Blockchain concept, BSAX has unique characteristics in terms of distributed, scalable, and trustless system, assuming a certificate chain has been pre-uploaded.

Distributed: The distributed aspect allows vehicles entering and leaving the networks at any times, since BSAX operates on top of pre-uploaded certificate chains and public ledgers contributed only by current members of the networks.

Scalable: All three ledgers, i.e. CBC, RBC, and MBC, in BSAX are built based on a hash function, which is a light-weight security operation, resulting in scalability in the networks. Thus, the varied number of vehicles in the networks, such as dense vehicle density in urban area and sparse vehicle density rural area, does not affect the performance of the proposed BSAX.

Trustless: The trustless system makes BSAX well suited to a dynamic topology of the vehicular networks. Since there is no need of a centralized trust entity, such as cluster heads, BSAX can deal with changes of the network topology very well.

B. Security Analysis

BSAX also achieves several security requirements in vehicular communication networks discussed as follows;

Authentication: Based on Blockchain, by checking CBC and RBC public ledger, vehicles with invalid certificates or revoked public keys can efficiently excluded from the networks, and hence prevent the entire network from jamming and interference risks. Since both CBC and RBC are mainly based on a hash function, checking validity of both certificates and revoked public keys, then, requires low computing time and resources.

Message Integrity: Integrity of messages has been achieved through a digital signature. By verifying the digital signature of both ambulances and relay vehicles, all messages in the networks cannot be altered or modified by any other vehicles, due to the use of private keys. The message integrity efficiently helps to prevent networks from message forgery attacks.

Non-repudiation: A digital signature not only provides message integrity, but also provides non-repudiation. Since the digital signature can created by each individual private key, it is undeniable, if a message is signed by one's private key. Additionally, all messages in the network accumulated in the MBC ledger are auditable. These non-repudiation and message traceability become very beneficial in terms of law investigations, such as a case of accident. Furthermore, the digital signature and a private key concepts are also an effective countermeasure to impersonation. Without an authentic private key, no one can masquerade as an ambulance or another vehicle.

Message Freshness: Time stamps used in BSAX mainly provide freshness to each created and relayed message. Because each massage cannot be altered and the time stamp is part of such message, all vehicles can determine whether they should accept the message or not. For example, if the different between the current time and the attached time stamp is over the defined threshold, the messages will be discarded. The message freshness then can protect the network from replaying any old messages back into the network.

Anonymity: Privacy and security in the most cases are in different directions and must be traded. BSAX, on the other hand, can achieve both security and privacy. By using a chain of certificates containing a chain of pseudonyms, no one can reveal a true identity of each vehicle. Furthermore, tracking an individual is also limited, due to the use certificate chain. At one point of the time, depending on how often users switch to a next certificate in the chain, vehicle tacking cannot be continue due to a non-correlation between the previous and the currently used certificates. Therefore, privacy in terms of anonymity and vehicle tracking is efficiently preserved. Links between pseudonyms and real identities must only be revealed in a case of law-related investigations.

V. Conclusion

A novel Blockchain-based Secure Ambulance-to-Everything Communications in Emergency Rescue Operations (BSAX) is proposed in this paper to provide secure and anonymous A2X communications during rescue operations. Our analysis shows that based on Blockchain concept, BSAX can operate in distributed, scalable, and trustless environments in accordance to non-centralized, dynamic topology, and varied number of vehicles in the vehicular communication networks. Additionally, BSAX also achieves security in terms of authentication, message integrity, non-repudiation, message freshness, and anonymity. Therefore, BSAX can prevent the networks from diverse types of threats including network jamming, replay and forged messages, and impersonations. Ultimately, a level vehicle's privacy is preserved using a chain of pseudonym-based certificates. In the future, a numerical analysis for evaluating the proposed method will be conducted and compared with the results of other related papers. For these reasons, BSAX could become one of the solutions to provide secure and anonymous communications in vehicular networks, especially for ambulance-to-everything communications in rescue operations.

Acknowledgment

This work is supported in part by the Hubei Province International Science and Technology Collaboration Program under Grant 2021EHB012, the Suzhou Municipal Key Industrial Technology Innovation Program under Grant SYG202123, and EU H2020 MSCA-RISE-2020 under Grant 101008085.

References

[1] A National Perspective on Ambulance Crashes and Safety, [Online]. Available: https://www.ems.gov/pdf/EMSWorldAmbulanceCrashArticlesSept2015.pdf

[2] C. Suthaputchakun and Y. Cao, "Ambulance-to-Traffic Light Controller Communications for Rescue Mission Enhancement: A Thailand Use Case," in IEEE Communications Magazine, vol. 57, no. 12, pp. 91-97, December 2019, doi: 10.1109/MCOM.001.1900038.

[3] C. Suthaputchakun and A. Pagel, "A Novel Priority-Based Ambulance-to-Traffic Light Communication for Delay Reduction in Emergency Rescue Operations," 2019 International Conference on Information and Communication Technologies for Disaster Management (ICT-DM), 2019, pp. 1-6, doi: 10.1109/ICT-DM47966.2019.9032930.

[4] Y. Han, N. -N. Xue, B. -Y. Wang, Q. Zhang, C. -L. Liu and W. -S. Zhang, "Improved Dual-Protected Ring Signature for Security and Privacy of Vehicular Communications in Vehicular Ad-Hoc Networks," in IEEE Access, vol. 6, pp. 20209-20220, 2018, doi: 10.1109/ACCESS.2018.2822806.

[5] D. Wang, P. Ren, Q. Du, L. Sun and Y. Wang, "Security Provisioning for MISO Vehicular Relay Networks via Cooperative Jamming and Signal Superposition," in IEEE Transactions on Vehicular Technology, vol. 66, no. 12, pp. 10732-10747, Dec. 2017, doi: 10.1109/TVT.2017.2703780.

[6] W. Hathal, H. Cruickshank, Z. Sun and C. Maple, "Certificateless and Lightweight Authentication Scheme for Vehicular Communication Networks," in IEEE Transactions on Vehicular Technology, vol. 69, no. 12, pp. 16110-16125, Dec. 2020, doi: 10.1109/TVT.2020.3042431.

[7] Z. Lu, Q. Wang, G. Qu and Z. Liu, "BARS: A Blockchain-Based Anonymous Reputation System for Trust Management in VANETs," 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 2018, pp. 98-103, doi: 10.1109/TrustCom/BigDataSE.2018.00025.

[8] H. Liu, P. Zhang, G. Pu, T. Yang, S. Maharjan and Y. Zhang, "Blockchain Empowered Cooperative Authentication With Data Traceability in Vehicular Edge Computing," in IEEE Transactions on Vehicular Technology, vol. 69, no. 4, pp. 4221-4232, April 2020, doi: 10.1109/TVT.2020.2969722.

[9] D. Chulerttiyawong and A. Jamalipour, "A Blockchain Assisted Vehicular Pseudonym Issuance and Management System for Conditional Privacy Enhancement," in IEEE Access, vol. 9, pp. 127305-127319, 2021, doi: 10.1109/ACCESS.2021.3112013.

[10] A. S. Kulathunge and H. R. O. E. Dayarathna, "Communication framework for vehicular ad-hoc networks using Blockchain: Case study of Metro Manila Electric Shuttle automation project," 2019 International Research Conference on Smart Computing and Systems Engineering (SCSE), 2019, pp. 85-90, doi: 10.23919/SCSE.2019.8842814.