Research Article

International Journal of Advanced Technology and Engineering Exploration, Vol 8(81)
ISSN (Print): 2394-5443   ISSN (Online): 2394-7454
http://dx.doi.org/10.19101/IJATEE.2021.874294

A security scheme based on blockchain and a hybrid cryptosystem to reduce packet loss in IoV

Won Jin Chung[1] and Tae Ho Cho[2]*
Department of Electrical and Computer Engineering, Sungkyunkwan University, Suwon, Republic of Korea[1]
Department of Computer Science and Engineering, Sungkyunkwan University, Suwon, Republic of Korea[2]

Received: 24-June-2021; Revised: 08-August-2021; Accepted: 13-August-2021

Abstract

The internet of vehicles is a future technology that uses autonomous vehicles and road infrastructure to provide convenience to drivers and prevent accidents caused by driver negligence. However, autonomous vehicles are vulnerable to network attacks because they collect information using wireless communication. An attacker penetrates the autonomous vehicle's network to drop information or forge and retransmit information. An autonomous vehicle that collects forged information may cause an accident due to incorrect driving. A scheme applying blockchain to the internet of vehicles has been proposed to prevent attacks occurring on autonomous vehicles. Blockchain has excellent security and has better performance when operating in a small network. However, blockchain is difficult to operate in a large network, and it takes a long time to encrypt and decrypt messages. Blockchain technology can cause packet loss when used in environments with many driving vehicles. In this paper, we solve the packet loss problem using a security scheme that combines blockchain and a hybrid cryptosystem. The proposed scheme constructs a block chain with only the road infrastructure and verifies information through a control center. Autonomous vehicles use the hybrid cryptosystem to collect information while maintaining security. In the proposed scheme, the time consumed for encryption/decryption can be reduced by using a hybrid cryptosystem. As a result of the experiment, the proposed scheme reduces accidents caused by packet loss by about 80% compared to the existing scheme using a private block chain.

Keywords

Blockchain, Internet of vehicles, Network security, V2X communication.

1.Introduction

Recently, the focus of smart vehicles that relied on sensors has changed due to advances in the Internet of Things (IoT) and networks. Various information can be exchanged while applying IoT technology to automobiles, which allows drivers to pursue convenience. The Internet of Vehicles (IoV) is a technology that combines Intelligent Transportation Systems (ITS) and IoT, and vehicular ad-hoc network (VANET), the current communication, is being developed into IoV [1]. IoV allows autonomous vehicles to communicate with other autonomous vehicles or various road infrastructures to understand road conditions. Autonomous vehicles recognize the road environment with sensing techniques such as cameras, radars, and riders, and identify road topography using High-definition (HD) maps [2] and the Global Navigation Satellite System (GNSS) [3].

Furthermore, autonomous vehicles communicate with objects on the road using the Vehicle to Everything (V2X) communication, collect information, and plan routes based on it [4]. Autonomous vehicles collect various situational information, such as road control areas caused by accidents and roads where rush hour occurs through V2X communication. Using this information, automatic vehicles can avoid road congestion and navigate and drive on roads that allow for the shortest travel time [4]. V2X communication that can collect information is a necessary technology for autonomous driving, and the stability of the network must be ensured while the vehicle is communicating. This is because such information can be sent and received in real time to cope with the situation. Therefore, for autonomous driving, a high network transmission speed must be guaranteed and data must be protected from attackers [5]. An attacker infiltrates networks used by autonomous vehicles to delete or forge data. Accidents occur because autonomous vehicles receive forged data or fail to

*Author for correspondence

receive data. Such accidents can cause not only property damage, but also human casualties. To maintain the security of the network, a security scheme using blockchain technology has been proposed in the IoV environment [6–8]. Blockchain ensures the integrity of data by encrypting it with a hash function and linking the encrypted data. However, blockchain takes a long time to create blocks and has poor scalability, so there are limitations in using the technology in the IoV environment. In this paper, to solve this problem, we propose a scheme using a combination of blockchain and a hybrid cryptosystem. In the proposed scheme, the data are verified by forming a blockchain only with the road infrastructure. In addition, autonomous vehicles use hybrid cryptosystems instead of blockchain's to communicate with the road infrastructure. The goal of the proposed scheme is to reduce traffic accidents caused by packet loss through fast encryption/decryption. In addition, the scalability problem is solved by configuring the blockchain formation only with road infrastructure excluding Roadside Units (RSU). In other words, the proposed scheme uses this approach to reduce the overhead on blockchain formation, reducing the probability of packet loss and preventing traffic accidents. In addition, the scalability problem is solved by composing the block chain formation only with road infrastructure. Proposed schemes enable smooth driving, helping to ensure safe driving in IoV. The composition of the paper is as follows. Section 2 describes IoV, autonomous vehicle security, blockchain, and hybrid cryptosystems. Section 3 describes the proposed scheme. Section 4 demonstrates the performance of the proposed scheme compared to existing schemes. Discussion is in Section 5. Finally, Section 6 describes the conclusion and future research.

2.Literature review

This section discusses IoV and autonomous vehicles, as well as attacks and security schemes that arise from autonomous vehicles. In addition, the blockchain and hybrid security system to defend against attacks in the proposed scheme were explained.

2.1Internet of vehicles

With the development of IoT, various convergence technologies have been proposed. IoV is a technology that combines IoT and ITS. IoV can deploy RSU to collect information in real time. Therefore, IoV improves the efficiency of the network compared to the existing scheme, VANET, and solves traffic safety problems. Therefore, IoV is being developed to overcome the limitations of ITS and can support traffic management services and vehicle safety services [9]. An autonomous vehicle, a key element of IoV, is a vehicle that drives itself to a destination [10–12]. Autonomous vehicles provide driver convenience and prevent accidents caused by driver negligence. Automatic driving technology is divided into six levels, depending on the controller and responsibility [13]. From Level 3, the system is in charge of driving control and detecting variables during driving. In level 5 autonomous driving, the vehicle calculates its own route to the destination specified by the driver and drives to it. For autonomous driving, sensing, maps, current location awareness, and planning is important. In order to do the level 5 automatic driving mentioned above, vehicles must be able to recognize various objects such as transportation infrastructure and pedestrians. This requires the vehicle to be equipped with sensors that can recognize all objects in the environment. The types of sensors attached to the automatic vehicle include cameras, radars, and Light Detection and Ranging (LiDAR) [11, 12]. In the case of LiDAR, it can detect any object within 100 meters in all directions around the vehicle. LiDAR has good sensing technology, but it is expensive, so you often cannot attach many to a vehicle. Radar is a technology that measures objects using electromagnetic waves. Therefore, the sensors required for autonomous driving depend on radar and cameras. This technology does not require much computing power and data as compared to LiDAR. The camera is a cheap and easily obtained sensor that allows color recognition. Automatic vehicles use good sensors for driving, but blind spots and bad weather can make the environment unrecognizable. Automatic vehicles solve these problems using V2X communication [14]. V2X communication is divided into various types, such as Vehicle to Vehicle (V2V) communication, Vehicle to Infrastructure (V2I) communication, Vehicle to Pedestrian (V2P) communication, and Vehicle to Device (V2D) communication, depending on the target [4]. V2V communication is a system that prevents traffic accidents by exchanging location information, speed information, and surrounding situation information between vehicles within a certain range. These communications are used to prevent unexpected situations or crashes near the vehicle. V2I communication is a technology that collects driving information while exchanging information between the vehicle and RSUs and provides traffic situation and accident information to the vehicle by analyzing the information in a control center. Since the information delivered to the vehicle can grasp the real-time traffic situation, traffic jams and traffic accidents can be prevented. Although V2X communication provides real-time information to vehicles, there are various problems, such as network infrastructure construction, hacking and information leakage, and frequency interference.

2.2Attack and security

Autonomous vehicles collect real-time information from vehicles and road infrastructures using V2X communication. This real-time traffic information should be delivered safely to vehicles without compromising the information to hackers. Because V2X communication is wireless communication, security is weak. Hackers can use these vulnerabilities to obtain personal information and traffic situation information. Since the acquired situation information is forged and transmitted to vehicles, it may cause traffic accidents [15]. *Table 1* shows the attacks occurring on the autonomous vehicle's network.

Table 1 Network attacks from IoV

Attack type	Attack
Confidentiality/privacy attacks	Interception attack [16]
	Eavesdropping attack [17]
Data integrity/data trust attacks	Masquerading attack [18]
	Data tampering attack [19]
	Replay attack [20]
Authenticity/identification attacks	GNSS spoofing attack [21]
	Timing attack [22]
	Falsified entities attack [23]
Availability attacks	Denial of Service attack [24]
	Jamming attack [25]
	Wormhole attack [26]
	Flooding attack [27]

The attacks that occur on autonomous vehicles are diverse, and if security is not provided, a traffic accident may occur, potentially resulting in the loss of life. Therefore, the security of autonomous vehicle is important and various security techniques are being studied [15]. An eavesdropping attack is an attack that allows an attacker to check the driver's destination by snooping on network communication. These attacks cannot cause traffic accidents, but they are a privacy-infringement because driver information is exposed. On the contrary, flooding attacks and replay attacks are attacks that directly damage the vehicle and cause traffic accidents. In particular, replay attacks are difficult to filter in the middle because the previously transmitted data is retransmitted. Thus, replay attacks can be prevented using security techniques such as sequence numbers and timestamps [28, 29] is a scheme for detecting replay attacks using sequence numbers. The security scheme using the sequence number has the advantage that fast filtering is possible. However, sequence numbers are not encrypted for fast filtering. As a result, an attacker can attempt an attack using the sequence number. A timing attack, which is a different type of attack that sends messages continuously, is an attack that delays message transmission. Such an attack can be a dangerous attack in applications where real-time processing is important. In order to detect a Sybil attack, a security scheme for estimating the location of a vehicle by installing a beacon through an RSU has been proposed [30]. These security schemes can detect accurately, but they cause additional equipment problems.

2.3Blockchain

Blockchain is an algorithm that negotiates the information content of connected blocks to secure and maintain integrity [31]. These algorithms are distributed Peer-to-Peer (P2P) systems in the ledger that utilize software elements. Although blockchain is widely applied in various fields, it is especially highlighted in cryptocurrency because it is a real case that has the greatest impact on the economy. If blockchain is used for management purposes, it can be used in the field of ownership management of digital goods. Blockchain uses a hash function, which is one-way, and any data are converted into a number of a certain length regardless of the input length. Hash functions allow us to provide hash values for all data immediately and avoid conflicts because they all come with different values depending on the input. Blockchain connects the values obtained through the hash function in the form of a chain (linked list). Also, blockchain has the structure of a Merkle tree. These structures are useful when all data present at the same time are grouped together, and approached with a single hash reference [32]. Blockchain is divided into public blockchain, private blockchain, and consortium blockchain according to the access control mechanism

[33]. *Table 2* summarizes the characteristics of blockchain.

Public blockchain is a blockchain that has decentralization characteristics and operates without a central administrator. Therefore, public blockchain does not have an administrator, allowing all accessors to participate as nodes on that platform and to freely validate all transactions. However, public blockchain has the disadvantages of long processing times, unclear operating entities, and difficulty in changing the rules. Public blockchain is effective when strong security is required. Conversely, private blockchain is a blockchain in which a central administrator exists. Therefore, participation is limited because a central administrator manages the platform. However, since private blockchain has a central administrator, it is possible to operate more stable than public blockchain and to respond quickly in the case of failure. In addition, private blockchain has a faster processing speed than public blockchain due to central administration, and rules can be easily changed according to the administrator's will. Finally, consortium blockchain is located in the middle between public blockchain and private blockchain and is a technology that combines the elements of the two chains. Consortium blockchain is characterized by being able to flexibly change the rules because a small number of groups are validators and can be viewed by an authorized individual or all according to the consensus of the verification group. Consortium blockchain can be effectively used for organizations that need smooth communication. The blockchain is applied to IoV to detect various network attacks is a security scheme that applies public blockchain to IoV [34]. The public blockchain has the advantage that nodes can freely connect or disconnect from the network. The public blockchain scheme applied to IoV allows vehicles to freely enter the network and communicate safely and exchange information. However, due to the nature of the blockchain, it takes a lot of time to form the block and must possess information from all other vehicles. Therefore, autonomous vehicles must collect a lot of information on high traffic roads. As a result, autonomous vehicles can cause overhead on information processing and cause packet loss. Another method, [35] is a private blockchain technology for IoV. This scheme allows faster processing than public blockchain's because the vehicle's network connection or disconnection is determined by the central administrator. However, the fundamental time problem for blockchain formation is difficult to solve.

Table 2 Blockchain type

	Public	**Private**	**Consortium**
Concept	All nodes hold records	Only certain nodes hold records	Only certain nodes hold records
Management entity	All nodes	Central authority retains all authority	Nodes that belong to the consortium
Data access	Anyone can access	Only authorized users can access	Only authorized users can access
Network extension	Difficult	Very easy	Easy
Speed	Slow	Fast	Fast
Identifiability	Anonymity	Identifiable	Identifiable

2.4Hybrid cryptosystem

A hybrid cryptosystem is a security system that combines symmetric keys with public keys [36]. The encryption method that uses symmetric keys can be encrypted with a single key and communication that maintains confidentiality is possible, but there is a problem in delivering the key [37]. The method of using the public key includes a private key and a public key, and both encryption keys are used for encryption and decryption [38]. Data encrypted with the private key must be decrypted with the public key, and data encrypted with the public key must be decrypted with the private key [38]. Due to these characteristics, the public key method is used for data encryption as well as authentication. The public key cryptography method solves the key delivery problem, but is slower than the symmetric key cryptography method. The hybrid cryptosystem was proposed to solve these problems [36]. The hybrid cryptosystem encryption/decryption method is as follows. To encrypt the message, a session key generated by a random number generator is used. The session key is encrypted with the recipient's public key, and then the session key is sent to the recipient, together with the ciphertext encrypted with the symmetric key. After separating the session key and the cipher text, the receiver decrypts the session key with its own private key. Thereafter, the ciphertext is decrypted using the decrypted session key. The receiver can safely receive messages through this method.

3.Methods

In this section, the description of the proposed scheme for defending against network attacks occurring in IoV is presented.

3.1Overview

IoV is a technology that can change the paradigm of automobiles in the near future, providing convenience to drivers and reducing accidents. The automatic vehicle, a key element of IoV, uses sensors to understand the road environment, collect information through V2X communication, calculate the optimal route, and safely drive to the destination. However, since V2X communication is wireless communication, an attacker can drop information or deliver forged information, which can cause accidents. To defend against such attacks, a security technique applying blockchain to IoV has been proposed. Because blockchain has excellent security, it is useful in an environment where accurate information must be received. The autonomous vehicle must continuously collect real-time information and drive safely to its final destination. However, the processing efficiency is not good in environments where there are many driving vehicles, due to poor scalability and slow encryption/decryption when blockchain is used.

3.2Detailed procedure

The proposed scheme reduces packet loss by combining blockchain and a hybrid cryptosystem in IoV to transmit data quickly and safely. *Figure 1* shows the overall structure of the proposed scheme.

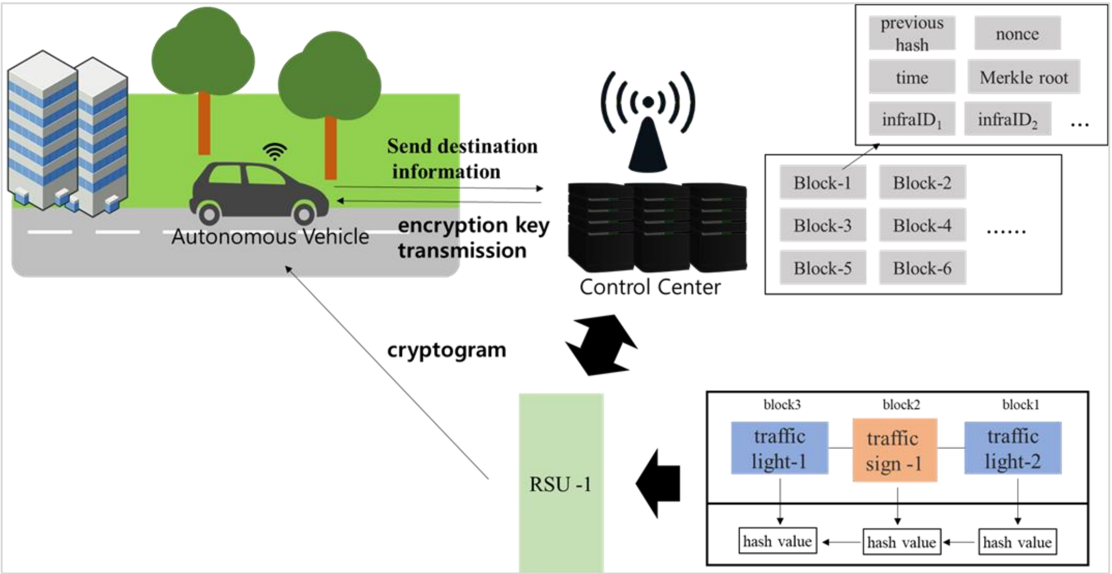

Figure 1 Proposed scheme overview

An autonomous vehicle delivers destination information to the control center. The control center verifies the autonomous vehicles and generates a session key for the autonomous vehicle. After that, the control center encrypts the session key with the public key of the autonomous vehicle and transmits it to the corresponding autonomous vehicle. The control center sends a verification request message to the RSU in the path of the autonomous vehicle. The RSU uses information from the infrastructure to form a blockchain. Hash values used to create the blocks utilize information from the road infrastructure communicating with the RSUs. The RSU sends the generated blockchain to the control center, and the control center verifies the blocks. When the block verification is completed, the control center delivers the session key delivered to the autonomous vehicle to the RSU. The control center performs the same verification process for all RSUs in the autonomous vehicle's destination path. Afterwards, when the autonomous vehicle reaches the RSU, it generates an information request message using the session key received from the control center and transmits it to the RSU. The RSU decrypts the message using the session key received from the control center and authenticates the autonomous vehicle. When authentication is completed, the RSU encrypts the road infrastructure information with the session key received from the control center and delivers it to the autonomous vehicle. The autonomous vehicle can decrypt received ciphertexts into session keys to gather real-time traffic information. This process is repeated until the autonomous vehicle reaches its destination.

Figure 2 shows the operation process of the proposed scheme through a block diagram. In the Blockchain Formation phase, the blockchain is formed by forming a group of surrounding road infrastructures installed in the zone. The formed blockchain is periodically transmitted to the control center to demonstrate the integrity of the data generated from the road infrastructure. When road infrastructure verification is completed, the proposed technique verifies whether the RSU is compromised in the RSU Verification phase. RSU does not form road infrastructure and blockchain for smooth communication. Consequently, the proposed scheme should monitor the RSU at all times to determine whether it is compromised. After verification of all road infrastructure, the Autonomous Vehicle Verification phase proceeds. The autonomous vehicle entering the road delivers destination information and vehicle information to the control center to collect traffic information. The control center inquires and verifies the vehicle and generates a session key to use the hybrid cryptosystem. The generated session key is transmitted to the vehicle after encryption using the public key of the autonomous vehicle. When the vehicle receives the key, the Secure Channel Connection phase proceeds. In this phase, the session key exchanged with the autonomous vehicle is transmitted to the verified RSU. All road infrastructure verification procedures must be completed before session key transmission. After receiving the session key, the RSU encrypts the acknowledgment request message with the session key and transmits it to the vehicle. When the autonomous vehicle receives the message and sends an acknowledgment message encrypted with the session key, a secure channel between the RSU and the vehicle is established. After that, the RSU uses the channel to transmit the traffic information collected from the road infrastructure to the vehicle. The last phase of the proposed scheme, Encryption Key Management, will be described. Since autonomous vehicles are connected to multiple RSUs during the driving process, it is necessary to share a session key. The control center can identify the RSU that needs to be connected when the autonomous vehicle drives to its destination. After that, the control center transmits the same session key to the RSU on the driving path. After that, the RSU proceeds with the procedure to create a secure channel when the vehicle is connected to the network. In addition, after a certain period of time, the control centre communicates with the RSU and the autonomous vehicle to exchange the existing session key with the new session key. The purpose of updating the session key is to prevent it from being stolen from the attacker.

Figure 3 shows the sequence diagram for the autonomous vehicle to collect real-time traffic information. In this way, the proposed scheme protects the traffic information from attackers and quickly transmits it to the autonomous vehicle. In addition, scalability issues are addressed because autonomous vehicles collect information through the Hybrid cryptosystem.

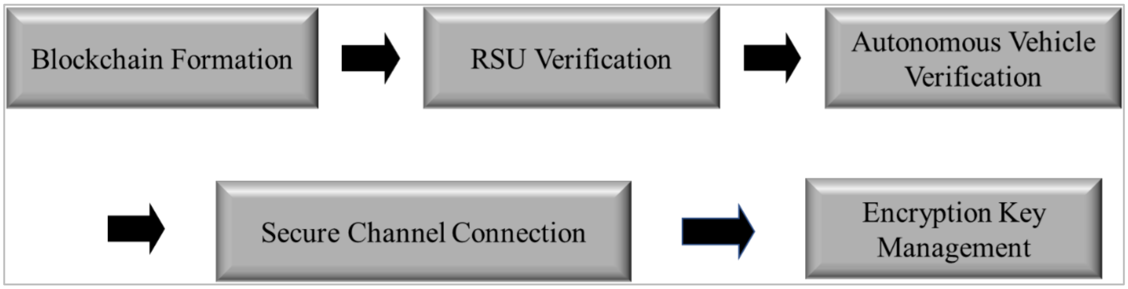
Blockchain Formation
RSU Verification
Autonomous Vehicle Verification
Secure Channel Connection
Encryption Key Management

Figure 2 Proposed schematic block diagram

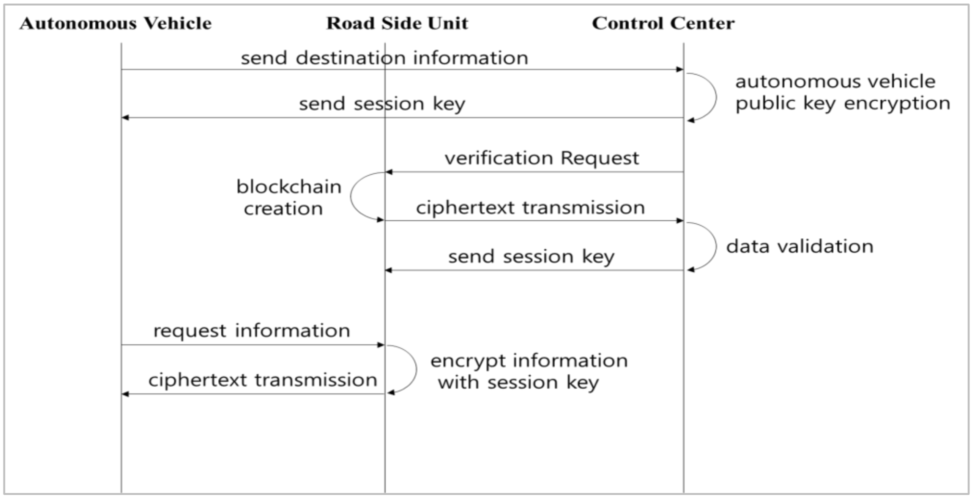

Figure 3 Proposed scheme sequence diagram

4.Results

This section describes the simulation environment for performance evaluation of the proposed scheme and explains the performance of the proposed scheme through graphs.

4.1Simulation environment

The proposed scheme simulates the process of two automatic vehicles driving to a destination in a pre-designed road environment. The simulations measure packet transmission and the number of traffic accidents in situations where attacks occur. *Figure 4* shows the designed road environment. As shown in *Figure 4*, on an RSU basis, the surrounding road infrastructure forms a blockchain. Road infrastructures can determine whether the device is compromised in the control center by periodically delivering the generated block to the control center through the RSU. The roles of the road infrastructures shown in the figure are explained together in the description of *Table 3.*

The designed road environment has two departure points and four destinations. The vehicle departs by randomly preempting the location among the two departure points, and the destination is also randomly preempted. *Table 3* shows the types and number of road infrastructures deployed on the designed roads [39–41].

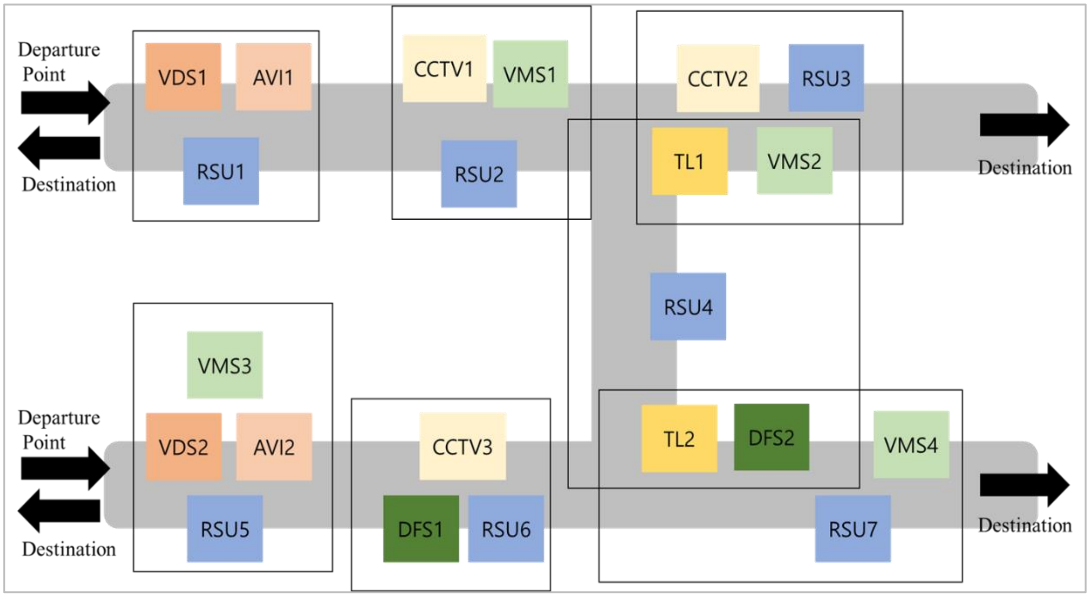

Figure 4 Designed road environment

Table 3 Infrastructure used in the experiment

Infrastructure	Number of objects
Roadside Unit	7
Vehicle Detection System (VDS)	2
Automatic Vehicle Identification (AVI)	2
Variable Message Sign (VMS)	4
Closed-circuit Television (CCTV)	3
Traffic Lights	2
Driver Feedback Sign	2

The RSUs are installed by section to collect road infrastructure information and deliver it to vehicles. A VDS and an AVI system are installed at the departure point because they collect information and record when a vehicle enters. A VMS is a device that delivers various information such as road control, weather conditions, and road congestion. In the simulation, various situational events are generated and transmitted to the vehicle. CCTV serves to store road condition information. Data recorded through CCTV are transmitted to the control center. The Traffic Lights (TL) used in the simulation are three-color TL consisting of red, yellow, and green, and the signal is maintained at a 4:2:4 ratio. Finally, a Driver Feedback Sign (DFS) is a device that displays vehicle speed information. In the simulation environment, the area where the DFS is placed has a speed limit (60 km/s) and a warning message is sent when the vehicle exceeds the speed limit.

4.2Performance evaluation

The proposed scheme uses blockchain and hybrid cryptosystem to reduce packet loss and prevent traffic accidents. The proposed scheme was compared with the private blockchain security technique applied to IoV. The proposed scheme evaluates the performance by comparing the transmitted packets, the number of security breaches, and the accidents caused by packet loss with the existing schemes.

Figure 5 shows the number of packets transmitted per 100 RSUs. The proposed scheme was compared with the existing scheme, private blockchain [35], and the number of packets received by two vehicles was measured. The existing scheme shows approximately 2.9205% packet loss as compared to the proposed scheme. The experiment was conducted using two autonomous vehicles. As the number of autonomous vehicles increases, the number of packets transmitted and received increases, which may widen the packet loss gap.

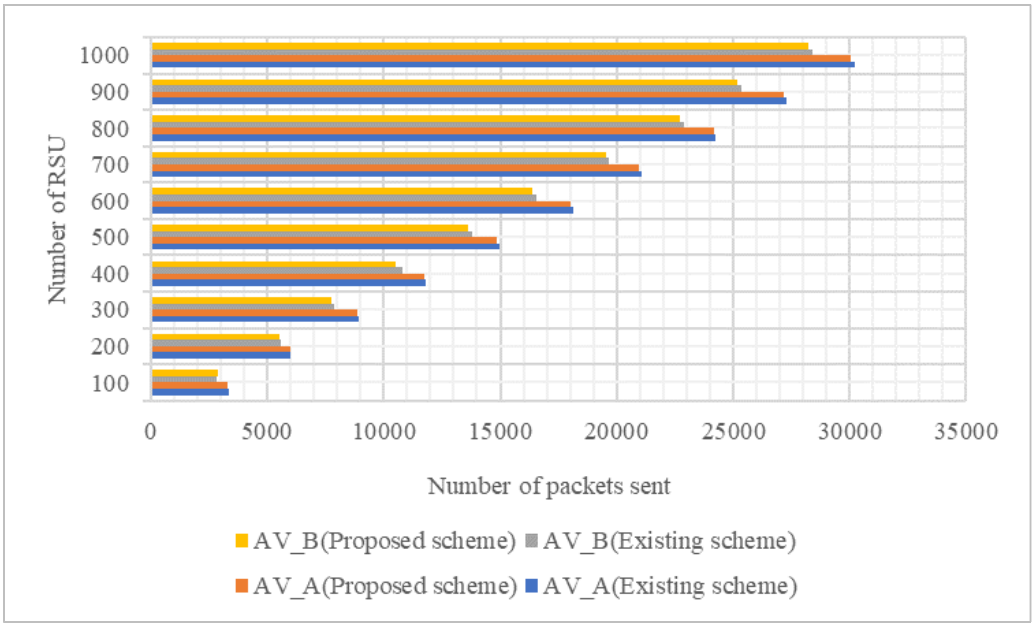

Figure 5 Number of packets sent to the autonomous vehicles

Figure 6 shows the number of infringement incidents against the number of attacks. Since the private blockchain, which is the existing scheme, is managed by the control center, the attacker's target is only the control center. However, since the proposed scheme stores the security key not only in the control center but also in the RSU. The RSU is also an attack target. Compared with the existing scheme, it can be confirmed through the graph that with the proposed scheme about 12.9032% of the 10,000 attacks are infringed. Since the proposed scheme has more targets to be attacked than the existing scheme, relatively more attack infringement occurs. This is a problem caused by an attacker using a compromised RSU to deliver incorrect information [42]. Therefore, if the security strength of the RSU is increased, this problem is solved.

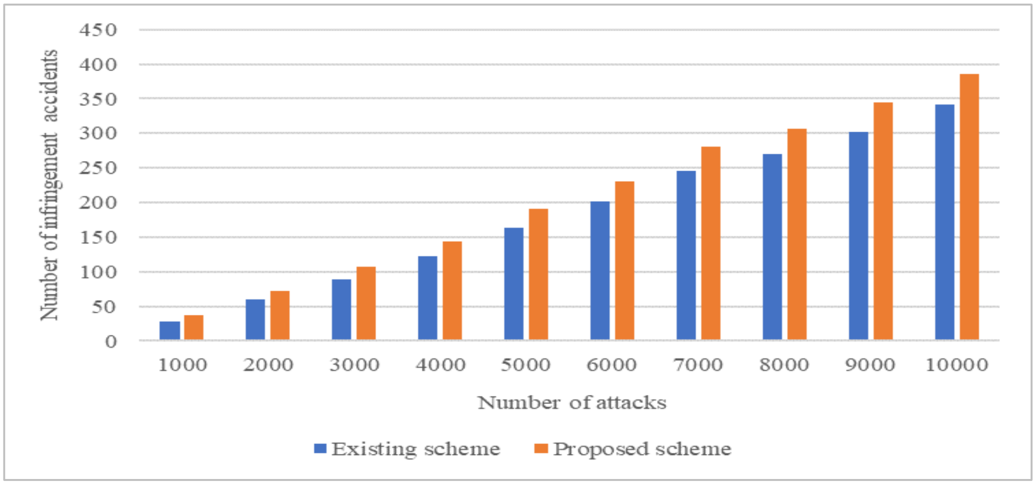

Figure 6 Number of attack breaches by number of attacks

Figure 7 shows the probability of an accident due to packet loss caused by blockchain generation by comparing the proposed scheme with the existing scheme. Simulation results show that in the event of 10,000 attacks, the proposed scheme reduces accidents by about 80.3278% as compared to the existing scheme. Since the proposed scheme has more targets than the existing scheme, the number of attack breaches is large. However, for autonomous vehicles, receiving information in real time is also a very important issue. For security reasons, when packet transmission is delayed or packet loss occurs, the autonomous vehicle cannot collect necessary information and an accident may occur. Therefore, the proposed scheme can prevent accidents by prioritizing packet delivery in real time.

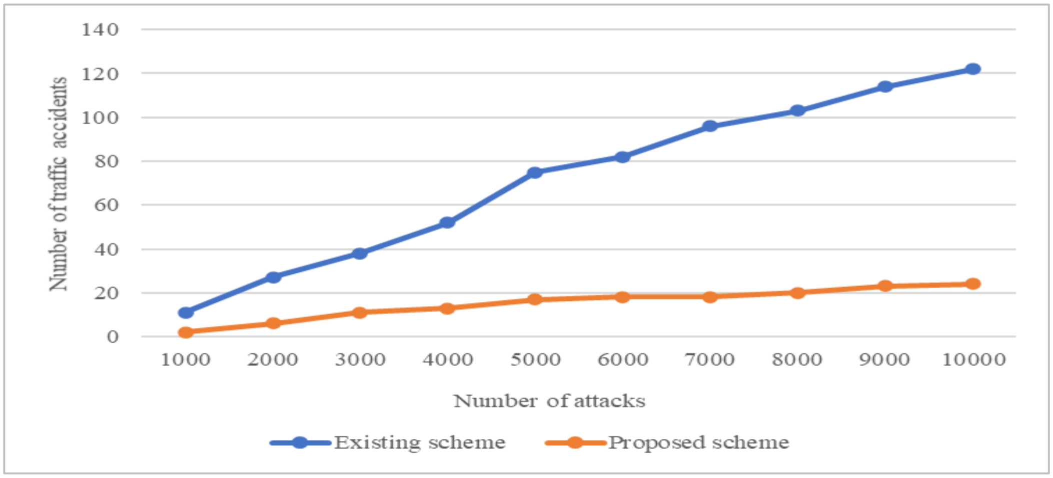

Figure 7 Number of accidents by number of attacks

5.Discussion

The proposed scheme aims to reduce accidents by reducing packet loss in the security technique using blockchain. Since the existing scheme uses blockchain to encrypt the message, the probability of sending a forged message is very low. However, there is a risk of accidents if information is delayed or packet loss continues to occur because autonomous vehicles need to receive information through real-time communication. Blockchain spends a lot of time forming blocks for security. Since IoV requires real-time information to be transmitted to autonomous vehicles, the time issue needs to be resolved in order to apply blockchain to IoV. To solve this problem, the proposed scheme forms a blockchain by composing only road infrastructure excluding RSU. However, the proposed scheme has a lot of attack targets, which is less effective in detecting attacks than existing schemes. To address these issues, further research is needed to strengthen RSU security. The strength of the proposed scheme is to prevent accidents by reducing packet loss. In autonomous vehicles where real-time information delivery is important, information can be transmitted and processed at the time needed through proposal schemes, and the information can be transmitted through encryption to be trusted. Complete list of abbreviations is shown in *Appendix I*.

6.Conclusion and future work

IoV is the future technology in which autonomous vehicles and road infrastructure communicate, calculate destinations by themselves, and drive safely. IoV promotes driver convenience and can prevent accidents caused by driver negligence. The autonomous vehicle performs V2X communication and collects various traffic information. They can then use the collected information to explore the optimal path and avoid situations in which vehicles are unable to drive, such as traffic jams and road control. In addition, autonomous vehicles can use V2X communication to prevent accidents and serial crashes with surrounding vehicles. However, since autonomous vehicles use wireless communication, attackers can attempt various attacks using them. An attacker can break into the autonomous vehicle's network and drop or falsify information and retransmit. If these attacks continue, they can lead to traffic accidents. Many security schemes have been studied to prevent attacks from autonomous vehicles, and blockchain technology that can be used for IoV has also been proposed. Blockchain technology can ensure data integrity by composing ciphertext in the form of a chain, and stable network operation is possible.

Thus, when blockchain is applied to IoV, an environment where traffic information can be safely transmitted to autonomous vehicles is created. In addition, IoV can utilize public and private blockchain's according to the situation to protect transmitted information. However, blockchain has scalability problems and takes a long time to create blocks. Since autonomous vehicles use a lot of resources to generate blocks, a large number of packet losses occur. In an environment where there are many driving vehicles, real-time information needs to be delivered quickly, so packet loss may occur when using a blockchain with a slow processing speed. If such packet loss continues, a traffic accident may occur. In this paper, we propose a security scheme that combines blockchain and a hybrid cryptosystem to solve these problems. An RSU creates a block using the infrastructure and transmits it to the control center. After that, the control center verifies the information and sends the session key. In this process, data is encrypted and decrypted using a hybrid cryptosystem to maintain security. After that, the traffic information is encrypted with the session key and transmitted to the autonomous vehicle. The proposed scheme solves the scalability problem while maintaining security through the combined method and enables fast encryption/decryption, thereby reducing packet loss. The proposed scheme reduced the packet loss rate by about 3% compared to the existing scheme through experiments and prevented about 80% of accidents. However, the proposed scheme causes more accidents due to attack infringement by about 12% than the existing scheme. However, since the proposed scheme also stores the security key in the RSU, an attacker can obtain the security key by hacking the RSU. Since this problem attempts to attack with the security key of the compromised RSU, the security strength must be increased to prevent the RSU from being compromised. These problems are fatal flaws in the proposed scheme and must be resolved. In the future, we plan to study security schemes using contextual knowledge to solve these problems.

Acknowledgment

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korean government (MSIT) (No. NRF-2021R1A2C2005480).

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] Gerla M, Lee EK, Pau G, Lee U. Internet of vehicles: from intelligent grid to autonomous cars and vehicular clouds. In world forum on internet of things 2014 (pp. 241-6). IEEE.

[2] Howard DL, De JMD, Lau D, Hay D, Varcoe-cocks M, Ryan CG, et al. High-definition X-ray fluorescence elemental mapping of paintings. Analytical Chemistry. 2012; 84(7):3278-86.

[3] Dow JM, Neilan RE, Rizos C. The international GNSS service in a changing landscape of global navigation satellite systems. Journal of Geodesy. 2009; 83:191-8.

[4] Chen S, Hu J, Shi Y, Peng Y, Fang J, Zhao R, et al. Vehicle-to-everything (V2X) services supported by LTE-based systems and 5G. IEEE Communications Standards Magazine. 2017; 1(2):70-6.

[5] Sun Y, Wu L, Wu S, Li S, Zhang T, Zhang L, et al. Attacks and countermeasures in the internet of vehicles. Annals of Telecommunications. 2017; 72:283-95.

[6] Mollah MB, Zhao J, Niyato D, Guan YL, Yuen C, Sun S, et al. Blockchain for the internet of vehicles towards intelligent transportation systems: a survey. IEEE Internet of Things Journal. 2020; 8(6):4157-85.

[7] Li W, Nejad M, Zhang R. A blockchain-based architecture for traffic signal control systems. In international congress on internet of things 2019 (pp. 33-40). IEEE.

[8] Lu Z, Liu W, Wang Q, Qu G, Liu Z. A privacy-preserving trust model based on blockchain for VANETs. IEEE Access. 2018; 6:45655-64.

[9] Contreras-castillo J, Zeadally S, Guerrero-ibañez JA. Internet of vehicles: architecture, protocols, and security. IEEE Internet of Things Journal. 2017; 5(5):3701-9.

[10] Rasouli A, Tsotsos JK. Autonomous vehicles that interact with pedestrians: a survey of theory and practice. IEEE Transactions on Intelligent Transportation Systems. 2019; 21(3):900-18.

[11] Wang J, Liu J, Kato N. Networking and communications in autonomous driving: a survey. IEEE Communications Surveys & Tutorials. 2018; 21(2):1243-74.

[12] Yurtsever E, Lambert J, Carballo A, Takeda K. A survey of autonomous driving: common practices and emerging technologies. IEEE Access. 2020; 8:58443-69.

[13] SAE International. Automated driving levels of driving automation are defined in New SAE International Standard J3016.

[14] Wang J, Shao Y, Ge Y, Yu R. A survey of vehicle to everything (V2X) testing. Sensors. 2019; 19(2):1-20.

[15] Cui J, Liew LS, Sabaliauskaite G, Zhou F. A review on safety failures, security attacks, and available countermeasures for autonomous vehicles. Ad Hoc Networks. 2019.

[16] Bariah L, Shehada D, Salahat E, Yeun CY. Recent advances in VANET security: a survey. In vehicular technology conference 2015 (pp. 1-7). IEEE.

[17] Mokhtar B, Azab M. Survey on security issues in vehicular ad hoc networks. Alexandria Engineering Journal. 2015; 54(4):1115-26.

[18] Amoozadeh M, Raghuramu A, Chuah CN, Ghosal D, Zhang HM, Rowe J, et al. Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. IEEE Communications Magazine. 2015; 53(6):126-32.

[19] Whaiduzzaman M, Sookhak M, Gani A, Buyya R. A survey on vehicular cloud computing. Journal of Network and Computer Applications. 2014; 40:325-44.

[20] Al-shareeda MA, Anbar M, Hasbullah IH, Manickam S, Abdullah N, Hamdi MM. Review of prevention schemes for replay attack in vehicular ad hoc networks (VANETs). In international conference on information communication and signal processing 2020 (pp. 394-8). IEEE.

[21] Dasgupta S, Rahman M, Islam M, Chowdhury M. Prediction-based GNSS spoofing attack detection for autonomous vehicles. arXiv preprint arXiv:2010.11722. 2020.

[22] Mejri MN, Ben-othman J, Hamdi M. Survey on VANET security challenges and possible cryptographic solutions. Vehicular Communications. 2014; 1(2):53-66.

[23] Mokhtar B, Azab M. Survey on security issues in vehicular ad hoc networks. Alexandria Engineering Journal. 2015; 54(4):1115-26.

[24] Biron ZA, Dey S, Pisu P. Real-time detection and estimation of denial of service attack in connected vehicle systems. IEEE Transactions on Intelligent Transportation Systems. 2018; 19(12):3893-902.

[25] Feng S, Haykin S. Cognitive risk control for anti-jamming V2V communications in autonomous vehicle networks. IEEE Transactions on Vehicular Technology. 2019; 68(10):9920-34.

[26] Singh PK, Gupta RR, Nandi SK, Nandi S. Machine learning based approach to detect wormhole attack in VANETs. In workshops of the international conference on advanced information networking and applications 2019 (pp. 651-61). Springer, Cham.

[27] Sakiz F, Sen S. A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV. Ad Hoc Networks. 2017; 61:33-50.

[28] Li W, Song H. ART: an attack-resistant trust management scheme for securing vehicular ad hoc networks. IEEE Transactions on Intelligent Transportation Systems. 2015; 17(4):960-9.

[29] Wang Q, Sawhney S. VeCure: a practical security framework to protect the CAN bus of vehicles. In international conference on the internet of things (IOT) 2014 (pp. 13-8). IEEE.

[30] Rabieh K, Mahmoud MM, Guo TN, Younis M. Cross-layer scheme for detecting large-scale colluding sybil attack in VANETs. In international conference on communications 2015 (pp. 7298-303). IEEE.

[31] Lin IC, Liao TC. A survey of blockchain security issues and challenges. International Journal of Network Security. 2017; 19(5):653-9.

[32] Di PM. What is the blockchain? Computing in Science & Engineering. 2017; 19(5):92-5.

[33] Zheng Z, Xie S, Dai HN, Chen X, Wang H. Blockchain challenges and opportunities: a survey. International Journal of Web and Grid Services. 2018; 14(4):352-75.

[34] Shrestha R, Bajracharya R, Nam SY. Blockchain-based message dissemination in VANET. In international conference on computing, communication and security 2018 (pp. 161-6). IEEE.

[35] Li M, Zhu L, Lin X. Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing. IEEE Internet of Things Journal. 2018; 6(3):4573-84.

[36] Darwish A, El-gendy MM, Hassanien AE. A new hybrid cryptosystem for internet of things applications. In multimedia forensics and security 2017 (pp. 365-80). Springer, Cham.

[37] Thakur J, Kumar N. DES, AES and blowfish: symmetric key cryptography algorithms simulation based performance analysis. International Journal of Emerging Technology and Advanced Engineering. 2011; 1(2):6-12.

[38] Mollin RA. RSA and public-key cryptography. Chapman and Hall/CRC; 2002.

[39] Shivaldova V, Paier A, Smely D, Mecklenbräuker CF. On roadside unit antenna measurements for vehicle-to-infrastructure communications. In international symposium on personal, indoor and mobile radio communications 2012 (pp. 1295-9). IEEE.

[40] Cavalcante ES, Aquino AL, Pappa GL, Loureiro AA. Roadside unit deployment for information dissemination in a VANET: an evolutionary approach. In proceedings of the annual conference companion on genetic and evolutionary computation 2012 (pp. 27-34). ACM

[41] Lochert C, Scheuermann B, Wewetzer C, Luebke A, Mauve M. Data aggregation and roadside unit placement for a VANET traffic information system. In proceedings of the ACM international workshop on vehicular inter-networking 2008 (pp. 58-65).

[42] Hao Y, Cheng Y, Ren K. Distributed key management with protection against RSU compromise in group signature based VANETs. In GLOBECOM, global telecommunications conference 2008 (pp. 1-5). IEEE.

Won Jin Chung Received a B.S. degree in Information Security from Baekseok University, Korea, in 2016 and is now working toward a Ph.D. degree in the Department of Electrical and Computer Engineering at Sungkyunkwan University, Korea.

Email: wonjin12@skku.edu

Tae Ho Cho Received a Ph.D. degree in Electrical and Computer Engineering from the University of Arizona, USA, in 1993, and B.S. and M.S. degrees in Electrical and Computer Engineering from Sungkyunkwan University, Republic of Korea, and the University of Alabama, USA, respectively. He is currently a Professor in the College of Computing, Sungkyunkwan University, Korea.
Email:thcho@skku.edu

Appendix I

S. No.	Abbreviation	Description
1	AVI	Automatic Vehicle Identification
2	DFS	Driver Feedback Sign
3	GNSS	Global Navigation Satellite System
4	HD	High-definition
5	IoT	Internet of Things
6	IoV	Internet of Vehicles
7	ITS	Intelligent Transportation Systems
8	LiDAR	Light Detection and Ranging
9	P2P	Peer to Peer
10	RSU	RoadSide Units
11	TL	Traffic Lights
12	VANET	Vehicular ad-hoc Network
13	VDS	Vehicle Detection System
14	V2D	Vehicle to Device
15	V2I	Vehicle to Infrastructure
16	V2P	Vehicle to Pedestrian
17	V2V	Vehicle to Vehicle
18	V2X	Vehicle to Everything
19	VMS	Variable Message Sign