IEICE TRANS. INF. & SYST., VOL.E105–D, NO.2 FEBRUARY 2022

PAPER Special Section on Blockchain Systems and Applications

Toward Blockchain-Based Spoofing Defense for Controlled Optimization of Phases in Traffic Signal System

Yingxiao XIANG[†a)], **Chao LI**[†b)], **Tong CHEN**[†c)], **Yike LI**[†d)], **Endong TONG**[†e)], **Wenjia NIU**[†f)], **Qiong LI**[†g)], **Jiqiang LIU**[†h)], ***and*** **Wei WANG**[†i)], ***Nonmembers***

SUMMARY Controlled optimization of phases (COP) is a core implementation in the future intelligent traffic signal system (I-SIG), which has been deployed and tested in countries including the U.S. and China. In such a system design, optimal signal control depends on dynamic traffic situation awareness via connected vehicles. Unfortunately, I-SIG suffers data spoofing from any hacked vehicle; in particular, the spoofing of the last vehicle can break the system and cause severe traffic congestion. Specifically, coordinated attacks on multiple intersections may even bring cascading failure of the road traffic network. To mitigate this security issue, a blockchain-based multi-intersection joint defense mechanism upon COP planning is designed. The major contributions of this paper are the following. 1) A blockchain network constituted by road-side units at multiple intersections, which are originally distributed and decentralized, is proposed to obtain accurate and reliable spoofing detection. 2) COP-oriented smart contract is implemented and utilized to ensure the credibility of spoofing vehicle detection. Thus, an I-SIG can automatically execute a signal planning scheme according to traffic information without spoofing data. Security analysis for the data spoofing attack is carried out to demonstrate the security. Meanwhile, experiments on the simulation platform VISSIM and Hyperledger Fabric show the efficiency and practicality of the blockchain-based defense mechanism.

key words: *traffic signal system, connected vehicles, data spoofing attack, blockchain, defense mechanism*

1. Introduction

Intelligent transportation systems (ITSs) [1] play a significant role in development of smart cities, aiming to achieve a safe and efficient integrated transportation system, and have attracted increasingly more attention from government departments, scientific research institutions, and scientific and technological enterprises. ITSs have been widely studied and applied due to their environmental friendliness, high performance, and easy deployment. For instance, since September 2016, the U.S. Department of Transportation has piloted the deployment of the intelligent traffic signal system (I-SIG) [2] in some U.S. states, including California, Florida, and New York. The Ministry of Transportation of China relied on Didi to pilot the intelligent traffic signal system at 344 road intersections in Jinan, Shandong Province in 2018. As a critical component, the I-SIG system is responsible for performing dynamic and optimal signal control based on automatic traffic situation awareness, by leveraging the emerging connected vehicle (CV) technology [3], [4], which empowers vehicles to communicate with the surrounding environment, including Road-side Units (RSUs), traffic signal control infrastructure, and nearby vehicles, by using On-Board Units (OBUs) to periodically broadcast Basic Safety Messages (BSMs) including real-time vehicle trajectory data (e.g., location and speed), as shown in Fig. 1.

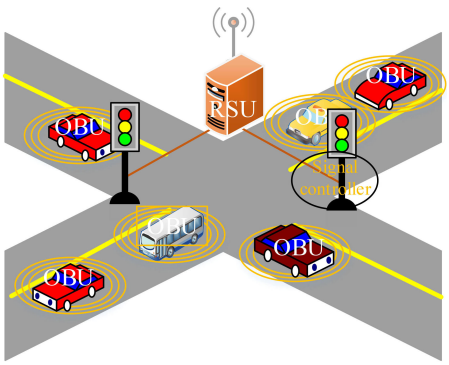


Fig. 1 Intelligent traffic signal control scenario.

Unfortunately, with the rapid development of CV technology, growing connectivity also opens a new door for cyber attacks. In some recent studies [5]–[7], it has been revealed that traffic control systems are at risk of malicious attacks, in which the attackers can process vehicle information such as location, speed, direction, and acceleration to affect the results of the signal planning algorithm (e.g., controlled optimization of phases – COP [8], [9]). For instance, in [5], attackers can compromise the OBUs on their vehicles in an I-SIG and send malicious BSM messages such as speed and location to affect the traffic control decisions at proper timing, causing unexpected heavy traffic congestion. The authors showed that one single attack vehicle is able to cause a total delay 11 times higher, which greatly hinders the development and future large-scale deployment. Previous works mainly reveal the existence of data spoofing attacks that can cause severe traffic congestion [5], [6]

Manuscript received May 21, 2021.
Manuscript revised June 27, 2021.
Manuscript publicized September 13, 2021.

[†]The authors are with Beijing Jiaotong University, Beijing, 100044, China.
a) E-mail: yxxiang@bjtu.edu.cn
b) E-mail: li.chao@bjtu.edu.cn
c) E-mail: tongchen@bjtu.edu.cn
d) E-mail: yikeli@bjtu.edu.cn
e) E-mail: edtong@bjtu.edu.cn (Corresponding author)
f) E-mail: niuwj@bjtu.edu.cn (Corresponding author)
g) E-mail: liqiong@bjtu.edu.cn
h) E-mail: jqliu@bjtu.edu.cn
i) E-mail: wangwei1@bjtu.edu.cn
DOI: 10.1587/transinf.2021BCP0014

or collisions [7]. Meanwhile, in several studies [10], [11], efficient detection and prediction methods of traffic congestion caused by spoofing attacks and related client-site detection approaches [12]–[14] have been proposed. Additional studies [15]–[18] on researching the security of ITSs mainly focus on the authentication and privacy-preserving mechanisms for the connected vehicular cloud services.

The focus of this paper is the study of defending COP in a traffic signal system, I-SIG, against data spoofing attacks. In the I-SIG system, there is only one source of data about the attack vehicle, i.e., the attacker-controlled trajectory data via BSM messages [19] that are still correctly signed. Therefore, defense must rely on the filter and detection of attack vehicles by using the reliable data, which while worthy of study is still an open issue. One challenge is how to ensure the safety and reliability of data storage; that is, to ensure that data cannot be tampered with. The other challenge is how to detect and filter attack vehicles automatically.

To meet the above challenges and solve the above problems, a blockchain-based multi-intersection joint (BMJ) defense mechanism is presented to defend intelligent traffic signal control systems against data spoofing attacks by storing the vehicle data on RSUs in a way that is both tamper proof and provides traceability. As one of the most popular technologies, blockchain is a distributed ledger that could be used to improve data security owing to its transparency, immutability, and traceability. The natures of blockchain are especially suitable for the requirements of data security, which encouraged its exploitation in the present work to present a defense mechanism based on blockchain technology. In the BMJ defense mechanism, the blockchain network is constituted by RSUs of multiple intersections that are responsible for validating BSM data sources, creating the block, and storing data. Then, a consensus mechanism determines the messages to be written and the order in which they are written. In addition, a smart contract is introduced to automatically implement the spoofing detection function and handling function of the attack vehicle. Ensure that signal controllers execute COP with reliable data. The major contributions of this paper are the following.

1) Our work introduces the first study of a COP defense mechanism in intelligent traffic signal systems from the perspective of data security, including research of the safety of data sources and data storage.

2) Based on blockchain technology, RSUs are organized at multiple intersections to construct a blockchain network. Then, a smart contract is introduced to implement the spoofing detection and filter algorithm for attack vehicles based on the data storing on the blockchain. Finally, based on the detection result, RSUs can automatically refuse the forthcoming data of attack vehicles to ensure the normal planning of COP.

3) The proposed BMJ defense mechanism is evaluated using simulation experiments on the Hyperledger Fabric and VISSIM platforms.

2. Related Work

The security problems of the intelligent traffic signal system based on CV technology have been being revealed in several recent works [5]–[7]. For instance, Chen et al. [5] revealed a threat of data spoofing over the intelligent traffic signal system - I-SIG. The data spoofing can cause severe traffic congestion via a single attack vehicle. Jeske [6] demonstrated how hackers can take control of navigation systems in practice, in order to trick navigation services and cause congestion. The authors of [7] analyzed security attacks on a vehicle stream; such attacks can use message falsification (modification), spoofing (masquerading), or replay attacks to maliciously affect the vehicle stream, leading to rear-end collisions in severe cases.

Typical approaches to handling such attacks are via authentication and information-preserving mechanisms to prevent attack vehicles from joining CV networks and tampering with data. Gupta et al. [15] proposed an authorization framework – an extended access control oriented (E-ACO) architecture for CVs to secure the Internet of Vehicles (IoV). In [18], the authors proposed a blockchain-assisted lightweight anonymous authentication mechanism for distributed vehicular fog services that can provide flexible cross-datacenter authentication for connected vehicles. The authors in [16] presented a secure and efficient transmission method by combining the core concepts of game theory and information theory to ensure the integrity of transmission data. Fan et al. [17] proposed a ciphertext-based search system that can protect information from tampering during its retrieval. In addition, there are some recent work, such as [20]–[22], that focused on reliable blockchain-based signature and authentication for trust computing of edge computing system. These studies mainly focused on the problem of vehicle identity authentication in order to prevent untrusted outsiders.

Unlike the above studies, the attack vehicle in the present study of an adversary case is a trusted insider with a valid certificate, and it could be either a physical or virtual vehicle. Therefore, to solve this problem, the feasible solutions may be to detect or predict such attacks after they occurred, or to prevent such attacks. In terms of detection and prediction, in some works, such as [10], [11], the spoofed traffic flow data were analyzed to detect or predict the data spoofing attack. Li et al. [10] proposed a CycleGAN-based prediction approach using traffic image features that reflects the relationship between attack and the congestion caused. The authors in [11] proposed an explainable congestion attack prediction approach using a deep learning model, i.e., Tree-regularized Gated Recurrent Unit (TGRU), and they tried to explain the relationship between the traffic flow feature and the lanes in which the congestion attack vehicle locates. Compared to these studies, the present work is focused on preventing spoofing attacks.

Since its invention, blockchain technology has been mainly applied in the field of cryptocurrency based on a

peer-to-peer system named Bitcoin [23]. There are very few works in which a defense mechanism based on blockchain for the signal control system of the ITS has been studied. In a recent paper [24], Li et al. proposed a blockchain-based, decentralized architecture to improve the data security for traffic signal control systems. They introduced witness vehicles and nearby RSUs together as references and designed a Consensus Protocol to validate data source. However, the architecture can not ensure the trustworthiness of witness vehicles and nearby RSUs, so there may still be security problems. The main difference between the present work and this previous study is that in the blockchain-based defense mechanism proposed herein, the blockchain network is constituted by RSUs at multiple intersections, and the smart contract introduced is used to implement the spoofing detection and filter.

3. Preliminary

3.1 Intelligent Traffic Signal System

The physical architecture of the intelligent traffic signal control system is shown in Fig. 2, showing five main segments as follows: OBUs are hardware devices deployed on CVs. RSUs are responsible for receiving and maintaining BSM messages broadcast by CVs. The roadside safety processor is a general purpose computer that performs the core intersection-level functions, such as traffic signal planning. The traffic signal controller receives signal control commands and then executes them. The field sensor/detector can detect the vehicles using detection technologies, and provides information to the traffic signal controller.

3.2 Adversary Model

Figure 3 shows the attack strategy of an adversary in [5], which is studied in the present work. In this strategy, the attacker changes the location and speed information in a vehicle's BSM messages to alter the vehicle's arrival time and its requested signal phase; thus, the corresponding arrival table elements are changed. The false vehicles' trajectory data input to the COP algorithm will cause the COP to execute improper signal planning and output the wrong signal scheme. The appearance of spoofed vehicles make the queue of vehicles on the lane longer, and there is an increment of the duration of green light allocated by the COP algorithm for the current phase, which delays the next start time of the green light of all the phases, increasing the delay for vehicles to pass. In particular, with the last vehicle attack, even the spoofed data from a single attack vehicle can significantly affect signal planning.

In the adversary case studied in this work, there are two types of spoofing attack, as shown in Fig. 4. The first is called physical vehicle attack and the second virtual vehicle attack. The virtual vehicle attack (see the top part of Fig. 4) refers to the fact that an attacker adds a virtual vehicle at

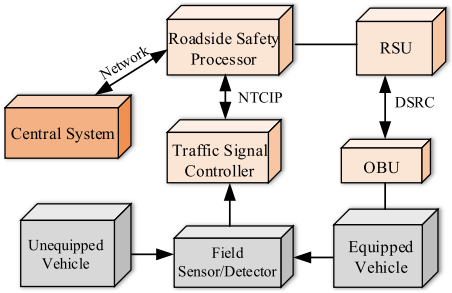


Fig. 2 Physical architecture of intelligent traffic signal control.

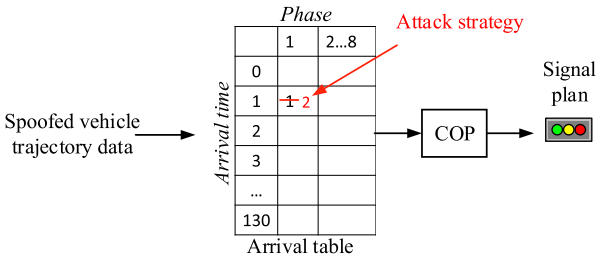


Fig. 3 Attack strategy of adversary.

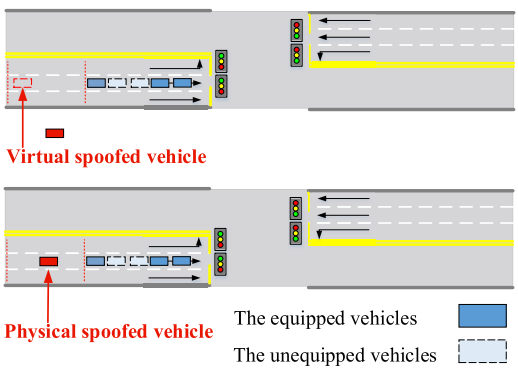


Fig. 4 Attack scenario of data spoofing.

the end of the vehicle queue by modifying the BSM information of the vehicle, resulting in the change of the queue length in the lane. Therefore, COP will count it due to the signal planning, and then the signal control logic changes. The physical vehicle attack (see the bottom part of Fig. 4) means that the attack vehicle turns repeatedly at a certain intersection and always appears at the end of the geographic check scope of the signal planning when counting the vehicles at the intersection, thus affecting the COP planning results.

4. BMJ Defense Mechanism

In this section, the proposed blockchain-based multi-intersection joint (BMJ) defense framework, which is constituted by RSUs at multiple intersections, is described.

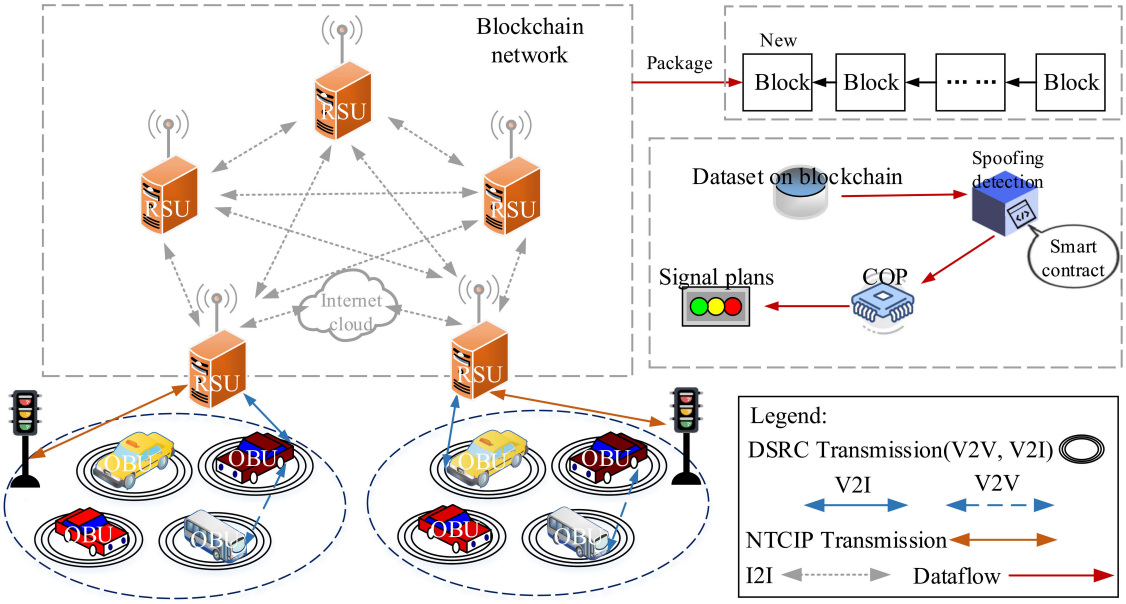


Fig. 5 Framework of the blockchain-based multi-intersection joint defense for COP.

4.1 Framework Overview

Figure 5 shows the BMJ defense framework, which has the following three main segments.

- Blockchain network construction: The RSUs act as miners in the BMJ defense mechanism and are responsible for creating the block of BSM messages and storing messages.
- Consensus and write block: The RSU aggregates the BSM messages of all verified CVs and packages them into blocks. After reaching a consensus, the block will be added to the end of the blockchain.
- Spoofing attack detection: The detection algorithm, including both virtual and physical attack vehicle detection, will be periodically executed by the smart contract.

The defense procedure of the proposed BMJ defense mechanism proceeds as follows. First, the blockchain network composed of RSUs passively collects BSM messages for the CVs and stores data on the blockchain. The trajectory information of all vehicles is calculated according to the data on the blockchain. Then, the smart contract detects the attack vehicles according to the trajectory information, including both virtual and physical attack vehicles, and adds the attack vehicles to the blacklist according to the detection results. RSUs will refuse to receive the information of attack vehicles in the next week. The COP algorithm will obtain more reliable vehicle information through the periodic detection executed by the smart contract.

4.2 Blockchain Network

In this paper, the premise of constructing a blockchain network is that RSUs in the I-SIG system are distrusted and may be attacked by the adversary, and the safety processor is trusted. Thus, RSUs may provide spoofed vehicle data due to being attacked. This situation will affect the accuracy and credibility of signal planning outputted by COP. Therefore, how to ensure the security and reliability of data on RSUs is worthy of further study. In the work described in this paper, a consortium blockchain based on the Hyperledger Fabric [25] is adopted to construct our blockchain network. The blockchain network is constituted by RSUs at multiple intersections that are responsible for uploading their received vehicle information to the blockchain. As shown in Fig. 6, multiple RSUs will be installed at each intersection to reduce the attack strength of the entire I-SIG system. This is because, for attackers, attacking multiple RSUs at the same time requires more computing resources.

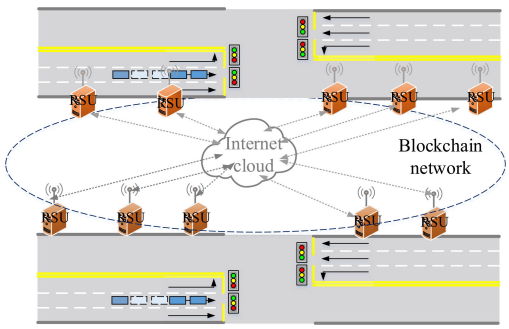


Fig. 6 Blockchain network constituted by RSUs.

According to the consensus mechanism (using the practical byzantine fault tolerance (PBFT) consensus algorithm [26]), the RSUs will package the BSM messages on it into blocks. Unlike traditional blockchains, in the proposed BMJ defense mechanism block bodies record the BSM mes-

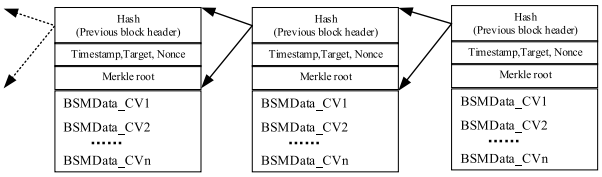


Fig. 7 BSM data of CVs stored in blocks of a blockchain.

Record ID	Vehicle ID	Lane	Location	Speed	Acceleration	Timestamp
1	322	1	1.8	28.43	0.2	144
2	319	1	28.2	34.81	−0.59	144
3	308	1	192	26.08	−2.69	144
...						

Fig. 8 Specific information on blockchain.

sages broadcast by CVs instead of transaction records. As illustrated in Fig. 7, each block body contains the BSM messages indexed by the vehicle ID. The new block will be added to the end of the blockchain after achieving a consensus. All RSUs in the blockchain network have the same blockchain data copies, and each copy cannot be modified. Therefore, the blockchain network could provide an immutable and secure storage environment for vehicle trajectory information.

The specific information recorded on the blockchain is shown in Fig. 8. The information maintained on the blockchain will be used to detect the attack vehicles, which cannot deny the detection results.

4.3 Smart Contract

To detect the spoofing attack vehicles, two detection algorithms were designed: one for the virtual vehicle attack and the other for the physical vehicle attack. The detection results are recorded in the blockchain and all RSUs will know the results. Once the attack vehicles have been detected, the BSM messages broadcast by these vehicles will not be accepted by RSUs in the next week. Based on the requirements of detecting attack vehicles and automatic execution, the smart contract is implemented to meet these requirements. Therefore, in this work, the smart contract specifies how the attack vehicles are detected and what should be done after the attack vehicles are detected. The smart contract is written to implement the detection function and handling function of attack vehicles. The spoofing detection process including both virtual and physical attack vehicle detection is shown in Algorithm 1.

Algorithm 1 Spoofing detection algorithm

Input: Trajectory data of vehicles, including location x, speed v, acceleration a, time t, indexed by ID n
Output: ID n of spoofing vehicle

initialization: maximum time T, maximum vehicle number N, parameters $\xi = 10(m)$, $\eta = 40(s)$, range of intersection $w = \{x^j \in w | j = 1, 2, \ldots, max\}$
//Detection of virtual vehicle
function $F1(n, x, v, a, t)$
  for $n = 1$ to N **do**
    for $t = 1$ to T **do**
      if $x_{t+1} - x_t > \xi$ **then**
        return True
      end if
    end for
  end for
  return False
end function
//Detection of physical vehicle
function $F2(n, x, v, a, t)$
  for $n = 1$ to N **do**
    for $j = 1$ to max **do**
      for $t = 1$ to T **do**
        if $x_{n,t} \in w, t \triangleq t^n_{new}(w_j)$ **then**
          $T^n(w_j) = \{t^n_i(w_j) | i = 1, 2, \ldots, max\}$
          append $t^n_{new}(w_j)$
        end if
      end for
      if $len(T^n(w_j)) > 0$ and $min\{t^n_{i+1}(w_j) - t^n_i(w_j)\} < \eta$ **then**
        return True
      end if
    end for
  end for
  return False
end function
for $n = 1$ to N **do**
  $r_1 = F1()$;
  $r_2 = F2()$;
  if r_1=True or r_2=True **then**
    return n *//spoofing vehicle ID*
  end if
end for

5. Security and Performance Analysis

5.1 Security Analysis

As introduced in Sect. 3.2, the attackers can modify the BSM messages of their vehicle to spoof the RSUs, which can cause incorrect intersection vehicle data to be input into the signal planning algorithm (COP). If the RSUs at an intersection receive spoofing vehicle information, it will affect the result of the entire intersection signal planning.

In the primary CV environment, the RSUs of each intersection are independent, and the data on RSUs are distrusted. The proposed defense mechanism enables RSUs at multiple intersections to jointly form a blockchain network and upload vehicle data to the blockchain. Once the data have been uploaded to the blockchain, they will be immutable. The constituted blockchain can provide transparent, trustable trajectory data of all CVs. The detection algorithm and exception handling algorithm have been written on the smart contract so that attack vehicles can be detected periodically. Therefore, all RSUs in the blockchain network can obtain the detection results. As a punishment, the attack vehicles will be rejected by RSUs for one week.

5.2 Performance Analysis

Simulations were conducted to evaluate the performance of the proposed BMJ defense mechanism by comparing its performance in the primary CV environment under the data

spoofing attack.

5.2.1 Experimental Setup

First, the blockchain network was deployed on the Hyperledger Fabric [25] platform, which maintains a distributed ledger for storing and sharing the CV information containing vehicle ID, lane, location, speed, acceleration, and timestamp. COP and VISSIM were then run for real-time traffic flow signal control, and the corresponding traffic simulation was carried out. The trajectory data of all vehicles was packaged into the blockchain, and then the smart contract is written to implement the spoofing detection and exception handling functions.

For defense effect evaluation, the average delay and the average congestion degree for all intersections with and without the proposed BMJ defense mechanism were compared. The delay time and congestion degree are defined as follows.

- *Delay time (DT)*. The DT for a vehicle spent in an intersection is calculated as the actual time AT that the vehicle spent to pass the intersection subtracting the free-flow travel time FT; thus, $DT = AT - FT$.
- *Congestion degree*. The vehicle number queuing in the kth phase is denoted Q_k, and Q_{normal} is the vehicle number of normal queuing, which is a constant. The congestion degree of the kth phase can then be computed by $PCD_k = Q_k/Q_{normal}$, and the global congestion degree for an intersection is $ICD = \sum_{k=1}^{8} PCD_k$.

5.2.2 Experimental Results

The effectiveness of the BMJ defense mechanism was evaluated first. The number of intersections was set to four, number of attack vehicles to one, and simulation time to 0.5 h. The results are shown in Figs. 9 and 10, showing the trend of the average delay and the average congestion degree with and without the BMJ defense mechanism. It can be seen from the figures that, under the same conditions, the trends of the average delay and average congestion degree with the BMJ mechanism are relatively stable, indicating that the proposed BMJ defense mechanism is effective for defending the signal planning algorithm COP in the CV environment against the data spoofing attack. This is because, in the case of without BMJ, COP will be continuously input into the spoofed trajectory data of the attack vehicle, leading to the continuous increase of the delay and congestion degree. However, in the case with BMJ, the smart contract periodically detects attack vehicles according to all vehicle trajectory data on the blockchain, and RSUs can refuse to receive spoofed trajectory data. Therefore, the congestion degree will not continue to increase and the trend of vehicle delay will be relatively stable.

The effect of different numbers of attack vehicles on BMJ defense mechanism performance was studied next. Similar to the previously described experiment, four intersections were set up, the simulation time set to 0.5 h, and the number of attack vehicles to one to four. The congestion degree of different numbers of attack vehicles were compared to study the impact of attack vehicle number on the BMJ defense mechanism. Figure 11 depicts the comparison results. With the change of time, although the congestion degree will increase slightly at some moments, it will decrease rapidly afterward. Compared with the congestion changes in the case of without BMJ, the average congestion degree decreased by 84%, 84%, 74%, and 66%, respectively, as the number of attacking vehicles increases. This is because once the smart contract of the BMJ defense mechanism has detected attack vehicles, the trajectory data of the vehicle will be rejected, so it will not cause a continuous increase of congestion degree. Therefore, the proposed BMJ defense mechanism is not affected by the number of attack vehicles.

In addition, the average congestion degree was compared with different numbers of intersections participating in the blockchain network. For a region with eight intersections, the number of attack vehicles was set to four, and the

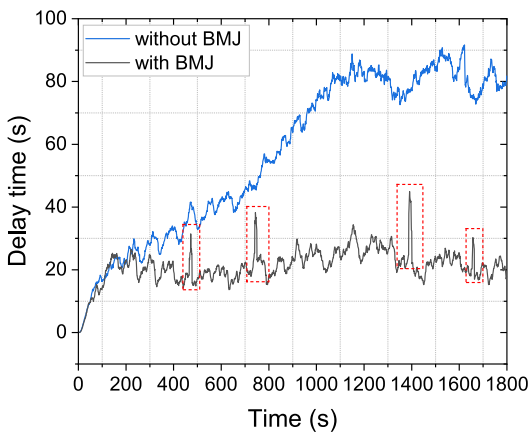


Fig. 9 Average delay curves with and without BMJ defense mechanism. Red dotted lines denote that the delay time is significantly increased at the moment.

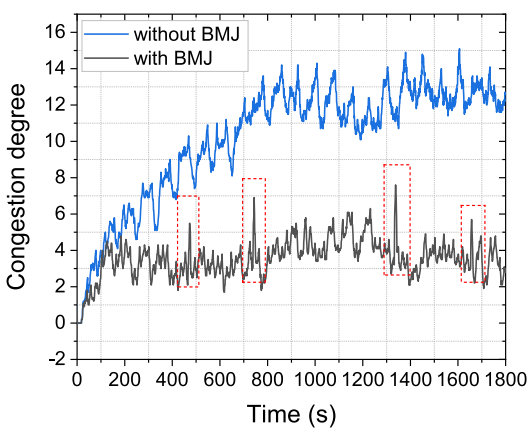


Fig. 10 Average congestion degree curves with and without BMJ defense mechanism. Red dotted lines denote that the congestion degree is significantly increased at the moment.

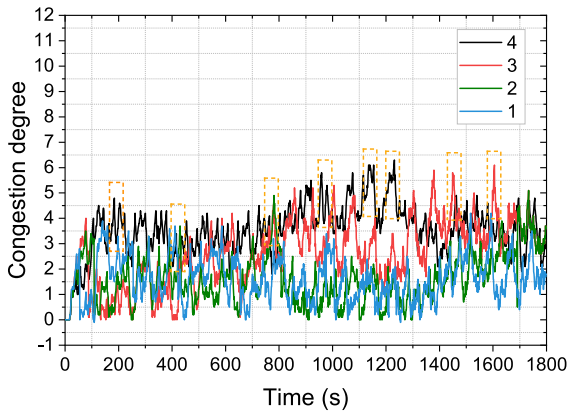


Fig. 11 Average congestion degree curves under the different numbers of attackers. Yellow dotted lines denote that the congestion degree is significantly increased at the moment.

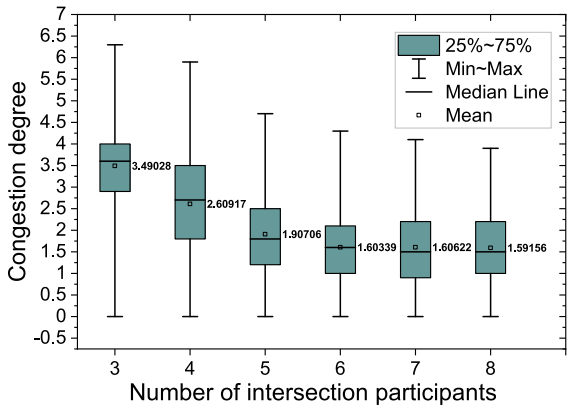


Fig. 12 Average congestion degree within 0.5 h under different numbers of intersections participating in blockchain network.

influence of different numbers of intersection participants, from three to eight, on the defense mechanism performance was investigated. In Fig. 12, the average congestion degrees in 0.5 h under different numbers of intersection participants were compared. It can be seen that when the number of intersection participants increases the average congestion degree in 0.5 h drops. In the proposed mechanism, due to the joint defense of multiple intersections, the more intersections that participate, the more complete the trajectory data, and the easier it is to detect attack vehicles. Therefore, in a particular region the more intersections there are participating in the blockchain network, the better the performance of the proposed BMJ defense mechanism.

6. Conclusion

The focus of this work is the problem of spoofing attacks in intelligent traffic signal systems. To defend the traffic signal planning algorithm against the data spoofing attack, it is necessary to detect and filter the attack vehicles based on the trajectory data of all vehicles. Two main challenges are posed, one of which is how to ensure the safety and reliability of trajectory data storage, and the other is how to detect and filter attack vehicles automatically. To address these challenges, a blockchain-based multi-intersection joint (BMJ) defense mechanism is presented. A blockchain network constituted by RSUs at multiple intersections, which can store the trajectory data in a way that is both immutable and traceable, is developed. Thus, trusted trajectory data on the blockchain can be used to detect attack vehicles. In addition, a smart contract is written to implement the detection of attack vehicles and to filter them periodically. As a result, continued congestion will not occur. Furthermore, a security analysis for data spoofing attacks was conducted, and the results of extensive experiments on the simulation platforms VISSIM and Hyperledger Fabric demonstrated the superiority of the presented BMJ defense mechanism for COP in the traffic signal system.

Acknowledgments

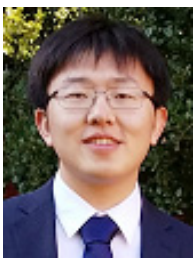
The work was supported by the National Natural Science Foundation of China under Grant Nos. 61972025, 61802389, 61672092, U1811264, and 61966009, the National Key R&D Program of China under Grant Nos. 2020YFB1005604 and 2020YFB2103802, and the Fundamental Research Funds for the Central Universities of China under Grant No. 2021JBM006.

References

[1] L. Zhu, F.R. Yu, Y. Wang, B. Ning, and T. Tang, "Big data analytics in intelligent transportation systems: A survey," IEEE Trans. Intell. Transp. Syst., vol.20, no.1, pp.383–398, 2019.
[2] "Usdot: Multimodal intelligent traffic safety system (mmitss)," https://www.its.dot.gov/research_archives/dma/bundle/mmitss_plan.htm.
[3] "U.s.dot connected vehicle pilot deployment program," https://www.its.dot.gov/pilots/.
[4] "Connected vehicle applications," https://www.its.dot.gov/pilots/cv_pilot_apps.htm.
[5] Q.A. Chen, Y. Yin, Y. Feng, Z.M. Mao, and H.X. Liu, "Exposing congestion attack on emerging connected vehicle based traffic signal control," Network and Distributed System Security Symposium, pp.39.1–15, 2018.
[6] T. Jeske, "Floating car data from smartphones: What google and waze know about you and how hackers can control traffic," 2012.
[7] M. Amoozadeh, A. Raghuramu, C.-N. Chuah, D. Ghosal, H.M. Zhang, J. Rowe, and K.N. Levitt, "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving," IEEE Commun. Mag., vol.53, no.6, pp.126–132, 2015.
[8] S. Sen and K.L. Head, "Controlled optimization of phases at an intersection," Transportation Science, vol.31, no.1, pp.5–17, 1997.
[9] Y. Feng, K.L. Head, S. Khoshmagham, and M. Zamanipour, "A real-time adaptive signal control in a connected vehicle environment," Transportation research, Part C. Emerging technologies, vol.55, pp.460–473, 2015.
[10] Y. Li, Y. Xiang, E. Tong, W. Niu, B. Jia, L. Li, J. Liu, Z. Han, and Z. Zhou, "An empirical study on gan-based traffic congestion attack analysis: A visualized method," Wirel. Commun. Mob. Comput., vol.2020, pp.8823300:1–8823300:14, 2020.
[11] X. Wang, Y. Xiang, W. Niu, E. Tong, and J. Liu, "Explainable congestion attack prediction and software-level reinforcement in intelligent traffic signal system," 26th IEEE International Conference on Parallel and Distributed Systems, ICPADS 2020, Hong Kong, Dec.

2-4, 2020, pp.667–672, IEEE, 2020.
[12] W. Wang, J. Song, G. Xu, Y. Li, H. Wang, and C. Su, "Contractward: Automated vulnerability detection models for ethereum smart contracts," IEEE Transactions on Network Science and Engineering, vol.8, no.2, pp.1133–1144, 2021.
[13] W. Wang, Y. Li, X. Wang, J. Liu, and X. Zhang, "Detecting android malicious apps and categorizing benign apps with ensemble of classifiers," Future Generation Computer Systems, vol.78, pp.987–994, 2018.
[14] W. Wang, X. Wang, D. Feng, J. Liu, Z. Han, and X. Zhang, "Exploring permission-induced risk in android applications for malicious application detection," IEEE Trans. Inf. Forensics Security, vol.9, no.11, pp.1869–1882, 2014.
[15] M. Gupta and R.S. Sandhu, "Authorization framework for secure cloud assisted connected cars and vehicular internet of things," Proc. 23nd ACM on Symposium on Access Control Models and Technologies, SACMAT 2018, Indianapolis, IN, USA, June 13-15, 2018, ed. E. Bertino, D. Lin, and J. Lobo, pp.193–204, ACM, 2018.
[16] Y. Yang, X. Niu, L. Li, and H. Peng, "A secure and efficient transmission method in connected vehicular cloud computing," IEEE Netw., vol.32, no.3, pp.14–19, 2018.
[17] K. Fan, X. Wang, K. Suto, H. Li, and Y. Yang, "Secure and efficient privacy-preserving ciphertext retrieval in connected vehicular cloud computing," IEEE Netw., vol.32, no.3, pp.52–57, 2018.
[18] Y. Yao, X. Chang, J.V. Misic, V.B. Misic, and L. Li, "BLA: blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services," IEEE Internet Things J., vol.6, no.2, pp.3775–3784, 2019.
[19] "Mmitss final conops: Concept of operations," http://www.cts.virginia.edu/wp-content/uploads/2014/05/Task2.3._CONOPS_6_Final_Revised.pdf.
[20] W. Wang, H. Xu, M. Alazab, T.R. Gadekallu, Z. Han, and C. Su, "Blockchain-based reliable and efficient certificateless signature for iiot devices," IEEE Trans. Ind. Informat., pp.1–9, 2021.
[21] W. Wang, H. Huang, L. Zhang, and C. Su, "Secure and efficient mutual authentication protocol for smart grid under blockchain," Peer-to-Peer Networking and Applications, vol.14, no.5, pp.2681–2693, 2021.
[22] L. Zhang, Y. Zou, W. Wang, Z. Jin, Y. Su, and H. Chen, "Resource allocation and trust computing for blockchain-enabled edge computing system," Computers & Security, vol.105, p.102249, 2021.
[23] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," Technical report, Manubot, 2019.
[24] W. Li, M. Nejad, and R. Zhang, "A blockchain-based architecture for traffic signal control systems," 2019 IEEE International Congress on Internet of Things, ICIOT, pp.33–40, 2019.
[25] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A.D. Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolic, S.W. Cocco, and J. Yellick, "Hyperledger fabric: a distributed operating system for permissioned blockchains," Proc. Thirteenth EuroSys Conference, EuroSys 2018, Porto, Portugal, ed. R. Oliveira, P. Felber, and Y.C. Hu, pp.30:1–30:15, April 23-26, 2018.
[26] M. Castro and B. Liskov, "Practical byzantine fault tolerance," Proc. Third USENIX Symposium on Operating Systems Design and Implementation (OSDI), New Orleans, Louisiana, USA, Feb. 22-25, 1999, ed. M.I. Seltzer and P.J. Leach, pp.173–186, USENIX Association, 1999.

Yingxiao Xiang received the B.S. degree in computer science and technology from Taiyuan University of Technology in 2016, Master degree from Beijing Jiaotong University in 2019. She is currently a Ph.D. candidate of cyber security in Beijing Jiaotong University. Her research interests are in information security and AI security.



Chao Li is an Assistant Professor in the School of Computing and Information Technology at Beijing Jiaotong University. He received his Ph.D. degree from the School of Computing and Information at University of Pittsburgh and his MSc degree from Imperial College London. His current research interests are focused on Blockchain and Data Privacy.

Tong Chen received the M.S. degree in Cyber security from Beijing Jiaotong University, Beijing, China in 2018. She is currently a Ph.D. candidate of cyber security in Beijing Jiaotong University, Beijing. Her main research interests are Cyber security and reinforcement learning security.

Yike Li received Bachelor degree from Hefei University of Technology in 2018. She is currently a graduate student of Beijing Jiaotong University. Her current research interests include AI security and Image generation.

Endong Tong received the Ph.D. degrees from Chinese Academy of Sciences, Beijing, China, in 2013. He is currently an assistant professor of Beijing Jiaotong University. His current research interests include AI Security Services Computing and Data Mining. He has published more than 30 research papers in refereed international conferences and journals.

Wenjia Niu obtained his Bachelor degree from Beijing Jiaotong University in 2005, PhD degree from Chinese Academy of Sciences in 2010, all in Computer Science. Now He is currently a professor in Beijing Jiaotong University. His research interests are AI Security, Agent and Data Mining.

Qiong Li received the M.S. degree in Signal and Information Processing from Beijing Jiaotong University in 2014. She is currently a teacher of information security in Beijing Jiaotong University. Her main research direction is multimedia security.

Jiqiang Liu received the B.S. and Ph.D. degrees from Beijing Normal University, Beijing, China, in 1994 and 1999, respectively. He is currently a professor with the School of Computer and Information Technology, Beijing Jiaotong University, Beijing. His main research interests are trusted computing, cryptographic protocols, privacy preserving, and network security.

Wei Wang received the Ph.D. degree in control science and engineering from Xi'an Jiaotong University, in 2006. He is currently a professor and chairs the Department of Information Security, Beijing Jiaotong University, Beijing. His main interests are computer technology, software engineering, and artificial intelligence.