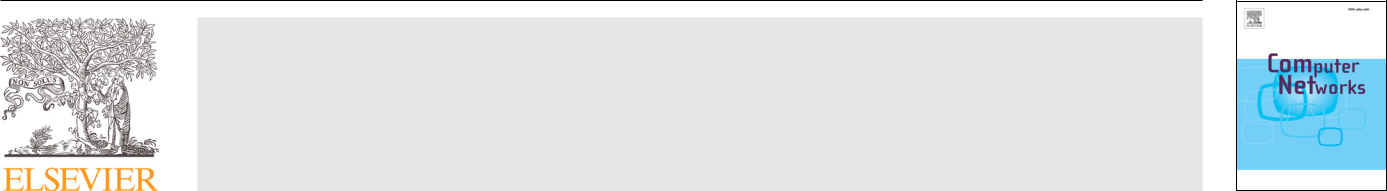
[Computer Networks 176 (2020) 107283](https://doi.org/10.1016/j.comnet.2020.107283)



Contents lists available at [ScienceDirect](http://www.ScienceDirect.com)

Computer Networks

journal homepage: [www.elsevier.com/locate/comnet](http://www.elsevier.com/locate/comnet)

A privacy preserving scheme for vehicle-to-everything communications using 5G mobile edge computing



Iftikhar Rasheed[∗,](#page1) Lin Zhang, Fei Hu

*Electrical and Computer Engineering, The University of Al-abama, USA*

a r t i c l e i n f o

*Keywords:*

Edge computing

5G

Vehicle-to-anything (V2X)

Road condition monitoring

Security and privacy,

a b s t r a c t

Recently much research has been carried out towards the road condition monitoring system for improving the road safety and moving towards modern intelligent transportation system (ITS). 5G-based vehicle-to-everything (V2X) communication oﬀers wider support and enhances the capabilities of road monitoring systems. The road monitoring systems utilizes the vehicles to report road conditions, traﬃc information or accidents to the roadside units (RSUs), which further relays such information to the cloud server for computing and processing. Then the cloud computing network redirects the necessary actions based on the these received reports. The major problem with this type of architecture is that it requires long computational time and causes high network latency. This also leads to poor utilization of bandwidth. As a result, in this paper a new network protocol has been proposed based on edge-based computing. In this paper, we present a new privacy preserving protocol to boost the security in vehicular network, by utilizing the concept of edge-based computing. The major concern in edge-based architecture is that all the data processing is performed at edge nodes which have various security holes. To secure the edge-based processing, we propose the idea of improved certificate-less aggregation sign-cryption scheme (iCLASC) with incorporating the information transmission protocol to formulate the road monitoring data. Confidentiality, integrity, joint authentication, privacy and anonymity are the key components of the security protocol. Lastly, we make the comparisons of the proposed work with the existing works in terms of computational cost, communication overhead and security feature analysis. Our scheme outperform all the previous methods and shows satisfactory security and communication performance requires for 5G-V2X Communication.

**1. Introduction**

5G will bring new capabilities for autonomous vehicles as well as for modern intelligent transportation system (ITS) [[1]](#page11). The feature such as ultra-high throughput (i.e. up to multi-Gpbs with additional unifor-mity), also incorporating the wider bandwidths with advanced antenna systems, would provide an inherent support for some data-intensive ap-plications such as autonomous driving. 5G can achieve a 1*ms* end-to-end latency over a malleable frame structure. It has advanced functionalities like new uplink RSMA non-orthogonal access, which makes 5G meet the low-latency criteria for eﬃcient Vehicle-to-Everything (V2X) communi-cations more easily and eﬃciently than any of the previous available technologies [[2–4]](#page11).

One of the key features required for eﬃcient modern transporta-tion system, especially for the applications such as autonomous driving, would be having correct and accurate knowledge of the road conditions. As the highly dynamic road conditions is diﬃcult to predict.Therefore it is even more diﬃcult to get the road information like traﬃc density, road accident, etc. in the ever-changing road environment. There is a

∗ Corresponding author.

*E-mail address:* [irasheed@crimson.ua.edu](mailto:irasheed@crimson.ua.edu)(I.Rasheed).

need for eﬃcient monitoring of road conditions, which immensely im-pact and improve the overall road safety mechanism and will pave a way for fully autonomous vehicles on the road. In many places the poor weather conditions (snow, freezing rain, storm, etc.) could cause dam-age to vehicles, motorists, pedestrians and roadside properties. There-fore, eﬃcient road monitoring system is critical.

Using advance vehicular technologies like Vehicle-to-Everything (V2X) communications, combined with the eﬀective cloud-supported networks, can be used to formulate road monitoring system. 5G-V2X communications plays an important role in this regard, since we can get road monitoring reports from the vehicles through 5G links with roadside units (RSUs) at a faster rate with lower latency [[5]](#page11). Thus the eﬀectiveness of these monitoring reports would increase as one can re-ceive the real-time road condition reports in less time, which is very im-portant for mission-critical applications like autonomous driving. Some researchers have suggested an eﬀective road condition monitoring sys-tem based on advance vehicular network technologies. One of the key architectures being considered for this purposed concept is cloud-based vehicular network. [Fig. 1](#page2) shows such a vehicular network. It has been

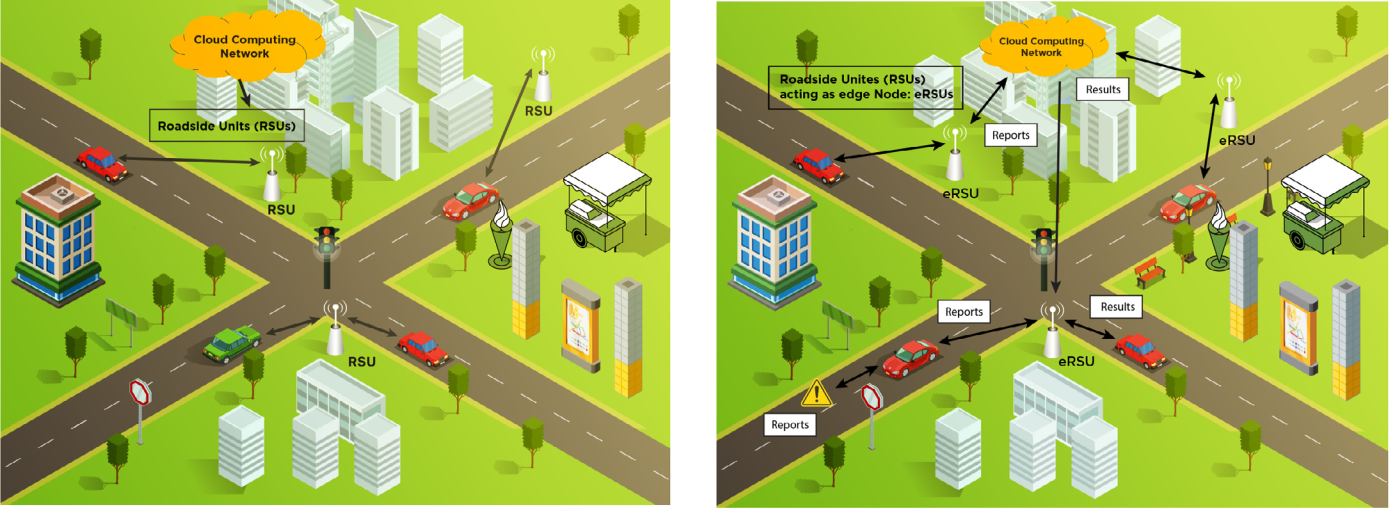
<https://doi.org/10.1016/j.comnet.2020.107283>

Received 20 November 2019; Received in revised form 20 April 2020; Accepted 23 April 2020

Available online 1 May 2020

1389-1286/© 2020 Elsevier B.V. All rights reserved.

*I. Rasheed, L. Zhang and F. Hu* *Computer Networks 176 (2020) 107283*



**Fig. 1.** Vehicular cloud based network. **Fig. 3.** Road monitoring using edge based network.



**Fig. 2.** An example of road monitoring using vehicular network.

used in various applications for intelligent transportation system. It con-sists of roadside units (RSUs), mobile vehicles on the road, and cloud computing infrastructure. The cloud allows an eﬀective way for data collection, analysis, processing and storage. The typical application of such a vehicle network architecture can be seen in [Fig. 2](#page2), where some warning messages or reports about the road conditions monitored by the vehicles can be transmitted through the vehicular network to the RSU, which can transfer the received reports to the cloud servers which pro-cess the corresponding information and suggest the necessary actions to be transmitted back to the RSUs, and the RSUs convey those actions to the vehicles on the road.

The cloud infrastructure plays a vital role in this system for perform-ing computations and maintaining privacy and security of the entire V2X system [[6]](#page11). But this architecture may not be suitable for appli-cations that requires real-time decision making, especially in V2X en-vironments with autonomous vehicles which require fast sensing data processing. The architecture may bring a long response time as all the data processing is performed at the cloud. Thus, it would impact many modern vehicular applications as they require a network topology with high data rates ( *>* 1*Gbps*) and lower latency ( *<* 10 ms). Mobile edge computing can solve this issue, as in this network model the concept of edge processing is adopted, which can avoid possible long delay issue in cloud processing.

The edge-based cloud computing [[7]](#page11) not only achieves lower delay, but also provides higher data rate and wider bandwidth. [Fig. 3](#page2) shows an edge-based vehicular network topology. It oﬀers lower latency with bet-ter location understanding, improves Geo-distribution with an increased support of mobility and real-time data processing. Once reports are be-ing received by an edge RSU (eRSU), it performs all the computation locally and generates the desired actions via reinforcement learning al-gorithms. Then these actions are transmitted to the vehicles. Final con-trol results are delivered to the cloud.

We therefore present a vehicular communication system based upon this edge computing concept. Based on this type of network we fur-ther investigate the security and privacy concept. In these scenarios we are interested in protecting the confidentiality and integrity of the mes-sages to be sent also want to provide joint authentication, privacy and anonymity. Overall we want to provide a privacy scheme that protects the vehicle-related information such as vehicle ID, positions, etc. and it is able to provide location and identity privacy.

As vehicle’s location information can be linked to its owner there-fore the location privacy becomes one of the most important features for an eﬃcient vehicular communication network. Therefore, a vehicu-lar network can be more viable and acceptable to the users if the pri-vacy preserving scheme oﬀered by the network is able to ensure location privacy. Previously various works has been done in providing location privacy in vehicular communication scenarios for example [[8–13]](#page11). In

1. a location privacy centered on pseudonym self-delegated genera-tion with conditional tracking is proposed. In this approach whenever a vehicle changes over its pseudonyms, the location privacy can be as-sured. In [[9]](#page11) Lite-CA-based public key crypt-o-system is used for provid-ing location privacy in vehicular networks. Similarly, a location privacy scheme was suggested by [[10]](#page11) using social-tier dissemination phase, in this phase the vehicles are requested to forward data to its neighboring vehicles or roadside units forming a social spots communication net-work topology. [Lu et al. [11]](#page11) recommended an alternative method us-ing changing pseudonyms and forming a small social spot. This method was able to achieve location privacy in vehicular network. In another work [[12]](#page11) the concept of changing pseudo identities periodically was presented. This also achieves location privacy in vehicular network en-vironment. Similarly, in another work [[13]](#page11) the concept of global social spot and individual social spot are presented for ensuring location pri-vacy in vehicular communication.

Although all these works do provide location privacy in vehicular communications but the main problem with them is that they all require higher computational time with more complex algorithms. Higher com-putational time would mean higher network latency. A network with

*I. Rasheed, L. Zhang and F. Hu* *Computer Networks 176 (2020) 107283*

**Table 1**

Advantages of signcryption over traditional ECC authentication methods.

|  |  |  |
| --- | --- | --- |
| Metrics | Signcryption method | Traditional ECC authentication |
|  |  |  |
| **Computational Cost** | • Lesser Computational Cost | • More Computational Cost ( ~ 60% more) |
| **Communication Costs** | • Low Communication Cost ( ~ 40% less) | • Higher Communication Cost |
| **Message Expansion** | • 70% less in message expansion | • 70% more in message expansion |
| **Security Aspects** | • Higher Security | • Medium Security |
|  | • Unique unsigncryptability | • Do not have unique unsigncryptability. |
|  | • more secured as digital signatures as well as | • Medium Unforgeability |
|  | public key encryption. | • Provides Confidentailty with higher |
|  | • Provides better Unforgeability and | Communication overhead. |
|  | non-repudiation. |  |
|  | • Provides Higher Confidentiality |  |
| **Resources Requirements** | • Low resource requirements | • Higher resource requirements |
|  |  |  |

higher latency is not suitable for vehicular communications especially in case of autonomous driving where we do require a network with lower computational time. More importantly none of these previous works considers 5G-based vehicular networking scenarios.

Identity privacy is another key feature for vehicular communication network. Usually this is done in order to conceal real identity of the ve-hicle and its user. There are numerous previous stated works that focus on providing the identity privacy in vehicular communication network [[14–18]](#page11). In [[14]](#page11) the concept of pseudo-identity and anonymous creden-tial was used to provide the identity privacy in vehicular networking environment. [Lu et al. [15]](#page11) has focused on an approach where the RSU utilizes the activation passwords in order to authenticate the vehicle’s identity and transmits this information to tampered resistant devices for maintaining identity privacy. [Chim et al. [16]](#page11) introduced a policy that utilizes a distinct pseudo identity for each active session between RSU and on the road vehicle. This scheme preserves the identity privacy. In

1. the identity revocation certificates were used to maintain identity privacy in vehicular communication. In [[18]](#page11) the idea of cell-based com-munication and dividing the network into clusters have been proposed. In each cell pseudonyms are assigned to every vehicle for providing identity privacy.

All these above-mentioned identity privacy mechanisms do not pro-vide a systematic approach where identity privacy is incorporated with the location privacy to make vehicular networks more safe and secure. More importantly they do not consider the modern approaches like mo-bile edge communication in 5G-V2X communication scenarios. And they also do not consider network latency factor for their stated solution. Previously some researchers have focused on the protection of data in communication channels [[19–21]](#page11). But very little work has been done in preserving the authenticity and confidentiality for vehicular networks, especially for the case of road monitoring units and their local reports.

There are some key factors that are to be considered in designing an eﬃcient security protocol for road monitoring system using 5G-V2X Communication:

* The road reports should not be accessed during the transmissions by unverified vehicles/users.
* The system should be scalable to large V2X systems, and the gen-erated information should be encrypted and decrypted in the sys-tem eﬀectively, i.e. requiring low computational and communication cost.
* The system should also be able to perform joint authentication among the vehicles, eRSU and cloud computing network. Finally, the security protocols should have low overhead (computation com-plexity, storage space, etc.) and are robust to various threats.

Based upon these stated factors, certificateless public key cryptogra-phy (CLPKC) [[22]](#page11) has been used before. CLPKC evades the key escrow problem that is linked with many identity-based public key cryptogra-phy schemes (IDBC). Here the vehicles’ private keys are distributed via key generation system with a combination of key generation system’s

and the vehicles’ partial private keys. This key generation system does not have any knowledge about the vehicles’ full private key. Addition-ally, the CLPKC does not have to perform certificate management, i.e. it will avoid operations such as revoking, distributing and storing data. Further improvement in the computational and communication cost can be achieved by performing *signcryption*, which means realizing encryp-tion and signature in one step. Further a detail comparison between signcryption method used over traditional ECC authentication can be seen in [Table 1](#page3).

From [Table 1](#page3) it can be seen that signcryption schemes are more ef-ficient methods with lower computational and communication costs as they are able to perform two key steps at once during signcryption and unsigncryption process. Therefore, this makes signcryption methods to be computationally eﬀective as compared to traditional ECC authenti-cation methods. More importantly this reduction in cost does not im-pact on security aspects of these methods, in fact signcryption methods are able to provide higher security levels by ensuring unique unsign-cryptability (i.e. more secured as they have digital signatures as well as public key encryption), better unforgeability and non-repudiation with higher confidentiality. Whereas the Traditional ECC authentication methods provide medium level security as they do not have unique un-signcryptability and have medium level unforgeability with higher com-munication overhead. Moreover, signcryption methods also outperform traditional ECC authentication methods in terms of message expansion performance. In-fact signcryption methods requires 70% lesser message expansion as compare to the traditional approaches.

In this work we will adopt signcryption technique - *c*ertificate*l*ess *s*ign*c*ryption (CLSC), for securing communication that provides Confi-dentiality, integrity, joint authentication, privacy and anonymity. Thus it can lead to overall a privacy scheme that protects the vehicle-related information such as vehicle ID, positions, at much lower computational and communication cost. So providing Confidentiality, integrity, joint authentication, privacy and anonymity eﬀectively are the key compo-nents of our proposed security protocol.

The CLSC was initially proposed by [[23]](#page11). This scheme uses the method of aggregation to reduce the data and the time for signature verification and unsigncryption. This leads to better scalability, lower computational and communication overhead. Some researchers, such as Basudan et al. [[24]](#page11), Lu et al. [[25]](#page11), Wei et al. [[26]](#page11) and Eslami et al. [[27]](#page11), further proposed certificateless aggregate signcryption scheme (CLASC).

But these methods use many pairing and exponentiation operations that yields higher computational cost and increase time consumption which makes them unsuitable for 5G-V2X Communication system. In-fact their performance is much worse when the number of vehicles in-creases in the system. Another major problem of these method is that it only considers pseudo identities which is the hash of vehicle ID. This might not be enough to preserve the rider’s privacy as we will see in later sections. Moreover, vehicular network poses a greater threat as vehicle mobility pattern can be anticipated even if we are changing pseudo iden-

*I. Rasheed, L. Zhang and F. Hu*

tities, as other information like location information for the predicted traﬃc information can be used to tamper the privacy of the vehicles. To overcome these problems, we present the concept of a privacy preserv-ing scheme that has following key features:

* + A new improved and eﬀective certificateless aggregate signcryption (CLASC) scheme by building on the random oracle model that can be utilized in 5G-V2X communication scenario. Here we try to min-imize the pairing and exponentiation operations with the use of ef-ficient weil/tate pairing by using fast reduction elliptic curves. Fast data aggregation is performed. Our method has shown better per-formance and lower computational cost compared to the existing methods [[24–27]](#page11).
  + An eﬃcient privacy preserving protocol that can be used for im-proving security in data transmissions for road monitoring system by using mobile edge computing based on 5G-V2X communication architecture. The suggested method attains data confidentiality, in-tegrity, joint authentication, privacy and anonymity. We will use hybrid method based upon silent period [[28]](#page11) and create mix zones [[29]](#page11) to improve the location and identity privacy of the vehicle.

1. **Background**

This section presents an overview of the edge networking architec-ture, followed by an introduction to the present work for the road mon-itoring system. Then we present the concept of privacy preserving pro-tocol based upon certificateless aggregate signcryption scheme.

*2.1. Mobile edge computing architecture*

Edge networking is a modern networking architecture that of-fers storage, communications, control, configuration, measurement and management between the station connected devices. It provides better geographical distribution and lower network latency [[7,30]](#page11).

In this type of networking environment, a large number of dis-tributed mobile devices manage themselves to connect and possibly co-operate with each other via an edge node located at the edge of the cloud computing network. There are various available architectures and standard layouts [[7]](#page11). The required storage is performed at the near-end users. All the data processing and manipulation like network manage-ment, configuration and controlling, are performed at the edge side of the network.

Edge plays an important role in routing the information to the end users. Edge network topology greatly improves the overall performance of the networks, especially for the mobile networks like vehicular ad-hoc networks (VANETS), since it can be used to collect data from the vehicles without sending data to the cloud. This helps to reduce the over-all latency of network and improves the bandwidth utilization. Overall, the edge-based computing will greatly improve the QoS by decreasing the overall network latency which is very important for mission critical applications of 5G-V2X Communication.

*2.2. 5G-V2X Road monitoring systems*

With the incoming of 5G, V2X communication can be used for real-time road monitoring more eﬀectively and accurately. In [[31–33]](#page11) we can clearly find out that how 5G-V2X application can be applied to road monitoring scenarios. Furthermore, in [[34]](#page11) and [[35]](#page11) the concept of us-ing V2X to help the taxis to get to know the accurate road conditions have been proposed. Especially they look for potholes on the road. In

1. various vehicle sensors were used to formulate road monitoring reports. In [[37]](#page11) presented the secured V2G protocol framework for en-abling the vehicles to communicate or recharge at desired recharging stations. All of these proposed works used the cloud-based computing network structure and thus may suﬀer from high latency problem; which is a great concern for various applications for Vehicular network.

*Computer Networks 176 (2020) 107283*

*2.3. Certificateless aggregate signcryption scheme*

This work will be utilizing the concept of certificateless privacy preservation method based on improved aggregation of signcryption. This certificateless method was first coined by [[22]](#page11). The main reason for using the certificateless approach is to overcome the diﬃculties related to the key escrow problem, which is related to the identity-based encryption methods to preserve the certificate freeness. There are many other methods through which this can be achieved, examples include simple encryption schemes [[38,39]](#page11), digital signature [[40,41]](#page11), signcryption using certificateless methodology [[42,43]](#page11), and so on. As from [Table 1](#page3) we can see some advantages of signcryption scheme over traditional authentication methods. Further Certificateless aggregate signcryption scheme (CLASC) has been proved to be a robust security paradigm [[26,27]](#page11). Therefore, in this work we only focus on the CLASC scheme.

If we analyze Basudan et al. [[24]](#page11) method it does oﬀer integrity and confidentiality. But the major problem with this stated work was it lacks in providing anonymity and joint authentication. Moreover, it also has key escrow problem. The major drawback for this approach was that it has higher computational time and network latency i.e. ~ 20.8 ms which means it is not suitable for mission critical applications for V2X Com-munication like autonomous driving. Lu et al. [[25]](#page11) method provides adequate integrity and confidentiality with better key escrow mecha-nism, but it lacks in providing anonymity and joint authentication. The computational time and latency are very high i.e. ~ 49.7 ms as well thus, not suitable for mission critical applications for V2X Communi-cation like autonomous driving. Wei et al. [[26]](#page11) does oﬀer integrity & confidentiality with better key escrow strength. But it also shows poor performance in providing anonymity and joint authentication. More-over, its computational time and network latency are also very high as compared to Basudan et al. [[24]](#page11), Lu et al. [[25]](#page11) and Eslami et al.

1. i.e. ~ 4522 ms. Hence, not suitable for applications like V2X Com-munication especially autonomous driving. Similarly, if we analyze the Eslami et al. [[27]](#page11) it does oﬀer better computational time and network latency i.e. ~ 1527.7 ms as compare to Wei et al. [[26]](#page11) but it does not provide appropriate integrity, confidentiality, anonymity and joint au-thentication. Therefore, making this method not suitable for safe and eﬃcient V2X Communication. A summary of drawbacks for these meth-ods can be seen in [Table 2](#page5).

The major issue with these schemes is that they require substantial enhancements, particularly in the pairing of maps for lowering compu-tational time and complexity. Thus, we propose an improved and ef-fective CLASC (iCLASC) scheme by building the random oracle model that can be utilized in 5G-V2X communication scenarios. Our proposed work tries to address the limitations of the previous works as shown in [Table 2](#page5).

**3. System model**

This section presents an overview of the proposed system model, cor-responding attack model, and design goals for 5G-V2X communications.

*3.1. System prototype*

5G-V2X communication plays an important role in autonomous driv-ing, where real-time road traﬃc\condition monitoring will be utmost important thing. Thus, we contemplate the architecture with central controller system (CCS), vehicles (equipped with 5G-V2X capability), edge roadside units (eRSUs), and a cloud computing network for moni-toring real-time road condition, as shown [Fig. 4](#page5).

*3.1.1. Central controller system (CCS)*

From [Fig. 4](#page5) we can see that CCS is the command center of our entire proposed work. It is the trustworthy network entity and used for system

*I. Rasheed, L. Zhang and F. Hu*

**Table 2**

Problems with previous privacy preserving schemes.

Methods Issues

**Basudan** et al.[[24]](#page11) **• It does offer Integrity and Confidentiality.**

* But lacks in Anonymity and Joint authentication.
* Key escrow strength also has issues.
* Computational time and latency are also high i.e. ~ 20.8 ms.
* Not suitable for mission critical applications for V2X Communication like autonomous driving.

**Lu** et al.[[25]](#page11) **• It also offers Integrity & Confidentiality.**

* Poor in providing Anonymity and Joint authentication.
* Key escrow strength is better.
* Computational time and latency are very high i.e. ~ 49.7 ms.
* Not suitable for mission critical applications for V2X Communication like autonomous driving.

**Wei** et al.[[26]](#page11) **• It provides Integrity & Confidentiality.**

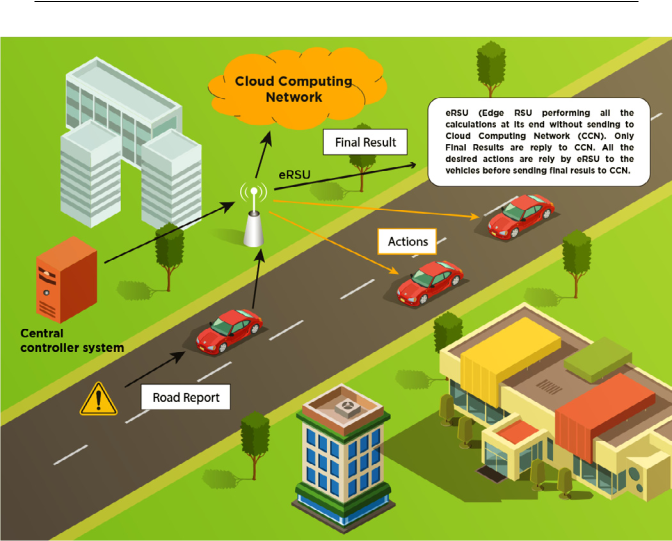
* Poor in providing Anonymity and Joint authentication.
* Key escrow strength is better.
* Computational time and latency are very high i.e. ~ 4522 ms.
* Not suitable for mission critical applications for V2X Communication like autonomous driving.

**Eslami** et al.[[27]](#page11) **• It lacks in providing appropriate Integrity & Confidentiality.**

•Poor in providing Anonymity and Joint

authentication.

* Key escrow strength is better.
* Computational time and latency are very high i.e. ~ 1527.7 ms.
* Not suitable for mission critical applications for V2X Communication like autonomous driving.



**Fig. 4.** Proposed system model.

initialization. It acts as *key generation* center, and it only generates pri-vate keys in bid to prevent any key escrow problem. It is also restricted to access the sensitive data of vehicles and eRSUs. Furthermore, it is assumed that the CCS has adequate computation and storage capacity.

*3.1.2. Vehicles*

Another important element of this proposed work is 5G-enabled ve-hicles. In case of autonomous vehicles or 5G connected vehicles, it is assumed that they generate and process a large amount of data that

*Computer Networks 176 (2020) 107283*

includes location information, time, road safety messages, road moni-toring messages, desired action signals, etc.

*3.1.3. Edge roadside unit (eRSUs)*

Another important entity in this system is edge Roadside unit (eR-SUs) as shown in [Fig. 4](#page5). They are assumed to have mobile edge comput-ing (MEC) capabilities, i.e., having eﬀective computational and storage capacity and reaching out to the cloud services as well as the edge node. eRSUs is fully capable of making decisions and reacting to certain events as it is directly linked with vehicles.

All the real-time information is passed to the eRSUs from the vehicles on the road. After processing this information eRSUs can send further action instructions to the vehicles. For example, it provides warning messages about the road conditions like the accident ahead etc.

*3.1.4. Cloud computing network*

Cloud computing network has the data centers in the system. History reports are kept in the cloud which can be used later. The key advantage of mobile edge computing is that rather than transmitting the data from vehicles to the cloud computing network for further processing, eRSUs perform that work at the edge and only final results are transmitted to the cloud computing network and the connected vehicles as we can see this from [Fig. 4](#page5). This improves bandwidth utilization and decreases the latency, which is a critical factor for 5G-V2X communications, especially for autonomous vehicle case.

*3.2. Attack model*

In this work we assume that the link between the eRSUs and cloud computing network is secure. Therefore, the major target of the attacker is the link between the vehicles and eRSUs. Especially in road events monitoring application the loss of content-oriented privacy may enable the eavesdroppers to reveal the road event information of the vehicle (source) and provide false road information to the vehicle (receiver).

Malicious attackers can also make fake information in order to take control of the entire transmission channel, or they can observe the en-tire data flow in a network channel. Furthermore, message tampering, dropping the packets and changing the entire original message can also be performed. The major concern here is that attacker can apprehend and concede some eRSUs and vehicles as well. In that case all the infor-mation sent or received through these conceded eRSUs and vehicles can be captured and examined by the attacker.

Here we also take into consideration the situation that the eRSU be-comes malicious and sends false reports to the connected vehicles. Con-sequently, a vehicle might also become compromised and start trans-mitting malicious reports for its own advantage.

*3.3. Design goals*

Here we will define the main security performance requirements to assess the security and eﬃciency of the mobile-edge-based 5G-V2X com-munication.

The key security design requirements for this work are as follow:

* K1: Integrity

All the communications that involve information exchanged in the network should not be changed or tampered.

* K2: Confidentiality

The sensitive information of all the involved network entities should remain confidential.

* K3: Anonymity

The vehicles identity must be concealed from a standard message receiver during the process of authentication in order to keep the sender’s vehicle information private.

* K4: Joint authentication

Vehicles and eRSUs should first authenticate each other as it ensures that data exchange will not be corrupted.

*I. Rasheed, L. Zhang and F. Hu* *Computer Networks 176 (2020) 107283*

* + K5: Key escrow strength

As CCS only has partial private keys for the network entities, it is necessary to make sure that any attacker does not have access to the full private keys.

The key performance design requirements for this work are as follow:

* + P1: Smaller Communication overhead with quicker verification pro-cess

Security method should have lower communication overhead and latency, as security scheme must process a great number of report signatures that are needed to be authenticated first followed by un-signcrypted in a very short time.

* + P2: Robustness

The system should be robust as the information generated by ve-hicles must not be accessed in the situation that private keys are compromised.

* + P3: Lower Computation Cost

Although vehicles will be equipped with 5G-V2X equipment but still have restricted power and storage capacity. Thus the proposed work should have lower computational cost so that it can work eﬃciently under such limited constraints.

1. **Proposed improved CLASC (iCLASC)**

In this section we will present our proposed improved CLASC (iCLASC) method that can be used as privacy preserving protocol for 5G-V2X based upon mobile edge computing. This work is enhancement of the previous work by [[24,26]](#page11). In these works, bilinear mapping was used; but these approaches have high computation complexity and time because a large number of pairing operations are performed during var-ious stages of iCLASC scheme. Although Basudan et al. [[24]](#page11) did try to minimize the computational complexity by reducing the number of pair-ing operations; but its results were not satisfactory. In our scheme we will minimize the pairing operations with the use of eﬃcient weil/tate pairing by using fast reduction elliptic curves. [Table 3](#page6) provides the no-tation guide used in this work.

The Improved and eﬃcient iCLASC scheme is composed of the fol-lowing phases:

*4.1. Phase1: Initializing the network entities phase*

The security parameters are defined as *p*. Key generation is initiated based on *p*. Next the selection of a cyclic additive group *AG* with prime order of *n* is performed by using fast reduction elliptic curve which was not present in the previous work. Arbitrary generator *L* is generated from *AG*. Multiplicative cyclic group *AGM* of the prime order *n* is formed byusing bilinear mapping:

*̂*= × → .

Now we can randomly pick up a master private key ∈ ∗ for cal-

culating the public master key = . Next we choose four protected hash functions:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ∶ {0*,* 1}∗ → | | | | | ∗ |  |
|  | 1 | |  |  |  |  |
| *Has* | 2 | : {0, 1}∗ | | → {0, 1}*nb* where *nb* is the bit-length of plaintexts. | |  |
|  | : {0, 1}∗ | |  |  |  |
| *Has* | 3 | → *AG* |  |  |
| ∶ | | | ∗ → | |  |  |
|  | 4 | |  |  |  |  |

Note that these hash operations are performed in parallel so that computational time can be decreased. Further the pairing operations are performed with eﬃcient weil/tate pairing by using fast reduction elliptic curves. These approaches were not followed in the previous works. After these hash operations all the parameters are published, i.e.,

{ =  *, , ,̂ , ,*  *, , , ,* } Here the

1 2 3 4

private keys are maintained by the CCS.

*4.2. Phase2: Keys generation phase*

The algorithm is repeatedly run via various vehicles using *,* and

CCS generates the keys as follows: The vehicle using randomly

chooses a secret value, i.e., ∈ ∗*,* and finds out partial public key

for corresponding vehicle =  *.*Next the vehicle sends out its and *Ziy* as ( , *Ziy*) to the eRSU.

Now the eRSU randomly selects some secret value: ′ ∈ ∗*,* and finds

′

out partial public key for corresponding vehicle = . Therefore the

complete public key for the vehicle is (*Ziy*, *Zix*).

The eRSU calculates the partial private key as follows:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | = ′ | + ∗ |  | where |  | =( | ). And this partial private key |  |
|  |  |  |  | 1 |  |  |

is sent to the vehicle .

**Table 3**

Notation Guide.

|  |  |
| --- | --- |
| Symbol | Definition |
|  |  |
| eRSU | Edge Roadside unit |
| CCS | Central Controller System |

* security parameters

*AG* cyclic additive group

* Arbitrary generator

*̂* Bilinear Mapping

*AGM* Multiplicative cyclic group

*si* secret value

* master private key

|  |  |  |  |
| --- | --- | --- | --- |
| *Ki* |  | partial private key |  |
| *Lpub* |  | public master key |  |
| *Has* (.) |  | Fast Hash Operation |  |
|  |  | Sender’s ID |  |
| (*Ziy* , *Zix* ) |  | public key for the vehicle |  |
|  |  | Receiver’s ID |  |
| *i* |  | Signcrypt function |  |
| *CT* |  | Aggregated ciphertext |  |
| \_ |  | Exclusive OR operation |  |
|  | Aggregated Road Reports |  |
|  | |  |  |
| *Tij* |  | The time when vehicle *i* is transmitting the data for event *j* |  |
| *Lij* |  | the location of the roadside event with respect to vehicle position. |  |
| *Aij* |  | The action which contains details of the roadside event. |  |
|  |  | Adversary |  |

* Challenger

*mmi* Message

*⊥*False

*I. Rasheed, L. Zhang and F. Hu*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Once vehiclehas received the partial private key, it will now | | | | | |  |
|  |  |  |  |  |  |  |
| validate this received key as below: | | | | | |  |
|  | = | + |  | ( | ). |  |
|  |  |  | 1 |  |  |

In this phase three main steps are performed:

* Setting the Secret Value;
* Partial private key generation and extraction;
* Setting the public key.

Once these three main steps are performed the generated public key

{(*Ziy*, *Zix*)} is kept at CCS in public tree, whereas full private key {(*si*, *Ki*)} is hidden from the vehicle.

*4.3. Phase3: Signcrypt phase*

Here the transmitting vehicle performs the signcryption of the

message *mmi* with the ID of receiving vehicle . The key steps in-

volved are as follows:

The sender vehicle randomly selects *t* ∈ *Y*∗*n* and calculates =

.

Next it finds = .

Then it finds = ( + ).

Now it can calculate the parallel fast hash function as below:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *ℎ* |  | =( |  | ∥ | ∥ | ∥ △ ∥ | | ∥ |  | | ∥ |  | ) |  |  |  |
|  | 2 |  |  |  |  |  |  |  |  |  |  |
|  | | = *ℎ ⊕* | |  |  |  |  |  |  |  |  |  |  |  |  |  |
| *ℎ* |  | =( |  | ∥ | ∥ | ∥ △ ∥ |  | ∥ | | ∥ | |  | ∥ | ∥ | ) |  |
|  | 3 |  | |  |  |  |  |  |  |  |  |  |
| *ℎ* |  | =(△) | |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 4 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

After finding these parallel fast hash functions we compute the Sign-crypt function as below:

= *ℎ*+ *ℎ*+ *ℎ*

After all these steps we will get the ciphertext as:

=( *, ,* )

*4.4. Phase4: Aggregation phase*

In this phase the aggregation is performed based on the signcryption function found in phase 3 for the receiving vehicle .

∑

=

=1

Therefore, the aggregated ciphertext is:

=( 1… *,* 1… *,* )

*4.5. Phase5: Aggregate verification phase*

In this phase aggregate verification is performed by using the re-ceiver’s .

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *ℎ* |  | =( | |  | ∥ | ∥ | ∥ △ ∥ | | | ∥ | ∥ |  | ∥ | ∥ | ) |  |
|  | 3 |  |  |  |  |  |  |  |  |  |  |  |  |
| For = 1 … … *,* | | | | | |  |  |  |  |  |  |  |  |  |  |  |
| *ℎ* |  | =(△) | | |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 4 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Verification is then performed: | | | | | | | |  |  |  |  |  |  |  |  |  |
| *̂*( *,* ) = *̂*( | | |  |  |  |  |  | ) *̂*( |  | |  |  |  |  |  |  |
| ∑ | |  |  |  | ∑ | |  |  | ∑ | |  |  |
| =1( +*,ℎ* | | | | | =1*,* | | | ) *̂*( | | =1*,* ) | |  |

If this equation is verified, then the output is correct; otherwise, it can not trust the output.

*Computer Networks 176 (2020) 107283*

*4.6. Phase6: Aggregation unsigncrypt phase*

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | After the verification of the aggregation calculations, the receiver | | | | | | | | | | | | | | | | |  |
| vehicle | | |  | performs aggregate-unsigncrypt operation. | | | | | | | | | | | | |  |  |
|  |  | |  | ′ = | |  |  |  | and ′ = | | | |  |  |  |  |  |  |
|  | It finds | |  |  | |  |  |  |  |  |  |  |
|  |  |  | | |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Next it will compute hash for these found quantities. | | | | | | | | | | | | | | | |  |  |
| *ℎ*′ | =( | |  | | ∥ | |  |  | ∥ |  | ∥△∥∥ ′∥ | | | | | ′ ) |  |  |
|  | 2 |  |  |  |  | | |  | |  |  |  |  |  |  |  |
| And retrieving the received message | | | | | | | | | | | | | | ′ | |  |  |  |
|  | |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |
|  | ′ |  |  | ′ |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| = | | | | *ℎ* |  |  |  |  |  |  |  |  |  | |  |  |  |  |
| The received message will be: { } =1 | | | | | | | | | | | | | | |  |  |  |  |
| *4.7. Phase 7: Signature accuracy and correct message after decryption* | | | | | | | | | | | | | | | | | |  |
|  | For signature accuracy we can perform the following tests: | | | | | | | | | | | | | | | | |  |
| *̂*( *,* ) = *̂*( | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| ∑ | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| =1*,*) | | | | | | |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | |  |  |  |  |  |  |  | ) |  |  |  |  |  |  |
|  | ∑ ( | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | =  *̂*( | =1 | | | *ℎ* | | | + *ℎ* + *ℎ* | | | | *,* ) | | |  |  |  |  |
|  |  |  |  | |  |  |  |  | ) *̂*( | |  |  |  |  |  |  |  |  |
|  | ∑ | | | |  |  |  |  | ∑ |  |  |  | ∑ |  |  |  |
|  | =  *̂*( | =1  *,* *ℎ* | | | | | | | =1 *, ℎ* ) *̂*( | | | | =1  *,ℎ* ) | |  |  |
|  |  |  |  | |  |  |  |  | ) *̂*( | |  |  |  |  |  |  |  |  |
|  | ∑ | | | |  |  |  |  | ∑ |  |  |  | ∑ |  |  |  |
|  | =  *̂*( | =1  *,* *ℎ* | | | | | | | =1*,ℎ* | | | ) *̂*(=1 *, ℎ* ) | | |  |  |
|  |  |  |  | |  |  |  |  |  |  |  |  |  |  |  |  | ) |  |
|  | ∑ | | | |  |  |  |  |  |  |  |  |  | ∑ |  | ∑ |  |
|  | =  *̂*( | =1 ( +)*,ℎ* ) *̂*( =1 *,ℎ* ) *̂*( =1 *,ℎ* | | | | | | | | | | | | | | |  |
| As =  *,* | |  |  | =and=+. | | | | | | | | | | | | |  |  |

For accurate message decryption, we can perform the following com-putations:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ′ | = |  | ′ |  |  |
|  | *ℎ* |  |  |
|  | =2(∥∥∥△∥∥∥) | | | *ℎ*′ |  |

* *ℎℎ*′=

Thus, we obtain the original accurate message.

1. **Proposed improved and eﬃcient privacy preserving protocol for 5G-V2X communication using mobile edge computing**

This section presents the details of our proposed improved and eﬃ-cient privacy preserving protocol for 5G-V2X communication by using mobile edge computing. In this work we have considered roadside units to be acting as edge nodes (eRSUs), and they are immediate in con-tact with the vehicles on the roads capable of 5G-V2X communications. These eRSUs are further connected with cloud computing network. The major application we are considering is to obtain road monitoring re-ports (*RMR*).

This work consists of four key stages: (1) parameter initialization stage, (2) data encryption and transmission stage, (3) road monitoring reports (*RMR*) aggregation and its authentication stage, and (4) lastly secured data extraction stage.

*I. Rasheed, L. Zhang and F. Hu*

*5.1. Parameter initialization stage*

First of all, the vehicles on the road and eRSUs have to register them-selves with the CCS so that their private keys and public keys can be generated. At this point the pattern for road monitoring reports (*RMR*) is also considered and routing path is established.

Security parameters are also defined as *p*. Key generation is initiated for security parameters *p*. Next it selects a cyclic additive group *AG* with prime order of *n* using fast reduction elliptic curve. Arbitrary generator *L* is generated from *AG*. Multiplicative cyclic group *AGM* of the prime

order *n* is formed using bilinear mapping  *̂* = × → .

Now we can randomly select a master private key *k* ∈ *Y*∗*n* and calcu-late the public master key = . We choose four protected parallel

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| fast processing hash functions *Has* | | | | 1 | : {0, 1}∗ → *Y*∗ | | |  | *Has* | 2 | : {0, 1}∗ → {0, |  |
|  |  |  |  |  |  | *n* | |  |  |  |
| 1}*nb*, where *nb* is the bit-length of plaintexts, *Has* | | | | | | | | 3 | : {0, 1}∗ → *AG*, and | | |  |
| ∶ | ∗ →  *.* After this it publishes all the parameters, i.e.: | | | | | | | | | | |  |
| 4 |  |  |  |  |  |  |  |  |  |  |  |  |
| {=  *, ,* | | *,̂ , ,* |  | | | *, , , ,* } | | | | | |  |
|  |  |  | 1 | 2 |  | 3 |  | 4 |  |

The format of *RMR* is set up for the event along the roadside. *eRSUi*

will generate the information = { *,* *,* }*,* where *Tij* is

the time when vehicle *i* is transmitting the data for event *j*; *Lij* is the location of the roadside event with respect to vehicle position, and *Aij* is the action which contains details of the roadside event.

Now the vehicle will forward this report to the eRSU as: =

( )

( *,* )*,* where *Ni* is the hash of vehicle ID so that

vehicle privacy can be kept, and *Sigcrypt* is signcryption algorithm for the data to be sent.

The vehicle using randomly chooses some secret value, i.e. ∈

∗*,* and finds out partial public key for the corresponding vehicle= *.*

Now the eRSU sends its identity and partial public key, i.e. (*Zi*, *Zix*), to CCS for registration purpose. CCS randomly selects some secret value ′ ∈ ∗ and finds out partial public key for the corresponding vehicle

= ′ *.*

Therefore the complete public key for the vehicle is (*Ziy*, *Zix*). Next

′

the CCS calculates the partial private keys = + ∗ where =

( )*,* and this partial private key is sent to the eRSU through the

1

protected transmission channel. The generated public key {(*Ziy*, *Zix*)} is kept at CCS in public tree.

Vehicle receives the partial private key *Ki* and adds its secret value *si* to form full private key (*Ki*, *si*). The validation can be done

through:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | = | + |  | ( | ). |  |
|  |  |  | 1 |  |  |

*5.2. Data encryption and transmission stage*

Road monitoring results will be reported by multiple vehicles trav-

elling on that road at certain time. A road event report will be =

( )

( *,* )*,* where *Ni* is the hash of vehicle ID so that

vehicle privacy can be kept, and *Sigcrypt* is signcryption algorithm for the data to be sent. This data will be put forward to the improved cer-tificateless scheme with fast reduction elliptic curves and parallel fast hash function.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | For example, Sender Vehiclerandomly selects ∈ | | | | | | | | | | | | | | | ∗ | and cal- |  |
| culates | | | = . | | |  |  |  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | Then it calculates = *,* and finds = ( +). | | | | | | | | | | | | | | | |  |  |
|  |  | Now it calculates the parallel fast hash function as below: | | | | | | | | | | | | | | |  |  |  |
| *ℎ* |  | =( | |  | ∥ | ∥ | ∥ △ ∥ | | ∥ |  | | ∥ |  | ) |  |  |  |  |  |
|  | 2 |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | | = *ℎ ⊕* | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| *ℎ* |  | =( | |  | ∥ | ∥ | ∥ △ ∥ |  | ∥ | | ∥ | |  | ∥ | ∥ | ) |  |  |  |
|  | 3 |  |  | |  |  |  |  |  |  |  |  |  |  |  |
| *ℎ* |  | =(△) | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 4 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

*Computer Networks 176 (2020) 107283*

Now after finding these parallel hash functions we can compute the Sign-crypt function:

= *ℎ*+ *ℎ*+ *ℎ*

After all these steps we can get the ciphertext as:

=( *, ,* )

|  |  |  |
| --- | --- | --- |
| Basically, the following result is sent out: | | |
| The | ( | ) |

= =( *,* *,* )

major problem of this method is that it only considers pseudo identity, i.e., *Ni*, which is the hash of vehicle ID. This might not be enough to preserve the rider’s privacy. Moreover, vehicular network poses a greater threat as vehicle mobility pattern can be anticipated even if we are changing pseudo identities, as other information like lo-cation information for the predicted traﬃc information can be used to tamper the privacy of the vehicles.

To solve this problem, various approaches are used, for example, we may use silent period [[28]](#page11) and create mix zones [[29]](#page11).

In our proposed work we will use hybrid method based upon these two methods. First of all, mix zone approach will be adopted when the vehicles will be approaching any junction (can be an intersection). They interact with eRSU and alter their pseudo identities simultane-ously. Therefore, their corresponding public and private keys will be also updated.

Next, we can use silent period method when the vehicle travels to deliver unlink-ability to a vehicle entering the network, by enforcing that the vehicle will remain silent for a randomly chosen period of time. By incorporating this hybrid method, the overall privacy preservation for this proposed work can be improved and the whole network becomes more secure.

*5.3. Road monitoring reports (*RMR*) aggregation and its authentication*

The protection target which we consider here is the interaction be-tween a vehicle and the eRSU. Road monitoring will be reported by multiple vehicles travelling on that road at certain time. A road event report will be having various key information related to time, location and action. Many vehicles on the road would mean a large amount of data, i.e., a greater number of reports. Thus, eRSU must receive each piece of data separately and perform signature verification/unsigncrypt operations. This would mean a longer delay or latency.

In order to overcome this issue, we utilize the mobile edge comput-ing concept to eﬃciently reduce the computational cost and improve the bandwidth utilization. In this work we have used the concept of ef-ficient data aggregation for these multiple reports. If *nb* is the number of vehicles sending the road monitoring reports to eRSU, i.e., the number of reports will be *nb*. The ciphertexts produced by these mobile vehi-cles will be = ( *, ,* ) with ( ) =1*,* where *Ni* is the hash of each

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| sending vehicle identity, i.e., |  | =( | ) for state information that |  |
|  | 1 |  |  |

can be stated as △. This state information is basically a secret value to protect the aggregation step.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Next, we calculate the signature aggregation: | | |  |
|  |  |  |  |  |
| = | ∑ |  |  |  |
|  |  |  |  |
|  | =1 |  |  |  |
|  | The aggregated reports can be written as, | | |  |
|  |  |  | …*,*1… *,*) |  |
| \_=(( )=1 | | *,* 1 |  |

After this we need to perform batch verification for this aggregated ciphertext concurrently. This is done by using the receiver’s identity, i.e., .

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *ℎ* |  | =( |  | ∥∥ | ∥ △ ∥ |  | ∥ | ∥ |  | ∥ | ∥ | ) |  |
|  | 3 |  |  |  |  |  |  |  |  |

For = 1 … … *,*

*ℎ*= (△)

4

*I. Rasheed, L. Zhang and F. Hu*

The verification process is as follows:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| *̂*( *,* ) = *̂*( |  | ) *̂*( |  | ) *̂*( |  | ) |  |
| ∑ | ∑ | ∑ |  |
| =1( +*,ℎ* | =1*,* | =1*,* |  |

If this equation is verified, then the output is correct; otherwise, it cannot trust the output. Further unsigncryption step can be performed.

*5.4. Secured data extraction*

Here eRSU will decrypt the *RMRs* after signature verification is done to recover the original message:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ′ | = |  | ′ |  |  |
|  | *ℎ* |  |  |
|  | =2(∥∥∥△∥∥∥) | | | *ℎ*′ |  |

* + *ℎℎ*′=

1. **Security analysis** In this section the analysis of security performance achieved by our

proposed work is presented.

*6.1. K1 & K2: Integrity and confidentiality*

As the vehicle sends road monitoring report *ReportDataj* as = ( *, ,* )*,* i.e., in Signcrypt form, and *Txi* and *Pi* satisfy the encryption criteria, and *i* will provide digital signature. The unsigncryption can be only done by eRSU by finding these parameters. Therefore, this en-cryption and signature will provide confidentiality and integrity in our proposed work. For better analysis lets evaluate the proposed security approach by using game theory analysis and show that the proposed work eﬀectively provides data confidentiality and integrity.

*6.1.1. Game 1*

Let’s consider a scenario where an attacker/adversary ( ) and Chal-lenger (*c*) plays a game that ensure the confidentiality of the data being transmitted. The Challenger (*c*) takes security parameter *p* and computes public master key *Lpub* private master key *k* and parameters (*para*). It sends *para* to the Adversary ( ). Next Adversary ( ) starts the polyno-mially bounded number of the above queries. In next step the Adversary ( ) sends out ( *, ,* ) where *mmi* is the road report and

is sender vehicle ID and is receiver ID. We can also see here that

’s full private key has not been extracted by the Adversary ( ). Simi-

larly, the ’s partial private key has not been extracted and its public

key has not been substituted concurrently. The Challenger (*c*) chooses

*Y* ∈{0, 1} randomly and perform the proposed algorithm with( *,*

*,* ) and transmits these results to the Adversary ( ).

Adversary ( ) further enquiries adaptively. But, the full private key

for may not be extracted by Adversary ( ) and the partial private

key for may not be extracted if the public key of has been

replaced in as above mentioned step. Only after the public key \_ or \_ has been replaced, CLASC-unsigncrypt query on *mmY* with sender and receiver is allowed.

At the Guess Stage: Adversary ( ) outputs his guess ′ and if ′ = Then Adversary ( ) wins the game. Thus, we can write an expression for advantage for an adversary ( ) for our proposed work is:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| = | [ | = |  | ] − 2 | |  |
|  | ′ |  |  | 1 | |  |
|  |  |  |  |  |  |  |
|  |  |  |  |

As this advantage will be considered negligible. Thus, the proposed work is well secured against eﬀective Adversary ( ), Therefore making confidentiality criteria to hold.

*Computer Networks 176 (2020) 107283*

*6.1.2. Game 2*

Let’s consider a scenario where an attacker/adversary ( ) and Chal-lenger (*c*) plays a game that ensure the Unforgeability of the data being transmitted. The Challenger (*c*) takes security parameter *p* and computes public master key *Lpub* private master key *k* and parameters (*para*). It sends *para* to the Adversary ( ). Next Adversary ( ) starts the queries

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ∗ | ∗ | *,* | ∗ | ). |  |
| process (like above). Further Adversary ( ) sends out ( *,* |  |  |  |
|  |  |  |  |
|  |  |  |  |  |  |

It must not be an output of the CLASC-signcrypt query. The full private

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| key of ∗ | must not be extracted by adversary ( ) during the Train- | | |  |
|  |  |  |  |  |
|  |  |  |  |  |
| ing Phase. Moreover, the adversary ( ) must have not replaced ∗ | | | ’s |  |
|  |  |  |  |  |
| public key and extracted ∗ | |  |  |  |
| ’s partial private key simultaneously. If | |  |
|  |  |  |  |  |
|  |  |  |  |  |

the output of CLASC-unsigncrypt is not *⊥*, adversary ( ) wins the game. Therefore, the proposed work is well secured against eﬀective Adversary ( ).

*6.2. K3: Anonymity*

In this work eRSU receives the pseudo identity *Ni*, which is obtained

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| from the vehicle identity |  | = | | . This would be mean that |  |
|  |  | 1 |  |  |
| no one is able to find out exact | | | identity of the vehicle during the whole | |  |
| ( | ) |  |

transmission process. Thus the anonymity is achieved. Further we have used hybrid method based upon silent period and mix zone approach. First of all, mix zone approach will be adopted when the vehicles will be approaching any junction (can be an intersection). They interact with eRSU and alter their pseudo identities simultaneously. Therefore, their corresponding public and private keys will be also updated. Next, we can use silent period method when the vehicle travels to deliver unlink-ability to a vehicle entering the network, by enforcing that the vehi-cle will remain silent for a randomly chosen period of time. By incor-porating this hybrid method, the overall privacy preservation for this proposed work can be improved and the whole network becomes more secure.

*6.3. K4: Joint authentication*

eRSU can verify the signcryption on the road monitoring report pro-duced by the vehicle. Especially eRSU only needs to use the private key to perform unsigncryption. The vehicle only calculates the *Zix* and *Zty* through this method to provide joint authentication. eRSU will verify *RMR* by authenticating the signcryption on the received data from thevehicles. Thus, the attacker cannot duplicate the signature without full private key.

*6.4. K5: Key escrow strength*

This work achieves key escrow strength as it is based on certificate-less public key cryptography. Even the CCS can only produce the partial private key which are further used to calculate the full private key by the corresponding eRSU or vehicle. Thus if the CCS is conceded, we still make sure that attacker cannot get eRSU or vehicles’ full private key.

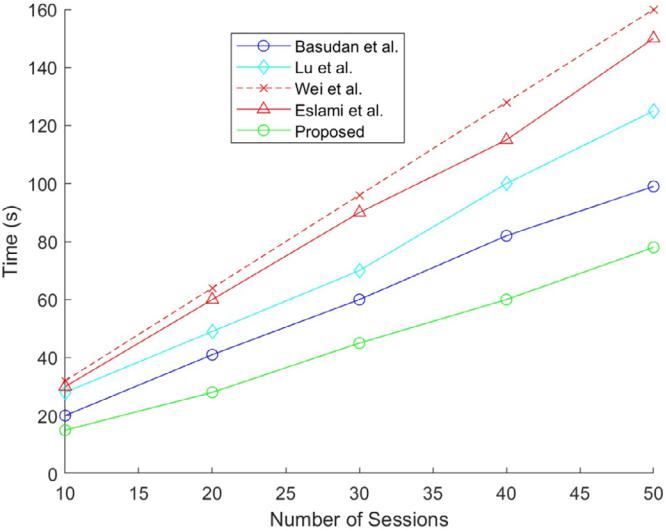
**7. Performance evaluation**

We have evaluated the performance for our proposed work based on the following important performance metrics, i.e., computational cost and communication overhead, network latency and security features.

To establish the eﬃciency and accuracy of this work, we have com-pared our work with [[24–27]](#page11) previous approaches. These works suﬀer from pairing and exponentiation problems which take much computa-tion time, therefore impacting the latency of the network, which is very critical for 5G-V2X communication. We require extremely low latency for various mission critical applications, especially for autonomous driv-ing.

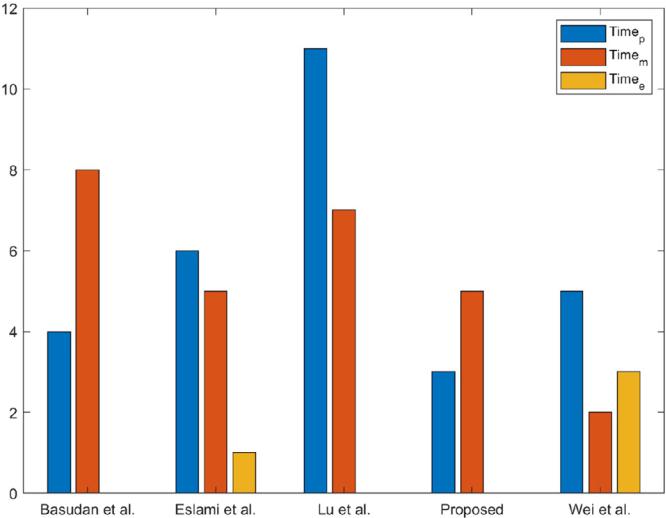
*I. Rasheed, L. Zhang and F. Hu* *Computer Networks 176 (2020) 107283*

**Table 4**

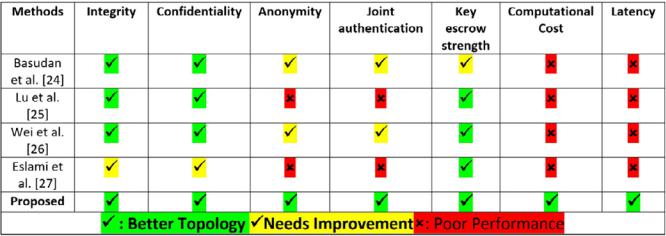


Comparison in terms of pairing, multiplication and exponentiation time.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Methods | Signcryption Phase | |  | UnSigncryption Phase | | |
|  |  |  |  |  |  |  |
|  | *Timep* | *Timem* | *Timee* | *Timep* | *Timem* | *Timee* |
|  |  |  |  |  |  |  |
| Basudan et al. [[24]](#page11) | 0 | 6 | 0 | 4 | 2 | 0 |
| Lu et al. [[25]](#page11) | 1 | 5 | 0 | 10 | 2 | 0 |
| Wei et al. [[26]](#page11) | 3 | 1 | 2 | 2 | 1 | 3 |
| Eslami et al. [[27]](#page11) | 1 | 4 | 1 | 5 | 1 | 0 |
| **Proposed** | **0** | **4** | **0** | **3** | **1** | **0** |
|  |  |  |  |  |  |  |



**Fig. 6.** Number of Session vs Time.



**Fig. 5.** Eﬃciency Comparisons.

**Fig. 7.** Security feature analysis.

*7.1. Computational cost and communication overhead*

To find computational cost we have considered three time-related metrics:

* *Timep*: Time taken for pairing;
* *Timem*: Time needed for multiplication;
* *Timee*: Time needed for exponentiation process.

[Table 4](#page10) shows a detail comparison between the proposed work and other preexisting works. During the signcryption algorithm the total multiplication performed are four with zero pairing time and no ex-ponentiation is needed for our proposed work. Whereas in case of Un-signcryption phase our method only requires three pairing operations with one multiplication operation. As seen from the [Table 4](#page10) and [Fig. 5](#page10), our proposed work requires less pairing time and multiplication time compared with previous works.

The measured values for *Timep* is 4.2 ms, *Timem* is 0.5 ms, and *Timee* is 1.5 s. Therefore we can compute the exact total time taken by each algorithm as shown in [Table 5](#page10). The proposed work has shown to take less time than all other works in this regard. In terms of communica-tion overhead, the proposed algorithm showed similar communication overhead, which is due to the fact that certificateless scheme requires two parts of ciphered data for decryption. Further + 1 elements are

**Table 5**

needed in additive group *AG*. Thus, we have achieved less computa-tional cost without increasing the communication overhead. The pro-posed work requires less computational time, as compared to the previ-ous works.

For better understanding and evaluation of the proposed work, we consider multi-session performance metric which will provide better un-derstanding if the number of vehicles sending the reports has increased. From [Fig. 6](#page10) we can compare the result in terms of total time vs. number of sessions. Here the proposed work outperforms the existing works. The overall impact of the number of sessions being increased has the minimum eﬀect, compared with other works.

*7.2. Security features*

[Fig. 7](#page10) provides a detail security analysis of the proposed work. It can be seen that the proposed work provides a better privacy-preserving methodology for 5G-V2X communication environment, as it provides integrity, confidentiality, anonymity, joint authentication and better key escrow strength at lower computational cost and lower network latency.

Computational cost and communication overhead.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Methods | **Total time equation** | | | | | | | | Time | Communication OverHead | | | | | | | |  |
|  |  | |  | | | |  |  |  |  | |  |  | | | |  |  |
| Basudan et al. [[24]](#page11) | 4 | | + 8 | | | | + 3 |  | 20.8 ms | ( +1) | |  | + | | | | | |  |
|  | 5 |  | + 2 |  |  | |  | ( | + 1) |  |  | + | | |  |  |
| Lu et al. [[25]](#page11) | 11+7 | | | | | | |  | 49.7 ms | ( +1) | |  | + | | | |  | | |  |
|  |  | | | | | |  |
|  | 6 |  | + 5 |  |  | | + 1 |  | ( | + 1) | | | | | + | | |  | | |  |
| Wei et al. [[26]](#page11) |  |  |  |  | |  |  |  | 4522 ms |  |  |  | | |  | | |  |
|  |  |  | | ( | + |  |  | | |  |
|  |  | **+** | |  |  |  | + 1) | | | | | | |  |
| Eslami et al. [[27]](#page11) |  |  |  |  | |  |  |  | 1527.7 ms |  |  | | | | |  |  |  | | |  |
|  |  |  |  |  |  |  |  |  |  |  |  | | | | |  | | |  |  |
| **Proposed** |  |  |  |  |  |  |  |  | **15.1 ms** |  |  |  | | |  | | |  |
|  |  |  |  |  |  |  |  |  |  | | |  |
|  |  |  |  |  |  |  |  |  |  |  |  | | | | |  | | |  |  |

*I. Rasheed, L. Zhang and F. Hu*

**8. Conclusions**

In this paper, we have presented an improved privacy-preserving protocol for boosting the security in vehicular network being used for road monitoring system, by utilizing the concept of edge-based comput-ing. As edge-based structure has major concerns regarding the security and privacy of the vehicle, we have used the idea of improved certificate-less aggregate signcryption scheme (iCLASC) that was shown to be very eﬀective. Based on this method an information transmission protocol is presented for formulating the road monitoring reports. Confidentiality, integrity, joint authentication, privacy and anonymity are the key pa-rameters considered while formulating this security protocol. Lastly the comparison of proposed work with the existing works is performed in terms of computational, communication overhead and security analysis is performed.

**Author Statement**

I am submitting a manuscript for consideration of publication in El-sevier Computer Network journal. The manuscript is entitled “A Pri-vacy Preserving Scheme for Vehicle-to-EverythingCommunications Us-ing 5GMobile Edge Computing”.

It has not been submitted simultaneously for publication elsewhere.

Thank you very much for your consideration.

**Declaration of Competing Interest**

The authors declare that they do not have any financial or nonfinan-cial conflict of interests

**Supplementary material**

Supplementary material associated with this article can be found, in the online version, at doi:[10.1016/j.comnet.2020.107283](https://doi.org/10.1016/j.comnet.2020.107283).

**References**

1. [M. Yao, M. Sohul, V. Marojevic, J.H. Reed, Artificial intelligence defined 5G radio](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0001) [access networks, IEEE Commun. Mag. 57 (3) (2019) 14–20.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0001)
2. [Z. Lin, X. Du, H.-H. Chen, B. Ai, Z. Chen, D. Wu, Millimeter-wave propagation mod-eling and measurements for 5G mobile networks, IEEE Wireless Commun. 26 (1)](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0002) [(2019) 72–77.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0002)
3. [A. Vladyko, A. Khakimov, A. Muthanna, A.A. Ateya, A. Koucheryavy, Distributed](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0003) [edge computing to assist ultra-low-latency vanet applications, Future Internet 11](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0003)

[(6) (2019) 128.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0003)

1. I. Rasheed, F. Hu, Y. Hong, B. Balasubramanian, Intelligent vehicle network routing with adaptive 3d beam alignment for mmwave 5g-based v2x com-munications, IEEE Transactions on Intelligent Transportation Systems (2020), doi:[10.1109/TITS.2020.2973859](https://doi.org/10.1109/TITS.2020.2973859). 1–13
2. [S. Kekki, W. Featherstone, Y. Fang, P. Kuure, A. Li, A. Ranjan, D. Purkayastha,](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0005) [F. Jiangping, D. Frydman, G. Verin, et al., Mec in 5g networks, ETSI white paper](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0005) [28 (2018) 1–28.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0005)
3. N.P. Saraiya, L.M. Matter, A. Rishi, Method and system of scaling a cloud computing network, 2015, US Patent 8,989,187.
4. [R. Roman, J. Lopez, M. Mambo, Mobile edge computing, fog et al.: a survey and](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0006) [analysis of security threats and challenges, Future Generation Computer Systems 78](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0006) [(2018) 680–698.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0006)
5. [R. Lu, X. Lin, T.H. Luan, X. Liang, X. Shen, Pseudonym changing at social spots: an](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0007) [eﬀective strategy for location privacy in vanets, IEEE Trans. Veh. Technol. 61 (1)](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0007) [(2011) 86–96.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0007)
6. [K. Mershad, H. Artail, A framework for secure and eﬃcient data acquisition in ve-hicular ad hoc networks, IEEE Trans. Veh. Technol. 62 (2) (2012) 536–551.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0008)
7. [X. Lin, R. Lu, X. Liang, X. Shen, Stap: A social-tier-assisted packet forwarding proto-](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0009)

[col for achieving receiver-location privacy preservation in vanets, in: 2011 Proceed-ings IEEE INFOCOM, IEEE, 2011, pp. 2147–2155.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0009)

1. [R. Lu, X. Lin, T.H. Luan, X. Liang, X. Shen, Anonymity analysis on social spot based](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0010) [pseudonym changing for location privacy in vanets, in: 2011 IEEE International Con-ference on Communications (ICC), IEEE, 2011, pp. 1–5.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0010)
2. [R. Lu, X. Lin, X. Liang, X. Shen, Flip: An eﬃcient privacy-preserving protocol for](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0011)

[finding like-minded vehicles on the road, in: 2010 IEEE Global Telecommunications](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0011) [Conference GLOBECOM 2010, IEEE, 2010, pp. 1–5.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0011)

1. [R. Yu, J. Kang, X. Huang, S. Xie, Y. Zhang, S. Gjessing, Mixgroup: accumulative](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0012) [pseudonym exchanging for location privacy enhancement in vehicular social net-works, IEEE Trans Dependable Secure Comput 13 (1) (2015) 93–105.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0012)
2. [T.W. Chim, S.-M. Yiu, L.C. Hui, V.O. Li, Vspn: vanet-based secure and privacy-pre-serving navigation, IEEE Trans. Comput. 63 (2) (2012) 510–524.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0013)

*Computer Networks 176 (2020) 107283*

1. [H. Lu, J. Li, M. Guizani, A novel id-based authentication framework with adaptive](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0014) [privacy preservation for vanets, in: 2012 Computing, Communications and Applica-tions Conference, IEEE, 2012, pp. 345–350.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0014)
2. [T.W. Chim, S.-M. Yiu, L.C. Hui, V.O. Li, Specs: secure and privacy enhancing com-munications schemes for vanets, Ad Hoc Netw 9 (2) (2011) 189–203.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0015)
3. [Y. Sun, R. Lu, X. Lin, X. Shen, J. Su, An eﬃcient pseudonymous authentication](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0016) [scheme with strong privacy preservation for vehicular communications, IEEE Trans.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0016) [Veh. Technol. 59 (7) (2010) 3589–3603.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0016)
4. [L.A. Maglaras, D. Katsaros, Enhanced spring clustering in vanets with obstruction](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0017) [considerations, in: 2013 IEEE 77th Vehicular Technology Conference (VTC Spring),](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0017) [IEEE, 2013, pp. 1–6.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0017)
5. [T.D. Little, A. Agarwal, et al., An information propagation scheme for vanets, in:](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0018) [Proc. IEEE Intelligent Transportation Systems, 2005, pp. 155–160.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0018)
6. [C.-T. Li, M.-S. Hwang, Y.-P. Chu, A secure and eﬃcient communication scheme with](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0019) [authenticated key establishment and privacy preserving for vehicular ad hoc net-works, Comput Commun 31 (12) (2008) 2803–2814.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0019)
7. [H. Zhu, X. Lin, R. Lu, P.-H. Ho, X. Shen, Aema: An aggregated emergency mes-sage authentication scheme for enhancing the security of vehicular ad hoc net-works, in: 2008 IEEE International Conference on Communications, IEEE, 2008,](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0020)
   1. [1436–1440.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0020)
8. [S.S. Al-Riyami, K.G. Paterson, Certificateless public key cryptography, in: Interna-tional conference on the theory and application of cryptology and information se-curity, Springer, 2003, pp. 452–473.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0021)
9. [M. Barbosa, P. Farshim, Certificateless signcryption, in: Proceedings of the 2008](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0022) [ACM symposium on Information, computer and communications security, ACM,](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0022) [2008, pp. 369–372.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0022)
10. [S. Basudan, X. Lin, K. Sankaranarayanan, A privacy-preserving vehicular crowd-sensing-based road surface condition monitoring system using fog computing, IEEE](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0023) [Internet Things J. 4 (3) (2017) 772–782.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0023)
11. [H. Lu, Q. Xie, An eﬃcient certificateless aggregate signcryption scheme from pair-ings, in: 2011 International Conference on Electronics, Communications and Control](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0024) [(ICECC), IEEE, 2011, pp. 132–135.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0024)
12. [J. Wei, X. Wang, N. Li, G. Yang, Y. Mu, A privacy-preserving fog computing frame-work for vehicular crowdsensing networks, IEEE Access 6 (2018) 43776–43784.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0025)
13. [Z. Eslami, N. Pakniat, Certificateless aggregate signcryption: security model and a](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0026) [concrete construction secure in the random oracle model, Journal of King Saud Uni-versity-Computer and Information Sciences 26 (3) (2014) 276–286.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0026)
14. [K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, K. Sezaki, CARA-VAN: Providing location privacy for VANET, Technical Report, Washington Univ](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0027) [Seattle Dept of Electrical Engineering, 2005.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0027)
15. [J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, J.-P. Hubaux, Mix-zones](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0028) [for location privacy in vehicular networks, ACM Workshop on Wireless Networking](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0028) [for Intelligent Transportation Systems (WiN-ITS), 2007. CONF](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0028)
16. [Y.C. Hu, M. Patel, D. Sabella, N. Sprecher, V. Young, Mobile edge computinga key](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0029) [technology towards 5g, ETSI white paper 11 (11) (2015) 1–16.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0029)
17. [I. RASHEED, Basics of 5G, in: Opportunities in 5G Networks, CRC Press, 2016,](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0030)
    1. [23–38.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0030)
18. [R.S. Thoma, C. Andrich, G. Del Galdo, M. Dobereiner, M.A. Hein, M. Kaske,](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0031) [G. Schafer, S. Schieler, C. Schneider, A. Schwind, et al., Cooperative passive co-herent location: a promising 5g service to support road safety, IEEE Commun. Mag.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0031) [57 (9) (2019) 86–92.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0031)
19. [G. Elia, M. Bargis, M.P. Galante, N.P. Magnani, L. Santilli, G. Romano, G. Zaﬃro,](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0032) [Connected transports, v2x and 5g: Standard, services and the tim-telecom italia ex-periences, in: 2019 AEIT International Conference of Electrical and Electronic Tech-nologies for Automotive (AEIT AUTOMOTIVE), IEEE, 2019, pp. 1–6.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0032)
20. [J. Eriksson, L. Girod, B. Hull, R. Newton, S. Madden, H. Balakrishnan, The pothole](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0033) [patrol: using a mobile sensor network for road surface monitoring, in: Proceedings](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0033) [of the 6th international conference on Mobile systems, applications, and services,](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0033) [ACM, 2008, pp. 29–39.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0033)
21. [P. Mohan, V.N. Padmanabhan, R. Ramjee, Nericell: rich monitoring of road and traf-](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0034)

[fic conditions using mobile smartphones, in: Proceedings of the 6th ACM Conference](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0034) [on Embedded Network Sensor Systems, ACM, 2008, pp. 323–336.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0034)

1. [A. Mednis, A. Elsts, L. Selavo, Embedded solution for road condition monitoring us-ing vehicular sensor networks, in: 2012 6th International Conference on Application](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0035) [of Information and Communication Technologies (AICT), IEEE, 2012, pp. 1–5.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0035)
2. A. Irshad, M. Usman, S. Ashraf Chaudhry, H. Naqvi, M. Shafiq, A provably secure and eﬃcient authenticated key agreement scheme for energy internet based vehicle-to-grid technology framework, IEEE Transactions on Industry Applications (2020), doi:[10.1109/TIA.2020.2966160](https://doi.org/10.1109/TIA.2020.2966160). 1–1
3. [S.-H. Seo, M. Nabeel, X. Ding, E. Bertino, An eﬃcient certificateless encryption for](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0037) [secure data sharing in public clouds, IEEE Trans Knowl Data Eng 26 (9) (2013)](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0037) [2107–2119.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0037)
4. [A.W. Dent, A survey of certificateless encryption schemes and security models, Int.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0038) [J. Inf. Secur. 7 (5) (2008) 349–377.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0038)
5. [X. Huang, Y. Mu, W. Susilo, D.S. Wong, W. Wu, Certificateless signature revisited,](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0039) [in: Australasian Conference on Information Security and Privacy, Springer, 2007,](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0039)
   1. [308–322.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0039)
6. [B.C. Hu, D.S. Wong, Z. Zhang, X. Deng, Certificateless signature: a new security](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0040) [model and an improved generic construction, Designs, Codes and Cryptography 42](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0040)

[(2) (2007) 109–126.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0040)

1. [F. Li, M. Shirase, T. Takagi, Certificateless hybrid signcryption, in: International](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0041) [Conference on Information Security Practice and Experience, Springer, 2009,](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0041)
   1. [112–123.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0041)
2. [W. Xie, Z. Zhang, Eﬃcient and provably secure certificateless signcryption from](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0042) [bilinear maps, in: 2010 IEEE International Conference on Wireless Communications,](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0042) [Networking and Information Security, IEEE, 2010, pp. 558–562.](http://refhub.elsevier.com/S1389-1286(19)31565-8/sbref0042)

*I. Rasheed, L. Zhang and F. Hu*



**Iftikhar Rasheed** received the B.E. degree from the NUSTSchool of Electrical Engineering and Computer Sciences (NSEECS), Islamabad, Pakistan, and the M.S.E.E. degree from the University of Engineering and Technology, Taxila, Pak-istan. He is currently pursuing the Ph.D. degree in Electrical Engineering from The University of Alabama, Tuscaloosa, AL, USA. His research interests include wireless communications, 5G cellular systems, and artificial intelligence, vehicle to ev-erything (V2X) communications and cyber security.



**Lin Zhang** (S’14) received the B.S. degree in Radio Engineer-ing from Fuzhou University, Fuzhou, Fujian, China, in 2001, and the M.S. degree in Electrical Engineering from The Uni-versity of Texas at Dallas, Richardson, TX, USA, in 2008. He is currently pursuing the PH.D. degree with the 3S (Security, Sig-nals and Sensors) Lab, The University of Alabama, Tuscaloosa, AL, USA. He has over 10 years of industry experiences. Be-fore joining the 3S Lab, he worked as an Analog IC Design Engineer in The Vehicular Electronics Engineering Center of The Chinese Academy of Science, Shanghai Institute of Mi-crosystem and Information Technology (SIMIT), Shang Hai, China, mainly focusing on Power Management IC and Vehic-ular CAN/LIN Transceiver IC. His research interests include wireless networks, machine learning, deep learning, cyber se-curity, and circuit and system design.

*Computer Networks 176 (2020) 107283*



**Fei Hu** (M’01) received the first Ph.D. degree in signal process-ing from Tongji University, Shanghai, China, in 1999, and the second Ph.D. degree in electrical and computer engineering from Clarkson University, New York, NY, USA, in 2002. He is currently a Professor with the Department of Electrical and Computer Engineering, University of Alabama, Tuscaloosa, AL, USA. He has published over 200 journal/conference pa-pers and book (chapters) in thefield of wireless networks and machine learning. His research interests are wireless net-works, machine learning, big data, network security and their applications. His research has been supported by U.S. NSF, DoE, DoD, Cisco, and Sprint.