SPECIAL ISSUE ARTICLE - PREPRINT

Transactions on Emerging Telecommunications Technologies

Chaos-Based Privacy Preserving Vehicle Safety Protocol for 5G Connected Autonomous Vehicle Networks.

Shuja Ansari[1]* | **Jawad Ahmad**[2]* | **Syed Aziz Shah**[3] | **Ali Kashif Bashir**[3] | **Tuleen Boutaleb**[4] | **Sinan Sinanovic**[4]

[1]James Watt School of Engineering, University of Glasgow, UK

[2]School of Computing, Engineering and Built Environment, Glasgow Caledonian University, UK

[3]School of Computing, Edinburgh Napier University, UK

[4]School of Computing, Manchester Metropolitan University, UK

Correspondence
Syed Aziz Shah PhD, School of Computing, Manchester Metropolitan University, UK
Email: S.Shah@mmu.ac.uk

Funding information

There is a high demand for secure and reliable communications for Connected Autonomous Vehicles (CAVs) in the automotive industry. Privacy and security are key issues in CAVs, where network attacks can result in fatal accidents. The computational time, cost and robustness of encryption algorithms are important factors in low latency 5G-enabled secure CAV networks. The presented chaotic Tangent-Delay Ellipse Reflecting Cavity-Map (TD-ERCS) system and Piece-Wise Linear Chaotic Map (PWLCM) based encryption on short messages exchanged in a CAV network provide both robustness and high speed encryption. In this work, we propose a 5G radio network architecture, which leverages multiple radio access technologies and utilizes Cloud Radio Access Network (CRAN) functionalities for privacy preserved and secure CAV networks. The proposed Vehicular Safety Message (VSM) identifier algorithm meets transmission requirements with a high probability of 85% for low round trip delay of $\leq$ 50 ms. The proposed chaos based encryption algorithm exhibits faster speeds with a computational time of 2-3 ms, showcasing its lightweight properties ideal for time critical applications.

* Equally contributing authors.

1 | INTRODUCTION

Connected Autonomous Vehicles (CAVs) are an important use case of future 5G enabled vehicular networks. CAVs are vital in improving mobility, increasing comfort and addressing the socio-environmental cost of transport. These vehicular networks enable communication with each other or with the infrastructure. There are a number of unprecedented benefits of communication enabled applications. CAVs tend to improve road safety by exploiting safety application protocols, providing a new field of view and range, which in turn can provide quantitative and qualitative information to be shared through V2V (Vehicle-to-Vehicle) and V2I (Vehicle-to-Infrastructure) communications. The cost of positioning and communications hardware is significantly less than the sensing equipment required to cover the 360-degree envelope around the vehicle. UK government has plans to eliminate road signs on highways by 2027 [1]. The road signs along with other information will be disseminated to vehicles on the highway using radio technologies. With all these applications, key concerns with the integrity and privacy of wireless communications are on the rise. Preserving integrity and robustness of these vehicular networks is vital. Hijack of controls or reception of false information can be a safety hazard for CAVs, resulting in fatal accidents and loss of life. This gives rise to an entire domain of cyber security for automotive [2].

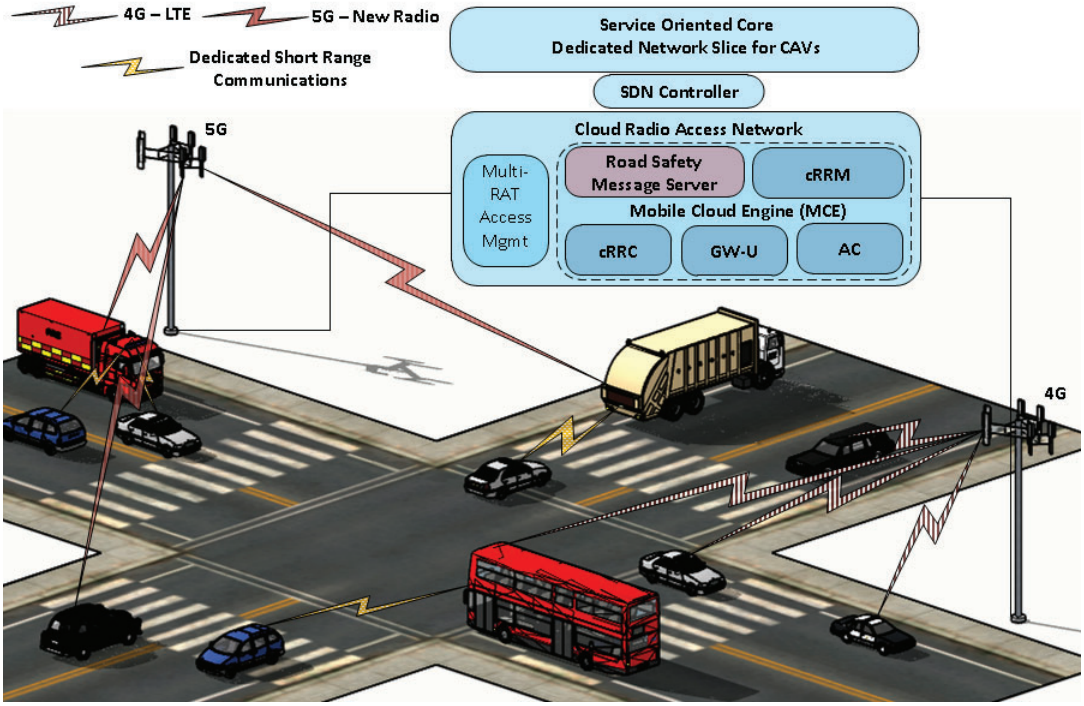


FIGURE 1 5G Communication Network for CAVs.

A variety of Radio Access Technologies (RATs) including 5G New Radio (NR), 4G Long Term Evolution (LTE) [3], Dedicated Short Range Communications (DSRC - IEEE 802.11p) [4] etc, have been proposed for vehicular communications. The ubiquitous nature of mobile networks, LTE and corresponding 5G technologies, makes them potential candidates

for CAV communications. Sub-domains or additional functionalities of these technologies such as LTE-Vehicular (LTE-V), Device to Device (D2D communications), evolved Machine Type Communications (eMTC), etc. have also been studied extensively to achieve V2V communications. However, current research has proposed achieving V2V communications through the infrastructure to preserve the privacy of users, avoiding the complexities of direct communications. The most promising RAT is the 5G New Radio (NR), which proposes a dedicated service oriented core for CAVs. Furthermore, 5G affiliated technologies such as Cloud Radio Access Network (CRAN) employing Mobile Edge Computing (MEC) are becoming favourites for achieving robust and low latency communications [5].

Heterogeneous Vehicular Networks (HetVANETs) suggest an interface that can integrate DSRC, 4G LTE and 5G NR to achieve a 100% up-time. Figure 1 illustrates a 5G architecture that employs a multi-RAT access management protocol to sustain the heterogeneous radio network in harmony. The core network (CN) have a dedicated slice for vehicular safety communications and consists of Software Defined Network (SDN) controllers that enable the interface of CRAN with the CN using a set of underlying forwarding nodes.

CAVs will continuously share their information with other vehicles and the infrastructure. This information includes vehicle properties and behaviours, gathered from the on-board vehicle sensors. In the case of an attack, the adversary can eavesdrop on the sensitive information being shared between the vehicles. The content of this information depends on the application being utilised by the vehicle. In the case of safety applications, the content can be the vehicle location, speed or direction. The road safety message server on receiving this information, maintains a comprehensive picture of the vehicular network. Specific warnings and notifications are then forwarded to vehicles which are potentially in a dangerous scenario. In these cases, a small change in this information by the attacker can have a chain reaction leading to fatal accidents. The motivation of this work is to protect the integrity of this sensitive information while maintaining the application's transmission requirements. In this paper, we implement privacy preserving protocol while addressing CAV latency requirements and computational time cost of chaotic encryption. Vehicular networks have stringent transmission requirements which are scarcely met by present day network functionalities [6]. Adding privacy to these links brings about overheads that in turn increase latency.

Encryption is a process that convert plaintext data to a form known as ciphertext data so that an intruder/attacker cannot access the original information. Decryption is the reverse process of encryption where the ciphertext message is converted back to the original data. In the past two decades, a strong relationship between chaos and cryptography has been proved, specified in [7, 8, 9, 10]. Chaotic maps produce random output which is highly sensitive to the initial condition known as the key parameters. Decryption of plaintext is not feasible if initial condition is unknown. Only an authorised person who has the key can decrypt the original data. Due to initial parameter sensitivity and light-weight nature of chaotic maps, it is widely used for real-time encryption of sensitive information [9, 10]. Such lightweight chaotic encryption are instrumental for low latency communications in CAV networks due to their lower computational time cost and robustness to attacks. In line with the key concerns and corresponding research gaps discussed above, the contributions of this paper include the following:

1. 5G radio network architecture utilizing multiple radio access technologies and exploiting CRAN virtual network functionalities for serving connected autonomous vehicle networks.
2. Vehicular safety message notification identifier algorithm that tends to meet safety application requirements while efficiently utilizing radio resources.
3. TD-ERCS and PWLCM based encryption for preserving privacy in CAV networks.

2 | VEHICULAR ROAD SAFETY PROTOCOLS

Vehicle safety is of paramount importance for CAVs and a number of applications that increase road safety can be achieved With transmission of data between vehicles and infrastructure. These safety applications are for vehicles both with or without driver. A number of studies, meetings, and proceedings have put forth various communication use cases for road safety. Some of these presented use cases vary depending on their development organisation, while most tend to cover major aspects of road safety. Major use cases with their required transmission parameters compiled with the survey of [11, 12, 13, 14, 15] are included in Table 1. These applications are notifications for vehicles, drivers and road users which serve the purpose of increasing road safety, reducing hazard risks and eventually improving driver assistance/experience. These same notifications can help autonomous vehicles make real-time decisions on the road. This opens up the space for autonomous vehicles to be safer than regular vehicles as it would be aware of situations not visible or perceivable by naked eye or on-board sensors.

European Telecommunications Standards Institute (ETSI) in [16, 17] classified these short vehicular safety messages (beacons) into Cooperative Awareness Message (CAMs) and Decentralized Environment Notification Messages (DENMs). CAMs are distributed within the network and provide information like the presence, position as well as basic set of communications within the neighbouring vehicles over a single hop. CAMs come under the category of periodic messages and are transmitted or received by all the vehicles present in the awareness range[1]. On the reception of CAMs, the vehicle is made aware of all the neighbours and their positions, movements and other basic attributes along with basic sensor information. On the other hand DENMs are used by Cooperative Road Hazard Warnings (CRHW) and come under the category of event messages, which include all event-based applications. When an event is detected, DENMs specific to that event are transmitted with a certain periodicity. This broadcasting of DEN messages continues until the end or expiry of the event.

Broadcasting, multicasting or unicasting are used for the transmission of these messages among vehicles. From Table 1, it can be observed that most of these safety messages are supposed to be delivered in the vicinity of the transmitter. For example, vehicles involved in an intersection collision and present in the surrounding area are notified of the hazard by the vehicle that detects the collision through their sensors by periodically broadcasting CAMs message. Vulnerable drivers, motorcycles and emergency vehicles can also broadcast DENM messages to make others aware of their presence in the vicinity. With the information of surrounding traffic situation, vehicle drivers can also be assisted in changing lanes, stopping at stop signs, merging into main roads, etc.

Another salient feature of safety applications is the periodicity of message transmission. Due to the rapid topology change and high mobility of vehicles, safety application requires the safety beacons to be transmitted at a certain frequency depending on the application. For instance, intersection collision warning is required to be transmitted 10 times a second which means the message needs to be transmitted every 100 ms. Kato [19] defined the concept of data freshness and used this parameter to evaluate the performance of LTE networks for vehicular communications. If a vehicle application transmits a packet at a frequency of 10 Hz, which means a message is transmitted every 100 ms, the freshness requirement for that specific application would be 100 ms. By this principle, if the message is received after 100 ms it can be considered as lost. Similarly, for other applications like slow vehicle indication, 2 messages per second are sufficient. This periodicity puts load on the network and as evident from previous studies carried out by [20, 21], network degrades with the increasing message frequency.

Applicability of safety messages are usually constrained within a certain radius. For instance, traffic light speed

[1] Araniti [3] and Bazzi [18] elaborated awareness range, which is the geographical area around the vehicle, where all the neighbours are to be made cognizant of the vehicle. Awareness range is also termed as relevance range for DENMs and in general are also termed as the applicable transmission range of safety messages.

TABLE 1 Vehicular Safety Applications and their Transmission Requirements.

Safety Application	Message Type	Communication Mode	Minimum Frequency	Critical Latency	Awareness Range
Intersection Collision Warning	CAM	Broadcasting Periodic Messages	10 Hz	~100ms	150m
Lane Change Assistance	CAM	Cooperation awareness between vehicles	10 Hz	~100ms	150m
Slow Vehicle Indication	CAM / DENM	Broadcasting State Periodically	2 Hz	~100ms	200m
Traffic Light Speed Advisory/Violation	CAM / DENM	Broadcasting Periodic Messages	2 Hz	~100ms	150m
Overtaking Vehicle Warning	CAM	Broadcasting overtaking state	10 Hz	~100ms	300m
Head on Collision Warning	CAM	Broadcasting Periodic Messages	10 Hz	~100ms	200m
Collision Risk Warning	CAM / DENM	Time Limited Periodic messages on event	10 Hz	~100ms	300-500m
Cooperative Forward Collision Warning	CAM	Cooperation awareness between vehicles	10 Hz	~100ms	150m
Emergency Vehicle Warning	CAM / DENM	Broadcasting Periodic Messages	2 Hz	~100ms	300m
Cooperative Merging Assistance	CAM	Cooperation awareness between vehicles	1 Hz	~1000ms	250m
Speed Limits Notification	CAM	Broadcasting Periodic Messages	1 – 10 Hz	~100ms	300m
Motorcycle Approaching Indication	CAM	Cooperation awareness between vehicles	2 Hz	~100ms	150m
Curve Speed Warning	DENM	Broadcasting curve location, curvature and speed limit	1 Hz	~1000ms	200m
Stop Sign Assist	CAM / DENM	Broadcasting stop sign position	10 Hz	~100ms	300m
Hazardous Location Warning	CAM / DENM	Broadcasting Periodic Messages	10 Hz	~100ms	200-500m

advisory and violation would only be around the traffic light, while an emergency vehicle would need to notify vehicles of its presence in its routes vicinity. Message type, communication mode, message frequency, critical latency and awareness range included in Table 1 are the most critical aspects to be addressed by communication technologies for vehicle road safety.

2.1 | C-RAN for C-V2X

Cloud Radio Access Network promises to bring the server processing to the edge of the network, subsequently reducing experienced end-to-end delay. The Scalability of mobile network servers where different locations of the server are

evaluated show that by having forwarding mechanism implemented close to the base station, it significantly increases the network capacity, where almost 50% more vehicles experience the required transmission delay [6]. The CRAN functionality, splitting the network functionality and introducing mobile edge computing [22], allows the implementation of message forwarding server close to the access network edge. For the evaluation of CRAN for V2X, we implement the Road Safety Message Server on the Mobile Cloud Engine residing at the edge of the network. We discuss our findings later in the Section 4. The mobile cloud engine (MCE) residing within the CRAN comprises of network functionalities for radio resource management and application provision. RAN functions such as cloud Radio Resource Control (cRRC) is to facilitate multi-connectivity and new technology deployment, whereas the centralized Radio Resource Management (cRRM) entity is to ensure efficient coordination of resources in heterogeneous networks. CRAN will also have a user-plane gateway (GW-U) and an authentication confirmation (AC) entity. The role and functionality of the Vehicular Road Safety (VRS) Message Server is explained in the following subsection.

2.2 | VSN Protocol Identifier (VSN_{id})

Radio resources in the licensed band are expensive, which calls for mechanisms to efficiently utilize the wireless reserves. The vehicle safety network protocol identifier (VSN_{id}) proposed in Algorithm 1 adds a notification identifier that specifies the Vehicle Road Safety (VRS) server about the application requirements. These include the required awareness range and the demanding periodicity of the message. The VRS server maintains a look up table containing the applications and their corresponding transmission requirements. Assuming vehicle (veh_i) transmits a Vehicle Safety Message (VSM) containing the VSN_{id}. The VRS server will obtain the awareness range (R_i) and periodicity requirements (also termed as beacon frequency (BF)) from its look up table. Among other information, the exchanged packet also contains vehicle location (d_i), using this in conjunction with the information from the map database and R_i, the VRS server determines the intended receiving vehicles set also termed as forwarding set (F_{ij}). [6, 23] Exploiting the state-of-the-art CRAN technologies, the virtualized VRS server operating at the radio edge will then multicast the VSM to the forwarding set of vehicles given by:

$$\mathbf{F}_{ij} = \{\forall k : d_{ij} < R_i, i \neq j\}, \tag{1}$$

Similar principles can be used in exchanging control messages for fleets of autonomous vehicles. As mentioned in Section 1, controlling the vehicle remotely in the case of sensor failure has found much importance. Exchanging of this control information will require privacy preserving mechanisms to avoid threats and fatalities. Therefore, this paper extends this contribution by proposing the use of TD-ERCS and PWLCM based privacy preserving encryption on VSM payloads.

2.3 | Privacy Preserving Lightweight Encryption

A chaotic map can effectively provide the required confusion and diffusion necessary for effective encryption [24]. In cryptography, confusion and diffusion are two main steps which were defined by Shannon in his theory in the year 1945 [25]. Chaotic maps has application in numerous fields including image, video and audio encryption [9, 10, 26]. Initially, the purpose of chaos-based cryptography was mainly focused on higher speed rather than just security, however, the focus of research has now shifted toward higher security while maintaining these high speeds so that an intruder cannot decode the original real-time information [10]. In this work, we propose a secure, light-weight and efficient encryption

Algorithm 1 VSM Forwarding Algorithm

Input: $VSMs : veh_i \longrightarrow VRS$
Output: $VSMs : VRS \longrightarrow veh_j$
System Setup :
VRS maintains local area road map
while $VRS \leftarrow encrypted(VSM_i)$ **do**
  VRS decrypts payload
  $VSM_i \longrightarrow (VSN_{ID}, VSM(veh_i))$
  $VSN_{ID} \longrightarrow (R_i, BF_i)$
  $VSM(veh_i) \longrightarrow Position(d_i)$
  $(R_i, d_i) \longrightarrow Distance(d_{ij})$
  $\mathbf{F}_{ij} = \{\forall k : d_{ij} < R_i, i \neq j\}$,
  Encrypt (VSM_i)
  $VRS \Rightarrow veh_j \in \mathbf{F}_{ij}$ at BF_i
end while
return $\mathbf{F}_{ij}$

scheme for vehicle safety. The proposed scheme is based on two chaotic maps: (i) TD-ERCS and (ii) PWLCM which are further explained in Section 3.2.

3 | SYSTEM MODEL

3.1 | CAV Connectivity Simulation Environment

The vehicular network is assumed to be composed of N vehicles uniquely identified by their number i, ($i = 1 \ldots N$). For the sake of consistency, vehicles are assumed to use LTE FDD radio transceivers. The work in this paper builds on to the performance evaluation from [20] that takes in account multicell and multipath propagation along with 3GPP specified Extended Vehicular A (EVA) fading environment. The network modeled is a $2 \times 2\,\text{km}^2$ area of Glasgow city center (GCC) (Figure 2) implemented in ns-3 [27]. Mobility of the vehicles in the network is generated using routes mobility model which assigns each vehicle with a route generated using Google maps API [28]. The network design considers enhanced realism through models employing the site configuration used by UK's mobile operator EE in Glasgow [29]. The CRAN functionality is modelled by introducing the proposed message forwarding mechanism implemented as a detached entity located within the RAN using an extended version of LTE EPC Network simulAtor (LENA) module [30].

Parameters chosen for the simulation model are given in Table 2. Vehicular safety messages are modeled as packets of 256 bytes including all protocol headers and associated overheads. In order for the vehicle to access multiple radio interfaces, encryption is carried out on the payload of the packet. This is comprised of 184 bytes carrying vital information about the vehicle. The following subsection presents the chaotic encryption scheme utilized.

3.2 | TD-ERCS and PWLCM chaotic Maps

In the recent years, chaos-based cryptography has received a lot of attention from the research community [31]. This is due to the sensitivity and random nature of chaotic maps which can play a vital role in privacy preservation and encryption technologies. However, research shows that one dimensional (1D) chaotic maps such as logistic and skew tent map are insecure and cannot provide effective solution in cryptography [32]. This is due to the lower key space and low range for the initial conditions. Professor Li proposed [33] a novel 2D discrete chaotic map known as Tangent-Delay

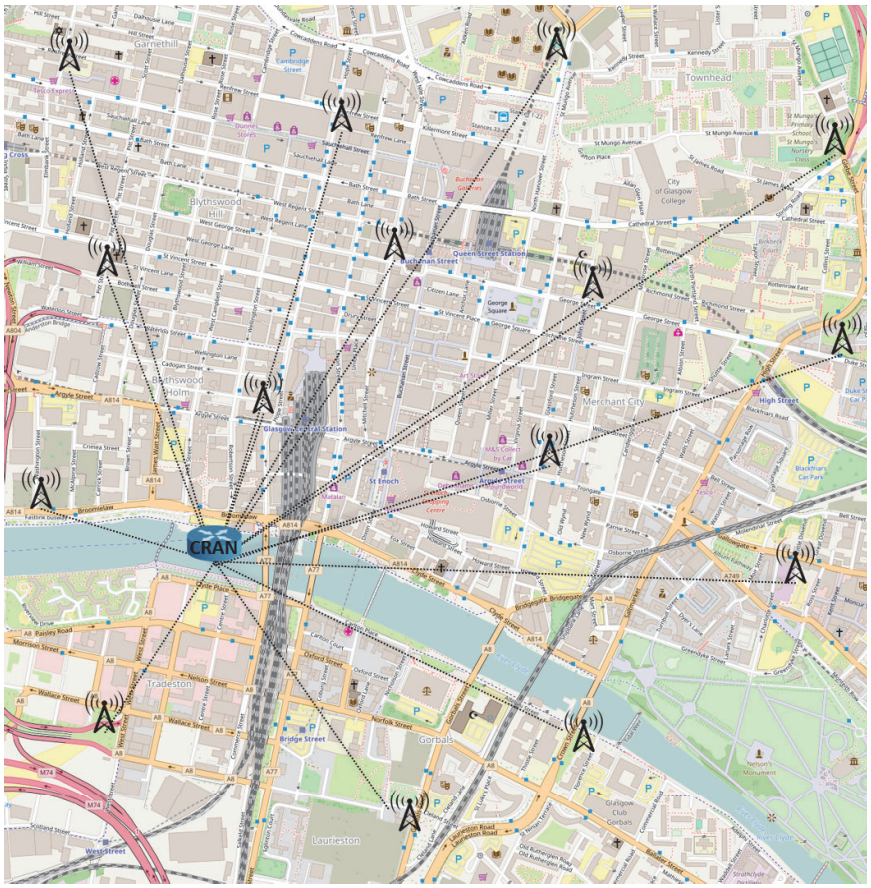


FIGURE 2 The 2x2 km^2 modelled area of Glasgow City Centre with 14 existing LTE Masts of EE.

Ellipse Reflecting Cavity-Map System (TD-ERCS) which can effectively reduce 1D chaotic map issues and hence it can be employed in any system for secure communication. The random outputs produced from TD-ERCS map are equi-probable, zero correlation in total field and significant initial value space [24]. In TD-ERCS iteration double precision floating points are used, where mathematically the equation for TD-ERCS can be written as [33, 24]:

$$\begin{cases} x_n = -\frac{2k_{n-1}y_{n-1}+x_{n-1}(\mu^2-k_{n-1}^2)}{\mu^2+k_{n-1}^2} \\ y_n = k_{n-1}(x_n - x_{n-1}) + y_{n-1}, \quad n = 1, 2, 3\ldots \end{cases} \tag{2}$$

where

$$k_n = \frac{2k'_{n-m} - k_{n-1} + k_{n-1}(k'_{n-m})^2}{1 + 2k_{n-1}k'_{n-m} - k(k'_{n-m})^2} \tag{3}$$

TABLE 2 Vehicle Connectivity Simulation Parameters

Parameter	Value
Simulation time	100 seconds.
Road model	Glasgow City Center (GCC) (2km x 2km)
Network layout	14 sites with 3 cells/site, UK Operator EE mast data [29].
Scheduling algorithm	Proportional Fair.
Handover algorithm	A2A4RSRQ, RSRQ threshold -5 dB,
	and NeighbourCellOffset=2 (1 dB).
Frequency reuse	Distributed Fractional Freq. Reuse.
Path loss model	LogDistance ($\alpha = 4$) and
	3GPP Extended Vehicular A model.
Safety message format	256 bytes UDP.
Number of vehicles	100, 150.
Average vehicle's speed	20 km/h, 40 km/h.
Beacon frequency	1 Hz, 10 Hz.

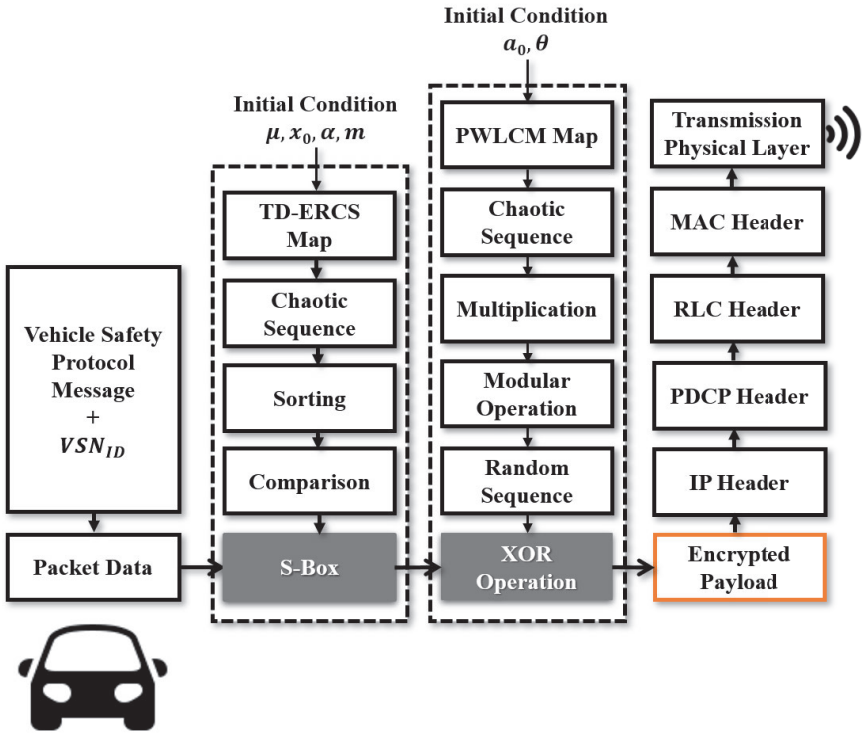


FIGURE 3 Uplink flow diagram

$$k'_{n-m} = \begin{cases} -\frac{x_{n-1}}{y_{n-1}}\mu^2 & n < m \\ -\frac{x_{n-m}}{y_{n-m}}\mu^2 & n \geq m \end{cases} \tag{4}$$

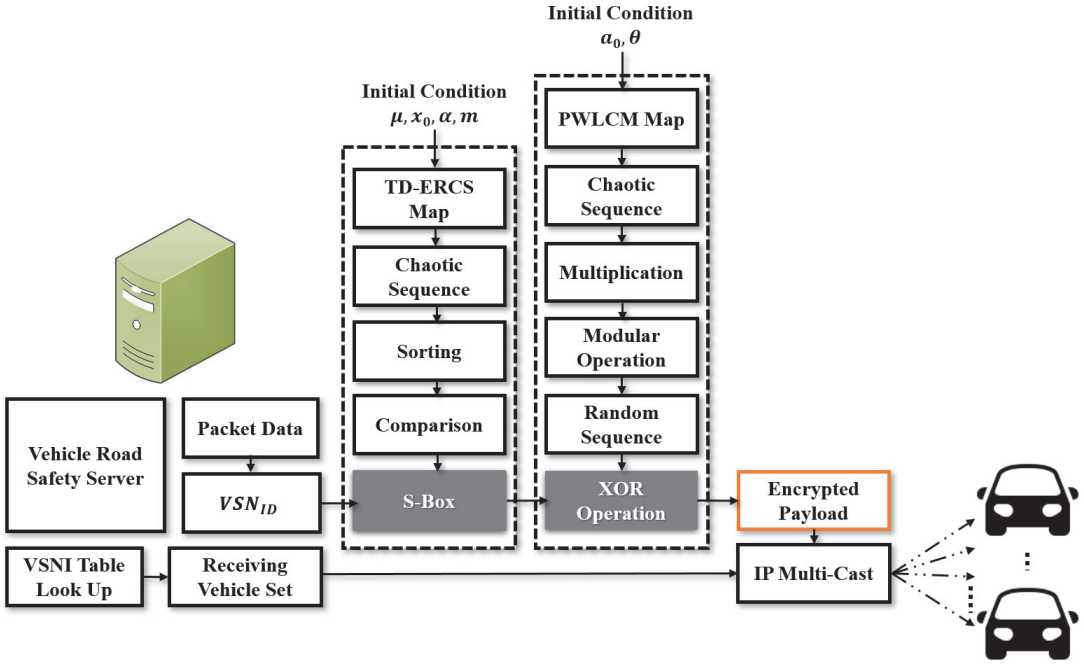


FIGURE 4 Downlink flow diagram

$$y_0 = \mu\sqrt{1 - x_0^2} \tag{5}$$

$$k_0' = -\frac{x_0}{y_0}\mu^2 \tag{6}$$

$$k_0 = -\frac{\tan\alpha + k_0'}{1 - k_0'\tan\alpha} \tag{7}$$

$$\begin{cases} \mu \in (0, 1) \\ x_0 \in [-1, 1] \\ \alpha \in (0, \pi) \\ m = 2, 3, 4, 5\ldots \end{cases} \tag{8}$$

In above equations, x_n and y_n are random sequences generated using seed parameters μ, x_0, α and m of TD-ERCS map. These seed parameters are used as secret keys when encrypting the data. The output of Piece Wise Linear Chaotic Map (PWLCM) is more chaotic than the traditional logistic map as outlined in [24]. A small change in initial key parameters

can drastically change the output of the map. Mathematically, PWLCM is written as [34]:

$$z_{n+1} = f(z_n, \mu) = \begin{cases} \frac{z_n}{\mu}, & \text{if } z_n \in [0, \mu] \\ \frac{1-z_n}{1-\mu}, & \text{if } z_n \in (\mu, 0.5] \\ F(1 - z_n), & \text{if } z_n \in (0.5, 1] \end{cases} \tag{9}$$

where, z_n is random chaotic values and μ is control parameter. These mechanisms are implemented within the LTE V2X uplink and downlink flows as shown in Figure 3 and Figure 4 respectively.

Furthermore, chaotic maps such as Logistic and Skew tent maps exhibit complex properties in a very simple mathematical formula and one can encrypt a message using the properties of chaos maps. However, as mentioned earlier, one-dimensional maps such as Logistic and Skew maps have lower key space issues, making way for an attacker to launch key space/brute force attack. One of the properties of a chaotic map is that a small change in initial conditions can generate a different output which is an important property for an encryption algorithm. TD-ERCS map generate different output when the initial conditions are slightly changed. In the Figure 5, when the initial conditions are slightly changed from 0.6000 to 0.6001, it can be observed that after the 14th iteration, the map produced a different output.

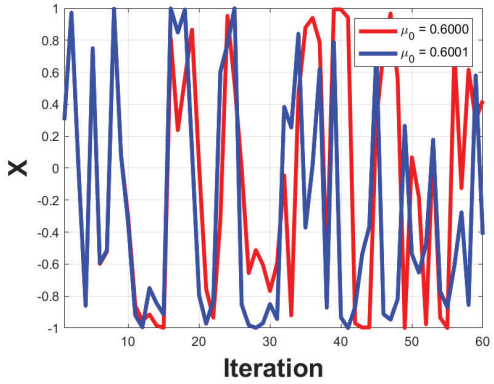


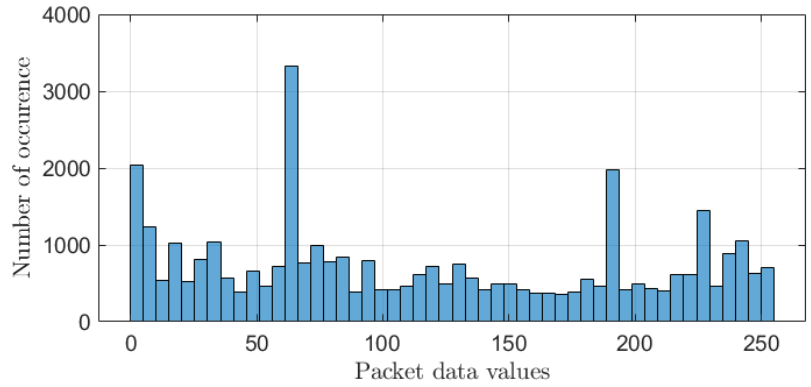
FIGURE 5 Change in the Initial Condition of Chaotic Map.

3.3 | Security Analysis and Latency Performance

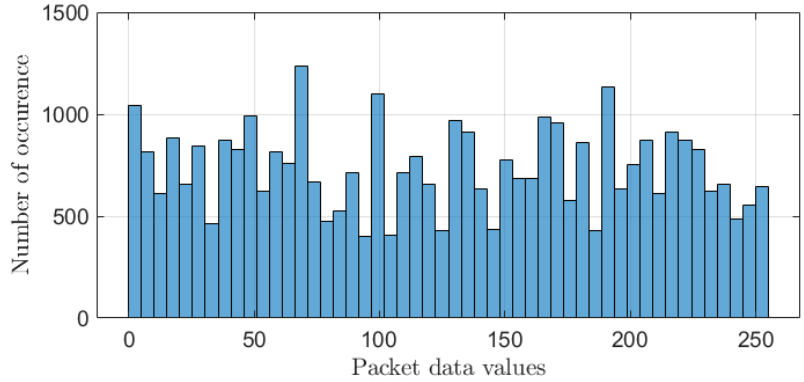
Due to the imperative safety, most of the applications require the transmission and successful reception of message to have an end-to-end delay of less than 100 ms. These requirements are set forth by SDOs and OEMs, however, authors in [35, 36] benchmarked their evaluations with latency being less than 50 ms.

4 | FINDINGS AND DISCUSSION

The histogram shown in Figure 6 highlights the security of the proposed chaos-based encryption. One can see from the Figure 6(b) that the histogram of the encrypted data is different from the original data histogram (Figure 6(a). Additionally, the encrypted data histogram is comparably flat. In previous research [24], it is outlined that the keyspace of an



(a) Original Data



(b) Histogram of plaintext and encrypted data

FIGURE 6 Vehicular Safety Protocol Packet Data.

encryption algorithm must be greater than 2^{100}. In the proposed scheme, the keyspace for TD-ERCS and PWLCM is 2^{299} which is much higher than traditional Data Encryption Standard (DES) and Advanced Encryption Standard (AES). The speed of the proposed chaos-based scheme along with AES is evaluated on Intel Core i5, 4GB RAM using native C/C++ implementation, exhibiting significantly lower latency than AES with a time cost of only 2-3 ms to encrypt the packet. As a result,the proposed scheme does not introduce any significant delay for real-time applications. Furthermore, we have carried out correlation coefficient, number of bit change rate (NBCR) and unified average change intensity (UACI) tests [24]. Simulation results show that the correlation between original and ciphertext message is 0.05. Mathematically, the value of correlation is between -1 and 1, where 1 shows exactly similar, 0 shows completely different and -1 shows negative of original message. In our case, correlation value of 0.05 indicates a higher security of the proposed scheme. Moreover, for a slight change in chaotic map parameters, a significant change in NBCR and UACI is observed during simulation. The value of NBCR and UACI are 99.19% and 33.11, respectively. The aforementioned security evaluation parameters shows that proposed scheme is resistant against entropy, statistical and differential attacks.

The fast changing topology of vehicular networks due to their mobile nature brings about challenges in message dissemination. The evaluation of experienced latency over such an architecture is vital. We compare our proposed scheme with the traditional vehicular networks communicating over a similar architecture with no encryption in

place. First we compare results for 100 and 150 vehicles operating in our defined simulation model, utilizing the VSN protocol with 1 Hz message periodicity against similar scenario employing the proposed privacy preserving lightweight encryption.

Figure 7 shows a cumulative density function (CDF) of end-to-end delay experienced by 100 and 150 vehicles transmitting one message every second. It is evident for 100 vehicles the probability of having an end-to-end delay of less than or equal to 50 ms is about 85%. Adding encryption to this scenario changes this probability by only 1%. This negligible increase in delay occurs because of the lightweight nature of the proposed encryption. As discussed in the last subsection, the size of the packet remains the same with the addition of encryption, hence, due to no added overheads the network latency remains the same with slight addition of encryption/decryption computational time. With the message periodicity of 1 Hz, the network does not undergo significant loads. Therefore, to get a more clearer picture, we next evaluate the network with a message periodicity of 10 Hz.

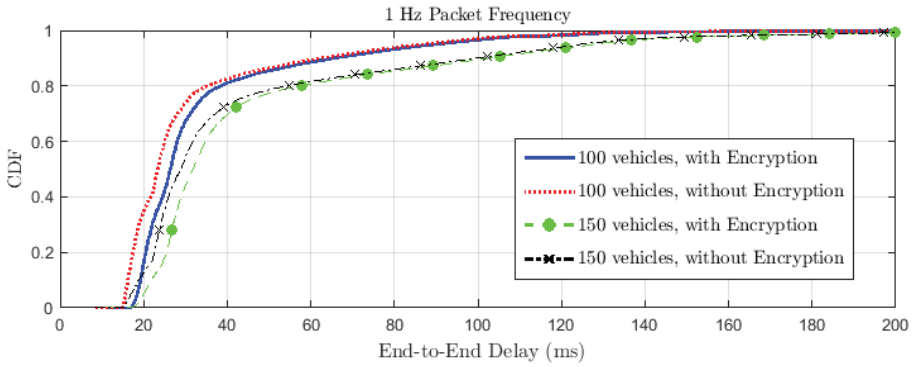


FIGURE 7 End-to-End delay with 100 and 150 vehicles transmitting vehicle safety messages at 1 Hz packet frequency.

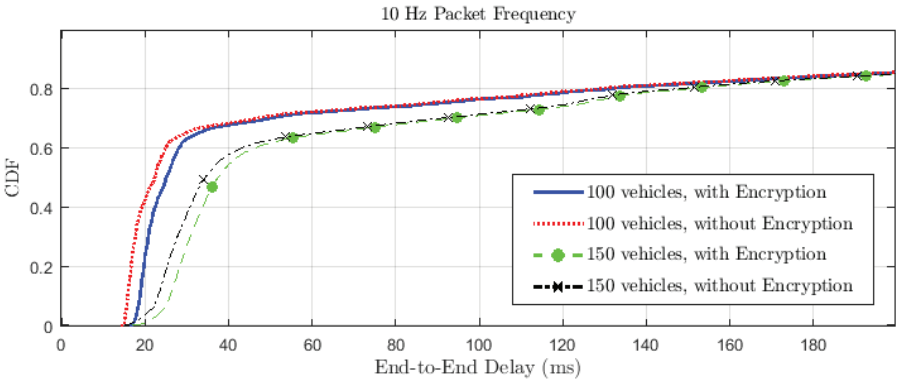


FIGURE 8 End-to-End delay with 100 and 150 vehicles transmitting vehicle safety messages at 10 Hz packet frequency.

In Figure 8 the vehicles transmit 10 messages every second. With this beacon frequency, a considerable load is

placed on the network, resulting in higher delays due to network congestion. The probability of delay being ≤ 50 ms decreases from 85% to almost 70% for 100 vehicles. However, only 1% difference with the addition of our proposed encryption scheme is observed. Similarly, for 150 vehicles, the probability of delay being ≤ 40 ms is 58% which decreases to roughly around 56% with the proposed encryption scheme. The results for the two scenarios as illustrated in Figure 7 and Figure 8, show that the proposed encryption scheme maintains the latency and fulfils the strict transmission requirements of CAVs.

5 | CONCLUSIONS

This paper proposed a reliable, secure and privacy-preserving message dissemination scheme for CAV networks. Low latency communication is an important factor for 5G-enabled CAV networks and demands fast encryption algorithms that can meet the transmission requirements. A 5G radio network architecture with multiple radio access technologies, exploiting CRAN functionalities is presented and evaluated for secure CAV networks. The novel secure VSM identifier algorithm introduced in this work, meets the end-to-end delay demands with a high probability of 85% for a round trip time (RTT) of 50ms. A robust and high speed chaotic encryption scheme based on TD-ERCS system and PWLCM is proposed and utilized for messages exchanged in a CAV network. The presented encryption scheme is evaluated using histograms and keyspace analysis for robustness, while computational time cost is measured to evaluate the impact on network end-to-end delay. The presented chaos based encryption algorithm has a computational time cost of 2-3ms, which has insignificant impact on total transmission delays. In the future, we plan to extend our simulations to include direct communications and real-time control of CAVs along with the modelling of network attacks with higher dimensional chaotic maps.

REFERENCES

[1] Speed limits to be beamed into cars on sign-free roads | News | The Times;. https://www.thetimes.co.uk/article/speed-limits-to-be-beamed-into-cars-on-sign-free-roads-hrcq7wlg9.

[2] Alnasser A, Sun H, Jiang J. Cyber security challenges and solutions for V2X communications: A survey. Computer Networks 2019;151:52 – 67. http://www.sciencedirect.com/science/article/pii/S1389128618306157.

[3] Araniti G, Campolo C, Condoluci M, Iera A, Molinaro A. LTE for vehicular networking: a survey. Communications Magazine, IEEE 2013;51(5):148–157.

[4] Yin J, Yeung G, Ryu B, Habermas S, Talty T. Performance Evaluation of Safety Applications over DSRC Vehicular Ad Hoc Networks. Information Sciences 2004;p. 1–9.

[5] Katsaros K, Dianati M. 5. In: Evolution of Vehicular Communications within the Context of 5G Systems John Wiley Sons, Ltd; 2019. p. 103–126. https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119515579.ch5.

[6] Ansari S, Sánchez M, Boutaleb T, Sinanovic S, Gamio C, Krikidis I. SAI: safety application identifier algorithm at MAC layer for vehicular safety message dissemination over LTE VANET networks. Wireless Communications and Mobile Computing 2018;2018.

[7] Shujun L, Xuanqin M, Yuanlong C. Pseudo-random bit generator based on couple chaotic systems and its applications in stream-cipher cryptography. In: International Conference on Cryptology in India Springer; 2001. p. 316–329.

[8] Chen G, Mao Y, Chui CK. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons & Fractals 2004;21(3):749–761.

[9] Ahmad J, Khan MA, Ahmed F, Khan JS. A novel image encryption scheme based on orthogonal matrix, skew tent map, and XOR operation. Neural Computing and Applications 2018;30(12):3847–3857.

[10] Ahmad J, Larijani H, Emmanuel R, Mannion M, Javed A. Occupancy Detection in Non-residential Buildings–A Survey and Novel Privacy Preserved Occupancy Monitoring Solution. Applied Computing and Informatics 2018;.

[11] Vehicle Safety Communications Project Task 3 Final Report. US Department of Transportation; 2005.

[12] Intelligent transport systems (ITS); basic set of applications; Part2: specification of cooperative awareness basic service; 2011.

[13] Intelligent transport systems (ITS); basic set of applications; part3: specifications of decentralized environmental notification basic service; 2010.

[14] C L Robinson, D Caveney, L Caminiti, G Baliga, K Laberteaux and P R Kumar. Efficient message composition and coding for cooperative vehicular safety applications. IEEE Transactions on Vehicular Technology 2007;56(6):3244–3255.

[15] Derek Caveney. Cooperative vehicular safety applications. IEEE Control Systems 2010;30(4):38–53.

[16] ETSI (European Telecommunications Standards Institute). ETSI TS 102 637-2 Vehicular Communications ; Basic Set of Applications ; Part 2 : Specification of Cooperative. History 2011;1:1–18.

[17] Etsi. TS 102 637-3 - V1.1.1 - Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service 2010;1021(1):637–643.

[18] Bazzi A, Masini BM, Zanella A. Performance Analysis of V2V Beaconing Using LTE in Direct Mode With Full Duplex Radios. IEEE Wireless Communications Letters 2015 Dec;4(6):685–688.

[19] Kato S, Hiltunen M, Joshi K, Schlichting R. Enabling vehicular safety applications over LTE networks. 2013 International Conference on Connected Vehicles and Expo, ICCVE 2013 - Proceedings 2013;p. 747–752.

[20] Z H Mir, and F Filali. LTE and IEEE 802.11p for vehicular networking: a performance evaluation. EURASIP Journal on Wireless Communications and Networking 2014;(1):1–15.

[21] Harding J, Powell G, Yoon R, Fikentscher J, Doyle C, Sade D, et al. Vehicle-to-Vehicle Communications : Readiness of V2V Technology for Application 2014;(August):327.

[22] Liarokapis D. Mobility prediction for traffic offloading in cloud cooperated mmWave 5G networks. In: Proceedings 9th IEEE-GCC 2017 IEEE; 2018. Acceptance note in SAN Contacted author re expected publication date, author confirmed delay in paper appearing in IEEE Xplore 23-7-18 Changed template to proceedings.

[23] Ansari S, Boutaleb T, Gamio C, Sinanovic S, Krikidis I, Marvin S. Vehicular Safety Application Identifier Algorithm for LTE VANET Server 2016;p. 37–42.

[24] Ahmad J, Hwang SO. A secure image encryption scheme based on chaotic maps and affine transformation. Multimedia Tools and Applications 2016;75(21):13951–13976.

[25] Shannon CE. Communication theory of secrecy systems. Bell system technical journal 1949;28(4):656–715.

[26] Habib Z, Khan JS, Ahmad J, Khan MA, Khan FA. Secure speech communication algorithm via DCT and TD-ERCS chaotic map. In: 2017 4th International Conference on Electrical and Electronic Engineering (ICEEE) IEEE; 2017. p. 246–250.

[27] Model library release ns-3.2. Ns-3 network simulator; 2015, https://www.nsnam.org/docs/models/html/lte-design.html.

[28] Cerqueira T, Albano M. RoutesMobilityModel: Easy Realistic Mobility Simulation Using External Information Services. In: Proceedings of the 2015 Workshop on Ns-3 WNS3 '15, New York, NY, USA: ACM; 2015. p. 40–46. http://doi.acm.org/10.1145/2756509.2756515.

[29] CellMapper, Cellular Coverage and Tower Map for EE Network in Glasgow;. https://www.cellmapper.net/.

[30] Baldo N. The ns-3 LTE module by the LENA project;.

[31] Murillo-Escobar MA, Meranza-Castillón MO, López-Gutiérrez RM, Cruz-Hernández C. Suggested Integral Analysis for Chaos-Based Image Cryptosystems. Entropy 2019;21(8):815.

[32] Elmanfaloty RA, Abou-Bakr E. Random property enhancement of a 1D chaotic PRNG with finite precision implementation. Chaos, Solitons & Fractals 2019;118:134–144.

[33] Sheng LY, Sun KH, Li CB. Study of a discrete chaotic system based on tangent-delay for elliptic reflecting cavity and its properties 2004;.

[34] Khan MA, Ahmad J, Javaid Q, Saqib NA. An efficient and secure partial image encryption for wireless multimedia sensor networks using discrete wavelet transform, chaotic maps and substitution box. Journal of Modern Optics 2017;64(5):531–540.

[35] Eren H, Pakka H, Alghamdi A, Yue Y. Instrumentation for safe vehicular flow in intelligent traffic control systems using wireless networks. In: Proceedings of the 2013 IEEE International Instrumentation and Measurement Technology Conference IEEE; 2013. p. 1301–1305.

[36] Vinel A. 3GPP LTE versus IEEE 802.11p/WAVE: Which technology is able to support cooperative vehicular safety applications? IEEE Wireless Communications Letters 2012;1(2):125–128.