Journal of Autonomous Intelligence (2024) Volume 7 Issue 5
doi: 10.32629/jai.v7i5.1613

ORIGINAL RESEARCH ARTICLE

Minimizing hazardous conditions in transportation through wireless sensor networks with VANET

T. Sarath Babu[1], D. Venkata Srihari Babu[2], J. Balamurugan[3,*], Muniyandy Elangovan[4], Amit Verma[5], Gunji Sreenivasulu[6], R. Senthamil Selvan[7]

[1] *Department of ECE, G Pulla Reddy Engineering College (Autonomous), Kurnool, Andhra Pradesh 518007, India*

[2] *Department of Electronics and Communication Engineering, G pulla Reddy Engineering College, Kurnool, Andhra Pradesh 518007, India*

[3] *Department of Master of Business Administration, St. Joseph's College of Engineering (An Autonomous Institution) Chennai, Tamil Nadu 600119, India*

[4] *Department of Biosciences, Saveetha School of Engineering. Saveetha Institute of Medical and Technical Sciences, Chennai 600077, India*

[5] *University Centre for Research and Development, Chandigarh University, Gharuan Mohali, Punjab 140413, India*

[6]*Department of Computer Science and Engineering, Madanapalle Institute of Technology & Science, Madanapalle, Andhra Pradesh 517325, India*

[7] *Department of Electronics and Communication Engineering, Annamacharaya Institute of Technology and Sciences, Tirupati, Andhra Pradesh 517520, India*

*** Corresponding author:** J. Balamurugan, drjbalamuruganpdf@gmail.com

ABSTRACT

Through facilitating connectivity between automobiles and their surroundings, vehicular ad hoc networks, or VANETs, significantly contribute to improvements in road safety, traffic efficiency, and passenger comfort. Nevertheless, because networks are both open and changing, roadside devices collect vital safety information. By bolstering general security with the use of wireless communication networks (WSNs), this study helps bring about a safe transportation system. The proposed system employs a distributed network of mobile sensors embedded inside the VANET framework to track and detect roadside surroundings. Together, these sensors gather and process information about the movements of vehicles and traffic patterns. The authority, secrecy, integrity, availability of multifunctional safety applications have been implemented through use of V2V (vehicle to vehicle) connectivity and collected data. NS 2.35 platform is used to validate simulated analysis, and it is shown that suggested analysis works well with various transport intelligence systems in ad hoc networks (VANETs). In light of this, deployment demonstrates data confidentiality, integrity, overall network resilience, opening the door to more secure and safe communication. The performance evaluation metrics are quality of service (QoS) for forward collision warning (FCW) and lane change warning (LCW), communication delay (CD) and packet loss rate (PLR) used for this experiment.

Keywords: intrusion detection system (IDS); vehicle ad hoc network (VANET); wireless sensor network

1. Introduction

VANETs are increasingly crucial in improving traffic flow, road safety, and overall transportation systems. By allowing cars to connect with one other and with roadside infrastructure, these networks facilitate the sharing of vital information to improve situational awareness. It is critical to address the security issues caused by these readily available dynamic settings in light of the impending deployment of VANETs[1,2].

In VANETs, communication and data security are of utmost importance, especially because wireless connections might be vulnerable. Using wireless sensor networks (WSNs) to build a VANET-based secure transportation system. In order to quickly detect, identify, react to security issues, automobile sector

ARTICLE INFO

Received: 5 March 2024
Accepted: 8 April 2024
Available online: 22 August 2024

strategically deploys WSNs[3,4].

Building a strong security architecture to protect VANETs from threats like hacking, illegal access, and privacy breaches is the main goal of this solution. The strengthen vehicular communication safety by including wireless sensor networks, or WSNs, into the design of vehicle ad-hoc networks (VANETs)[5,6]. They are committed to guaranteeing the honesty and reliability of the data that is exchanged. In the subsequent sections of this study, analyze specific components and methodologies employed in implementation. This entails employing advanced cryptographic techniques to provide secure communication, implementing wireless sensors for detecting unauthorized access, implementing dynamic key management strategies, and utilizing trust management systems to assess the reliability of the nodes involved.

The proposed secure transportation system aims to address privacy concerns associated with the dissemination of sensitive vehicle data, while also ensuring the protection of the authenticity and secrecy of cooperative awareness messages (CAMs). Ensuring a safe and resilient VANET infrastructure is of utmost importance as the presence of connected and autonomous vehicles increases in the transportation industry. This study establishes the foundation for future transportation systems that prioritize safety and efficiency by providing assistance to the current endeavors in developing a dependable and protected communication framework within VANETs.

2. Literature review

VANET privacy solutions aim to thwart the possibility of linking cooperative awareness messages (CAMs) by regularly altering pseudonyms within unmonitored mix-contexts. To ensure that an opponent cannot link the two consecutive messages of the previous and current pseudonyms with the CAM spatiotemporal data, it is essential to maintain unobservability. To avoid a situation where a single pseudonym change can be easily linked, numerous neighboring cars simultaneously change their pseudonyms in a mixed setting. Unobserved mix-contexts are commonly established through the modification of pseudonyms within cryptographic mix-zones or by incorporating a period of silence before a pseudonym change. Changing pseudonyms alone does not effectively prevent vehicle tracking without the presence of unobserved mix-contexts[7,8]. While cars merge or switching lanes while entering or leaving a roadway, Sampigethaya and colleagues[9] utilize silent intervals in vehicle ad hoc network (VANETs). A symmetric key may be obtained from the road-side unit (RSU) in charge of the mix zone, allowing cars to scramble all messages within the Cryptographic MIX-zone (CMIX), according to Freudiger et al.[10]. Vehicles inside the permitted region

can request to have keys sent to them so that the riverside unit (RSU) can decode communications received by cars outside of that range. Buttyan and others[11] states that the plan is to stop sending messages when a car slows down, such at a crossroads. The rationale behind selecting low-speed engagements is that intersections and comparable locations inherently host a large number of cars, rendering them perfect settings for interactions between vehicles. Plus, accidents resulting in death are less common while traveling at slower speeds. Wei and Chen[12] suggest using a safety analysis method to determine an appropriate distance to conceal a vehicle's position, velocity, and direction. Additionally, they suggest adjusting the length of the quiet period according on the distance between other cars. Therefore, the duration of the period of inactivity decreases as the distance between cars increases. A paradigm for mix zone design and deployment, the MobiMix framework is introduced by the aforementioned Palanisamy et al.[13] and successfully defends against timed and transition assaults. Introducing MixGroup, a mechanism that makes the most of the few chances for cars to change their pseudonyms during meetings, is the most recent suggestion of Yu et al.[14]. They also build long zones for changing pseudonyms, where cars may use group signature to progressively change pseudonyms. It costs money to keep people's location secrets private. If applications' pseudonyms are changed or they are idle for a while, their performance could drop. Communications quality, quality of data (position inaccuracy), and app needs are the three metric categories that may be used to quantify quality of service (QoS) in connected work. Many factors are considered while evaluating QoS. Looking at how changes to pseudonyms affect spatial routing performance is something that Schoch et al.[15] do in the field of communication quality. Low traffic density as well as frequent frequency shifts (i.e., intervals of less than 30 s) significantly degrade performance, according to their findings. By analyzing the time of its receipt at various distances and relative speeds, Calandriello et al.[16] evaluate the effects of altering a pseudonym. For applications that monitor traffic, Hoh and colleagues[17] provide a QoS measure. Considering data quality parameters, this metric calculates the error linked to each location sample.

Problem identification

Determining privacy-related issues in VANETs is essential to creating workable solutions. The following are some major issues with privacy in VANETs:

1) Location privacy: Vehicles that continuously broadcast their location are vulnerable to tracking, which could result in privacy violations.
2) Identity linkage: User privacy may be jeopardized when unique identifiers or pseudonyms are connected to the true identities of automobiles.
3) Communication-related data leakage: Unprotected routes of communication can leave confidential information open to prying eyes and illegal access.

3. Proposed methodology

3.1. Forward collision warming (FCW)

Problem with a lane change notice shows in **Figure 1**. While another car (OV1) is in the blind spot, the target vehicle (SV) must transfer lanes to the left. One possible cause of rear-end collisions is another vehicle's (OV2) high speed. The presence of a third car (OV3) in the third path, however, shouldn't pose any danger of a collision[18].

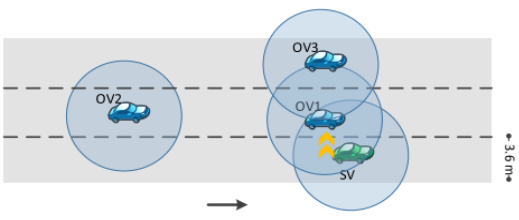


Figure 1. Problem with a lane change notice.

Forward collision warming (FCW) system flow chart shown in **Figure 2**. The purpose of the FCW use was to provide the target vehicle's (SV) driver enough warning before a different car (the OV) in the same zone might cause a collision. To do this, the computer must be able to do two things accurately: (1) choose which OV lane to use and (2) determine the time to contact (TTC) within a small margin of error. The first need can only be satisfied with a thorough familiarity with the lateral locations of the SV and OVs. The second criterion can be met if the following information is known: the longitudinal locations and speeds of the following OV in the same lane, as well as the SV. By calculating the likelihood of accurate positives (Ptrue) and negatives (Pfalse) using the approach outlined, the lanes of the OV1, OV2 s may be accurately identified as Equations (1) and (2).

$$\text{Ptrue} += \text{P}(|y\text{OV1} - y\text{SV}| \leq 1.8) \quad (1)$$

$$\text{Pfalse} += \text{P}(|y\text{OV2} - y\text{SV}| \leq 1.8) \quad (2)$$

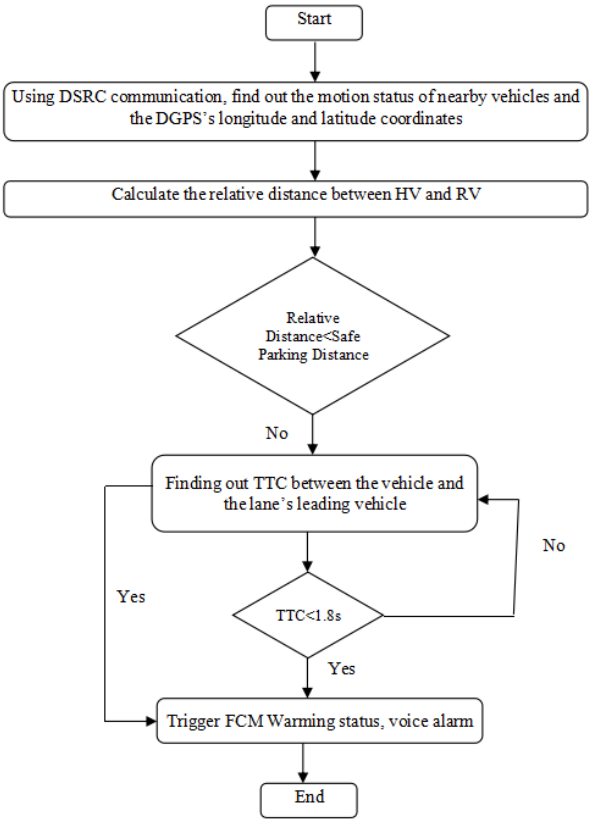


Figure 2. Forward Collision Warming (FCW) system flow chart.

Assuming the SV is coming towards the OV1 at a speed differential of 5 to 15 m/s will allow us to fulfill the second condition. In this case, for example, OV1's real position is determined to be one second before SV's actual location, presuming that TTC is likewise three seconds. In this case, we don't use binary classification to find false positives; instead, we determine the likelihood of determining TTC within a 500 ms limit. The maximum time for providing a helpful warning is 500 ms, as demonstrated by Shladover and Tan[19]. Here are the procedures to calculate the period from collision to collision (PTTC) and get a precise estimate with 500 ms as Equations (3) and (4):

$$\text{TTC} = x\text{OV1} - x\text{SV}\dot{x}\text{SV} - \dot{x}\text{OV1} \quad (3)$$

$$\text{PTTC} = P(|\text{TTC} - 3| \leq 0.5) \quad (4)$$

Equations (3) and (4) computes the frequency at which the discrepancy between the actual time to collision (TTC), which is 3 s, and the estimated TTC is smaller than the tolerance level of 0.5 s. Ultimately, if all three probabilities are independent as Equation (5),

$$\mathrm{PFCW}\Delta s = \mathrm{Ptrue} + \times (1 - \mathrm{Pfalse}+) \times \mathrm{PTTC}\Delta s \quad (5)$$

3.2. Lane change warning (LCW)

Blind spot and passing are the two primary situations shown in the graphic that pertain to LCW use. A possible accident might occur when the topic vehicle (SV) switches lanes because another vehicle (OV1) is traveling at a comparable speed in the next lane, slightly behind the SV, in the blind spot region. Since OV3 is in the third lanes and doesn't pose a threat to the SV, it's the LCW system that's connected to the SV should only warn users to OV1 instead of alerting them to OV3. When an overtaking scenario arises, the OV2 car comes up behind the SV car at a fast enough speed to pass it when they both switch lanes at the same time. Due to the fact that OV2 might potentially overtake the SV after a lane change if it is traveling at a speed that permits it to quickly approach, a warning should be sent. By switching the positions of OV and SV, this shows how the passing scenario is identical to the FCW scenario[20].

The SV needs to correctly detect three needs in order to fix the blind spot. Finding the horizontal location of OV1 in the next lane (whose precise midway is 3.6 m from the SV) is the first step. Furthermore, its longitudinal location should be estimated to be somewhat behind the SV, ranging from 1.5 m to 6 m behind the SV's longitudinal position. Hence, its midway within this range, 3.75 m from the SV, is considered to be its exact longitudinal placement. Second, we need to find OV3 and determine that it is not in the lane next to us; this will tell us that its real lateral location is 7.2 m away from the SV. The last requirement is that, for example, the velocity differences of OV1 or SV should be recognized as being similar to within a small margin of 3 m/s. As a result, we will pretend that SV and OV1 really travel at the same speed. This study presupposes that the SV's reliance on internal sensors rather than a VANET transmission to get position and speed information is the primary cause of the SV measurements' errors. According to these parameters, the following are the locations and speeds of SV, OV1, and OV3 as Equations (6)–(12):

$$y\mathrm{SV} = 1.8 + N(0,0.5) \quad (6)$$

$$x\mathrm{SV} = 3.75 + N(0,0.5) \quad (7)$$

$$\dot{x}\mathrm{SV} = \hat{x}\mathrm{SV} + N(0,0.02 \cdot \hat{x}\mathrm{SV}) \quad (8)$$

$$y\mathrm{OV1} = 5.4 + \delta y \quad (9)$$

$$x\mathrm{OV1} = \delta x \quad (10)$$

$$\dot{x}\mathrm{OV1} = \hat{x}\mathrm{OV1} + \delta\dot{x} \quad (11)$$

$$y\mathrm{OV3} = 9 + \delta y \quad (12)$$

If $\dot{x}\mathrm{OV1}$ is equal to $\hat{x}\mathrm{OV1}$, then $\hat{x}\mathrm{SV}$ is the filtered longitudinal speed. For each condition, further analysis is needed for those Monte Carlo equations. Since the SV and ovarian cancer1 are both 2 m wide, the OV1 must make sure that the SV has enough space to go into the adjacent lane. The exact center of the OV1 should be three meters from the opposite border of the lane when the SV switches lanes. Consequently, the blind spot warning system should go off if there's an estimated distance of 4.8 m or less among the subject car (SV) and the other car (OV1). To avoid an incorrect OV3 warning, picture a three-meter-wide vehicle moving exactly along the third lane's edge. About fifteen meters from the lane boundary is where the object's center is situated[21]. Hence, the system shouldn't sound an alarm if there's more than 6.9 m among the centers of OV3 and SV. Therefore, assessing OV1 for an angle less than 6.9 m determines the chance of accurately selecting a good outcome. When the estimated OV3 is within 4.8 m, or less, the false negative probability is computed. In addition, OV1 needs to be precisely located within the Sr's blind area, which means it needs to be 1.5 to 6 m back the SV so it doesn't draw the attention of the driver. The velocities of OV1 and SV must also be approximated as being similar, with a small margin of uncertainty around 3 m/s. Here is the way these probabilities are expressed as Equations (13)–(17):

$$\mathrm{Ptrue}+= P(y\mathrm{OV1} - y\mathrm{SV} < 6.9) \quad (13)$$

$$\text{Pfalse}+= P(y\text{OV3} - y\text{SV} \leq 4.8) \quad (14)$$

$$\text{Plong} = P(x\text{SV} - x\text{OV1} < 6 \wedge x\text{SV} - x\text{OV1} > 1.5) \quad (15)$$

$$Ps = P(|\dot{x}\text{OV1} - \dot{x}\text{SV}| \leq 3) \quad (16)$$

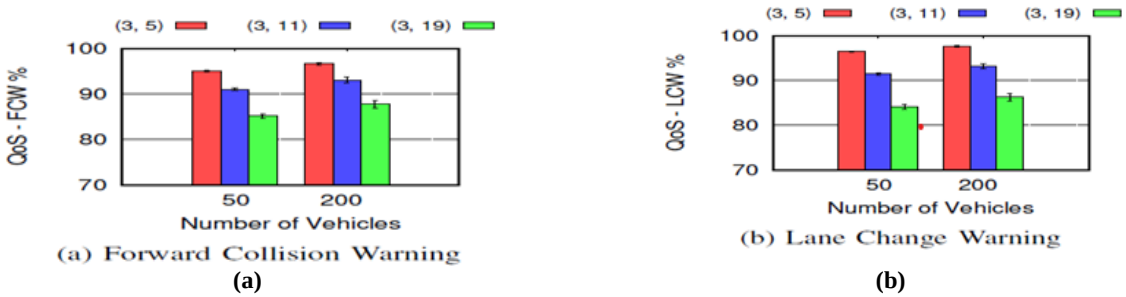
$$\text{PLCW} = \text{Ptrue} + \times (1 - \text{Pfalse} +) \times \text{Plong} \times Ps \quad (17)$$

Calculate the privacy loss without channels weighting (PLCW) and privacy factor without channel weighing (PFCW) to evaluate how a privacy strategy impacts the QoS of safety apps. To get the final QoS %, take the lowest figure among the two and multiply it by 100. In official terms, a privacy scheme's quantity of service (QoS) as Equation (18):

$$\text{QoS} = \{\text{PFCW}, \text{PLCW}\} \times 100 \quad (18)$$

4. Result and discussion

The performance evaluation metrics are quality of service (QoS) for forward collision warning (FCW) and lane change warning (LCW), communication delay (CD) and packet loss rate (PLR) used for this experiment.



(a) **(b)**

Figure 3. (a) quality of service (QoS) of forward collision warning (FCW); **(b)** quality of service (QoS) of lane change warning (LCW).

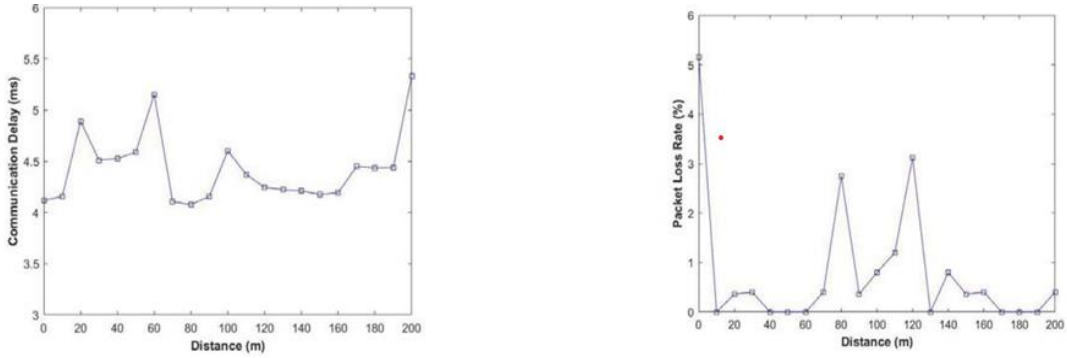
Figure 3a,b displays the quality of service (QoS) of FCW and LCW applications in STRAW traces that have been altered by the random quiet period privacy method, with a CAM rate of 2 Hz. When a silent period ranging from 3 to 11 seconds is used, it is possible to achieve a quality of service (QoS) level over 90% in all scenarios. The simulation research demonstrates that the quality of service (QoS) is satisfactory for both FCW and LCW. The execution outcome demonstrates superior quality of service (QoS) in LCW as opposed to FCW.

$$\text{QoS} = \min\{\text{PFCW}; \text{PLCW}\} * 100$$

Relationship diagrams:

Figure 4a illustrates the correlation between the transmission delay and the interaction distance. The highest delay detected within the 0–200 m range is 5.3 milliseconds. The incremental increase in distance will have minimal impact on the delay, which remains relatively consistent within the range of 4.1–4.8 ms. In a few instances, the delay may slightly surpass 5 ms.

The relationship between the distance of communication between devices and the packet loss rate is shown in **Figure 4b**. Over the communication range of 0–200 inches, the packet loss rate of the DSRC transmitters BSM payload varies, although it typically remains around 3%. The data packet loss peaks at 5% at a length of 0 inches, which is quite high. The change in coupling mode and the close proximity of the OBEs are the causes of this. Because two-vehicle collisions and intersections are the norm, may ignore this situation. Tags encapsulate the user's text.



(a) **(b)**

Figure 4. (a) communication delay (CD) and distance; **(b)** packet loss rate (PLR) and distance.

5. Conclusion

A new class of apps that collect supplementary data on how people move has emerged as a result of the broad adoption of advanced position-tracking and mobile communications technologies. So far, this technique in order to increase route confusion, built and evaluated a data perturbation approach that slightly alters the reported locations of two nearby users. This approach may protect forward collision warming (FCW), unlike other location privacy. This method has the potential to limit the amount of time an attacker may follow and spy on a certain person. When contrasted to a lane change warning (LCW) method improves privacy by decreasing the average location error, which leads to a smaller penalty for quality of service. In addition, the user concentration goals of traffic tracking devices are well-aligned with the promising outputs of the proposed method in an area with around 10 cars per square mile.

Author contributions

Conceptualization, TSB and DVSB; methodology, TSB; software, TSB; validation, TSB, DVSB and JB; formal analysis, AV; investigation, ME; resources, RSS; data curation, GS; writing—original draft preparation, TSB; writing—review and editing, AV and RSS; visualization, ME; supervision, JB; project administration, GS. All authors have read and agreed to the published version of the manuscript.

Conflict of interest

The authors declare no conflict of interest.

References

1. Okpok M, Kihei B. Challenges and Opportunities for Multimedia Transmission in Vehicular Ad Hoc Networks: A Comprehensive Review. Electronics. 2023; 12(20): 4310. doi: 10.3390/electronics12204310
2. Khanpara P, Bhojak S. Routing Protocols and Security Issues in Vehicular Ad hoc Networks: A Review. Journal of Physics: Conference Series. 2022; 2325(1): 012042. doi: 10.1088/1742-6596/2325/1/012042
3. Choudhary D, Pahuja R. Awareness routing algorithm in vehicular ad-hoc networks (VANETs). Journal of Big Data. 2023; 10(1). doi: 10.1186/s40537-023-00742-3
4. Oladimeji D, Gupta K, Kose NA, et al. Smart Transportation: An Overview of Technologies and Applications. Sensors. 2023; 23(8): 3880. doi: 10.3390/s23083880
5. Ali ZH, Ali HA. Energy-efficient routing protocol on public roads using real-time traffic information. Telecommunication Systems. 2023; 82(4): 465-486. doi: 10.1007/s11235-023-00993-8
6. Toulni H, Miyara M, Filali Y, et al. Preventing urban traffic congestion using VANET technology in urban area. Koumétio Tékouabou SC, Chenal J, Diop EB, Azmi R, eds. E3S Web of Conferences. 2023; 418: 02005. doi: 10.1051/e3sconf/202341802005
7. Emara K, Woerndl W, Schlichter J. Vehicle tracking using vehicular network beacons. In: Proceedings of the 2013 IEEE 14th International Symposium on “A World of Wireless, Mobile and Multimedia Networks” (WoWMoM). doi: 10.1109/wowmom.2013.6583473
8. Wiedersheim B, Ma Z, Kargl F, et al. Privacy in inter-vehicular networks: Why simple pseudonym change is not

enough. In: Proceedings of the 2010 Seventh International Conference on Wireless On-demand Network Systems and Services (WONS). doi: 10.1109/wons.2010.5437115
9. Sampigethaya K, Li M, Huang L, Poovendran R. AMOEBA: Robust location privacy scheme for VANET. IEEE Journal on Selected Areas in communications. 2007; 25(8): 1569-1589.
10. Freudiger J, Raya M, Felegyh M, et al. Mix-Zones for Location Privacy in Vehicular Networks. In: ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS); Vancouver, Canada; 2007. pp. 1-7.
11. Buttyán L, Holczer T, Weimerskirch A, Whyte W. Slow: A practical pseudonym changing scheme for location privacy in vanets. In: Proceedings of the 2009 IEEE vehicular networking conference (VNC); 28–30 October 2009; Tokyo, Japan. pp. 1-8.
12. Wei YC, Chen YM. Safe distance based location privacy in vehicular networks. In: Proceedings of the 2010 IEEE 71st Vehicular Technology Conference; 16–19 May 2010; Taipei, Taiwan. pp. 1-5.
13. Palanisamy B, Liu L. Attack-Resilient Mix-zones over Road Networks: Architecture and Algorithms. IEEE Transactions on Mobile Computing. 2015; 14(3): 495-508. doi: 10.1109/tmc.2014.2321747
14. Yu R, Kang J, Huang X, et al. MixGroup: Accumulative Pseudonym Exchanging for Location Privacy Enhancement in Vehicular Social Networks. IEEE Transactions on Dependable and Secure Computing. 2016; 13(1): 93-105. doi: 10.1109/tdsc.2015.2399291
15. Schoch E, Kargl F, Leinmüller T, et al. Impact of pseudonym changes on geographic routing in vanets. In: Proceedings of the Security and Privacy in Ad-Hoc and Sensor Networks: Third European Workshop, ESAS; 20–21 September 2006; Hamburg, Germany. pp. 43-57.
16. Calandriello G, Papadimitratos P, Hubaux, JP, Lioy A. Efficient and robust pseudonymous authentication in VANET. In: Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks; 2007. pp. 19-28.
17. Hoh B, Gruteser M. Protecting location privacy through path confusion. In: Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05); 5–9 September 2005; Athens, Greece. pp. 194-205.
18. Lefevre S, Petit J, Bajcsy R, Laugier C, Kargl F. Impact of v2x privacy strategies on intersection collision avoidance systems. In: Proceedings of the IEEE Vehicular Networking Conference; 16–18 December 2013; Boston, MA, USA. pp. 71-78.
19. Yang T, Zhang Y, Tan J. Research on forward collision warning system based on connected vehicle V2V communication. In: Proceedings of the 5th International Conference on Transportation Information and Safety (ICTIS). pp. 1174-1181.
20. Shladover SE, Tan SK. Analysis of Vehicle Positioning Accuracy Requirements for Communication-Based Cooperative Collision Warning. Journal of Intelligent Transportation Systems. 2006; 10(3): 131-140. doi: 10.1080/15472450600793610
21. Senthamil Selvan R, Analysis of EDFC and ADFC Algorithms for Secure Communication. Journal of Advanced Research in Dynamical and Control System. 2017; 9(18): 1171-1187.