A Survey on Secure Safety Applications in VANET

Ruqayah Al-ani*, Bo Zhou*, Qi Shi*, Ali Sagheer+
* Department of computer Science Liverpool John Moores University Liverpool, UK
+Al Qalam College, Kirkuk, Iraq
Email: R.A.Alani@2015.ljmu.ac.uk

***Abstract*—Providing an efficient secure authentication scheme in safety applications in Vehicular Ad-hoc Networks (VANETs) is a challenging issue. This is because these applications need to react to their messages, in a timely manner, before their respective deadlines. Preserving the privacy of the exchanged messages is also important since these messages include sensitive information, such as geographical locations. In this paper, we review the existing schemes that aim to meet the requirements of security and privacy. Then, we specify these requirements with a view to design an efficient scheme for secure real-time applications in VANET environments.**

Index Terms— security, privacy preserving, VANET, safety applications

I. INTRODUCTION

Due to the increasing demands to improve traffic safety, Vehicular Ad-hoc Networks (VANETs) have attracted attention from governments, car manufactures, and researchers. In VANETs, vehicles equipped with on-board units (OBUs) are able to collect, process and exchange traffic-related messages with nearby vehicles through Vehicle-to-Vehicle (V2V) communications, or communicate with nearby road-side units (RSUs) through Vehicle-to-Roadside (V2R) communications.

Most VANET safety applications require timely reactions to the broadcasted messages. Relying on a Dedicated Short-rang communication (DSRC), instead of a cellular network communication, would reduce delays when uploading and downloading traffic-related messages. Accordingly, the IEEE 1609.2 standard mandates a DSRC system when developing VANET applications, which supports both V2V and V2R communications. Moreover, safety-related applications rely on a single-hop beaconing message, wherein messages are broadcast every 100-300 ms within a communication range of 300 m. A beaconing message may contains a vehicle's position, speed, acceleration, and the direction of a vehicle, which all can be used towards cooperative-awareness between vehicles. In addition, they may also contain safety events, such as when an accident occurs.

Despite the advantages that can be obtained from VANET safety applications, the sole source of communication of this network is through wireless links, which are vulnerable to a variety of attacks. For example, they are susceptible to third parties injecting bogus messages, replaying old messages, and modifying messages. Since these messages are urgent and often life-critical, it is a highly important to implement a security mechanism for authenticating these messages. Furthermore, an attacker can collect these messages and compromise the privacy of the driver, by obtaining his location. Thus, the privacy of the driver must be protected from unauthorised accesses.

The designed scheme should achieve an acceptable balance between security and privacy requirements. Moreover, the scheme should be highly efficient in supporting applications with real-time requirements.

pseudonym-based authentication schemes are widely used in order to enable the authentication of the broadcast messages anonymously [1]. This is when aauthentication between vehicles is conducted through dummy identities, which are authenticated by the trusted authorities (TAs) in order to reveal the real identity in case of a dispute.

The unique characteristics of VANETs, such as their high mobility and their large number of nodes, would challenge the exiting security schemes. For example, most of pseudonym-based authentication schemes employ digital signatures to offer secure communication between VANET entities, which leads to processing delays of traffic-related messages.

In this paper, we highlight the security and privacy requirements of safety applications. First, some safety applications are given in subsection II.A. Then, the security, privacy requirements and their main challenges in VANET are outlined in II.B, II.C, and II.D, respectively. In section III, the well-known pseudonym schemes, along with their changing strategies, are illustrated. After this, some existing work to enhance the efficiency of the verification process is given in section III. Finally, in section IV, we discuss and conclude the main requirements to designing an efficient privacy preserving authentication scheme for VANET safety applications.

II. VANET APPLICATIONS, REQUIREMENTS AND ITS CHALLENGES

A. Road-Safety Applications

Drivers are responsible for most hazardous road accidents [2]. Road-safety applications are primarily aimed at reducing these accidents and saving lives on the road through exchanging safety messages between nearby vehicles and RSUs. Accordingly, these messages may assist drivers to broaden their knowledge about their surrounding environment, through exchange messages regarding intersections, traffic-jams, accidents, and even by predicting collisions [3]. Most of these applications demand strict requirements, such as low latency, which is 100-1000 ms, broadcasting messages every 10 Hz [4]. Moreover, most of these applications depend on information that is directly exchanged between vehicles, i.e. single hop communications, in order to reduce the delay due to multi-hop communications. Some of these applications are given below which are described in [3, 5-9].

- Lane change warnings: warn the driver if the lane change occurs in their blind spot area. This has potentially reduced crashes during lane change scenarios.
- Forward collision warnings: warns the driver of an expected rear-end collision with a heading vehicle driving in the same lane and direction, due to, for example, slowdowns or the road curvature.
- Head on collision warnings: provide early warnings that are sent to vehicles that are travelling in opposite directions.
- Intersection collision warnings: warn the driver when approaching road intersections if there is a high collision probability with other vehicles.
- Emergency vehicle warnings: if there is an active emergency vehicle, such as a police car or an ambulance, a warning is sent to nearby vehicles as well as RSUs which they re-broadcast in order to free a corridor.

B. *Security Requirements*

Security is obviously paramount in road-safety applications. Malicious messages sent out by attackers could cause severe damage, and threaten our safety. In this subsection, we outline the major security requirements for VANET:

- Sender validity: one major requirement of VANET is to ensure that a received message is generated by a legitimate entity. This is because vehicles make decisions depending on the received message, which can be life-critical [10].
- Message integrity: the integrity of the received message is important when ensuring that the messages send over the network have not been altered by malicious attacks or signal failures [11].
- Non-repudiation: users should not be able to deny sending a message. Thus, in case of dispute, the sender would accountable. However, only a TA authority should be allowed to trace the message of the misbehaving sender [10].

C. *Privacy Requirements*

In VANET, it is essential to protect the privacy of the driver/vehicle, rather than RSUs and public vehicles, such as ambulances. However, we encourage road users to share as much information as possible in order to enhance the accuracy and timeliness of road-safety applications. Aattackers actually could identify and extract useful information, such as the whereabouts of a particular user, simply based on the message he/she periodically broadcasts. It may put the user off if their privacy cannot be protected. Schaub et al.[12] identify the following privacy requirements:

- Minimum disclosure: Only the required information should be disseminated during communication.
- Conditional anonymity: the incentive sender of the message should be unknown. However, identity resolution by legal authorities is possible in some situations, such as misbehaving situations.
- Unlinkability: messages sent by the same vehicles are not linkable. However, safety-applications require short-term linkability[13].
- Distributed resolution authority: it is preferable that identity resolution can only be conducted by the cooperation of several entities.
- Perfect forward privacy: the resolution of a specific events to its identity should not reveal further information that decreases its unlinkability.

D. *VANET Challenges*

The special behaviour and characteristics of VANETs leads to particular challenges, which impact the future deployments of these networks, as discussed below.

- The trade-off between security and privacy requirements: to provide secure communication, it is necessary to authenticate all exchanged messages. However, this leads to identifying and tracking vehicles from these messages. The use of pseudonyms as short-term public keys without any identification information has emerged as a solution to provide an acceptable balance between these requirements [1]. Pseudonym-based schemes will be explained later in this paper.
- Real-time constraints: in safety-related applications, the broadcast messages are time-critical and they have expiration time of 100-1000 ms within a communication range of 300- 1000 meters [8]. Thus, it is necessary to minimizing the processing overhead due to the timeliness of these messages.
- Dynamic nature and high mobility: the topology of VANET changes rapidly from time to time, as a result of the speed of vehicles, especially on highways [14]. Thus, cooperative authentication protocols [15-17] and RSU-aided authentication protocols [18-20] are not feasible, due to frequent link disconnections.
- The large scale of the network: in the future, VANET will compromise millions of vehicle. Thus, applications and mechanisms should be able to handle a large number of vehicles [12].

III. SURVEY ON PREVIOUS WORKS

In this section, we carry out a survey on existing works in relation to secure VANET communications. We categorise these works based on the strategies they employ.

A. *Categories of Pseudonym schemes:*

Pseudonym authentication schemes have been widely used to secure communications between VANETs entities. Anonymous keys are used to digitally sign the sent messages. Then, the signature is used to verify the integrity and the authenticity of the received message. To apply pseudonymity within secure communication in VANET, most researchers have utilised asymmetric key cryptography concept. On the other hand, other researches, due to the delay constrains for safety messages, have utilised symmetric key cryptography concept. The main motivations of these schemes are given below.

a) *Public key Based cryptography (PBC) schemes:* Public key cryptography is an asymmetric form of cryptography in which a pair of keys are used to achieve the secure communications between VANET entities. One key is used to sign the sent message, which is the private key, while the other key is used to verify the received message, which is the public key. The public key must be certified by a TA to verify the legitimacy of the sender. Then, the certified public key is used as a pseudonym instead of the real identity [21]. However, using a static pseudonym is insufficient to protect the privacy, due to tracking and eavesdropped messages for a long time. Thus, Raya and Hubax suggest providing each vehicle with a set of pseudonyms and corresponding key pairs (public key and private key) [22]. Each pseudonym is valid for a specific period. Vehicles sign messages using the private key of the current valid pseudonym. Each pseudonym is valid for a specific period.

b) *Identity based cryptography (IBC) schemes:* Identity based cryptography is related to the public key cryptography concept with the significant difference that only a key generation centre (KGC), which is assumed to be a TA, is able to derive the pair of keys from the node's public information, such as their name, email address, telephone number, etc. The IBC concept was first proposed by Shamir (1984), who suggest that secure communication between entities can be achieved without exchanging keys, since the public key is derived from the identity of the node. Moreover, there is no need for an explicit certificate, because the only one who is able to derive the pair of keys is the KGC, i.e. implicitly certificate keys [23]. In VANET, to achieve pseudonymity, these keys should be extracted from arbitrary strings and used as a pseudonym. Then, this pseudonym would be sent with the signed message for authentication. The communication overhead will be enhanced over the PKC, because there is no need for exchanging the certificates for this pseudonym [24]. However, IBC is similar to PKC, because it still needs a number of pseudonyms to protect individuals' privacy.

c) *Group based cryptography (GBC) schemes:* Group based cryptography is asymmetric cryptography, which was first introduced by Chaun and Van Heyst in 1991 [25], who proposed a group manger (GM), which is assumed to be a TA, who is responsible for issuing a shared public key for each group to be used as a pseudonym during communication, while each group member has its own private key to generate the signature over the exchanged messages. Thus, GBC would preserve individuals' privacy without the need to change pseudonyms, which leads to eliminating the need for issuing and storing thousands of pseudonyms in PKC and IBC [26].

d) *Symmetric based cryptography (SBC) schemes:* In symmetric based cryptography, the same key is used to sign and verify the exchanged message. These schemes are highly efficient in term of computational and communicational overheads because the main underlying cryptographic function is a hashed-based message authentication code (HMAC) [27, 28].

B. Privacy Preserving Strategies

In the PBC, IBC and SBC schemes, pseudonyms must be changed periodically to avoid long-term tracking. On the other hand, in GBC schemes, full anonymity is achieved within the group members.

All messages authenticated with one pseudonym are linkable to each other. Short-term linkability is important for safety applications, such as if an accident happened and two messages with different pseudonyms were received from the same sender, the receiver would think there are two accidents. Thus, there is a need to find a balance between the privacy level and its impact on the quality of safety applications. In addition, simple pseudonyms changing are insufficient in avoiding long-term tracking, because attackers can re-identify vehicle by analysing their messages [29]. There is a large body of literature that examines changing pseudonyms, with view to achieve a sufficient level of privacy protection. We will discuss some strategies below.

- A vehicle changes its pseudonyms depending on a fixed time, i.e. each pseudonym would be valid for a specific time slot [30]. However, tracking is trivial in this strategy, because it is easy for the observer to know the period of time that the pseudonyms change. To solve this, a random period was suggested in [31]. However, tracking is still trivial if there is just a few number of vehicles on the road. Thus, in [32], changing pseudonyms are mandated depending on the density of the vehicles. A better strategy was suggested in [30] to collaboratively changing pseudonyms with neighbours' vehicles.

- In [33-35] hindering vehicle prediction tracking was suggested when changing its pseudonym by remaining silent for a period of time after changing. However, during this period, it may be the case that there is a critical situation happened that could occur that compromises safety.

- A mix-zone strategy was proposed in [36] to avoid tracking vehicles when changing their pseudonyms. In this strategy, a vehicle will change its pseudonym in a spatial area where there are no-location based applications. This approach would be ineffective if there is a few number of vehicles in the mix-zone area. Accordingly, [37] suggests to place the mix-zone areas at social spots, such as parking areas, to increase the number of vehicles and then confuse tracking. In [38], cryptographic mix-zone areas are proposed, in which RSU distributes a symmetric key for all legitimate vehicles in its communication range, wherein all vehicles use the same key to encrypt messages. Therefore, adversary cannot track specific vehicles. However, the insider attack may still broadcast bogus messages, which could be life-critical. Traceability is hindered, because all vehicles use the same key. Moreover, the insider attacks can still decrypt all messages and thus compromise individuals' privacy.

- A distributed mechanism was proposed in [39], wherein each vehicle is responsible to decide when and where to change its pseudonyms, depending on its beacon context, such as its speed and direction. The same mechanism was enhanced by [40], in which a silent-period strategy was applied to increase the level of privacy. In [41], using content-based changing in [39] was combined with a number of criteria towards performing pseudonym

changing, such as the age of a pseudonym. This would decrease the need for changing pseudonyms.

C. Enhancing Scaliability in Safety applications

Current standardisations and research efforts mainly support the use of the PBC system using the traditional Public Key Infrastructure (PKI) for key management. Furthermore, to reduce communicational overheads, ECDSA is used to sign the exchanged messages, due to its small key size when compared with other cryptosystems, such as RSA i.e. to reach a security level of 128 bits, ECDSA requires 256-bit key size while RSA requires 3072-bit key size. The use of PKI with ECDSA system was already adopted by the initial IEEE 1609.2 standard [42] to secure VANET safety applications.

The existing PKI schemes still suffer from high computational costs in the verification process of both certificate and signature verification. This would not be an issue in a sparse density areas, but it fails to meet the requirement of verifying hundreds of messages per second in high density areas. Therefore, an efficient scheme is still needed to increase the number of verified messages before being expired.

According to IEEE 1609.2 standards, vehicles will periodically broadcast beacon messages about their current status every 100-300 ms to enable safety applications. These messages need to exchange information securely. Security overheads should be as low as possible to allow timely reactions to the broadcast messages. Spatially, it is likely that other applications would run on the same OBU. However, the existence of security mechanisms incur considerable communication and computation overheads, which can influence the performance of these applications in high-density traffic scenarios [43].

In order to solve the issue of receiving a large number of messages in a short time period in VANET real-time applications, researchers have been working to design an efficient PBC security mechanism. Some of these efforts are mentioned below.

a) *Probabilistic verification schemes:* in [22], Raya and Hubax suggested verifying only the relevant messages. Similarly, Grover and Lim in [44] designed a probabilistic scheme to maximise the number of relevant verifications in which a higher priority will be assigned for messages received from a closer vehicle. However, this method is vulnerable to signature flooding, where the attacker sends many bogus messages and has an impact on verifying legitimate messages.

b) *Hybrid verification schemes:* in [45], the combination of symmetric and asymmetric cryptography mechanisms is proposed, in which HMAC and ECDSA is used to securely broadcast messages. The non-repudiation of critical messages is achieved by using the ECDSA. The fast verification for non-critical messages is enabled using a simple HMAC. However, this scheme still cannot meet timely verification, due to delay of key disclosure. Moreover, the communication cost would be increased as a result of sending both HMAC and digital signatures along with each message.

c) *Prediction Based schemes:* To allow for timely-verification in the hybrid schemes, in [46, 47] exploit the ability of a vehicle to predict future beacons. Then, the sender constructs a Merkle Hash Tree (MHT) to generate a common public key. It first derives a number of private keys, which are associated with the predicted beacons. Then, the private keys tie together to produce the common public key, which is sent to the receiver in advance to enable the timely-reactions of exchanged messages. However, these schemes incur communication overheads due to the size of their signatures and keys [46].

d) *Trusted authentication Schemes:* in [48, 49], firstly, RSU authenticates vehicles using ECDSA and then a secret sharing key is exchange between legitimate vehicles. The drawback of these schemes are the difficulties to establishing consistent neighbours, as well as the fact that insider attackers can send bogus messages.

IV. Discussion

The schemes in section III.A. have faced strong challenges to efficiently secure safety applications, due to the following reasons:

- IBC and GBC schemes are mainly dominated by a few pairing operations. Batch verification is widely used to reduce the processing overheads of pairing in which multiple messages are verified at once [50-54]. However, these schemes are mainly dependent on RSUs, because its computational overhead still not affordable for vehicles with a 400 MHz processor [47].
- GBC and SBC schemes suffer from key distributing issues. Thus, their schemes are mainly dependent on the existing RSUs' ability in securely issuing their keys [55].
- SBC schemes are lacking in the timely authentication of messages, due to delayed key disclosure to ensure the source of the messages [45]. Moreover, symmetric schemes have difficulties when providing non-repudiation [56].

After providing an overview of the primary security and privacy requirements, as well as their impact on the efficiency of VANET applications, we outlined the following real-time authentication requirements:

- It is impractical to authenticate safety-message depending on the support of backend infrastructure such as RSUs. This is because of the sparse disseminations of RSUs.
- Cooperative authentication schemes are impractical due to the speed of vehicles, i.e. vehicle connections with their neighbours do not last for a long time.
- Improving the efficiency of verification is important in high density areas, since vehicles would sign one message while need to verify *n* messages from *n* neighbouring vehicles. This may lead to scalability issues.
- A decentralised authentication scheme is preferable, in which a vehicle can authenticate messages individually due the intermittent connectivity with other entities and the timeliness of safety messages. Thus, the delivery delay is reduced when messages are sent in a single-hop.

- Changing pseudonyms should not impact the quality of applications, such as in a silent period strategy. At the same time, the level of privacy should be kept high. Moreover, it is difficult to build trust between VANET entities, which may affect the cooperative changing strategy. Thus, a distributed strategy seems to be a better candidate, but the existing mechanism need to be investigated in order to achieve an acceptable level of privacy preservation.

V. CONCLUSIONS AND FUTURE WORK

To conclude, Public Key Cryptographic (PBC) schemes seem to be the better candidates towards securing messages with real-time requirements in VANETs. However, the existing schemes still suffer from an issue in a high density scenario. Accordingly, we have outlined in section III. number of research efforts to enhance the efficiency of verifying messages.

Moreover, we highlighted number of pseudonyms changing strategies research efforts to enhance the efficiently of protecting the privacy of vehicles. In their methods the quality of safety applications still need to be improved.

In our future work, we will focus on enhancing the efficiency of verifying hundreds of messages in the case of density traffic scenarios. Then, we plan to design an improved pseudonyms changing strategy to obtain an acceptable balance between the privacy level and the quality of safety applications.

REFERENCES

[1] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," IEEE communications surveys & tutorials, vol. 17, no. 1, pp. 228-255, 2015.

[2] K. Kowalenko, "Keeping cars from crashing," IEEE The Institute, vol. 9, no. 1, 2010.

[3] G. Karagiannis et al., "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions," IEEE communications surveys & tutorials, vol. 13, no. 4, pp. 584-616, 2011.

[4] F. Bai, T. Elbatt, G. Hollan, H. Krishnan, and V. Sadekar, "Towards characterizing and classifying communication-based automotive applications from a wireless networking perspective," in Proceedings of IEEE Workshop on Automotive Networking and Applications (AutoNet), 2006, pp. 1-25: San Francisco, CA, USA.

[5] T. ETSI, "Intelligent transport systems (ITS); vehicular communications; basic set of applications; definitions," Tech. Rep. ETSI TR 102 6382009.

[6] R. Brignolo, G. Vivo, V. Visintainer, F. Belarbi, and M. Dozza, "Use cases, functional specifications and safety margin applications for the SAFESPOT project," SAFESPOT deliverable SF_D8, vol. 4, 2008.

[7] R. Sengupta, S. Rezaei, S. E. Shladover, D. Cody, S. Dickey, and H. Krishnan, "Cooperative collision warning systems: Concept definition and experimental implementation," Journal of Intelligent Transportation Systems, vol. 11, no. 3, pp. 143-155, 2007.

[8] F. Ahmed-Zaid et al., "Vehicle Safety Communications–Applications (VSC-A) Final Report: Appendix Volume 3 Security," 2011.

[9] J. A. Misener, R. Sengupta, and H. Krishnan, "Cooperative collision warning: Enabling crash avoidance with wireless technology," in 12th World Congress on ITS, 2005, vol. 3.

[10] V. S. Yadav, S. Misra, and M. Afaque, "Security in vehicular ad hoc networks," Security of Self-Organizing Networks: MANET, WSN, WMN, VANET, vol. 227, 2010.

[11] F. Kargl and J. Petit, "Security and privacy in vehicular networks," in Vehicular Communications and Networks: Elsevier, 2015, pp. 171-190.

[12] F. Schaub, Z. Ma, and F. Kargl, "Privacy requirements in vehicular communication systems," in Computational Science and Engineering, 2009. CSE'09. International Conference on, 2009, vol. 3, pp. 139-145: IEEE.

[13] A. Studer, E. Shi, F. Bai, and A. Perrig, "TACKing together efficient authentication, revocation, and privacy in VANETs," in Sensor, Mesh and Ad Hoc Communications and Networks, 2009. SECON'09. 6th Annual IEEE Communications Society Conference on, 2009, pp. 1-9: IEEE.

[14] W. Yang, "Security in Vehicular Ad Hoc Networks (VANETs)," in Wireless Network Security: Theories and Applications, L. Chen, J. Ji, and Z. Zhang, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 95-128.

[15] X. Lin and X. Li, "Achieving efficient cooperative message authentication in vehicular ad hoc networks," IEEE Transactions on Vehicular Technology, vol. 62, no. 7, pp. 3339-3348, 2013.

[16] Y. Hao, Y. Cheng, C. Zhou, and W. Song, "A distributed key management framework with cooperative message authentication in VANETs," IEEE Journal on selected areas in communications, vol. 29, no. 3, pp. 616-629, 2011.

[17] X. Zhu, S. Jiang, L. Wang, and H. Li, "Efficient privacy-preserving authentication for vehicular ad hoc networks," IEEE Transactions on Vehicular Technology, vol. 63, no. 2, pp. 907-919, 2014.

[18] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks," in Communications, 2008. ICC'08. IEEE International Conference on, 2008, pp. 1451-1457: IEEE.

[19] Y. Jiang, M. Shi, X. Shen, and C. Lin, "BAT: A robust signature scheme for vehicular networks using binary authentication tree," IEEE Transactions on Wireless Communications, vol. 8, no. 4, pp. 1974-1983, 2009.

[20] J. Shao, X. Lin, R. Lu, and C. Zuo, "A threshold anonymous authentication protocol for VANETs," IEEE Transactions on vehicular technology, vol. 65, no. 3, pp. 1711-1720, 2016.

[21] M. Gerlach, "Assessing and improving privacy in VANETs," ESCAR, Embedded Security in Cars, 2006.

[22] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," Journal of computer security, vol. 15, no. 1, pp. 39-68, 2007.

[23] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy-preserving protocol for vehicular communications," IEEE Transactions on vehicular technology, vol. 56, no. 6, pp. 3442-3456, 2007.

[24] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in INFOCOM 2008. The 27th Conference on Computer Communications. IEEE, 2008, pp. 246-250: IEEE.

[25] D. Chaum and E. Van Heyst, "Group signatures," in Workshop on the Theory and Application of of Cryptographic Techniques, 1991, pp. 257-265: Springer.

[26] X. Chen, G. Lenzini, S. Mauw, and J. Pang, "A group signature based electronic toll pricing system," in Availability, Reliability and Security (ARES), 2012 Seventh International Conference on, 2012, pp. 85-93: IEEE.

[27] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "The TESLA broadcast authentication protocol," Rsa Cryptobytes, vol. 5, 2005.

[28] Y. Xi, K. Sha, W. Shi, L. Schwiebert, and T. Zhang, "Enforcing privacy using symmetric random key-set in vehicular networks," in Autonomous Decentralized Systems, 2007. ISADS'07. Eighth International Symposium on, 2007, pp. 344-351: IEEE.

[29] M. Burmester, E. Magkos, and V. Chrissikopoulos, "Strengthening privacy protection in vanets," in Networking and Communications, 2008. WIMOB'08. IEEE International Conference on Wireless and Mobile Computing, 2008, pp. 508-513: IEEE.

[30] D. Eckhoff, C. Sommer, T. Gansen, R. German, and F. Dressler, "Strong and affordable location privacy in VANETs: Identity diffusion using time-slots and swapping," in Vehicular Networking Conference (VNC), 2010 IEEE, 2010, pp. 174-181: IEEE.

[31] Y. Pan, J. Li, L. Feng, and B. Xu, "An analytical model for random changing pseudonyms scheme in VANETs," in Network Computing and Information Security (NCIS), 2011 International Conference on, 2011, vol. 2, pp. 141-145: IEEE.

[32] B. K. Chaurasia, S. Verma, G. S. Tomar, and S. Bhaskar, "Pseudonym based mechanism for sustaining privacy in VANETs," in Computational Intelligence, Communication Systems and Networks, 2009. CICSYN'09. First International Conference on, 2009, pp. 420-425: IEEE.

[33] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "CARAVAN: Providing location privacy for VANET," Washington Univ Seattle Dept Of Electrical Engineering2005.

[34] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA: Robust location privacy scheme for VANET," IEEE Journal on Selected Areas in communications, vol. 25, no. 8, 2007.
[35] K. A. A. E.-S. Emara, "Safety-aware location privacy in vehicular ad-hoc networks," Technische Universität München, 2016.
[36] L. Buttyán, T. Holczer, and I. Vajda, "On the effectiveness of changing pseudonyms to provide location privacy in VANETs," in European Workshop on Security in Ad-hoc and Sensor Networks, 2007, pp. 129-141: Springer.
[37] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in vanets," IEEE Transactions on Vehicular Technology, vol. 61, no. 1, pp. 86-96, 2012.
[38] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, and J.-P. Hubaux, "Mix-zones for location privacy in vehicular networks," in ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS), 2007, no. LCA-CONF-2007-016.
[39] M. Li, K. Sampigethaya, L. Huang, and R. Poovendran, "Swing & swap: user-centric approaches towards maximizing location privacy," in Proceedings of the 5th ACM workshop on Privacy in electronic society, 2006, pp. 19-28: ACM.
[40] L. Buttyán, T. Holczer, A. Weimerskirch, and W. Whyte, "Slow: A practical pseudonym changing scheme for location privacy in vanets," in Vehicular Networking Conference (VNC), 2009 IEEE, 2009, pp. 1-8: IEEE.
[41] Y.-S. Chen, T.-T. Lo, C.-H. Lee, and A.-C. Pang, "Efficient pseudonym changing schemes for location privacy protection in VANETs," in Connected Vehicles and Expo (ICCVE), 2013 International Conference on, 2013, pp. 937-938: IEEE.
[42] I. S. Association, "IEEE guide for wireless Access in vehicular environments (WAVE) architecture," IEEE Std, pp. 1609.0-2013, 2013.
[43] D. Eckhoff, N. Sofra, and R. German, "A performance study of cooperative awareness in ETSI ITS G5 and IEEE WAVE," in Wireless On-demand Network Systems and Services (WONS), 2013 10th Annual Conference on, 2013, pp. 196-200: IEEE.
[44] K. Grover and A. Lim, "Performance Comparison between Broadcast Authentication Methods for Vehicular Networks," in Proceedings of the 4th International Conference on Information and Network Security, 2016, pp. 39-44: ACM.
[45] A. Studer, F. Bai, B. Bellur, and A. Perrig, "Flexible, extensible, and efficient VANET authentication," Journal of Communications and Networks, vol. 11, no. 6, pp. 574-588, 2009.
[46] H.-C. Hsiao et al., "Flooding-resilient broadcast authentication for vanets," in Proceedings of the 17th annual international conference on Mobile computing and networking, 2011, pp. 193-204: ACM.
[47] C. Lyu, D. Gu, Y. Zeng, and P. Mohapatra, "PBA: Prediction-based authentication for vehicle-to-vehicle communications," IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 1, pp. 71-83, 2016.
[48] Y. J. Abueh and H. Liu, "Message authentication in driverless cars," in Technologies for Homeland Security (HST), 2016 IEEE Symposium on, 2016, pp. 1-6: IEEE.
[49] E. Schoch and F. Kargl, "On the efficiency of secure beaconing in vanets," in Proceedings of the third ACM conference on Wireless network security, 2010, pp. 111-116: ACM.
[50] A. Wasef and X. Shen, "ASIC: Aggregate signatures and certificates verification scheme for vehicular networks," in Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE, 2009, pp. 1-6: IEEE.
[51] J.-L. Huang, L.-Y. Yeh, and H.-Y. Chien, "ABAKA: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks," IEEE Transactions on Vehicular Technology, vol. 60, no. 1, pp. 248-262, 2011.
[52] T. W. Chim, S.-M. Yiu, L. C. Hui, and V. O. Li, "SPECS: Secure and privacy enhancing communications schemes for VANETs," Ad Hoc Networks, vol. 9, no. 2, pp. 189-203, 2011.
[53] M. Bayat, M. Barmshoory, M. Rahimi, and M. R. Aref, "A secure authentication scheme for VANETs with batch verification," Wireless networks, vol. 21, no. 5, pp. 1733-1743, 2015.
[54] Y. Xie, L. Wu, J. Shen, and A. Alelaiwi, "EIAS-CP: new efficient identity-based authentication scheme with conditional privacy-preserving for VANETs," Telecommunication Systems, vol. 65, no. 2, pp. 229-240, 2017.
[55] K. Lim, K. M. Tuladhar, X. Wang, and W. Liu, "A scalable and secure key distribution scheme for group signature based authentication in VANET," in Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), 2017 IEEE 8th Annual, 2017, pp. 478-483: IEEE.
[56] Y.-C. Hu and K. P. Laberteaux, "Strong VANET security on a budget," in Proceedings of Workshop on Embedded Security in Cars (ESCAR), 2006, vol. 6, pp. 1-9.