Efficient Distribution of Key Chain Commitments for Broadcast Authentication in V2V Communications

Mujahid Muhammad
Birmingham City University
Birmingham, UK
mujahid.muhammad@bcu.ac.uk

Paul Kearney
Birmingham City University
Birmingham, UK
paul.kearney@bcu.ac.uk

Adel Aneiba
Birmingham City University
Birmingham, UK
adel.aneiba@bcu.ac.uk

Andreas Kunz
Lenovo, Oberursel, Germany
akunz@lenovo.com

Abstract— **Road safety applications such as intersection collision warning, emergency brake warnings, etc., rely on the periodic broadcast of messages by vehicles and roadside infrastructure. PKI-based approaches ensuring the integrity of messages and the legitimacy of the sender are computationally expensive and result in long messages. Approaches based on hashed key chains such as Timed Efficient Stream Loss-tolerant Authentication (TESLA) offer an alternative solution. Because they use symmetric-key cryptography, the messages are shorter and less expensive to verify. However, they bring their own challenges. This paper focuses on one challenge, the problem of distributing key chain commitments required for message verification. We propose and evaluate two techniques, respectively involving periodic broadcast of commitment keys by the vehicles themselves and selective unicasting by a central V2X Application Server (VAS). We find that the VAS-centric solution has advantages over the vehicle-centric solution and a related solution proposed by other researchers.**

Keywords—authentication, message integrity, commitment key, V2V communication, security

I. INTRODUCTION

INTELLIGENT transportation systems (ITS) integrate information and communication technologies with transport entities. They include services that help drivers to be aware of other vehicles within their vicinity, disseminate warnings about road hazards, provide real-time information about traffic conditions, and contribute to road safety and traffic efficiency. These services rely on messages exchanged between vehicles (V2V), and between vehicles and roadside infrastructure (V2I).

A receiver of a message must be able to verify that it is sent by a legitimate vehicle or infrastructure element and not altered during transmission. V2V/I use-cases have characteristics that constrain solutions to this problem: (1) mobility (2) time sensitivity (3) a non-uniform environment with varying density and speed of vehicles and (4) broadcast transmission.

The IEEE 1609.2 standard adopted in the US [1] and ETSI-ITS standard adopted in Europe [2] recommend the use of asymmetric digital signatures for securing broadcasts messages in V2V systems. Each vehicle is assigned a set of public key certificates that allows it to sign messages and enables receivers to confirm its legitimacy and the authenticity of the messages. The certificates need to be issued and revoked by a trusted authority, which implies the use of a vehicular public key infrastructure (VPKI).

The research community has considered lower cost broadcast security solutions such as Timed Efficient Stream Loss-tolerant Authentication (TESLA) [3]. TESLA is built on symmetric cryptography and so offers authentication at reduced cost and dependence on PKI. However, it has its own problems that need to be tackled in order to make it effective for V2V. Little attention has been given to distribution of the commitment keys used to verify the keys that authenticate messages. This is problematic in the highly dynamic V2V context. In this paper, we present two contrasting schemes, one of them novel, that could be employed to distribute commitment keys efficiently.

This paper is organized as follows. Section II presents the state of the art regarding adaptation of TESLA to V2V. Section III describes our proposed commitment key distribution solutions, which are analyzed comparatively in Section IV. The security of our solutions as compared to other existing solution in Section V. Finally, in Section VI, we summarize the main conclusions of the paper.

II. RELATED WORK

Studies have confirmed through simulations [4], practical tests on real equipment [5] and modelling [6] that the signature verification overhead of VPKI-based schemes leads to excessive latency or packet loss when road traffic is dense. TESLA, offers an efficient alternative. It uses a one-way hash function (e.g. SHA256) to generate a chain of keys that are subsequently used to sign and authenticate messages in successive time intervals by means of a symmetric Message Authentication Code (MAC) algorithm. An element of asymmetry is introduced by disclosing each key in an interval after it was used for signing. Consequently, senders and receivers must be synchronized. TESLA's main advantages are low computation and communication overheads arising from use of symmetric cryptography. Disadvantages include delayed authentication, the need for efficient distribution of key authentication information (commitment keys), and lack of a non-repudiation mechanism.

The works of [7] and [8] were among the early research studies proposing TESLA as a viable option to secure V2V messages. Subsequent works have aimed to mitigate its problems. For example, [9] and [10] address delayed authentication using a prediction-based approach. However, few works address distribution of commitment keys. These are the keys at the end of a key chain generated by iterated application of the hash function and can be used to confirm the authenticity of disclosed message-signing keys. A vehicle must have the commitment keys of its current neighbors in order to verify received messages. In the open and dynamic V2V context, a vehicle's neighbors are changing constantly, which makes efficient commitment key distribution challenging.

In [11], the authors proposed a reactive approach; if V_A receives a message from V_B, but does not have its commitment key then it sends a key request message to V_B. A Bloom filter obtained from a Roadside Unit (RSU) is used in validating V_B's response. This is compared with our schemes in Section IV. [12] also proposed a reactive commitment key exchange method. On receiving a message from an unknown vehicle, the receiver broadcasts its own commitment key along with a list of vehicles (including the sender) whose commitment keys it needs. This approach may result in vehicles being overwhelmed with lots of messages containing commitment keys that they already possess. It is computationally expensive to verify the broadcast messages and the scheme is vulnerable to denial of service attacks. The authors of [13] adopted periodic broadcasts of commitment keys at a fixed time intervals in their cooperative message verification scheme. However, they did not evaluate its performance and did not provide the time interval that should be used for the periodic distribution. We analyze the behavior of this type of distribution scheme in Section IV as it is similar to one of the schemes we propose.

III. Commitment Key Distribution

In this section, we present two different solutions that provide efficient ways to distribute commitment keys in a V2V environment. First, we begin with a brief description of the problem. For the sake of clarity, the following conventions have been adopted. We use V_A to denote the identity of vehicle *A* and K_{0A} to refer to the commitment for its current key chain. An uppercase subscript (e.g. A) indicates a particular vehicle by name, whereas a lower case subscript (e.g. i) refers to a vehicle in terms of its position in a list or array. Superscripts are used to differentiate the candidate solutions.

A. Problem Statement

Suppose vehicle V_A broadcasts a message at time T and discloses the corresponding key at time $T+Q$, where Q is the key disclosure time interval. A receiving vehicle, V_B, wishing to make prompt use of the message will need to be in possession of the commitment for the key chain containing this key before $T+Q$. We say that a vehicle V_A is *relevant* to vehicle V_B at time T if knowledge of V_A*'s* state at T could potentially influence V_B*'s* behavior at $T+Q$. For simplicity, we define the term "relevance" in a way that if V_A is "relevant" to V_B, then V_B is within range of messages broadcast by V_A and (if communication is reliable) should receive all safety messages, but not all of them will be important for it.

The commitment distribution problem that has to be fulfilled can be stated as follows: for any pair of vehicles, (V_A, V_B), if V_A is relevant to V_B at time T, then V_B must receive the commitment for the key chain in use by V_A at time T before $T+Q$.

We present two main solutions, distinguished primarily by the entity responsible for the distribution, as follows.

B. V2X Application Server (VAS) Centric Solution

This solution involves the use of a central trusted entity called the V2X Application Server (VAS) that first determines vehicles that are relevant to each other, and then forwards the commitment keys to each vehicle through unicast transmission. The VAS exists at the application layer and communicates with the vehicles on the user plane. All vehicles are required to a) register with the VAS and b) send the commitment of their latest key chain (updated whenever a key chain is regenerated). The VAS maintains a commitment key table, KT_{VAS}, relating vehicle IDs to current commitments such that $KT_{VAS}(V_A) = K_{0A}$.

As part of the registration process, a secret symmetric cryptographic key is agreed between the vehicle and the VAS. This key is used to generate and check MACs to ensure the integrity and authenticity of messages exchanged between them. In particular, the messages notifying the VAS of a new commitment key and informing a vehicle of commitment keys of relevant vehicles are protected in this way.

The VAS could adopt a reactive, on-demand distribution strategy whereby vehicles request commitment keys as and when they need them. Effectively, the vehicles are determining their relevance in this case. The requesting vehicle must wait for at least one round trip communication delay to obtain the commitment keys. To avoid this delay, we instead consider a proactive distribution strategy in which the VAS predicts the needs of vehicles and delivers the commitment keys just in time for use. To enable this, the VAS also maintains a commitment distribution table *CDT*, such that $CDT(V_A, V_B)$ is true if and only if V_B has been sent V_A*'s* current commitment, i.e. K_{0A}. The relevant entry in *CDT* is set whenever the VAS sends out a commitment key and unset whenever a commitment key is updated or becomes invalid for some reason.

The VAS executes a relevance prediction function, *rel*, such that $rel(V_A, V_B, \Delta T)$ returns true if and only if V_A is relevant to V_B for at least part of the interval between the current time T and ΔT i.e. $T+\Delta T$. The third argument ΔT thus determines how far ahead the relevance function is looking. Clearly, the VAS must possess sufficient knowledge of the vehicles' states and other factors in order to evaluate *rel*. If *rel* evaluates to true for a given vehicle pair (V_A, V_B) and the corresponding entry in *CDT* is false, then the VAS sends V_B the V_A's current commitment key and changes $CDT(V_A, V_B)$ to true.

We define an approximation to the general relevance prediction function that depends only on the straight-line distance between the two vehicles and the average vehicle speed in the locality, expressed as:

$$rel(V_A, V_B, \Delta T) = rel(V_B, V_A, \Delta T) = true, \text{ if and only if } d(V_A, V_B) \leq r(v(V_A \text{ or } V_B), \Delta T)$$

$$r(v, \Delta T) = r_0 + r_1(v) + r_2(v, \Delta T) \quad (1)$$

$$r_0 = a_0,\ r_1(v) = a_1.v\ ,\ r_2(v, \Delta T) = a_2.v.\ \Delta T$$

where $d(V_A,V_B)$ is the distance between V_A and V_B, and $v(V_A) \approx v(V_B)$ is the average speed of vehicles in the vicinity of V_A and V_B, which is assumed to vary slowly with position.

One can imagine three circles centered on V_A as illustrated in Fig. 1. A circle of radius r_0 encompasses all vehicles judged to be relevant to V_A when traffic is stationary. It seems reasonable for the 'radius of relevance' to grow with vehicle speed, hence a circle of radius $r_0+r_1(v)$ encompasses all vehicles relevant to V_A at the current time when the traffic speed, v, is finite. The largest circle, of radius $r_0+r_1(v)+r_2(v, \Delta T)$ adds vehicles that might become relevant in the next ΔT.

Each vehicle i locally maintains a table KT_i, to store current commitment keys of other vehicles received from the VAS and uses it to check whether the commitment key of a safety message sender is available or not in order to proceed with message verification.

We assume VAS executes the distribution procedure periodically at intervals of δT^{VAS}, which is reasonable if it is running as a thread within a server that also has other tasks to perform. For each ordered pair of vehicles (V_i, V_j) registered with it, the VAS checks that V_j has not already been sent V_i's current commitment key and that V_i is, or is expected soon to be, relevant to V_j. If this is true, then the VAS sends V_i's current commitment key to V_j and records this fact in *CDT*. Once all ordered pairs have been considered, the VAS waits for the next scheduled time to repeat the process.

C. Analysis of VAS-centric Solution

Suppose the VAS is used to distribute commitment keys, a given vehicle V_A will receive an initial burst of messages informing it of the commitments of vehicles within its radius of relevance. If $\rho(V_A)$ is the density of vehicles in the vicinity of V_A, then the size of this burst will be: $\rho(V_A).\pi r^2(V_A, \Delta T)$. Subsequently, V_A will receive further messages as additional vehicles enter its radius of relevance. The rate will be proportional to the circumference of V_A's circle of relevance and the vehicle speed. Thus, the total number of messages sent to V_A up to time T will be approximately:

$$M^{VAS}(V_A,T,\Delta T)=\rho(V_A).\pi r^2(V_A\,\Delta T)+\rho(V_A).2r(V_A,\Delta T).v(V_A).T \quad (2)$$

Now, $r(V_A, \Delta T)$ increases with ΔT, so the $M^{VAS}(V_A, T, \Delta T)$ does also. If part of our goal is to minimize the number of messages sent / received, then ΔT should be kept as small as possible. A lower bound on ΔT is dictated by the time it takes the VAS to complete one cycle. ΔT must therefore equal or exceed δT^{VAS}. We choose $\Delta T = \delta T^{VAS}$ and make δT^{VAS} as small as possible. The minimum value for δT^{VAS} will depend on the processing capacity of the VAS, the number of vehicles registered to it, and the time taken for a commitment key sent by the VAS to reach and be verified by the destination vehicle.

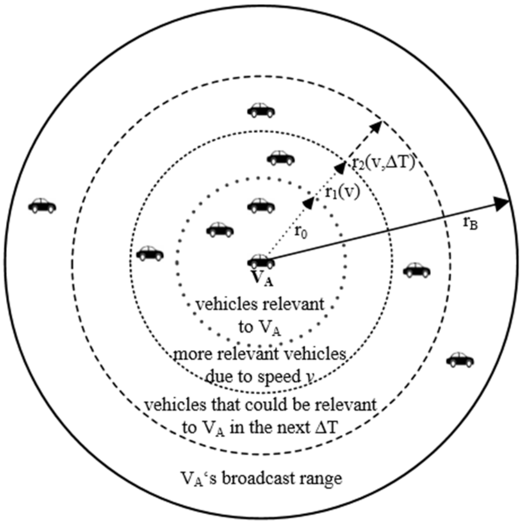
r2(v,ΔT)
r1(v)
r0
rB
VA
vehicles relevant to VA
more relevant vehicles due to speed v
vehicles that could be relevant to VA in the next ΔT
VA's broadcast range

Fig. 1: Radius of relevance vs broadcast range

D. Vehicle-centric Solution

In this solution, vehicles are responsible for sending the commitment of their latest key chain to their neighbors using the same direct communication channel employed to broadcast safety messages. A VAS is still required, but its role is greatly reduced. Similarly to the VAS-centric solution, vehicles are required to register with, and forward their current commitment keys to the VAS. However, in this case, the VAS only signs the commitment key and returns it to the vehicle. Contrary to the VAS-centric case, an asymmetric digital signature mechanism is used to protect the integrity of the commitment key messages. Each vehicle holds the public key of the VAS which can be pre-provisioned or obtained during registration, and this is used to verify the commitment keys sent by its neighbors.

As in the VAS-centric case, it is possible to adopt a reactive, on-demand approach as proposed in [12]. In this case, the verification of a received safety message is delayed by at least the request-response round trip time. Again, we consider an alternative, proactive, approach. Here, all vehicles broadcast their commitment keys repeatedly at intervals of δT^{veh}. Now, commitment keys are received at approximately the same time as the first safety messages from a new neighbor. This makes the acquisition of commitment keys faster, but at additional overhead cost, which will be described later.

E. Analysis of Vehicle-centric Solution

The broadcast of commitment keys every δT^{veh} increases the chances of vehicles that are within the radius of broadcast r_B to have a copy of each other's commitment keys. However, the rate at which messages are sent and received by each vehicle: $M'^{veh}(V_A)=(\rho(V_A).\pi.r^2{}_B)/\delta\mathrm{T}^{\mathrm{veh}}$, is greater than in the VAS-centric case from (2): $M'^{VAS}(V_A,T,\Delta T)= \rho(V_A).2r(V_A, \Delta T).v(V_A)$. This is because the vehicle-centric messages include duplicate commitment keys that are received from the same vehicle while it is still in the broadcast range.

The choice of δT^{veh} has a direct effect on the number of messages received. A small value of δT^{veh} makes it more likely that commitment keys are received before they are needed, but at the cost of an increased number of messages that may overwhelm the processing and buffer capacity of the vehicle's OBU. On the other hand, using large δT^{veh} interval leads to fewer messages, but some vehicles might not receive some commitment keys in time, especially when traffic speed is high.

Now, the purpose of the commitment key is to validate a message-signing keys. There is no advantage, therefore, in broadcasting the commitment key more frequently than the safety messages themselves. In fact, one simple strategy is to send them at approximately the same time.

IV. Comparative Analysis of Commitment Key Distribution Solutions

Here we compare the performance of VAS-centric and vehicle-centric distribution solutions with each other and with a reactive vehicle-centric solution due to Bao et al [11]. The performance metrics used for comparison are commitment key distribution time, computational cost, communication overhead, security overhead cost, and reliability of the commitment key distribution solution.

A. Commitment Key Distribution Time

The commitment key distribution time has the following main components:

δT, the time interval between successive commitment key distribution opportunities.

T_{trans}, the time taken for the commitment key message to propagate from sender to receiver

T_Q, the queuing delay, which is the sum of queuing delays at the sender (T_{SQ}) and receiver (T_{RQ})

T_{verify}, the security overhead due to signing and verifying the commitment key message

Thus, in general: $T_{CT} = \delta T + T_{trans} + T_Q + T_{verify}$. M/M/1 queuing theory is used to estimate T_{RQ} for V_i: $T_{RQ} = 1/(\mu - M'(V_i))$, where μ denotes vehicle's processing capacity in messages per second and $M'(V_i)$ is messages received per unit time by the i^{th} vehicle. T_{SQ} is assumed to be negligible in all cases. T_{trans} depends on the communication mode (direct LTE-V2V PC5 or IEEE 802.11p, or unicast over the cellular network) and the message size. T_{trans} for IEEE 802.11p is estimated following an approach similar to the one presented in [14]. δT^{VAS} depends on the traffic load and the processing capacity of the VAS. We consider a typical value for it to be 10ms following the results obtained in a similar implementation in reference [15]. δT^{Bao} is taken to be zero as the approach used is reactive. δT^{veh} is set to be equal to the safety message broadcast interval.

Table 1 summarizes parameter values used to compare performance, either benchmark values used in [11] and [14] or our estimates. With these settings, T_{CT} is compared for the two distribution solutions and that of [11] for different values of vehicle density as shown in Fig. 2.

TABLE I. MAIN INPUTS AND SETTINGS

Parameter	Value		
	VAS-centric	**Vehicle-centric**	**Ref.** [11]
Channel bandwidth	50Mps	24Mbps	24Mbps
Radius of relevance/ r_B	100m	300m	300m
δT	10ms	500ms	0
T_{verify}	2µs	6ms	6ms
Message size	384 bits	736 bits	672 bits
M	500 messages/second		
ρ	0 – 200 vehicles/km^2		

The VAS-centric time varies only slowly with vehicle density and mostly depends on δT^{VAS}. Moreover, the predictive VAS-centric approach aims to get the commitment keys to vehicles before they are needed. The distribution time increases more rapidly in the other two cases. Performance becomes bad when the traffic density is high such that the signature verification time for received commitment keys becomes significant in the vehicle-centric case, and in the case of Bao et al., when the number of request/response pairs is excessive. The distribution time may further increase if any of the request/response messages are lost.

In a TESLA-based approach, the upper limit on T_{CT} is approximately the key disclosure time interval, which is set according to the safety application's needs. According to the ITS standard, the maximum latency of some safety messages is 100ms, suggesting a T_{CT} of 50ms since two time intervals are required for transmission and verification of messages.

B. Reliability of Commitment Key Distribution

In the VAS-centric solution, commitment key distribution depends on the successful delivery of a single message over the unicast channel between VAS and vehicle. The vehicle-centric solution is more tolerant to message loss as vehicles broadcast their commitment keys repeatedly and it is likely that neighboring vehicles will have multiple opportunities to receive a message successfully. Thus, the vehicle-centric solution can be considered more reliable. The work of Bao et al has the least reliability because four successful independent message receptions are required to get a commitment key.

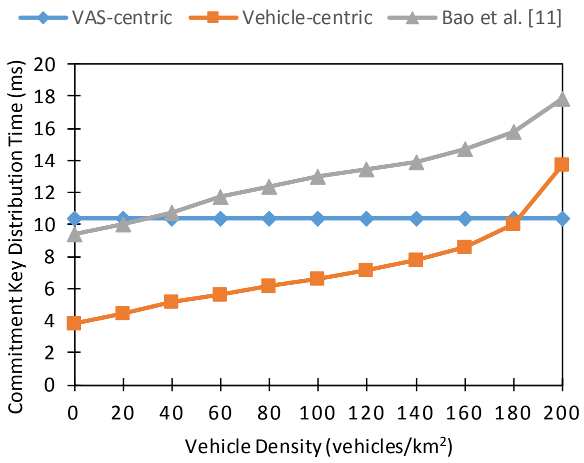

Fig. 2. Commitment key distribution time vs vehicle density

C. Bandwidth Efficiency

Here we consider the average cost of delivering a commitment key message. For the VAS-centric solution, the communication cost per commitment key is 384 bits (160 bits each for commitment key and MAC, 32 bits each for vehicle ID and timestamp). In the vehicle-centric case, each commitment key requires 736 bits (160 bits commitment key, 512 bits digital signature, and 32 bits each for vehicle ID and timestamp). For the Bao et al solution, its total cost is (864 + *m*) bits; 32 bits for each request message, 224 bits for the commitment key response message, and 576+*m* bits for the response from the RSU, where *m* is the length of the Bloom filter, which depends on the number of elements present in the filter. The VAS-centric solution causes the lowest bandwidth consumption. It decreases the overhead to 44% or less of the Bao et al value.

D. Storage Cost

Here we consider the amount of buffer space required on the vehicles to store the commitment key messages received. Fig. 3 examines the influence of vehicles' speed on the rate at which commitment keys are received. For the VAS-centric case, the message rate depends directly on speed, and also indirectly via the radius of relevance, which grows with speed. In contrast, the vehicle-centric is independent of vehicle speed. In both cases the number of commitment key messages increases linearly with vehicle density, and consequently so does the memory requirement. In Bao et al, the message rate is increased due to the need to receive two separate messages each time: a commitment key from the relevant vehicle and a Bloom filter value from a nearby RSU. Therefore, the VAS-centric solution has the lowest memory requirement of the three.

E. Processing Overhead due to the Security Mechanism

Here we consider the effect of cryptographic operations on the distribution time and the message size. The symmetric MAC operations performed in the VAS-centric solution have minimal overhead cost compared to the digital signature verification performed in the vehicle-centric case. Bao et al use *k*-hash functions for the Bloom filter used to verify a commitment key, and a digital signature to verify the legitimacy of the RSU that sent the filter itself. This incurs more security overhead than our two solutions.

F. Summary of the Comparison

Our two distribution solutions each has its own strengths and weaknesses. The effectiveness of the VAS-centric solution largely depends on the server's processing capacity and the accuracy of the relevance function. In contrast, the vehicle-centric solution's attraction is simplicity, with little computation required, while its weaknesses are a) the large receiver queuing delay, which is due to the higher number of commitment key message received and increases with vehicle density, and b) the high requirement for buffer space. Therefore, we believe the two solutions can be targeted at different scenarios.

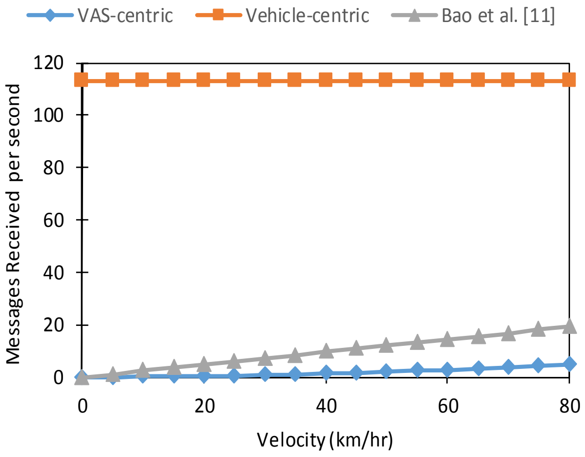

Fig. 3. Messages received per second vs vehicle velocity

In congested areas, such as city centers, the VAS-centric solution can be used. This is because it is expected that cellular communication coverage will be good there. Furthermore, the traffic speed in such areas is usually low, which means that vehicles will most likely be relevant to each other for an extended period of time.

In highway or rural areas, the vehicle-centric solution would be favored. This is because there may be partial or no availability of communication network. Also, since the density of vehicles is mostly low and speed is high in these areas, vehicles might not stay long in the broadcast range, and therefore the number of commitment key messages received per unit time will be less. Moreover, duplicate transmissions could be useful because the high speed of vehicles increases transmission errors due to rapid variations in channel conditions.

For Bao et al, there are limitations that could prevent the practical realization of the solution. Vehicles depend on RSUs to enable verification of commitment keys, thus the method relies on appropriately–equipped RSUs being installed widely. The area of coverage of an RSU will be relatively small, so that large numbers of them will be required. It seems unlikely that sufficient coverage could be provided outside urban areas and major highways. Consequently, a back-up solution would be required for use away from RSUs. Bao et al have not considered multi-RSU scenarios. Mechanisms to cater for handover of responsibility for a vehicle from one RSU to another, dealing with situations where mutually-relevant vehicles are connected to different neighboring RSUs, and where a vehicle connected to more than one RSU at the same time need to be addressed.

V. Security Analysis

In this section, we analyze the security of VAS-centric, vehicle-centric and Bao et al solutions. We assume that the VAS has high computational resources and cannot be compromised.

1) Replay Attack: An attacker may capture and replay a legitimate vehicle's commitment key update messages to the VAS. However, replaying a correct message would only increase the reliability but could lead to a DoS situation, see 3).

2) Bogus Commitment Key Messages: An attacker may attempt to distribute bogus commitment key messages to the vehicles so that verification of received safety messages will fail. However, in the VAS- and vehicle-centric cases, the messages are protected against forgery and modification by MACs and signatures respectively. In the Bao et al case, an attacker can send bogus commitment keys to vehicles. However, their verification will fail, since the bogus commitment key is not among the elements used in constructing the Bloom filter value by the RSU.

3) Denial of Service (DoS) Attack: An attacker may try to overwhelm vehicles resources with frequent commitment key updates. In the VAS-centric case, commitment keys are sent to the VAS for distribution. The VAS can monitor update freqencies and apply appropriate sanctions to vehicles that misbehave. In contrast, the vehicle-centric solution is vulnerable to DoS attack because an attacker can broadcast its commitment key repeatedly to cause congestion on the communication channel or to overwhelm the resources of the receiving vehicles with frequent signature verification process. Similarly, the Bao et al soultion is vulnerable because an attacker can repeatedly send its commitment key causing receiving vehicles to repeatedly request Bloom filter from RSU for verification. This can lead to high communication overhead on the communication channel and also exhaust the vehicles' resources in verifying the RSU's signature for each received Bloom filter value .

4) Impersonation Attack: An attacker can pretend to be the VAS, persuading vehicles to register with it rather than the real VAS. However this can be defeated if the authentic VAS's certificates and other credentials are installed in the vehicle's OBUs so that the VAS's identity can be verified during registration.

VI. Conclusion and Further Work

We have identified the distribution of commitment keys to moving vehicles as a major problem that constrains the effectiveness of TESLA–based V2V security. We have considered two schemes. The VAS-centric scheme is an original proposal that utilizes a central trusted entity to forward commitment keys to vehicles only when they are identified to be in need. In contrast, the vehicle-centric approach entails repeated broadcast of commitment keys by the vehicles.

Our analysis shows the two solutions to be effective in distributing commitment keys with low overhead cost compared to a related published work. The VAS-centric solution has demonstrated desirable properties compared to the vehicle-centric solution throughout a range of theoretical evaluations and security features. Moreover, it provides vehicles with commitment keys in advance.

In future work, we will improve the accuracy and efficiency our VAS-centric approach by considering road geometry and direction of vehicles movement in predicting relevance. Also, we will address key traceability and trapdoor linkability.

VII. References

[1] IEEE, "IEEE Standard for Wireless Access in Vehicular Environments Security Services for Applications and Management Messages, Revision of IEEE Std 1609.2-2013," IEEE, 2016.

[2] ETSI, "Intelligent Transport Systems (ITS); Security; ITS Communications Security Architecture and Security Management," ETSI, 2018.

[3] A. Perrig, R. Canetti, D. Tygar and D. Song, "The TESLA broadcast authentication protocol," *Rsa Cryptobytes,* vol. 5, pp. 2-13, 2002.

[4] B. Fernandes, J. Rufino, M. Alam and J. Ferreira, "Implementation and analysis of ieee and etsi security standards for vehicular communications," *Mobile Networks and Applications,* vol. 3, no. 23, pp. 469-478, 2018.

[5] J. Dai, L. Pu, K. Xu, M. Z. Z. Liu and L. Zhang, "The implementation and performance evaluation of wave based secured vehicular communication system," in *In 2017 IEEE 85th Vehicular Technology Conference (VTC Spring)* , 2017.

[6] M. Muhammad, P. Kearney, A. Aneiba and A. Kunz, "Analysis of Security Overhead in Broadcast V2V Communications," in *38th International Conference on Computer Safety, Reliability and Security*, Turku, 2019.

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

[8] X. Lin, X. Sun, X. Wang, C. Zhang, P. Ho and X. Shen, "TSVC: Timed efficient and secure vehicular communications with privacy preserving.," *IEEE Transactions on Wireless Communications,* vol. 7, no. 12, pp. 4987-4998, 2008.

[9] 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.

[10] M. Lalli and G. S. Graphy, "Prediction based dual authentication model for VANET," in *International Conference on Computing Methodologies and Communication (ICCMC)*, 2017.

[11] S. Bao, W. Hathal, H. Cruickshank, Z. Sun, P. Asuquo and A. Lei, "A lightweight authentication and privacy-preserving scheme for VANETs using TESLA and Bloom filters," *Elsevier ICT Express,* 2017.

[12] Y.-C. Hu and K. P. Laberteaux, "Strong VANET security on a budget," *Proceedings of Workshop on Embedded Security in Cars (ESCAR),* vol. 6, pp. 1-9, 2006.

[13] H. Jin and P. Panos, "DoS-resilient cooperative beacon verification for vehicular communication systems," *Ad Hoc Networks 90,* p. 101775, 2019.

[14] A. Bazzi, B. M. Masini, A. Zanella and I. Thibault, " On the performance of IEEE 802.11 p and LTE-V2V for the cooperative awareness of connected vehicles," *IEEE Transactions on Vehicular Technology,* vol. 66, no. 11, pp. 10419-10432, 2017.

[15] P. Cincilla, O. Hicham and C. Benoit, "Vehicular PKI scalability-consistency trade-offs in large scale distributed scenarios.," in *IEEE Vehicular Networking Conference (VNC)*, 2016.