Adaptive security provisioning for vehicular safety applications

Elyes Ben Hamida, Muhammad Awais Javed, Wassim Znaidi

Adaptive Security Provisioning for Vehicular Safety Applications

Elyes Ben Hamida

Technological Research Institute - IRT SystemX, 8 avenue de la vauve, 91120, Palaiseau, France
E-mail: elyes.ben-hamida@irt-systemx.fr

Muhammad Awais Javed

Comsats Institute of Information Technology, Islamabad, Pakistan
E-mail: awais.javed@comsats.edu.pk

Wassim Znaidi

Qatar Mobility Innovations Center, Qatar Science and Technology Park, PO Box 210531, Doha, Qatar
E-mail: wassimz@qmic.com

Abstract: Vehicular ad hoc network provides safety applications for next generation intelligent transport systems. By periodically transmitting mobility information in basic safety messages (BSMs), vehicles get an overview of the neighborhood. As applications involving vehicular networks impact human safety, reliability of BSMs is a key requirement, which however is a challenging task in heavy traffic scenarios where many BSMs are queued up simultaneously for signature verification. This results in long verification delays for many critical BSMs from nearby vehicles. To overcome this challenge, we propose two adaptive security mechanisms in this paper that can be used by the ITS applications to enhance their QoS and maintain good level of security. The first technique is a receiver-oriented technique that uses channel aware mechanism to prioritize the signature verification of BSMs from closer neighbors. The second technique is transmitter based that can adaptively select the best security level for BSMs according to cryptographic loss rate. Simulation results verify the performance enhancement achieved by the proposed framework in terms of several safety awareness metrics as compared with the existing schemes.

Keywords: Vehicular Applications; Intelligent Transport Systems; Basic Safety Messages; Elliptic Curve Digital Signature Algorithm; Adaptive Security Provisioning.

Biographical notes:

Elyes Ben Hamida is a Research Projects Manager at the Technological Research Institute (IRT) SystemX. He holds a Ph.D. (2009) and M.S. (2006) degrees from INSA Lyon France, and a Dipl.-Ing. (2005) degree from INSAT Tunisia. His research interests include algorithms and protocols design for emerging wireless technologies and networks.

Muhammad Awais Javed is an Assistant Professor at COMSATS Institute of Information Technology, Islamabad. He completed his Ph.D. from The University of Newcastle, Australia in Feb. 2015 and B.Sc. from University of Engineering and Technology Lahore, Pakistan in Aug. 2008. His research interests include algorithms for efficient communications in mobile ad hoc networks, protocol design for emerging wireless technologies.

Wassim Znaidi is a Senior R&D engineer at QMIC (formerly QUWIC). He holds a Ph.D (2010) from INSA Lyon France, a M.S. (2007) from University Grenoble Alpes France and a Dipl. - Ing (2006) from Polytechnic School Tunisia. His research interest include protocols design for network security, efficient algorithm for resilient embedded systems and internet of things.

This paper is a revised and expanded version of a paper entitled "*Channel-Aware ECDSA Signature Verification of Basic Safety Messages with K-Means Clustering in VANETs*" presented at the 30th IEEE International Conference on Advanced Information Networking and Applications (IEEE AINA 2016), Crans-Montana, Switzerland, March 23-25, 2016.

1 Introduction

Vehicular ad hoc network (VANET) is a core component of the future intelligent transport systems. By enabling wireless data exchange between vehicles (V2V) or between vehicles and infrastructure (V2I), various applications for traffic safety and user convenience could be realized. Cooperative awareness, emergency warning notification, efficient route guidance and multi-player games are few of the possible applications using VANET paradigm (1).

Cooperative safety awareness applications using VANETs rely on regular broadcast of mobility information by every vehicle within its neighborhood. These broadcast messages are known as basic safety messages (BSMs) in the WAVE standard (2) and cooperative awareness messages (CAMs) in the ETSI standard (3). BSMs allow vehicles to extend their vision beyond line of sight and develop a local dynamic map (LDM) (4) containing a clear picture of surrounding traffic. LDM is a database that collects information from various sensors, road side units and neighborhood vehicles to facilitate various ITS applications (5), such as intersection collision warning, wrong way driving warning, approaching emergency vehicle warning application, etc.

Since vehicles make driving decisions based on their LDM, its accuracy is a key application requirement which in turn is dependent on the fidelity of BSMs. A malicious user can severely impact the vehicle safety by injecting false messages in a vehicular network (6). Hence, authentication is a key procedure in the transmission of BSMs. Once a BSM is generated by the application layer, a digital signature is added to it before transmission. At the receiver, the received BSM is placed in a security queue where it is verified at its turn before passing it to the application layer.

Both the WAVE and the ETSI ITS standards recommend the usage of Elliptic Curve Digital Signature Algorithms (ECDSA) for signing and verifying BSMs. However, this renders additional communication and processing overheads that degrades the quality of service of BSMs, as highlighted in our recent works (7; 8; 9). This is especially true in high density VANETs scenarios, where each vehicle might receive several hundred (or thousand) BSMs per second from neighboring vehicles, and which could not all be verified due to the limited computational resources. As a result, several important BSMs from close by neighbors get dropped due to timeout, resulting in loss of awareness for safety applications (5). A number of techniques have been proposed in the literature to optimize verification processing time of BSMs (10; 11; 12; 13; 14; 15; 16), and thus to improve the vehicle situational awareness. However, these approaches present major limitations, especially in supporting safety applications.

Another key challenge in security of vehicular networks is the static security level selection. Due to large number of BSMs queued for verification, network congestion at the receiver security queue exists. A possible solution to this problem is to adaptively select the security levels so as to maintain a high level of QoS at slightly reduced security. Indeed application reliability will increase if more packets are received correctly and within due time.

In this paper, we propose two adaptive security mechanisms with an aim to increase over all reliability of vehicular safety applications. Due to high network densities and large data traffic in vehicular networks, both transmitter and receiver need to take responsibility for dynamic adaptation of security. Thus, these adaptive security mechanisms introduce novel additions to the security procedure at the transmitter and receiver.

At the receiver side, we present a new channel-aware authentication framework that prioritizes the signature verification of critical BSMs in a safety application, where nearby vehicles represent a higher safety concern in comparison to vehicles which are located further away. At first, vehicles classify the received signal strength of BSMs into several safety areas based on the k-means clustering algorithm during an online or offline training phase. The BSMs assigned to different safety areas are then mapped to a multi-level priority queue (MLPQ). This process enables BSMs from closer neighbors to be placed in the high priority queues and hence verified quickly. We analyse the performance of the proposed framework and compare it with existing schemes using simulations. Results show that the channel aware authentication framework can significantly reduce the verification delay of BSMs from closer neighborhood and hence, improve various performance metrics of safety applications.

On the transmitter side, we propose two novel security mechanisms for safety applications. The robustness of the security algorithm (or security level) is dependent on the length of its key size, however, a higher key size improves security but leads to higher security processing delays as well. To maintain security-QoS tradeoff, the first mechanism uses random selection of transmitter security level to reduce cryptographic loss rate (CLR). The second mechanism adaptively selects the optimal security level by iteratively calculating CLR and upgrading or downgrading the security level keeping CLR below the required threshold. Using simulations, we compare our proposed mechanisms against the static security technique proposed in the ETSI standard and show significant improvement in terms of safety and QoS metrics.

The remainder of this paper is organized as follows. Section 2 describes the existing work in the literature related to transmitter and receiver side security mechanisms. Section 3 explains the design methodology of the proposed receiver side security mechanism. Section 4 describes the working of adaptive security scheme at the transmitter side. Performance evaluation is presented in Section 5 and conclusions are drawn in Section 6.

2 Related Works

In this section, we present the previous work related to adaptive security techniques for vehicular networks. We categorize the literature review into two section, focusing on receiver side and transmitter side security mechanisms.

2.1 Receiver Side Security Mechanisms

At the receiver side, a number of schemes have been proposed in the literature to reduce verification processing time of BSMs (10; 11; 12; 13; 14; 15; 16). These can be classified into three main categories: random, batch and priority based signature verification.

The random based verification schemes pick only a few BSMs for verification to reduce the congestion at the security queue. In (10), signing of only random messages at the transmitter is proposed to reduce the security overhead. Additionally, random BSMs are picked at an OBU for verification process to reduce the end-to-end delay. The scheme proposed in (11) uses off-line information provided by the central authority to sign and verify safety messages with a lower security overhead.

The batch based verification techniques group together several packets to verify them at the same time. The protocol presented in (12) proposes a binary authentication tree based batch verification mechanism where several BSMs are verified together. Another similar technique to (12) generates pseudo identities based private keys and bi-linear mapping to facilitate quick batch verification of the safety messages (13).

The priority based approach rely on the BSMs location information (e.g. GPS location, headings, etc.) to prioritize the processing of these messages based on their relative proximity with the vehicle (receiver). Resource aware verification of BSMs is proposed by (14) that prioritizes the security queue based on the distance between transmitter and receiver. By using bloom filter to compute relevance of the safety messages, (15) uses a priority based BSM verification mechanism. Finally, (16) divides geographical area in to zones and utilizes priority based verification of BSMs by taking into account vehicle mobility. A key limitation of the priority based schemes is their dependence on transmitter-receiver distance which could not be calculated before the packet is authenticated. Indeed, since these location information are exploited prior to their verification (using ECDSA), existing approaches can be vulnerable to various security threats, including broadcast tampering and denial of service (5), impacting thus the safety of the end-to-end ITS application.

2.2 Transmitter Side Security Mechanisms

At the transmitter side, various adaptive security algorithms have been proposed in the context of mobile networks in previous work. In (17), authors propose a security service as a middleware that can adaptively select security protocol for communication between wireless nodes. The work considers wireless channel condition, system resource capacity and application QoS metrics to select the optimal security protocol for mobile computing applications.

The authors in (18) proposed a conceptual event driven adaptive security model to maximize service utility of the users in the Internet of things. The work in (19) divides wireless sensor data into three categories, one for mobile codes, other for the sensor location an last for particular application data. Each of this data category is assigned a unique security level.

Another work in (20) proposes a scheduling scheme for multi-media streaming applications. The protocol uses graph theory to develop and authentication model and considers the application delay requirements. Finally, work done by (21) suggest the use of adaptive encryption algorithms to meet timing requirements of an embedded system.

2.3 Motivation

The previous work in both of the above categories have severe limitations which is the motivation behind this paper. At the receiver side, the drawback of random sign and verification omission techniques is that the authentication of important BSMs from nearby vehicles cannot be ensured. An issue with the batch verification techniques is the loss of several packets if a single batch could not get authenticated. Priority based verification approaches rely on the BSMs location information (e.g. GPS location, headings, etc.) to prioritize the processing of these messages based on their relative proximity with the vehicle (receiver). However, since these location information are exploited prior to their verification (using ECDSA), existing approaches can be vulnerable to various security threats, including broadcast tampering and denial of service (5), impacting thus the safety of the end-to-end ITS application. To overcome these issues, we propose a channel-aware priority based verification mechanism at the receiver in Section 3.

At the transmitter side, all techniques discussed in Section 2.2 aim to improve the security-QoS tradeoff of wireless networks. In the context of vehicular network, solutions are needed to efficiently verify BSMs and reduce safety message delay. However, no such current work investigates the performance of random transmitter security level on QoS. Additionally, true measure of congestion at the receiver's security queue to adaptively select the appropriate security algorithm has not been used. Since packets lost due to slow security verification i.e., cryptographic loss provides an accurate evaluation of security queue congestion, we utilize this key metric to develop our proposed transmitter side mechanism in Section 4. As shown in previous work (22), cryptographic loss impacts vehicle safety, so the proposed solution enhances safety as well as QoS.

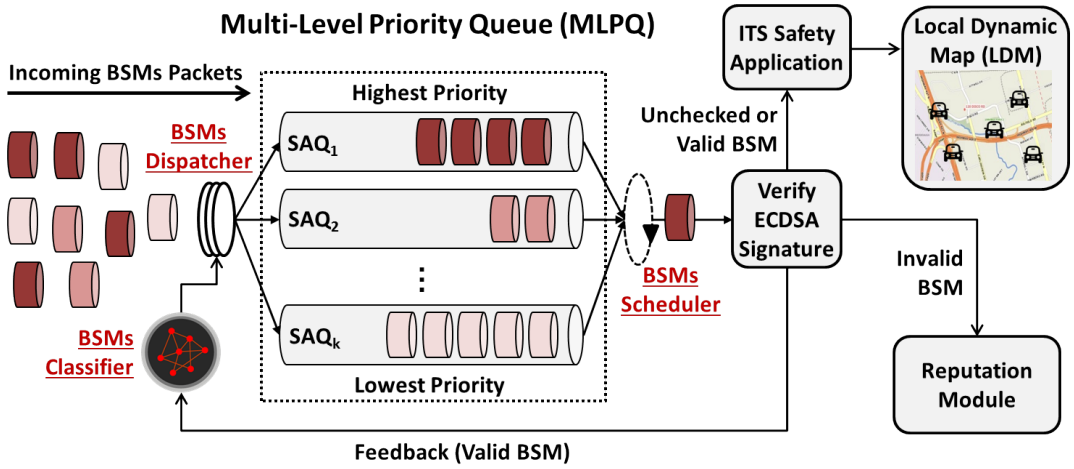

Figure 1: Multi-Level Priority Queue for Optimized ECDSA Signature Verification of VANETs BSMs.

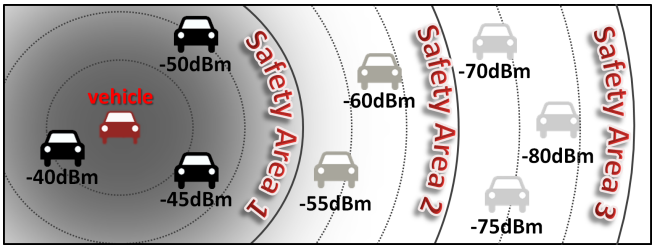

Figure 2: Received signal strength decreasing with distance and safety areas concept.

3 Proposed Channel-Aware ECDSA Signature Verification Framework (Receiver-Side Security)

In this section, we propose a new channel-aware ECDSA signature verification framework for high density VANETs. The key idea is to prioritize the verification of BSMs based on the estimated safety areas that are computed using the received signal strengths as shown in Figure 2. From the ITS safety applications points of view, nearby vehicles represent a higher safety concern. Indeed, the BSMs received from the nearest vehicles should be verified in priority; whereas the verification of the BSMs generated by vehicles further away could be delayed or discarded, without impacting the safety of ITS applications.

The key rationale for using the received signal strengths to prioritize the verification of incoming BSMs is to overcome the limitations of priority based approaches. As already discussed in Section 2, these approaches rely on BSMs' contained information, such as GPS location, speed and heading, and whose integrity and authenticity can only be guaranteed after the signature verification process. Hence, vehicle-related information cannot be used to prioritize the verification of incoming BSMs.

To achieve the above goal, our proposed framework consists in taking advantage of the fact that received BSMs have different received signal strengths in such a way that greater the distance between a vehicle and its neighbor, lower the signal strength of its received BSMs, as shown in Figure 2. In free space, the propagation of radio signals obey to the inverse-square law which states that the path loss is generally proportional to the square of the distance between a transmitter and a receiver. In reality, however, the propagation of radio signals over the wireless channel is generally impacted by three indendendent phenomena (23), namely the path-loss (or path attenuation), small-scale or multipath fading (caused by destructive interference between multiple replicas of the transmitted signal) and large-scale shadowing (due to moving or static obstacles). For instance, experimental VANETs studies (24; 25) have shown a clear correlation between distance and received signal strength in both line-of-sight (LOS) and non-line-of-sight (NLOS) conditions (e.g. vehicles or static obstructions). In particular, it has been shown that a single obstructing vehicle could cause a drop of over 20dB in the received signal strength (24).

The other key aspect of our proposed framework consists in exploiting the concept of safety areas, as shown in Figure 2. Based on the ITS safety applications requirements, vehicles can classify the geographical region around them into several safety areas. Using the received signal strengths and k-means clustering algorithm, BSMs are mapped to their corresponding safety areas, and are dispatched into a multi-level priority queue (MLPQ) in order to optimize their verification. The MLPQ allows the vehicles to schedule the verification of BSMs based on their priority classes. As a consequence, high priority BSMs (received from nearby vehicles) are verified with the lowest latency possible.

As shown in Figure 1, the high level architecture of our proposed framework consists in three main features which are described below in more details.

Algorithm 1 BSMs Classification using K-Means Clustering

Require: P_m $(m = [1, ..., n])$: set of received signal strengths
Require: k $(k \leq n)$: number of safety areas
1: **for** $l = 1$ to k **do**
2: μ_l = Random() ▷ Initialize the centroid of all safety areas with random values
3: **end for**
4: **do**
5: $SA_l = \{m : ||P_m - \mu_l||^2 \leq ||P_m - \mu_i||^2 \forall i, 1 \leq i \leq k\}$ ▷ Assign each received signal strength to the closest safety area
6: $\mu_l = \frac{1}{|SA_l|} \sum_{P_m \in SA_l} P_m, \forall l$ ▷ Recalculate the centroid values of all safety areas
7: **while** (convergence, i.e. assignments no longer change)
8: **return** $\{\mu_1, \mu_2, ..., \mu_k\}$

3.1 BSMs Classification using K-Means Clustering Algorithm

The first feature of our proposed framework consists in a training phase where received BSMs are classified according to their corresponding safety areas (SAs). These SAs are mainly defined based on the requirements of the ITS safety applications in order to prioritize the processing of the incoming BSMs, and ensure the best quality of service (QoS) for the verification of high priority messages. For example, and without loss of generality, an ITS application could require the classification of incoming BSMs according to five ($k = 5$) main SAs (or priority classes), as follows:

- Safety area 1 (SA_1): if $d^T_{i,j} \in [0...50]$ meters;
- Safety area 2 (SA_2): if $d^T_{i,j} \in]50...100]$ meters;
- Safety area 3 (SA_3): if $d^T_{i,j} \in]100...150]$ meters;
- Safety area 4 (SA_4): if $d^T_{i,j} \in]150...200]$ meters;
- Safety area 5 (SA_5): if $d^T_{i,j} > 200$ meters;

where $d^T_{i,j}$ consists in the distance between a vehicle i (BSM receiver) and a neighbor vehicle j (BSM transmitter) at a time instant T. Since vehicles on-board units (OBUs) are equipped with GPS devices, each vehicle can determine its exact GPS location, and thus based on the BSMs location information can compute the distances with respect to each of its neighbor vehicles. However, BSMs location information cannot be used prior to their verification (using ECDSA), since malicious users can inject false BSMs location data, and thus impact the safety of the end-to-end ITS application.

To that end, we propose the use of the k-means clustering algorithm (Lloyd's algorithm (26)), to classify the incoming BSMs, based on their received signal strengths, according to their corresponding SAs. As shown in Figure 1, once BSMs are verified by the ECDSA algorithm, the BSMs classifier module is notified about the valid BSMs and their received signal strengths. Given a set of valid BSMs observations $(b_1, b_2, ..., b_n)$, where each observation is a one-dimensional vector which contains the BSM received signal strength $(P_m, \forall m, 1 \leq m \leq n)$, k-means clustering aims to partition the n BSMs observations into k $(\leq n)$ safety areas sets $SA = \{SA_1, SA_2, ..., SA_k\}$ so as to minimize the within-cluster sum of squares (least-squares estimator), i.e.,

$$\underset{SA}{arg\,min} \sum_{l=1}^{k} \sum_{P_m \in SA_l} ||P_m - \mu_l||^2 \quad (1)$$

where μ_l is the mean of points in SA_l. In other words, μ_l is the centroid value (or mean received signal strengths) of the cluster (or safety area) SA_l, i.e.,

$$\mu_l = \frac{1}{|SA_l|} \sum_{P_m \in SA_l} P_m \quad (2)$$

where $|SA_l|$ represents size of the safety area set SA_l. The k-means clustering algorithm is shown in Algorithm 1, and works according to three main steps. During the first initial step (line 2 in Algorithm 1), each safety area (or cluster), SA_l, is assigned a random centroid value (μ_l). Then, each point (P_m) is assigned to the SA_l that has the closest centroid value (line 5 in Algorithm 1). After that, when all points have been assigned to their corresponding safety areas, centroid values are recomputed according to Equation 2 (line 6 in Algorithm 1). Steps 2 and 3 are then repeated until centroid values are no longer updated (convergence).

This training phase aims at classifying the received signal strengths into a set of corresponding safety areas, and can be performed either *offline* or *online*.

The *offline* approach aims at performing measurement campaigns to fully characterize the road environments (e.g. dense urban areas, road tunnels, highways, etc.) at different times of day (e.g. rush hour). In this case, each vehicle will be pre-loaded with ready-to-use safety areas mappings, which can be updated over-the-air, using vehicle-to-infrastructure (V2I) communications, to cope with evolving road environments.

The *online* approach aims at analyzing periodically the received BSMs to adjust the computed safety areas mappings, and thus to be able to cope with dynamic mobility environments. Since BSM generation rate is at least 1 packet/second, and at most 10 packets/second, each vehicle is expected to receive a large number of BSMs and hence, can complete this online training phase within few minutes, especially in high density VANETs (27). This online training phase could be performed on the vehicle itself, using

Table 1 Security Processing parameters for different Security Algorithm and key sizes (Intel Xeon Processor (7))

Security Level	Security Overhead without Certificate	Security Overhead with Certificate	Signature Delay	Verification Delay	Verification per Second
1 - NISTP-192 with SHA-256	90 bytes	240 bytes	0.2ms	1.52ms	658
2 - NISTP-224 with SHA-224	98 bytes	264 bytes	0.27ms	2.1ms	483
3 - NISTP-256 with SHA-256	106 bytes	288 bytes	0.38ms	3.1ms	327
4 - NISTP-384 with SHA-384	138 bytes	384 bytes	0.639ms	8.46ms	118

its on-board processing unit (OBU). In this context, enhanced versions of the basic K-Means clustering algorithm (e.g. (28)) could be implemented to provide higher performance, while providing the same results as the standard k-Means algorithm(28). Another approach would be to offload this tedious task to the vehicular cloud system (29), by exploiting the surrounding road side units (RSUs) and V2I communications. In this case, the training phase will be handled by powerful servers, which will in turn provide the computed safety areas mappings to the remote vehicles.

At the end of this offline or online training phase, each vehicle i is thus able to fully characterize its k safety areas SA_l ($\forall l, 1 \leq l \leq k$) along with their signal strength means μ_l (or centroid values) as listed in Algorithm 1.

3.2 BSMs Dispatching into Multi-Level Priority Queue

The second feature of our proposed framework consists in the real-time dispatching of incoming BSMs into a multi-level priority queue (MLPQ), as shown in Figure 1. The MLPQ includes a set of k first-come first-served (FCFS) safety area queues (SAQ) which are ranked from the highest to the lowest priority depending on the considered SAs. Each SAQ_l ($1 \leq l \leq k$) is responsible for storing the incoming BSMs which are associated with the safety area SA_l. Given an incoming BSM with associated received signal strength P_m, the message is assigned to the target SAQ_l, such that it minimizes the absolute difference between its SA_l centroid value μ_l and P_m, i.e.,

$$SAQ_l = arg\ min_l |\mu_l - P_m| \quad (3)$$

Hence, BSMs generated by vehicles located within a same safety area, SA_l, will be grouped all together into the same SAQ_l, and will be processed based on their priority ($l = 1$ being the highest priority level). It should be noted that if the list of SA_l are still not yet fully characterized or unknown, all incoming BSMs will be inserted into the default highest priority queue (i.e. SAQ_1).

3.3 BSMs Multi-Level Priority Queue Scheduler and ECDSA Signature Verification

The third feature of our proposed framework consists in the BSMs multi-level queue scheduling algorithm which aims at extracting BSMs from the MLPQ to verify their signatures (using ECDSA), as listed in Algorithm 2.

The algorithm is based on the first-come first-served (FCFS) and round-robin scheduling techniques. At every new run, the algorithm starts by checking the highest priority SAQ_l (i.e. $l = 1$) for stored BSMs. If a queue is empty, it will check the immediate lower level queue, until a BSM is found and extracted. Then, the age of the extracted BSM is checked against a predefined timeout. This timeout aims to discard those BSMs that contain an outdated information. The typical value of this timeout corresponds to the BSM generation period, i.e. $100ms$. Hence, BSMs that are not verified within $100ms$ are dropped from the security queue, and the ITS safety application is notified about the unchecked BSM. This BSM loss is known as the cryptographic packet loss which is due to slow security verification.

Finally, once an extracted BSM has a valid age value, its signature is verified using the ECDSA algorithm. If the BSM signature is valid, the ITS safety application is notified to update its local dynamic map, as well as the BSM classifier module to train the k-means clustering algorithm, as already discussed in SubSection 3.1. In particular, the information contained inside the verified BSMs (e.g. vehicles' GPS location, speed, heading) could be exploited to prevent road accidents from happening by notifying the drivers regarding any eventual danger in their vicinity. However, in case of invalid BSM signature (due to malicious data injection attacks), a reputation module (30) could be notified to enable the detection and isolation of malicious nodes in the network, which is outside the scope of this paper.

3.4 Discussions

The proposed channel-aware ECDSA signature verification framework has many benefits. First, by taking advantage of the fact that BSMs have different received signal strengths and by using the concept of safety areas, our framework is able to classify the incoming messages based on the relative proximity of the neighbor vehicles. The highest priority BSMs are thus processed in priority with the lowest latency possible, increasing thus the accuracy of situational awareness between vehicles.

Second, thanks to the use of the concept of safety areas, our proposed framework is able to take into account the requirements of different ITS applications. For cooperative awareness applications, vehicles within a distance of 150m are most critical and hence, can be assigned priority as explained in SubSection 3.1(1). On

Algorithm 2 Scheduling of BSMs ECDSA Signatures Verification

```
1: procedure BSMs_Scheduling()
2:     while (true) do
3:         for l = 1 to k do
4:             if queue(SAQ_l).size() > 0 then
5:                 BSM = queue(SAQ_l).poll()
6:                 break
7:             end if
8:         end for
9:         if (Now() - BSM.timestamp) < timeout then
10:            notification = ECDSA_verify(BSM)
11:            switch notification do
12:                case valid
13:                    notify(ITS_Safety_Application, Valid_BSM)
14:                    notify(BSMs_Classifier, Valid_BSM)
15:                case invalid
16:                    notify(Reputation_module, Invalid_BSM)
17:        else
18:            discard(BSM)
19:            notify(ITS_Safety_Application, Unchecked_BSM)
20:        end if
21:    end while
22: end procedure
```

Algorithm 3 Adaptive Security Level Selection for Safety Vehicular Applications

function SECURITY_LEVEL(level,ops,k,k_{min},k_{max},th_{down},th_{up}, W)

Input:

level= [...], list of available security levels

ops= [...], list of operations per second corresponding to security levels

k, default security level array index

k_{min} minimum security level array index

k_{max}, maximum security level array index

th_{down}, threshold to reduce security level

th_{up}, threshold to increase security level

W, time window after which this function is repeated

At time instant T, calculate number of received safety packets by the security queue as P_r during the time interval $[T, T-W]$

At time instant T, calculate number of lost safety packets due to verification delay of greater than 100ms P_l during the time interval $[T, T-W]$

At time instant T, calculate cryptographic loss ratio as $CLR = \frac{P_r}{P_l}$

if $CLR > th_{down}$ **then**
  if level[k] >level[k_{min}] **then**
    $k = k - 1$
  end if
end if

if $(CLR < th_{up}) \wedge (P_r <ops[k+1])$ **then**
  if level[k] <level[k_{max}] **then**
    $k = k + 1$
  end if
end if

For the current level[k] calculate security overhead, signature delay and verification delay from Table. 1

end function

the other hand, applications such as emergency warning notification that require multi-hop transmissions could prioritize the BSMs coming from further distances to enable quick delivery of data over a geographical area (31; 32).

Third, our proposed security verification framework which is based on k-means clustering has a low computational time complexity of $O(n^{dk+1} \log n)$ (33), since k and d are fixed in our case. Here n is the number of received signal strength observations (i.e. P_m) taken from the received BSMs, k is the number of clusters or safety areas (taken as 5 in our algorithm but can be more based on ITS application requirements), d is the dimension of data points (its value is 1 in our case since we only use received signal strength for cluster formation). If i is the number of iterations needed to converge, the running time of k-means clustering algorithm can be given as $O(nkdi)$. Generally, the algorithm converges in around 12 iterations if the data has a clustering structure.

Finally, our framework operates on top of the VANETs MAC layer (e.g. IEEE 802.11p, or 4G/LTE), and is fully compliant with the WAVE IEEE 1609 (US) (2) and ETSI TC ITS (European) (3) standards. In fact, our proposed framework could be integrated within the security layer of these standards, without impacting the format of the exchanged messages and by using the recommended ECDSA schemes, i.e. ECDSA-256-SHA-256 for ETSI TC ITS and ECDSA-224-SHA-224 for IEEE 1609 (34).

4 Proposed Adaptive ECDSA Signature Generation Framework (Transmitter Side Security)

While security improves the reliability of vehicular applications, it generates increased packet size and delay for signing and/or encrypting packets at the transmitter. Higher packet sizes and processing times increase the end-to-end transmission delay of basic safety messages (BSMs). Hence, a clear tradeoff emerges between quality of service and safety awareness of vehicular applications (35).

In high density scenarios, each vehicle may receive several hundreds (or thousand) BSMs per second from neighboring vehicles, and which could not all be verified due to the limited computational resources. Indeed, we have shown in our recent experimental works (7; 34) that typical vehicular processors (1GHz) can hardly keep pace with the required real-time performance (e.g. up to 50 BSMs verified per second using the NISTP-256 with SHA-256 security algorithm (7)); whereas higher CPUs processors would result in increased performance. For example, an Intel Xeon processor can achieve up to 327 BSMs signature verification per second using the NISTP-256 with SHA-256 security algorithm (7), as shown in Table 1. However, even high CPU processors are not able to keep acceptable real-time performance, especially under high density vehicular scenarios.

In the remainder of this section, we introduce two novel adaptive transmitter security mechanisms to improve the scalability of secure vehicular applications. The first one uses a random security level selection approach whereas the second mechanism is based on adaptive security technique using security queue congestion metric i.e., CLR.

4.1 Random Security Level Selection Mechanism

In the random security level selection mechanism, each transmitter vehicle uses a random security level for BSM transmission. In Table. 1, we list the available security levels using ECDSA algorithms. Depending on Elliptic Curve prime field (NISTP) and Secure Hash Algorithm (SHA) digest size, different levels of security is possible. A higher NISTP and SHA value corresponds to a more robust security level. However, as shown in Table. 1, it increases the security processing delays.

We display the security overhead with and without certificate, signature delay, verification delay and verification operations per second (ops) in Table. 1. This table is formulated using our recent work where we experimentally benchmarked security processing parameters for various ECDSA algorithms using different CPU architectures (7). Safety messages, security header, certificate formats and security profiles were all implemented as per the ETSI ITS standard (3). In Table. 1, experimental security parameter values from our study for a medium speed Intel Xeon processor are listed.

In random mechanism, each vehicle picks one of the four possible security levels every transmission. This security level is sent as part of the packet that is used by the receiver to perform appropriate verification. The rationale behind random security level selection is to switch between different security levels especially in a dense network so that congestion at the security queue can be mitigated. Using a static security level selection, for example ECDSA NISTP256-SHA256 as proposed in ETSI standard, could result in increased cryptographic loss in a high density traffic scenario.

4.2 Adaptive Security Level Selection Mechanism

The goal of the adaptive security level selection mechanism is to select the best possible security level (i.e., security algorithm key size) and minimize the cryptographic loss. The proposed mechanism is shown in Algorithm 3. As mentioned earlier, each vehicle uses one of the available ECDSA algorithms to sign BSMs at the transmitter which are verified at the receiver using the same algorithm. Depending on the processor speed and security level, only a certain number of security operation per second can be performed. A higher NISTP and SHA values makes communications more secure, but

reduces the number of operations per second and hence, increases the signature and verification delays.

The proposed adaptive security mechanism adaptively takes a decision about the security level to be used by the transmitter every time window W. During this time window W, each vehicle evaluates the total packets that are received for verification at the security queue as P_r. Similarly, vehicles find the number of packets which could not get verified within the timeout period (taken as 100ms for safety applications) as P_l. To find cryptographic loss ratio CLR, vehicles take a ratio of P_r and P_l.

Each vehicle uses a threshold th_{down} which defines a tolerable level of CLR beyond which vehicles need to reduce their security level. This reduction in security level is to ensure safety applications do not lose packets because of security mechanism which can negatively impact their safety. The rationale is to maintain QoS while selecting best possible security level. If CLR is lower than th_{down} during current time window W, vehicle select the next lower available security level. This results in packet transmissions at a lower security level during the up coming time interval of W.

Vehicles can also move to a higher level of security if CLR falls below a threshold th_{up} and received BSMs P_r are less than the operations per second (ops) that can be performed for the next higher security level i.e., index $k+1$. The later condition ensures that an increase in security level will not result in congestion at the security queue. In this case, vehicles select the next security level from the available security levels. The use of two thresholds th_{down} and th_{up}, one for decreasing the security level and other for increasing the security level, is done to avoid rapid fluctuations of security level selection. In between these two thresholds, security level selection remains stable.

Finally, after appropriate security level selection, vehicles evaluate the security overhead, signature delay, verification delay and operation per second using Table. 1. The proposed algorithm iteratively runs every time window W and adapts the security level of each vehicle according to its CLR. Depending on neighborhood vehicle density, vehicles could receive different number of packets at the security queue and hence, operate at a different security levels according to Algorithm 3.

5 Performance Evaluation

In this section, we present the detailed performance evaluation of both receiver and transmitter side security mechanisms.

5.1 Simulation Setup

We develop a simulation model in NS-3 to analyse the performance of our proposed channel-aware signature verification framework of BSMs in VANETs.

The simulation parameters have been selected in accordance with practical settings in a vehicular environment. The propagation model uses dual slope path loss model with Nakagami-m fading as suggested in ETSI standard (36). Practical experiments have shown that signal propagation follows Nakagami-m fading in vehicular environment (37).

For mobility model, we have simulated practical urban road topology setting in SUMO traffic simulator. The simulated model is a grid shaped road structure of 2km×2km area with intersections. Moreover, SUMO uses realistic traffic flow model (car following model) to simulate car movements (38). The vehicle density is set to 200 vehicles/km^2 to create a dense network. To avoid border effect, the results are only evaluated within 1km×1km region in this scenario. The maximum vehicle speed is taken as 22m/s.

We have also used realistic IEEE 802.11p protocol stack available in NS-3 to evaluate network performance of ITS application (39). The protocol stack includes Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) based medium access protocol and IEEE 802.11p based physical layer parameters. In addition, the data traffic generation parameters are in accordance with ETSI standard (40). The WAVE model in NS-3 is used for BSM transmission exchange between vehicles. The packet size of BSM including the security overhead is taken as 300 bytes. Each vehicle generates 10 BSMs per second with a transmission range and data rate of 500m and 6Mbps respectively. The ECDSA-256-SHA-256 security algorithm is used to sign and verify BSMs (3). The typical time required to sign and verify the BSMs using this algorithm is 2ms and 5ms respectively (7; 16). BSMs that could not get verified within 100ms time interval are dropped from the security queue and this loss is termed as cryptographic loss.

For the available security level selection as per ETSI standard, We display the security overhead with and without certificate, signature delay, verification delay and verification operations per second (ops) in Table. 1. This table is formulated using our recent work where we benchmarked security processing parameters for ECDSA algorithm using different CPU architectures (7). Safety messages, security header, certificate formats and security profiles were all implemented as per the ETSI standard. In Table. 1, experimental security parameter values from our study for a medium speed Intel Xeon processor are listed.

The complete simulation parameters are listed in Table 1.

5.2 Simulation Results (Receiver Side Security)

We compare our proposed channel aware multi-level priority queue (MLPQ-CA) based signature verification mechanism with two existing techniques. The first technique is the single queue first-come-first-served (SQ-FCFS) which is the default signature verification mechanism in the WAVE and the ETSI standards

Table 2 Simulation parameters

Parameter		Value
Traffic	Road Area	2km×2km
	No. lanes	6 (3 per direction)
	Vehicle Density	200 vehicles/km^2
	Vehicle Speed	22 m/s
BSM	Packet Size	200 bytes
	Security overhead	100 bytes
	Generation Interval	100ms
	Data rate	6Mbps
	Transmission range	500m
Propagation model	Pathloss	Dual-slope
	Fading	Nakagami m = 1-3
Security	Algorithm	ECDSA-256-SHA-256
	Sign Duration	2ms (16; 34)
	Verify Duration	5ms (16; 34)

(2; 3). The second technique is the single queue random signature verification (SQ-Random) that randomly picks BSM for verification (10; 11).

5.2.1 Clustering and Classification

The proposed classification of BSMs based on the clustering mechanism is shown in Figure 3. As can be seen, BSMs are classified into five main clusters based on received powers to represent the considered safety areas. Using an online training phase, the cluster centroids are first calculated. These centroid values are also depicted in Figure 3. Once the centroid values are fixed, all incoming BSMs are directed to the corresponding safety areas and multi-level priority queues.

The accuracy of BSM classification using k-means clustering algorithm given in Table 3 is defined as the percentage of BSMs that were classified into the correct safety areas once the training phase is over. The global accuracy of this classification mechanism is around 63.2% whereas the accuracy is nearly 87.3% and 75.4% within a safety area of $50m$ and $100m$, respectively. It should be noted that the classification accuracy can not reach 100% because the received power is not perfectly correlated with the distance due to multi-path fading and shadowing effects. Nonetheless, the performance of safety messages is significantly enhanced, as it will be shown in the following sub-sections (e.g. cryptographic packet loss, delay, etc.)

5.2.2 Cryptographic Packet Loss (CPL)

Cryptographic packet loss is defined as the packets which were dropped from the security queue due to timeout i.e., slow security verification. We display the result in Figure 4. Both single queue approaches (SQ-FCFS and SQ-Random), exhibit a high number of cryptographic

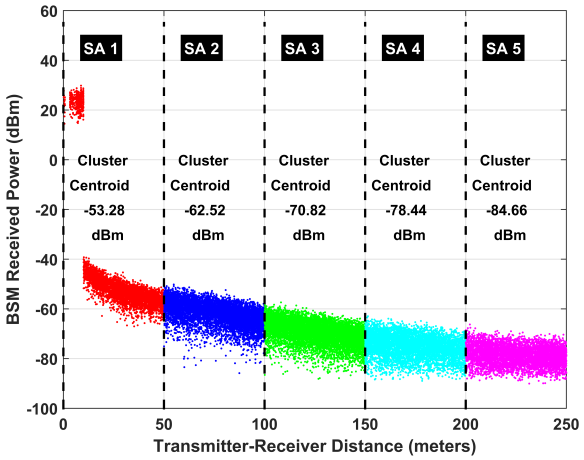

Figure 3: BSMs Received Powers Classification into Five Main Safety Areas.

Table 3 Accuracy of BSM classification based on K-Means Clustering

K-Means dispatching	Accuracy	Standard deviation
SA_1<= 50.00m	87.290%	0.333%
SA_2<= 100.00m	75.436%	0.430%
SA_3<= 150.00m	68.679%	0.464%
SA_4<= 200.00m	61.775%	0.486%
SA_5>200.00m	64.688%	0.478%

losses. However, we can notice that our proposed MLPQ-CA approach reduces the cryptographic losses for the

closest safety areas. Hence, less important packets are dropped (i.e. packets coming from nearby vehicles).

For a distance ≤ 150m, our proposed MLPQ-CA scheme incurs CPL below 1% whereas CPL is around 12 to 14% for other techniques. Also, we can notice that our approach generates higher CPL for distance > 200m in comparison to other approaches. This is not critical because our goal is to optimize BSMs processing for safety applications, where BSMs coming from closest vehicles are more important than the ones coming from further away vehicles.

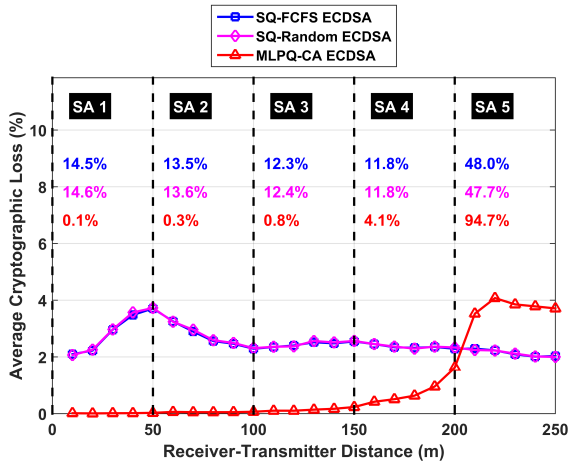

Figure 4: Average Cryptographic Packets Loss (95% confidence interval).

5.2.3 End-to-End BSM Delay

End-to-end delay is defined as the time duration between the packet generation and its reception at the receiver. This includes time for BSM signing, channel access, propagation, BSM waiting in the security queue and BSM verification. As shown in Figure 5, the delay experienced by BSMs when security is disabled is around 15ms in all the safety areas. When enabling security queuing, the delay increases to around 90ms. Random-based signature verification can reduce the delay to around 55ms. Finally, our approach is outperforming existing approaches, especially on the closest safety areas, with a achieved delay between 20ms and 30ms.

Since the end-to-end BSM delay depends on the security queuing delay which is the sum of BSM waiting time in the security queue and signature verification delay, it is displayed in Figure 6 for the different approaches. As the proposed MLPQ-CA approach assigns priority to the BSMs coming from nearby vehicles, it significantly reduces the security queuing delay compared with the single queue schemes. Specifically, this delay improvement is up to $30 - 70$ms within a safety area of 150m. The lower security queuing delay directly translates to quicker BSM transmission process, hence improving the capacity of the VANET system.

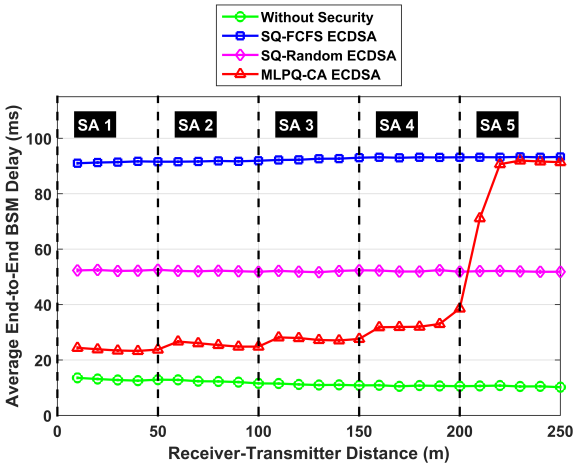

Figure 5: Average End-to-End Delay (95% confidence interval).

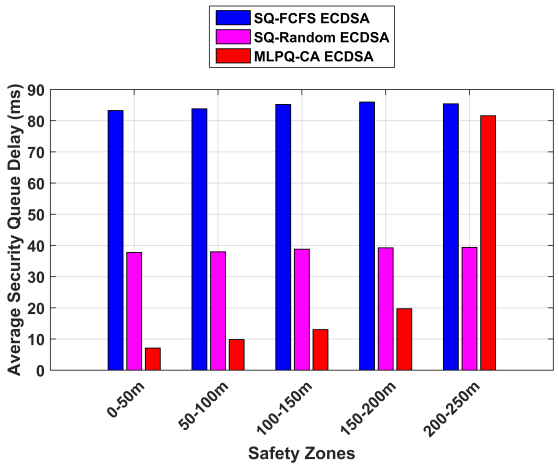

Figure 6: Average Security Queuing Delay (including 4ms for ECDSA signature verification).

5.2.4 Inter-BSM Delay

Inter-BSM delay is defined as the time difference between arrival of two consecutive BSMs from the same sender (27; 1; 22). As shown in Figure 7, our approach is behaving as in the ideal case (without security) on the closest safety areas. At a receiver-transmitter distance of 150m, our proposed MLPQ-CA scheme results in an inter-BSM delay of 150ms which is similar to the case when authentication is not used. However, by using the single queue schemes, the inter-BSM delay goes beyond 200ms.

It can be noted that the inter-BSM delay incurred by our proposed scheme increases at further safety areas. For example, this delay value can go up to 400ms at a safety distance of 200m. Since the security framework is to be used for the safety applications that prioritizes the nearby vehicles, our approach provides the best QoS.

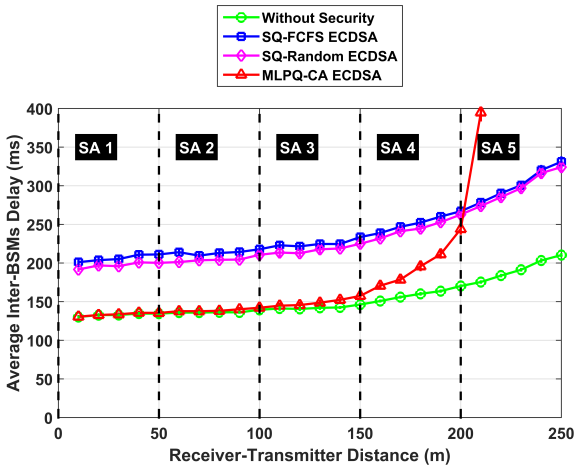

Figure 7: Average Inter-Message Delay (95% confidence interval).

5.2.5 *Cooperative Awareness Quality Level (AQL)*

The cooperative awareness quality level (AQL) metric within an area k as proposed by (41) is defined as the average *Awareness* of all M vehicles during T time instants i.e.,

$$AQL(k) = \frac{\sum_{j=1}^{T} \sum_{i \in M} Awareness_k{}^T(i)}{T \times M} \quad (4)$$

Here *Awareness* is calculated by the intersection of actual number of neighbors and the number of neighbors discovered using BSM i.e

$$Awareness_k{}^T(i) = \frac{|N_k{}^T(i) \bigcap V_k{}^T(i)|}{V_k{}^T(i)} \quad (5)$$

where $V_k{}^T(i)$ represents actual number of neighbors of vehicle i and $N_k{}^T(i)$ represents advertised number of neighbors received by vehicle i in BSM within an area k at a certain time T.

AQL provides information about how many of the actual neighbors a vehicle is aware of and gives a measure of application reliability. A higher AQL value implies a more reliable cooperative awareness application.

We depict the cooperative awareness quality level (AQL) in Figure 8. It can be seen that the global AQL (computed across a safety area of 500m) is almost the same for all approaches, and is very low around 15%. The reason behind this reduced awareness is the high packet loss due to collisions in the dense network. Additionally, multi-path fading at a high distances between receiver and transmitter also results in severe packet loss. Finally, the security overhead and verification processing time also results in degradation of awareness quality level (22).

However, when computing the AQL on the most important safety areas (<100m), our proposed MLPQ-CA approach is able to enhance the vehicle awareness level (70%) in comparison to the existing approaches (<50%). As the vehicles that are in the closer vicinity are a higher safety concern, the improved vehicle awareness can improve the QoS of cooperative awareness applications. While maintaining the authentication of BSMs from closer safety areas, the proposed approach results in a higher delivery ratio of those BSMs.

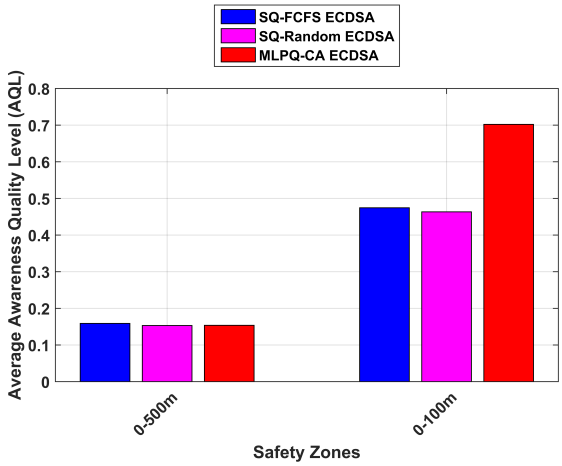

Figure 8: Average Cooperative Awareness Level for Areas: $0-100m$ and $0-500m$.

5.3 *Simulation Results (Transmitter Side Security)*

In this section, we present simulation results of proposed transmitter side security mechanisms i.e., random and adaptive, and compare it with the static security algorithm selection that uses the default recommended scheme in the ETSI standard i.e., ECDSA NISTP-256-SHA-256.

5.3.1 *Security Level Selection*

We display the percentage of received packets that were transmitted with a particular security level in Figure 9. For the static algorithm, all received packets were signed using the default security level of $P = 256$ and $SHA = 256$. On the other hand, proposed random mechanism uses all of the security levels with an equal percentage for security signature. In comparison, proposed adaptive mechanism uses network congestion measure i.e., CLR to select the best possible security level. Since we simulate a high density scenario, most of the received BSMs reduce the security level to the lowest possible in order to avoid packet loss due to slow security verification. Particularly, for a time window of 1s and 3s, the lowest security level is used by 48% and 65% of the received packets. The selection of time window W is a design parameter. As W is increased, the sample size for CLR calculation is increased and security level selection becomes more stable. However, too high value of W would increase the time after which adaptation is performed which might not be useful for road safety applications.

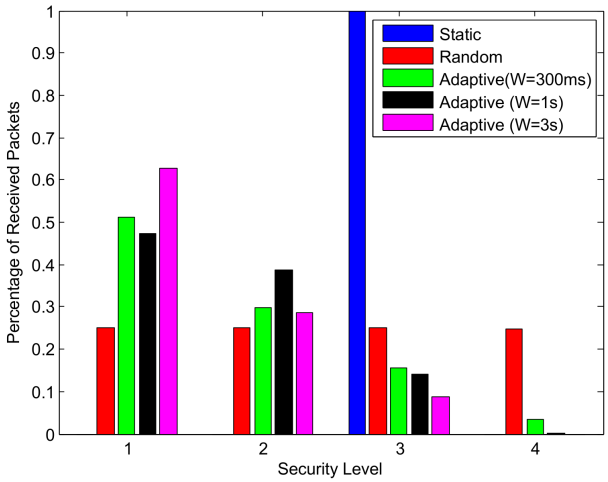

Figure 9: Percentage of received packets with a particular security algorithm.

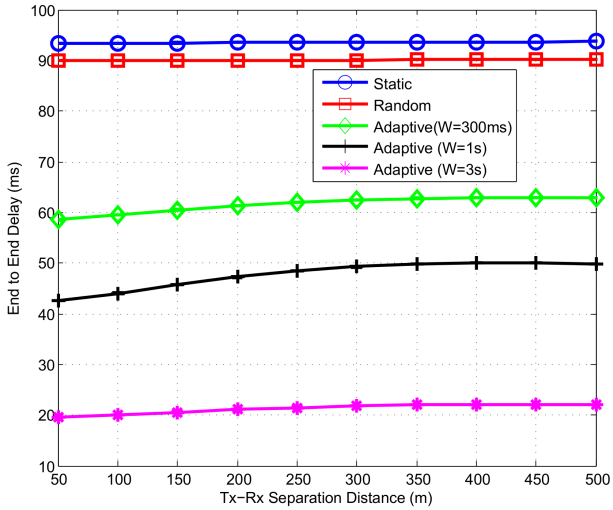

Figure 10: End-to-End Delay at different Tx-Rx Separation Distance and Vehicle Densities [confidence interval 95%].

5.3.2 End-to-End Delay

We present the end-to-end delay of BSMs in Figure 10 which is defined as the time interval between packet generation at the transmitter and when the packet was correctly verified at the receiver. It can be seen that static technique results in the largest delay of more than 90ms followed by the proposed random mechanism. In comparison, proposed adaptive mechanism significantly lowers the required end-to-end delay. Since the signature and verification delays are lower for the adaptive mechanism which uses lower security level as evident from Figure 9, packets are processed faster resulting in lower end-to-end delay. For the time window of 300ms, 1s and 3s, the end-to-end delay is 60ms, 45ms, and 20ms respectively.

5.3.3 Packet Inter-arrival Time

We show the packet inter-arrival time of BSMs in Figure 11 which is taken as the time between reception of two consecutive BSMs from the same sender. Since BSMs are generated every 100ms, an inter-arrival time closer to this time is deemed ideal. We can see that the static and random techniques result in an increased inter-arrival time reaching up to more than 170ms within a distance of 150m. For the adaptive technique, the inter-arrival time is maintained lower than 140ms. The reason is that the adaptive technique optimally selects the best possible security level to reduce congestion and hence, improves the packet inter-arrival delay. As a result, vehicles receive more frequent information of the neighborhood improving their safety.

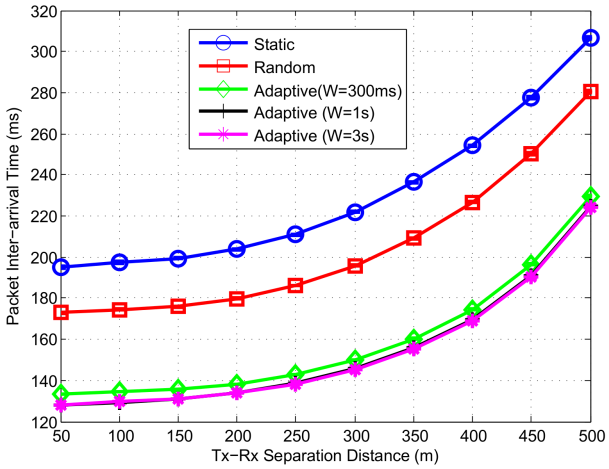

Figure 11: Packet Inter-arrival time at different Tx-Rx Separation Distance and Vehicle Densities [confidence interval 95%].

5.3.4 Cryptographic Loss Ratio

Cryptographic Loss Ratio is defined as the percentage of received BSMs which could not get verified within the 100ms timeout period as described earlier in Section III. From the results in Figure 12, we can see that the static and random techniques both result in large CLR of around 0.26 and 0.35. This amounts to a significant number of packets that can not get verified and safety information is lost. Since both techniques do not use any security adaptation, the queue congestion causes such a large packet loss. On the other hand, proposed adaptive technique selects the appropriate security level to minimize CLR. As a result, CLR is reduced to less than 0.06 for a time window of 300ms. A higher time window further improves the CLR reducing it to 0.025 at W equal to 3s.

5.3.5 Packet Delivery Ratio

We display packet delivery ratio (PDR) which is a metric that measures percentage of successfully received packets

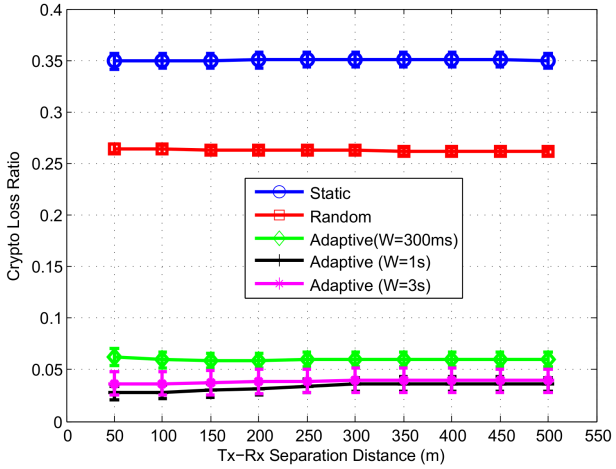

Figure 12: Cryptographic Loss Ratio at different Tx-Rx Separation Distance and Vehicle Densities [confidence interval 95%].

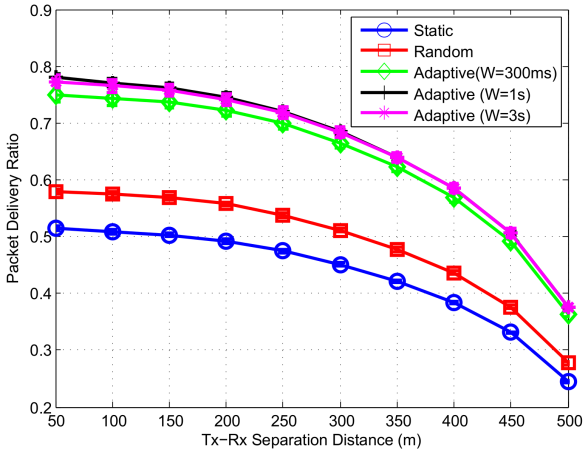

Figure 13: Packet Delivery Ratio at different Tx-Rx Separation Distance and Vehicle Densities [confidence interval 95%].

in Figure 13. PDR takes into account packet loss due to collisions, fading and cryptography. As can be seen, static and random techniques cause a significantly lower PDR due to their increased CLR. At a transmitter receiver distance of 150m, PDR is lower than 0.6 for both the techniques. On the other hand, adaptive technique improves PDR by $0.2 - 0.25$ in comparison with both techniques.

5.3.6 Safety Awareness Level

To evaluate the level of vehicle safety, we use safety awareness level metric proposed in (8).This metrics takes into account the quantity as well as accuracy of received safety information and hence, precision of LDM. We can see that the safety awareness of vehicles when using static and random technique is lower than 0.5. By using an adaptive selection of security level, we enhance the safety awareness by $0.15 - 0.2$.

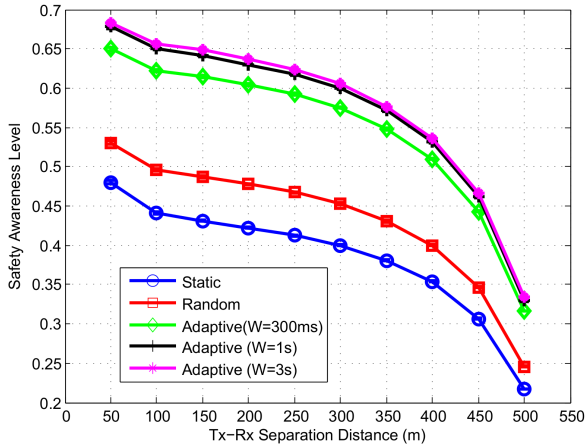

Figure 14: Safety Awareness Level at different Tx-Rx Separation Distance and Vehicle Densities [confidence interval 95%].

5.4 Discussions

From the results, it is evident that both proposed techniques i.e., transmitter and receiver side, perform better than the static security verification and security level selection as in the ETSI standard. Particularly, for a high density urban scenario, where vehicles receive large number of packets for verification, these techniques can be combined to significantly improve QoS of safety applications. Channel aware verification technique can reduce the over all delay by quickly processing the critical BSMs.

At the transmitter side, random technique reduces cryptographic loss by choosing a uniformly distributed security level at each transmission. However, it lacks an adaptive mechanism based on security queue congestion metric. This adaptive selection of security level based on network traffic at the security queue is the basis of our second proposal. The adaptive mechanism thus balances the security-QoS tradeoff for safety application.

6 Conclusion

In this paper, we propose two adaptive security mechanisms, one at the receiver and other at the transmitter side of a vehicular network. At the receiver, a channel aware based approach is proposed to prioritize the signature verification time of received BSMs. The proposed scheme uses a BSM classification mechanism based on received power and safety areas with the help of k-means clustering algorithm. BSMs that arrive from close proximity are assigned higher priority using a multi-level priority queue ensuring their quick verification. At the transmitter side, we propose the use of random and adaptive security level selection techniques, thus choosing optimal security based on cryptogaphic loss rate. Using simulation results, both proposed mechanisms have shown significant

improvement in terms of cryptographic packet loss, end-to-end delay, inter-BSM delay and awareness quality level. Vehicular network can thus gain maximum benefit by combining these two techniques to maintain security-QoS tradeoff.

Acknowledgment

This article was made possible by NPRP grant #[7-1113-1-199] from the Qatar National Research Fund (a member of Qatar Foundation). The statements made herein are solely the responsibility of the authors.

References

[1] M. A. Javed, D. T. Ngo, and J. Y. Khan, "Distributed spatial reuse distance control for basic safety messages in SDMA-based VANETs," *Vehicular Communications*, vol. 2, no. 1, pp. 27 – 35, 2015.

[2] "Ieee guide for wireless access in vehicular environments (wave) - architecture," IEEE, Tech. Rep., March 2014.

[3] ETSI TR 101 607, "Intelligent transport systems (ITS); cooperative its (c-its); release 1," Version 1.1.1, ETSI ITS WG2, Sophia Antipolis, France, May 2013.

[4] ETSI EN 302 895, "Intelligent transport systems (ITS); vehicular communications; asic set of applications; loal dynamic map (ldm)," Version 1.1.1, ETSI ITS WG2, Sophia Antipolis, France, Sep. 2014.

[5] E. B. Hamida, H. Noura, and W. Znaidi, "Security of cooperative intelligent transport systems: Standards, threats analysis and cryptographic countermeasures," *Electronics*, vol. 4, no. 3, p. 380, 2015. [Online]. Available: http://www.mdpi.com/2079-9292/4/3/380

[6] L. Ben Othmane, A. Al-Fuqaha, E. Ben Hamida, and M. van den Brand, "Towards extended safety in connected vehicles," in *Intelligent Transportation Systems - (ITSC), 2013 16th International IEEE Conference on*, Oct 2013, pp. 652–657.

[7] M. A. Javed, E. Ben Hamida, and W. Znaidi, "Security in intelligent transport systems for smart cities: From theory to practice," *Sensors*, vol. 16, no. 6, 2016. [Online]. Available: http://www.mdpi.com/1424-8220/16/6/879

[8] E. B. Hamida and M. A. Javed, "Channel-aware ECDSA signature verification of basic safety messages with k-means clustering in VANETs," in *Proc. IEEE Intl. Conf. on Advanced Information Networking and Applications*, March 2016, pp. 1–8.

[9] M. A. Javed and E. B. Hamida, "Adaptive security mechanisms for safety applications in internet of vehicles," in *Proc. IEEE Intl. Conf. on Wireless and Mobile Computing, Networking and Communications*, Oct. 2016, pp. 1–7.

[10] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing vehicular communications," *Wireless Communications, IEEE*, vol. 13, no. 5, pp. 8–15, October 2006.

[11] S. Biswas and J. Misic, "Location-based anonymous authentication for vehicular communications," in *Personal Indoor and Mobile Radio Communications (PIMRC), 2011 IEEE 22nd International Symposium on*, Sept 2011, pp. 1213–1217.

[12] 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, April 2009.

[13] 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*, April 2008.

[14] Z. Li and C. Chigan, "On resource-aware message verification in vanets," in *Communications (ICC), 2010 IEEE International Conference on*, May 2010, pp. 1–6.

[15] S. Biswas and J. Misic, "Relevance-based verification of VANET safety messages," in *Proc. IEEE Intl. Conference on Communications*, June 2012, pp. 5124–5128.

[16] S. Banani and S. Gordon, "Selecting basic safety messages to verify in VANETs using zone priority," in *Proc. Asia-Pacific Conference on Communications*, Oct 2014, pp. 423–428.

[17] B. P. Rocha, D. N. Costa, R. A. Moreira, C. G. Rezende, A. A. Loureiro, and A. Boukerche, "Adaptive security protocol selection for mobile computing," *Journal of Network and Computer Applications*, vol. 33, no. 5, pp. 569 – 587, 2010, middleware Trends for Network Applications.

[18] W. Aman and E. Snekkenes, "Managing security trade-offs in the internet of things using adaptive security," in *Proc. International Conference for Internet Technology and Secured Transactions*, Dec 2015, pp. 362–368.

[19] S. Slijepcevic, M. Potkonjak, V. Tsiatsis, S. Zimbeck, and M. B. Srivastava, "On communication security in wireless ad-hoc sensor networks," in *Enabling Technologies: Infrastructure for Collaborative Enterprises, 2002. WET ICE 2002. Proceedings. Eleventh IEEE International Workshops on*, 2002, pp. 139–144.

[20] L. Zhou, A. V. Vasilakos, N. Xiong, Y. Zhang, and S. Lian, "Scheduling security-critical multimedia applications in heterogeneous networks," *Computer Communications*, vol. 34, no. 3, pp. 429 – 435, 2011, special Issue of Computer Communications on Information and Future Communication Security.

[21] M. Saadatmand, A. Cicchetti, and M. Sjödin, *Design of Adaptive Security Mechanisms for Real-Time Embedded Systems*. Springer Berlin Heidelberg, 2012, pp. 121–134.

[22] M. A. Javed and E. B. Hamida, "Measuring safety awareness in cooperative ITS applications," in *Proc. IEEE Wireless Communication and Networking Conference*, April 2016, pp. 1–7.

[23] E. Ben Hamida and G. Chelius, "Investigating the impact of human activity on the performance of wireless networks - an experimental approach," in *World of Wireless Mobile and Multimedia Networks (WoWMoM), 2010 IEEE International Symposium on a*, June 2010, pp. 1–8.

[24] R. Meireles, M. Boban, P. Steenkiste, O. Tonguz, and J. Barros, "Experimental study on the impact of vehicular obstructions in vanets," in *Vehicular Networking Conference (VNC), 2010 IEEE*, Dec 2010, pp. 338–345.

[25] T. Abbas, F. Tufvesson, and J. Karedal, "Measurement based shadow fading model for vehicle-to-vehicle network simulations," *CoRR*, vol. abs/1203.3370, 2012. [Online]. Available: http://arxiv.org/abs/1203.3370

[26] S. Lloyd, "Least squares quantization in pcm," *IEEE Trans. Inf. Theor.*, vol. 28, no. 2, pp. 129–137, Sep. 2006. [Online]. Available: http://dx.doi.org/10.1109/TIT.1982.1056489

[27] M. B. Brahim, E. B. Hamida, F. Filali, and N. Hamdi, "Performance impact of security on cooperative awareness in dense urban vehicular networks," in *2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Oct 2015, pp. 268–274.

[28] Y. Ding, Y. Zhao, X. Shen, M. Musuvathi, T. Mytkowicz, and M. Musuvathi, "Yinyang k-means: A drop-in replacement of the classic k-means with consistent speedup," in *Proceedings of the 32nd International Conference on Machine Learning, ICML 2015, Lille, France, 6-11 July 2015*, July 2015, p. 579587.

[29] E. Lee, E. K. Lee, M. Gerla, and S. Y. Oh, "Vehicular cloud networking: architecture and design principles," *IEEE Communications Magazine*, vol. 52, no. 2, pp. 148–155, February 2014.

[30] S. Dhurandher, M. Obaidat, A. Jaiswal, A. Tiwari, and A. Tyagi, "Vehicular security through reputation and plausibility checks," *Systems Journal, IEEE*, vol. 8, no. 2, pp. 384–394, June 2014.

[31] M. A. Javed, J. Y. Khan, and D. T. Ngo, "Joint space-division multiple access and adaptive rate control for basic safety messages in VANETs," in *Proc. IEEE Wireless Communication and Networking Conference*, April 2014, pp. 1–5.

[32] M. A. Javed and J. Y. Khan, "A geocasting technique in an IEEE802.11p based vehicular ad hoc network for road traffic management," in *Proc. IEEE Australasian Telecommunication Networks and Applications Conference*, Nov 2011, pp. 1–6.

[33] M. Inaba, N. Katoh, and H. Imai, "Applications of weighted voronoi diagrams and randomization to variance-based k-clustering: (extended abstract)," in *Proceedings of the Tenth Annual Symposium on Computational Geometry*, ser. SCG '94. New York, NY, USA: ACM, 1994, pp. 332–339. [Online]. Available: http://doi.acm.org/10.1145/177424.178042

[34] E. Ben Hamida, W. Znaidi, and H. Menouar, "Implementation and evaluation of the ETSI security architecture for cooperative intelligent transport systems," in *Proc. IEEE Vehicular Technology Conference (VTC-Fall)*, Sep. 2015, pp. 1–5.

[35] M. A. Javed and E. B. Hamida, "On the interrelation of security, qos, and safety in cooperative its," *IEEE Transactions on Intelligent Transportation Systems*, vol. PP, no. 99, pp. 1–15, 2016.

[36] The European Telecommunications Standards Institute, "ETSI TR 102 861 v1.1.1 - Intelligent transport systems (ITS) - STDMA recommended parameters and settings for cooperative ITS; Access Layer Part," Tech. Rep., 2012.

[37] J. Karedal, N. Czink, A. Paier, F. Tufvesson, and A. Molisch, "Path loss modeling for vehicle-to-vehicle communications," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 1, pp. 323–328, Jan. 2011.

[38] "Sumo car-following models [online]," www.sumo.dlr.de/wiki/Car-Following-Models, accessed: 2017-01-20.

[39] "Ns-3 wave model [online]," www.nsnam.org/docs/models/html/wave.html, accessed: 2017-01-20.

[40] The European Telecommunications Standards Institute, "ETSI TS 102 637-2 v1.2.1 - Intelligent transport systems (ITS) - Vehicular communications - Basic set of applications - Part2: Specification of cooperative awareness basic service," Tech. Rep., 2011.

[41] M. Feiri, J. Petit, R. Schmidt, and F. Kargl, "The impact of security on cooperative awareness in vanet," in *Proc. IEEE Vehicular Networking Conference*, Dec 2013, pp. 127–134.