Adaptive Security for Intelligent Transport System Applications

Muhammad Awais Javed, Elyes Ben Hamida, Ala Al-Fuqaha, Bharat Bhargava

Adaptive Security for Intelligent Transport System Applications

Muhammad Awais Javed, Elyes Ben Hamida, Ala Al-Fuqaha and Bharat Bhargava

***Abstract*—The transportation system is gradually migrating toward autonomous, electric and intelligent vehicles. Wireless-enabled vehicles along with infrastructure units on the road are connected with traffic management centers that use intelligent data analysis tools to efficiently manage city's traffic. However, such wireless connectivity can make the ITS networks vulnerable to security threats; thus, impacting the application's reliability. On the other hand, the use of robust security techniques could hamper applications' quality of service (QoS). To understand the interplay between these two conflicting requirements, this article reviews the security and QoS design challenges in the ITS aspect of smart cities. Using an experimental test-bed, we evaluate the standard compliant security processing delays, develop an online tool that presents detailed security benchmark results, and study the impact of security on QoS using simulation results. We also discuss how machine learning based adaptive signature verification techniques can enhance QoS in ITS. We further present future opportunities to optimize the security-QoS balance for ITS applications.**

I. Introduction

In the current era of connectivity, a number of transportation applications are envisaged to utilize mobile and wireless technologies. Traffic management and passenger safety are important domains where ubiquitous connectivity between vehicles can play a vital role. In Jan. 2016, The Wall Street Journal published an article that indicates that the US federal government is planning to spend $4 billion over the next ten years to encourage the development of autonomous and semi-autonomous vehicles [1]. Moreover, M-City at the University of Michigan provides 32 acres and 3000 test vehicles to study the different aspects of Connected Vehicles.

Intelligent Transportation Systems (ITS) are expected to provide safer travel to commuters, manage traffic to reduce road congestion, and offer various infotainment services. Using data exchange between different ITS entities such as vehicles, road side units (RSUs) and traffic management centers, a reliable traffic management system will be developed. With a decade of research that has been conducted in the field of Vehicular Ad-hoc Networks (VANETs), ITS standards have already been finalized and many ITS applications are set to become reality.

Muhammad Awais Javed is with the Electrical Engineering Department, COMSATS Institute of Information Technology, Pakistan. (e-mail: awais.javed@comsats.edu.pk)

Elyes Ben Hamida is with the Institute for Technological Research SystemX, France. (e-mail: elyes.ben-hamida@irt-systemx.fr)

Ala Al-Fuqaha is with the with the Computer Science Department, Western Michigan University, USA. (e-mail: ala.al-fuqaha@wmich.edu)

Bharat Bhargava is with the Department of Computer Sciences, Purdue University, USA . (e-mail: bb@cs.purdue.edu)

Security and privacy of data shared between the different entities of an ITS is a key technical challenge [2]. With the plethora of applications offered by ITS, there exists a susceptibility to network attacks by malicious nodes [3]. Particularly, applications that involve human safety such as those that impact vehicle driving decisions could be at greater security risk. Therefore, it is important to provide data integrity, authenticity, confidentiality and non-repudiation for all smart city applications. Moreover, each ITS entity should maintain its privacy and anonymity.

Since ITS rely on developing secure communications between different ITS entities, denial of service (DoS) attacks could severely disrupt its functionality by congesting the network with bogus messages. Furthermore, malicious nodes could pretend to be real vehicles or infrastructure units disseminating inaccurate or false information about vehicle locations, traffic densities, etc. within the ITS network. Another possible attack involves eavesdropping where vehicles could listen to secret communications between users or passengers' private data while making mobile online transactions. Finally, hardware sensors could also experience a fault, generating inaccurate data and impact the functionality of various applications.

To counter the security threats related to ITS applications, security procedures and algorithms have been defined in the IEEE Wireless Access for Vehicular Environments (WAVE) standard in the United States and European Telecommunications Standards Institute (ETSI) TC ITS standard in Europe [4], [5]. Elliptic Curve Cryptography (ECC) based algorithms are the chosen schema for digital signature, certification and encryption. Secure messages can be transmitted using the default wireless technology for ITS (i.e., IEEE 802.11p). With the pervasive deployment and use of ITS applications, significant traffic load is introduced in the network. Hence, QoS becomes more critical with the presence of many bandwidth hungry applications. A key challenge is thus to satisfy the network requirements of each application. Security algorithms may enhance protection against network attacks but they also incur a cost in terms of packet overhead and security processing delay. This could defeat the purpose of reliable transmission of data within the ITS network if communications is secured but the packets are not delivered within the latency requirements. Therefore, it is critical to study this security-QoS tradeoff in the context of ITS and chalk out a dynamic approach in this regard.

The objective of this article is to review the challenges and opportunities in the domain of security-QoS tradeoff for ITS applications. We first introduce the communications architecture of ITS followed by the security and QoS design

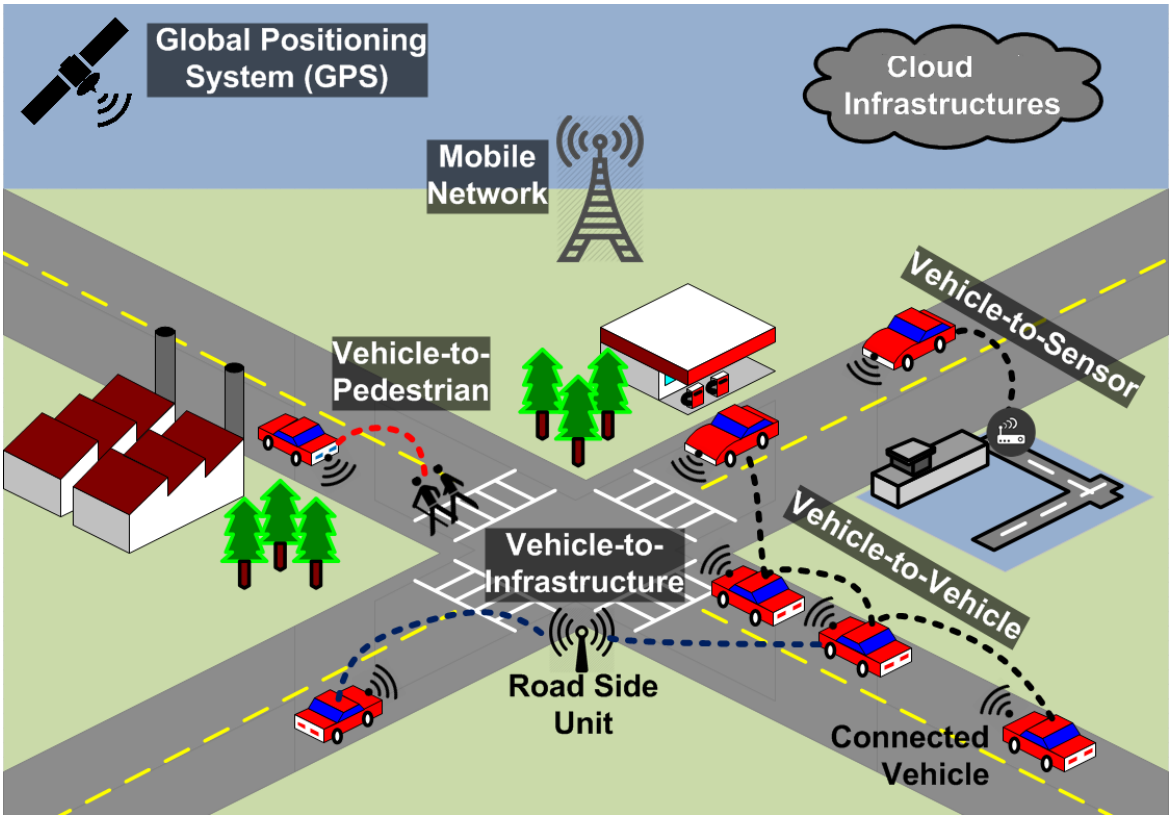


Fig. 1: Communications in ITS.

challenges. After that, we implement the ETSI ITS security standard as per the latest technical specifications (i.e., ETSI TS 103 097 [5]) and present experimental benchmark results for security processing delay. We also develop an online tool to show detailed benchmark results for various security parameters. We further present simulation results that summarize the impact of security on ITS applications' QoS. We then present an adaptive signature verification mechanism from our previous work [6] to demonstrate how the conflicting security-QoS requirements can be balanced for ITS safety applications. We also show how adaptive signature verification can help vehicles to use cheaper processors with lower clock rates. At the end of article, we highlight future research directions to jointly improve the security and QoS of ITS applications.

II. Communications in ITS based Smart Cities

ITS is a pivotal technology with major transportation, efficiency and safety applications [7]. To form an ITS network, vehicles exchange information with each other, geographical infrastructure road-side units and human sensors as shown in Fig. 1. A lot of standardization work has been completed in the ITS domain including the IEEE WAVE and the ETSI ITS standards that define the functionalities of the data generation, data dissemination and security procedures for ITS applications.

The typical data that is generated in an ITS includes periodic safety messages containing vehicle position, heading and speed information known as Basic Safety Messages (BSMs) in the IEEE WAVE standard and Cooperative Awareness Messages (CAMs) in the ETSI TC ITS standard. These messages help vehicles to build a local database of the neighborhood traffic called Local Dynamic Map (LDM) facilitating them to take critical driving decisions such as lane change and applying brakes. Other types of data that are generated in ITS include warning notifications, efficient route guidance for traffic management and Internet-based entertainment and convenience services such as access to multimedia files and banking transactions.

With the Internet connectivity feature in the form of ITS, vehicles could benefit from many potential infotainment and IoT applications. For example, using Internet collected data with machine learning techniques, vehicle dynamic and power terrain modules could be controlled to reduce energy consumption of vehicles. Moreover, vehicles could be remotely monitored by the authorities in terms of their registration and operational management. In addition, applications such as real-time fleet management, optimized logistics and infotainment solutions could be enabled using ITS.

Each application in ITS as defined in ETSI standard [8] has its own set of system requirements in terms of communications modes, transmission range, transmission frequency, critical latency and level of required security as shown in our proposed Table. I. Active safety applications have stringent requirements of latency as well as security because they involve human safety. So, they need to maintain data integrity, keep privacy and anonymity of the vehicle identities, and non-repudiation. Traffic efficiency applications such as route guidance can

TABLE I: System Requirements of ITS Applications.

Application	Use Cases	Communication Modes	Tx Range	Tx Frequency	Critical Latency	Security Requirements
Active Road Safety	Cooperative awareness Collision warning Emergency notification	Broadcast Single-hop/Multi-hop	300m to 1km	10 Hz	<100ms	Data integrity Privacy and Anonymity Non-repudiation
Traffic Efficiency	Route guidance Optimal green light advisory	Broadcast Multi-hop	1km	2 Hz	<500ms	Data integrity Privacy and Anonymity
Global Internet Services	Multimedia download Multiplayer games	Unicast Multi-hop	1km	1 Hz	<1s	Data integrity
Pedestrian Comfort	Pedestrian crossing	Broadcast Single-hop	500m	5Hz	<200ms	Data integrity Privacy and Anonymity Non-repudiation
Electronic Commerce	Online transactions	Unicast Multi-hop	1km	1Hz	<500ms	Data integrity Data confidentiality

afford a higher delay and work well with a medium level of security. On the other hand, Global Internet services that are not time critical and have lesser impact on human safety can use a light weight cryptography. Pedestrian comfort applications such as vehicle-pedestrian collision avoidance also require a high level of security. Applications that provide electronic commerce are prone to security threats and even though their transmission requirements are not that strict, they require data confidentiality and encryption to secure the user private data.

III. Security and QoS Design Challenges for ITS

Security and QoS are network services that are interlinked and have an impact on each other [9]. Some of the key security and QoS design challenges for ITS applications are discussed below.

A. Key Security Design Challenges

Security is a vital requirement for a reliable data exchange in ITS. Applications that involve vehicle safety or sharing personal information are prone to security threats and need to be secured against network attacks. Generally speaking, ITS needs to ensure the following security requirements and take the appropriate measures.

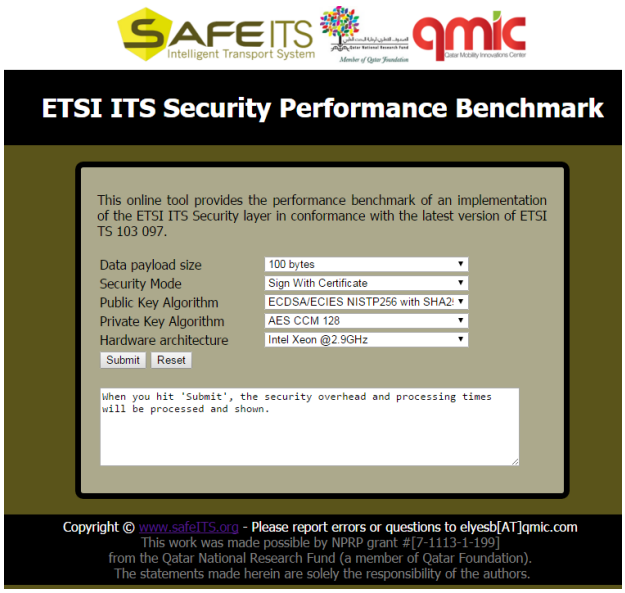
- Data Integrity and Authenticity: To ensure that the data transmission in ITS is free of any unapproved alteration by a malicious user, it is necessary to sign messages with a digital signature. This allows receivers to verify the message authenticity and integrity.
- Data Confidentiality: Access to the data packets shared in ITS should be restricted to prevent information leakage to unauthorized users. This can be achieved with the help of data encryption which makes it intelligible only to the approved nodes.
- Privacy and Anonymity: Identification of drivers and their vehicles should be not disclosed and user shall retain the right to control sharing of his personal information.
- Identity and Non-repudiation: Each ITS entity should have a distinct identity so that the identity of the message originator can be verified. A centralized certificate authority should issue digital certificates that can be used to verify the identity of sending nodes in ITS.
- Security overhead: The security overhead is defined as the cost incurred to implement a security procedure (e.g., signature, encryption, verification, decryption, etc.) in terms of packet size. The security overhead affects network metrics such as packet delivery ratio and end-to-end delay. Since most applications in ITS require real-time availability of information, it is important to select a light-weight cryptographic algorithm which incurs a low security overhead while still ensuring data security.
- Security robustness: Security robustness is defined in terms of strength of the employed security algorithms against network attacks. A more robust security algorithm (with a higher key size) requires a higher security overhead; however, it also provides greater resilience against malicious nodes. The level of security robustness in terms of the use of digital signatures, certificates, encryption or a combination of these, should be decided based on the application. For example, safety ITS applications such as cooperative awareness must use a digital signature with every message to avoid getting false negatives/positives. Similarly, an online payment for phone bill or parking payment in ITS should use encryption to prevent access to the credit card information. Certain other non-safety applications such as multi-player games may work well even with a reduced level of security.

B. Key QoS Design Challenges

QoS defines network requirements in terms of performance, service availability and scalability. ITS target a wide range of applications, use-cases and requirements, for example, in terms of communications mode, messaging type, critical latency, communications range and so on. Thus, the ITS protocol stack should be able to adapt to context changes and support different levels of QoS. The major ITS design challenges in terms of performance and QoS are as follows:

- Frequent Context Changes: ITS exploit different types of communications modes (e.g., multi-hop Vehicle-to-Vehicle (V2V), vehicle-to-infrastructure (V2I), short/long

(a) ETSI TC ITS Compliant Security Module (BeagleBone version).



(b) Online tool for ITS Security Performance Benchmark [10].

Fig. 2: ETSI TC ITS Security Standard Compliant Experimental Test-Bed and Online Tool.

range, etc.), and operate in various environments (e.g., indoor, outdoor, low or high network density, etc.). Thus, the ITS radio and protocol stack should be efficient and capable of adapting to frequent context changes.

- Dynamic Network Conditions: ITS entities such as vehicles are highly mobile and the resulting network topology is thus dynamic, and evolves over time due to changing network and connectivity conditions.
- Reliable Connectivity: On board Units (OBUs) of vehicles and Road-Side Units (RSUs) support a wide range of communications technologies including infrastructure-based, ad-hoc and device-to-device options (e.g., IEEE 802.11p, WiFi/WiFi-Direct, Bluetooth Smart, 4G/LTE-Direct, etc.). As a consequence, the ITS protocol stack should be able to support opportunistic communications mechanisms to guarantee reliable and stable end-to-end network connectivity between surrounding vehicles, RSUs and remote ITS servers.
- Hard Delay Requirements: ITS applications have to meet hard delay and real-time constraints, especially in the context of road safety applications. The critical latency is thus the main performance metric for ITS systems.

IV. Impact of Security on QoS in ITS

The interdependency of security and QoS impacts the application's performance in ITS. The security procedure in ITS works in a two-step process. At the transmitter, packets are signed and/or encrypted and a certificate is eventually attached to the packets before sending them over the wireless channel. At the receiver side, each packet is verified and/or decrypted before passing it to the application layer. The ITS standards including the IEEE WAVE and the ETSI ITS define the use of Elliptic Curve Cryptography (ECC) based algorithms for digital signature and encryption of messages [4], [5]. The data generated in ITS is signed using the Elliptic Curve Digital Signature Algorithm (ECDSA NIST-P256 with SHA 256) and encryption is achieved with the help of Elliptic Curve Integrated Encryption Scheme (ECIES NIST-P256 with AES-CCM-128). Note that the latest IEEE 1609.2 standard [4] also includes an option to sign ITS packets using elliptic curve brainpoolP256r1, which is not considered as part of this paper.

From the point of view of computational cost associated with the security procedure, three parameters are important including security overhead, ENCAP delay (for signature/encryption operations) at the transmitter, and DECAP delay (for security verification/decryption) at the receiver. A higher security overhead increases the packet size and hence the packet transmission time and channel utilization. ENCAP delay is the time required for preparation of the secured message at the transmitter. DECAP delay is the time required at the receiver to verify and/or decrypt the packet. It is a vital parameter since vehicles receive many packets simultaneously and a higher DECAP delay would result in congestion at the receiver.

A. Test-bed and Experimental Benchmark

To evaluate security processing parameters for ITS applications, we used a cryptographic API known as Bouncy Castle to implement ECDSA and ECIES security procedures as per the ITS standards. The cryptographic procedure included the ETSI security header, certificate format and security profiles according to latest version of ETSI ITS standard [3]. Our cryptographic implementation was tested and validated using the web validator named Fraunhofer FOKUS ETSI TS 103 097 during the 4^{th} ETSI ITS Plugtest event.

Compared to the IEEE 802.11p standard, the ETSI ITS standard defines additional facilities layer and extended network layer to include geonetworking functionality. The facilities layer collects, stores and provides safety information which

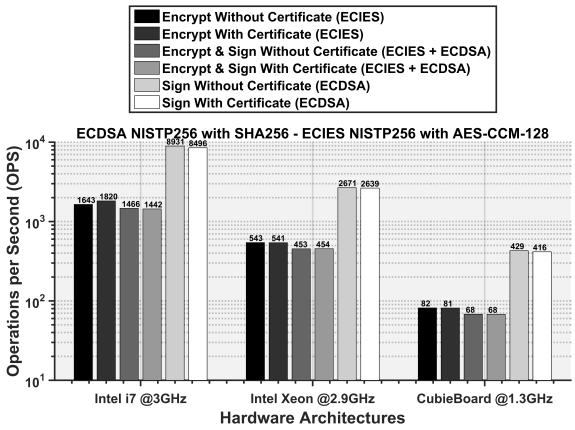


Fig. 3: Number of ENCAP operations per second for different security procedures and processor speeds using the ETSI standard.

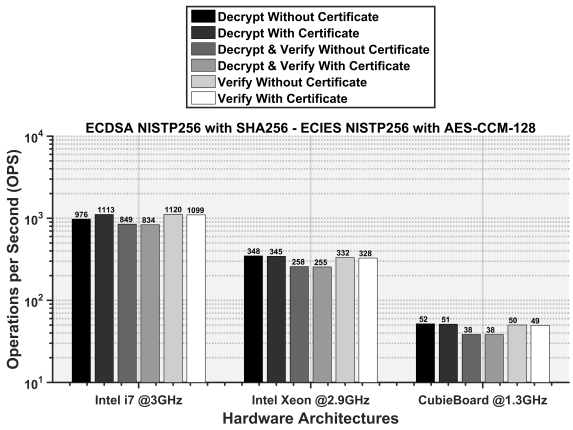


Fig. 4: Number of DECAP operations per second for different security procedures and processor speeds in ETSI standard.

is required by many ITS applications. The geoNetworking protocol layer defines the network routing functions using the geographical location information of nodes. We integrated these two layers through standard compliant service access points; thus, developing a stand-alone software module as shown in Fig. 2a [3].

The testbed on which cryptographic procedures were implemented include three different CPU architectures including Intel i7, Intel Xeon and CubieBoard. We performed experiments at different levels of security depending on whether packet is only signed and/or encrypted with or without a certificate. The realistic values of security processing parameters including security overhead, ENCAP delay and DECAP delay based on our experimental studies are listed in an online tool developed by us as shown in Fig. 2b.

Fig. 3 illustrates the average number of ENCAP operations per seond (i.e., number of security signature and/or encryption operations per second that can be performed by a particular CPU processor) using different CPU processors. The cryptographic key size and other security parameters are set as recommended per the ETSI standard. It can be seen that a faster processor with higher clock rate performs more security operations per second. For example, a 3GHz Intel i7 processor can perform more than 8000 signature operations per second whereas a 1.3GHz CubieBoard processor can only perform less than 500 signature operations per second.

Fig. 4 illustrates the average number of DECAP operations per second (i.e., number of security verification and/or decryption operations per second that can be performed by a particular CPU processor) using different CPU processors. A CubieBoard processor of 1.3GHz can only perform $38 - 52$ security processing operations per second and hence, incurs a very high security processing time. In comparison, Intel Xeon processor with a speed of 2.9GHz, is able to process $255 - 348$ packets per second and a more powerful 3GHz Intel i7 processor improves the security processing rate to 1120 packets per second. Since the "decrypt and verify"' security operation is the most complex security operation, a CPU can perform less number of DECAP operations per second as compared to other security operations (e.g., decrypt, verifty, etc.).

The security processing rate also depends on the level of security added to a packet. For example, if a packet is both signed and encrypted along with a certificate, it takes the highest time to process at the receiver. Therefore, such a security level should only be restricted to critical applications. For complete set of security parameters including ENCAP and DECAP delays, readers can refer to our online tool [10].

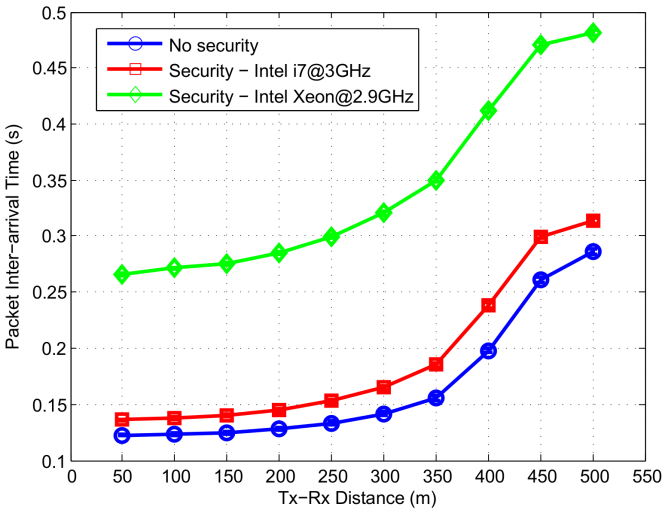


Fig. 5: Average Inter-CAM Delay (95% confidence interval).

B. Simulation Results

To study the impact of security on QoS, we perform simulations in NS-3 simulator for a safety ITS application where each vehicle periodically broadcasts CAMs to inform neighboring vehicles of its mobility information. Each transmitted CAM is signed using the ECDSA algorithm whereas certificate information is sent only once per second as per the ETSI ITS standard [5]. The received CAMs which cannot be verified within 100ms time interval are dropped. We use a vehicle

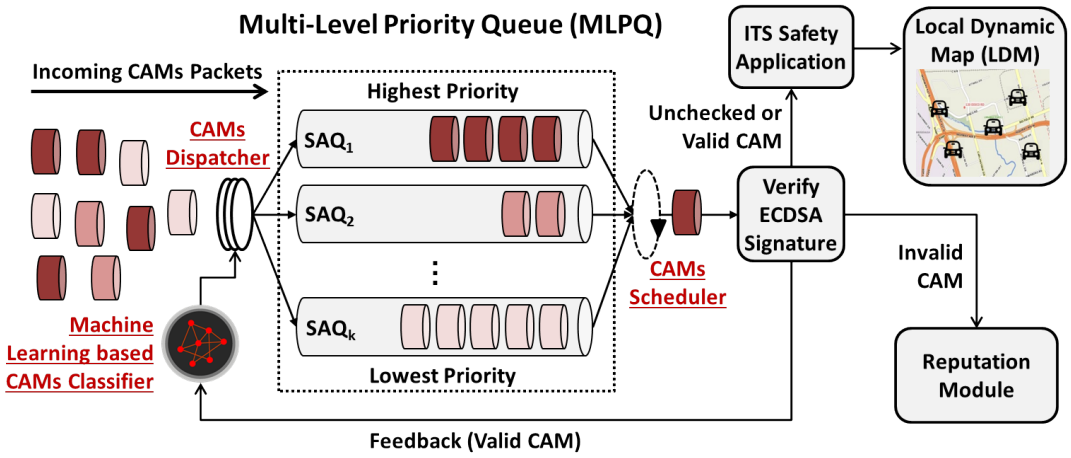


Fig. 6: Adapting Security and QoS in ITS by using k-means clustering and Safety Area Queues (SAQ).

density of 200 vehicles/km^2 to model a high density scenario and the CAM generation rate is set to 10 packets per second. The transmission range is taken as 500m and Nakagami fading is used to model propagation loss.

The packet inter-arrival time of CAMs is shown at different transmitter-receiver distances in Fig. 5. Without using security, the message inter-arrival time remains below 150ms within a Tx-Rx distance of 300m. Since CAMs are sent every 100ms, the increased inter-arrival time is the result of packet loss due to collisions and fading. The message inter-arrival time further increases if security signature is added to the packets. The ENCAP delay, DECAP delay and security overhead contribute to the increased packet inter-arrival times. Particularly, for Intel Xeon whose security processing time is approximately 3 times higher than Intel i7 results in a packet inter-arrival time of 321ms at a Tx-Rx distance of 300m. In comparison, Intel i7 maintains a packet inter-arrival time of less than 170ms within this distance.

Since safety messages in ITS are transmitted at a maximum rate of 10 packets per second, a high density scenario results in vehicles receiving hundreds (or thousand) of packets for security processing [11]. While a powerful processor in the vehicle reduces the security processing time resulting in reduced packet latency, it will increase the cost of on board unit in the vehicle. For instance, for some hardware security modules (HSM), the cost is even more than the cost of an entry-level car. Therefore, vehicles require a cheaper processor that can provide relatively acceptable security processing times. Additionally, to achieve the security-QoS balance, adaptive security techniques and congestion control mechanisms should be developed.

V. Adaptive Security in ITS

To achieve the required QoS for ITS applications without compromising security, adaptive mechanisms are required. Specifically for safety applications, messages are signed using ECDSA algorithm before transmission. At the receiver, these messages are placed in a security queue and verified on a first-come, fist-served basis. In high traffic density scenarios, vehicles could receive more packets than they can verify, causing high latency and packet losses due to timeout (taken as 100ms) also known as cryptographic packet loss.

A. Machine Learning Based Adaptive Signature Verification in ITS

To overcome the problem of cryptographic packet loss, an adaptive machine learning based signature verification technique for safety ITS applications can be utilized as proposed in our previous work [6]. The central idea of the adaptive technique is to assign verification priority to the packets from nearby vehicles that are a source of greater safety danger. On the other hand, verification of messages from vehicles farther away could be delayed or discarded without impacting safety.

Since the transmitting vehicle's position cannot be evaluated before the safety message is authenticated, transmitter-receiver distance is unknown. As a solution to this challenge, received signal strength can be used [12]. Experimental studies have shown a correlation between received signal strength and transmitter-receiver distance [6]. Vehicles can classify the geographical region around them into several safety areas (SA). Using the received signal strength, safety messages can be mapped to their corresponding SAs. As vehicles change their position, neighboring vehicles in the SAs change, however this mapping function remains the same. Another advantage of using received signal strength to find vehicle position is that malicious users can not launch location spoofing attack.

This mapping can be further improved by the CAM classifier module that utilizes the k-means clustering algorithm and a feedback of valid CAMs that have been verified correctly at the receiver as shown in Fig. 6. Based on a set of valid CAM observations $(c_1, c_2, ..., c_n)$, where each observation is a one-dimensional vector which contains the CAM received signal strength $(P_m, \forall m, 1 \leq m \leq n)$, k-means clustering aims to partition the n CAM 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 (i.e., least-squares estimator)

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

where μ_l is the mean of points in SA_l (i.e., mean received signal strength). Vehicles compute accurate received signal strength to safety area mapping after a training phase of few iterations. The safety messages are further dispatched to a Multi-Level Priority Queue (MLPQ) in order to optimize their verification as depicted in Fig. 6. Each message is placed in the corresponding safety area queue (SAQ) to assign priority. Every time a new packet is to be verified, the first packet in the highest safety area queue is extracted. As a result, messages originating from closer vehicles are verified first and latency for critical packets is improved.

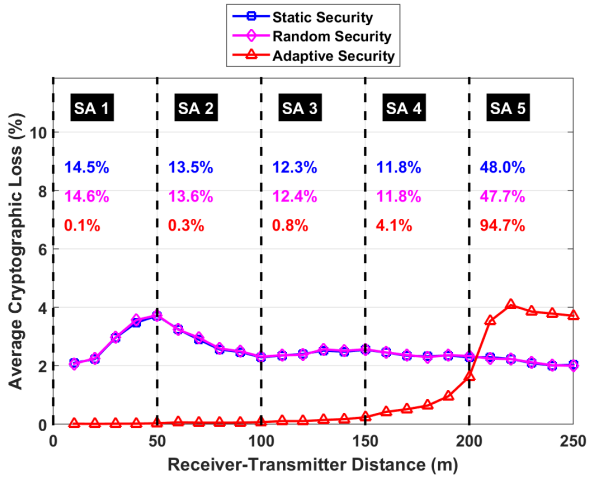


Fig. 7: Average Cryptographic Packet Loss (95% confidence interval).

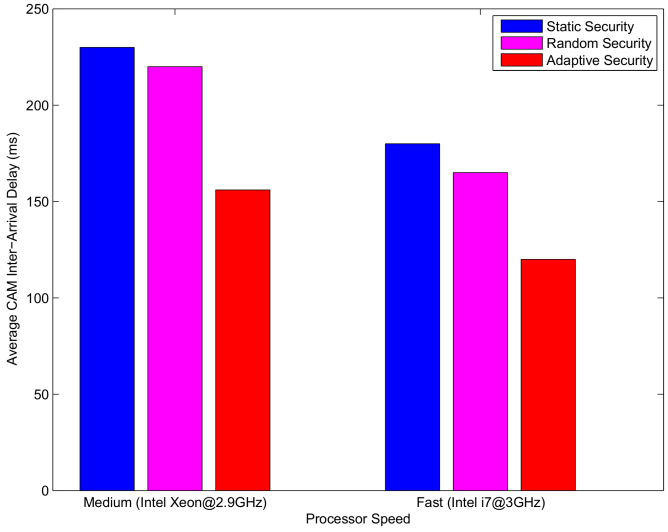


Fig. 8: Average CAM Inter-arrival Delay.

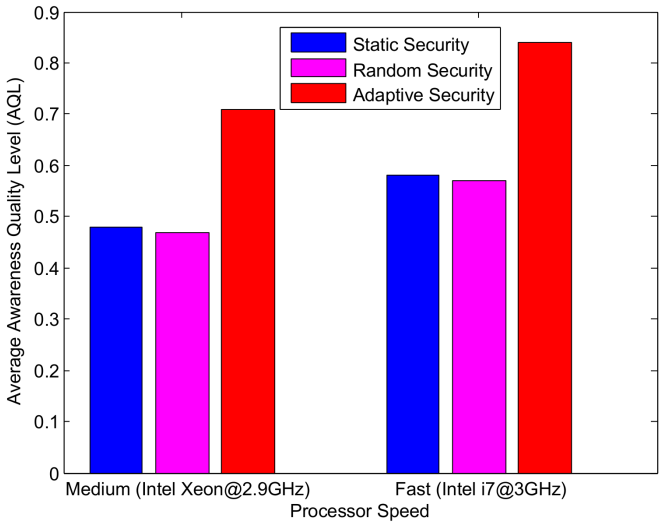


Fig. 9: Awareness Quality Level.

B. Performance Improvement

The simulation configuration used for our evaluation experiments is described in Sec. IV-B. We display the average cryptographic packet loss (CPL), percentage of packets which could not be verified within 100ms, at different transmitter-receiver distances in Fig. 7. The five selected SAs are marked as $50m$, $100m$, $150m$, $200m$, and $> 200m$. The adaptive security technique is compared against two mechanisms, namely a static security mechanism that verifies packets without any priority and a random security mechanism that randomly picks a packet out of the security queue for verification. The marked numbers in the figure indicate the total CPL within a safety area. Since fresh messages are sent every 100ms, the packets which could not get verified within this time are dropped from the security queue due to timeout (i.e., slow security verification).

Both static and random security techniques result in large CPL for closer safety areas. The peak in CPL at $40 - 50$m distance bins indicates the highest number of packets received from this region, hence resulting in more CPL. However, the adaptive security mechanism verifies the packets from nearby vehicles with priority, hence reducing the CPL. Particularly, within a distance of 150m, this loss is below 1% for the adaptive mechanism compared to $12 - 14\%$ for the other techniques. Beyond this distance, the CPL for the adaptive technique is increased, which however does not effect the safety application.

Fig. 8 illustrate the average inter-arrival delay between two consecutive CAMs (within a safety area of 150m) using different processor speeds. As expected, the adaptive security mechanism results in a significant improvement of around $70 - 80$ms in inter-arrival delay when compared to both the static and random security techniques. Through prioritized verification of packets from nearby vehicles, the adaptive mechanism results in a quicker update of the mobility information about neighboring vehicles as received in the CAMs.

It can also be noted that a fast processor (Intel i7) results in a significant reduction of CAM inter-arrival delay. This

is because a faster processor can perform more DECAP operations per seconds as shown in Fig. 4. Another key point here is that the adaptive security technique enables vehicles to use cheaper CPUs with lower clock rates. For example, in this case, the adaptive security can provide $10-15$ms lower inter-arrival delay even with a mid range processor as compared to static and random security techniques with a fast processor.

Finally, we show the awareness quality level (AQL) metric (within a safety area of 150m) as proposed by the authors in [13]. The AQL metric provides a measure of how many of the actual neighbors of a vehicle are aware of it at any given time. As shown in Fig. 9, the adaptive security mechanism improves the AQL metric by $22-24\%$ within 150m when compared to the static and random security techniques. By using a fast processor, the adaptive security mechanism provides a AQL of greater than 84%. The remaining loss is due to packet collisions in the considered high density scenario and multi-path fading. Nonetheless, the adaptive security technique maintains a much better level of awareness for vehicles within the vicinity. Note that in this paper, we do not consider memory size of OBU transceiver that can limit the number of CAMs that can be stored in the security queue.

VI. Opportunities and Challenges

Maintaining security and satisfying QoS requirements are essential to achieve the task of reliable communications in ITS. The following are some of the opportunities and challenges in this domain.

A. Cryptographic Hardware Accelerators

To minimize the impact of security on the application's QoS and achieve an important speedup in handling secure ITS communications, one way is to delegate all the cryptographic operations to dedicated Hardware Security Modules (HSM) or Trusted Platform Modules. Vehicles OBUs should be equipped with such hardware modules, as security co-processors. As shown in Fig. 4, the usage of higher CPU frequencies can enable the handling of a higher number of cryptographic operations, such as ECDSA signature verifications. Even though this scheme can achieve security and QoS gains, the additional cost of a separate HSM could be costly. An important challenge is to design a cryptographic hardware module with a special focus on ITS applications. Such a module should provide implementation of light weight cryptographic algorithms suited for ITS applications and available at an affordable price.

B. Adaptive Security-QoS Schemas

Existing ITS standards have a static selection of the security schemas which are based on expensive cryptographic operations and are uncapable of handling a large amount of messages, without impacting the systems critical latency. As already shown in this article, adaptive security algorithms can significantly enhance the application's QoS. Moreover, adapting the security schemas and algorithms based on context changes (e.g. wireless channel conditions, available resources, etc.) can improve the scalability of ITS systems, but at the cost of lower security levels.

A joint security-QoS adaptation mechanism can assist ITS applications to maintain their QoS while ensuring security of data exchanges. Vehicles can continuously monitor their QoS indicators and adjust their security in terms of key management, key lengths, algorithm types and security levels accordingly. Moreover, vehicles can also adapt and optimize their priority mechanism depending on the type of application. For example, for non-safety applications, priority could be assigned based on application criticality instead of receiver-transmitter distance. Vehicles could also use dynamic adaptation of safety areas according to application requirements.

In addition, decentralized congestion control mechanisms as defined in the ETSI standard can also be used to adaptively adjust transmission parameters according to traffic densities on the roads [14]. For example, in a high density scenario, ITS applications could reduce the packet generation rate or transmit power in order to accommodate security overheads. Dynamic optimization of the networking services, in terms of optimal service differentiation schemes, access categories and priorities can also help maintain security-QoS balance in ITS. In summary, an intelligent security-QoS framework is required to combine the various techniques to adjust security and QoS according to application's needs.

C. Social Network based reputation

In ITS, vehicles interact with their neighboring vehicles and infrastructure to form a transportation social network. Moreover, other entities in ITS such as pedestrians, passengers, etc. exhibit social affiliations and exchange data with their social peers [15]. In fact, a reputation system can be deployed on ITS entities to select security levels based on the social interactions and reputation of the nodes. For example, nodes with high centrality and strong ties are less prone to be malicious.

VII. Conclusion

In this article, we highlight the relationship between security and QoS for ITS applications. We present the generic communications model of ITS and discuss the major design challenges related to security and QoS. We benchmark the security processing times required for standard-compliant security procedures and analyze the QoS of secured ITS safety applications. To improve the safety application's QoS while keeping the security intact, we discuss a machine learning based adaptive signature verification scheme. Finally, we discuss some of the future opportunities on how dynamic adaptation of security and QoS can benefit ITS.

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] "The wall street journal [online]," http://www.wsj.com/articles/obama-administration-proposes-spending-4-billion-on-driverless-car-guidelines-1452798787, accessed: 2016-02-28.

[2] J. Fuentes, A. Gonzlez-Tablas, and Ribagorda, *Handbook of Research on Mobility and Computing*. IGI Global, 2010, ch. Overview of security issues in Vehicular Ad-hoc Networks.

[3] M. A. Javed, E. B. Hamida, and W. Znaidi, "Security in intelligent transport systems for smart cities: From theory to practice." *Sensors*, vol. 16, no. 6, p. 879, July 2016.

[4] The Institute of Electrical and Electronics Engineers, "IEEE Std 1609.2-2016, IEEE standard for wireless access in vehicular environments (WAVE) - Security services for applications and management messages," Tech. Rep., 2016.

[5] The European Telecommunications Standards Institute, "ETSI TS 103 097 v1.2.1 (2015-06) - Intelligent transport systems (ITS) - security; security header and certificate formats," Tech. Rep., 2015.

[6] 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*, 2016, pp. 1–8.

[7] C. H. Wang, C. T. Chou, P. Lin, and M. Guizani, "Performance evaluation of ieee 802.15.4 nonbeacon-enabled mode for internet of vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 6, pp. 3150–3159, Dec 2015.

[8] The European Telecommunications Standards Institute, "ETSI TS 102 637-1 v1.1.1 - Intelligent transport systems (ITS) - Vehicular communications - Basic set of applications - Part1: Functional requirements," Tech. Rep., 2010.

[9] F. Qu, Z. Wu, F. Wang, and W. Cho, "A security and privacy review of VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 6, pp. 2985–2996, Dec 2015.

[10] "Safeits project: ETSI ITS security performance benchmark [online]," http://safeits.org/bench, accessed: 2016-04-17.

[11] T. Darwish and K. A. Bakar, "Traffic density estimation in vehicular ad hoc networks: A review," *Ad Hoc Networks*, vol. 24, Part A, pp. 337 – 351, 2015.

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

[13] 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.

[14] M. Sepulcre, J. Gozalvez, O. Altintas, and H. Kremo, "Integration of congestion and awareness control in vehicular networks," *Ad Hoc Networks*, vol. 37, Part 1, pp. 29 – 43, 2016, special Issue on Advances in Vehicular Networks.

[15] Q. Yang and H. Wang, "Toward trustworthy vehicular social networks," *IEEE Communications Magazine*, vol. 53, no. 8, pp. 42–47, August 2015.