Adaptable Safety and Security in V2X Systems

Miguel Villarreal-Vasquez, Bharat Bhargava
Department of Computer Science
Purdue University
West Lafayette, IN, USA
{*mvillar, bbshail*}*@purdue.edu*

Pelin Angin
Department of Computer Engineering
Middle East Technical University
Ankara, Turkey
pangin@ceng.metu.edu.tr

***Abstract*—With the advances in the areas of mobile computing and wireless communications, V2X systems have become a promising technology enabling deployment of applications providing road safety, traffic efficiency and infotainment. Due to their increasing popularity, V2X networks have become a major target for attackers, making them vulnerable to security threats and network conditions, and thus affecting the safety of passengers, vehicles and roads. Existing research in V2X does not effectively address the safety, security and performance limitation threats to connected vehicles, as a result of considering these aspects separately instead of jointly. In this work, we focus on the analysis of the tradeoffs between safety, security and performance of V2X systems and propose a dynamic adaptability approach considering all three aspects jointly based on application needs and context to achieve maximum safety on the roads using an Internet of vehicles. Experiments with a simple V2V highway scenario demonstrate that an adaptive safety/security approach is essential and V2X systems have great potential for providing low reaction times.**

***Keywords*-V2X systems; safety; security; authentication; adaptability**

I. Introduction

Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) networks, collectively known as V2X systems or Internet of vehicles have been receiving increasing attention because of their significant contributions to improving the safety of vehicles, and consequently drivers, in a world of ever increasing casualties due to traffic accidents. Due to this growing popularity, V2X networks are hot targets for attackers, who try to exploit the software vulnerabilities of these systems and compromise the security, privacy and most importantly the safety of vehicles and users. Hence, in order to function safely, a V2X system needs security and communication infrastructures to enable and ensure the trustworthiness of communication between vehicles and road side units (RSUs). The source of each message needs to be trusted and message content needs to be protected from outside interference. In order to create the required environment of trust, a V2X system must include a security infrastructure to authenticate each message, as well as a communication network to relay security credentials and related information from vehicles to the entities providing system security (and vice versa).

Most previous research on VANETs [1], [2], [3], [4], [5], [6], [7], [8], [9] have mainly focused on the development of the MAC layer, infotainment and collision avoidance applications, and the analysis of security mechanisms that might be applied to protect the network. Few works [10], [11], [12] have been directed to address the implementation of security mechanisms in VANETs and evaluate the impact of the different security mechanisms on the safety of drivers. The main issues with existing approaches for V2X safety and security are as follows:

- The safety, security and performance issues are generally considered separately for V2X systems, and are evaluated independently. Nevertheless, these issues are strongly related and they significantly affect the critical latency of V2X systems. If they are not all considered together, they will cause obstacles for the adoption of V2X systems at large.
- Existing V2X networking services have critical shortcomings, which cause unacceptable performance under high traffic scenarios [13] and cause time-critical safety applications to exceed maximum acceptable delays [14]. This hurts the effectiveness of time-critical safety applications for V2X.
- Existing V2X research is either based on unrealistic simulation studies as in [15], [16], or on basic experimental deployments, where the security solutions are either evaluated independently from the other layers (e.g. Network, MAC, PHY, etc.) [17], or under limited operating conditions ([18], [19]).
- Existing studies qualitatively model the relationships between safety and security mechanisms. For instance, they consider the worst case behavior in analyzing the cross-interference of the mechanisms on the security and safety of the system. For effective safety, the relationships between the safety, security and performance issues should be modeled quantitatively.
- Existing V2X systems have a static selection of the security, networking and safety features. For maximum effectiveness, V2X systems should be able to adapt the security, performance and safety features at runtime based on the user/application needs and context.

In order to address the shortcomings of previous work, we propose a systematic approach to figure out how V2X technologies increase safety, and how much the use of secure communication in V2X negatively affects it. The ultimate goal of this study is to find the optimally secure solution for V2X technologies. Since all V2X messages do not have the same level of sensitivity to security and privacy, and different security policies incur different overhead (generally, high overhead for stronger security policies and vice versa), we propose an adaptive security model for V2X networks that changes the configuration parameters of the secure channel dynamically based on the sensitivity of the V2X messages, safety level of vehicles, and also the current network context.

In this work we concentrate on an empirical analysis of the safety level and the tradeoffs between security and safety in V2X systems, which is required for developing adaptive security mechanisms. Specifically we regard reaction time as our measure of safety and study it considering non-V2V, V2V and secured V2V solutions on a 2-vehicle scenario. We observe that the incorporation of V2V into vehicle systems significantly reduces the reaction time of the vehicle. With the addition of security mechanisms to guarantee message authentication, a significant communication overhead is observed, but still the obtained reaction times are better than the case when V2V is not considered at all.

The rest of this paper is organized as follows: Section II provides an overview of previous/existing V2X projects and safety/security approaches for V2X. Section III gives some preliminary concepts crucial to understanding the conducted analysis. Section IV discusses the V2X system model considered. Section V discusses the proposed adaptable safety/security approach. Section VI provides the results of preliminary safety evaluation experiments and section VII concludes the paper.

II. Related Work

Design and development of V2X systems has been the focus of many research projects. PRECIOSA [20] analyzed privacy issues in cooperative vehicular and road safety systems, and proposed a privacy-aware architecture for V2X communications. EVITA [21] proposed a secure in-vehicle communication architecture mitigating tampering attacks and protecting sensitive data inside the vehicle. SEVECOM [22] proposed a security architecture for vehicular communications systems, including privacy, identity management and data consistency. OVERSEE [23] realized an open in-vehicle platform for developing secure V2X applications, providing high isolation between independent applications. IntelliDrive [24] designed new security mechanisms for V2X communications, which were evaluated with real deployments. SafeSpot [25] designed dynamic and cooperative ad-hoc networking and localization mechanisms for V2X communications.

Besides completed projects, there are more recent projects that were launched to advance research in the field. SESAMO [26] aims to model the relations between functional safety and security mechanisms in embedded systems in multiple domains. PRESERVE [27] aims to design, develop and evaluate secure and scalable V2X communication systems in realistic scenarios. COMeSafety2 [28] aims to facilitate the development and deployment of cooperative safety applications and to promote their benefits towards real-world users. CopITS [29] focuses on the development of advanced communication protocols and networking services to enhance the data transfer over V2X links, and evaluation of these using an ETSI ITS standard [30] compliant platform and real deployment scenarios. CellCar [31] proposes new strategies for combining IEEE 802.11p with LTE to improve the network performance and enable delay-tolerant services.

V2X security has been the focus of many research projects in the past decade, as the security challenges were observed to be a significant barrier to the widespread use of V2X. The proposed solutions concentrate on the following aspects of security [32]:

- Identity and liability: Ability to prove that a specific vehicle or driver is responsible for a specific event by binding the entity to that event.
- Devices: Making sure that on-board units (OBUs) and electronic control units (ECUs) of vehicles are not tampered with by attackers.
- Communication links: Protecting the confidentiality, integrity and authenticity of within-vehicle (between ECUs) messages as well as messages exchanged with other vehicles, remote services and external devices.

Safety and security used to be considered as adjunct to the system design ([33], [34]) in the past. This assumption was challenged by Bloomfield et al., who argued that a system is not safe if it is not secure [34]. Most of the existing V2X security solutions ([35], [32]) are known for their high computation and delay overheads. The experimental evaluation and benchmarking of these security solutions [18] have been conducted under limited operating conditions, and their impact on the critical latencies of V2X systems needs further study. The investigation of self-protecting software is a recent [36] contribution to the field of security, and needs to be explored further for its utility in V2X systems.

III. Preliminaries

A. Categories of Safety Messages

As it has been indicated in [11], safety messages can be divided into three main categories.

- The first category, traffic information messages, is used to disseminate the current conditions of specific areas and they indirectly affect safety.
- The second category is general safety messages, which are used for cooperative driving and collision avoid-

ance, and require an upper bound on the delivery delay of messages.
- The third category refers to liability-related messages, which are exchanged after an accident occurs.

Some of these categories listed above are time-critical while others are not. This difference is crucial in our analysis since we are particularly interested in time-critical messages only. Our interest is measuring how much safety is improved by V2X infrastructures and evaluating how this improvement is affected as security mechanisms are applied to secure the communication among vehicles. This study will be limited to general safety messages.

B. Semantics of Safety Messages

The semantics of general safety messages changes according to the situation and the type of road where vehicles are driven. It is not unusual that the same vehicle can be driven in rural areas, streets in populated areas, highways and through traffic lights. For each of these scenarios the semantics of messages varies, as well as the safety requirements. Our interest is studying the tradeoffs between safety and security in all of them and proposing the best security algorithms in each to increase safety. Here we focus on an analysis of the highway scenario.

C. Scope of Analysis

The scope of the analysis here involves two vehicles moving in the same direction at a constant speed and separated by a constant distance. The vehicle in the front is assumed to suddenly stop and send a message to the vehicle behind. The semantics of the message in our experiment is assumed to be "stop right away". As specified in [37], the stopping distance for vehicles is determined by four factors: (1) driver perception time, (2) driver reaction time, (3) vehicle reaction time and (4) vehicle breaking capability. In our scenario V2V allows the removal of the first two factors since it eliminates the need for drivers to make the decision of pushing the brake pedal. At the moment the vehicle receives and processes the message, the vehicle is assumed to brake automatically. The distance the vehicle moves forward from the moment the brake is pushed until it completely stops is known as braking distance. The braking distance is not of our interest because it mainly depends on weather conditions and vehicle capabilities, but not on V2V communication delays. Our interest is limited to the reaction time.

Our results in section VI show that the distance a vehicle moves forward due to reaction time with and without V2V are significantly different. V2V allows faster reaction time, which implies a smaller distance since the moment the car in the front stops and generates the safety message. V2V messages with authentication information increase the reaction time, but it remains negligible compared to the estimated reaction time of drivers of vehicles without V2V.

IV. System Model

In this section we formally present the scenario and assumptions in our analysis. Figure 1 shows the scenario we study.

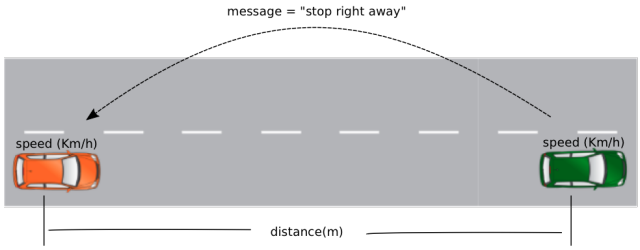

Figure 1: Highway scenario.

From this point on we will refer to the vehicle in the front (green vehicle) as car A and the vehicle in the back (orange vehicle) as car B. The scenario describes the situation when car A suddenly stops and car B reacts based on that. Our main assumption in this scenario is that when V2V is available, car A suddenly stops and sends a stop right away message to car B. Car B will process the received message and automatically react based on the instruction received from car A.

A. Stopping Distance

Many drivers have a false belief that if the car in the front starts braking, they can react, brake and come to a stop, still leaving the same distance between the two vehicles. The total minimum stopping distance of vehicles actually depends on four factors [2]:

- Driver's perception time: It is the time it takes for a driver to see a hazard and realize he/she needs to take an immediate action.
- Driver's reaction time: It is the time it takes for a driver to push the brake pedal after realizing the imminent hazard.
- Vehicle's reaction time: At the moment the brake pedal is pushed, it will take a certain amount of time for the vehicle to react and start stopping. This depends on the conditions of the vehicle and in particular the condition of the brake system.
- Vehicle's braking capability: This factor is different from the previous one because it is affected by elements other than the braking system. In general, this factor depends, for example, on tire pressure, weight of the vehicle, vehicle suspension system and road surface.

The last two determine the distance braking, which is the distance a vehicle moves forward once the brake pedal has been applied [37]. As described above, these factors do not depend on the driver's reaction. Instead they depend on the conditions of the vehicle and environment. Therefore the use of V2V does not affect them at all.

On the other hand, the first two factors completely depend on the driver. They vary depending on the driver and external elements such as the use of alcohol and drugs while driving, tiredness, fatigue and lack of concentration. Obviously, V2V has a direct impact on these factors since it allows vehicles to make smart decisions regardless of the condition of the driver. The scope of this work will be focused on analyzing the decrease in the reaction time achieved with V2V without the overhead of security mechanisms and with V2V when the communication channel between vehicles is secured.

The experiments section will be dedicated to analyzing the results obtained with V2V (with and without security mechanisms), and comparing them with the results published by RSA (Road Safety Authority) [37], as shown in Table I.

Table I: Minimum reaction/braking/stopping distances advised by Road Safety Authority [37]

Speed (Km/h)	Minimum Reaction Distance (m)	Minimum Braking Distance (m)	Minimum Stopping Distance (m)
30	6	6	12
40	8	10	18
50	10	15	25
60	12	21	33
80	16	36	52
100	20	50	70
120	24	78	102

B. Network Model

There are many wireless technologies available for V2V. We assume our communication channel is compliant with IEEE 802.11p. The vehicles will move in the same direction at the same speed, allowing us to assume a constant distance between them.

For the time being, we ignore the effects of any other vehicles on the road. IEEE 802.11p offers a bandwidth of 6Mbps, 9Mbps, 12Mbps, 18Mbps, 24Mbps, 36Mbps, 48Mbps and 54Mbps. We will assume the smallest one, 6Mbps, in our empirical evaluation.

C. Security Mechanisms in V2X

In a V2X network, where safety is the highest priority, we are more concerned about the authenticity and integrity of the received messages than the privacy of the message itself. Because of that, in this work we only explore the overhead caused by authentication mechanisms on V2V. As part of future work, we will investigate the overhead of encryption so that we can guarantee the confidentiality of the interchanged messages.

In our experiments we assume a PKI infrastructure as suggested in [11], where each vehicle has been assigned a public and private key. Each vehicle, with security enabled, sends messages of the following form:

$$M_{AUTH} = < (M|T),\ Sign(M|T),\ Cert_{CASIGNED} >$$

Here, M is the message in plaintext, T is a timestamp (to prevent the reception of obsolete messages), and $|$ represents concatenation. *Sign(M|T)* is the signature of the message concatenated to the timestamp. The sender vehicle signs the message with its private key. *Sign(M|T)* is a certificate signed by the Certificate Authority (CA) that contains the ID and public key of the sender vehicle. The receiver vehicle is assumed to have the CA Root Certificate it can use to extract the ID and public key of the sender to verify the received signature.

D. Security Costs in V2X

The addition of authentication imposes some overhead and causes an extra delay in the communication among vehicles. There are two main costs we are interested in:

- Processing cost: The generation and verification of signatures seems to have a constant delay independent of the size of the message to be signed. In our experiments we used ECDSA as our public key cryptosystem. A summary of the processing cost from [11] is presented in Table II.

Table II: Signature generation and verification times

Public Key Cryptosystem	Generation (ms)	Verification (ms)
ECDSA	3.255	7.617

- Communication cost: The communication cost (delay) is given by the following formula:

$$d_{com} = d_{transmission} + d_{propagation} + d_{queueing}$$

We assume a queuing delay of zero here, since the communication involves only two vehicles. The transmission delay and propagation delay are given by L/R and d/s respectively, where L is the length of the message, R the transmission rate or bandwidth (assumed 6Mbps), d the distance between the two vehicles, and s the speed of the communication link (assumed 3 x 10^8 m/s).

E. Tradeoffs Between Security and Safety

This work aims to evaluate how much V2V infrastructures improve the reaction time in the scenario described above. Without V2V, drivers are responsible for making decisions, as they perceive hazards on the road. Sometimes the reaction time of drivers is too long, which puts their safety at risk. The incorporation of V2V technologies into vehicles aims to increase the safety of drivers, as vehicles are able to make faster decisions based on information received from either road infrastructures or other vehicles. Understanding how the reaction in vehicles differs in these two cases (with and without V2V) is one of the goals of this study.

A second goal of the study is analyzing the impact that authentication mechanisms in V2X have over the safety of drivers. As V2V enables communication among vehicles on the road, there is an imminent risk if no security mechanisms are applied. In order to guarantee safety, at least integrity and authenticity in the exchanged information is required. However, the interdependency of security mechanisms and the extra overhead impacts the performance of V2V networks, incurring larger delays in the communication, which in turn increase the reaction time of the vehicles.

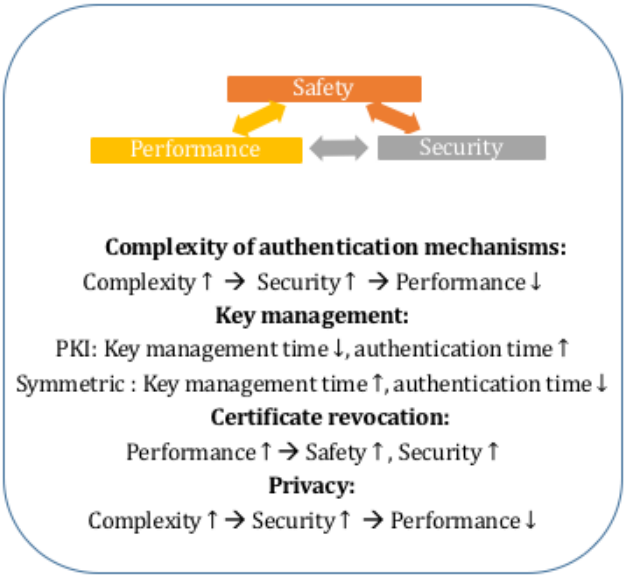

Figure 2: Safety/Security/Performance Tradeoffs in V2X.

Figure 2 shows a summary of the main tradeoffs between safety/security/performance of V2X systems.

V. Adaptable Safety/Security Approach

Self-adaptive software solutions are capable of adjusting their behavior at runtime to achieve certain functional or quality of service goals. A common approach to achieve self-adaptation is the architecture-based approach, which was proposed by Yan et al. [38] for self-protecting software that are capable of detecting security threats and mitigating them through runtime adaptation techniques. Esfahani et al. [39] developed a framework that implements the approach. In this work, we consider safety and performance requirements besides the security aspect. The architecture-based adaptation approach that we consider needs to enforce the safety and performance requirements besides the security requirements and consider the relationships between the requirements of the three aspects, i.e. safety, security, and performance.

Figure 3 provides an overview of the proposed adaptive safety approach for V2X. The model involves three measurement units integrated into the V2V-enabled vehicle. These units measure the sensitivity of the messages to be

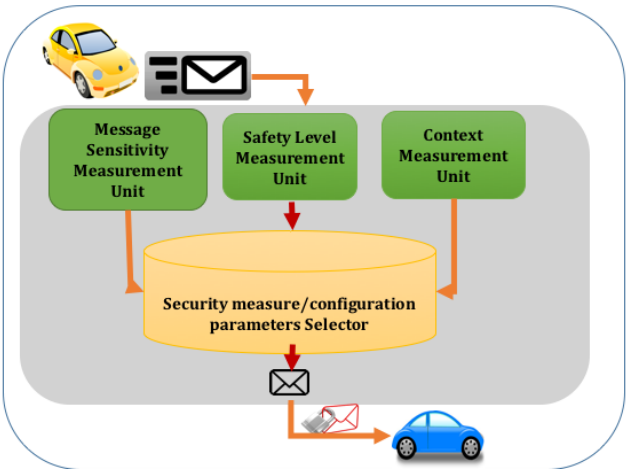

Figure 3: Adaptive Safety Model Overview.

sent, the current safety level of the vehicle and contextual parameters such as road conditions, V2V network conditions etc. The measurements are processed by security measure/-configuration parameters selector to choose the appropriate dissemination mechanism for the message to be sent to the other vehicles and infrastructure. Here, the goal is to provide an adaptive security-aware V2X framework, which is an extension of the one proposed in [39], continuously monitoring its surrounding environment in real-time and adapting the security and performance, while enforcing the safety of the V2X system. The framework monitors behavior and collects performance metrics that are used to detect emerging behaviors, impact of the adaptation on the system using machine learning techniques and updates the knowledge base to detect violations of the software goals/requirements, and plans the adaptation to optimize the goals, adapting the system at runtime according to the plan.

Software adaptation relies on monitoring the behavior of software. However, monitors can interfere with V2X systems, because they would share the same resources. Therefore, we need to isolate the monitoring activity from V2X. We previously proposed the use of Aspect Oriented Programming (AOP) [40] to monitor Web services and identify violation of Service Level Agreements (SLA). This approach enables triggering of actions when specific conditions are met. The same approach can be utilized to monitor the behavior of V2X software. Typical examples of performance metrics that could be monitored in real-time are: the number of outgoing/incoming packets per second, the signature generations/verifications per second, the packet delays, the transmission delays, the message encryption/decryption delays, the number of neighboring vehicles and/or RSUs, the received signal strength indicator of packets, the quality of radio links etc. Based on the monitoring results and inferences on the tradeoffs between safety/security/performance based on a quantitative model,

the behavior of the V2X system will be adapted. A typical example of this adaptation is using more lightweight cryptosystems even if they provide less advanced security features in the case of an emergency, where processing time for messages is critical.

VI. Experiments

Experiments were conducted using ECDSA as the public key cryptosystem. The processing time required to generate and verify signatures using ECDSA were taken from [11] and are shown in Table II. Delays for messages sent in the experiments were empirically obtained according to the setup of parameters. The details of each measurement are presented in the following subsections.

A. Measurement of delays of V2V messages with and without security

This experiment was conducted to measure the delay of the messages sent from car A to car B. In order to measure the relation between delay and length of a message, messages of different sizes were sent with and without security mechanisms. The input parameters for this experiment were as follows:

- Speed of vehicles: 120 Km/h
- Distance between vehicles: 120 m

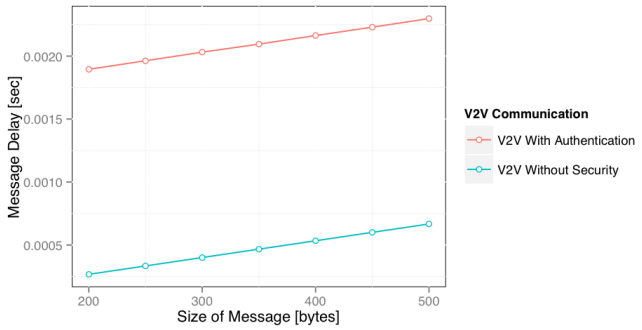

Figure 4: Measurement of message delay as a function of message length.

The size of messages without security is our independent variable, while the delay of the corresponding message with and without authentication mechanism is our dependent variable. As expected, the delay linearly increases with the size of the message. This is because the size of the signature does not change significantly with the size of the message and certificates were of fixed size as well. The size of signatures varies from 102 to 104 bytes, while the size of the certificate was of 1111 bytes.

The distance between vehicles was set to 120m because part of our experiments requires estimating the *reaction time distance* of cars moving at 120Km/h and this distance is slightly larger than the distance among cars at this speed recommended by the RSA (Road Safety Authority) [37]. This distance also gives us the worst scenario since the delay increases as the distance does.

B. Measurement of the capacity of the link

The second experiment was conducted to measure the number of messages that car A can send to car B with and without security enabled assuming a link bandwidth of 6Mbps. The input parameters for this experiment were as follows:

- Speed of vehicles: 120 Km/h
- Distance between vehicles: 120 m

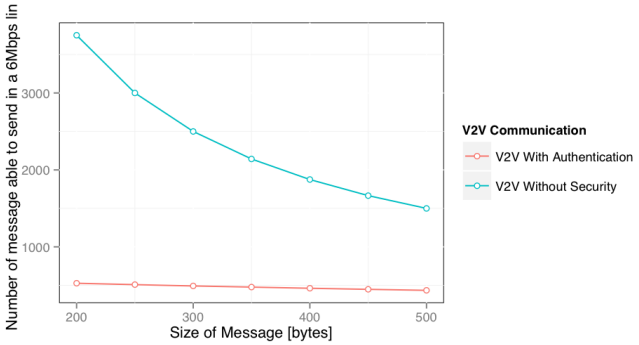

Figure 5: Number of messages able to be sent on 6Mbps link.

The size of messages without security is our independent variable, while the number of messages able to be sent with and without authentication mechanism is our dependent variable.

As we can see, the number of messages that can be transmitted remains below 500 when authentication mechanisms are enabled. This implies that under a more realistic scenario with more vehicles involved, there could be lost messages if more than 500 are sent simultaneously to the same vehicle.

C. Reaction time with V2V enabled

This experiment was conducted to measure the *reaction time distance* that car B moves from the moment car A stops and starts generating the safety message. This requires obtaining the total delay (communication and processing delay) it takes for car B to interpret the received message to calculate the distance car B moves. The input parameters for this experiment were as follows:

- Size of messages without authentication overhead: 200 bytes
- Distance between vehicles: 120 m

It can be stated that the difference is relatively significant, but still too small in both cases when compared to the values given in Table 1.

These results show that V2V significantly reduces the reaction time when it is compared to vehicles that operate

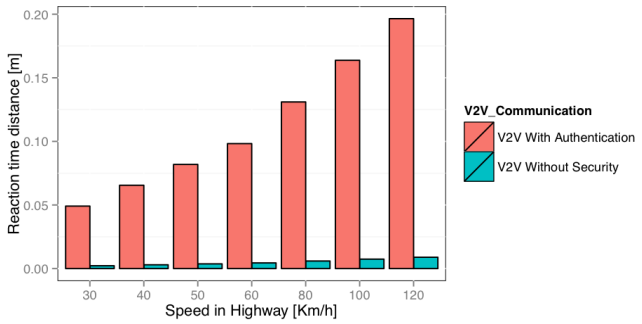

Figure 6: Number of messages able to be sent on 6Mbps link.

without V2V. This is a promising result since we are interested in evaluating a more realistic scenario with more vehicles involved and the huge difference among these two results (with and without V2V secured or not) indicates that the addition of more vehicles might not affect the V2V performance to the point that it would become less efficient than a system without V2V.

VII. Conclusion

In this work we have explained the reasons for which V2X networks strictly require integrity and authentication and not confidentiality. We proposed a dynamic adaptability approach considering the aspects of safety/security/performance jointly based on application needs and context to achieve maximum safety on the roads using an Internet of vehicles. We assumed a PKI infrastructure and ran experiments that allow us to observe how V2V improves the safety of drivers. Specifically, we concentrated on the scenario of two vehicles driven on a highway at the same speed separated by a constant distance. We presented a table containing the Road Safety Authority (RSA) estimated reaction time for drivers in vehicles without V2V and compared it with V2V-enabled vehicles in two configurations: (1) V2V without any security mechanism, and (2) V2V with authentication mechanisms. We found that V2V, in any of its two configurations, allows a significant reduction in the reaction time.

The results obtained in this work are promising, since they show that the reaction time achieved via V2V (with or without security) is significantly smaller than a system without V2V. In future work, we will focus on the development of the proposed adaptability framework integrating a quantitative model of tradeoffs between the safety/security/performance aspects, as well as an extended evaluation with different scenarios and conditions.

Acknowledgment

This publication 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. The authors would also like to thank Dr. Weichao Wang and Dr. Leszek Lilien for their valuable comments and discussions.

References

[1] P. Tyagi and D. Dembla, "A taxonomy of security attacks and issues in vehicular ad-hoc networks (vanets)," *International Journal of Computer Applications*, vol. 91, no. 7, pp. 22–29, 2014.

[2] S. Zeadally, R. Hunt, Y. Chen, and A. Hassan, "Vehicular ad hoc networks (vanets): status, results and challenges," *Telecommunication Systems*, vol. 50, no. 4, pp. 217–241, 2012.

[3] C. Smith, *Car Hacker's Manual*. Theia Labs, 2014.

[4] J. Isaac, S. Zeadally, and J. Camara, "Security attacks and solutions for vehicular ad hoc networks," *IET Communications*, vol. 4, no. 7, pp. 894–903, 2010.

[5] P. Angin, B. Bhargava, R. Ranchal, N. Singh, M. Linderman, L. B. Othmane, and L. Lilien, "An entity-centric approach for privacy and identity management in cloud computing," in *Proceedings of the 29th IEEE Symposium on Reliable Distributed Systems (SRDS '10)*, 2010, pp. 177–183.

[6] C. Qu, D. A. Ulybyshev, B. K. Bhargava, R. Ranchal, and L. T. Lilien, "Secure dissemination of video data in vehicle-to-vehicle systems," in *Proceedings of the 34th IEEE Symposium on Reliable Distributed Systems (SRDS '15) Workshops*, 2015, pp. 47–51.

[7] C. Valasek and C. Miller", "Adventures in automotive networks and control units," http://www.ioactive.com/pdfs/IOActive_Adventures_in_Automotive_Networks_and_Control_Units.pdf, 2014.

[8] I. A. Soomro, H. Hasbullah, and J. bin Ab Manan, "User requirements model for vehicular ad hoc network applications," in *International Symposium on Information Technology (ITSim)*, 2010.

[9] R. K. Schmidt, T. Leinmller, E. Schoch, A. Held, and G. Schfer, "Vehicle behavior analysis to enhance security in vanets," in *in Proceedings of 4th Workshop on Vehicle to Vehicle Communications (V2VCOM 2008)*, 2008.

[10] X. Liu, Z. Fang, and L. Shi, "Securing vehicular ad hoc networks," in *2nd International Conference on Pervasive Computing and Applications*, 2007.

[11] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks," in *Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '05)*, 2005, pp. 11–21.

[12] C. Valasek and C. Miller", "A survey of remote automotive attack surfaces," http://www.ioactive.com/pdfs/IOActive_Remote_Attack_Surfaces.pdf, 2014.

[13] V. P. Harigovindan, A. V. Babu, and L. Jacob, "Ensuring fair access in ieee 802.11 p-based vehicle-to-infrastructure networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2012, no. 1, p. 168, 2012.

[14] R. Chen, D. Ma, and A. Regan, "Tari: meeting delay requirements in vanets with efficient authentication and revocation," in *2nd International Conference on Wireless Access in Vehicular Environments (WAVE)*, 2009.

[15] R. K. Schmidt, T. Köllmer, T. Leinmüller, B. Böddeker, and G. Schäfer, "Degradation of transmission range in vanets caused by interference," *PIK-Praxis der Informationsverarbeitung und Kommunikation*, vol. 32, no. 4, pp. 224–234, 2009.

[16] V. D. Khairnar and K. Kotecha, "Performance of vehicle-to-vehicle communication using ieee 802.11 p in vehicular ad-hoc network environment," *arXiv preprint arXiv:1304.3357*, 2013.

[17] M. Cazorla, K. Marquet, and M. Minier, "Survey and benchmark of lightweight block ciphers for wireless sensor networks," in *Security and Cryptography (SECRYPT), 2013 International Conference on*. IEEE, 2013, pp. 1–6.

[18] P. Demo, "Secure communication in vehicular networks," in *2012 IEEE Vehicular Networking Conference (VNC): Demo Summaries*, 2012, p. 11.

[19] R. K. Schmidt, B. Kloiber, F. Schüttler, and T. Strang, "Degradation of communication range in vanets caused by interference 2.0-real-world experiment," in *International Workshop on Communication Technologies for Vehicles*. Springer, 2011, pp. 176–188.

[20] "Privacy enabled capability in co-operative systems and safety applications (preciosa)," accessed: November, 2013. [Online]. Available: http://www.preciosa-project.org/

[21] "E-safety vehicle intrusion protected applications (evita)," accessed: November, 2013. [Online]. Available: http://www.evita-project.org/

[22] "Secure vehicular communication eu funded project," accessed: November, 2013. [Online]. Available: http://www.sevecom.org

[23] "Open vehicular secure platform (oversee)," accessed: November, 2013. [Online]. Available: https://www.overseeproject.com/

[24] "Intellidrive for safety, mobility, and user fee project: Driver performance and distraction evaluation," accessed: November, 2013. [Online]. Available: http://www.its.umn.edu/Research/ProjectDetail.html?id=2011091

[25] "Cooperative systems for road safety "smart vehicles on smart roads" (safespot)," accessed: November, 2013. [Online]. Available: http://www.safespot-eu.org/

[26] "Security and safety modelling (sesamo)," accessed: November, 2013. [Online]. Available: http://www.sesamo-project.eu

[27] "Preparing secure vehicle-to-x communication systems (preserve)," accessed: November, 2013. [Online]. Available: http://www.preserve-project.eu/

[28] "Communications for esafety (comesafety2)," accessed: November, 2013. [Online]. Available: http://www.comesafety.org

[29] ""cooperative cars and roads for safer and intelligent transportation systems (copits)," nprp 3 project," accessed: November, 2013. [Online]. Available: http://www.copits.org

[30] "Intelligent transport systems, etsi," accessed: November, 2013. [Online]. Available: http://www.etsi.org/technologiesclusters/technologies/intelligent-transport/

[31] ""advanced cellular technologies for connected cars (cellcar)," nprp 5 project," accessed: November, 2013. [Online]. Available: http://www.cellcar.org/

[32] L. B. Othmane, H. Weffers, M. M. Mohamad, and M. Wolf, "A survey of security and privacy in connected vehicles," in *Wireless Sensor and Mobile Ad-Hoc Networks*. Springer, 2015, pp. 217–247.

[33] A.-L. Carter, "Safety-critical versus security-critical software," in *System Safety 2010, 5th IET International Conference on*. IET, 2010, pp. 1–6.

[34] R. Bloomfield, K. Netkachova, and R. Stroud, "Security-informed safety: if its not secure, its not safe," in *International Workshop on Software Engineering for Resilient Systems*. Springer, 2013, pp. 17–32.

[35] S. Gillani, F. Shahzad, A. Qayyum, and R. Mehmood, "A survey on security in vehicular ad hoc networks," in *International Workshop on Communication Technologies for Vehicles*. Springer, 2013, pp. 59–74.

[36] E. Yuan, N. Esfahani, and S. Malek, "A systematic survey of self-protecting software systems," *ACM Transactions on Autonomous and Adaptive Systems (TAAS)*, vol. 8, no. 4, p. 17, 2014.

[37] R. S. Authority", "Rules of the road," http://www.rotr.ie/Rules_of_the_road.pdf.

[38] E. Yuan, S. Malek, B. Schmerl, D. Garlan, and J. Gennari, "Architecture-based self-protecting software systems," in *Proceedings of the 9th international ACM Sigsoft conference on Quality of software architectures*. ACM, 2013, pp. 33–42.

[39] N. Esfahani, A. Elkhodary, and S. Malek, "A learning-based framework for engineering feature-oriented self-adaptive software systems," *IEEE transactions on software engineering*, vol. 39, no. 11, pp. 1467–1493, 2013.

[40] G. Kiczales, J. Lamping, A. Mendhekar, C. Maeda, C. Lopes, J.-M. Loingtier, and J. Irwin, "Aspect-oriented programming," in *European conference on object-oriented programming*. Springer, 1997, pp. 220–242.