CS 435 - Project Report

Guilherme A.S. Milanez - 200491783[1]

[1]University of Regina.
Email: {guilherme.aguiar}@ufv.br

***Abstract*—Connected vehicles show even more fragility than regular vehicles once they have a lot of functionality integrated into different kinds of networks, once this fragility is the focus of a lot of recent research the following project aims to analyze the recent works and advances related to the security of VANETs. The focus of this project is to explore novel approaches in security mechanisms using encryption, authentication, and so forth. As long as the current literature is exposed, the final purpose of this work is to evaluate the most suitable techniques, in terms of implementation and computational cost, available for enhancing the security of vehicular communication.**

I. Introduction

Nowadays, many research efforts in the field of networks have been looking at Vehicular ad-hoc Networks as a research topic with great potential for academia and the industry in general. Vehicular networks (VANETs), can be defined basically as ad-hoc networks that provide communication among vehicles on the road, bringing several benefits. VANETs can be used to ensure the comfort, reliability, and safety of both driver and passenger in vehicles that are in some way connected[5]. Besides that, the capability to provide intervehicle communication (IVC), can bring advantages to the traffic environment like collision avoidance, road-hazard notification, and coordinated drive system [1].

In terms of comfort, connected vehicles can allow the integration with points of interest based on geographical position, and provide information about the traffic condition and weather [2].

The objective of this work is to analyze some recent works that propose methods to ensure secure communication between vehicles connected to a network. The contributions of this work are I) a summary of selected works, as well as their list based on citations and publication date; II) a comparison of the experiments used by each work; III) a relation between the computational costs of the works that provided such information.

The rest of the work is divided into the following sections: II) Theoretical Background, III) Methodology; IV) Security Schemes, V) Comparisons, and finally VI) Conclusion.

II. Theoretical Background

The following part of this report moves on to describe in detail the theoretical knowledge used by the selected works. Each sub-section explains the main parts of the theory necessary to understand the approaches proposed by the related papers.

A. Ad Hoc networks

In this survey the main topic, Vehicular networks is a sub-field of a particular kind of network, called ad hoc networks. This category of networks is known to enable, independent and wireless networking in environments where there is no infrastructure like wired or cellular architecture to stand the communication [3] .

Those networks are designed for special and customized applications, like Wireless sensor networks, IoT monitoring networks, and Vehicular networks. Besides that, the protocols and embedded applications are designed for the specific goal and to work with some kind of restrictions. [3]

B. Vehicular networks

In vehicular networks, the entities are the vehicles, and those entities are embedded with OnBoard Units (OBUs) devices, this device enables Vehicle to Infrastructure (V2I) and Vehicle to Vehicle (V2V)

wireless communications when using Dedicated Short Range Communication (DSRC) protocol standard [4], [5], [6], [7].

In terms of security in vehicular networks is important to address different kinds of requirements to make a network reliable and secure. There are different kinds of requirements according to the [8]:

- Data origin authenticity: the data origin is authentic and reliable
- Integrity: The data is authentic even after being transferred
- Access control: allows information access only for authorized users
- Freshness: time information of the related message
- Non-repudiation: undeniability of the entity's actions
- Privacy: keep the entity information confidential
- Confidentiality: only approved entities can obtain the information
- Availability: the services delivered are functional

The fig. 1 shows the respective requirement that should be addressed for a group of protocols that must work together to provide full security and reliability to a specific vehicular network. All the works in this review are addressing the communication security challenge. Although, it is relevant to explain briefly some aspects of communication in VANETs.

1) Secure communication: Another field with the severe necessity to be secure and reliable to provide a satisfactory vehicular network service is communication. In a context in which there is a numerous quantity of vehicles connected and sharing information with specific spots and other vehicles, the used protocols need to guarantee reliable communication to maintain the integrity of the shared information. To assure secure communication, the available protocols can use different kinds of approaches. In the current literature, we can find works using message authentication, data encryption, intrusion protection, and so forth [9].

Fig. 1. Security requirements.

C. Security methods

The following part defines the procedures used by the selected works in order to establish secure communication between peers in a vehicular network.

1) RSA RIVEST-SHAMIR-ADLEMAN: Before showing the proper definition of the RSA algorithm it is important to explain public-key cryptography. In this kind of procedure, instead of using permutations and substitutions, the algorithm works over mathematical functions. Another main difference between public-key cryptography and other cryptography schemes is in this first one, there are two different keys [10]. The RIVEST-SHAMIR-ADLEMAN [11] algorithm works using an expression with exponentials. The plaintext is encrypted in blocks, and each of those blocks has a binary value associated with less than some number n. The block size, then, should be less than or equal to

$$log_2(n) + 1$$

The encryption and decryption form, for some plaintext block M and ciphertext block C, follows the above scheme [10]:

$$\mathrm{C} = \mathrm{M}^e \bmod n$$
$$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$$

2) Message Authentication: Another method used in the revised works is message authentication techniques. This procedure basically is a method to verify if the received messages come from the

alleged source and it is identical to the original message. Message authentication can also verify sequencing and timeliness [10].

Any procedure of message authentication has two levels of functionality. At the lower level, we can find some sort of function that produces an authenticator. An authenticator is a value that is used to authenticate a message. This lower-level function triggers the higher-level authentication protocol that allows a receiver to verify the genuineness of a message. [10]

In this context, a technique widely used is the Message authentication code MAC in this technique we need to use a secret key to generate a fixed-size block of data, called a cryptographic checksum which is added to the message. In order To work satisfactorily, it is necessary that the two communicating parties share a common secret key. This procedure can be simplified as a triple of algorithms [12].

Composed of three main parts:

1) **Key Generation**: An algorithm to generate a key that takes as input a security parameter and gives as an output a secret key.
2) **Tagging** Consists of a proper authentication algorithm, taking as an input the secret key and the message and giving as an output an authentication tag.
3) **Verification** This last algorithm has the functionality of taking, the key, the message, and the tag as input and producing a decision (accept, reject) as an output.

3) Key Management: Throughout this survey, the term Key Management is used to refer to the overall process in which a system can handle all the process that uses some security keys, the general goal of a key management system is to provide secure techniques for addressing cryptographic keying material, then those keys can be used in symmetric or asymmetric cryptographic algorithms [13]. The main functions of this procedure are entity registration, key generation, certification, authentication, key distribution, and key maintenance [13].

III. Methodology

The intention of the following section is to define how the research on the current literature was conducted, how the works were chosen, and based on which kind of attributes they had been classified to belong to this review.

To achieve the goal of this project was necessary to read and select the best papers over a wide range available that cover good approaches to ensure security in VANET's. All of the works presented in this review bring a different approach to ensure safe communication between the vehicles in those networks.

For this project, all works used to integrate the review were found by the google search mechanism to find research papers, called google scholar [14]. The steps for the research were the following:

- Searching for the key-words
- filtering by date and number of citations
- Choosing a paper based on the above criteria
- Look up those related papers associated with the one picked

The research was conducted following the flow of the scheme in fig 2.

IV. Security schemes

The section that follows, will provide a brief description of the selected works. Each one of those works shows a different technique to deliver more security to connected vehicles. They had proposed solutions to satisfy mainly two kinds of security requirements explained in the theoretical section, secure communication, and reliable privacy. The table I summarizes the selected works in terms of the research factors used to classify them.

A. A Modified RSA Cryptography Algorithm for Security Enhancement in Vehicular Ad Hoc Networks

The authors in this work [15], seeks to deliver a new scheme based on the RSA algorithm to provide reliable communication in the vehicular network. To do that, they propose the MRSA, a modification of the classical algorithm using three prime numbers j, k, and l instead of the usual approach which uses only two numbers. By adding a new factor to the prime number set used in the encryption the authors

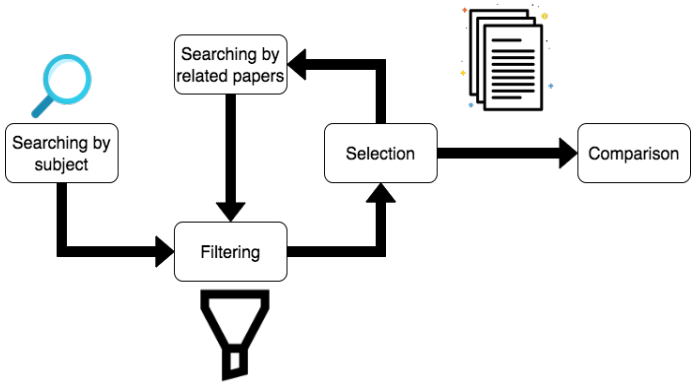

Fig. 2. Research schema.

Name	Security Technique	Citations	Publication date	Vehicle
MRSA	RSA	2	2018	Springer
DSPA	ID-based cryptography and hash authentication code	70	2018	IEEE
SmartVeh	message access control and authentication scheme	16	2018	Sensors
TLS	TLS	30	2017	ACM
PW-CPPA-GKA	Authentication	134	2018	Elsevier
PPDA	Authentication	159	2017	IEEE

TABLE I
SELECTED WORK

can deliver a scheme with security enhancement, therefore to do that time complexity is increased as well.

B. Decentralized and scalable privacy-preserving authentication scheme in VANETs

A decentralized and scalable privacy-preserving authentication (DSPA) scheme for secure vehicular ad hoc networks had been proposed in [16] . The authors aspired to provide a scheme to deliver functions like node authentication, message authentication, non-repudiation, privacy, and so forth. To do that they used ID-based cryptography and hash authentication code. The structure of the scheme is divided into phases: Phase-I: system initialization, Phase-II: Vehicle to Infrastructure (V2I) wireless communication pre-authentication, and Phase-III: Vehicle to Vehicle (V2V) communication authentication. In the end, using, simulations, the authors proved that the proposed scheme can significantly reduce communication and computation overheads.

C. SmartVeh: Secure and Efficient Message Access Control and Authentication for Vehicular Cloud Computing

In this work [17], the authors aim to provide a scheme to supply security in the message exchange between the vehicles in a VANET. To do that, the authors propose a secure and efficient message access control and authentication scheme for vehicular cloud computing based on hierarchical attribute-based encryption and attribute-based signature.

D. On Using TLS to Secure In-Vehicle Networks

Similarly to the other works, in [18] the authors shows a scheme capable of providing secure communication. To perform that, the authors evaluate how cryptographic protocols like TLS can be employed to provide secure communication between Electronic Control Units that realize various vehicular functions over the hardware and software. The work shows an analysis of key management and the use of TLS to protect in-vehicle communication.

E. A robust and efficient password-based conditional privacy-preserving authentication and group-key agreement protocol for VANETs

The work [19] presents a new protocol that combines different techniques to provide satisfactory authentication to vehicles in VANETs. The authors propose password-based conditional privacy-preserving authentication and group-key generation (PW-CPPA-GKA) protocol. The work offers group-key generation, a user leaving, the user joins, and password facilities. In terms of computational resources, the proposed protocol is addressed like a lightweight scheme since it was designed without bilinear-pairing and an elliptic curve. Besides that, the protocol can provide a group-key generation technique, where vehicles can only communicate with vehicles in the same group key [19].

F. Efficient privacy-preserving dual authentication and key agreement scheme for secure V2V communications in an IoV paradigm

In [20], the author seeks to provide a scheme to guarantee security in terms of authentication of the vehicles in the network. To do that, they present a Privacy-Preserving Dual Authentication and Key Agreement Scheme, PPDA. This scheme provides vehicle identity authentication and reputation evaluation enhanced when compared to the previous literature. The method proposed offers a procedure in which once an authentication session has opened the system sets a temporary encryption key using bilinear pair theory. Besides that, the work brings new solutions to enhance privacy and time management in terms of delay tolerance.

V. Comparisons

A. Experimentation type

One way to compare the works is to evaluate how each of them proves their efficiency. To guarantee that the research work is valid, the result should be passed through some research method. There are different kinds of methodologies to evaluate results like simulations, real experimentations, mathematical proofs, and so forth. In the case of computer networks, even though generally the measurements in real scenarios are commonly non-viable, those kinds of measurements show better relations with reality. In this context, in table II the only paper that has evaluated their results in an environment with approximate real conditions was [18].

B. Computational cost

Of the works analyzed, only 3 of them provided analyzes of the computational cost associated with certain operations, this relation can be observed in the table III. This type of analysis is of great value to list good security algorithms since they provide information on the computational requirement necessary to execute such methods with satisfaction. PPDAS provides an analysis where $C_m, C_h C_{bp}, C_{se}$ are the costs associated with multiplication, hashing, bilinear pairing, and symmetric cipher operations. PW provides analysis based on hash operating time, for two steps. To facilitate the comparison, in this work we combined the two costs to perform a general analysis. $T_H V$ consists of the hash time for the authentication message verification operation and $T_h G$ authentication message generation operation. The same combination was made for the SmartVeh work, in which the variables T_0, T_t, represent the costs of operations on multiplicative groups with the same prime order p during the Bilinear Map operation respectively, and T_r represents the cost of the pairing operation.

All three analyzes were performed on OBUs, however, as each cost is associated with a different type of operation, it would not be fair to list an algorithm with the best fit according to its computational cost. The other selected algorithms do not provide computational cost analysis but provide comparisons of running time over simulation with other algorithms in the literature.

VI. Conclusion

In this work, 6 scientific articles have been listed that deal with methods of guaranteeing security in the communication of elements in vehicular networks. In terms of scientific relevance, the work that most stands out, considering the number of citations and the date of publication, is the [20], as it presents a large number of citations. When analyzing the implementation support for real devices, the [18] work

Name	Experimentation type
MRSA	Simulations
DSPA	Simulations using ns-3, traffic simulators SUMO and MOVE
SmartVeh	Simulation + Mathematical analysis
TLS	Analysis over development boards with real resources
PW-CPPA-GKA	Simulations + Mathematical analysis
PPDA	Simulations + Heuristic evaluation

TABLE II
CONDUCTED EXPERIMENTS

Computational cost	Algorithm
$C_M + 2C_H + C_{BP} + CSE$	PPDAS
$4T_H V + 6T_h G$	PW-CPPA-GKA
$3T0 + T_t + T_r$	SmartVeh

TABLE III
COMPUTATIONAL COSTS

is shown to be more relevant because it presents implementation on real boards for the development of this type of technology, when presenting results with this type of experiment, the work has an ease of adherence and implementation in the industry. Regarding the computational cost comparison, since they do not have the cost associated with an operation of the same type, presenting a prominent algorithm would not be fair. Because of that, for this part, there is only the compiled finding of the costs associated with each method.

REFERENCES

[1] J. J. Blum, A. Eskandarian, and L. J. Hoffman, "Challenges of intervehicle ad hoc networks," *IEEE transactions on intelligent transportation systems*, vol. 5, no. 4, pp. 347–351, 2004.

[2] J. Jakubiak and Y. Koucheryavy, "State of the art and research challenges for vanets," in *2008 5th IEEE Consumer Communications and Networking Conference*. IEEE, 2008, pp. 912–916.

[3] P. Mohapatra and S. Krishnamurthy, *AD HOC NETWORKS: technologies and protocols*. Springer Science & Business Media, 2004.

[4] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed aggregate privacy-preserving authentication in vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 3, pp. 516–526, 2016.

[5] V. Daza, J. Domingo-Ferrer, F. Sebé, and A. Viejo, "Trustworthy privacy-preserving car-generated announcements in vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 4, pp. 1876–1886, 2008.

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

[7] S. S. Manvi and S. Tangade, "A survey on authentication schemes in vanets for secured communication," *Vehicular Communications*, vol. 9, pp. 19–30, 2017.

[8] O. Henniger, L. Apvrille, A. Fuchs, Y. Roudier, A. Ruddle, and B. Weyl, "Security requirements for automotive on-board networks," in *2009 9th International Conference on Intelligent Transport Systems Telecommunications,(ITST)*. IEEE, 2009, pp. 641–646.

[9] Q. Hu and F. Luo, "Review of secure communication approaches for in-vehicle network," *International Journal of Automotive Technology*, vol. 19, no. 5, pp. 879–894, 2018.

[10] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 5th ed. USA: Prentice Hall Press, 2010.

[11] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[12] Y. Dodis, E. Kiltz, K. Pietrzak, and D. Wichs, "Message authentication, revisited," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2012, pp. 355–374.

[13] W. Fumy and P. Landrock, "Principles of key management," *IEEE Journal on selected areas in communications*, vol. 11, no. 5, pp. 785–793, 1993.

[14] P. Jacsó, "Google scholar: the pros and the cons," *Online information review*, 2005.

[15] D. Roy and P. Das, "A modified rsa cryptography algorithm for security enhancement in vehicular ad hoc networks," in *Proceedings of the International Conference on Computing and Communication Systems*. Springer, 2018, pp. 641–653.

[16] S. Tangade, S. S. Manvi, and P. Lorenz, "Decentralized and scalable privacy-preserving authentication scheme in vanets," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 9, pp. 8647–8655, 2018.

[17] Q. Huang, Y. Yang, and Y. Shi, "Smartveh: Secure and efficient message access control and authentication for vehicular cloud computing," *Sensors*, vol. 18, no. 2, p. 666, 2018.

[18] D. Zelle, C. Krauß, H. Strauß, and K. Schmidt, "On using tls to secure in-vehicle networks," in *Proceedings of the 12th International Conference on Availability, Reliability and Security*, 2017, pp. 1–10.

[19] S. H. Islam, M. S. Obaidat, P. Vijayakumar, E. Abdulhay, F. Li, and M. K. C. Reddy, "A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for vanets," *Future Generation Computer Systems*, vol. 84, pp. 216–227, 2018.

[20] Y. Liu, Y. Wang, and G. Chang, "Efficient privacy-preserving dual authentication and key agreement scheme for secure v2v communications in an iov paradigm," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 10, pp. 2740–2749, 2017.