International Journal of Engineering & Technology, 7 (4) (2018) 5288-52991

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i4.13840
Research paper

Broadcasting messages securely in VANET

Mounia Miyara [1] *, Hamza Toulni [1], Benayad Nsiri [2]

[1] GITIL Laboratory. Faculty of Sciences Aïn Chock, Hassan II University of Casablanca, Casablanca, Morocco
[2] Research Center STIS, M2CS, Higher School of Technical Education of Rabat (ENSET), Mohammed V University in Rabat, Morocco
**Corresponding author E-mail: b.nsiri@um5s.net.ma*

Abstract

In Vehicular Ad hoc Networks, the secure sharing of information exchanged is necessary, due to the importance and sensitivity of this information exchanged. But the features and requirements of VANET prevent direct application of existing security solutions impossible. In this paper, we propose an effective solution to ensure the security of critical and urgent information. The solution provides authentication and confidentiality while minimizing the time required to decrypt the messages.

Keywords: *Vehicular Ad-Hoc Networks; Security; Public Key Exchange; Broadcast Encryption.*

1. Introduction

Vehicular ad-hoc networks (VANET) is a new advanced technology, which establishes the future of the intelligent systems of transport [1]. In fact, VANETs are considered a particular case of Mobile Ad hoc Networks (MANET) where nodes are replaced by vehicles, and their main purpose is to solve the problems bound to the road transport, such as the accidents and the congestion on the road. Hence the crucial role VANET in the success of the emergent smart cities.

VANET inherits the same characteristics of MANET, but with some differences, as the high mobility of nodes, which involves frequent topological changes. Consequently, a vehicle can quickly join or leave a group of vehicles. In addition, VANET provides high-speed connectivity, besides a number of technical solutions such as location and with great accuracy. So, VANET operates in an environment very different from that of the MANET.

VANET is an ideal target for various attacks [2], because vehicles share all kinds of information via wireless links, without any administration by a centralized infrastructure, which facilitates the malicious interception of information exchanged or the injection of erroneous information in the network. Hence the importance of securing VANET to protect communication within the network. However, the addition of the security mechanism implies an additional computing cost, thus influencing the transmission performance.

Additionally, most of the safety applications in VANET use broadcast communications [3] to spread information with the urgent character in the network. Thus security is an unsurpassable precondition for the deployment of VANET.

To address this critical question of security, an effective approach to broadcasting a message securely is present in this paper to protect the broadcasts messages in VANET. Besides insurance of broadcasting communication; the proposed solution significantly reduced the time for the decrypting, improving the performance of VANET.

The rest of the paper is organized as follows; the following section provides an overview of the security requirements in VANET. Section 3 gives a state of the art work of security solutions in VANET, In Section 4, we present an overview of cryptography. In Section 5, we present our proposed solution. Finally, we conclude the paper in Section 6.

2. Security requirements in VANET

The information sharing between the drivers on the road allows to recognize and to avoid the potential dangers, and so to improve the road safety. For this, VANET must ensure the transmission of information in a short time and without loss in any situation. Furthermore, it must ensure the authenticity of the information:

Authentication: is the process of verifying that allows the network members to ensure the correct identification of the vehicles with which they communicate, and thus to know more information about the emitting vehicle as its identifier, its address, its properties and its geographical position.

Integrity: This required security property ensures that the data exchanged are not subject to wilful or accidental forgery. Thus, it allows recipients to detect the manipulation of data by unauthorized entities and to reject packets.

Confidentiality: This security property requires that only authorized entities can access data transmitted over the network. However, the confidentiality of the information in VANET depends on the request and the communication scenario, especially in the case of emergency warning messages that must be read by an entity in VANET.

Non-repudiation: This required property security ensures that no sender can refuse to be the source of a message. This goal is essential in sensitive communications. Thus, the general purpose of non-repudiation is to collect, maintain, and make available all evidence of an event or action, in order to resolve disputes about its occurrence. Non-repudiation also depends on authentication, and the system can identify the author of a malicious message.

Availability: This property is necessary to ensure that authorized entities have access to network resources with adequate quality of service. Resources must remain available even if the network fails. This not only ensures the operation of the system, but it also makes it fault-tolerant. In addition, resources should remain available until the threat is exceeded.

3. Related work

To meet security requirements and overcome threats of attack in VANET, many researchers have proposed mechanism and solutions to ensure secure communication within VANET:
In [4], the authors propose a privacy-preserving defense technique for network authorities to handle misbehavior in VANET access, considering the challenge that privacy provides a venue for misbehavior. The proposed system employs an identity-based cryptosystem where certificates are not needed for authentication. This system uses a cryptography based on the identity which allows the public key to be diverted from the public identity of the user, as his name or its email address. This cryptographic system uses a plan of defense in which the signature of threshold and the authentication of threshold must be taken into account to assure the conservation of the confidentiality and the detached capacities against the defective knots of the arbitrators and to facilitate the distribution of preprints.
In [5], the authors propose a new collaborative protocol for enforcing anonymity in multi-hop VANETs, closely inspired by the well-known Crowds protocol. In a nutshell, our anonymous-reporting protocol depends on a forwarding probability that determines whether the next forwarding step in message routing is random, for better anonymity, or in accordance with the routing protocol on which our approach builds, for the better quality of service. Different from Crowds, our protocol is specifically conceived for multi-hop lossy wireless networks.
In [6], the authors present a Vehicle Ad-Hoc Network Reputation System (VARS), a completely distributed approach based on reputation. This work is based on the following assumptions: cars move at a high average speed; VANETs may become very large, in the order of thousands or even millions of nodes, so that authenticated identities are not feasible; a solution has to be completely decentralized; available bandwidth for communication remains limited, while processing power and memory continue to increase.
In [7], the authors propose a novel secure scheme for vehicular communication on VANETs. The proposed scheme not only protects the privacy but also maintains the liability in the secure communications by using session keys. To make more secure, they used Advanced Encryption Standard (AES); and to provide confidentiality and non-repudiation, the message is signed by sender's private key. This scheme is based on the certificate based public key cryptography so the overhead of such scheme can create delays in transmission.
In [8], the authors propose an anonymous authentication protocol featured with conditional privacy preservation and non-repudiation for the vehicular ad-hoc network. This proposition is based on Certificate-based Cryptography (CBC) combines the advantages of ID-based cryptography (implicit certification) and traditional PKI approach (no key escrow). First, a certificate-based signature scheme with only one pairing computation and only one element signature is proposed. Then, an anonymous authentication protocol is constructed by applying the proposed signature scheme and a novel concept called the account index which helps to realize On-Board Units anonymity, non-reputation, and conditional privacy preservation. A secure session key is established in the protocol, which provides perfect forward secrecy.
In [9], the authors propose an event-based reputation system to prevent the spread of false traffic warning messages. In this system, a dynamic reputation evaluation mechanism is introduced to determine whether an incoming traffic message is significant and trustworthy to the driver. The proposed system is characterized and evaluated through experimental simulations. This system can effectively prevent false messages spread on various VANET environments.
In [10], the authors propose a framework for data-centric trust establishment: First, trust in each individual piece of data is computed; then multiple, related but possibly contradictory, data are combined; finally, their validity is inferred by a decision component based on one of various evidence evaluation techniques. In this framework, a collection of multiple reports is passed to a decision logic module. Specific weights associated with these reports are also passed along with these reports to the module where different techniques are applied to derive the level of trust of the given data.
In [11], the authors propose a road-side unit (RSU) and beacon-based trust management system, called RaBTM, which aims to propagate message opinions quickly and thwart internal attackers from sending or forwarding forged messages in privacy-enhanced VANET. The authors use Tanimoto coefficient measure to determine the trustworthiness of the vehicles; they compare the sent an estimated position of the vehicles and calculate the difference to estimate the trustworthiness. In the indirect method, the trustworthiness of the message is determined by checking the trust value between sender and receiver.

4. Cryptographic solution

The cryptography is the technique used to make the confidential data by the encryption at source node and decryption at the destination node. It can be considered as a key solution for the most part of the attacks.
We distinguish two types of encryption and decryption algorithms.

- Symmetric key algorithms in which all nodes have the same encryption key.
- Asymmetric key algorithms where we distinguish the use of two keys, a public key known by all the nodes and the private one for each node.

To ensure that information is accessible only by authorized entities, the most reliable solution is to use asymmetric algorithms. This infrastructure is known as public key infrastructure that we will note PKI (Public Key Infrastructure).
In a PKI, the communication is encrypted with a digital certificate, this certificate is requested from the Registration Authority. This generates a couple of keys (public key, private key) and sends the private key to the requesting entity only.
The production, transmission, and memory keys are called key management; all cryptographic systems must address key management issues. Since all private keys in PKI cryptosystem must remain secret, PKI often has difficulty providing secure key management, especially in open systems with a large number of users.
Due to a large number of vehicles and their speeds, minimizing end-to-end delay in VANET is very important to ensure the smooth operation of services and applications while satisfying security requirements in this type of network. But the use of traditional security mechanisms as PKI has negative effects on the quality of services and applications because these mechanisms are complex and time-consuming, resulting in additional delays in getting information to its destination, even if energy, memory and computing capacity do not constitute an obstacle in VANET.
Broadcast encryption [12] is an effective way to securely broadcast a message, that many privileged receivers can decrypt it. So this approach used a single public key for all entities to decrypt the message and each entity has a private key to encrypt the message. That way we could improve the management of keys.

5. Description of the solution

Broadcasting or multicasting in VANET is the distribution of information for sharing with multiple vehicles. But, given the importance of the shared information, the vehicles must know that the information received is actually sent by the sender claimed, and that information is received from the source without any modification.
Therefore Broadcast Encryption guaranteed the requirements already mentioned in the distribution of information. Suppose that there is a vehicle group, numbered from 1 to N, and each of them keeps a private key and the whole group has the same public key. A sender encrypts a message M directed to the vehicles of the group using its private key as an encrypted message. Upon receipt

of the encrypted message, the vehicle decrypts the encrypted message using the public key.

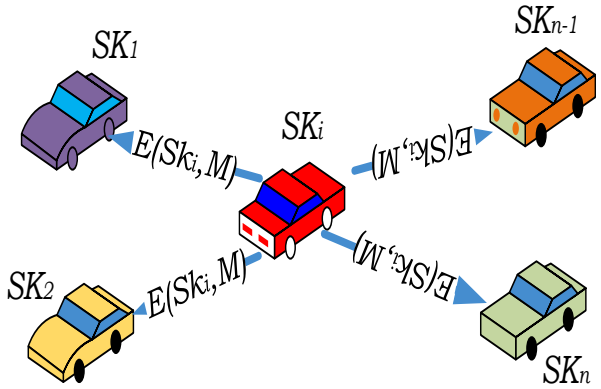

Fig. 1: The Broadcasting of an Encrypted Message.

5.1. The formation of groups

VANET is characterized by a highly dynamic topology, which implies frequent changes of position and a limited life of connections between vehicles. However, as the vehicles move according to the laws of the traffic and according to the ways already predefined by the road infrastructure. Thus, the use of the path and the vehicle speed can improve and optimize the stability of the link and the distance between vehicles.
So the choice of vehicles of the group is done according to:

- Speed: the speed of each vehicle in the Group should be around the same average speed so that communication remains established.
- Direction: all vehicles in the group should move in the same direction.

Once the group is formed and the communication between the vehicles is established, a pivot is elected according to its position which must be at the center of the group. This pivot will act as a certification authority. Therefore, he receives the public keys of all the vehicles of the group and he sends his public key to these vehicles.

5.2. The dissemination of information

The dissemination of information by one vehicle to the other vehicles of the groups takes place in three main phases, as shown in Fig 2:
Phase 1: The vehicle initiator A sends the encryption of message M_A by his private key SK_A to the pivot vehicle.
Phase 2: The pivot vehicle decrypt $E(SK_A, M_A)$ by the public key PK_A of vehicle A. After that it makes $E(SKp, M_A)$ the encryption of message M_A by its private key SKp, and sends it to all vehicles of the groups.
Phase 3: Each vehicle decrypts the $E(SK_p, M_A)$ by the public key PKp of the pivot vehicle.

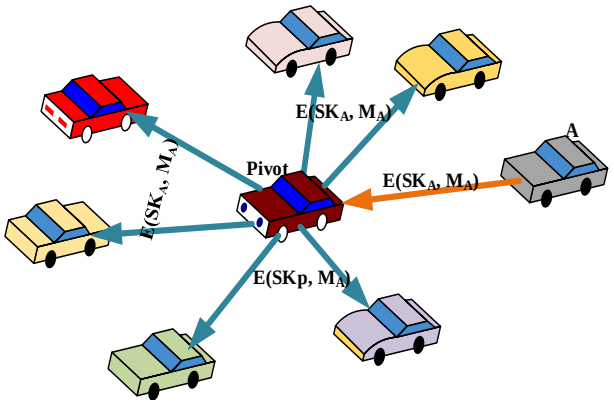

Fig. 2: The Dissemination of Information in the Group.

5.3. Simulation

We choose SUMO (Simulation of Urban Mobility) and NS2 (Network Simulator 2) as simulation platforms to test the effectiveness of our proposed routing protocol.
SUMO is a purely microscopic traffic simulator, designed to handle large real-time route maps, which can be downloaded from OpenStreetMap, allowing simulations of different scenarios in different parts of the world. SUMO has the ability to function as a server and to report real-time simulation data to external applications via TraCI (Traffic Control Interface) which uses the TCP protocol.
In our case, we use SUMO to allow the simulation scenarios to be changed in NS2 at run time and thus provide a dynamic simulation in NS2 and highlight the effectiveness of our solution.
The purpose of this simulation is to compare the performance of the proposed solution, so we consider multiple scenarios according to the number of vehicles. We used the same scenarios for the two solutions; we use the following simulation parameters:

Table 1: Simulation Parameters

Map size	1500m x 1500m
Number of vehicles	20,50,80,100
Average speed	15m/s
Simulation time	900s
MAC protocols	IEEE 802.11p
Routing protocols	AODV
Encryption algorithm	RSA

For both solutions, and for each scenario, we calculate the average time needed for the message to be decrypted by the vehicles in the group.

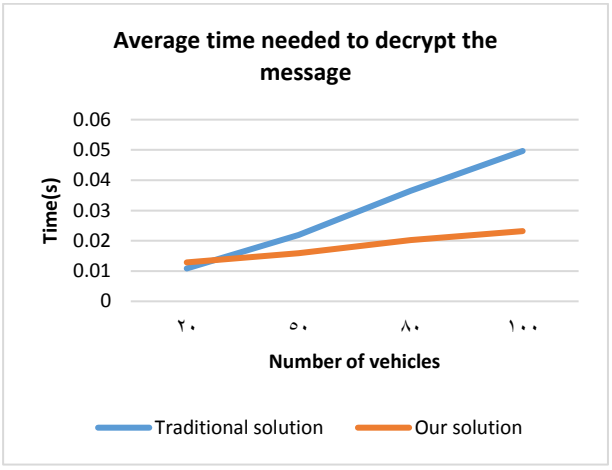

Fig. 3: Time Needed to Decrypt the Message.

In Fig. 3 which illustrates the results of the simulation, we note that, if the network size increases, with more vehicles, the time of the decryption increases slightly in both solutions. But the time needed to decrypt the message in our solution is greatly less than the time needed in the traditional solution.

6. Conclusion

VANET is a special case of MANET which is formed solely by vehicles traveling on the road. However, VANET is vulnerable to attack due to the lack of infrastructure and the use of wireless links. In this paper, a new solution to share and disseminate critical and urgent information.
The proposed solution aims at securing communication between vehicles in a single group, and thus ensures:
Authentication, which consists of verifying that the received data are actually sent by the requested sender. In the proposed solution, each vehicle in the group uses the public key of the pivot vehicle to decrypt the message. The encryption of each message distribut-

ed by the private key provides the authentication of each vehicle in the group.
Confidentiality ensures that only intended recipients can read the messages. In the proposed solution, each vehicle can encrypt the messages only with its private key.
The proposed solution is simulated and it has been compared with the traditional solution in several conditions, the experimental result shows that the proposed solution is very effective. In the future work, we will try to improve the proposed solution by adding more complexity in different attacks.

References

[1] H. Hartenstein,K. Laberteaux "VANET: vehicular applications and internetworking technologies" USA: John Wiley & Sons; 2009.

[2] Sumra, I.A.; Bin Hasbullah, H.; Bin AbManan, J.-L., "Effects of attackers and attacks on availability requirement in vehicular network: A survey," in Computer and Information Sciences (ICCOINS), 2014 International Conference on , vol., no., pp.1-6, 3-5 June 2014.

[3] A. Singh, M. Kumar, R. Rishi, and D.K. Madan "A relative study of MANET and VANET: Its Applications, Broadcasting Approaches and challenging Issues", N. Meghanathan et al. (Eds.): CCSIT 2011, Part II, CCIS 132, pp. 627–632, 2011. https://doi.org/10.1007/978-3-642-17878-8_63.

[4] J. Sun C. Zhang Y. Zhang Y. Fang "An identity-based security system for user privacy in vehicular ad hoc networks" IEEE Trans. Parallel Distrib. Syst vol. 21 no. 9 pp. 1227-1239 Sep. 2010. https://doi.org/10.1109/TPDS.2010.14.

[5] C. T. Barba et al. "A collaborative protocol for anonymous reporting in vehicular ad hoc networks" Comput. Std. Interfaces vol. 36 no. 1 pp. 188-197 Nov. 2013. https://doi.org/10.1016/j.csi.2013.06.001.

[6] F. Dotzer, L. Fischer and P. Magiera, "VARS: a vehicle ad-hoc network reputation system," Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks, pp. 454-456, 2005. https://doi.org/10.1109/WOWMOM.2005.109.

[7] Neng-Wen Wang, Yueh-Min Huang, Wei-Ming Chen, A novel secure communication scheme in vehicular ad hoc networks, In Computer Communications, Volume 31, Issue 12, Pages 2827-2837, 2008. https://doi.org/10.1016/j.comcom.2007.12.003.

[8] X. Wang, T. Liu, and G. Xiao, "Certificate based anonymous authentication protocol for vehicular Ad Hoc network," IETE Technical Review, Vol. 29, no. 5, pp. 38893, Sep. 2012. https://doi.org/10.4103/0256-4602.103172.

[9] Nai-Wei, L., Hsiao-Chien, T.: A reputation system for traffic safety event on vehicular ad hoc networks. EURASIP Journal on Wireless Communications and Networking, 2009

[10] M. Raya, P. Papadimitratos, V. D. Gligor and J. P. Hubaux, "On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks," IEEE INFOCOM 2008 - The 27th Conference on Computer Communications, Phoenix, AZ, 2008, https://doi.org/10.1109/INFOCOM.2008.180.

[11] Wei YC, Chen YM. An Efficient Trust Management System for Balancing the Safety and Location Privacy in VANETs. IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, Liverpool. p. 393-400. 2012 https://doi.org/10.1109/TrustCom.2012.79.

[12] Fiat A, Naor M. Broadcast Encryption. Crypto1993, LNCS 773, Santa Barbara, California, USA. Springer-Verlag: Berlin, 1993; 480–491.