Security Challenges for Emerging VANETs

Faisal Al-Hawi

Chan Yeob Yeun

Mahmoud Al-Qutayti

Computer Engineering Department

Khalifa University of Science, Technology and Research

P.O. Box 573, Sharjah, United Arab Emirates

Tel: +971 6 504 3503

Fax: +971 6 561 1789

Emails:

f.alhawi@kustar.ac.ae

cyeun@kustar.ac.ae

mqutayri@kustar.ac.ae

Security Challenges for Emerging VANETs

Faisal Al-Hawi

Khalifa University of Science Technology and Research, UAE

f.alhawi@kustar.ac.ae

Chan Yeob Yeun

Khalifa University of Science Technology and Research, UAE

cyeun@kustar.ac.ae

Mahmoud Al-Qutayti

Khalifa University of Science Technology and Research, UAE

mqutayri@kustar.ac.ae

ABSTRACT

Vehicle ad-hoc networks (VANETs) are a prominent form of mobile ad-hoc networks. This paper outlines the architecture of VANETs and discusses the security and privacy challenges that need to be overcome to make such networks practically viable. It compares the various security schemes that were suggested for VANETs. It then proposes a new implementation of an identity based cryptosystem that is robust and computationally efficient.

Key Words: VANETs, Security, Privacy, Identity Based Cryptosystem

1. Introduction

Pervasive Networks (PN) are those networks that provide a diversity of services from single access points. One example of such networks is the Mobile Ad-hoc Network (MANET) where nodes are highly mobile hence constantly reforming the topology of the network. An application of these networks is the emerging VANET.

VANETs are wireless ad-hoc networks where the nodes, either vehicles or road side units (RSU), can communicate and exchange data for purposes of information inquiry or distribution. This can be achieved by allowing nodes to connect within certain ranges (typically 5-10 Kilometers) in order to exchange information about traffic conditions [1]. VANETs can greatly help in providing safety services and improving the driving experience. For example, the provision of road conditions such as environmental hazards information, traffic conditions and congestions' locations, accident reporting which help the authorities to maintain road status.

Moreover, entertainment options can be provided for customers. An example of such an option is the TracNet system which was introduced by Microsoft and KHV [2] to provide internet access in vehicles. The diversity of applications is driven by the fact that VANETs are ultimately considered a form of ubiquitous networks which intend to

provide many services with a single access point.

To date, communication technologies in VANETs are based on existing protocols. An example of such protocols is the IEEE 802.11 (i.e. Wi-Fi) standards [3] with its different enhancements (802.11b/g). Some application of VANETs such as toll payments system used in the UAE 'Salik' also rely on Radio Frequency Identification (RFID) which is a type of Dedicated Short Range Communication (DSRC) standard suit [3]. However, these methods introduce some latency problems which are intolerable in such networks. Therefore, an IEEE project to provide a new enhancement to the 802.11 standard that will improve communication for such network is in progress. The new standard, known as IEEE 802.11p [3], will be based on DSRC but with an addition of Wireless Access for Vehicular Environments (WAVE). This will support both Vehicle-to-Vehicle (V2V) and Vehicle-to-RSU (V2R) communication in VANETs [4], [5].

In order for VANETs to be used in the future they must provide adequate levels of security and privacy to the users. These aspects of the system are of paramount importance as they affect people safety and may compromise their personnel privacy if not properly addressed.

The paper is organized as follows: section two discusses the challenges that are facing VANETs. Section three explores previous related works in the field of VANET security. In section four, we provide an example of how Identity-Based Cryptography (IDBC) can be used in VANETs. Then, we present our proposed implementation of IDBC in VANETs.

2. VANETs Challenges

The ultimate goal of VANETs is to enhance the driving experience by providing different measures of safety while driving. However, in order to achieve this goal; some challenges must be considered. In this paper, we categorize challenge aspects into two major groups that must be considered: security and privacy. Although privacy aspects will be reviewed and discussed, the paper will focus more on the security aspects that are taken into account in order for users to trust using such networks.

2.1. Security challenges

One of the major challenges of securing VANETs is communication security. This aims to provide secure communication between vehicles, which is referred to as Inter-Vehicle Communication (IVC), and between vehicles and Road Side Units (RSU); Vehicle-to-RSU Communication (VRC). Any security framework must ensure that basic security services are provided in VANETs. These services include: information confidentiality which aims to prevent unauthorized access to information. For example, vehicles cannot access events recorders or other vehicles. Also, integrity of exchanged messages must be provided in order to detect malicious intent such as information alteration and prevent vehicles from spreading false traffic conditions. Additionally, vehicle authentication is important to ensure that all nodes within the network are who they claim to be. Hence preventing impersonation attacks where a vehicle pretends to be an authority or another vehicle. Other services include: availability of network services for all users at all times and accountability which aims to associate events with particular nodes for future references in order to prevent attempts to provide false claims or reject true ones (i.e. a node claiming that it was not at a certain location; where in fact it was) [1], [6]. Some recent works have been done to achieve security in VANETs; the use of cryptography primitives such as encryption and digital signatures proved to be able to provide security services of confidentiality, integrity and authentication in vehicular networks.

Another salient challenge that faces the security of VANETs is the process of key management. The key in the security domain is the number sequence that is used to encrypt and decrypt information. The issue of key management has many categories that must be resolved when designing security protocols for such networks. One important category is the process of key revocation which is the process of discarding suspected key or keys that are bound to malicious nodes. Traditional methods of revocation such as Certificate Revocation Lists (CRLs) are not suitable for VANETs because of large scale of the network (i.e. millions of vehicles) [7] which make these lists huge and increase the overhead of the revocation process. A second category is the process of group key management since VANETs inherit the characteristic of mobility from Mobile Ad-hoc Networks (MANETs). What makes this issue a problem is the fact that vehicles rarely form groups in VANETs since two vehicles may only be in close range for short amounts of time. Therefore, the security framework must resolve this issue to prevent malicious vehicles from compromising the security of the network.

2.2. Privacy challenges

The privacy issue is concerned with protecting personal information of drivers; such as name, location and plate number, within the network. This may seem easy at first, however the network protocol has to be designed in such a way that hides this information from other nodes; but allows it to be extracted by authorities in cases of accidents or malicious intent as a mean of auditing for authority usage. Hence, achieving conditional privacy is desirable for VANETs rather than unconditional privacy [7] and that could be a major challenge. Moreover, the tradeoff between robustness measures, such as the inclusion of personal information during communication which makes the task of malicious node detection easier, and the protection of drivers' information makes the issues of privacy more challenging [7] [8].

The eventual goal of VANET security protocols is to provide a vehicular communication network that is able to resist malicious activities and attacks and provide the highest possible level of node privacy. This is very challenging due to some of the unique features of VANETs such as the high mobility and the large network scale (i.e. millions of vehicles) [7].

3. Related works

This section examines major previous works that is related to the field of vehicular communication and VANET security.

3.1. Public-Key approaches for security and privacy

Hubaux *et al.* [8] have drawn the attention to security and privacy issues in vehicular communication. They highlighted how privacy concerns arose due to the fact that the license plates were replaced with electronic identities as a method of tracking vehicles used by authorities.

They proposed the use of public key cryptography (PKC) in vehicular communication in order to allow authorities and vehicles to certify identities of other vehicles; using 'Electronic License Plates' (ELP). They also suggest desirable privacy protocols that preserve drivers' personal information and mention some applications that could use the ELP. To ensure privacy preservation, they point out that privacy protocols must be based on anonymity schemes that hide the relationship between drivers' information and some random identifier.

In [1], a new architecture is proposed where vehicles have two extra hardware units; the Event Data Recorder (EDR) to record all events and the Tamper-Proof Hardware (TPH) that is capable of performing cryptographic processing. The article argues that the proposed architecture provides authentication, authorization and

accountability. They suggest the use of public key cryptography with a manageable and robust PKI since symmetric key cryptography does not support accountability. Authentication is performed by digital signatures of communicated messages; they proposed the use of Elliptic Curve Cryptography (EEC) since it reduces the processing requirements.

3.2. Certificate revocation

Raya *et al.* [1] proposed a security architecture for vehicular communication that aims to provide security services for such networks. They also proposed a novel certificate revocation technique through three protocols: the Revocation protocol of Tamper-Proof Device (RTPD), Distributed Revocation Protocol (DRP) and Revocation protocol using Compressed Certificate Revocation Lists (RCCRL). These protocols are introduced since they argue that standard methods of revocation such as Certificate Revocation Lists (CRLs) causes substantial amount of overhead and requires pervasive infrastructure.

In [7], a novel method for certificate revocation in VANETs is proposed; termed RSU-aided Certificate Revocation (RCR). In this method, the Third Trusted Party (TTP) (i.e. CA) grants secret keys for each RSU which enables it to sign all messages communicated within its range. Whenever a certificate is detected to be invalid; the CA issues a warning message to all RSUs which in turn use broadcast messages to all vehicles in respective ranges in order to revoke the particular certificate and stop all communication with that node. They also explain how silent attacks (i.e. where a node disables message broadcasting feature in order to be camouflaged from the RSU) can be prevented using the RCR.

3.3. Privacy Preservation in VANETs

In [1], a novel approach for privacy preservation is proposed by using of a set of anonymous keys, which have short life-times, that is previously stored in the TPD for a certain amount of time, i.e. a year or several months. Once a key is used it is declared void and cannot be used again and all key distribution and management is performed by the CA of the network. However, they stress on the point that these keys have to be traceable to the driver only in case of emergencies or authority requirements.

The article in [7] addresses the 'conditional' privacy preservation in VANETs. This is a desirable characteristic for VANET because it ensures that recipients are not able to extract senders' personal information; however, authorities are able to do so in cases of accidents or network misuse. They explain why the pseudonym-based approaches are not suitable for VANETs since at each revocation process, the CA is requires to search exhaustively a large database. Moreover, as the network scale grows larger, CRLs become very difficult to manage.

3.4. Identity Based Approaches for VANETs

In [9], an ID-based framework that could achieve privacy and non-repudiation is introduced. The work in [9] also explained why previously proposed ID-based solutions to achieve privacy; such as ring signatures, do not suit VANET environments since it results in 'unconditional privacy'. The latter term refers to the inability to reveal the identity of vehicles under all circumstances; which should not be the case in VANETs. They suggest the use of 'distributed control' where a single authority is unable to reveal drivers' personal information. Instead, they proposed having multiple authorities to participate in a collaborative process in case an identity needs to be revealed for legal reasons.

The framework relies on the pseudonym-based approach to achieve non-repudiation in VANETs. This approach was introduced previously in [1] and it involves preloading vehicles with a set of short-lived keys that cannot be used more than one time, hence

other vehicles are unable to track the identity of particular vehicles. They proposed the addition of a Pseudonym Lookup Table (PLT) that can be used to associate random identifiers (pseudonyms) with the real identity of the vehicle. They also suggest the use of existing wireless infrastructure to perform key revocation processes since there does not exist a dedicated vehicular communication infrastructure. However, the proposed framework assumes the use of Tamper-proof Hardware (TPH) which ensures that the master secret of the TTP is never disclosed.

Although the proposed framework is based on IDBC, they also acquire the use of public or symmetric key cryptography for further communication once mutual authentication has been established between nodes in VANETs. They proposed a method based on ID-based threshold signatures to provide non-repudiation services for authorities in VANETs [9].

4. Our implementation of IDBC in VANETs

This paper proposes the use of identity-based cryptosystem for VANETs as it has a number of distinguished features. Firstly, the TTP has to perform a single task of generating the private key for users after an authentication process is performed. Hence, it does not keep any records binding keys to users and once the keys are distributed which reduces the overhead on the TTP. This coincides with the infrastructure-less nature of VANETs since there is no need for Certificate Authorities (CA) or Key Distribution Centers (KDC). Secondly, all security activities (i.e. encryption, decryption, signing and verifying) are performed by nodes without intervention of the TTP which reduces the communication delays and overhead. This will ensure real-time responses for VANET communication as it is a major requirement in such networks. Moreover, assuming that the TTP is fully-trusted, personal information about a particular vehicle will not be exposed unless absolutely required by authorities (e.g. in case of accident investigation); which ensure that conditional privacy is provided.

Figure 1 illustrates deploying Identity-Based Encryption (IDBE) in a VANET. The public key of a node can be a combination of its plate number and license registration number (e.g. $X^{public} = (plate\ number\ ||\ license\ registration\ number)$. The TTP can be any governmental organization (e.g. the Road & Transportation Authority; RTA), and it should handle the process of issuing private keys for nodes (i.e. vehicles) after they have been authenticated. The process of authentication of vehicles can be similar to the methods used by authorities today; i.e. presenting identification documents to prove that you are the owner of the vehicle. The underlying security framework uses IDBC as a security measure.

When two nodes wish to communicate as shown in the figure, the sender X uses the public key of the recipient Y, which is publicly known since it is a unique identifier such as an email address to encrypt the message and send it via the communication protocols in use. Upon receiving the encrypted message, the recipient uses its private key (which was previously extracted from the TTP) to decrypt the message and obtain the original plaintext.

Figure 2 describes the process of the proposed IDBC system. There are 4 stages for the system: The *setup* stage where all system parameters are initialized and then the public/private key pair of the TTP is computed. Next is the *extract* stage where the user's private key is computed. Then, at the *encryption* stage the encryption key is used to encrypt the plaintext message using the Blowfish encryption scheme [9]. Finally, in the *decryption* stage, the cipher is decrypted using the Blowfish decryption scheme.

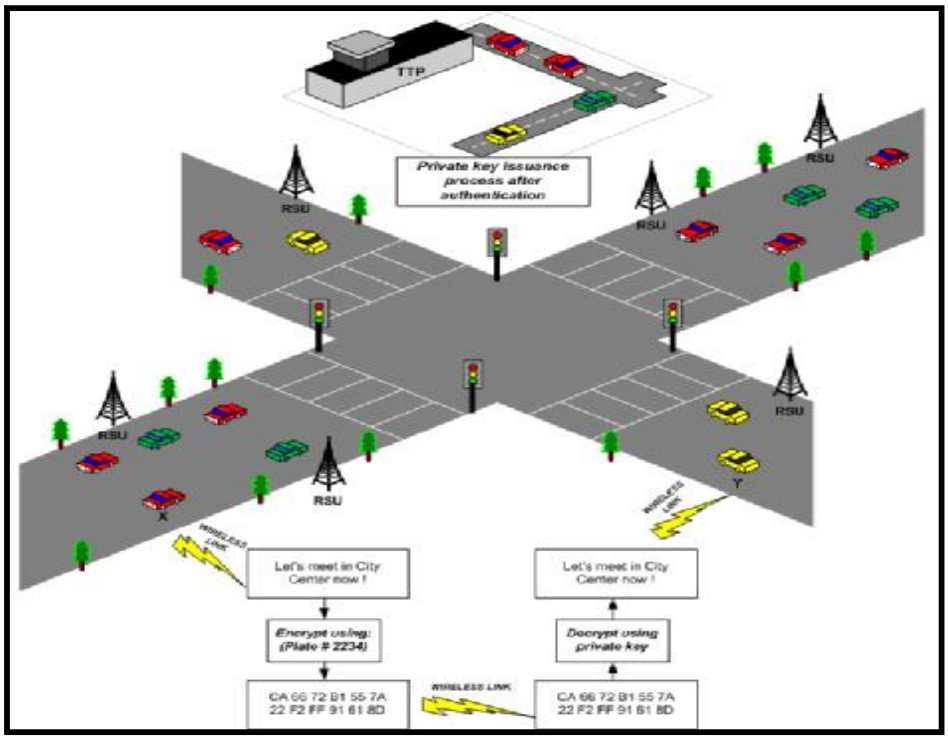

Figure 1: How IDBC can be deployed in VANETs

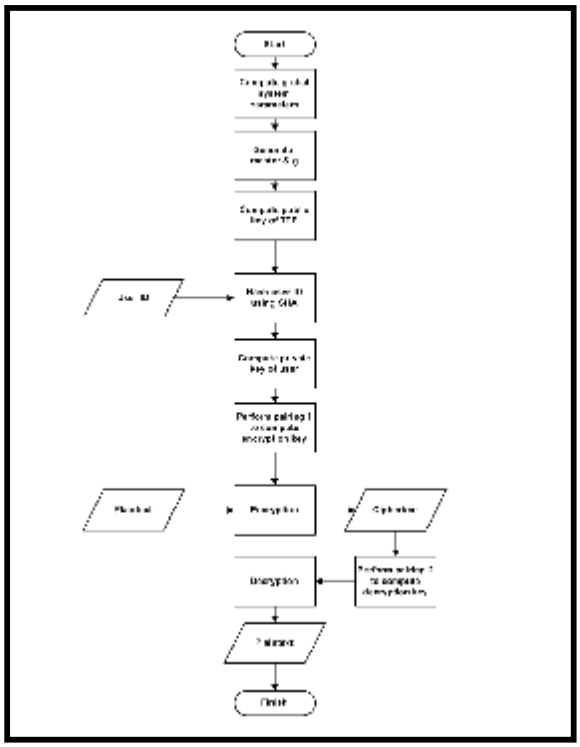

Figure 2: The Functionality of IDBC system

5. Conclusion

This paper surveyed VANETs and their applications and highlighted the major challenges facing such networks. It also reviewed previous schemes proposed in order to provide security and privacy for VANETs. It subsequently introduced a new implementation of an IDBC system. The distinguished features of the cryptosystem were described as well as the algorithms used throughout the process. Other features of the IDBC and more rigorous testing will be the subject of future work.

References

[1] M. Raya, P. Papadimitratos, J. Hubaux, "Securing vehicular communication", IEEE Wireless Communication, Vol. 13, pp. 8-15, October 2006.

[2] TracNet System, http://www.kvh.com/ as of March 9th 2009.

[3] Standard Documentation of Dedicated Short Range Communication (DSRC),http://www.standards.its.dot.gov/Documents/advisories/dsrc_advisory.htm, as of March 9th 2009.

[4] K. Bilstrup, "A Survey regarding wireless communication standards intended for high-speed vehicle environment", School of Information Science, Computer and Electrical Engineering, Halmstad, Sweden, SE-

30118, 2007. https://dspace.hh.se/dspace/handle/2082/2391 as of 28th March 2009.

[5] IEEE Projects Time-line, http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm, last modified: September 2008

[6] E. Maiwald, *Fundamentals of Network Security*, Illinois: McGraw Hill, 2004.

[7] P. Golle, D. Greene and J. Staddon, "Detecting and correcting malicious data in VANETs", in Proceedings of First ACM Workshop on Vehicular Ad-hoc Networks, pp. 29-37, 2004.

[8] J. Haubaux, S. Capkun and J. Luo, "The security and privacy of smart vehicles", IEEE Security & Privacy, Vol. 2, pp. 49-55, May-June 2004.

[9] P. Kamat, A. Baliga amd W. Trappe, "An Identity-based security framework for VANETs", in Proceedings of 3rd international workshop on Vehicular ad hoc networks, pp. 94-95, 2006.

[10] The Blowish Encryption Scheme, http://www.schneier.com/blowfish.html, as of March 9th 2009.