International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:10, No:6, 2016

VANETs: Security Challenges and Future Directions

Jared Oluoch

Abstract—Connected vehicles are equipped with wireless sensors that aid in Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communication. These vehicles will in the near future provide road safety, improve transport efficiency, and reduce traffic congestion. One of the challenges for connected vehicles is how to ensure that information sent across the network is secure. If security of the network is not guaranteed, several attacks can occur, thereby compromising the robustness, reliability, and efficiency of the network. This paper discusses existing security mechanisms and unique properties of connected vehicles. The methodology employed in this work is exploratory. The paper reviews existing security solutions for connected vehicles. More concretely, it discusses various cryptographic mechanisms available, and suggests areas of improvement. The study proposes a combination of symmetric key encryption and public key cryptography to improve security. The study further proposes message aggregation as a technique to overcome message redundancy. This paper offers a comprehensive overview of connected vehicles technology, its applications, its security mechanisms, open challenges, and potential areas of future research.

Keywords—VANET, connected vehicles, 802.11p, WAVE, DSRC, trust, security, cryptography.

I. Introduction

THE ubiquity of wireless devices and recent advancements in Information and Communication Technology (ICT) have spawned the concept of connected vehicles. This revolutionary Intelligent Transportation System (ITS) enables vehicles to form a network called Vehicular Ad Hoc Networks (VANETs). In this network, vehicles connect with mobile devices, Global Position Systems (GPS), routers, and roadside infrastructure to exchange information among themselves. These devices have sensors that detect obstacles [1]. Connected vehicle technology has the potential to improve transport efficiency, reduce traffic congestion, and provide infotainment to road users.

Vehicle to Vehicle (V2V) communication enables vehicles within a communication range to exchange wireless data regarding position, speed, and location to avoid potential hazards. V2V communication for safety reduces road crashes by helping vehicles to: 1) Sense threats and hazards, with 360 degrees awareness of the position of other vehicles. 2) Issue driver warning. 3) Take preemptive action to mitigate crashes [2]. Fig. 1 shows VANET architecture.

Car companies are currently working towards developing connected vehicles technology. In the United States, some states have passed legislations that would allow autonomous vehicles to be driven in roads. The deployment of connected vehicles on roads appears imminent. The United States Department of Transportation (USDOT) is planning to make it a requirement for vehicles to be equipped with VANET technologies.

J. Oluoch is with the Department of Engineering Technology, University of Toledo, Toledo, OH, 43606 USA, Phone 419-530-3272 (e-mail: jared.oluoch@utoledo.edu).

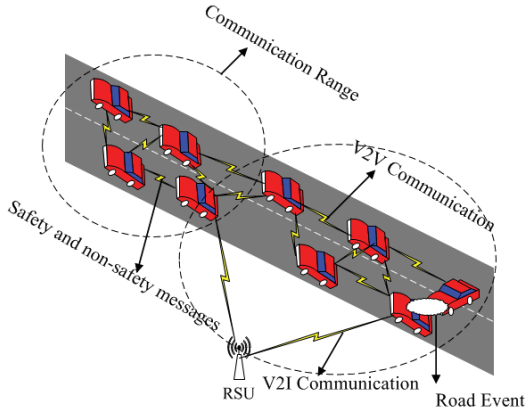

Fig. 1 VANET architecture represents V2V and V2I communication

Despite the promise of connected vehicles as an enabling technology for road safety, security concerns still exist. Existing solutions for VANET security fall in two categories: ID based cryptography and group signatures.

A. ID Based Cryptography

Public key cryptography solutions for security in connected vehicles abound. Kamat et al.,[3] presented an elaborate identity-based cryptographic scheme for VANETs. A Trusted Authority (TA) produces a master secret key for the base station and secret keys corresponding to vehicle IDs. The TA also provides each vehicle with a public certificate which includes the vehicle's public key and private key. The base station issues pseudonyms to vehicles with valid certificates. Hu and Laberteaux [4] proposed an asymmetric key mechanism that generates a long chain of keys to sign messages. When a sender signs a message, the sender uses each key for a short period of time. Keys that are expired are publicly revealed. Choi and Jung [5] presented a solution that uses a third party ID and self-generated public keys to verify a vehicle's ID. In the scheme proposed by [6], vehicles are assigned anonymous key pairs that are periodically renewed. Only the CA has knowledge of the keys. In a similar approach by [7], pseudonyms are generated for vehicles to sign messages to protect the identity of vehicles.

Alternatives to centralized key infrastructure use distributed mechanisms to generate keys. Cabarello *et al*., [8] proposed an authentication scheme in which vehicles verify the public keys of other vehicles on their own. Each node chooses the public certificate of its local store through an algorithm. Each node uses a mechanism to convince another node of its possession

of a secret key. Kumar *et al*., [9] proposed an elaborate key management design that incorporates a Bayesian Coalition Game (BCG) and Learning Automata (LA). Each vehicle in the network is considered as an automaton. Symmetric keys are exchanged among vehicles, and a hash function is implemented. Misbehaving vehicles are punished by revoking their certificates, while honest vehicles get rewards.

Other schemes group vehicles into clusters for security, reliability, or efficient routing [10]-[12]. Similarly, [13] divide nodes into clusters with good connectivity and high stability. Cluster heads are elected depending on their mobility and trust level.

B. Group Signatures

Privacy preservation is an important security requirement for connected vehicles. To achieve this objective, group signature schemes can be utilized for maximum benefits. The seminal work on group signatures was presented by [14]. The central idea of their scheme is as follows: Entities form a group and only members of a particular group can sign messages. When an entity receives a signed message, the entity can verify the validity of the signature but cannot know who signed the message. A group manager can open the signature to reveal who signed the message.

Tajeddine *et al*., [15] divide nodes into groups with each group member accountable to a group manager. When a group member signs a message, the identity of the signer is concealed and only the group manager has knowledge of the signer's ID. Outsiders members of a group can neither forge certificates nor sign messages with a group they do not belong to. Guo *et al*., [16] presented a group signature scheme where signers of a message are anonymous, and two messages signed by the same entity are not linkable. In the scheme by [17], an entity sends a message on behalf of the group using the group's private key. The RoadSide Unit distributes the group private key to all vehicles in its coverage area. Other group signature schemes for VANETs have been proposed by [18]-[20].

While cryptographic solutions exist for connected vehicles, there does not exist adequate literature that discuss the underlying technologies of VANETs, their uniqueness, characteristics, and open challenges. With the imminent deployment of connected vehicles technology, there is need to provide a state of the art overview of this promising technology, and the challenges ahead. This paper provides a thorough discussion of existing security solutions for VANETs, their applications, characteristics, desired features, and an application hierarchy for VANETs.

The rest of this paper is structured as follows. Section II discusses communication standards in VANETs. Section III discusses unique properties and desirable features of VANETs. Section IV describes VANET applications. Section V points to future directions. Section VI concludes the paper.

II. Communication Standards in VANETs

The US Department of Transportation (USDOT) has designed Dedicated Short Range Communication (DSRC) as the communication media of choice for inter-vehicular communication. The US Federal Communication Commission (FCC) specifically assigned a spectrum of 75 MHz in the 5.9 GHz band for DSRC in the United States [21]. USDOT settled on DSRC for connected vehicles communication because of its secure wireless interface, tolerance for multi-path transmissions, robustness against extreme weather conditions, and support for vehicle to vehicle and vehicle to infrastructure communication [21]. Moreover, DSRC is preferred over unlicensed Wi-Fi beacuse of its fast network acquisition, low latency, high interpretability, priority for safety applications, and security [21].

TABLE I
WAVE Protocol for VANETs

Protocol	Layer	Application
IEEE 802.11p	Physical	Wireless Medium
IEEE 802.11p	MAC	MAC & PHY Mapping
IEEE 1609.4	MAC Sub Layer Extension	Multi-channel Operation
IEEE 1609.3	Network & Transport	Network standards
IEEE 1609.2	Network & Transport	Secure Message
IEEE 1609.1	Application	Basic Message Alerts

Wireless Access in Vehicular Environment (WAVE) protocols provide the communication infrastructure for connected vehicles. WAVE is defined by IEEE 802.11p protocol, and IEEE 1609.x protocols. Their operations are structured according to the internet protocol stack. Table I shows the layered architecture of WAVE. IEEE 802.11p operates at the physical and data link layers. IEEE 1609.x operate at the network, transport, and application layers.

1) 802.11p: This protocol is an enhancement of 802.11a with a focus on the physical and MAC layers to achieve low latency and high reliability over short radio communication links [22]. It operates both at the physical and MAC layers. It provides direct interface with wireless medium and mapping between MAC and physical data. At the MAC layer, it provides media access rules and helps in multi-channel operations [23]. 802.11p provides security through authentication and encryption of confidential messages.

It is assumed that all vehicles will be registered by a Motor Vehicle registration unit. This would give vehicles their MAC IDs. Alternatively, Vehicle Identification Numbers (VINs) can be used as the MAC addresses for vehicles. Vehicles will acquire their IP addresses upon joining the network. Vehicles will be identified by their MAC addresses, IP addresses or publicly issued IDs.

2) IEEE 1609.4p: Support for multi-channel operations is accomplished through time division such that radios can switch alternatively between different channel intervals. The two channels are: Control Channel (CCH) and Service Channel (SCH). Continuous safety messages are channeled through CCH, while other applications are channeled through SCH [24].

3) IEEE 1609.3p: This protocol defines network and transport layer services. IP addressing and routing take place here.

4) IEEE 1609.2p: This protocol defines secure message exchanges and encryptions.

5) IEEE 1609.1p: This protocol defines formats for basic message alerts and probe vehicle messages.

An improvement to IEEE 1609.x is currently under development. According to [25], these improvements include: 1) Draft IEEE 1609.5 to manage communication between vehicle to vehicle and vehicle to infrastructure. 2) Draft IEEE 1609.6 to provide remote management between On Board Units (OBUs) and RoadSide Units (RSUs). 3) IEEE Std 1609.11 for secure electronic payments. 4) IEEE Std 1609.12 for specifying the allocation of value identifiers in WAVE.

III. Desired Features for VANETs

VANETs are characteristic by certain distinct features. First, contact of vehicles is ephemeral. Second, network topologies that are formed by vehicles change rapidly. Third, safety messages require real-time dissemination. However, the large nature of VANETs and communication overhead make this quite a challenge. Finally, because it is a relatively new technology, interpretability of equipment among different vendors is a big concern [25].

Connected vehicles must have certain desired features to enhance security, privacy, and trust. Zhang [26] discussed some of the features in his work. This section discusses in depth the desired properties for connected vehicles.

Message Confidentiality: Only the intended recipient should be able to read the message. An attacker who intercepts the encrypted message should not decipher the original plain text message.

Message Integrity: A message in transit should not be altered. If the message is altered, the receiver should detect that the message was indeed altered.

Authentication: Through public key cryptography, the receiver is able to verify the identity of the sender and the source of the message.

Non-repudiation: The sender cannot deny that it sent the message.

Privacy Preservation: The identity and location of the sender is protected through use of pseudonyms and other mechanisms. Privacy violation in connected vehicles is possible through three mechanisms. 1) Finger print extracting through Radio Frequency (RF) signals. 2) Protocol identification by means of IP addresses and MAC addresses. 3) Message analysis by looking at the information contained in messages, for example position and speed.

Robustness: The system should defend itself against attacks such as Denial of Service (DOS), sybil, and badmouthing.

Scalability: The system should accommodate additional vehicles in the network without compromising safety, trust, and privacy.

Fault Tolerance: Back up measures are necessary to prevent the network from complete failure in the event of malfunction of some equipment.

Dynamism: The frequent changing nature of roads demands that the connected vehicle network copes with ever-changing road situations. In addition, the system should be able to operate and make decisions even with few vehicles in the network.

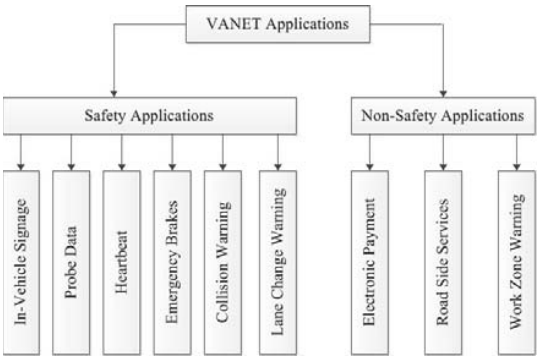

Fig. 2 VANET applications are safety related or non-safety related

Efficiency: Communication and computation need to be done in a manner that does not require a lot of resources.

Decentralization: Communication among vehicles need to occur in a fully distributed manner.

When designing VANET frameworks, it is important to consider trade offs. For example, security mechanisms require authentication and identity. Therefore, privacy can be overlooked in this scenario. Likewise, trust for vehicles can be achieved while at the same time violating privacy.

IV. VANET Applications

Applications in vehicular networks are either safety related or non-safety related. Messages in these applications are sent either through vehicle-to-vehicle or vehicle-to-infrastructure. Kenney [23] illustrated how these messages are transmitted in DSRC protocol. This section discusses and refines various applications of VANETs as proposed by [27]. It also includes other materials not proposed by [27]. Fig. 2 shows VANET applications.

A. Safety Applications

Safety applications are time-critical and impact the overall safety of the network.

In Vehicle Signage: The vehicle On Board Unit receives communication from the RoadSide Unit. The message contains information about position, speed, and location of vehicles. The message is sent in either graphical or audible format. The receiving vehicle analyzes the information, and based on the trajectory and its predicted path, takes corrective action.

Probe Data Collection: This applications gathers data around the vehicle, including position; summarizes the data gathered, and provides that data in a snapshot to the RoadSide Unit.

Heartbeat: Sends speed and position data to vehicles every 100 milliseconds.

Electronic Emergency Brakes: This application sends time-critical emergency messages to vehicles in roads.

Approaching Emergency Vehicle: Sends alerts about approaching emergency vehicles that may not be visible to other vehicles in the surrounding environment.

Co-operative Collision Warning: Warns vehicles about imminent collisions.

Lane Change Warning: Vehicles send messages about changing lanes.

B. Non-Safety Applications

These applications are not necessarily safety related, but they help vehicles share information about other road conditions. They also allow road users to get access to entertainment services and toll payment.

Electronics Payment: Sends alerts to vehicles about the availability of toll payment stations and parking slots available.

RoadSide Services Finder: Allows vehicle to find road services such as rest areas and gas stations.

Work Zone Warning: Alerts drivers about work zones in the area.

V. Future Directions

VANETs will be effective if they can ensure security, privacy, and trust for road users. Due to the large number of vehicles, several challenges exist for public key management. First, the certificate revocation list will be very large. In addition, there will be a lot of communication overhead. A solution to this problem is to design a scheme that does not require public key certificates. Symmetric keys can come in handy for VANETs, although they cannot guarantee non-repudiation. A better alternative is to combine both symmetric key encryption and public key cryptography. Another solution is to aggregate messages to avoid redundancy. Secure and efficient aggregation algorithms are necessary for connected vehicles technology. If connected vehicles technology is to gain widespread adoption, skeptical users will have to be convinced that their privacy will not be violated. The question that then arises is this: how can VANETs ensure security and trust without infringing on privacy of road users? Certainly, short-lived anonymous private and public keys seem to be a great solution. More research is needed to verify the validity and effectiveness of this scheme in VANETs. More specifically, how the certificates will get updated and re-filled.

Existing solutions assume RoadSide Units will be universally available in roads. However, there is no guarantee that this will be the case. Therefore, security solutions should be fully distributed such that vehicles authenticate messages through inter-vehicular communication.

More than anything else, intrusion detection methodologies to identify malicious vehicles is a must-have for VANETs. Misbehavior detection frameworks should include position verification, signal strength sensing, and information validation. The scheme must evict all malevolent vehicles and exclude them from contributing to message dissemination. There are currently solutions that can be built on and improved towards this end [13], [28]-[31]. Secure routing is also an important part of VANETs. Future technologies must adopt routing protocols that are not only secure, but also efficient.

VI. Conclusion

This paper presented a comprehensive overview of VANETs. It discussed existing security mechanisms for safety in vehicular environments. In addition, it discussed in details the underlying technology for vehicular communication - WAVE. Moreover, it explained the desired features and characteristics of VANETs. Furthermore, it designed an application hierarchy for VANETs that shows at a glance both safety and non-safety applications. Finally, it highlighted directions for future research in VANETs such as: 1) privacy preservation, 2) secure routing, 3) symmetric key encryption, and 4) public key cryptography.

The contribution of this paper is that it offers an overarching overview of connected vehicles technology, its applications, its security mechanisms, open challenges, and potential areas of future studies. Thus, this paper is as applicable to academic research institutions as it is to the automobile industry.

References

[1] George Dimitrakopoulos. Intelligent transportation systems based on internet-connected vehicles: Fundamental research areas and challenges. In *ITS Telecommunications (ITST), 2011 11th International Conference on*, pages 145–151. IEEE, 2011.

[2] National Highway Traffic Safety Administration. Vehicle-to-vehicle communications for safety, 2015.

[3] Pandurang Kamat, Arati Baliga, and Wade Trappe. An identity-based security framework for vanets. In *Proceedings of the 3rd international workshop on Vehicular ad hoc networks*, pages 94–95. ACM, 2006.

[4] Yih-Chun Hu and Kenneth P Laberteaux. Strong vanet security on a budget. In *Proceedings of Workshop on Embedded Security in Cars (ESCAR)*, volume 6, pages 1–9, 2006.

[5] Jaeduck Choi and Souhwan Jung. A security framework with strong non-repudiation and privacy in vanets. In *Consumer Communications and Networking Conference, 2009. CCNC 2009. 6th IEEE*, pages 1–5. IEEE, 2009.

[6] Maxim Raya and Jean-Pierre Hubaux. The security of vanets. In *Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks*, pages 93–94. ACM, 2005.

[7] Giorgio Calandriello, Panos Papadimitratos, Jean-Pierre Hubaux, and Antonio Lioy. Efficient and robust pseudonymous authentication in vanet. In *Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks*, pages 19–28. ACM, 2007.

[8] Cándido Caballero-Gil, Pino Caballero-Gil, and Jezabel Molina-Gil. Mutual authentication in self-organized vanets. *Computer Standards & Interfaces*, 36(4):704–710, 2014.

[9] Neeraj Kumar, Rahat Iqbal, Sudip Misra, and Joel JPC Rodrigues. An intelligent approach for building a secure decentralized public key infrastructure in vanet. *Journal of Computer and System Sciences*, 81(6):1042–1058, 2015.

[10] Chen Chen, Jie Zhang, Robin Cohen, and Pin-Han Ho. A trust modeling framework for message propagation and evaluation in vanets. In *Information Technology Convergence and Services (ITCS), 2010 2nd International Conference on*, pages 1–8. IEEE, 2010.

[11] Luciano Bononi and Marco Di Felice. A cross layered mac and clustering scheme for efficient broadcast in vanets. In *Mobile Adhoc and Sensor Systems, 2007. MASS 2007. IEEE International Conference on*, pages 1–8. IEEE, 2007.

[12] Luciano Bononi and Carlo Tacconi. Intrusion detection for secure clustering and routing in mobile multi-hop wireless networks. *International journal of information security*, 6(6):379–392, 2007.

[13] Hichem Sedjelmaci and Sidi Mohammed Senouci. An accurate and efficient collaborative intrusion detection framework to secure vehicular networks. *Computers & Electrical Engineering*, 43:33–47, 2015.

[14] David Chaum and Eugène Van Heyst. Group signatures. In *Advances in CryptologyEUROCRYPT91*, pages 257–265. Springer, 1991.

[15] Ayman Tajeddine, Ayman Kayssi, and Ali Chehab. A privacy-preserving trust model for vanets. In *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on*, pages 832–837. IEEE, 2010.

[16] Jinhua Guo, John P Baugh, and Shengquan Wang. A group signature based secure and privacy-preserving vehicular communication framework. *Mobile Networking for Vehicular Environments*, 2007:103–108, 2007.

[17] Yong Hao, Yu Cheng, and Kui Ren. Distributed key management with protection against rsu compromise in group signature based vanets. In *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*, pages 1–5. IEEE, 2008.

[18] Xiaoting Sun, Xiaodong Lin, and Pin-Han Ho. Secure vehicular communications based on group signature and id-based signature scheme. In *Communications, 2007. ICC'07. IEEE International Conference on*, pages 1539–1545. IEEE, 2007.

[19] Albert Wasef and Xuemen Shen. Efficient group signature scheme supporting batch verification for securing vehicular networks. In *Communications (ICC), 2010 IEEE International Conference on*, pages 1–5. IEEE, 2010.

[20] Yipin Sun, Zhenqian Feng, Qiaolin Hu, and Jinshu Su. An efficient distributed key management scheme for group-signature based anonymous authentication in vanet. *Security and Communication Networks*, 5(1):79–86, 2012.

[21] United States Department of Transportation. Connected vehicles dedicated short range communications frequently asked questions, 2015.

[22] AS Chekkouri, A Ezzouhairi, and S Pierre. Connected vehicles in an intelligent transport system. *Vehicular Communications and Networks: Architectures, Protocols, Operation and Deployment*, page 193, 2015.

[23] John B Kenney. Dedicated short-range communications (dsrc) standards in the united states. *Proceedings of the IEEE*, 99(7):1162–1182, 2011.

[24] Qi Chen, Daniel Jiang, and Luca Delgrossi. Ieee 1609.4 dsrc multi-channel operations and its implications on vehicle safety communications. In *Vehicular Networking Conference (VNC), 2009 IEEE*, pages 1–8. IEEE, 2009.

[25] Mohamed Nidhal Mejri, Jalel Ben-Othman, and Mohamed Hamdi. Survey on vanet security challenges and possible cryptographic solutions. *Vehicular Communications*, 2014.

[26] Jie Zhang. A survey on trust management for vanets. In *Advanced Information Networking and Applications (AINA), 2011 IEEE International Conference on*, pages 105–112. IEEE, 2011.

[27] The VII Consortium. Final report:vehicle infrastructure integration proof of concept. *US Department of Transportation*, page 193, 2009.

[28] Uzma Khan, Shikha Agrawal, and Sanjay Silakari. Detection of malicious nodes (dmn) in vehicular ad-hoc networks. *Procedia Computer Science*, 46:965–972, 2015.

[29] Omar Abdel Wahab, Hadi Otrok, and Azzam Mourad. A cooperative watchdog model based on dempster–shafer for detecting misbehaving vehicles. *Computer Communications*, 41:43–54, 2014.

[30] Carlos Gañán, Jose L Muñoz, Oscar Esparza, Jorge Mata-Díaz, and Juanjo Alins. Epa: an efficient and privacy-aware revocation mechanism for vehicular ad hoc networks. *Pervasive and Mobile Computing*, 2014.

[31] Esther Palomar, José M de Fuentes, Ana I González-Tablas, and Almudena Alcaide. Hindering false event dissemination in vanets with proof-of-work mechanisms. *Transportation Research Part C: Emerging Technologies*, 23:85–97, 2012.