Security in VANETs

Mohan Li mohan.li (at) wustl.edu (A paper written under the guidance of Prof. Raj Jain)

Download 

Abstract:

Vehicular Ad-hoc Networks (VANETs) are gaining growing interest and research efforts over recent years for it offers enhanced safety and enriched travel comfort. However, security concerns that are either general seen in ad-hoc networks or unique to VANET present great challenges. This paper surveys recent advances in research that aim to strengthen security from an architectural and systematic approach. Proposals on specific security issues are also presented and their key results summarized.

Keywords:

VANET Security, Smart Vehicle, Security Attacks, Defensive Mechanisms, Position Detection, Trust Grouping, User Privacy, Security Metrics.

Table of Contents:

1. Introduction: VANET State of the Art

In recent years, there have been growing interest and research efforts in the area of Vehicular Ad-hoc Networks (VANET) because of the variety of services it can offer. These services fall into the categories of safety applications and non-safety applications. Safety is one of the most important goals of VANET since enhanced

safety reduces accidents and therefore can improve traffic conditions and even save lives. Besides safety, other services such as Internet access, weather forecast and geo-location information can enrich travel experience by providing travel comfort, convenience and infotainment.

Committees are devoting efforts to finalize standards for VANET. These standards include IEEE 1609.x, 802.11p and Wireless Access in Vehicular Environment (WAVE). WAVE is a layered architecture for devices complying IEEE 802.11 to operate on Dedicated Short Range Communication (DSRC) band. The IEEE 1609 family defines the architecture and the corresponding protocol set, services and interfaces that allow all WAVE stations to interoperate within the VANET environment. The WAVE architecture also defines the security of message exchange. Together the WAVE standard family forms the basis to implement a wide range of VANET applications across domains such as security, enhanced navigation, automatic tolls and traffic alerts, etc. The different standards of the 1609 WAVE architecture and their integration into the OSI reference model are summarized in figure 1.

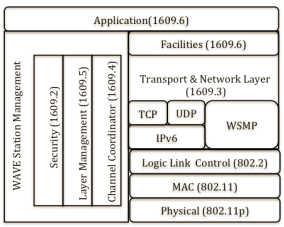

Figure 1. WAVE Architecture and Protocol Stack. [IEEE 1609.0-2013]

In the United States, FCC specifies the DSRC spectrum to be from 5.850 GHz to 5.925 with seven 10 MHz wide channels numbered 178, 172, 174, 176, 180, 182 and 184. To maximize the interoperability and the speed up the standardizations, the use of the DSRC band license-free in the sense that a license is not needed but the use of the spectrum is limited to strict rules. As shown in figure 2, channel 178 in the central is the control channel (CCH). Other 2 extreme channels 172 and 184 are reserved for future safety applications such as accident avoidance. Specifically, channel 172 is reserved for high availability and low latency applications while channel 184 is reserved for high power and public safety applications. The rest 4 channels are service channels (SCH) that can be used for both safety and non-safety applications. The rationale behind such bandwidth allocation with special focus on safety indicates the primal importance of safety for VANET applications.

Figure 2. DSRC Spectrum Allocation.

The architecture of VANET spans across various hardware and software components. Two major types of devices are On Board Unit (OBU) and Road Side Unit (RSU). OBUs are mounted on vehicles whereas RSU are deployed along roadside as infrastructure. Accordingly, two major types of communication in VANET are Vehicle-to-Vehicle (V2V) where vehicles communicate directly with each other and Vehicle-to-Infrastructure (V2I) where vehicles communicate with nearby infrastructure.

In VANET, a node can be a vehicle with a radio system operating in the DSRC channels. The node can be also a roadside equipment to communicate with mobile ad hoc vehicular nodes. Such roadside units serve as gateways to provide access to infrastructures for mobile nodes. We refer to the radio system on vehicular node as On Board Unit (OBU) and the unit fixed to roadside as Road Side Unit (RSU).

The above VANET architecture and communication model are illustrated in figure 3. The main component of the ad-hoc part of VANET is vehicles equipped with sensors, the OBU and the Trusted Platform Module (TPM). On the other hand, the infrastructure part is comprised of the manufacturers, Trusted Third Party (TTP), legal authorities as well as service providers. In the infrastructure part, the RSU serves as a bridge between the infrastructure environment and the ad-hoc environment.

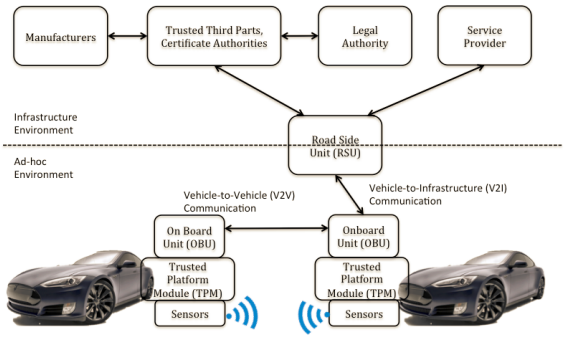

Figure 3. VANET Components and Communication Model. [Mejri14]

The vehicles in VANET are envisioned to be smart in the following perspectives. First, they should incorporate the basic set of sensors such as front and rear radar that receive extra information from surroundings that the human driver is unable to perceive. Secondly, positioning systems such as the Global Positioning System (GPS) are also found essential for driving assistances. Finally, a smart vehicle should also be equipped with a communication system with potentially multiple interfaces, a central computing system and an Event Recording Device (ERD) whose functioning is similar to the black box of an aircraft. There are also proposals stressing that a smart vehicle should also be equipped with Electronic License Plates or Electronic Chassis Number to better represent the identity of the vehicle and easy the verification and logging process. [Samara10] Figure 4 illustrates aforementioned smart vehicle model.

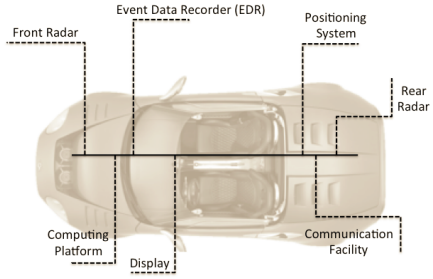

Figure 4. Envisioned Smart Vehicle Prototype. [Mejri14]

The rest of this article is organized as follows. Section 2 overviews the security issues and classifies the threats and attacks in VANET. Section 3 introduces proposals that try to enhance vehicular network security from an architectural perspective including works on general cryptographic solutions, the framework for trust grouping and the system to preserve user privacy base on vehicle identity. Section 4 focuses on specific proposals aiming at solving a particular security issue concerning VANET, including position detection, security measurements and metrics as well as mechanisms to defend VANET. Finally the key results of recent advances are summarized in section 5.

2. VANET Security Overview

This section overviews the security challenges and highlights corresponding approaches proposed recently for VANET. The classification of attacks in VANET is also presented that serve as a basis for following discussion of various security issues.

2.1 VANET Security

Safety in VANETs is of special concern because human lives are constantly at stake whereas in traditional networks the major security concerns include confidentiality, integrity and availability none of which involves primarily with life safety. Vital information cannot be neither modified nor deleted by an attacker. Nonetheless, security in VANET also indicates the ability to determine the driver responsibility while maintaining driver privacy. Information about the vehicles and their drivers within must be exchanged securely and more importantly, timely in that the delay of message exchange may cause catastrophic consequences such as collision of vehicles.

The deployment of a comprehensive security system for VANET is very challenging in practice. A security breach of VANET is often critical and hazardous. Moreover, the nature of vehicular network is highly dynamic with frequent and instantaneous arrivals and departures of vehicles as well as short connection durations. In addition to its dynamic nature and high mobility, the use of wireless media also makes VANET vulnerable to attacks that exploit the open and broadcast nature of wireless communication. [Sumra11]

Cryptographic attacks in VANET are categorized in the next section. Besides general networks security issues, unique security challenges rises because of the unique characteristics of VANET such as high mobility, dynamic topology, short connection duration and frequent disconnections. These unique features bring security issues such as trust group formation, position detection and protection as well as certificate management. Corresponding recent work will be presented in following sections based on the nature of the security issue.

2.2 Classification of Attacks

VANETs are exposed to various threats and attacks. Since the vehicle itself is a sufficient source of electricity, OBU does not have to bear the bottleneck of limited battery life like other mobile devices such as smart phones and wearable devices. Therefore, we can integrate all kinds of processors and chips into the OBU to grant the vehicle workstation-scale computing capability. Unfortunately, this advantage is only one side of the coin. Such computational capability also enables attacks that are computationally intensive and are not feasible in normal ad-hoc networks.

Therefore, it is necessary to classify the attacks in VANET because the unique nature of VANET that brings unique vulnerabilities and various kinds of attacks that requires significant computing. [Merij14] propose the use of a cryptographic based categorization that is easy and plain to understand since the similar approach it takes as done in traditional network security. The classification and typical attacks are presented in figure 5. The classification categorize an attack based the security requirement it tries to compromise. The major categories are threat and attacks on Confidentiality, Integrity and Availability. Other categories include attacks on authentication and accountability.

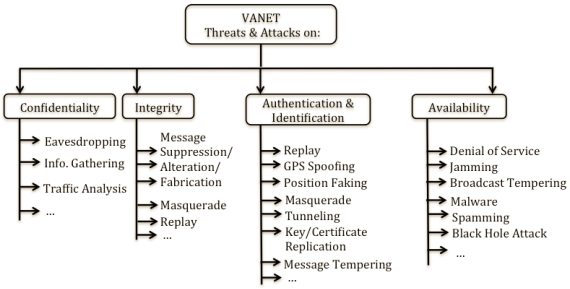

Figure 5. VANET Attacks Classification and Examples. [Mejri14, Issac10]

3. Systematic and Architectural Security Approaches

In this section we focus on recent proposals that aim to enhance VANET security in systematic and architectural approaches. The discussion also includes various attacks and corresponding cryptographic solutions.

3.1 Cryptographic Solutions

The wireless medium used in VANET has drawbacks that can render the network vulnerable to security attacks such as interference, jamming and eavesdropping. In addition, the upper layers of VANET protocol stack reference the Open System Interconnection (OSI) network model. Therefore vehicular networks inherit the its vulnerabilities. Luckily, VANET can also benefit from the existing cryptographic solutions for dealing security attacks.

[Mejri14] have done a very comprehensive survey on the classification of attacks and corresponding solutions. [Issac10] also survey the major security attacks and present the corresponding countermeasures and cryptographic solutions. In comparison, the work summarized in [Mejri14] is more recent and comprehensive. Therefore we summarize the key results from [Mejri14] and complement with the results from [Isaac10].

Table. 1 Major Attacks, Cryptographic Solutions and Proposals. ([Mejri14, Issac10])

Attacks	Targeted Service	Cryptographic Solutions and Proposals
Jamming	Availability	Pseudorandom Frequency Hopping (section 4.3)
Eavesdropping	Confidentiality	Encryption on Sensitive Messages
Traffic Analysis	Confidentiality	Randomizing Traffic Patterns
Dos	Availability	Signature-based Authentication and Access Control
Message Modification	Integrity	Integrity Metrics for Content Delivery (section 4.1)
Brute Force Attacks	Confidentiality	Public Key Schemes
Illusion/Impersonation	Authentication	Trusted Hardware Module (section 3.2)
Position Faking	Authentication	Active Detection Systems (section 4.2)
Illegal Tracking	Privacy	ID-based System for User Privacy (section 3.3)

Major attacks in VANET, targeted security services and the corresponding cryptographic solutions are

summarized in table 1. Many attacks and related VANET security issue will be discussed in detail in the sections indicated in the table. For other major attacks, [Mejri14, Issac10] presents the general cryptographic solutions such as standard public and secret key encryption schemes, signature-based authentication, network access control schemes, etc. The following sections are dedicated to security issues and attacks that are more unique and challenging to VANET such as position faking and illegal tracking, vehicle impersonation and jamming.

3.2 Trust Grouping Framework

One of the core issues of VANET security is exchanging safety messages that keep neighboring vehicles aware of road conditions and hazardous situations. These messages fall into the categories of periodic and event-driven safety messages. Periodic message by its name is exchanged periodically several times per second with neighboring vehicles and it carries information such as vehicle location, speed and direction. Event-driven messages, on the other hand, are issued only when hazardous situations like accidents emerge within proximity. Intuitively, since lives are at stake, event-driven messages should be delivered to all vehicles of concern in as quickly as possible. Because encryption and decryption of the message cause extra time at both ends, the necessity of securing the message is at question. However, a false message or an intentional delay can also cause hazardous situations like collisions. Therefore a tradeoff must be found between speed and security.

In IEEE 1609.2, as a default trial security mechanism, an asymmetric Public Key Infrastructure using Elliptic Curve Digital Signature Algorithm (PKI/ECDSA) is proposed for VANET security. However, ECDSA involves intensive computation and can cause longer delay of safety messages. Therefore researchers have been working on alternative solutions that use symmetric cryptographic schemes. And accordingly, the strength of security is reduced. To balance the need for security and the need for speed, researchers in [Wagan10] come up with a hybrid method that take advantage of both asymmetric and symmetric cryptographic schemes. The method employs hardware that integrates both asymmetric and symmetric cryptography modules for safety messaging. In addition, trust grouping strategies are developed for vehicles in vicinity. As shown in figure 6, there are four major components in this framework: message dispatcher, TPM, group entity and group communication. All these components form the desired trusted group through following interactions.

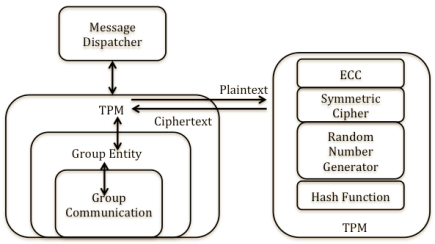

Figure 6. Trust Grouping Framework and TPM architecture. [Wagan10]

The TPM module bears the cryptographic capabilities including asymmetric (ECC) and symmetric encryption, random number generation and hash function. It takes the messages form the message dispatcher and returns the encrypted message with desired security strength and speed. The ECC module also generates signatures for messages together with the hash function. Group entity consists of a group leader, usually the RSU, and group members that are vehicular units in vicinity. The leader generates one-time secret session keys and distributes to its members using the asymmetric ECC scheme. Under such framework, the vehicles in the network form trusted groups that use symmetric scheme for message security while preserving the security strength of asymmetric schemes.

3.3 ID-Based Security System for User Privacy

The fundamental security requirements of VANET should include authentication, integrity and nonrepudiation. In some specific scenarios, confidentiality should also be provided against attackers. In addition, userâ€™s privacy such as identity and location history is sensitive information and should be preserved against illegal tracking and user profiling for advertisements. Otherwise it would cause hesitation for users to welcome the convenience of VANET at the price of their privacy. Nonetheless, law enforcement authorities still need some degree of traceability of vehicles and users for liability issues upon accidents or crimes.

Moreover, it is part of the VANET administration to enforce privilege revocation of misbehaved users. While it is fairly simple to deny access of unauthorized misbehavers since their communication requests can be discarded by the neighboring users and roadside unites, preventing the misbehavior of legit users is more difficult and complex because these authorized users posses credentials and can pass through authentication process. Proposals on systems using anonymous credentials during authentication make it even harder to detect misbehavior of legit users.

[Sun10] propose an identity-based security system for VANET that can effectively solve the conflicts between privacy and tractability. The system uses a pseudonym-based scheme to preserve user privacy. It employs a threshold signature-based scheme to enable tractability for law enforcements. The integral part of the system is the privacy-preserving defense scheme that leverages the authentication threshold. Any extra authentication beyond the threshold will indicate misbehavior and result in revocation of the userâ€™s credentials. Besides, the scheme employs a dynamic accumulator for the authentication thresholding that places further restrictions beyond the threshold on other communicating users. This is particularly attractive to service providers since they can achieve better efficiency of their services.

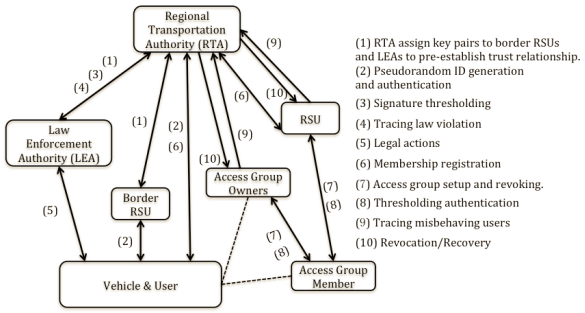

Figure 7. Interactions of the ID-based Security System. [Sun10]

Figure 7 depicts the entities and their interactions in the ID-base system. The arrows indicate the direction of packet flow or physical communications. The details of message exchange of each arrow are numbered and explained on the right side. It is worthy noting that vehicle users are further split into members and access group owners because only group owners can access RSUs. The ID-based cryptosystem facilitates further design of an efficient communication and storage schemes. Through the security and efficiency analysis, the system is shown to satisfy the security objectives including preserving user privacy, enable traceability and nonframeability with desirable efficiencies.

4. Proposals on Specific Security Challenges

This section discusses the proposals that focus on a specific area of VANET security such as modeling attacks,

position detections, and integrity measurement as well as anti-jamming strategies.

4.1 Integrity Metrics for Content Delivery

Content delivery is one of the core services of VANET applications. It should provide timely and accurate information for drivers in order to enhance safety and enrich travel experiences. Due to the distributed, wireless and open nature of vehicular network, its content delivery faces serious security challenges. And common security metrics are needed to measure the effectiveness of VANET security measures and thusly assuring userâ €™s confidence in adopting and participating in the network.

[Azogu12a] propose an Asymmetric Profit-Loss Markov (APLM) model that measures the integrity level of the security schemes for VANET content delivery. The model took a black-box approach to document the â €œprofitâ€ and â€œlossâ€ of data delivery where â€œprofitâ€ is defined as the successful detection of data corruption and â€œlossâ€ the reception of corrupted data. The model uses Markov chains to record the systemâ €™s ability to adjust itself given profit and loss. The model is asymmetric in that normally the system experiences more loss than profits. Given the measurement by the model as heuristics, integrity schemes for VANET can be optimized to provide better content delivery.

The optimization results in a new integrity scheme for VANET content delivery called VOR4VANET (Voting on Reputation for VANET). The new scheme takes advantage of device-centric approaches through recording the performance history of individual vehicle as its â€œreputationâ€. And it operates locally on individual vehicles in a distributed fashion, making it easy to implement. To further improve the scheme, data-centric approaches, i.e. â €œvotingâ€ is also utilized to complement for the scenario where data discrepancy from a vehicleâ€™s reputation occurs. In such cases, based on the reputation, the integrity of a vehicleâ€™s data is voted on. Despite the novelty of their work, the researchers of [Azogu12a] only provide sample results of their evaluation model and their proposed integrity scheme. Further simulations as well as cost-performance tradeoff are mentioned as future work to validate the effectiveness of the integrity metrics and the resulting scheme.

4.2 Position Detection

There are considerable amount of VANET applications that are position-based such as navigation and weather forecast. Positions of vehicles in VANET are considered sensitive information vulnerable to attackers for abusive purposes. Malicious users can also fake their true positions in order to misbehave. Typical position-based attacks include: dropping packet, inserting bogus packets and replaying packets. [Yan11] propose a novel position detection scheme to prevent position-based attacks. Their intuition came from the general need to form the topology for applications like the alert system for congestion. These applications normally require using all available position detection devices such as radio transceiver and cameras.

As the proverb goes: â€œSeeing is believingâ€. The system employs detectors onboard like radars, cameras and infrared detectors as the virtual â€œeyeâ€ of the vehicle to â€œseeâ€ other surrounding vehicles. On the other hand, the virtual â€œearâ€ of a vehicle can use the radio transceiver to â€œhearâ€ their position coordinates. Then the vehicle can corroborate the real position of the surrounding vehicles through cross-referencing what is â €œseenâ€ and what is â€œheardâ€. Such a novel combination takes advantages of both â€œeyeâ€ devices and â€œearâ€ devices. The scheme also adds a challenge-and-confirm verification process for remote vehicles to make up the weakness of â€œeyeâ€ and â€œearâ€ devices.

The proposed vehicle model uses four types of sources of observations, namely, eye-device data, ear-device data, upcoming (opposite direction) vehicleâ€™s eye-device and ear-device data. Under the position detection scheme, a vehicle will regularly broadcast its positional information and receive such information from its neighbors. Upon receiving positional information from a nearby vehicle, if line of sight is not blocked, the receiver will cross check the accuracy of the information with its own observed eye-device and ear-device data. If line of sight is blocked, the receiver will further request the sender vehiclesâ€™ eye-device and ear-device data about its own position and check with its own speed and location information.

If there is any discrepancy between during these cross checking, the sender vehicle maybe marked as suspicious and untrustworthy. This black listing is done locally and therefore is efficient to implement. On top of local positional security, global positional security can be achieved by collecting local blacklists into a centralize database and periodically broadcasting the regional blacklist for the vehicles traveling in that region. Another way mentioned in [Yan11] to achieve positional security in a larger scope is to exchange blacklists among vehicles in vicinity in an ad-hoc fashion. The researchers run simulations to investigate the contribution of eye-devices and ear-devices and as a major result, the more type of detecting devices used, the more accurate and secure of the positional information detection and exchange as the cost of more energy consumption and computational as well as communicational overhead.

4.3 Defensive Mechanisms

As discussed in previous sections, VANET needs hybrid cryptography schemes to balance the tradeoff between the high computational cost of asymmetric schemes and the low security of symmetric schemes. In addition, active defensive mechanisms like the one proposed in [Prabhakar13] are also essential complements to the passive mechanisms of encryption. For inputs as given security measures of the VANET, the defensive mechanism adopts game theoretic approaches and is comprised of three stages. The first stage uses heuristics based on ant colony optimization to identify known and unknown opponents. In the second stage, Nash Equilibrium is employed for selecting the model for a given security problem. The third stage enables the defensive mechanism to evolve over traffic traces through the game theoretic model from the first stage. Such architecture is shown in figure 8.

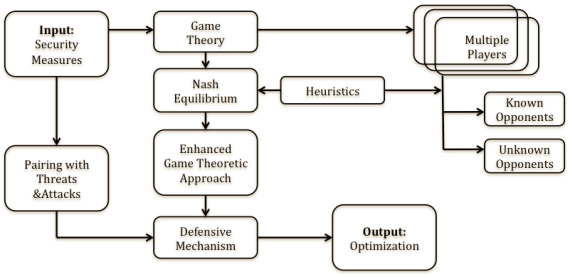

Figure 8. Defensive Mechanism Stage Flowchart. [Prabhakar13]

The defensive mechanism is evaluated from three perspectives: reliability, defensive probabilities and security. Reliability is measured based on the integrity of the received message and the truthfulness of the source. The probability of successful defense is computed based on the optimality of the deployment of traffic control for both static and dynamic traffic conditions. Finally, security takes into consideration of both rural and urban traffic rates since in rural areas the vehicle density is low whereas in urban areas the vehicles density is significantly higher. The simulation results show that the proposed defensive mechanism achieves higher reliability as well as

security in comparison to the existing defensive mechanisms for VANET. The major contributions of this work is its novelty to combine game theory with colonial optimization to complement the security schemes and protect the vehicular network proactively.

Besides general defense of network security, VANET also raises unique challenges to detect jamming and deploy countermeasures because VANET applications are delay-sensitive, making it impractical to adapt anti-jamming systems used in IEEE 802.11 networks such as filtering processes. Currently, few tools available integrate vehicular traffic model with data communication model. Existing proprietary traffic simulators lack feedback mechanism, prohibiting further meaningful study of their impact on wireless signal propagation models and communication protocols.

[Azogu12b] explore security metrics for VANET that can in turn guide the design of defense mechanisms against jamming-style Deny-of-Service attacks. The researchers came up with a new class of anti-jamming defensive mechanisms: hideaway strategy. Compared to traditional channel surfing tactically known as retreat strategy, the effectiveness of this new class is investigated in simulations. The researchers implement a simulation package integrating VANET modules (OBU and RSU) and attack/defense modules along with traffic simulation. The key result shows that the hideaway strategy achieves steady efficiency advantage over traditional anti-jamming schemes. Nonetheless, their work is clearly in its early stage with the designed metrics and the strategy framework. The implementation is mentioned to be the future work to test real world impact of the hideaway prototype.

5. Summary

VANET is an emerging research area with promising future as well as great challenges especially in its security. It shares general ad-hoc network security concerns and faces attacks such as eavesdropping, traffic analysis and brute-force attacks. The unique nature of VANET also raises new security issues such as position detection, illegal tracking and jamming. General cryptographic approaches that apply in VANET include public key schemes to distribute one-time symmetric session keys for message encryption, certificate schemes for authentication and randomizing traffic patterns against traffic analysis. The trust-grouping framework takes a hybrid approach of symmetric and symmetric cryptographic schemes in order to achieve both desirable processing speed and security strength. The pseudo ID-based system is then covered and it uses thresholding techniques for authentication and message signing in order to strike a balance between the need to preserve user privacy and the requirement for traceability for law enforcement authorities.

Besides architectural approaches, proposals on particular security issues of VANET are also discussed. The asymmetric profit-loss Markov model generates security metrics through counting successful detection of corrupted message upon receiving as â€œprofitâ€ and failure as â€œlossâ€. The resulting metrics serve future research by providing network message integrity evaluations. A novel position detection schemes using vehicle radar and camera as â€œeyesâ€ and radio as â€œearsâ€ to collaborate the accuracy and truthfulness of positions of surrounding vehicles. The defensive mechanism for VANET applies game theory and colonial optimization approaches to â€œevolveâ€ the network to improve its security. Finally the hideaway strategy for anti-jamming is introduced and it differs from existing retreat strategy in that it acts reactively instead of actively.

6. List of Acronyms

The acronyms are listed alphabetically.

Acronym	Standing For
CCH	Control Channel
DoS	Denial-of-Service
DSRC	Dedicated Short Range Communication
ECDSA	Elliptic Curve Digital Signature Algorithm
ERD	Event Recording Device
FCC	Federal Communication Commission
GPS	Global Positioning System
OBU	On Board Unit
OSI	Open System Interconnection
RSU	Road Side Unit
SCH	Service Channel
TPM	Trusted Platform Module
TTP	Trusted Third Party
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
VANET	Vehicular Ad-hoc Network
WAVE	Wireless Access in Vehicular Environment

7. References

References are listed in order of their importance and contribution to this article.

[Mejri14] Mohamed Nidhal Mejri, Jalel Ben-Othman, Mohamed Hamdi, â€œSurvey on VANET security challenges and possible cryptographic solutionsâ€, Vehicular Communications, Volume 1, Issue 2, April 2014, Pages 53-66, ISSN 2214-2096, URL: http://dx.doi.org/10.1016/j.vehcom.2014.05.001

[Yan11] Gongjun Yan; Bista, B.B.; Rawat, D.B.; Shaner, E.F., "General Active Position Detectors Protect VANET Security," Broadband and Wireless Computing, Communication and Applications (BWCCA), 2011 International Conference on , vol., no., pp.11,17, 26-28 Oct. 2011. doi: 10.1109/BWCCA.2011.12 URL:http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6103009

[Wagan10] Chowdhury, P.; Tornatore, M.; Sarkar, S.; Mukherjee, B., Wagan, AA; Mughal, B.M.; Hasbullah, H., "VANET Security Framework for Trusted Grouping Using TPM Hardware," Communication Software and Networks, 2010. ICCSN '10. Second International Conference on, vol., no., pp.309, 312, 26-28 Feb. 2010. doi: 10.1109/ICCSN.2010.115 URL: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5437680

[Azogu12a] Azogu, I.K.; Ferreira, M.T.; Hong Liu, "A security metric for VANET content delivery," Global Communications Conference (GLOBECOM), 2012 IEEE , vol., no., pp.991,996, 3-7 Dec. 2012. doi: 10.1109/GLOCOM.2012.6503242 URL: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6503242

[Prabhakar13] Taiming Feng; Lu Ruan, â€œDesign of a Survivable Hybrid Wireless-Optical Broadband-Access Networkâ€, Prabhakar, M.; Singh, J.N.; Mahadevan, G., "Defensive mechanism for VANET security in game theoretic approach using heuristic based ant colony optimization," Computer Communication and Informatics (ICCCI), 2013 International Conference on, vol., no., pp.1,7, 4-6 Jan. 2013. doi: 10.1109/ICCCI.2013.6466118 URL: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6466118

[Sun10] Jinyuan Sun; Chi Zhang; Yanchao Zhang; Yuguang Fang, "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks," Parallel and Distributed Systems, IEEE Transactions on, vol.21, no.9, pp.1227,1239, Sept. 2010. doi: 10.1109/TPDS.2010.14 URL: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=5383352

[Azogu12b] Azogu, I.K.; Ferreira, M.T.; Larcom, J.A.; Hong Liu, "A new anti-jamming strategy for VANET metrics-directed security defense," Globecom Workshops (GC Wkshps), 2013 IEEE, vol., no., pp.1344,1349, 9-13 Dec. 2013. doi: 10.1109/GLOCOMW.2013.6825181 URL: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?&arnumber=6825181

[Isaac10] Isaac, J.T.; Zeadally, S.; Camara, J.S., "Security attacks and solutions for vehicular ad hoc networks," Communications, IET , vol.4, no.7, pp.894,903, April 30 2010. doi: 10.1049/iet-com.2009.0191 URL: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=5454258

[Samara10] Ntuli, N. and S. Han (2012). Samara, G.; Al-Salihy, W.A.H.; Sures, R., "Efficient certificate management in VANET," Future Computer and Communication (ICFCC), 2010 2nd International Conference on, vol.3, no., pp.V3-750,V3-754, 21-24 May 2010. doi: 10.1109/ICFCC.2010.5497419 URL: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?&arnumber=5497419

[Sumra11] Sumra, I.A.; Hasbullah, H.; Manan, J.A., "VANET security research and development ecosystem," National Postgraduate Conference (NPC), 2011, vol., no., pp.1,4, 19-20 Sept. 2011. doi: 10.1109/NatPC.2011.6136344 URL: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?&arnumber=6136344

Last Modified: December 1, 2014
This and other papers on current issues in network security are available online at
http://www.cse.wustl.edu/~jain/cse571-14/index.html
Back to Raj Jain's Home Page