Overview on Security Approaches in Intelligent Transportation Systems

Searching for hybrid trust establishment solutions for VANETs

Christoph Ponikwar, Hans-Joachim Hof

MuSe - Munich IT Security Research Group
Department of Computer Science and Mathematics
Munich University of Applied Sciences (MUAS), Germany
e-mail: christoph.ponikwar@hm.edu, hof@hm.edu

***Abstract*—Major standardization bodies developed and designed systems that should be used in vehicular ad-hoc networks. The Institute of Electrical and Electronics Engineers (IEEE) in America designed the wireless access in vehicular environments (WAVE) system. The European Telecommunications Standards Institute (ETSI) did come up with the "ITS-G5" system. Those Vehicular Ad-hoc Networks (VANETs) are the basis for Intelligent Transportation Systems (ITSs). They aim to efficiently communicate and provide benefits to people, ranging from improved safety to convenience. But different design and architectural choices lead to different network properties, especially security properties that are fundamentally depending on the networks architecture. To be able to compare different security architectures, different proposed approaches need to be discussed. One problem in current research is the missing focus on different approaches for trust establishment in VANETs. Therefore, this paper surveys different security issues and solutions in VANETs and we furthermore categorize these solutions into three basic trust defining architectures: *centralized*, *decentralized* and *hybrid*. These categories represent how trust is build in a system, i.e., in a centralized, decentralized way or even by combining both opposing approaches to a hybrid solution, which aims to inherit the benefits of both worlds. This survey defines those categories and finds that hybrid approaches are underrepresented in current research efforts.**

Keywords–security; security issues; security architectures; VANET; MANET; ITS.

I. Introduction

This paper surveys different security architecture techniques for VANETs used in ITSs. Security plays a significant role in modern Cyber-Physical Systems (CPSs), which include intelligent transport systems. Trust establishment describes how trust is formed, which in return defines the fundamental security architecture of a system. The future of ITS is a networked one where vehicles and infrastructure do communicate to make traffic more efficient and safer. As vehicles are inherently mobile and self containing, the only way to communicate on the move is via wireless technology. Wireless has proven over time that getting security right in wireless technology is hard. An example of security done wrong is the utterly broken WEP technology, which is an acronym for "Wire Equivalent Privacy", but it was never able to fulfill that promise. Not only do security issues in regards to authentication exist but furthermore there are also security issues, like denial of service, replay or spoofing attacks, which vary in severity and easy of exploitability. But overall security in wireless technologies is boiling down to how trust is established and which methods and algorithms are used to secure the trust establishment.

One centralized approach for conveying trust is the mode of operation that is used in telecommunication standards all over the world, i.e., Global System for Mobile Communications (GSM), Code division multiple access (CDMA), Universal Mobile Telecommunications System (UMTS) or Long-Term Evolution (LTE). That mode of operation is building trust based on a shared symmetric secret. Until recently the weaknesses were discussed, like the important dependence of secrecy of this shared secret, but arguments were often discarded because of the needed effort to steal the secret key of each customer and the high security approach network operators supposedly are taking to secure those secrets. The treasure trove of leaked information by former National Security Agency (NSA) contractor Edward Snowden, showed the security community again once more how bad our assumptions were in this regard. As documents provided by the online publication THE INTERCEPT [1] show that American (NSA) and British spy agencies Government Communications Headquarters (GCHQ) managed to steal those important secrets directly from the manufacturer, in this case Gemalto. The theft means, on a technical level, that authenticity and confidentiality of a communication, supposedly secured by those stolen secrets, is compromised. The methods supposedly used to execute that theft raise many questions but this discussion might fit better in a legal or social publication and should not be discussed in this paper. Another rather recently uncovered attack on several banks (ca. 100 banks) around the world (ca. 30 countries) where a so called "Carnbanak cybergang" have stolen an estimated amount of 1 billion United States dollar (USD). While the used malware does not appear to be of very high sophistication, only the weakest trust relationship in computing, between a human and a machine was exploited via spear phishing, the orchestration, endurance and the targeted approach of the attackers where extremely remarkable, as reported by Kapersky Labs [2].

The underestimation, to what length state actors would go to achieve informational advantage in combination with how persistent and patient criminal actors are becoming, previously only attributed to state actors, goes to show how wrong and weak our current assumptions on cybersecurity have been. All central approaches bear the risk of being exploited by targeted attacks on the central trust anchors. And this is why we urge every researcher to reevaluate their assumptions and seek for alternative designs. Both currently developed major standards, IEEE WAVE [3] or ETSI ITS-G5 [4], favor a centralized security architecture, with trust rooting in central authorities, which represent a high value target for attackers to exploit.

Decentralized approaches could be such an alternative, by making such attacks much more risky and costly due to the distribution of trust relations. Distributed trust relations have their own issues, like performance or new attack opportunities not present in centralized architectures. Therefore, the combination of both architectural approaches, in this paper called hybrid approaches, could pose a overall security improvement, especially in the current environment with increasing proliferation of attack and exploitation techniques accessible to criminals and state actors alike. Attacking seams to be easier than defending, this is why we argue a easy to defend security architecture is paramount for any information system or network nowadays, especially in the field of ITSs, which are in focus of this paper.

As stated previously trust establishment can be achieved via a centralized way e.g., a Public Key Infrastructure (PKI), decentralized e.g., a Web of Trust (WoT) or by using a hybrid approach, which tries to combine the benefits of both approaches. Security issues in mobile ad-hoc networks are used to find solution for them and then categorizing those solutions into their general security architecture. We limit ourselves to some of the following major issues in ITS mentioned by various researches like Hubaux et al.[5], Lin et al.[6] or in an already summarized from by Yang [7].

- Impersonating by false, stole identities, Message spoofing or replay attacks
- Tampering with data in-transit
- Send false feedback to silence other vehicles
- Sinkhole attack via false routing information to effectively execute Man-in-the-Middle (MitM) attacks
- Sybil attack by creating virtual sock puppet identities to manipulate voting procedures to the attackers benefit
- An eclipse attack is similar to an sybil attack it specifically tries to split a network by using means of a malicious group of nodes
- Manipulating the network topology and disturbing node by connecting far away segments via a hidden tunnel (wormhole attack)
- Privacy violation caused by continues communication
- Denial of Service (DoS) by jamming signals or overloading specific nodes

In [8], Agrawal et al. present a short overview of different security issues and solutions with their objectives and draw backs. Mishra et al. [9] display a wide array of research effort in regards to security issues and solutions, which they think are important. A detailed introduction into VANETs is given by Raya et al. [10] they furthermore expand on, security issues and solutions in VANETs. Zhang[11] categorizes trust management for VANETs in three models: *Entity-oriented Trust Model*, *Data-oriented Trust Model* and *Combined Trust Model*. We differentiate various approaches to security issues in VANETs into three categories: *Centralized*, *Decentralized* and *Hybrid* as we think these categories describe the way trust is build better.

We define those categories in detail in the following Section II. Thereafter in separate sections we describe eight different security issues, already defined by Yang [7]. Each of these section contains solutions to its security issues, which are categorized according to our definition into: *Centralized*, *Decentralized* and *Hybrid* solutions. A summary of this paper is provided in the last Section III.

II. Analysis

One of the main issues in ad-hoc-communication is trust. It is a basic problem in security to establish so-called trust anchors. Several models for trust management exist. The surveyed approaches with their assigned categories are listed in the summary table I.

Centralized: A central trust model may for example be implemented by a PKI. A PKI consists of one or more Certificate Authorities (CAs) that issue certificates to the participants of the system. The issue of certification may be delegated to Sub-CAs, resulting in a hierarchy of CAs. A certificate of a participant is considered to be legitimate, if it is possible to find a certification path from the certificate to a known and trusted CA. Several (yet unknown) Sub-CAs may be on the certificate path. Per se, all legitimate certificates are considered trusted. Hence, all the known and trusted certificates represent trust anchors for one participant. Using a PKI simplifies trust establishment to secure setup of trust anchors on an instance of the system.

Decentralized: A decentralized trust model may for example be a so WoT. In a WoT scenario, each participant of the whole network is also a CA and may express trust in a certificate of another participant. Each participant keeps a list of other participants of the system that are trusted and another list of participants that are trusted to express trust in other participants. As with the PKI, establishing trust in an unknown participant requires to build a trust path between the unknown participant and oneself. However, as no hierarchy exists, finding such a path is a hard task. Another approach to trust establishment are reputation models. No certificates are issued but the behavior of participants is monitored and trust values are assigned based on different attributes like former or expected behavior. Participants may exchange trust values of each other.

Hybrid: A hybrid trust model is one that makes use for example of a distributed PKI, which assigns identities to participants, mainly for liability reasons. This trust path is only used in case of an accident or when certain conditions are met. But the operational trust between participants is realized via a reputation system and only if enough evidence of bad or malicious behavior was recorded, the PKI infrastructure would step in to permanently revoke or destroy the cryptographic material of the offending node. Hybrid solutions are trying to combine both central and decentral approaches, to get the benefits of both approaches, like somewhat independence of central infrastructure or better privacy features.

A. Impersonation

Defending against replay or whole message spoofing attacks is usually done at a protocol level. If used communication

TABLE I. ANALYSIS OVERVIEW

Security Issues	Centralized	Decentralized	Hybrid	Ref.
Impersonation	[12],[5],[13]	[14],[15]	[16]	II-A
Data Tampering	[17],[12],[10]	[14]	[18]	II-B
Routing Attacks	[19],[20],[21]	[22],[23]	[13]	II-C
Sybil Attacks	[24]	[25],[26]	[27]	II-D
Eclipse Attacks	[28]	[25]	-	II-E
Wormhole Attacks	-	[29],[19]	-	II-F
Denial of Service	[13]	[30]	-	II-G
Privacy Violation	[12],[31],[16],[28],[32]	[17]	[33],[34]	II-H

protocols do not defend against those attacks a communication system, regardless its architecture will be hard to secure. Communication systems usually use some kind of identities to distinguish between different participants. Those identities usually need to be protected against impersonation to sustain distinguishability.

Centralized: In case strong identities are needed like in a system utilizing identity based cryptography [35] Sun et al. [12] propose storing identities in a tamper proof hardware to prevent identity theft. So do Hubaux et al. [5] they store their form of identity, called electronic license plate, in an event date recorder (EDR), similar to a black box in an aircraft. The EDR in return itself should be "protected [...] physically"[5]. Similarly Raya et al. [13] are using a "trusted component" in their protocols to store and protect identity data against theft.

Decentralized: Every participant in a VANET should have its own model of its vicinity and validate every piece of data received, according to Golle et al. [14]. They authenticated communication via public/private key pairs but they are self generated by each node and should be refreshed constantly [14]. Additionally, they propose using "location-limited channels"[15] to distinguish nodes. As an example of a "location-limited channel"[15] is the use of infrared signaling given by Golle et al. [14].

Hybrid: In an approach called "Efficient Decentralized Revocation Protocol"[16] (EDR) Wasef et al. propose a way to revoke trust in identities based on "probabilistic random key distribution technique and a novel pairing-based threshold scheme"[16]. It uses PKI but the revocation process is decentralized and facilitated by voting.

B. Data Tampering

Depending on how nodes are communicating in a VANET, whether it is single hop or multi hop communication, different opportunities arise for data tampering or manipulation. If transmitted data is not integrity protected, any intermediate system or bystander could change the information for its own benefit.

Centralized: One of the more complete approaches was proposed by Li et al. [17]. They based their scheme also on identity based cryptography [35]. But they extended it with blind signatures and one-way hash chains to provide mutual authentication, confidentiality and integrity, while preserving privacy. This approach is similar to that of Sun et al. [12], which also is based on identity cryptography and aims to deliver on the same security requirements [10].

Decentralized: Using a reputation system in conjunction with collecting and querying for additional data, to verify and attest trustworthiness of information is proposed by Golle et al. [14]. Every node builds up his own model of the network around him and validates data against it.

Hybrid: In [18], Zhang et al. present a scheme called "RAISE" a Roadside Unit(RSU)-adied message authentication scheme, which uses keyed-hash message authentication where the secret key is known by the RSU, which in return can therefore attest that the message is authentic. The proposed scheme is compatible with traditional PKI-based systems, further more it makes use of PKI as a fallback mechanism.

C. Routing Attacks

To prevent congestion in ad-hoc wireless environments nodes are listening to its neighbors and if a neighbor is better suited to forward messages it stops rebroadcasting messages. If an attacker could convince a node that he is better positioned, the attacker can silence other nodes. Which would make them effectively disappear from the VANET, so called silencing attacks. Also a vehicular ad-hoc network where bandwidth is limited, and far reaching connections to central systems needed to be routed through long range wireless communication technology like LTE or UMTS. Those communication technologies are expensive to use compared to a node posing as a high speed uplink or gateway reachable via ad-hoc communication, called sinkholing attack. This enables MitM attacks, where a malicious gateway can intercept or even alter the sent and received messages.

Centralized: One of the first secure routing protocols for VANETs were proposed by Eichler et al. [19] called AODV-SEC based on "Ad-hoc On-demand Distance Vector" (AODV). Lu et al. designed the "social-based privacy-preserving packet forwarding" [20] (SPRING) to be resistant against black holing attacks by utilizing road side infrastructure. Relying on PKI for strong identities but giving incentives, based on game theory, to nodes taking part in a mobile ad-hoc network, was proposed by Zhong et al. [21]. Sprite, "a simple, cheat-proof, credit-based system for mobile ad-hoc networks" [21] also needs a central Credit Clearance Service (CCS) to function.

Decentralized: In [22], Huang et al. propose a cluster based intrusion detection system to detect various attacks, among them sinkholing or blackholing. Their approach is focused on detection of those attacks and mitigation is left for the network to handle. The CONFIDANT protocol by Buchegger et al. [23] consist out of four entities present in each node: Monitor, Reputation System, Path Manager and Trust Manager. The Trust Manager collects events via the Monitor and uses the Reputation System to evaluate the events and the result of the evaluation are used by the Path Manager to adjust the rounting, to mitigate attacks like sinkholing.

Hybrid: To detect and respectively mitigate misbehaving nodes Raya et al. [13] propose two methods "Misbehavior Detection System (MDS)" and "Local Eviction of Attackers by Voting Evaluators (LEAVE)". When detecting a misbehaving node, LEAVE is used to degrade the attackers trust until a central certificate authority revokes its certificates. LEAVE is resilient to interference as long as colluding attackers are a minority.

D. Sybil Attacks

When protocols with voting procedures are used or if some kind of collaboration between nodes for making collective group decisions is needed, then a so called sybil attack could be used to influence protocols or decisions. This is done by creating sock puppets that the attacker controls to act on behave of him. In an vehicular environment, if an attacker would like to push the envelope, he and his sock puppets could simulate braking or congestion, and then tricking the victims into believing him. Protocols like the previously mentioned LEAVE Protocol by Raya et al. [13] have a certain threshold to, which they are resilient against a sybil attack. The important factor is the size of the sock puppet group in comparison to the amount of honest nodes.

Centralized: An easy protection against sybil attacks is the use of centrally enforced and distributed strong identities. Identities are created by a central authority and handed down to the nodes prior to their deployment as stated by Piro et al. [24]. This process could be upfront or part of a VANET joining protocol. Either way a central entity knows to whom it has handed a specific identity. With autonomous vehicles at the horizon it may be even more compelling or tempting to use the vehicle identification number as such an id. This approach has many privacy implications, like unique traceable identities, or the central data storage would be a high value target for theft or intrusion.

Decentralized: In [25], Xiao et al. draft a technique called "Basic Signal-Strength-Based Position Verification" [25], which is used to verify the position by a claimer based on the signal strength. This technique is then used after collecting beacon messages to decide based on probability if there is a sybil node nearby and if so a statistic model is used to attribute the sybil nodes to one originating vehicle. Park et al. are using a timestamp based approach to detect sybil attackers [26].

Hybrid: An approach using timestamp series and RSUs issuing certificates was proposed by Park et al. [27]. The RSUs themselves have public private key pairs and a certificate from a central certificate authority. All vehicles must have the public key of the certificate authority pre-installed. Additional vehicles generate their own pair of keys. Similar timestamps series are identified as a sybil attack. To protect against sybil attack each data message must contain current timestamp certificate, RSU certificate, signed data and of course the data itself. If any inconsistencies occur the packets should be dropped. As the authors suggested by themselves [27] this approach is not suited for high traffic and urban scenarios, due to the spatial and temporal difference assumption falling apart.

E. Eclipse Attacks

An eclipse attack utilizes compromised neighbors to influence group decisions. It is also useful when the separation of nodes from other nodes weakens the whole network segment, by degrading the trust in the honest group while improving its own standing in the network. This approach usually eases and strengthens other attacks like DoS II-G.

Centralized: Quick and efficient removal of identified malicious nodes is key in protecting against eclipse attacks. Therefore Wasef et al. [28] proposed, based on a PKI system, not only a novel message authentication approach but also a quick certificate revocations approach to evict the trustworthiness of misbehaving nodes.

Decentralized: Some of the methods used to defend against sybil attacks also could be used to defend against eclipse attacks especially Xiao et al. [25] are trying to suppress sybil attacks in conjunction with opposite traffic flow and their ability to proof that they came from an upstream source.

Hybrid: **-** No hybrid approaches were found in literature.

F. Wormhole Attacks

When an attacker can control two nodes in different VANET segments and has a high speed link between those two, he can mount a so called wormhole attack. Illegal but correct traffic would originate from and to both ends of the tunnel, making vehicles suddenly appear in each others vicinity, while actually being in two remote locations. This type of attack could be the basis for executing other attacks, like sybil II-D, eclipse II-E or denial of service II-G attacks. A wormhole might be used by an attacker, to generate illegal traffic and let the nodes interfere with each trustworthiness in the connected segments, influence voting procedures or even cause a denial of service when the nodes in both segments revoke each others trustworthiness based on wrong positioning information.

Centralized: Assuming global network visibility is achieved, illegal traffic, which would be generated by a wormhole attack could be spotted by roadside units, acting as a sensor. The central network management system should then be able to correlate that the same traffic is visible in two remote locations. Mitigation of such an attack would only be a notice to affected nodes to discard traffic that is not in their vicinity. Most stronger responses like revoking the right to allocate a channel for communication would not harm the attacker in between but the nodes in their respective network segment. This could result in a DoS attack.

Decentralized: In [29], Safi et al. based their effort, like Eichler et al. [19], on the AODV Routing Protocol and enhanced it to include "geographical leashes" that should prevent the forwarding of packets from different geographic areas with additional packet authentication.

Hybrid: **-** No hybrid approaches were found in literature.

G. Denial of Service

Denial of service attacks are often used as distraction or an accompanying attack that should weaken the position of a system to ease the real attack or exploit. This type of issue is one of the harder ones to defend against. Because there are no purely technical means to defend against jamming attacks in wireless communication systems. Types of denial of service attacks include jamming of radio frequencies, traffic flooding or silver bullet attacks, where one specially crafted packet may be able to disrupt service.

Centralized: When a system needs a functioning PKI, like most of the mentioned approaches, or the one from Raya et al. [13]. A DoS attack could me mounted by creating a lot of identities and then report those same identities as malicious or fraudulent. This could result in a flood of certificate revocations, which could lead to DoS when revocation lists get to big or the revocation operation is computational intensive. To mitigate this threat Raya et al. [13] suggested the use of "Compressed Certificate Revocation Lists (RC^{2}RL)" and "Revocation of the Trusted Component (RTC)" protocols.

Decentralized: For VANETs Hamieh et al. [30] described a method to detect on going jamming attacks. They focused on attacks where the jammer is only sending when his hardware is allowed to, he abides the rules of the underlying IEEE 802.11p Standard. Their model is based on time correlation of errors and correct receptions to detect the presence of a jamming attack.

Hybrid: **-** No hybrid approaches were found in literature.

H. Privacy Violation

In a cooperative system where every neighboring node should have all the needed information to make intelligent decisions on its own and for the group, it is clear that all this information needs to be communicated. Therefore, when every node broadcasts his position, trajectory, acceleration, route or other data, basically a profile of the driver could be created. If this data is readable by everybody in the vicinity, somebody just needs to set up an antenna and can now make statistics where and when people are driving, when traveling past him.

Centralized: To protect privacy and making tracking harder most approaches use pseudonyms and rotating them, like [12], [31]. But everybody does it slightly different, Sun et al. [12] are using "preloading [...] pseudonym(s)" whereas Choi et al. [31] use generation of public keys by deriving it from the secret id only known to an authority and the vehicle itself. While still allowing the verification and certification based on time stamps and other public key parameters. But almost all approaches [16], [28], [32], found during our survey are using PKI to guarantee authenticity and non-repudiation. The latter one supposedly for liability reasons.

Decentralized: To preserve privacy Li et al. [17] presented a scheme called "SECSPP" utilizing non interactive identity based cryptography and a blind signature scheme for allowing anonymous usage of RSU services. Anonymous confidential communication between the RSU and vehicles make tracking or eavesdropping harder and more expensive.

Hybrid: A cluster based architecture utilizing PKI, theshold cryptography and location limited side channel [15], like license plate recognition is proposed by Bechler et al. [33] to secure ad-hoc communication, similar to an approach by Zhou et al. [34]. To adapt to different security levels the approach by Bechler et al. [33] supports 4 different modes of operation: no encryption, cluster key encryption, public key directly exchanged and public key certified by a distributed certificate authority, in this case the cluster heads.

III. Conclusion

Some security issues in ITSs are hard or outright impossible to mitigate on a purely technical basis, this is why we did not consider them in our review. Examples for this type of attacks are, jamming or physical tampering. An attacker with a radio frequency jammer can suppress any meaningful communication [5]. Often the solution to physical tampering is to even better tamper proof those devices, like sensors or Electronic Control Units (ECUs). This climaxes often in the inclusion of a Trusted Platform Module (TPM), which shifts the responsibility and trust to the manufactures of those components. But as explained in the introduction I, trust in those supposedly highly secure entities has been shattered in the recent years. Therefore relying on them can be the Achilles heal of a system. Besides those doubts there are many solutions for centralized architectures and some decentralized ones. We were able to find suitable hybrid solutions in the literature for only five out of eight security issues. Often only one hybrid solution could be found for a specific security issue. Our findings are summarized in the Table I. We therefore conclude that hybrid approaches are underrepresented in current research, which might be an indicator that further research is needed or that hybrid approaches appear to be fruitless endeavors. To answer those questions further research, including a comparative study, needs to be conducted. The direction the standardization efforts, by IEEE and ETSI, are heading, is towards centralized architectures with all benefits and weaknesses. Those will set the mark against all other solutions have to prove themselves. Eventually decentralized solutions could be considered for integration in those standards if proven beneficial.

References

[1] J. Scahill and J. Begley. The Great SIM Heist: How Spies Stole the Keys to the Encryption Castle. [Online]. Available: https://firstlook.org/theintercept/2015/02/19/great-sim-heist/ [retrieved: jul, 2015]

[2] Kaspersky Lab HQ. Carbanak_apt_eng.pdf. [Online]. Available: http://25zbkz3k00wn2tp5092n6di7b5k.wpengine.netdna-cdn.com/files/2015/02/Carbanak_APT_eng.pdf [retrieved: jul, 2015]

[3] Intelligent Transportation Systems Committee of the IEEE Vehicular Technology Society, "1609.0-2013 - IEEE Guide for Wireless Access in Vehicular Environments (WAVE) - Architecture," IEEE Std 1609.0-2013, Mar. 2014, pp. 1–78, bibtex: 6755433. [Online]. Available: http://ieeexplore.ieee.org/servlet/opac?punumber=6755431

[4] ETSI TR 102 962, "ETSI TR 102 962 v1.1.1 (2012-02) intelligent transport systems (ITS); framework for public mobile networks in cooperative ITS (c-ITS)," feb 2012, pp. 1–63.

[5] J.-P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," IEEE Security & Privacy Magazine, vol. 2, no. LCA-ARTICLE-2004-007, 2004, pp. 49–55.

[6] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho, and X. Shen, "Security in vehicular ad hoc networks," Communications Magazine, IEEE, vol. 46, no. 4, 2008, pp. 88–95.

[7] W. Yang, "Security in vehicular ad hoc networks (vanets)," in Wireless Network Security. Springer Berlin Heidelberg, 2013, pp. 95–128. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-36511-9_6

[8] A. Agrawal, A. Garg, N. Chaudhiri, S. Gupta, D. Pandey, and T. Roy, "Security on vehicular ad hoc networks (vanet): A review paper," International Journal of Emerging Technology and Advanced Engineering, vol. 3, 2013, pp. 231–235.

[9] B. Mishra, P. Nayak, S. Behera, and D. Jena, "Security in vehicular adhoc networks: a survey," in Proceedings of the 2011 International Conference on Communication, Computing & Security. ACM, 2011, pp. 590–595.

[10] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," Journal of Computer Security, vol. 15, no. 1, 2007, pp. 39–68.

[11] J. Zhang, "A survey on trust management for vanets," in Advanced Information Networking and Applications (AINA), 2011 IEEE International Conference on. IEEE, 2011, pp. 105–112.

[12] J. Sun, C. Zhang, and Y. Fang, "An id-based framework achieving privacy and non-repudiation in vehicular ad hoc networks," in Military Communications Conference, 2007. MILCOM 2007. IEEE. IEEE, 2007, pp. 1–7.

[13] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," Selected Areas in Communications, IEEE Journal on, vol. 25, no. 8, 2007, pp. 1557–1568.

[14] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in vanets," in Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks. ACM, 2004, pp. 29–37.

[15] D. Balfanz, D. K. Smetters, P. Stewart, and H. C. Wong, "Talking to strangers: Authentication in ad-hoc wireless networks." in NDSS, 2002.

[16] A. Wasef and X. Shen, "Edr: Efficient decentralized revocation protocol for vehicular ad hoc networks," Vehicular Technology, IEEE Transactions on, vol. 58, no. 9, 2009, pp. 5214–5224.

[17] C.-T. Li, M.-S. Hwang, and Y.-P. Chu, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks," Computer Communications, vol. 31, no. 12, 2008, pp. 2803–2814.

[18] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "Raise: an efficient rsu-aided message authentication scheme in vehicular communication networks," in Communications, 2008. ICC'08. IEEE International Conference on. IEEE, 2008, pp. 1451–1457.

[19] S. Eichler, F. Dotzer, C. Schwingenschlogl, F. J. F. Caro, and J. Eberspaher, "Secure routing in a vehicular ad hoc network," in Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th, vol. 5. IEEE, 2004, pp. 3339–3343.

[20] R. Lu, X. Lin, and X. Shen, "Spring: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks," in INFOCOM, 2010 Proceedings IEEE. IEEE, 2010, pp. 1–9.

[21] S. Zhong, J. Chen, and Y. R. Yang, "Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks," in INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies, vol. 3. IEEE, 2003, pp. 1987–1997.

[22] Y.-a. Huang and W. Lee, "A cooperative intrusion detection system for ad hoc networks," in Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks. ACM, 2003, pp. 135–147.

[23] S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the confi-

dant protocol," in Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing. ACM, 2002, pp. 226–236.

[24] C. Piro, C. Shields, and B. N. Levine, "Detecting the sybil attack in mobile ad hoc networks," in Securecomm and Workshops, 2006. IEEE, 2006, pp. 1–11.

[25] B. Xiao, B. Yu, and C. Gao, "Detection and localization of sybil nodes in vanets," in Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks. ACM, 2006, pp. 1–8.

[26] A. Patcha and J.-M. Park, "An overview of anomaly detection techniques: Existing solutions and latest technological trends," vol. 51, no. 12, 2007, pp. 3448–3470. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S138912860700062X

[27] S. Park, B. Aslam, D. Turgut, and C. C. Zou, "Defense against sybil attack in vehicular ad hoc network based on roadside unit support," in Military Communications Conference, 2009. MILCOM 2009. IEEE. IEEE, 2009, pp. 1–7.

[28] A. Wasef and X. Shen, "Maac: Message authentication acceleration protocol for vehicular ad hoc networks," in Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE. IEEE, 2009, pp. 1–6.

[29] S. M. Safi, A. Movaghar, and M. Mohammadizadeh, "A novel approach for avoiding wormhole attacks in vanet," in Internet, 2009. AH-ICI 2009. First Asian Himalayas International Conference on. IEEE, 2009, pp. 1–6.

[30] A. Hamieh, J. Ben-Othman, and L. Mokdad, "Detection of radio interference attacks in vanet," in Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE. IEEE, 2009, pp. 1–5.

[31] J. Choi and S. Jung, "A security framework with strong non-repudiation and privacy in vanets," in Consumer Communications and Networking Conference, 2009. CCNC 2009. 6th IEEE. IEEE, 2009, pp. 1–5.

[32] A. Wasef, R. Lu, X. Lin, and X. Shen, "Complementing public key infrastructure to secure vehicular ad hoc networks [security and privacy in emerging wireless networks]," Wireless Communications, IEEE, vol. 17, no. 5, 2010, pp. 22–28.

[33] M. Bechler, H.-J. Hof, D. Kraft, F. Pahlke, and L. Wolf, "A cluster-based security architecture for ad hoc networks," in INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies, vol. 4. IEEE, 2004, pp. 2393–2403.

[34] L. Zhou and Z. J. Haas, "Securing ad hoc networks," Network, IEEE, vol. 13, no. 6, 1999, pp. 24–30.

[35] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in Advances in CryptologyCRYPTO 2001. Springer, 2001, pp. 213–229.