Threats to Security in DSRC/WAVE

Christine Laurendeau and Michel Barbeau

School of Computer Science, Carleton University
1125 Colonel By Drive, Ottawa, ON Canada K1S 5B6
Tel.: 613-520-2600; Fax: 613-520-4334
{claurend, barbeau}@scs.carleton.ca

Abstract. Dedicated Short Range Communications (DSRC) enabled road vehicles are on the brink of actualizing an important application of mobile ad hoc networks. It is crucial that the messages exchanged between the vehicles and between the vehicles and specialized infrastructure be reliable, accurate and confidential. To this end, we propose to identify the security threats inherent in the emerging DSRC Wireless Access in Vehicular Environments (WAVE) architecture. We rank the identified threats according to the European Telecommunications Standards Institute's (ETSI) threat analysis methodology. We also discuss possible countermeasures to the most critical threats.

1 Introduction

As the emerging field of vehicle communications is poised to become the technology of the next decade, it becomes more imperative that the architecture and infrastructure upon which vehicular networks are based be reliable and secure. With new vehicles being outfitted with on-board equipment which essentially renders each one into a mobile device capable of communicating with other vehicles' equipment and with fixed roadside stations, drivers are able to call upon a veritable panoply of new and exciting applications. In addition to gaining access to an unending stream of navigational and localized information available through Location-Based Services (LBSs), vehicles can benefit from a tremendous increase in traffic safety when they receive real-time notification of upcoming road hazards, imminent collisions and movements of emergency vehicles. Dedicated Short Range Communications (DSRC) [1] and its wireless component, Wireless Access in Vehicular Environments (WAVE) [2] [3] [4] [5], provide an architecture for vehicular networks.

At present, there is a dearth of discussion on security issues pertaining to vehicle communications, although some issues have been addressed. In [6], Raya and Hubaux identify threats to the traffic messages exchanged between vehicles in Vehicular Adhoc NETworks (VANETs). The authors propose a security architecture featuring the use of digital signatures and multiple anonymous key pairs to deal with those threats. As well, Blum and Eskandarian [7] offer an outline of some security threats, including jamming, impersonation and fabrication, as they pertain to traffic messages. The authors outline an architecture for

T. Kunz and S.S. Ravi (Eds.): ADHOC-NOW 2006, LNCS 4104, pp. 266–279, 2006.

maintaining a VANET's integrity and functionality through the use of vehicular clusterheads managing access to the network.

Given the private nature of the application information exchanged and potential for attackers to wreak havoc in the vehicular network, there is a compelling need to identify and address the most severe security threats specific to the DSRC/WAVE architecture. We endeavour to present here an analysis of those threats using the European Telecommunications Standards Institute's (ETSI's) [8] methodology, where identified threats can be ranked as critical, major or minor depending on their likelihood of occurrence and impact on the user or the network.

Section 2 presents an overview of DSRC/WAVE's architecture as put forth in IEEE draft standards. Section 3 outlines the methodology used to rank the threats we uncover. Section 4 provides an analysis of the identified threats along with their risk assessments. Section 5 discusses possible countermeasures to the critical threats identified in Section 4, and Section 6 concludes the paper.

2 DSRC/WAVE Architecture

DSRC was conceived to provide an architecture for nodes within a vehicular network to communicate with each other and with the infrastructure in a secure and efficient manner. In DSRC, subsequently specialized as WAVE, GPS-enabled vehicles are equipped with On-Board Units (OBUs) which can communicate with each other to propagate safety warnings through Vehicle-to-Vehicle (V2V) communications. As well, OBUs have access to infrastructure devices called Road Side Units (RSUs) which are located intermittently along city streets and highways to provide access to a variety of services and applications, such as LBSs and wireline access, through Vehicle-to-Infrastructure (V2I) communications. Some OBUs may also be configured to provide service access to other OBUs through the *OBU to Vehicle Host Interface* (OVHI). Additionally, a special class of OBUs, called Public Safety OBUs (PSOBUs), are entrusted with special capabilities. These vehicles, which include police cars, fire trucks and ambulances, may operate as OBUs or RSUs, as circumstances dictate.

DSRC/WAVE operates in the 5.9 GHz band and has 75 MHz of bandwidth allocated for vehicle communications, which are based on line of sight with a range of up to 1 km and vehicle speeds of up to 140 km/h. While the standards upon which the WAVE architecture is based are still in development, a basic framework appears to have stabilized as outlined below.

2.1 Protocol Layers

The general WAVE architecture, along with the standards on which its different layers are based, can be found in Figure 1. The physical (PHY) and Medium Access Control (MAC) layers implement the IEEE P802.11p [2] standard. One of the additions in this standard consists of the use of dynamic MAC addresses to identify the OBUs in a somewhat anonymous manner. These MAC addresses

are initialized upon startup, then set to a new designation whenever a message is received from a nearby node with a duplicate address.

The IEEE P1609.4 Multi-Channel Operation standard [5] describes how WAVE's MAC layer operates with the available spectrum allocated as one control channel (CCH) and four to six service channels (SCHs). Traffic safety messages are broadcast on the CCH, as are announcements of available services. Subsequent communications between an OBU and a service provider occur on a SCH. However, the OBU is required to periodically monitor the CCH for incoming announcements.

The IEEE P1609.3 Networking Services standard [4] outlines the WAVE architecture at the network layer. Messages may be conveyed using one of two protocols: the Internet Protocol version 6 (IPv6) for transaction applications involving LBSs for example, or the custom WAVE Short Messages Protocol (WSMP) for broadcast applications which require low latency for delivering crucial safety information.

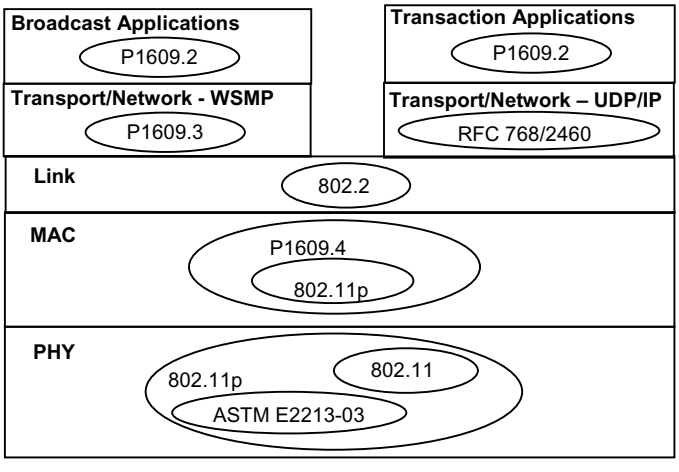

Fig. 1. DSRC/WAVE Protocol Layers and Standards

2.2 Security Measures

The IEEE P1609.2 standard [3] describes the measures designed to ensure that the messages exchanged in WAVE are secure.

Broadcast Messages are untargeted and usually related to traffic safety applications. They are broadcast using WAVE Short Messages (WSMs). Given the non-sensitive nature of the information carried in WSMs, these messages are not encrypted but merely signed with the sender's certificate. Every signed message includes the current timestamp, obtained from the OBU's internal clock which is synchronized with the GPS time. This timestamp is used by the receiver to verify the message against a cache of recently received messages to ensure against replay attacks. The signature algorithm specified in the standard is the Elliptic

Curve Digital Signature Algorithm (ECDSA) [9]. An example of a traffic application using broadcast messages is *platooning*, where vehicles can be organized as a convoy to increase capacity on major roads by having a lead OBU broadcast its changes in vehicle speed so that the OBUs behind it match its speed.

Transaction Messages are generally unicast and sent using the IP stack to an application running on a service provider host via either a RSU or another OBU over an OVHI. Because these messages may be used to access LBSs and personal data may be exchanged, they are encrypted with a symmetric encryption algorithm, such as the Advanced Encryption Standard in CCM mode (AES-CCM) [10], using a random key. This random key is in turn encrypted using the asymmetric encryption algorithm Elliptic Curve Integrated Encryption Scheme (ECIES) [11].

In order for vehicles to sign messages, they must possess a digital certificate. The standard recommends that procedures for PSOBU and RSU certificate enrollment include a manual component, but OBU certificate enrollment procedures have not yet been put forth. When signing a message, a vehicle may also include a *certificate chain*, i.e. the certificate that authorized the vehicle's certificate, as well as the certificate that authorized the certifying certificate, and so on, up to a *root certificate* which is issued by a higher authority such as a governmental agency responsible for licensing vehicles. Upon receipt of a signed message, each node must verify that it recognizes the root certificate used to authorize the sender's certificate. The node must also ensure that none of the certificate chain's members have been revoked by comparing each one against a Certificate Revocation List (CRL). These CRLs and the collection of valid root certificates are stored locally on each node and must be periodically updated.

3 Analysis Methodology

In 2003, the European Telecommunications Standards Institute (ETSI) developed a methodology for analyzing security threats to its meta-protocol, Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) [8]. This methodology allows for identified threats to be ranked in terms of risk, using estimated values for the likelihood of occurrence and impact upon the user or system.

The *likelihood* of occurrence of the threat indicates whether theoretical and practical knowledge is available for attackers to carry out an attack. Three levels of likelihood are defined with an associated numerical value: *Likely* (3) – all elements in place; *Possible* (2) – some elements in place; *Unlikely* (1) – important elements missing. Although the *impact* of a threat has no bearing on whether an attack occurs, it can indicate if the threat is serious enough to warrant further research into possible countermeasures. The values associated with the impact are the following: *High* (3) – serious consequences for the user or network; *Medium* (2) – short-term outages; *Low* (1) – minor consequences for the user or network. The *risk* is calculated as the product of the numerical values of the likelihood and impact. The categories in which the risk is deemed to fall are defined as:

Critical (9,6) – countermeasures must be devised without delay; *Major* (4) – the threat will eventually require attention; *Minor* (3,2,1) – the threat can be ignored in the short term.

In [12], we used the definitions provided in [8] to further break down the likelihood component into its two natural components: the technical difficulty in carrying out the threat and the motivation or potential gain on the part of the attacker for him or her to proceed. We make use of this idea here in order to fine-tune the risk assessment process. The values for technical *difficulty* can be defined in terms of whether or not the threat has previously been considered in theory or in practice: *None* – a precedent for the attack exists; *Solvable* – the attack is theoretically possible; *Strong* – theoretical elements missing. The levels for *motivation* include: *High* – significant gains for attacker; *Moderate* – service disruption only; *Low* – no significant gains. The technical difficulty and motivation associated with a given threat can be used with its impact to determine the risk assessment, as depicted in Table 1.

Table 1. Risk Assessment

<table>
<tr><th rowspan="2">Motivation</th><th rowspan="2">Difficulty</th><th rowspan="2">Likelihood</th><th colspan="3">IMPACT</th></tr>
<tr><th>High</th><th>Medium</th><th>Low</th></tr>
<tr><td rowspan="2">High</td><td>None</td><td rowspan="2">Likely</td><td colspan="2" rowspan="2">Critical</td><td rowspan="3">Minor</td></tr>
<tr><td>Solvable</td></tr>
<tr><td rowspan="2">Moderate</td><td>None</td><td rowspan="2">Possible</td></tr>
<tr><td>Solvable</td><td>Major</td></tr>
<tr><td>Low</td><td>Any</td><td rowspan="2">Unlikely</td><td colspan="3" rowspan="2">Minor</td></tr>
<tr><td>Any</td><td>Strong</td></tr>
</table>

4 Threat Analysis

In our analysis, we focus on the most basic security attributes to be preserved in vehicular networks: availability, authenticity and confidentiality. The collated list of threats, organized by risk category, can be found in Table 2.

4.1 Threats to Availability

Threats to the availability and consistent behaviour of the vehicular network include denial of service (DoS) attacks, the introduction of malicious software (malware) and the potentially high volume of messages introduced through spamming.

DoS. DoS attacks render the network unavailable to its users, for example by flooding the nodes with messages or by jamming signals at the physical layer. These attacks can be carried out either by network insiders turned rogue or by outsiders to the network.

Flooding. One way to incapacitate the vehicular network is to artificially generate such a high volume of false messages on the CCH that the network's nodes,

Table 2. Threat Analysis

Threat	**Motivation**	**Difficulty**	**Likelihood**	**Impact**	**Risk**
Black Hole, GPS Spoofing, Location Tracking	High	Solvable	Likely	High	Critical
Malware	Moderate	Solvable	Possible	High	Critical
DoS	Moderate	Solvable	Possible	Medium	Major
Masquerading, Replay, Transaction Tampering, Outsider Eavesdropping	High	Strong	Unlikely	High	Minor
Broadcast Tampering	Moderate	Strong	Unlikely	High	Minor
Spamming, Insider Eavesdropping	Moderate	None	Likely	Low	Minor

OBUs and RSUs alike, cannot sufficiently process the superfluous data. Important messages are lost as a result. Consequences may include accidents if collision warnings or platoon directives are not delivered.

Jamming. By creating interference on the CCH, an attacker can hamper message delivery, thereby compromising the traffic safety applications which depend upon it. Alternately, jamming can be used to cloak an attacker so that he or she cannot be identified.

Given that DoS represents a disruption rather than an opportunity for gain, the motivation required on the part of an attacker is rated as moderate according to the criteria provided in Section 3. The technical difficulty involved is solvable, given that it is theoretically possible. Since DoS would result in temporary outages, the impact on the network is ranked as medium, and according to Table 1, the threat is assessed as major.

Malware. The introduction of malware, such as viruses or worms, into the vehicular network has the potential to cause serious disruptions to its operation. Since the OBUs and RSUs are expected to receive periodic software and firmware updates, this threat is more likely to be carried out by a rogue insider than by an outsider. The associated motivation is ranked as moderate because it consists of a disruption in service. Since the threat is theoretically possible, the technical difficulty is a solvable one if countermeasures are not in place. The impact on the user is considered high due to the resulting long-lasting outages. As a result, the malware threat is ranked as critical.

Spamming. There is a risk in increased transmission latency due to the presence of spamming messages. The motivation for marketers to acquire a RSU or an OVHI-enabled OBU for this purpose is best rated as moderate. On one hand, it is likely to be very lucrative, but on the other hand, the business is ultimately accountable to its customers who typically resent such a waste of their time and

bandwidth. With the technical difficulty rated as low since the marketer is an insider, and with the impact on the user also low because it represents little more than an annoyance, the threat is ranked as minor.

4.2 Threats to Authenticity

Ensuring the authenticity of the network includes protecting legitimate nodes from rogue insiders and outsiders infiltrating the network under an assumed identity, detecting the presence of black holes, identifying attacks replaying legitimate interactions, exposing spoofed GPS signals, and thwarting the introduction of misinformation into the network.

Masquerading. By posing as legitimate nodes in the vehicular network, outsiders can proceed to conduct more types of attacks than they otherwise could, for example forming black holes or fabricating false messages. However, given how easy it is to become part of the network by simply joining it with a working OBU, the masquerading exercise for an outsider becomes analogous to breaking a window to get into a house when the front door is wide open. There is, however, much to be gained by a rogue insider masquerading as another OBU or a RSU. By assuming a false identity, an attacker can create mischief with impunity, such as injecting false messages into the network and deceiving authorities into believing that another node was responsible. With PSOBUs possessing special privileges within the network, and RSUs providing wireline access and LBS information, spoofing such nodes can be the first step in accessing personal user information and possibly compromising privacy. However, because OBUs and RSUs can be identified by their certificate which can be distributed in Certificate Revocation Lists (CRLs) if a node turns rogue, such a deception would be difficult to successfully carry out. With the strong technical difficulty in conducting this attack, despite its high impact on the user and the network due to compromised integrity, the threat is ranked as minor.

Black Hole. A black hole is formed by nodes which fail to propagate messages. Such an attack can only be carried out by rogue insiders, since network outsiders are not expected to repeat messages. The consequences of having a black hole in the network include dropped traffic messages, service requests and replies. With sufficient numbers of rogue nodes colluding to form a black hole past which no messages are propagated, it may be possible for attackers to partition the vehicular network in such a way that legitimate nodes never receive messages. If this scenario succeeds, nodes may be prevented from receiving critical updates to their root certificate lists and CRLs, leaving them vulnerable to masquerading attacks from nodes using expired, revoked or falsified certificates. With significant gains to be made from this attack, its technical difficulty solvable and its tremendous impact on the security of the network, the threat is ranked as critical.

Replay Attack. Vehicular networks operating in the WAVE framework are protected from replay attacks by having each node maintain a cache of recently

received messages against which new messages are compared. Messages older than a configurable time are discarded. The others are compared against this cache to ensure that they have not previously been received. This scheme assumes that an accurate source of time is available. The case where the clock accuracy is compromised is considered below in the section on GPS spoofing. Therefore, despite the potential gains to be made in terms of network manipulation, there are strong technical difficulties in carrying out a replay attack, rendering this a minor threat.

GPS Spoofing. By using a GPS satellite simulator to generate radio signals stronger than those received from the genuine GPS satellite, an attacker can lead nodes to believe they are in a different location than they actually are [13], potentially causing collisions. Also, if GPS time is used to timestamp messages, a spoofing of the GPS clock could result in nodes accepting expired messages as new ones and could thus lead to a successful replay attack. Given the potential gains for an attacker, the solvable technical difficulties involved in this type of attack and its high impact on the network and the users, the threat is ranked as critical.

Broadcast Tampering. It is possible that a rogue insider may attempt to inject false traffic safety messages into the network for the purpose of creating mischief, for example causing accidents by suppressing traffic warnings or manipulating the flow of traffic to clear a chosen route. Broadcast messages are meant for general consumption, but they need to be signed in order to deter attackers from generating false messages. Although a rogue insider, as a genuine, authenticated member of the network, could use its digital certificate to sign any number of false messages, it would soon find itself included on CRLs meant to black-list such nodes. The strong technical difficulty involved in carrying out this threat indicates that it is a minor one.

Transaction Tampering. Another possible threat to message integrity consists of an attacker modifying the messages exchanged in V2I in order to falsify transaction application requests or forge the associated replies. With a little imagination, a malicious agent could create an entire alternate life or lifestyle for an unsuspecting user. However, the technical difficulty involved is quite strong given that transaction messages must be encrypted as described in Subsection 2.2. As a result, the threat is minor.

4.3 Threats to Confidentiality

With the messages exchanged between the nodes of a vehicular network being accessible over the air, the threats to confidentiality include the illegitimate collection of transaction information through eavesdropping and the collection of location information available through the retransmission of broadcast messages.

Outsider Eavesdropping. Broadcast messages generally pertain to traffic safety information and are therefore uninteresting for the purposes of eavesdropping. The same cannot be said of LBS and other types of transaction application

information. In accumulating a series of such service requests, a malicious agent can construct a profile of a given user by observing which services are used regularly, when, from which location and how much is spent. However, even with the potential gains for the attacker, the associated technical difficulty is quite strong, given the level of encryption required to protect this type of information, as described in Subsection 2.2. The threat is therefore ranked as minor.

Insider Eavesdropping. As long as insider nodes collect information in keeping with the terms of an agreement with the user, there is no problem. However, there is the possibility that an insider may collect information at a time when the user is unaware of the collection. For example, a traveling sales agent may have an agreement with an employer to have his or her movements tracked during business hours and not afterward. Because the impact on the user constitutes no more than an annoyance, the threat is considered minor.

Location Tracking. With the emerging potential of vehicle locations being constantly tracked, it is not difficult to imagine the temptation for attackers to exploit this new opportunity. By collecting an unsuspecting individual's location trace over time, such information can be used in tracking, stalking, or in building a potentially damaging profile of the user. Every time an OBU propagates a broadcast message to alert other vehicles to traffic safety updates, it digitally signs the repeated message with its own certificate which can identify the OBU and its current position to the receiving nodes. Given the attacker's gain in personal location information, the solvable technical difficulties associated with this threat and its tremendous impact on the user, it is ranked as critical.

5 Countermeasures and Open Issues

In our analysis in Section 4, we uncovered four critical security threats inherent in the WAVE architecture: malware, black hole, GPS spoofing and location tracking, as well as one major threat, DoS. These problems need to be addressed before a WAVE implementation can be considered secure.

Malware. According to the security considerations outlined in the informative portion of the WAVE security standard [3], received software and firmware upgrades should only be permitted if they are sent and digitally signed by nodes which have the required permission. In [14], a new security standard proposed by a large consortium of smart phone vendors is discussed. Although the details are sketchy, it appears that this standard will be based on the Trusted Platform Module (TPM) chip used in PCs and laptops [15]. This chip protects a device from malware by providing authentication and cryptography services, allowing other trusted devices to selectively access the functions available on the device. This is in essence the same approach recommended (although not mandated) in the WAVE security standard. This countermeasure is considered to be state of the art for smart phones and other mobile devices. It may be equally effective in vehicular networks, provided that it is implemented. Otherwise, entry points for malware will need to be closed through future upgrades as they are discovered.

Black Hole. Broadcast messages in WAVE are propagated by flooding. All OBUs have the same range, and we may assume that the links are symmetrical. It may therefore be feasible to detect a black hole by having the sending nodes listen to their neighbors' retransmissions to ensure that they repeat the messages. This concept is known as passive acknowledgement [16]. According to the IEEE P802.11p [2] standard, nodes periodically send Nearby Station request messages to ensure that none of their neighbors have a duplicate MAC address. If a given node sends a broadcast message and knows who its neighbors are, it can flag a neighboring node which fails to repeat messages. It can then follow the appropriate repudiation procedure, as discussed in *Rogue Repudiation* in the sequel.

More conventional black hole prevention techniques, including multipath routing and the use of backup routes, are outlined in [17]. However, WAVE has a measure of resistance to black holes by design, due to the fact that it propagates messages by flooding without any route optimization mechanisms. With messages sent to every node within range, each of which repeats to all the nodes within its range, redundancy provides resilience to black holes. Alternately, it may be feasible to have RSUs repeat traffic messages as well. Although these infrastructure nodes are vulnerable to physical tampering, the non-responsiveness of known RSUs can raise an alarm.

GPS Spoofing. The WAVE security standard [3] recommends the implementation of plausibility rules regarding changes in vehicle location, as well as the use of special calibration measures on the OBU clock so that updates to the time are performed by accelerating or decelerating the clock in a continuous manner, rather than in an abrupt, discrete fashion. Such rules offer a good basis for a countermeasure to the GPS spoofing threat. Similar plausibility-based countermeasures are offered in [13], such as profiling satellite availability, locations and signal strength in order to detect unaccountable changes to the configuration. If an OBU knows that at a given set of coordinates it can usually receive signals from four satellites, each with a specific signal strength, and it suddenly receives much stronger signals from two or seven satellites, there is a chance that a GPS satellite simulator has been set up nearby. A problem arises with this countermeasure when environmental conditions, such as the weather or ionosphere, affect the quality of the received signal. Changes in signal strength may be due to the presence of a GPS simulator or to natural phenomena.

However, a countermeasure to the GPS spoofing threat already exists. It consists of using the encrypted Precise Positioning System (PPS) military signal rather than the Standard Positioning System (SPS) civilian signal. The state-of-the-art PPS-based GPS receiver known as Selective Availability Anti-Spoofing Module (SAASM) [18] uses a combination of symmetric and asymmetric encryption, where an asymmetric scheme is used to distribute a symmetric key, as outlined in [19]. As a result, if transportation authorities are granted permission from the U.S. military to use the SAASM receiver, as some other governmental

agencies have been, vehicular networks can be well protected from GPS spoofing attacks.

Location Tracking. Location tracking is an even more complex issue. An important conundrum is posed by the very nature of ad hoc vehicular networks: the balance of user privacy versus accountability. On one hand, users have the right to expect a certain level of confidentiality with regards to their identity, location and application use. The vehicular network must ultimately allow them to anonymously repeat broadcast traffic messages. On the other hand, it is imperative that malicious nodes be identified and neutralized in order to prevent serious harm to other users. This means that nodes must be uniquely and persistently identified so that attackers can be flagged over a significant distance and period of time. There is currently no mechanism in WAVE to support anonymous broadcast messages.

Much of the existing research into location privacy involves protecting users from LBS providers by blurring the user's exact location in space and time. By cloaking a user's LBS request so that it is indistinguishable from k–1 other requests, *k-anonymity* [20] [21] is achieved, with higher values of k resulting in greater anonymity and thus decreased granularity. One such implementation for vehicular networks is described in [22]. Unfortunately, such schemes are not applicable in traffic safety applications such as platooning and collision avoidance systems where each vehicle's precise location is of paramount importance.

DoS. DoS attacks in Internet applications and e-commerce can be mitigated by requiring sending nodes to perform a task such as solving a puzzle [23] before receiving services from a server. This idea ensures that legitimate nodes only have a simple computational chore to perform while attackers find themselves bogged down with the same task due to the sheer volume of messages sent. Ideally, DoS attacks should be mitigated at the lowest possible layer in the protocol stack. By providing link layer authentication, for example through the use of cryptographically generated MAC addresses, outsider attacks may be deterred. The concept of cryptographically generated IPv6 addresses, described in [24], may be applicable to MAC addresses in vehicular networks, although rogue insider nodes remain the greater threat. Further experiments need to be conducted to determine whether similar or other DoS prevention schemes can be applied to VANETs without adversely affecting transmission latency. It should be noted, however, that none of these countermeasures can prevent a wideband jammer from disrupting the VANET signals. Such an attack may be countered with the use of directional antennas which could allow vehicles to circumvent the jammed area.

In addition, a vehicular network bogged down with a significant load of legitimate messages becomes more vulnerable to DoS attacks. A further measure to increase WAVE's resilience to this threat would be the introduction of a routing protocol minimizing the number of broadcast messages.

Rogue Repudiation. Rogue nodes must be identified and repudiated as soon as they are detected. The WAVE security standard proposes to deal with such nodes by including their certificate identifiers on CRLs which are distributed to all other nodes in the vehicular network so that none will accept messages from a repudiated node. However, it is unclear how rogue nodes can be black-listed by the individual nodes detecting them.

It may be possible to use reputation systems such as [25] for each node to accrue good will or ill will, depending on how other nodes perceive its trustworthiness. Once a node has exceeded a pre-determined threshold for unreliability, it can be referred to some higher authority who can then black-list the sender by placing its certificate identifier on a CRL. Furthermore, once a rogue node moves out of the range of a given group of nodes, its reputation needs to follow it so that it cannot provoke another attack on a new group of unsuspecting nodes. The implementation of a rogue repudiation scheme, as well as the efficient dissemination of up-to-date CRLs to all the nodes, remain open issues.

6 Conclusions

We have identified some important threats to the security of DSRC/WAVE vehicular networks. Using the ETSI's threat analysis methodology, we have identified malware, black hole, GPS spoofing and location tracking as critical threats. The DoS attack is considered to be major.

We have outlined possible countermeasures to the critical and major threats. Malware threats can be dealt with by requiring that software and firmware upgrades be received only from authenticated nodes which possess the appropriate permissions, as outlined in the WAVE security standard. GPS simulators can be countered through the use of specialized GPS receivers accessing an authenticated signal. Passive acknowledgements may be used by sending nodes to detect black holes. Location tracking remains an open issue. DoS threats may be mitigated with the use of puzzles and directional antennas. Further work is required to simulate catastrophe situations in order to adequately assess the impact of the aforementioned attacks, most notably DoS.

It is clear that with some of these possible countermeasures and a rogue repudiation scheme still in the embryonic stages, the remaining security issues must be addressed before DSRC/WAVE vehicular networks and their applications can be fully realized.

Acknowledgements

The authors gratefully acknowledge the financial support received for this research from the Automobile of the 21st Century (AUTO21) Network of Centres of Excellence (NCE).

References

1. IEEE Vehicular Technology Society: 5.9 GHz Dedicated Short Range Communications (DSRC) - Overview. [Online]. Available: http://grouper.ieee.org.groups/scc32/dsrc/
2. IEEE 802 Committee of the IEEE Computer Society: Draft Amendment to Standard for Information Technology - Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Wireless Access in Vehicular Environments (WAVE). Draft IEEE Standard, IEEE P802.11p/D1.1, January 2005.
3. SCC32 Committee of the IEEE Intelligent Transportation Systems Society: Draft Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages. Draft IEEE Standard, IEEE P1609.2/D1.3, October 2005.
4. SCC32 Committee of the IEEE Intelligent Transportation Systems Society: Wireless Access in Vehicular Environments (WAVE) Networking Services. Draft IEEE Standard, IEEE P1609.3/D14, September 2005.
5. SCC32 Committee of the IEEE Intelligent Transportation Systems Society: Wireless Access in Vehicular Environments (WAVE) Multi-Channel Operation. Draft IEEE Standard, IEEE P1609.4/D03, April 2005.
6. M. Raya and J.-P. Hubaux: The Security of Vehicular Ad Hoc Networks. Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, 2005.
7. J. Blum and A. Eskandarian: The Threat of Intelligent Collisions. IT Professional, vol. 6, no. 1, January/February 2004, 24–29.
8. ETSI: Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Protocol Framework Definition; Methods and Protocols for Security; Part 1: Threat Analysis. Technical Specification ETSI TS 102 165-1 V4.1.1, 2003.
9. American National Standards Institute: Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA). ANSI Standard, X9.62-2005, 2005.
10. Internet Engineering Task Force: IETF Request for Comments: 3565, Use of Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS). IETF RFC 3565, 2003.
11. Certicom Research: Standards for Efficient Cryptography, SEC 1: Elliptic Curve Cryptography, Version 1.0. [Online]. Available: `http://www.secg.org/download/aid-385/sec1_final.pdf`
12. M. Barbeau: WiMax/802.16 Threat Analysis. Proceedings of the 1st ACM International Workshop on QoS and Security for Wireless and Mobile Networks (Q2SWinet), 2005.
13. J.S. Warner and R.G. Johnston: GPS Spoofing Countermeasures. The Weekly Homeland Security Newsletter, 12 December 2003. [Online]. Available: `http://www.homelandsecurity.org/bulletin/121203.htm`
14. N. Leavitt: Will Proposed Standard Make Mobile Phones More Secure? Computer, vol. 38, no. 12, December 2005, 20–22.
15. Trusted Computing Group: TCG TPM Specification. [Online]. Available: https://www.trustedcomputinggroup.org/groups/tpm/

16. J. Jubin and J.D. Tornow: The DARPA packet radio network protocols. Proceedings of the IEEE, vol. 75, no. 1, 1987, 21–32.
17. I. Aad, J.-P. Hubaux and E.W. Knightly: Denial of Service Resilience in Ad Hoc Networks. MobiCom '04: Proceedings of the 10th Annual International Conference on Mobile Computing and Networking, 2004.
18. J. Nielson, J. Keefer and B. McCullough: SAASM: Rockwell Collins' Next Generation GPS Receiver Design. Position Location and Navigation Symposium, IEEE 2000, March 2000, 98–105.
19. S. Callaghan and H. Fruehauf: SAASM and Direct P(Y) Signal Acquisition. GPS World, July 2002.
20. A. McDiarmid and J. Irvine: Achieving Anonymous Location-Based Services. Proceedings of the 60th International Conference on Vehicular Technology (VCT2004), vol.4, 2004.
21. B. Gedik and L. Liu: Location Privacy in Mobile Systems: A Personalized Anonymization Model. Proceedings of the 25th IEEE International Conference on Distributed Computing Systems, 2005.
22. M. Gruteser and D. Grunwald: Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking. Proceedings of the First International Conference on Mobile Systems, Applications and Services, 2003.
23. A. Juels and J. Brainard: Client Puzzles: A Cryptographic Countermeasure Against Connection Depletion Attacks. Proceedings of the 1999 Network and Distributed Systems Security Symposium (NDSS), February 1999, 151–165.
24. T. Aura: IETF Request for Comments 3972, Cryptographically Generated Addresses (CGA), 2005. [Online]. Available: `http://www.rfc-archive.org/getrfc.php?rfc=3972`
25. P. Michiardi and R. Molva: CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks. Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security, September 2002.