Comprehensive View of Security Practices in Vehicular Networks

Manveen Kaur  
School of Computing  
Clemson University  
Clemson, South Carolina  
mkaur@clemson.edu

James Martin  
School of Computing  
Clemson University  
Clemson, South Carolina  
jim.martin@cs.clemson.edu

Hongxin Hu  
School of Computing  
Clemson University  
Clemson, South Carolina  
hongxih@clemson.edu

Abstract—With expectation of widespread adoption of Connected Vehicles Technology (CVT), security within the vehicular networks has come under scrutiny. Owing to the nature of CVT applications, security flaws can result not only in loss of data or network function but also in fatal accidents. Security mechanisms that can account for privacy, authentication, integrity, and non-repudiation while having an acceptable communication overhead are imperative to the functioning of CVT applications. While this field of study is rapidly evolving with a wide range of studies and security solutions being proposed for different areas of CVT security, literature documenting the comprehensive picture of current security protocols and practices is missing. This paper attempts to remedy this by documenting recent advances in CVT security with the goal of providing an efficient jumping off point for future research in CVT security development.

I. INTRODUCTION

Development of connected vehicle technology (CVT) is aimed at allowing vehicles to perform Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication wirelessly to achieve safer, more convenient, and environment conscious commute. Using Dedicated Short Range Communications (DSRC) and principles of Vehicular Ad Hoc Network (VANET) communication, this technology will be utilized in building tools and applications that address safety and mobility issues faced by the current vehicular practices. CVT’s crash prevention applications will be able to prompt drivers to react to sudden changes in traffic patterns and thus, reduce the number of road accidents caused. Mobility applications for CVT will enable drivers to make route choices that reduce travel delay, and improve traffic conditions on generally busy sections of the road. Reduction in the time spent by vehicles on the road or stuck in traffic will also reduce the environmental impact that is caused by transportation systems. Some of the safety and mobility applications which are currently being developed and researched for CVT to achieve these goals are queue warning, incident detection and cooperative adaptive cruise control (CACC).

Securing the communication network that will be used by CVT is critical to its performance. Cyber threats to CVT are more damaging than threats to non-automated systems because the driver may not be able to override a malfunctioning system in time to prevent a potentially fatal accident. CVT applications face unique security constraints such as ensuring that the processing and bandwidth overhead are kept to a minimum because of the time critical nature of the applications. Messages need to be protected from attacks such as eavesdropping, spoofing, alterations, and unauthorized access to drivers’ personal information.

This paper provides a comprehensive view of security practices in vehicular networking, addressing the potential security risks and vulnerabilities along with the security mechanisms that can be used to mitigate the threats. Section II discusses classification of threats, and adversarial and trust models in CVT systems. Section III provides a brief introduction to the DSRC, Wireless Access for Vehicular Environments (WAVE), and Intelligent Transportation Systems (ITS) standards for CVT with focus on the security mechanisms provided within these standards. Sections IV and V discuss application and infrastructure level threats to the CVT system in detail. Threats at an infrastructure level are considered more critical than threats at an application level because of the greater area of impact. Section VI concludes the study with a discussion on the future of CVT security and the areas within this field which require further investigation.

II. THREATS TO CVT SECURITY

Threats to a CVT system can be classified in three categories: (1) In-vehicle threats, (2) V2V threats, and (3) V2I threats.

An in-vehicle network refers to the network of distributed electronic control units (ECUs) that form the automotive architecture of today’s vehicles. A vehicle’s ECUs communicate over different buses and protocols such as Local Interconnect Network (LIN) that is a local sub network used for automatic door locking mechanisms, power windows, and communication with smart sensors that detect conditions like darkness or rain; Controller Area Network (CAN) that is an even triggered bus system that handles real
time communication between controllers like engine management; and multimedia bus systems such as MOST that provides high performance, wide band communication channels to meet automotive demand for in-car entertainment [1]. Since the in-vehicle network is fully connected, any compromised ECU is capable of tampering with the vehicle’s functioning. Therefore, any ECU accessible from outside the vehicle can function as the potential intrusion point. While this study does not discuss in-vehicle security, studies such as [1], [2], and [3] discuss various attack models for in-vehicle systems along with a range of solutions that can be applied to mitigate these attacks.

Threats to the V2V and V2I environments can be categorized as application level threats and infrastructure level threats. Infrastructure level threats aim at incapacitating the network to prevent overall functioning of CVT system. Application level threats aim at sabotaging individual applications to prevent the application from functioning properly. Certain attacks, such as Sybil attack [4], are considered as threats at both the application and the infrastructure level.

A. Adversaries in CVT system

Attacks can be manifested in a CVT environment using different types of adversarial entities [5].

- Active adversaries – Entities with the ability to modify messages in the CVT environment through techniques such as eavesdropping, jamming, injection of false information into messages, and replaying messages.
- Passive adversaries – Entities with the ability to unlawfully collect information about nodes in the CVT system.
- External adversaries – Remote entities that can use valid nodes in the system as an attack proxy, or to provide misleading information to other nodes in the environment.
- Internal adversaries – Entities with valid credentials which are posing as valid nodes.

Multiple adversarial nodes can be present simultaneously in the CVT system. These nodes may act independently or they may coordinate their actions for a more effective attack [5].

B. Trust models in CVT systems

Trust models can be applied to accurately identify threat agents and isolate malicious nodes in a CVT system. Traditional trust models for vehicular networks can be classified as entity-oriented models that base trust on the legitimacy of the nodes, and data-oriented models that base trust on the legitimacy of the information received [6]. In [7], an entity-based trust model is proposed where reputation of sender nodes is assessed by classifying them within three different trust models using direct exposure, recommendations from surrounding nodes, and recommendation of a central authority as sources of information. In [8], the authors discuss an entity-oriented trust model based on reputation of nodes within a group. Each node is assigned to a static group offline and all messages originating from nodes belonging to a group are required to include an authentic group ID. Calculation of trust value at the receiver depends on the reputation value of the group. Group reputation values are assigned to the group based on the verification of the message sent by the nodes belonging to the group. In [18], the authors discuss a data-oriented trust model based on the incident reports received over the V2V network. Each node in a V2V network is required to broadcast incidents of interest to all nodes within the communication range. Receiver nodes that plan to accept this incident report can attach their endorsement opinion of the incident before forwarding the message further to other nodes and to a central authority residing in the V2I infrastructure. The central authority computes the trust value of the incident report based on the number of endorsements it received. Owing to the dynamic nature of a vehicular network, using only entity-based or data-based trust model leads to high reaction time to critical situations [5]. The increase in number of nodes during certain times of the day also attributes to increased reaction time. Different hybrid trust models such as those discussed in [9] have evolved to circumvent the shortcomings of these two models. In [9], the authors discussed a hybrid trust model that takes into account both the legitimacy of the information and the reputation of the node it is originating from. Table 1 provides a risk assessment summary of the attacks discussed in Sections IV and V. The severity of attacks in Table 1 is a preliminary ranking assigned based on the our theoretical understanding of the time taken to contain and mitigate the attack, and the consequences of the attack ranging between ‘mild traffic congestion’ (low), ‘serious traffic congestion’ (medium), and ‘fatal traffic incident’ (high). Attacks are numbered from A1-A11. Table 2 in Section IV of the paper uses this numbered representation to depict what aspects of security these attacks impact the most.

Table 1. Attacks and their risk assessment

<table>
<thead>
<tr>
<th>Attack</th>
<th>Risk Assessment</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>Platooning misbehavior</td>
<td>Infrastructure</td>
</tr>
<tr>
<td>A2</td>
<td>DoS Attack - WAVE BSM</td>
<td>Infrastructure</td>
</tr>
<tr>
<td>A3</td>
<td>Misbehaving/ Faulty node</td>
<td>Infrastructure</td>
</tr>
<tr>
<td>A4</td>
<td>Sybil attack</td>
<td>Infrastructure, Application</td>
</tr>
<tr>
<td>A5</td>
<td>Position attack</td>
<td>Infrastructure, Application</td>
</tr>
<tr>
<td>A6</td>
<td>DoS Attack</td>
<td>Application</td>
</tr>
<tr>
<td>A7</td>
<td>Message Falsification</td>
<td>Application</td>
</tr>
<tr>
<td>A8</td>
<td>Spoofing Attack</td>
<td>Application</td>
</tr>
<tr>
<td>A9</td>
<td>Blackhole</td>
<td>Application</td>
</tr>
<tr>
<td>A10</td>
<td>Replay Attack</td>
<td>Application</td>
</tr>
<tr>
<td>A11</td>
<td>Man-in-the-middle</td>
<td>Application</td>
</tr>
</tbody>
</table>

III. SECURITY WITHIN CVT STANDARDS

A. CVT Standards

DSRC is a set of standards that facilitates fast and secure vehicular communication. WAVE is a part of DSRC and is used to implement DSRC in higher layers of the DSRC protocol stack. DSRC operates in the 5.850 to 5.925 GHz band, and is capable of delivering 27 Mbps data rate through
the use of two-way line-of-sight short-range radio [10]. The two basic units of DSRC architecture are the Road-Side Unit (RSU) and the On-Board Unit (OBU). The OBU is a network device employed to perform vehicular communication in a vehicle; the RSU is a stationary unit that is used to connect the OBU to the access network and the core network. Communication between the OBU and the RSU is handled by the WAVE standards suite. Figure 1, which is derived from [11], illustrates the DSRC protocol stack along with protocols/standards correlating to different layers. The protocol stack for DSRC communication consists of the Physical layer (PHY), Data Link layer, Network/Transport Layer, and Application Layer. The Data Link layer includes medium access control (MAC). Within IEEE 802.11, DSRC is known as IEEE 802.11p (WAVE) which is utilized at the PHY and MAC layers [11]. The architecture and operational details of the DSRC channel are handled by IEEE 1609 standards at the higher layers of the DSRC protocol stack. The family of IEEE 1609 standards include IEEE 1609.2 - IEEE Standard Security Services for Applications and Management Messages, IEEE 1609.3 - Networking Services (including WAVE Short Message Protocol WSMP), IEEE 1609.4 - Multi-Channel Operation, IEEE 1609.11 - Over-the-Air Electronic Payment Data Exchange Protocol for Intelligent Transportation Systems (ITS), and IEEE 1609.12 - Identifier Allocations [12]. DSRC also supports TCP and UDP at the Transport layer and IPv6 at the application layer. While WSMP and IPv6+TCP/UDP can both be used for communication, the choice between the two depends on the application requirements. For example, WSMP is bandwidth-efficient and thus, preferred for single hop messages while IPv6 is used in instances where routing capabilities have higher priority [11].

While the standards mentioned above are used in US, the European markets use Intelligent Transport System (ITS) which has been created within European Telecommunication Standardization Institute (ETSI) [13]. ITS architecture is a layered model similar to the OSI model with an Application Layer (top), a Facilities layer, a Network and Transport Layer, and an Access Technologies Layer (bottom). The Access Technologies layer interfaces with the available communication technologies such as ITS-G5, Wi-Fi, 3G, and DSRC [14]. ITS-G5 is the equivalent of IEEE 802.11p and allows for direct and low latency V2V and V2I communication in a peer-to-peer configuration. It should be noted that DSRC refers to a different technology in Europe as compared to the US. In Europe, it is a short-range communication technology, which uses V2I communication in a master-slave configuration and is used for applications such as electronic toll collection [14].

B. Security Mechanisms in CVT Standards

IEEE 1609.2 covers methods of securing WAVE management/application messages. It defines the secure message formats that can be used as well the processing of such messages within the DSRC/WAVE systems. It also describes administrative functions necessary to support the core security functions. IEEE 1609.2 provides mechanisms for ensuring encryption of confidential data and authentication of messages by using the cryptographic mechanisms of secret-key or symmetric algorithms, public-key or asymmetric algorithms, and hash functions. IEEE Guide for Wireless Access in Vehicular Environments (WAVE) Architecture [15] has a detailed discussion on WAVE security mechanisms.

![Fig 1. Architecture and protocols for DSRC communication in US](image)

WAVE security services include two main components – Security Processing Services, and Security Management Services. Security Processing Services provide security for communications between the sender’s and receiver’s application/management basic service messages (BSMs). IEEE 1609.2 requires BSMs to be authenticated using a complicated public key infrastructure (PKI). When sending a BSM, the sender invokes the Security Processing Services to convert the BSM to a secure BSM before sending it to the receiver. The secure BSM contains data signed using a cryptographic private key and a corresponding digital signature for data authentication. The receiver, on receiving the secure BSM, invokes its Security Processing Services to decode and return the original BSM. Since BSMs are primarily broadcast messages, encryption of these messages is not practiced in this security standard. Security Management Services provide the Certificate Management Entity (CME) and Provider Service Security Management Entity (PSSME) to assist with handling certificates for this task. The CME stores information related to the trust state of certificates, which will be required for receiver-side processing of the Security Processing Services. When the receiver wants to verify the signed data received by it, it checks its local repository of known CA certificates to construct a certificate chain from the sender’s certificate to a known trust anchor. The PSSME manages the certificates that the sender uses to sign the BSMs [15].

A WAVE device can request Security Processing Services to sign a WAVE Service Announcement (WSA). A WSA is a management message containing information related to the announcement of the availability of an application-service. Signing a WSA authenticates that the WAVE device is authorized to advertise the signed application-services. This prevents privacy and operational risks that can be posed by an eavesdropper broadcasting bogus WSA advertising a service. Examples of such risks...
include personal data collection by such an eavesdropper, and creating denial-of-service attack by broadcasting bogus WSA{s that will be responded to by a high number of WAVE devices in an area of dense network traffic creating significant channel congestion. The IEEE 1609.2 standard also provides mechanisms to protect privacy. Threats to privacy in a CVT network can result from a number of different sources. Information from individual application messages from the same sender obtained by an unauthorized recipient can compromise the sender’s privacy. To counter these threats for broadcast applications, applications that don’t use encryption before broadcasting should not include personal driver information; for non-broadcast operations, encryption of messages should be used to provide confidentiality. At the application layer, vehicles can use either the security mechanisms specified in IEEE 1609.2 or they can use the applications’ security mechanisms to provide confidentiality, authentication, integrity, and non-repudiation. Below the application layer, Internet Protocol Security (IPSec) is also supported by the IEEE 1609 data plane. Information from signaling data such as source and destination addresses associated with an application should also be changed from time to time. IEEE 1609.4 provides an Address Change primitive to trigger a MAC address change [15]. To address overall platform security considerations, authorization and authentication should only be provided with certificates, and access to communication channels should only be guaranteed to authorized applications. It is also important that the CA knows an application to be trustworthy before it can apply for certificates. The process to ensure this has not yet been defined as a part of WAVE security considerations.

Within the ITS-G5 standard, each component of the vehicular network architecture (vehicle, roadside unit, backend unit) is referred to as an ITS-S (ITS-Station). Communication security requirements between sending and receiving ITS Stations can be categorized as external and internal security requirements[16]. External security is related to "security and trust towards external communication peers and the network" [16], internal security is related to the "protection of applications from actions of other applications and protection of shared information"[16]. Trust relations in ITS are built using certificates obtained through a Trusted Third Party called an Enrollment Authority (EA). A set of predefined security properties should be fulfilled by the ITS-S before it can be certified by an EA. This certificate by the EA allows the ITS-S to gain authorization into the ITS services. Confidentiality of information is protected using encrypted messages which can be decrypted only by the recipient. The true identity of the sender is kept confidential by sending all messages pseudonymously [16]. Discussion in this paper is centered around exploitation of technology used in the US, and attacks exploiting ITS have not been discussed.

IV. INFRANSTRUCTURE LEVEL ATTACKS

Attacks can be classified as infrastructure-level attacks if the outcome impacts multiple applications or common infrastructure such as VANETs, RSUs, or backend systems. Possible traditional attacks that can potentially disrupt vehicular network operations at the infrastructure-level are platooning attacks, Denial of Service (DoS) attacks, creating a black hole, abuse of RF fingerprinting, masquerade attack by malicious nodes, illusion attacks, position attacks, and Sybil attacks [17]. Variants of these attacks tailored to vehicular networks can result in disastrous consequences. This section discusses in detail both new and traditional attacks that pose threat to a vehicular network.

A. Platooning Attacks

Cooperative Adaptive Cruise Control (CACC) or platooning is used to control the speed of multiple vehicles (nodes) at an agreed upon inter-vehicle distance. Attacks leading to misinformation in the CACC system can have fatal consequences. In [18], the authors discuss attacks strategies for the CACC system and their respective mitigation techniques. The types of attacks introduced in [18] are:

- Reduced headway attack, which occurs when a malicious node ignores the recommended headway speed for a platoon.
- Misreport attack, where a node misinforms the following node to modify its behavior.
- Collision induction attack, which occurs when a leading node broadcasts a message indicating increase in speed while aggressively breaking to cause errors between itself and following nodes.

Each node is required to model the expected behavior of the node in front on it from the upstream control information broadcasted by that node. Attacks are detected by comparing this expected behavior with the observed behavior. If abnormal behavior is detected, the node can switch from cooperative ACC to radar-only ACC which is safe even if the preceding node is malicious.

B. DoS attack on a WAVE BSM

Vehicles in a vehicular environment achieve V2V communication by periodically broadcasting a BSM, which contains their positions and other metrics of interest. A DoS attack on an application that requires reliable transmission of BSMs from vehicles in the network could result in fatal consequences. The 802.11 MAC layer is vulnerable to a range of DoS attacks [19]. Owing to the mobility pattern in vehicular environment and the number of BMSs, the consequences of a DoS attack are capable of amplification, which exceeds the effect of similar attacks in other 802.11 based networks [19]. BSMs use the service channel of WAVE; the control channel is used by RSUs for system messages. A multi-channel coordination function in WAVE architecture dictates when each channel can transmit by dividing transmission time into control channel (CCH) interval and service channel (SCH) interval. There is a guard interval at the beginning of each CCH and SCH interval, during which no transmission is allowed – this guard interval is marked by a channel busy indication by the MAC layer. An attacker can exploit this channel synchronization property to cause channel congestion. If a transmission is sent after...
the guard interval expires but before the AIFS interval ends, all other nodes in the transmission range of the attacker who want to send a BSM would be delayed. The nodes that initiates the deferred BSM will begin their back-off processes simultaneously, which will result in extending the jamming caused by the attacker. Mobility of the vehicular network also carries the effect of this DoS attack beyond one or two hops.

In [19], the authors have simulated the DoS attack of WAVE BSM using the network simulator, Qualnet. The results from these simulations demonstrate that with the aggregate strength from the attacker’s and legitimate node’s signals, the effect of the DoS attack can reach far-away nodes which are beyond the radio range of the attacker. In [20], the authors provide an algorithm for real-time detection of DoS attacks in IEEE 802.11p vehicular networks using analytic models and detecting possible malicious behaviors. They define the optimal range of time duration between transmission of two BSMs such that BSMs from different vehicles don’t collide. This range is used to group vehicles in a platoon into different sets whose BSMs are unlikely to collide with each other. With the collision ruled out, the detector records the BSMs, which have been successfully received. If one BSM in not received in at least one group amongst all the sets, it is considered as an ‘alarm’ for a probable attack. Performance evaluation of this algorithm indicates an average probability of detection of DoS attack to be no lower than 0.9 and no false alarm for probability of attack.

C. Misbehaving and faulty nodes

Even though possession of the relevant certificates can be used to validate a node, they do not guarantee that the certified node will provide correct information. A certified node could also inject faulty data in the network. In [21], the authors propose a method of node revocation in case of misbehaving faulty nodes by using a combination of:

(i) Centralized revocation of a node by the CA.

This is done using Revocation of Trusted Center (RTC). Assuming each node has a Trust Component (TC), which is tamper resistant hardware and firmware that stores all cryptographic material, RTC can leverage the TC for revocation. When a Certificate Authority (CA) decides that a node should be revoked, it can initiate a two-party end-to-end protocol with the help of the RSU that instructs the TC to erase all cryptographic material (keys) it stores and stop its erase operation once the material has been erased. The

1 Arbitrary Inter-Frame Space (AIFS) is the period of time for which the media must be idle before the transmitting node (OBU) can begin its back-off procedure. Each transmitting node has a back-off counter that decrements by 1 with each timeslot that the AIFS is empty. When the back-off counter value becomes zero, the transmitting node can use the channel for transmission. Nodes that were jammed as a result of the initial DoS attack may accumulate a number of unsent messages which they might try to transmit once they are out of range of the attacker, extending the DoS attack.

(ii) Local detection of misbehavior performed by each node

A Misbehavior Detection System (MDS) is used to isolate a faulty node. A MDS consists of legitimate nodes evaluating their own sensory input and messages received from their neighbors against a set of evaluation rules to classify whether safety messages received by their neighbors are faulty or correct. Messages are considered false if they are outdated (indicative of replayed messages), contradictory to the state of the receiving node, or received beyond their area of propagation. For example, if a node receives a traffic jam message from one of its neighbors while its own velocity in the concerned area doesn’t indicate a traffic jam, the sending node can be considered as misbehaving.

Misbehavior detection in MDS is done in a manner similar to an Intrusion Detection Systems (IDS) by keeping a lookout for known misbehaviors (known attack signatures by malicious nodes) as well as data anomalies that do not follow a known pattern. Unlike IDS, the definition of normal behavior used to identify anomalies in vehicular networks is dynamic and changes constantly. The authors propose building data models on the fly using available literature on this topic to represent normal behavior.

(iii) A distributed, localized protocol for the eviction of an attacker.

The principle of Local Eviction of Attackers by Voting Evaluators (LEAVE) protocol is that upon detection of a misbehaving node by node n, n broadcasts warning messages to all nodes in range to temporarily evict the neighbor. This eviction only holds till the misbehaving node stays in contact with the nodes running LEAVE. But this gives the CA a chance to collect enough evidence against the node to initiate the revoking protocols. LEAVE also provisions against wrong accusations since all nodes can be attackers with the same probability. As stated in [21], accusation issued by a node has a lower weight when this node is already accused by other participants. If the sum of weighted accusations (the eviction quotient) against a vehicle exceeds a defined threshold, it is locally evicted by LEAVE.

D. Sybil attack and position attack

In a Sybil attack, the identity of the node performing the attack can masquerade as multiple simultaneous identities. Such a type of attack affects network topologies, bandwidth consumption, and vehicular network connections [4]. For instance, an attacker might give an illusion of 100 vehicles on a 1 km highway by assuming simultaneous identities.
These illusions change the network topology and interfere with correct usage of vehicular applications. When legitimate nodes try to communicate with the nodes created by Sybil attacks, they receive no response and as a result, retransmit the packets, which leads to unnecessary network bandwidth consumption. A position attack results from an attacker modifying position packets, replaying old or bogus position packets, or dropping urgent position packets [4]. A position attack and a Sybil attack can be combined to form a harmful attack that is harder to prevent. This is because the real nodes can only perceive the imaginary nodes through abstract information about bogus positions and thus, cannot physically verify the presence of those nodes. In [22], the authors have proposed a solution to Sybil attacks. Their solution uses data from 3 different sources to remedy the abstract nature of node information. Each of the three sources – radar detections, oncoming traffic reports, and neighbors’ reports are given weightings on terms of their potential reliability. Radar detections, when applicable, are most trustworthy and have the largest weight. If not, neighbors’ positions have the largest weight. The average position and velocity of the node under consideration is computed from all available reports and a history of the roadmap of all available data point over a period of time is stored. When a position based query about a node needs to be made, nodes can rebuild the target (attack) node’s map history virtually and validate the position information. In [23], a Sybil attack detection mechanism, Footprint, is discussed. Footprint adopts an event-oriented linkable ring signature scheme for RSUs to issue authorized messages to the vehicles that require such messages as proof or presence. These authorized methods are location hidden, and signature scheme for RSUs to issue authorized messages to

A. DoS Attack using radio jamming

Radio jamming can be used to block either the control channel or the service channels used by IEEE 802.11p standard. In [22], the authors demonstrate the negative impact of RF jamming on V2V communications by implementation of various OFDM jamming patterns and measurement of their impact on the packet delivery rate.

B. Message Falsification Attack

A message falsification attack is performed by listening on a wireless medium for BSMs, manipulating the contents of the received messages, and rebroadcasting them. The contents of the BSMs can be manipulated by changing values of different fields such as the acceleration field or the velocity field.

C. Spoofing Attack

A spoofing attack can be created by an adversary impersonating as another vehicle in the network in order to inject fraudulent information. Spoofing attacks can be used to inject false information in a CACC platoon to induce instability in the string and cause accidents.

D. Black Holes

Black holes are formed by nodes that fail to propagate messages. These nodes are typically misbehaving nodes in the vehicular network. The adverse effects of black holes include dropped traffic messages and service requests. With enough misbehaving nodes participating in the formation of a black hole, the attackers can partition the vehicular network in such a way as to isolate legitimate nodes with lack of information. Legitimate nodes may be prevented from receiving critical updates about revoked nodes leaving them and by extension the whole network vulnerable to masquerade attacks.

E. Replay Attacks

Replay attacks are attacks, in which an attacker resends old messages to achieve network manipulation. A simple measure to prevent these attacks is to have a cache of recently received messages at all nodes, and compare every new message against this cache to rule out a replay attack [24].

A strong cryptographic system can be utilized to defend against application layer attacks. Integrity, authentication, and non-repudiation of BSMs can be achieved by utilizing digital signatures. Digital signatures can also protect such messages from unauthorized changes. Public key infrastructure (PKI) is an example of such a cryptographic system. In vehicular PKI, each node is equipped with a public/private key pair, which has been certified by a Certification Authority. The sender node uses the private key to digitally sign the message and used the receiver node’s public key for validity of the message. Key distribution is a challenge for vehicular PKI. Digital signing algorithms such as RSA or ECC can be used for this purpose.

V. APPLICATION LEVEL ATTACKS

Attacks can be classified as application-level attacks if the impact of their outcome is limited to the application being attacked. Under normal attack conditions, these attacks can be isolated and mitigated without widespread impact to the vehicular network infrastructure. It should be noted that unanticipated escalation of these attacks could have widespread impact and also affect the infrastructure. This section discusses some of the traditional application-level attacks for vehicular networks.

A. DoS Attack using radio jamming

Radio jamming can be used to block either the control channel or the service channels used by IEEE 802.11p standard. In [22], the authors demonstrate the negative impact of RF jamming on V2V communications by implementation of various OFDM jamming patterns and measurement of their impact on the packet delivery rate.

B. Message Falsification Attack

A message falsification attack is performed by listening on a wireless medium for BSMs, manipulating the contents of the received messages, and rebroadcasting them. The contents of the BSMs can be manipulated by changing values of different fields such as the acceleration field or the velocity field.

C. Spoofing Attack

A spoofing attack can be created by an adversary impersonating as another vehicle in the network in order to inject fraudulent information. Spoofing attacks can be used to inject false information in a CACC platoon to induce instability in the string and cause accidents.

D. Black Holes

Black holes are formed by nodes that fail to propagate messages. These nodes are typically misbehaving nodes in the vehicular network. The adverse effects of black holes include dropped traffic messages and service requests. With enough misbehaving nodes participating in the formation of a black hole, the attackers can partition the vehicular network in such a way as to isolate legitimate nodes with lack of information. Legitimate nodes may be prevented from receiving critical updates about revoked nodes leaving them and by extension the whole network vulnerable to masquerade attacks.

E. Replay Attacks

Replay attacks are attacks, in which an attacker resends old messages to achieve network manipulation. A simple measure to prevent these attacks is to have a cache of recently received messages at all nodes, and compare every new message against this cache to rule out a replay attack [24].

A strong cryptographic system can be utilized to defend against application layer attacks. Integrity, authentication, and non-repudiation of BSMs can be achieved by utilizing digital signatures. Digital signatures can also protect such messages from unauthorized changes. Public key infrastructure (PKI) is an example of such a cryptographic system. In vehicular PKI, each node is equipped with a public/private key pair, which has been certified by a Certification Authority. The sender node uses the private key to digitally sign the message and used the receiver node’s public key for validity of the message. Key distribution is a challenge for vehicular PKI. Digital signing algorithms such as RSA or ECC can be used for this purpose.

V. APPLICATION LEVEL ATTACKS

Attacks can be classified as application-level attacks if the impact of their outcome is limited to the application being attacked. Under normal attack conditions, these attacks can be isolated and mitigated without widespread impact to the vehicular network infrastructure. It should be noted that unanticipated escalation of these attacks could have widespread impact and also affect the infrastructure. This section discusses some of the traditional application-level attacks for vehicular networks.

A. DoS Attack using radio jamming

Radio jamming can be used to block either the control channel or the service channels used by IEEE 802.11p standard. In [22], the authors demonstrate the negative impact of RF jamming on V2V communications by implementation of various OFDM jamming patterns and measurement of their impact on the packet delivery rate.

B. Message Falsification Attack

A message falsification attack is performed by listening on a wireless medium for BSMs, manipulating the contents of the received messages, and rebroadcasting them. The contents of the BSMs can be manipulated by changing values of different fields such as the acceleration field or the velocity field.

C. Spoofing Attack

A spoofing attack can be created by an adversary impersonating as another vehicle in the network in order to inject fraudulent information. Spoofing attacks can be used to inject false information in a CACC platoon to induce instability in the string and cause accidents.

D. Black Holes

Black holes are formed by nodes that fail to propagate messages. These nodes are typically misbehaving nodes in the vehicular network. The adverse effects of black holes include dropped traffic messages and service requests. With enough misbehaving nodes participating in the formation of a black hole, the attackers can partition the vehicular network in such a way as to isolate legitimate nodes with lack of information. Legitimate nodes may be prevented from receiving critical updates about revoked nodes leaving them and by extension the whole network vulnerable to masquerade attacks.

E. Replay Attacks

Replay attacks are attacks, in which an attacker resends old messages to achieve network manipulation. A simple measure to prevent these attacks is to have a cache of recently received messages at all nodes, and compare every new message against this cache to rule out a replay attack [24].

A strong cryptographic system can be utilized to defend against application layer attacks. Integrity, authentication, and non-repudiation of BSMs can be achieved by utilizing digital signatures. Digital signatures can also protect such messages from unauthorized changes. Public key infrastructure (PKI) is an example of such a cryptographic system. In vehicular PKI, each node is equipped with a public/private key pair, which has been certified by a Certification Authority. The sender node uses the private key to digitally sign the message and used the receiver node’s public key for validity of the message. Key distribution is a challenge for vehicular PKI. Digital signing algorithms such as RSA or ECC can be used for this purpose.
as NTRUSign, ECDSA, and RSA Sign can be used due to small signature size [25]. Another disadvantage of using a complex cryptographic system such as PKI is high bandwidth and resource utilization, which may lead to packet collision and degradation of service in a wireless channel. While adding digital signatures impacts the bandwidth usage, the excessive usage can be curbed by using a suitable method for distribution of certificates. In [26], the authors solve the problem of communication overhead in vehicular cybersecurity by combining pre-distribution of certificates instead of bundling all relevant certificates in a trust chain. In each signed message, and omission schemes which determine the frequency of omitting certificates. This technique is aimed at reducing cryptographic packet loss. The use of strong cryptographic system and pre-distribution of certificates also creates traceability that can be used to create awareness regarding a node outside of the local short-term cooperative awareness needed for vehicular network decisions. This traceability correlates to personal driver information which can be used for identity based attacks. To this end, pseudonymous identifiers that can change unpredictably can be applied to each vehicle to avoid traceability and linkability beyond a short period of time. [27] provides a survey of popular pseudonym mechanisms used in vehicular networks. To maintain integrity while providing navigational support about large areas of a road to a sizeable number of nodes, in-network data aggregators are used. These aggregators combine traffic reports and such from various nodes and aggregate the findings before sharing with the network. In [28], the authors have presented a novel cluster-based integrity protection mechanism suitable for in-network aggregation of traffic status and similar information. This approach does not require expensive hardware and is not limited to small scale events owing to its property of inter-cluster communications.

VI. FUTURE RESEARCH DIRECTIONS

Development of security within CVT systems gains more importance as the commercial use of this technology gains momentum. A Gartner report has forecasted the availability of a quarter billion connected vehicles on the road by 2020 [31]. Car manufacturers, tech companies, and car-hailing service providers (such as Uber) are all making strides in introducing self-driving cars to the consumer market. The primary challenge for protecting CVT systems is to design security mechanisms that are effective in highly dynamic network topologies. Within the last decade, several efforts have been devoted to designing solutions that accommodate this attribute of vehicular networks. Numerous publications such as [18], [21], and [22] have examined attack strategies relevant to CVT systems and have demonstrated resolutions of these attacks. Substantial progress has also been made in developing more efficient lightweight cryptographic systems, which can provide confidentiality and privacy with lower latency and bandwidth utilization. Security practices such as utilization of pseudonyms [27] are being developed to ensure that the personal information of drivers is not compromised. The standards used for vehicular networks have also evolved within the last decade to better serve security purposes in vehicular networks. A subject undergoing intense study currently is security within the CACC application of CVT. This could be because of automobile manufacturers’ interest in making this application commercially available as soon as possible. Several vehicles launched in 2016 already boast of the availability of CACC and other connected vehicles applications.

CVT applications being commercially available has also given rise to crucial discussions on the issues of regulation within software application development, cyber-liability in case of software/hardware malfunctioning, and infrastructural development to support connected vehicles. Some of the questions within infrastructural development at the software level include: how to ensure that the applications being used by the drivers are secure, how to send secure messages within cars at an acceptable low-latency, how to provide centralized security to the complete connected vehicles system (on-road and roadside both), and how to aggregate security data and provide relevant security updates to all concerned areas of the connected vehicles system.

While CVT security challenges have independently been sufficiently addressed by the research community, a centralized approach to security is missing. As an ongoing research effort, we are working towards development of a unified security framework that can be implemented within the connected vehicles system. The benefits of such a system would include easier management of the security infrastructure, faster response time to security concerns, centrally available comprehensive repository of metrics like attack signatures and node reputation that can be referred to in the decision making process, and more efficient enforcement of new relevant security policies. We are currently working on the development of a system design for connected vehicles, which focuses on the abstraction of different layers of functionality such as a messaging layer, a connectivity layer, and a backend management layer. The idea behind this abstraction is to limit the system information required by application developers to develop applications for connected vehicles and to allow the connected vehicles system to be the authority of how any incoming information gets handled. While the current state of our development is not specifically focused on security, we expect to use this system to build a security infrastructure in the near future. We envision incorporating principles of Software-Defined Networks (SDN) which align with the abstracted system model we are building to have a control plane that can dispense security decisions to a sub-section of the system. Central security decisions can ensure that all systems are equally secure and avoid threats from exploiting a weak link in the network. Owing to the large scale nature of the vehicular network (spanning across long stretches of the road network), we envision using Network Function Virtualization (NFV) to ensure dynamic availability and optimal utilization of resources. We expect roadside security infrastructure to work with multiple security devices (such as IDS, IPS, and firewalls) depending on the situation and
NFV is a comparatively lower cost, more dynamic method of achieving this. We plan to test the SDN and NFV incorporated architecture using the system design and testbed we have deployed at the Clemson University. We hope that the successful implementation of our design will assist in a more secure connected vehicles network for drivers and regulatory authorities alike.

REFERENCES


