A Systematic Approach for Attack Analysis and Mitigation in V2V Networks

Bharat Bhargava, Amber M. Johnson, Gisele Izera Munyengabe, and Pelin Angin*
Purdue University, West Lafayette, IN 47907 USA
{bbshail, john1333, gizeramu, pangin}@purdue.edu

Abstract

The increasing popularity of V2V networks with the rise of driverless cars in the recent years have made them vulnerable to attacks in growing complexity. Accurate assessment of the safety and security needs of V2V networks based on context and the costs associated with attack mitigation mechanisms are significant for successful operation of these networks despite adversaries trying to disrupt their functions. In this paper we provide an analysis of the major security and reliability issues in V2V networks, and propose a systematic approach for the analysis and mitigation of attacks, based on the break-down of attacks into common feature sets. We also provide cost analyses of major classes of V2V attacks using the proposed model. The proposed analysis approach is promising to provide guidance for research in optimization models for tradeoffs between security, safety and performance requirements in V2V.

Keywords: V2V networks, safety, security, attack mitigation

1 Introduction

Vehicle-to-vehicle (V2V) communication allows vehicles to communicate with other vehicles and roadside infrastructure in the network to exchange data related to traffic jams, safety warnings etc. [1, 2]. The main goal of V2V communications is to provide assistance to drivers and prevent accidents. When a vehicle receives data, its internal system responds accordingly in attempt to keep the vehicle safe. When vehicles communicate with one another, they pass messages that are processed by an internal system to issue safety preservation methods. Though these features are intended to increase the safety of the vehicle, they present vulnerabilities that can be exploited [2]. This can be viewed as an attack surface in which those with malicious intent can jeopardize the safety of a vehicle. The attack surface includes all the possible ways to attack a target. The more connectivity vehicles have, the larger is the attack surface, and the more vehicles are aware of their environment, the greater the harm that can be done when an attack is issued on a vehicle [3].

Major classes of attacks on V2V include threats against availability, integrity, authenticity, and confidentiality, among others [4]. Each of these attacks also have subclasses as listed below [4]:

- Availability
  - Denial of service (DoS)
- Integrity
  - Tampering

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 7:1 (Mar. 2016), pp. 79-96
*Corresponding author: Department of Computer Science, Purdue University, 305 N University St, West Lafayette, IN 47907, USA, Tel: +1-765-237-9037

  - Masquerade
  - Replay
  - Injection
- Authenticity
  - Tampering
  - Masquerade
- Confidentiality
  - Eavesdropping

In this paper we focus on analyzing the actions, impacts on safety and mitigation of V2V attacks, as well as the relationships between safety, security and performance requirements in V2V communication. We provide an analysis of the safety, security and performance requirements of V2V and V2I (vehicle-to-infrastructure) systems, and the possible mechanisms to enforce the security requirements. We mainly focus on the vulnerabilities of V2V communication that could be exploited by attackers, which can jeopardize the safety of a vehicle. We provide descriptions of major attacks on V2V according to a systematic attack analysis scheme we developed. Breakdown of attacks according to the proposed scheme will allow V2V researchers to easily associate costs with each attack when modeling the quantitative relationships between safety, security and performance requirements to provide optimal system functioning.

The overarching goal of this work can be summarized as follows:

- Analyzing a set of safety, security and performance requirements in V2V along with mechanisms for enforcing them, and techniques to assess these
- Providing guidance for dynamic adaptation of intelligent transportation system (ITS) applications to context and need changes using the results of the analyses
- Guiding the development of quantitative models for the relationships/tradeoffs between safety, security and performance in V2x

The rest of this paper is organized as follows: Section 2 gives a summary of the data security and reliability issues in vehicular ad hoc networks (VANETs). Section 3 presents our proposed approach for systematic analysis of attacks on V2V. Section 4 provides an analysis of major attacks on V2V using the proposed attack analysis scheme. Section 5 presents a novel mechanism for privacy-preserving dissemination of data in V2V. Section 6 concludes the paper with future work directions.

2 Data Security and Reliability Issues in VANETs

2.1 Data security issues

In a V2V network, vehicles rely on the integrity of data they receive from other vehicles and road side units to make decisions regarding safety messages and alerts. Various attacks and unfavorable conditions as listed below cause data security issues, which hurt the performance and safety of the networks in question.

- The amount of contact time with other vehicles might be limited for secure channel establishment, resulting in packet loss [5]

- Attackers may have full access to a generic DSRC (dedicated short-range communications) radio, which enables them to read the messages in the reception range, as well as broadcast messages and replay messages maliciously. Organized attackers might deploy grids containing hundreds of DSRC radios [5].
- If integrity of broadcast data is compromised, vehicles may present erroneous warnings to drivers, resulting in disastrous control decisions [6].
- If data authentication is not provided, malicious vehicles might impersonate an emergency vehicle to perform actions that would normally be punished [6].
- If non-repudiation is not supported, a malicious vehicle could report false emergency situations to obtain more favorable driving conditions for themselves [6].
- Attackers may broadcast packets with forged positions or block packet forwarding, resulting in decreased packet delivery [6].
- Authentication protocols face challenges including
  - Certification distribution and revocation
  - Computation and communication bottlenecks
  - Decreased reliance on tamper-proof devices

Data security in V2V networks is generally provided using well-known cryptographic protocols. Each protocol targets a different aspect of the system as listed below, to provide complete security.

- Certificate verification: Verification of certificates exchanged between vehicles and Road Side Units (RSUs) is required for all protocols. [6]
- Authentication: This is a core security requirement for VANETs to prevent message manipulation. [6]
- Secure positioning: RSUs, assumed to be trustworthy, determine vehicles' positions using distance bounding. Both GPS data from vehicles and position data from RSUs need to be secured. [6]
- Identification of misbehaving nodes: Revocation of misbehaving nodes is crucial. Fast identification of such nodes is needed for timely response. [6]

Identification of appropriate metrics for assessing the security of a V2V network is essential for development of performance and security models accurately representing real-world conditions. V2V researchers have proposed various metrics to measure the security of a V2V network. Among the ones with most widespread use are the following:

- Secure throughput: The amount of integrity-preserved payload size divided by the total time to process it using the authentication protocol
- Error detection rate / Acceptance of corrupt data: The percentage of errors detected in all erroneous packets transmitted and percentage of corrupt data accepted
- Certificate revocation speed: Time to detect fradulent users and revoke certificates issued to them
- Degree of privacy: Level of privacy protection provided for data transmitted by vehicular nodes (ideally to achieve at least the same level of privacy currently achieved without vehicular networks)

2.2 Reliability issues

The reliability of a V2V network is of utmost importance for the safety of the vehicles in the network. Three main factors hinder V2V reliability [7]:

- Hidden terminal problem in broadcast: Hidden terminals are two terminals sharing a set of terminals within the transmission range of both, while they are outside the interference range of each other. This is a critical issue in performance, as hidden nodes cause data packet collisions.
- Radio channel fading in DSRC: Multiple reflecting objects degrade quality of received signal. Fading effects from mobility of senders/receivers need to be accounted for.
- Impact of high mobility: High mobility may cause adverse effects on performance of sending/receiving (e.g. receivers may move out during transmission of safety-related message).

In order to match the reliability needs of safety-critical applications, the following requirements need to be met by V2V networks, based on the findings of previous research:

- DSRC safety-related communication must deliver messages with high reliability within their lifetime.
- The probability of the message delivery failure in a vehicular network should be less than 0.01 [8].
- Safety-critical applications require at most a 100 ms mean delay to be effective [9].
- Beacon messages essential for many safety applications need to be sent out at an updating rate as high as 10 messages per second [10].

Much like security metrics, reliability metrics carry significance in assessing the real-world performance and safety of V2V networks. Among the most commonly used reliability metrics proposed by previous research are the following [7]:

- Packet reception ratio: Percentage of nodes that successfully receive a packet from a given node among the ones that node sends packets to
- Packet delivery ratio: Ratio of the number of packets successfully received by all receivers to the number of packets transmitted
- Successful packet delivery probability: Probability that a node within the transmission range of the sender successfully receives a packet from a given node
- Effective range: The range within which the worst case quality of service metrics is satisfied
- Connectivity in multi-hop VANETs: Minimum number of vehicles needed to have sufficient data transfer, and how far information can be effectively propagated

3 Attack Analysis Approach

In order to analyze an attack effectively, we identify the anatomy of an attack and the cost associated with its implementation and mitigation. We also construct a cross-feature analysis, identifying similar features across different attacks. In our analysis, we take into consideration the category of messages used to trigger the attack. In this work we only consider safety messages, but the proposed model can

be applied to different classes of messages as well. Raya and Hubaux [2] mention three classes of safety messages: (1) "traffic information messages used to disseminate traffic conditions", (2) "general safety-related messages" used for "public safety" and (3) "liability-related messages" used in case of urgency situations such as accidents. These messages include traffic information, speed, position and direction of the vehicle, and specific traffic events such as work zone, etc. [2].

We assume that five basic security requirements are to be fulfilled by a secure system. Those requirements are the following:

1. Each message must be authenticated
2. Data in each message must be consistent
3. The network must be available all the time
4. The sender of each message must be identified reliably
5. "Strict time constraint" of real-time messages must be honored. [2, 11].

[11] groups vehicular network applications under two major categories: (1) safety applications and (2) non-safety applications. Safety applications include pre-crash applications also known as active safety applications, and passive safety applications such as airbag and seatbelt. The latter is also known as a post-crash application. Non-safety applications are composed of "convenience applications" such as road status services that provide information on road congestion and parking assistance systems, and "comfort applications" used for entertaining and comfort. In this study, we only analyze the target of the attack [12]. We assume that the attacker employs legitimate means of communication to send fabricated messages.

Anatomy of an attack

The anatomy of an attack in the proposed analysis approach is a step-by-step breakdown of the features (or actions) that occur when an attack is deployed on a vehicle [13]. Each attack in the model is represented by fitting its features into the template given below.

Template

Name

ATTACK represents an attack. ATTACK is followed by a number specifying a code for the attack or the mitigation mechanism. The name after the code corresponds to the attack or the mechanism being analyzed in the unit.

Description

Description defines an attack or a mechanism being studied.

Features

This part is made of transactions that form an attack. T stands for transactions. T00 corresponds to the initial step taken by the target. T0x transactions correspond to regular operations of the target component. T followed by another number is a unique code for a transaction or a feature. Attacks involving the same transaction will have the same encoding. The state of the target (connected (T01a) or disconnected (T01b)) is assumed to be connected at the beginning.

Mitigation

Each attack can be prevented by a corresponding mitigation mechanism. For a given mitigation mechanism, there is a cost associated with its deployment.

Cost
Each attack has an associated cost. That is, there is a cost associated with implementing the attack as well as the impact that it has after it has been implemented. Each mitigation mechanism has a cost associated as well, as mentioned above.

Impact on safety
This component specifies how utilizing a mitigation mechanism influences the safety of the system.

Impact on security
This component specifies how utilizing a mitigation mechanism influences the security of the system.

4 Analysis of Major V2V Attacks

In this section, we provide a cost analysis of major attacks on V2V using the proposed attack analysis model. We start with a statement of basic assumptions regarding the V2V network and description of security primitives.

Assumptions
We assume that the network standard, Dedicated Short Range communication (DSRC) [14], is used, where the size of the safety messages alone are about 200 bytes (100 bytes of payload, 100 bytes of header) [15, 16]. We also use the simulation model parameters proposed by [17] as variables in the total cost estimation equation to calculate the total overhead of each attack. The cost estimation for each attack is determined by the overhead of each of its features. We add a constant, μ, to the estimation equation each time a message is received to account for the transmission time.

Message authentication: Elliptic Curve Digital Signature Algorithms (ECDSA)
Each vehicle is assigned private key that will allow the vehicle to digitally sign messages and authenticate itself to receivers, and each message is encapsulated in a SecuredMessage [18], which provides a security profile for the message sent. When a vehicle sends a safety message, it first signs it with its private key, and integrates the certificate provided by the certificate authority. The algorithm used for signing and verifying signatures is the ETSI recommended, ECDSA-256-SHA-256, algorithm. We use the security methods proposed by [18] for the generation and verification of a signature as follows:

Signature generation:

1. Compute message digest (i.e. SHA-256)
2. Sign message digest using ECDSA-256-SHA-256 and the private key of the ITS station certificate
3. Store generated signature and signer's information

Signature Verification:

1. Check content of SecuredMessage against the rules of the corresponding security profile

Table 1: Attack feature costs

Code	Transaction	Response(s)	Time	Total Cost
T00	Receive Message	insert message into queue + waiting time in the queue Data rate = 6 Mbps Transmission time	< 100 ms (time to wait in the queue) 0.27 ms	50 ms + μ
T01	Get Satellite Signal	Update location (10 Hz)	100 ms	100 ms
T01a	GPS Connection	Initialize GPS location and maintains connection	$\leq$ 5s	5s
T01b	GPS Disconnected	Fails to maintain connection	100 ms	100 ms
T02	Compute Position	Determine approximate GPS location	0.3 ms	0.3 ms
T1	Message Authentication	generate signature verify signature	0.26 ms 1.22 ms	1.48 ms
T2	Collision Distance	read and update location compute proximity to preceding vehicle or car aside, update status	0.2 ms 0.3 ms	0.5 ms
T3	Send Notification	send notification if distance below threshold	0.5 ms (transmission time between sensor and notification system)	0.5 ms
T4	Sniffing CAN	-	unbounded	unbounded
T5	Send malicious workload in CAN network	-	15 ms	15 ms

2. Validate certificate against timing, location and security considerations. If signer's certificate is unknown, request an unrecognized certificate

3. Check signature of the message using the steps for signature generation

Message Protocol: Basic method

We consider a basic message protocol proposed by [19]. The DSRC standards specify the operational frequencies and system bandwidths, and are used in the proposed protocol. Under the standards, each vehicle periodically sends messages over a single hop every 300 ms within a range of 10 s travel time. The inter-message interval drops to 100 ms and the range to 15 m if the vehicles are travelling at less than 10 mph. Vehicles make decisions based on the relative distances and timestamps of received messages and may transmit new messages accordingly.

Table 1 summarizes the costs associated with different transactions in the analysis. Each attack has at least four minimal features. These features include: receive message (T00), message authentication (T1), collision distance (T2), and send notification (T3). The summation of the costs of these features is represented by the variable T_x in our cost estimation equation. The total overhead, T_v, for an attack is calculated by adding all of its cost features to T_x.

General estimation:

$$T_v = T_r + T_x \tag{1}$$

T_v: total overhead
T_r: summation of feature costs for attack
T_x: T00 + T1 + T2 + T3

4.1 Timing Attack

Description
An attacker intentionally creates a delay in the network, which prevents safety messages from reaching their users in time [20, 3, 12]. This attack targets pre-collision application and convenience applications. The intruder's goal is to render required information useless by flooding the network communication or adding timeslots to messages, triggering this attack [20].

Features
T00: Receive message
T1: Message Authentication
T2: Collision Distance *
T3: Notification

Output: alert/warning/information

Upon arrival at its destination, a received message is authenticated. T2 is a specific feature of the pre-collision system. The fact that messages are delayed to reach the vehicle takes advantage of system computation delays such as computing the distance between vehicles. If it takes 1 ms to compute the distance and send a notification, the response of the driver or the breaking system is delayed by that 1 ms, which reduces the stopping distance critical to avoid and minimize the effect of the collision.

[12] argues that a lane change message not received on time can delay response. This situation is highly dangerous during rush hour traffic if a node A changes lanes and delays to send a message to node B behind it. B may respond successfully to the current situation. However, nodes following B may not have time to respond accordingly, thus causing numerous collisions.

In the case of convenience applications, if information is downloaded by the services applications, e.g. road status, the vehicle experiences a delay in time to get to its destination.

Mitigation

1. Firewall to filter-out packets arriving at vehicular network to prevent network flooding
2. Timestamp can be used to assess the timeliness of messages

Cost of the attack
C1: Warning/alert is not received in a timely manner for usefulness
C2: Response delay
C3: Entering dangerous road situation such as collision or causing traffic jam

Cost of mitigation

Table 2: Timing attack cost

Code	Transaction	Total cost
T00	Receive message	μ
T1	Message Authentication	1.48 ms
T2	Collision Distance	0.5 ms
T3	Send Notification	2 ms
	Total overhead	5.48 ms + μ

Computation overhead increases system reaction time. Table 2 provides a summary of the cost analysis for this attack.

Impact on Safety

Checking arriving packets with a firewall in order to filter-out malicious data packets may result messages from other vehicles or roadside unit (RSU) not reaching the destination in time. E.g. if a message about collision or obstacle in front of the current vehicle is not received in time the vehicle might be involved in a collision.

Impact on Security

Since malicious data are filtered out, a firewall prevents an attacker from introducing harm to the vehicle. However, the level of security of the algorithm used incurs high computational overhead.

4.2 GPS spoofing and hidden vehicle attack

Description

The attacker creates a "GPS-simulator" to generate false readings to deceive other vehicles [20, 3, 12]. Falsified positions are used to update "location tables", which are utilized for the vehicles' awareness of their surroundings [3, 12]. The *hidden vehicle attack* is a concrete illustration of GPS spoofing. In this attack, the attacker vehicle attempts to deceive another vehicle into believing that he is better placed for forwarding some warning message, thus leading to silencing the victim vehicle and making it hidden. This is equivalent to disabling the system [21].

Features

T00: Receive message
T01: Get satellite signal
T02: Compute position
T1: Message authentication
T2: Collision distance
T3: Send Notification

Output: Alert

It is critical that GPS regularly updates the vehicle position and receives updated authentication position, also known as location table [3, 12]. Thus T01 and T02 are critical features for the vehicle to accurately compute how far it is from other vehicles. This distance is also called *collision distance* in the features.

Mitigation

Table 3: GPS spoofing and hidden vehicle attack cost

Code	Transaction	Total cost
T00	Receive message	μ
T01	Get Satellite Signal	100 ms
T02	Compute Position	0.3 ms
T1	Message Authentication	1.48 ms
T2	Collision Distance	0.5 ms
T3	Send Notification	2 ms
	Total overhead	104.28 ms + μ

1. Use digital signatures or HMAC, which will provide data integrity and message authentication. Attacker needs to forge the signature of the GPS-data source in order to pretend to be a GPS-source, which is infeasible. Digital signatures will provide non-repudiation as well.

2. Assuming that there are at most k attackers, the possible victim broadcasts until k + 1 cars receive messages. This makes sure at least one car is in the correct state. If a distributed trust level model is deployed, the victim node might stop broadcasting when it meets a trustworthy node, i.e. a car with high trust level.

Cost of the attack
C1: No alert issued since messages are silenced
C2: Response delay
C3: Entering dangerous road situation such as collision or causing traffic jam

Cost of Mitigation
C4: Digital signature verification will take time, the length depending on the algorithm (e.g. 5 ms).
C5: The increased number of broadcasts due to the mitigation protocol can saturate the network.
Table 3 provides a summary of the cost analysis for this attack.

Impact on Safety
Digital signature verification may result in cryptographic loss. Queue of signed messages waiting for verification may become overloaded/full and messages from authenticated GPS data sources might be lost or delivered too late, which will result in wrong/outdated positioning information.

Impact on Security
It has a negative effect on real-time transactions. Resource problems such as overloaded queues can become a source of vulnerability for the system.

4.3 Tunneling attack

Description
Tunneling attack is another attack that cheats on geographic position. The intruder exploits momentary loss of position signal by injecting false position information before the attacked node can receive authentic position information from satellites [3, 12].

Table 4: Tunneling attack cost

Code	Transaction	Total cost
T01b	GPS Disconnected	100 ms
T01a	GPS Connected	5 s
T00	Receive message	μ
T01	Get Satellite Signal	100 ms
T02	Compute Position	0.3 ms
T1	Message Authentication	1.48 ms
T2	Collision Distance	0.5 ms
T3	Send Notification	2 ms
	Total overhead	5204.28 ms + μ

Features
T01b: GPS disconnected
T01a: GPS Connected
T00: Receive message
T1: Message authentication
T01: Get satellite signal
T02: Compute position
T2: Collision distance
T3: Send notification

Output: Alert
As an example, a vehicle A sends a message to vehicle B while still in the tunnel. B receives the message when its GPS is reconnected. B performs authentication of the message and computes how far A is from B's current position. As a result, the computation may issue a collision alert, causing the driver to react accordingly.

Mitigation
Digital signatures can be used to provide authentication, integrity and non-repudiation.

Cost of the attack
C1: No alert is issued since messages are silenced
C2: Response delay
C3: Entering dangerous road situation such as collision or causing traffic jam

Cost of Mitigation
C4: Digital signature verification imposes computation overhead. Table 4 provides a summary of the cost analysis for this attack.

Impact on Safety
Digital signature verification may result in cryptographic loss.

Impact on Security
It has a negative effect on real-time transactions. Resource problems such as overloaded queues can become a source of vulnerability for the system.

4.4 Masquerade attack

Description

The attacker constructs malicious messages targeting vehicles' critical systems like brakes, engine, dashboard, lights or steering wheel and injects these messages into the vehicular network, pretending to be a trusted source [3, 22].

Features

T4: Sniffing CAN Traffic
T5: Send malicious workload in CAN network
T00: Receive message
T1: Message Authentication
T2: Collision Distance *
T3: Notification

Mitigation

1. Use digital signatures or HMAC, which will provide data integrity and message authentication. Attacker will need to forge the signature of the corresponding source ECU in order to construct malicious message coming from trusted source, which is infeasible. Digital signatures will provide non-repudiation as well.

2. Checksums offer weak protection since they rely on weak cryptographic functions, but impose small performance overhead and can be used in non-critical vehicle systems.

3. Active Bundles (AB) encapsulate sensitive data with policies and policy enforcement engine [23, 24, 25, 26, 27] to provide privacy and integrity protection. We provide a more detailed description of this approach in section 5.

Cost of the attack

C1: No alert issued since legitimate messages are silenced
C2: Response delay
C3: Entering dangerous road situation such as collision or causing traffic jam

Cost of mitigation

C4: Digital signature verification will take time, the exact amount depending on the algorithm. Table 5 provides a summary of the cost analysis for this attack.

Impact on Safety

Digital signature verification may result in cryptographic loss. Queue of signed messages waiting for signature verification may become overloaded / full and then messages from authenticated ECUs might be lost or delivered too late. It may result in applying brakes too late or in late reaction of wheels on steering wheel rotation or in engine failures. These negative consequences may lead to very serious accidents.

Active Bundles provide secure data dissemination in untrusted environments, which is required in V2V networks where topology may change fast. However, the authentication procedure between AB

Table 5: Masquerade attack cost

Code	Transaction	Total cost
T4	Sniffing CAN Traffic	-
T5	Send Malicious Workload in CAN Network	15 ms
T00	Receive message	μ
T1	Message Authentication	1.48 ms
T2	Collision Distance	0.5 ms
T3	Send Notification	2 ms
	Total overhead	18.98 ms + μ

and communicating service takes around 1 second, which makes it inapplicable for critical systems of the vehicle. Thus, ABs can be used in non-time critical communications, e.g. for secure dissemination of video data in V2V systems [28].

4.5 Replay attack

Description

This attack consists of multiple masquerade attacks. The attacker re-injects messages/warnings previously received by the receiver [3, 22].

Features

T4: Sniffing CAN Traffic
T5: Send malicious workload in CAN network
T00: Receive message
T1: Message Authentication
T2: Collision Distance *
T3: Notification

T2 is specific to the pre-collision system. Some vehicular components such as "odometer" or "speedometer" can be manipulated to display falsified speed by replaying the same message [22].

An attacker must understand how targeted ECU (electronic control unit) functions. Miller and Valasek argue that for this attack to succeed, the attacker must send messages more frequently than the responsible ECU [22].

Mitigation

1. Time stamped messages. An accurate source of time is required (i.e. synchronized clock)

2. Use unique sequence numbers. Keep a cache of recently received messages, against which new messages can be compared

Cost of the attack

C1: No alert issued since legitimate messages are silenced
C2: Response delay

C3: Entering dangerous road situation such as collision or causing traffic jam

Cost of mitigation
C4: Computation delay

Impact on Safety
Managing out-of-order packets will require a buffer at both sender and receiver's sides (like in the TCP protocol). If receiver's window is full then new arriving packets containing useful road information will be dropped, thus vehicle may enter jammed roads instead of making a detour and generally become more vulnerable for collisions.

5 V2V Privacy Protection with Active Bundles

We have developed a mechanism for privacy-preserving data dissemination in V2V systems such that:

- Each node is only able to access data items for which it is authorized
- Vehicle manufacturers, law enforcement and drivers are able to define access control policies for vehicles' data items
- Secure data dissemination in trusted and untrusted V2V environments is provided
- Message authenticity and integrity is provided

While developing this scheme, we analyzed existing sets of regulations for data security policies in V2V systems in the US and the EU. The proposed scheme is based on a data self-protection mechanism called "active bundle" [26]. Active bundles encapsulate private data in a package with data protection policies and an engine that is capable of enforcing the policies associated with the data in various domains.

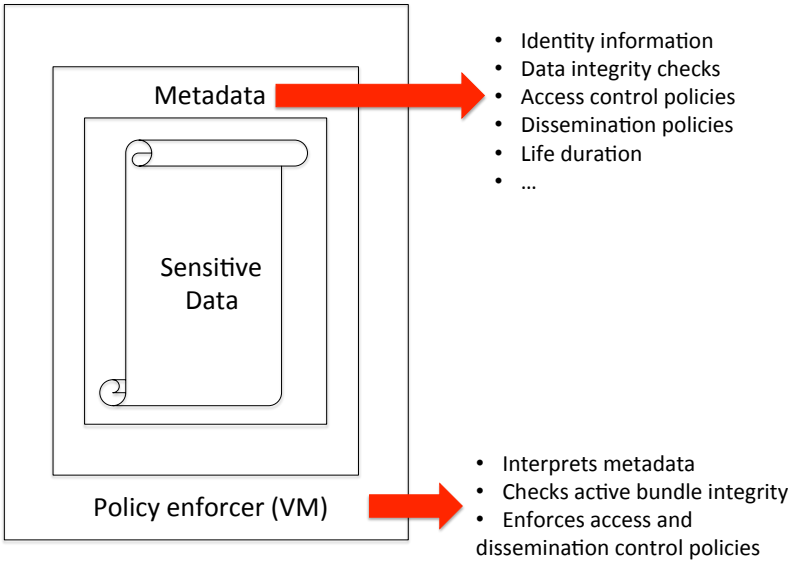

Figure 1: Active bundle structure.

The structure of an active bundle is shown in figure 1. Sensitive data constitutes content to be protected from privacy violations, data leaks and unauthorized dissemination. Metadata describes the active bundle and its privacy policies. The metadata includes (but is not limited to) the following components: (a) provenance metadata; (b) integrity check metadata; (c) access control metadata; (d) dissemination control metadata; (e) life duration value. The policy enforcer (virtual machine) manages and controls the program enclosed in a bundle. The main VM functions include (a) enforcing bundle access control policies through apoptosis (self-destruction) or data filtering (b) enforcing bundle dissemination policies; and (c) validating bundle integrity. Details of active bundle operation can be found in [26].

Active bundles provide self-protection of sensitive data with the help of an active policy and integrity enforcer, as they move through various foreign platforms. This makes them a perfect fit for dissemination of V2V data, which are subject to highly mobile environments with varying context and security requirements. We previously used active bundles as an effective mechanism for privacy-preserving identity management in the cloud [23, 24]. We developed a C++ application running on a Raspberry Pi board to illustrate secure dissemination of video data captured by a vehicle's camera, by applying different face recognition algorithms to the captured images for use in the access policies. We performed experimental evaluation of the proposed mechanism to measure the performance in terms of detection accuracy and response time, the details of which can be found in [28]. The results of the performed experiments provide a basis for the investigation of the tradeoffs between safety/security and performance in V2V systems.

6 Conclusion and Future Work

In this work we proposed a systematic approach for the analysis of attacks on V2V networks. The proposed approach is based on a break-down of attacks into feature sets, and enables simplified association of mitigation costs with various types of attacks for use in security/safety/performance optimization of V2V networks. We provided analyses of major V2V attacks using the proposed model, which will help guide research efforts focusing on the development of quantitative models of the tradeoffs between security and performance in V2V networks.

We presented active bundles as a mechanism for providing secure data dissemination in V2V networks. The active bundle approach enables dynamic adaptability of V2V data sharing to context and need changes. We plan to focus on the exploration of possible dynamic adaptability features in future work. The activities for this task will include consideration of tradeoffs between the complexity/performance overhead of security mechanisms and the level of security required based on operation context (emergency, normal conditions etc.). Our future work will also include development of data filtering mechanisms to provide fine-grain access control to V2V data according to context.

In future work we also plan to focus on more fine-grain performance overhead analysis. Every system of the vehicle such as the engine control, brake control, airbag control, light, air-conditioning etc. requires throughput measurements and estimation of maximum allowed performance overhead imposed by data protection and safety mechanisms. We aim to obtain realistic estimates for the performance overhead imposed by every protection mechanism in vehicle systems. We will identify and quantify costs associated with detection and mitigation of attacks. Tradeoffs between safety and data security will determine the applicability of a specific data protection mechanism for a specific vehicle's system.

Acknowledgments

This publication was made possible by NPRP grant # [7-1113-1-199] from the Qatar National Research Fund (a member of Qatar Foundation). The statements made herein are solely the responsibility of the authors.

References

[1] P. Tyagi and D. Dembla, "A taxonomy of security attacks and issues in vehicular ad-hoc networks (vanets)," *International Journal of Computer Applications*, vol. 91, no. 7, pp. 22–29, April 2014.

[2] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks," in *Proc. of the 3rd ACM Workshop on Security of ad hoc and sensor networks (SASN'05), Alexandria, Virginia, USA*. ACM, November 2005, pp. 11–21.

[3] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks: Status, results and challenges," *Telecommunication Systems*, vol. 50, no. 4, pp. 217–241, August 2012.

[4] "Intelligent Transport Systems (ITS); Security; Threat Vulnerability and Risk Analysis," ETSI TR 102893 V1.1.1, 2010-03.

[5] A. Sharma and Y. Singh, "Data security issues in vanet," *International Journal of Enhanced Research in Management and Computer Applications*, vol. 2, no. 7, pp. 5–7, July 2013.

[6] 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, no. 1, pp. 231–235, January 2013.

[7] X. Ma, X. Yin, and K. S. Trivedi, "On the reliability of safety applications in vanets," *International Journal of Performability Engineering*, vol. 8, no. 2, pp. 115–130, March 2012.

[8] Q. Xu, T. Mak, J. Ko, and R. Sengupta, "Vehicle-to-vehicle safety messaging in dsrc," in *Proc. of the 1st ACM International Workshop on Vehicular Ad hoc Networks (VANET'04), Philadelphia, PA, USA*. ACM, October 2004, pp. 19–28.

[9] "The CAMP vehicle safety communications consortium. Vehicle safety Communication Project Task 3 Final Report: Identify Intelligent Vehicle Safety Application Enabled by DSRC," USDOT, 2005.

[10] A. V. Vinel, Y. Koucheryavy, S. D. Andreev, and D. Staehle, "Estimation of a successful beacon reception probability in vehicular ad-hoc networks," in *Proc. of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly (IWCMC'09), Leipzig, Germany*, June 2009, pp. 416–420.

[11] I. Soomoro, H. Hasbullah, and J. bin Ab Manan, "User requirements model for vehicular ad hoc network applications," in *Proc. of the International Symposium on Information Technology (ITSim), Kuala Lumpur, Malaysia*. IEEE, June 2010, pp. 800–804.

[12] V. H. La and A. Cavalli, "Security attacks and solutions in vehicular ad hoc networks: A survey," *International Journal on AdHoc Networking Systems*, vol. 4, no. 2, pp. 1–20, April 2014.

[13] C. Smith, *Car Hacker's Manual*. Theia Labs, 2014.

[14] "5.9 GHz DSRC," http://grouper.ieee.org/groups/scc32/dsrc/, [Online; Accessed on March 30, 2016].

[15] I. A. Sumra, J.-L. A. Manan, and H. Hasbullah, "Timing attack in vehicular network," in *Proc. of the 15th WSEAS International Conference on Computers, Corfu Island, Greece*, July 2011, pp. 151–155.

[16] E.Hamida and M. Jayed, "Channel-aware ecdsa signature verification of basic safety messages with k-means clustering in vanets," in *Proc. of the 30th IEEE International Conference Advanced Information Networking and Applications (AINA'16), Crans-Montana, Switzerland (to appear)*, March 2016.

[17] M. Jayed and E.Hamida, "Measuring safety awareness in cooperative its applications," in *Proc. of the IEEE Wireless Communications and Networking Conference (WCNC'16), Doha, Qatar (to appear)*, April 2016.

[18] E.Hamida, W. Znaidi, and H. Menouar, "Implementation and evaluation of the etsi security architecture for cooperative intelligent transport systems," in *Proc. of the 81st IEEE Vehicular Technology Conference (VTC'15), Glasgow, UK*. IEEE, May 2015.

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

[20] J. T. Isaac, S. Zeadally, and J. S. Camara, "Security attacks and solutions for vehicular ad hoc networks," *IET Communications*, vol. 4, no. 7, pp. 894–903, April 2010.

[21] X. Liu, Z. Fang, and L. Shi, "Securing vehicular ad hoc networks," in *Proc. of the 2nd IEEE International Conference on Pervasive Computing and Applications (ICPCA'07), Birmingham, UK*. IEEE, July 2007, pp. 424–429.

[22] C. Miller and C. Valasek, "Adventures in automotive networks and control units," http://www.ioactive.com/pdfs/IOActive_Adventures_in_Automotive_Networks_and_Control_Units.pdf, [Online; Accessed on March 30, 2016].

[23] P. Angin, B. Bhargava, R. Ranchal, N. Singh, M. Linderman, L. ben Othmane, and L. Lilien, "An entity-centric approach for privacy and identity management in cloud computing," in *Proc. of the 29th IEEE Symposium on Reliable Distributed Systems (SRDS'10), New Delhi, Punjab, India*. IEEE, October 2010, pp. 177–183.

[24] R. Ranchal, B. Bhargava, L. Othmane, L. Lilien, A. Kim, M. Kang, and M. Linderman, "Protection of identity information in cloud computing without trusted third party," in *Proc. of the 29th IEEE Symposium on Reliable Distributed Systems (SRDS'10), New Delhi, Punjab, India*. IEEE, October 2010, pp. 368–372.

[25] R. Ranchal, "Cross-domain data dissemination and policy enforcement," Ph.D. dissertation, Purdue University, June 2015.

[26] L. B. Othmane and L. Lilien, "Protecting privacy in sensitive data dissemination with active bundles," in *Proc. of the 7th World Congress on Privacy, Security, Trust and the Management of e-Business (CONGRESS'09), Saint John, New Brunswick, USA*. IEEE, August 2009, pp. 202–213.

[27] L. Ben Othmane, "Protecting sensitive data throughout their lifecycle," Ph.D. dissertation, Western Michigan University, December 2010.

[28] C. Qu, D. Ulybyshev, B. Bhargava, R. Ranchal, and L. Lilien, "Secure dissemination of video data in vehicle-to-vehicle systems," in *Proc. of the 6th International Workshop on Dependable Network Computing and Mobile Systems (DNCMS'15), Montreal, Quebec, Canada*, September 2015, pp. 47–51.

Author Biography

Bharat Bhargava is a professor of the Department of Computer Science with a courtesy appointment in the School of Electrical and Computer Engineering at Purdue University. His research focuses on security and privacy issues in distributed systems. He is a Fellow of the Institute of Electrical and Electronics Engineers and of the Institute of Electronics and Telecommunication Engineers. In 1999, he received the IEEE Technical Achievement Award for his decade long contributions to foundations of adaptability in communication and distributed systems. He serves on seven editorial boards of international journals. He also serves the IEEE Computer Society on Technical Achievement Award and Fellow committees.

Amber Johnson is a graduate of The Lemoyne-Owen College, where she received a bachelor's degree in Computer Science and Jackson State University, where she obtained a masters degree in Computer Science. She is currently a Computer Science doctoral student at Purdue University, and her research interests are security in cloud computing and V2V systems.

Gisele Izera Munyengabe is a PhD student in Computer Science at Purdue University, with particular interest in vehicular security, safety and privacy. She holds a bachelor's degree in Computer Science from Spelman College.

Pelin Angin is a postdoctoral researcher at the Department of Computer Science at Purdue University. She received her BS degree in Computer Engineering at Bilkent University in 2007 and her PhD degree in Computer Science at Purdue University in 2013. Her research interests lie in the fields of mobile-cloud computing, cloud computing security, distributed systems and data mining. Her current work focuses on dynamic computation partitioning between mobile and cloud platforms for performance optimization of real-time computationally intensive applications and the associated security issues.