Security issues in Message Dissemination for Vehicular Ad-Hoc Networks

Miguel Morales Sandoval

Laboratorio de Tecnologías de Información
Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional
Tamaulipas, Mexico.

mmorales@tamps.cinvestav.mx

March 11, 2015

Abstract
Vehicular Ad hoc Networks (VANETs) are special cases of Mobile Adhoc Networks (MANETs). They are considered an important infrastructure for the deployment of Intelligent Transportation Systems (ITS). However, a requirement for practical use and deployment of VANETs is to address appropriately the information security aspects that rise from the existing mechanisms for message dissemination in VANETs, which constitute a fundamental part in safety applications.

Contents

1 Message dissemination in VANETs 1
2 Security issues in Broadcast Message Dissemination for VANETs 3
3 Security approaches in VANETs 4
   3.1 Entity centric approaches 5
      3.1.1 Key management and network authentication 6
      3.1.2 Relevant Entity Centric proposals 6
   3.2 Data centric approaches 7
      3.2.1 Relevant Data Centric proposals 8
4 Discussion 9

1 Message dissemination in VANETs

Broadcasting refers to the operation of disseminating a piece of information from one node to others in an ad hoc network, even if those destination nodes are unknown and unspecified. In VANETs, Broadcasting is a technique especially to aid safety applications as:
1. Cooperative collision warning
2. Intersection collision warning
3. Cooperative driver assistance system
4. Approaching emergency to vehicles

Intelligent transport systems (ITSs) are aimed to improve the safety measures and provide intelligent information to drivers, pedestrians, and passengers. For instance, exchanging messages about the geographic location of a recently occurred crash could help drivers in choosing alternative routes to avoid the crash site. To achieve this, timely and accurate message dissemination by means of wireless links is needed. Different approaches to enable information exchanging between vehicles have been proposed, ranging from the use of infrastructure-based networks (e.g., the cellular network) to the deployment of vehicular ad-hoc networks (VANETs). The research, development, and standardization communities have identified the latter approach as a key component of ITSs.

From these applications, message dissemination in VANETs could be of two kinds. 

i) Short distance dissemination - A vehicle warns nearby vehicles about its movements (braking, lane change, etc.). These alert messages only require a limited dissemination (less than a hundred meters) but have very strong real-time requirements (they must be processed very quickly).

ii) Long distance dissemination - A car sends announcements about road conditions (traffic jams, accidents) to other vehicles. Such announcement messages require a longer dissemination range. However, their requirement of real-time processing is much less strict than in the case of alerts.

A key communication pattern in VANETs is beaconing, the process of periodically and locally broadcasting nodes status information. Vehicles use this process to obtain information related to other vehicles. Beacon messages contain a vehicle’s identifier, its geographical position and possibly its velocity. The process of beaconing therefore provides a vehicle’s awareness of its surrounding. Considering that driving decisions might be made based on information from beacon messages, beaconing may be considered as mission critical. Beacons are considered passive messages, send periodically. Contrary, active messages take place when an event occurs and other vehicles must be notified.

Beacon messages must be received up to a certain distance with a specific freshness in order to be useful to VANET applications. The precise distance or freshness is determined by a VANET application and based on the objectives and demands of such applications.

The communication layer may opt for two options to broadcast these beacons. One is to use a high transmit power to reach the required dissemination distance in one hop. The other one is to use a small transmit power and cover the same distance by means of multi-hop relaying. Due to multi-hop nature of VANETs, flooding is a fundamental mechanism to implement the multi-hop broadcasting in a dense network. This introduces significant communication overhead (redundant re-broadcasting), leading to the well-known broadcast storm problem.
2 Security issues in Broadcast Message Dissemination for VANETs

In VANETs, routing and dissemination security issues could be divided into general attacks and position-related attacks. General attacks comprise:

i) Denial of service (DoS) attacks, aiming to bring down the VANET through methods such as channel jamming and aggressive injection of dummy messages. Jamming is a low-effort exploit opportunity. The attacker can easily, without compromising cryptographic mechanisms and with limited transmission power, partition the vehicular network.

ii) Black hole attacks (selective forwarding), carried through a node that has the ability to lure all data around an area through itself, then simply discards all data or only forwards portion of received data.

iii) Bogus information attack, where attackers diffuse false information to misguide other vehicles.

Position-related attacks comprise:

i) Location falsification, that is, a node claims a fake position to pretend to be optimal, then aggregates all data as a black hole. A such node can create clones that claim fake positions to gain high probability to be selected as forwarding node.

ii) The Sybil attack, where a node creates a large number of pseudonymous identities, using them to gain a disproportionately large influence.

Attacks by a malicious node include:

1. Replay - Record messages and later injects.
2. Change - Modify the message before forwarding.
3. Delete - Destroy the message as received.
4. Manufacture - Create fake message and injects in the network.

Specially interest is the spoofing attack where malicious nodes impersonate legitimate nodes, and transmit false information to contaminate the communication network. Thus, a vehicle could mislead other vehicles or impersonates RSU to spoof false service advertisements or safety hazard warnings.

Besides the threats and attacks previously commented, another requirement in VANETs is privacy. User information such as drivers name, license plate, model, and traveling route must also be protected. An attacker either passively or actively, and internally or externally could try to extract data such as time, location, vehicle identifier, technical descriptions, or trip details. To guarantee the privacy of mobile nodes, they must be both anonymous and untraceable.

Securing forwarding and dissemination is a critical issue in VANETs. An attacker can be seen as an entity who wants to spread false information in the network, interrupt communications, impersonate legitimate nodes and/or compromise their privacy, or take advantage of the network without cooperating in its normal operation. Attackers in VANETs applications are typically classified as described in table[1].

Attacks by a malicious node include:

1. Replay - Record messages and later injects.
2. Change - Modify the message before forwarding.
<table>
<thead>
<tr>
<th>Kind</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>outsider</td>
<td>The attacker node does not belong to the network and hence does not have any cryptographic material.</td>
</tr>
<tr>
<td>insider</td>
<td>Damage could be more severe, these nodes have cryptographic material and peers consider them as trusted.</td>
</tr>
<tr>
<td>passive</td>
<td>Illegitimate eavesdroppers, selfish nodes that do not cooperate with the purpose of energy saving and can severely degrade network by simply not participating in the network operations (drop useful packets). These nodes do not try to actively interfere with communications.</td>
</tr>
<tr>
<td>active</td>
<td>Misbehaving nodes spend some energy to perform a harmful action. They attempt to introduce invalid data into the network or to produce communication failures. Active malicious nodes can directly cause network traffic to be dropped, redirected to a different destination or to take a longer route to the destination by increasing communication delays.</td>
</tr>
</tbody>
</table>

Table 1: Attacker taxonomy in VANETs

3. Delete - Destroy the message as received.

4. Manufacture - Create fake message and injects in the network.

3 Security approaches in VANETs

There are still several technical challenges to resolve before VANETs can be deployed. The most critical pointed out in the literature are those related to security and privacy. Securing forwarding and dissemination is a critical issue in VANETs. Privacy of nodes is another security requirement, for example, data such as drivers name, license plate, speed, position, traveling routes and their relationships must be properly used and kept private to each node. An attacker in VANETs can be seen as an entity spreading false information in the network, interrupting communications, impersonating legitimate nodes and/or compromising their privacy, or taking advantage of the network without cooperating in its normal operation [18, 10, 4, 14]. In the literature, existing security and privacy mechanisms for VANETs are designed to ensure the following requirements:

- authentication - nodes’ identity is ensured and verified.
- integrity - information from sender to the receiver must not be altered or dropped.
- availability - the wireless channel must be available to communicate the messages in the underlying application.
- non-repudiation - sender should not be able to deny the transmission/reception of a message.
- privacy - node’s data is under its control and nor by other nodes in the VANET

For ensuring security and privacy in VANETs, existing mechanisms can be divided in two approaches. Those based on encryption techniques (entity-centric) focused on ensuring authentication, integrity, privacy, and non-repudiation of messages send and received by the nodes in a VANET, and those that do not rely on cryptographic techniques (data-centric), focused to build trust models to ensure integrity and reliability.

3.1 Entity centric approaches

Main effort on security aspects for VANETs are being carried out by organizations as Car2Car Communication Consortium, the EEE 1609.2 working group, the NoW and the SeVeCom project [18]. All of them agree that Public Key Cryptography (PKC) and a Certification Authority (CA) are the way to go about for VANETs security and a more suitable option for deploying vehicular communications security.

PKC and the CA conform what is known as a Public Key Infrastructure (PKI), used to introduce trust within the network. The presence of infrastructure in the network is vital for a security solution for VANETs under the entity-centric approach [17, 9, 19].

In PKC, each node $n$ in the network has two key, one being private used by $n$ to sign its outgoing messages and a public one, used by any other node in the network to ensure integrity, authentication and non-repudiation of messages coming from $n$. Public keys are certified by the CA and provided to any node in the network by means of a digital certificate prior registration. So, in order to communicate, a node in a VANET must be registered to the CA. The CA is responsible for checking if the right vehicle get the right key and if the vehicle is worthy of trusting before issuing the signed certificate.

Every subscriber vehicle within the VANET knows the public key of the CA and can check the validity of any other node’s public key issued by the CA. Any two vehicles in a VANET can exchange and validate their public keys without having access to any other node or gateway. If the certificates are valid, the vehicles can trust each other and establish a secure connection.

3.1.1 Key management and network authentication

To ensure the security of keys, nodes in a VANET use a tamper proof device (TPD), a critical device that internally stores the private keys and performs cryptographic operations such as hashing, signature generation/verification, random number generation, among others. To be part of a VANET, each vehicle has to store in the TPD its unique electronic identity (UEI), that can be either the electronic license plate (ELP) issued by government or its electronic chassis number (ECN) issued by the manufacturer. The governmental transportation authority will pre-load the ELP at the time of vehicle registration (in the case of the ECN, the manufacturer is responsible for its installation at production time). Together with UEI, the TDP must contain the vehicle’s certificate issued by the CA and attached to its identity. The CA gives each vehicle anonymous key pairs to preserve its privacy. These
anonymous keys are periodically renewed after all the keys have been used or their lifetimes have expired [18].

The entity-centric approach requires a certificate revocation (CR) mechanism to have up-to-date vehicles’ certificates [15]. A misbehaving node in the network could be sanctioned by revoking its certificate so that node should not take part in future communications. For this, road side units - RSUs - communicating with the CA are needed. The CA will inform all the RSUs about any certificate revocation. An RSU will broadcast warning messages such that all other approaching vehicles can update their control revocation lists (CRLs) and avoid communicating with compromised vehicles.

3.1.2 Relevant Entity Centric proposals

The entity-centric security approach is a fundamental part in the design of global security architectures for VANETs [12, 10, 4]. One of the main objectives in entity-centric security mechanism is to provide correct authentication of data packets’ origin and their integrity.

Security strategies based on the entity-centric approach have proven to thwart external attacks to VANETs as the injection of fake messages or the collection and replay of previous messages [19]. In the case of internal attacks, digital signatures ensure authentication and integrity for one-hop dissemination. Before a vehicle sends a safety message, it signs it with its private key and includes its certificate. A typical packet send by vehicle \( v \) in a one-hop dissemination using signatures for authentication is as follows:

\[
\text{PACKET} = \{ M, \sigma_{SK_v}[M|T], \text{Cert}_v \}
\]

In the above expression, \( \sigma_{SK_v}[M|T] \) represents the digital signature of \( v \) over the concatenation of message \( M \) and a timestamp \( T \). With \( T \), freshness check is possible to prevent replay of old messages. The signature is generated with the \( v \)'s private key \( SK_v \). Together with this signature, the packet includes the message \( M \) and the \( v \)'s digital certificate \( \text{Cert}_v \). Any node receiving this packet could verify the authenticity of the message by verifying the signature \( \sigma \) with the \( v \)'s public key contained in \( \text{Cert}_v \). However, attaching a digital signature and a certificate to each VANET message inevitably introduces computation and communication overhead.

In case of multihop broadcast forwarding, entity centric approaches usually restrict re-broadcast by either a timer live (TTL) counter value or a geographic destination area (GDA). In this case, an entity-centric security approach is not intended to only ensure integrity and authenticity, but also reliability among nodes involved in the multi-hop path [15]. For the multi-hop broadcast, the security processing varies depending on if a message is incoming or outgoing, if the message is created by the current node or forwarded only, and if the communication mechanism is TTLbased or GDA based.

For secure multi-hop broadcast, each new packet transmitted consist of two types of fields: mutable and immutable. The immutable fields contain the message itself, a timestamp to ensure message freshness, and a value to ensure message integrity. The mutable fields contain data that are accessed and changed by each node rebroadcasting the packet. Consider the case when a message \( M \) is created in a node \( v \). If the forwarding is TTL-based, the immutable fields are \( M \), the timestamp \( T \), and a hash chain value. The hash value prevents that malicious nodes manipulate the TTL and thus increase the multi-hop
propagation area (and hence forcing a wasting of network bandwidth). At vehicle $v$, a random value $r_v$ is generated and its hash $H_v$ is computed $TTL_{MAX}$ times. $r_v$ and the TTL conforms the mutable fields. The complete packet is formed as:

$$IMUT = \{M, H_v, T\}$$

$$MUT = \{r_v, TTL\}$$

$$ PACKET = \{IMUT, MUT, \sigma_{SK_v}[IMUT], Cert_v\}$$

When the packet arrives at a node $w$ it is inspected for checking security policies. What is verified is the certificate, signature, timestamp, and the hash chain. If any of these checks fail, the message is dropped (not forwarded). If all checks passed, the packet is forwarded and the mutable fields updated: the TTL is decreased and $r_v$ is replaced by $H_v$, i.e. the hash chain has to be shortened by one element because the routing has decreased the TTL value. The signature and the immutable fields are not modified by forwarding nodes.

Signatures and certificates are the basic building blocks to construct secure schemes that thwart severe attacks in VANETs as the Sybil attack \[5\], where a node creates a large number of pseudonymous identities and use them to gain a disproportionately large influence in the network. However, there is an unavoidable computation overhead introduced by signature generation/verification that affect the performance of multi-hop dissemination methods. In \[9\], authors use Prediction-based TELSA as an alternative to signatures to authenticate V2V communications. TELSA is cheaper because it is based on symmetric cryptography. Instant and light-weight authentication for broadcast is achieved by employing the predictability of future beacons. However, since TESLA cannot provide the property of non-repudiation, digital signatures with asymmetric encryption are still required.

In \[19\], authors propose alternatively to use a privacy preserving broadcast message authentication (PPBMA) scheme based on Message Authentication Code (MAC) through symmetric encryption. The PPBMA scheme was simulated and evaluated in terms of packet loss rate and message delivery latency.

Authors in \[16\] also address the excessive signature verification requests during message broadcasting in VANETs. For that, two broadcast authentication schemes are proposed: Fast Authentication (FastAuth) and Selective Authentication (Sel-Auth). FastAuth secures periodic single-hop beacon messages. SelAuth secures multi-hop applications in which a bogus signature may spread out quickly and impact a significant number of vehicles. SelAuth provides fast isolation of malicious senders, even under a dynamic topology at low computational costs.

### 3.2 Data centric approaches

In the entity-centric approach, the assumption is that an infrastructure is available and all nodes registered with the CA are trust. However, message authentication can only ensure that messages are sent from legitimate senders but it cannot prevent a legitimate sender from broadcasting bogus or altered messages to neighbor vehicles \[10\]. These bogus or altered messages can both decrease the network efficiency and cause accidental events. That is because the establishment of trust relationships is needed for distinguishing trustwor-
thy vehicles or messages from untrustworthy ones as well as for detecting the presence of faulty/misbehaving nodes [14, 7].

3.2.1 Relevant Data Centric proposals

In [20], authors propose a mechanism to detect a rogue node that is sending false emergency messages in VANETs by cooperative exchange of data without the need of any infrastructure or revocation list. However, as security assumptions, all vehicles must authenticate themselves with a certificate authority and obtain a valid certificate and public/private key pairs. A valid identity of vehicles is important for distinguishing them from each other but it is not used as the basis of the acceptance of data as trusted in the underlying dissemination protocol.

The need for reliable information from nodes in a VANET has been highlighted in the past. In [8], authors propose to regard information as reliable if it is confirmed by a number of various sources, greater than a given threshold and during a certain time interval. Privacy of nodes is kept by letting vehicles change their identity frequently. For their approach to operate, vehicles are equipped with black boxes that are configured during the manufacturing process to permit the generation of anonymous public/private key pairs and are able to issue certificates for those key pairs.

In [13], authors propose algorithms which detect false alert messages, so misbehaving nodes can be identified observing their actions after sending out the false alert messages. Thus, each vehicle can decide whether an information received is correct or false, based on the consistency of recent messages and new alerts with reported and estimated vehicle positions. The proposal assumes the existence of a CA, that imposes fines on misbehaving nodes (they are not revoked, so involved costs are avoided).

In [1], authors propose a vehicular security scheme through a trust-based algorithm based on reputation and plausibility checks, thus providing security against the attacks of event modification, false event generation, data aggregation and data dropping. Their scheme performs not only detection but also the isolation of malicious nodes in the network. Infrastructure is not assumed, their approach utilizes vehicle to vehicle communication only. Their proposed security mechanism should be affected by the dissemination protocol, as an event is determined to be genuine based on a threshold value. However an analysis to quantify the required redundancy was not addressed.

The most adopted mechanisms for misbehavior detection is position verification [16]. In [5], assuming that sensors in a node can be manipulated, authors evaluate the impact of faking position and speed in multi-hop vehicular beacon broadcast. Authors use a set of heuristics to detect fake positions and define a framework to integrate arbitrary trust sensors using Bayesian reasoning. In that work, message trustworthiness is modeled as a conditional probability.

An approach for consistency checks is to exploit redundant information dissemination [2, 3]. Under this approach, attacks could be detected if data is received and compared from both honest and malicious vehicles. In [2] it is presented an approach to detection of insider attacks in VANET using a redundancy-based statistical analysis. They propose a bandwidth-efficient protection mechanism for in-network aggregation based on data-consistency checking. Data mining techniques are combined to detect false informa-
tion with a filtering technique for forwarding paths. Their approach also assumes that infrastructure is in place, providing anonymous keys and allowing the signing of messages through certificates attached to them. However, signatures here are used to secure the communication path, rather than the message contents.

4 Discussion

Entity-centric approaches are mainly intended to provide a secure and reliable network and try to avoid outsider attackers that disrupt its correct operation. However, these solutions fail to achieve an integral solution as some security issues related to practical realization of VANETs and threats remain as open problems:

- The entity centric approach bases on the assumption that infrastructure is available to the VANETs. This assumption is far to be real in practical deployment of VANETs due to the cost implied to install RSU [1]. The most prominent and practical realization of VANETs in the short time is based on inter-vehicle (V2V) communication, where infrastructure is not available and where the use of a PKI would not be possible.

- An insider attacker is difficult to detect and deter only with entity-centric approaches. Those nodes are authentic but the information they distribute could not be reliable (messages could be modified or destroyed). Under that scenario, integrity and authenticity do not guarantee the correctness of transmitted data. The need for data verification could not be only due to possible insider attackers but also by malfunctioning hardware (faulty/misbehaving nodes) [13, 7].

- Since security solutions based on the entity centric approach rely on public key encryption operations, the event data recorder and the tamper proof device rely on proper functioning of node’s sensor. However, sensor malfunctioning is possible, and correction at run time are not possible with entity-centric mechanisms only.

- For multi-hop dissemination, the entity-centric approach is not viable since destination of messages is unknown, so it is hard to exchange certificates and/or private key and use encryption. Also, depending on the dissemination protocol, information received by a node in the network could be changed and modified. This is the case in the aggregation dissemination pattern, where vehicles combine known information and only disseminate summaries of them in larger regions [1].

To cope with the above problems, security schemes move from an entity-centric approach, where the major security requirement is authentication and integrity, to a data-centric approach, where trustworthy on data being distributed among nodes is a major concern. However, even in a data-centric approach, authentication, integrity and non-repudiation must still be guaranteed. For example, if in a data-centric security scheme the reputation of nodes is being built from collected data, keeping authentication in the broadcast method for detecting malicious messages is very important as it is possible to detect insider attackers and avoid them in future communications (i.e. by revocation of their certificates). Without non-repudiation, nodes cannot deny they send bogus information. Thus, data-centric approaches complement entity-centric solutions.
References


