Chapter 1

Reliable Traffic Information Propagation in Vehicular Ad hoc Networks

Soyoung Park, Cliff Zou, and Damla Turgut
School of Electrical Engineering and Computer Science,
University of Central Florida, Orlando, Florida 32816

A vehicular ad hoc network (VANET) allows vehicles share traffic information and alerting each other any emergency events. To achieve this goal, a security mechanism must be designed to guarantee that no malicious vehicles can intercept, manipulate, or modify the traffic information without being detected. In this chapter, we present two novel approaches to provide reliable traffic information propagation in a VANET: *two-directional data verification*, and *time-based data verification*.

The two-directional data verification approach uses vehicles in both driving directions of a two-way road as two separated media channels. A traffic message will be transmitted through both channels. A recipient vehicle verifies the message integrity by checking if data received from both channels are matched. This approach exploits the fact that it is difficult and costly to have two collaborative vehicles on both driving directions in the same region. The time-based data verification approach only uses vehicles in the opposite driving direction to propagate a traffic message by first issuing its public key commitment and later sending the actual traffic message. It relies on the time delay between these two messages and the mobility of vehicles to protect data integrity.

1.1. Introduction

With the significant development of network technologies, vehicular ad hoc network (VANET) has been emerging as a feasible and important application in a ubiquitous environment. In a VANET environment, each vehicle senses and creates its own traffic information and then shares with other vehicles to know the real-time traffic condition in both the local area and its interested areas. Some existing traffic broadcasting systems, such as traffic radio and road-side electronic bulletin boards, can provide traffic information periodically for some specific locations and directions. Compared to

these systems, a VANET system could provide much detailed, real-time, and individualized traffic service and also unlimited data services to vehicles.

To achieve a sustainable collaboration and data sharing among vehicles in a VANET, security mechanisms for trustable traffic message communication should be designed in the first place. The existing security research work in VANET may include self-organizing traffic information system (SOTIS),[1] security and privacy issues,[2–7] fast authentication,[8,9] secure data aggregation,[10,11] and detecting and correcting malicious data,[11,12] and so on. Among these security challenges, we focus on the reliable traffic information propagation through multiple vehicles over a relatively long distance. For example, aggregated traffic messages obtained in a road section, such as the average speed and density of vehicles, traffic hazard, accident and congestion events, can affect any future vehicles that will arrive at this road section in the next tens of minutes or even several hours. Therefore, these messages should be delivered to vehicles in a relatively long distance away from the road section. We name such an aggregated traffic message as "regional message" in this chapter.

We focus on the security of the long-existing regional traffic messages. Because these messages should spread over many vehicles through a public wireless network channel, the probability that they can be modified or forged by attackers and malicious drivers will greatly increase. If the original messages have been altered along the propagation, following vehicles should be able to detect the modification and they should not accept these altered messages.

We define that a given regional message is correct if the message is identical to the original regional message; the propagation is reliable and secure if any recipient vehicles can receive and detect the correct regional messages. This chapter provides two novel approaches for vehicle-assisted reliable traffic data propagation without any additional roadside infrastructure and special technologies. We show how we can use existing vehicles on two-way traffic roads to verify the correctness of any delivered regional messages under the existence of malicious drivers. Since two-way roads are the dominant vehicular environment, our approaches are applicable for most VANET scenarios.

1.1.1. *Contribution*

We provide two approaches for reliable regional traffic data propagation: two-directional data verification and time-based data verification.

Two-directional data verification: In this approach, vehicles in each direction of a two-way road form a separated media channel to forward regional messages along the road. Thus a generated regional message will have two separated and independent media channels to propagate. If a recipient vehicle on the propagation path wants to accept the regional message instead of simply forwarding it, the vehicle will need to receive the identical message from both directional channels to ensure that the message has not been altered by any vehicle along the data propagation path.

In order for an attacker to alter a propagating regional message without being detected, the attacker needs to: (i) have two cooperative vehicles on both driving directions and (ii) both malicious vehicles must be placed between the source of the regional message and the recipient vehicle. Such an attack is very hard to deploy on a two-way traffic road, because two collaborative malicious vehicles only meet once and they pass away toward each other's opposite direction very quickly. If attackers have such two cooperative vehicles, they can only attack our proposed system within a short time period when these two vehicles meet or are in a closed range.

Time-based data verification: The two-directional data verification approach works well when there are sufficient number of vehicles on both driving directions, which makes it suitable for VANETs in urban areas. However, in rural areas or during the late night, it is highly possible that vehicles are sparsely distributed. For these scenarios, we provide an alternative "time-based data verification" approach for reliable traffic data propagation.

In this approach, a regional message is transmitted in the form of two messages: a public key commitment message and a data message that contains the actual regional message. Both messages are transmitted only via vehicles driving on the opposite direction and with a predefined time delay between their transmissions—vehicles on the opposite direction carry these messages as they move and inform any vehicles they meet on the original driving direction.

In order to accept the regional message, a recipient vehicle should receive a valid pair of both the public key commitment message and the second

data message. Because of the time delay between a pair of message, a single malicious vehicle cannot obtain and modify both messages at the same time. In order for attackers to make a reasonable attack in this approach, attackers need to have two cooperative vehicles driving at the opposite direction, neither very close nor far away from each other, and collaborate to generate a valid pair of a fake message. Such an attack is both difficult and costly to implement.

For a practical use, we can easily combine the above two approaches together. We will describe the combined protocol in detail in Section 1.4.2.4 which takes the advantages of both approaches.

The biggest advantage of our schemes is that they are simple to setup for reliable data transmission without any additional roadside infrastructure or dedicated public key infrastructure for VANET. We do not need to use certificates and its related operations either. Our approaches exploit the unique features of bidirectional roadway and fast moving vehicles to protect traffic information propagation in a VANET.

We illustrate our VANET model and security issues in Section 1.3. We give detailed descriptions for our approaches in Section 1.4.1 and Section 1.4.2. We then analyze the security in Section 1.5 and show the simulation results in Section 1.6. We conclude our chapter in Section 1.7.

1.2. Related Work

Many existing work about secure vehicular communication[2–6] rely on established vehicular public key infrastructure for providing authentication, authorization, and accounting (AAA) framework. However, it may not be realistic to assume that we have a well established public key infrastructure in vehicular wireless networks, especially for the important initial stage of VANET deployment. The vast number of vehicles are manufactured by different companies which may follow different standards and registered in different regions where there could be vastly different legal policies and roadside infrastructure, designing a robust and scalable key management scheme for the (nation-wide or continent-wide) vehicular public key infrastructure is the biggest challenge. In addition, it needs to establish additional roadside infrastructure such as roadside access points, and to operate certificate authorities (CA) for issuing certificates about vehicular private/public key pairs.

Rahman and Hengartner[13] introduced the concept of cryptographically-verifiable road-worthiness certificates for secure crash reporting. However,

it needs the operation of additional governmental authorities and roadside access points to manage certificates required in the proposed approach. Zhao and Cao[14] presented vehicle-assisted data delivery protocols based on carry and forward solutions without discussing security issues. Our second approach, time-based data verification, uses the similar carry and forward concept. However, we exploit its unique security feature to develop a simple way to provide secure data propagation in a sparsely-distributed VANET.

Related to regional information delivery, Sun and Garcia-Molina[15] proposed bidirectional perimeter-based propagation of regional alerts for fast data delivery. This is similar to our concept in that it deals about the long-distance propagation of regional alerts, and that both vehicles on bidirectional traffic roads forward those messages for fast delivery. However, they[15] did not consider the security issue in data propagation. In the same paper,[15] they also presented an efficient message delivery protocol that minimizes the number of broadcasts needed for maintaining a regional alert over a period of time, which did not consider security issue.

1.3. VANET Model

In this section, we provide a clear definition of the network model and adversary model considered in our study.

1.3.1. *Network model*

The network basically consists of roads, cars and traffic messages.

(1) **Road:** We consider two-way traffic roads since they are the dominating form of automobile roads. Each road is logically divided into road sections and each road section has its unique ID number.
(2) **Car:** Each car is equipped with sensors, global position system (GPS), a preloaded digital map which has the road section information, networking and computing devices which store private/public key pairs (but without certificates) and creates messages and digital signatures. It also has its local traffic analyzer to store the regional messages and to analyze the correctness and consistency of the given regional messages.
(3) **Traffic messages:** Traffic messages we consider in this chapter are classified into typical messages and regional messages.
    - A typical message contains a vehicle's current speed, moving direction, any events detected and its public key. Every single vehicle

creates and broadcasts its typical messages with a periodicity of 100 to 300 ms.[2,11] These messages are broadcasted in a single data transmission range without propagating any further.
- A regional message contains its corresponding road section, direction, average speed, density and particular (long-term) events detected in its road section. Regional messages are propagated through multi-hop broadcasting. The propagation range can be flexible according to applications.

1.3.2. *Adversary model*

The majority of vehicles are honest. However, a few malicious vehicles can cause damage to the entire VANET. In this chapter, we focus on malicious attackers who may conduct the following attacks.

- Denial of service attacks: Adversaries can drop packets from the network.
- Fabrication and alteration attacks: Malicious vehicles can fabricate a driver's own information, including his identity, location, or other application specific parameters and then broadcast the false information into the network. Also, adversaries can alter existing data or replay earlier transmissions within a transmission.
- Bogus message insertion attacks: Adversaries can diffuse wrong information.

In this chapter, we focus on the security of the regional message's propagation. We do not study the possible maliciousness of a source vehicle that creates a false regional message. We assume that the source regional message is trustable. This can be enforced via some other security mechanisms and it is out of the scope of this work. For example, we can rely on neighborhood cooperative detection[16] to detect malicious source vehicles. Since the majority of vehicles are honest, new-coming honest sources can create correct regional-messages for the same road section as another example. In this case, most of recipient vehicles can accept the correct regional messages through the consistency verification about those regional messages.

1.4. Proposed Approaches

We provide two approaches for reliable regional traffic data propagation: two-directional data verification and time-based data verification. The basic idea is to make two different groups of vehicles (or two different vehicles that are out of each other's transmission range) deliver a regional traffic message. If the two messages given from both groups (or both vehicles) are either identical or correctly associated with each other, a recipient vehicle accepts that the received regional message is correct.

We describe our approach in detail in this section. Before we describe the way of propagating and verifying of the regional messages, we first give a short description about road sections and vehicular groups.

In a VANET every vehicle's trajectory follows existing roadways. Thus it is easy to set a group of vehicles by the geographical road information. Any roadway can be logically divided into small sections. We denote the boundary line between two road sections as *road section boundary line*, and also denote a short area around the boundary line as *boundary area*, as illustrated in Fig. 1.1. Every vehicle can easily recognize what road section it is passing through since it has GPS and a digital map with the road section information.

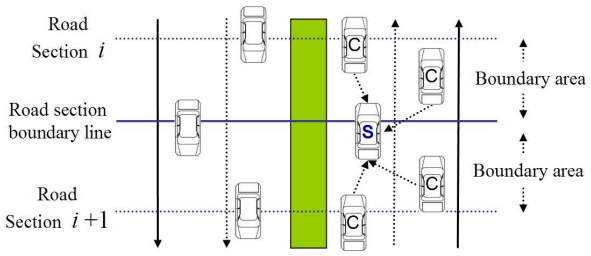

Fig. 1.1. Illustration of road section and source vehicle election

Vehicles are logically formed into groups based on road sections that they currently reside. Unlike the traditional group selection that is based on distance radius regardless of driving direction, in our approaches, only vehicles in the same driving direction in each road section are set as a group. This group definition has been previously used by Raya et al.[11] Such a group definition makes a vehicular group have the same driving direction, with the similar interests in traffic events, and most importantly, relatively stable group members and low relative mobility among group

members.

A group of vehicles in a single road section collaborate with each other to create a regional message about the road section by broadcasting their periodic typical traffic messages to each other. The created regional message is mainly propagated to vehicles that will soon move to this road section in the same driving direction because in most cases only these vehicles need this traffic message. If a vehicle leaves a road section and moves into a new road section, it becomes a group member of that new road section automatically.

1.4.1. *Two-directional data verification*

1.4.1.1. *Driving direction*

In this approach, vehicles on a two-way road are treated as two separated network channels according to their driving directions. If a vehicle receives a forwarded message, the receiver vehicle will forward only messages received from vehicles in the same driving direction. Therefore, it is important for a receiver vehicle to determine the moving direction of any vehicles. We present such an approach in the following called *neighbor-based data forwarding* method.

In our approach, neighbor vehicles are defined as follows:

- NV (Neighbor Vehicle): For a specific vehicle V, neighbor vehicle is the set of vehicles moving toward the same direction of V and in a single data transmission range of V.

Since we assume that every vehicle periodically broadcasts its typical message which includes its moving direction, speed, and public key, etc., a vehicle V can easily recognize its neighboring vehicles NV and construct its neighbor list. If vehicle V receives typical messages with the same public key repeatedly, it adds the public key to its neighboring list and keeps the key until it no longer receives messages with the same public key. The minimum number of messages with the same public key required for adding a neighboring vehicle is determined by vehicles moving speed, data transmission range and typical traffic message broadcasting period—it makes sure that no vehicles on the opposite driving direction can stay in the transmission range of V for transmitting this number of messages to V. Studer et al.[17] give several other ways to find out each vehicle's neighbor group, and thus we do not discuss this issue here any further.

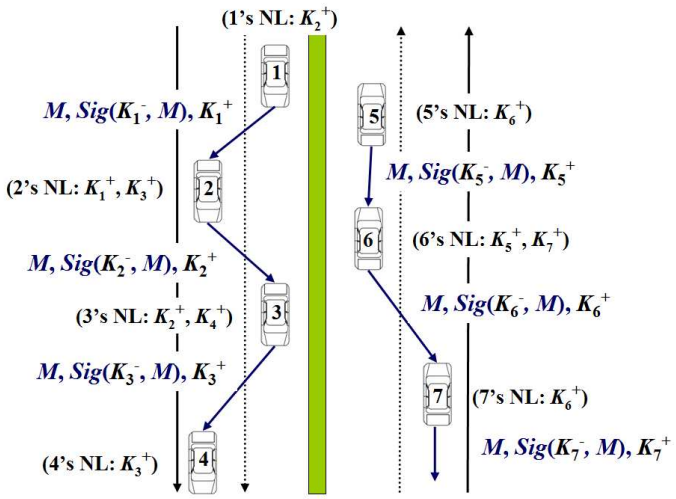

Fig. 1.2. Illustration of neighbor-based forwarding on each driving direction ("(3's NL: K_2^+, K_4^+)" means vehicle 3 has a neighboring list (NL) containing the public keys of vehicle 2 and vehicle 4)

Fig. 1.2 illustrates how the neighbor-based forwarding method works. At every regional message forwarding step, a sender i generates a digital signature $Sig(K_i^-, M)$ about the message M with its own private key K_i^- and forwards it together with its public key K_i^+. Consequently, any receiver vehicle will forward the given message only if the public key contained in the given message is in its current neighboring list (NL). For example, when vehicle 2 receives a set of messages $\langle M, Sig(K_1^-, M), K_1^+ \rangle$, it can verify that it is forwarded from its neighboring vehicle 1, since vehicle 2's current neighboring list contains K_1^+. Then, vehicle 2 creates a new message $\langle M, Sig(K_2^-, M), K_2^+ \rangle$ for the regional message M with its own private/public key pair $\langle K_2^-, K_2^+ \rangle$ and forwards it to vehicle 3. Other vehicles can verify and forward the given message similarly. In this way, the source's regional message can be delivered along both road directions independently.

We list the major notations used in this chapter in Table 1.1

1.4.1.2. *Data aggregation*

In order to aggregate the typical messages for each road section into a regional message, we need to elect a source vehicle as a group leader of the

Table 1.1. Major notations used in this chapter

Notation	Meaning
NV	Neighboring vehicles
K_i^+, K_i^-	Public key and private key for vehicle i
$Sig(K_i^-, M)$	Digital signature of message M using private key K_i^-
SNV	Source's neighbor vehicles
IV_F	Vehicles behind the source and moving toward the opposite direction
IV_B	Vehicles behind the source and moving toward the same direction
RI_F	Regional message propagating on the opposite direction of the source
RI_B	Regional message propagating on the same direction of the source
$Value$	Aggregated regional traffic information
DV	Delivery vehicles in the time-based approach
PKC, RI	Public key commitment and regional message in the time-based approach
TS_1, TS_2	Transmission time of PKC and RI in the time-based approach, respectively

road section. The source can be elected in a similar way of electing a group leader presented by Picconi et al.[10] The difference in our approach is that the closest vehicle to a new road section is selected as a source (or group leader)(see Fig. 1.1). If every source candidate in the boundary area of a new road section broadcasts a source-election-message, the vehicle that is the closest to the boundary line of the next road section is elected as a source of the road section (the vehicle labeled "S" in Fig. 1.1).

Once a source is elected, the source collects its neighboring vehicles' typical messages and creates an aggregated regional message. Any incident events such as sudden braking that only affects neighboring vehicles for a short time or abnormal data not consistent with the other data, are ignored in the aggregation.

Since group formation and data aggregation are not our main focus in this chapter, we do not consider security vulnerabilities which can take place in the source election and data aggregation such as broadcasting fake location information or traffic information by malicious neighboring vehicles. We believe the existing group formation and data aggregation schemes in a VANET can be easily applied to deal with such security problem.[11,12]

1.4.1.3. *Data propagation*

We define several sets of vehicles related to the data propagation. Fig. 1.3 shows the locations of these vehicles in terms of the source vehicle S.

- SNV (Source's Neighbor Vehicle): A set of vehicles in the boundary area of a road section and in a single transmission range of the source

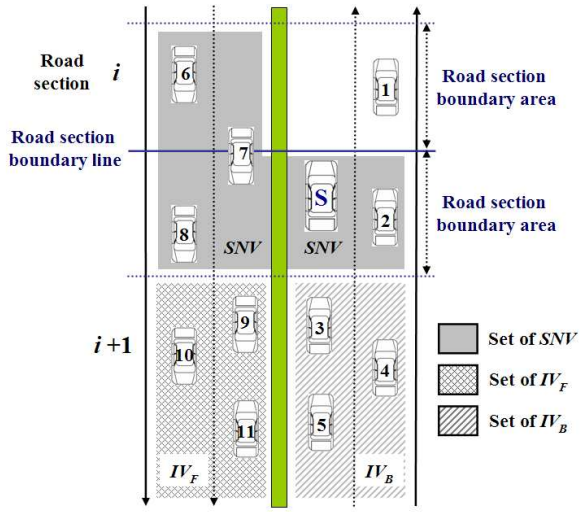

Fig. 1.3. Sets of vehicles on a bidirectional roadway. Each direction has 2 traffic lanes. Vertical arrows represent vehicles' driving directions. Horizontal solid line is the road section boundary line between road section i and $i+1$. Horizontal dotted line shows the road section boundary area.

excluding vehicles in front of the source at the same driving direction of the source. In Fig. 1.3, the SNV of the source S includes vehicles 2, 6, 7 and 8.

- IV (Intermediate Vehicle): A set of vehicles eligible for propagating the regional message to other vehicles. It is divided in IV_F and IV_B according to vehicles' moving direction.
  - IV_B: Vehicles behind the source and moving toward the same direction of the source. In Fig. 1.3 IV_B includes vehicles 3, 4 and 5.
  - IV_F: Vehicles behind the source and moving toward the opposite direction of the source. In Fig. 1.3 IV_F includes vehicles 9, 10 and 11.

The source's regional message is propagated as follows:

(1) The source creates two types of aggregated regional messages about its road section as follows:

$$RI_{PD} = \langle \text{“}RID||PD||MD||Value||SLoc||TS\text{”}\rangle$$

where RID is an identifier of the road section (road ID) and PD = {F, B} is the direction index of the message. If $PD = F$, only vehicles in IV_F forward the message; if $PD = B$, only vehicles in IV_B forward the message. MD is the moving direction of the source and $Value$ represents the aggregated regional information. $SLoc$ indicates the source's location and TS indicates the current transmission time.

(2) The source broadcasts two regional messages $\langle RI_F, RI_B \rangle$. Among vehicles that receive both messages from the source, only vehicles in SNV rebroadcast either RI_F or RI_B based on their driving direction.

(3) When a vehicle i, $i \in IV_F$ receives an RI_F, it discards the message if it has already forwarded it before. Otherwise, it checks if RI_F is given from one of its neighboring vehicles. If so, vehicle i generates its signature $SIG(K_i^-, RI_F)$ on RI_F then forwards $\langle RI_F, SIG(K_i^-, RI_F), K_i^+ \rangle$, where $\langle K_i^-, K_i^+ \rangle$ is vehicle i's private/public key pair. The signature is required for the neighbor-based data forwarding described in Section 1.4.1.1 (as shown in Fig. 1.2).

(4) When a vehicle i, $i \in IV_B$ receives an RI_B, it discards the message if it has already forwarded it before. Otherwise, it checks if RI_B is given from one of its neighboring vehicles. If so, vehicle i generates its signature $SIG(K_i^-, RI_B)$ on RI_B then forwards $\langle RI_B, SIG(K_i^-, RI_B), K_i^+ \rangle$.

Fig. 1.4 illustrates the propagation of a regional message.

The source does not specify the destination (or recipient) vehicle in advance; however, it can specify the propagation range of its regional message. Any vehicle in IV_B can be the destination of the source's regional message if the vehicle wants to read it. The destination vehicle will forward the given RI_B to downstream as long as RI_B is still in its defined propagation range.

1.4.1.4. *Data verification rule*

Once a recipient vehicle D receives both RI_F and RI_B, it accepts the regional message if the traffic data contained in RI_F is identical to the data contained in RI_B. If D could only receive one of the two messages, it treats the regional message as unverified—it can either accepts the message with certain security risk or wait for further messages forwarded from other sources.

Our approach relies on the fact that the probability of two cooperative, malicious vehicles existing in the same road section on opposite driving di-

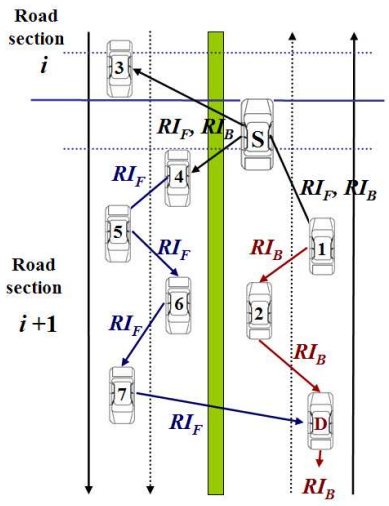

Fig. 1.4. Two-directional data propagation on a two-way road. S represents a source vehicle and D represents an arbitrary recipient vehicle. D can receive RI_B and RI_F from vehicles 2 and 7, respectively. D checks if the two messages are matched. D also propagates RI_B further (without waiting for RI_F to arrive) for vehicles behind it. Vehicles 1 and 2 can possibly receive RI_F broadcasted by vehicles 4, 5 or 6 as well; however, they will not forward RI_F since it belongs to the opposite driving direction.

rections is very low. If such two cooperative malicious vehicles exist, they can only cooperate to disrupt data propagation security within a short time period when they are in close range. The two-directional data verification approach, without any certificate authority[13] or other complicated security protocol, provides a simple yet effective way for reliable traffic data propagation.

1.4.2. *Time-based data verification*

We provided a simple way to verify the integrity of a regional message in the previous section. However, the two-directional approach requires a recipient to receive both RI_F and RI_B for a road section to verify the validity of a regional message. If a vehicle gets only one of them, it cannot accept the message as correct. The message either remains suspicious or discarded. This could happen frequently if a road has sparsely distributed vehicles, such as in rural areas or during the late night. For these scenarios, we propose another technique called "time-based data verification" approach for reliable regional data forwarding.

1.4.2.1. *Data propagation*

We define DV (Delivery Vehicles) as a group of vehicles in a single transmission range of a source at the source's opposite driving direction.

(1) Once a source is elected for a particular road section i, before the source starts to aggregate the regional message, it creates its public key commitment message and broadcasts it first as follows:
   (a) The source computes its public key commitment $KC = H(K_S^+)$, where $H()$ is a cryptographic one-way hash function such as SHA-1.
   (b) The source broadcasts the following public key commitment message to vehicles in its current DV_1 (suppose this action happens at time $t = TS_1$).

$$PKC = \langle M, Sig \rangle = \langle \text{“}RID||MD||KC||TS_1'', Sig(K_S^-, M) \rangle$$

(2) Every vehicle in DV_1 keeps broadcasting PKC periodically as it drives along the road.
(3) The source aggregates its regional message, which is identical to the data aggregation described previously.
(4) After a predefined delay time $Delay$ from the first PKC transmission (i.e., at time $t = TS_2$), the source generates the following data message and broadcasts to its current DV_2.

$$RI = \langle M, Sig, K_S^+ \rangle = \langle \text{“}RID||MD||Value||SLoc||TS_2'', Sig(K_S^-, M), K_S^+ \rangle$$

(5) Every vehicle in DV_2 keeps broadcasting RI periodically as it drives along the road.

One distinctive feature of this approach is that messages will not be forwarded by any vehicle—data propagation is accomplished by vehicles in DV as they move along the road and broadcast these messages.

The broadcasting frequency is calculated by vehicle's speed, wireless transmission range and road width. The guideline of this calculation is to make sure that every vehicle on the same driving direction of the source passing by the delivery vehicle could receive the broadcasted message at least once. In addition, the value of the predefined delay time, $Delay$, is determined such that DV_2 and DV_1 have no overlapped vehicles.

Fig. 1.5 shows the time-based data propagation. At time $t = TS_1$, the source S first broadcasts its PKC as it enters a new road section i (as shown in Fig. 1.5(a)). Vehicles numbered 3, 4 and 5 are the delivery vehicles for PKC at this moment. These three delivery vehicles keep broadcasting

PKC periodically so upcoming vehicles 7, 8 and 9 behind the source can obtain PKC from, for example, vehicle 3 (as shown in Fig. 1.5(b)). After S finishes aggregating its regional information and also a predefined time delay, S creates RI and broadcasts it as shown in Fig. 1.5(c) at time $t = TS_2$. New vehicles numbered 10 and 11 are the delivery vehicles for RI at this moment. These two vehicles will keep re-broadcasting RI periodically as they move on. In this way, vehicles 7, 8 and 9 will receive both messages and accept the regional traffic data.

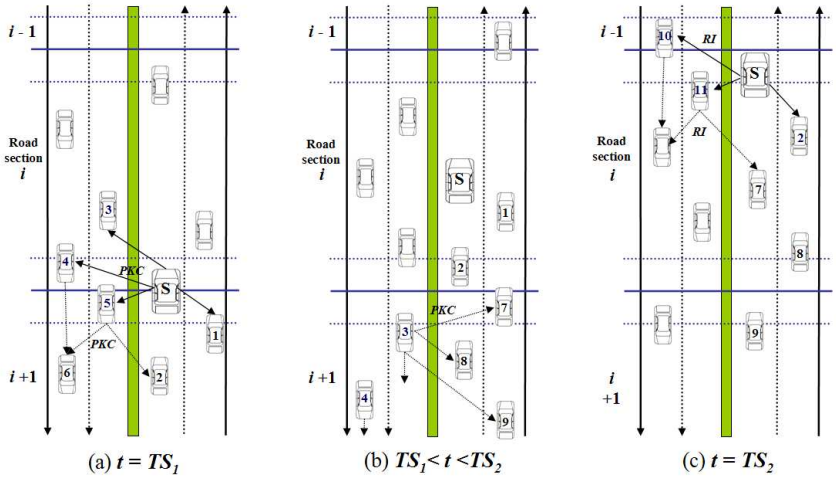

Fig. 1.5. Illustration of time-based data propagation at three different time

Unlike previous two-directional data propagation, message delivery depends on two small groups of delivery vehicles driving at the source's opposite direction. Messages are only periodically broadcasted by delivery vehicles—they will not be relayed hop-by-hop among vehicles. Since the two groups of delivery vehicles are out of each other's signal transmission range, no vehicle on the opposite direction of the source could obtain both messages. Thus a malicious vehicle cannot modify the regional message content without being detected by recipient vehicles. Even if any malicious delivery vehicle modifies, forges or drops a given message, other honest delivery vehicles keep delivering the original message so a recipient vehicle could obtain a correct message pair.

However, since message delivery speed is determined by the moving speed of delivery vehicles, message delivery takes longer time than the pre-

vious described two-directional approach.

1.4.2.2. *Data verification rule*

A recipient vehicle D first receives PKC for a specific road section. After some time delay, it receives its corresponding regional message RI. The regional message will be discarded if $TS_2 - TS_1$ is less than the predefined delay interval $Delay$ (PKC contains TS_1 and RI contains TS_2).

If $TS_2 - TS_1 \geq Delay$, the recipient vehicle D computes the hash value $H(K_S^+)$ of the public key K_S^+ in RI. If KC in PKC equals to $H_F(K_S^+)$, both messages are verified to have used the same public key. Then, vehicle D uses the public key K_S^+ and the Sig contained in RI to verify if received message M in RI is trustable or not.

Therefore, a recipient vehicle accepts a valid pair of $\langle PKC, RI \rangle$ when both messages are (1) signed by the same public key contained in RI; and (2) given with a time delay more than $Delay$ from two different vehicles driving at the opposite direction. The security of this approach relies on two facts. First, the probability is very low for two malicious vehicles, which are far not within the direct transmission range of each other to collaborate for making a reasonable attack (generate a valid message pair). Second, even if there are two pre-determined malicious vehicles driving with a reasonable distance, the probability of only these two vehicles being on the road is also very low. If there are other honest vehicles belonging to DV, these honest vehicles can keep broadcasting the original messages, and hence, a recipient vehicle can eventually receive the valid message pair.

1.4.2.3. *Extension to very sparse traffic situation*

The time-based data verification protocol can be easily modified to work in a very sparse traffic scenario, or when the penetration of smart (VANET-equipped) vehicles is very low at the initial transition stage.

As soon as a source is elected, it generates its PKC. If the source receives any beacon traffic messages from vehicles on its opposite driving direction, it broadcasts PKC to those vehicles. Otherwise, the source continue to carry PKC until it meets any (smart) delivery vehicle at the opposite direction. After waiting for a predefined delay time, $Delay$, since it sends out PKC, the source finds the next group of delivery vehicles for sending RI in the same way and broadcasts the RI message.

Likewise, instead of periodical broadcasting, delivery vehicles will carry messages as they move and broadcast the messages whenever they receive

any beacon traffic message from vehicles on same driving direction of the source.

1.4.2.4. *The combined data verification approach*

Two-directional data propagation approach is simple and delivers messages fast; however, each recipient vehicle is required to obtain the same regional message from both directions of a road. On the other hand, time-based data propagation approach has a higher acceptance rate; however, message delivery in this approach could be very slow (determined by delivery vehicle's speed). Therefore, we can combine both approaches to overcome these weaknesses. We describe this combined data verification approach in this section.

Once a source is elected for a particular road section i, the source S performs the combined data propagation protocol as follows:

(1) The source computes its public key commitment $KC = H(K_S^+)$ and generates PKC as described in Section 1.4.2.1.
(2) The source broadcasts PKC.
(3) Every vehicle in DV keeps broadcasting PKC periodically as it drives along the road.
(4) The source aggregates its regional message.
(5) Right before the source leaves its road section, the source generates three types of regional messages RI_F, RI_B and RI then broadcasts them. $\langle RI_F, RI_B \rangle$ are described in Section 1.4.1.3 and RI is described in Section 1.4.2.1.
(6) Every new vehicle in SNV propagates $\langle RI_F, RI_B \rangle$ according to the data propagation protocol described in Section 1.4.1.3 while vehicles in the current DV broadcast RI periodically as described in Section 1.4.2.1. A vehicle on the source's opposite direction can both forward RI_F and be a delivery vehicle in broadcasting RI.

A recipient vehicle D accepts a received regional message if either RI_F equals to RI_B, or the pair of $\langle PKC, RI \rangle$ matches with each other.

Since $\langle RI_F, RI_B \rangle$ propagate fast by vehicles on both directions, any recipient vehicle can check out the validity of a given regional message through the two-directional approach first. If any mismatch of the two messages occur, the recipient vehicle can wait for RI so it can verify if the pair $\langle PKC, RI \rangle$ is valid. Consequently, the combined data verification protocol overcomes weaknesses of both approaches and provides a strong

way for a reliable data propagation with a high acceptance rate.

1.4.3. *Comparison between two proposed approaches*

We have proposed two novel approaches and a combined approach for the reliable regional traffic information propagation. In this section, we compare and summarize the main features of each.

The two-directional data verification protocol is easy, simple and efficient to set up and verify the integrity of the regional information. The source of a regional message creates two same regional messages without any additional computations. Since the two generated messages are forwarded by intermediate vehicles between the source and any recipient vehicle, the message could be delivered quickly as long as there are a continuous data relay path.

The main drawback of the two-directional data verification protocol is that every recipient vehicle should be able to get the same regional message twice and from both driving directions. If one of those two road directions has a problem for data propagation, which could happen if there are not sufficient number of vehicles on one direction. In that case, a recipient will receive either only one regional message or unmatched two messages, then the recipient vehicle fails to accept the message.

Differing from the two-directional data verification approach, the time-based data verification approach uses only the opposite road direction as the network channel for data propagation—there will always exist vehicles driving on the opposite direction sooner or later for data delivery. Thus, regional messages are more likely to be successfully delivered than in the two-directional approach, especially in rural area or night time when there are not sufficient number of vehicles for the two-directional approach.

The main drawback of the time-based data verification protocol is that message delivery can be slow. Only delivery vehicles carry and broadcast the source's message and message delivery speed is dependent on the moving speed of those delivery vehicles. It is in general much slower than the first approach.

The combined scheme 1.4.2.4 takes advantages of both approaches effectively. It saves time for data verification in most cases, at the same time, it increases the acceptance rate of the regional messages when two-directional approach fails. The only drawback of the combined approach is that for each regional message the source needs to generate four messages (RI_F, RI_B, PKC, RI).

1.5. Security and Robustness

We show that our proposed scheme satisfies the security requirements defined in Section 1.3.

1.5.1. *Data integrity*

The goal of data integrity verification is to protect vehicles from accepting fake information manufactured by malicious vehicles. In the following, we show that our schemes work well against various malicious attacks.

1.5.1.1. *Two-directional data verification*

In the two-directional data verification protocol, the source's regional message is forwarded along two separate directions of a two-way road independently. We can consider two malicious scenarios: (1) only one of the two roadways has malicious vehicles, and (2) both roadways have malicious vehicles.

For the first case, a malicious vehicle M on one direction of a two-way road could modify or forge a given message and forward it. Suppose M drives behind the source on the same direction, for example, the vehicle 2 shown on Fig. 1.4. Instead of forwarding RI_B after receiving this message from vehicle 1, it can forge RI_B to become the forged message, FRI_B. Since FRI_B is not identical to RI_F, any destination vehicle (such as vehicle D) receiving a pair of $\langle RI_F, FRI_B \rangle$ will not accept the regional message based on the verification rule. Thus, this attack will not compromise data integrity in VANET communication. The denial-of-service effect caused by this attack is discussed in Section 1.5.2.

A malicious vehicle M could also carry out more active attacks such as inserting fake regional message about a road section. Suppose M creates a fake pair of messages $\langle FRI_F, FRI_B \rangle$ about the road section i. There are two possible attack scenarios according to M's current location, which are illustrated in Fig. 1.6.

(1) If M tries to generate a fake regional message for a road section ahead of its current location (as shown in Fig. 1.6(a)), the vehicles who directly receive messages from M, vehicles 6 and 8, should be able to receive FRI_F and FRI_B. Based on their current location, vehicles 6 and 8 know that vehicle M is the source; however, it is not reporting traffic event about its current road section. Thus vehicles 6 and 8 will not

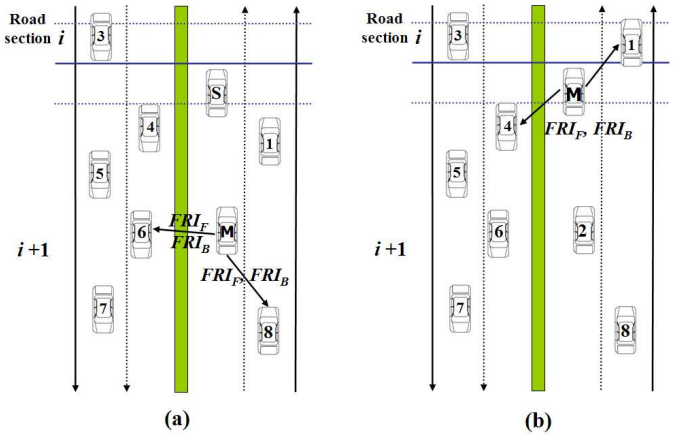

Fig. 1.6. Two possible forge attacks by a malicious vehicle M sending fake regional message about road section i

forward the faked messages.

(2) If M generates a fake regional message for its true location (as shown in Fig. 1.6(b)), among the neighboring vehicles, any vehicle who is at the same road section (such as vehicle 1), or who will move into the road section a moment later (such as vehicle 4), will know that the regional message received is not accurate based on their own observation of the road section i. Thus, they will not forward the messages, or they will immediately generate a warning message to alert others about this malicious attack.

Either way, a fake pair of messages will be either dropped or not be accepted by a recipient vehicle.

For the second case, if two malicious vehicles M_1 and M_2 are on the opposite driving direction, it is possible for them to modify a regional message without being detected under the following two conditions. First, they have to be positioned between the source and the destination vehicles. Second, they have to modify a regional message with the same faked data, even if they cannot communicate with each other (otherwise the faked FRI_F and FRI_B will not match). Since these two malicious vehicles are driving on the opposite direction, they can only successfully attack within a short time period. This means that such an attack is costly to deploy and only effective for a short time. Therefore, we believe our approach, although not perfect, is still effective in defending against most realistic attacks.

1.5.1.2. *Time-based data verification*

In the time-based data verification protocol, two separate groups of delivery vehicles take charge of delivering the source's message pair. There are two possible attack scenarios in this approach: (1) each group includes a combination of honest and malicious vehicles, and (2) both groups consist of only malicious vehicles.

In the first case, since the group of delivery vehicles DV (defined in Section 1.4.2.1) contains honest vehicles, the original pair of regional message (RI_F, RI_B) can always be delivered to any recipient vehicles by those honest vehicles.

In the second case, there is no honest vehicle in either of the groups. The malicious vehicles can make any attacks including modifying, forging, dropping or creating messages. However, the time-based approach makes sure that these two groups are out the communication range of each other (via the time delay between a message pair), thus they can produce a successful attack only if they generate a valid pair of fake messages by predefined rules. Such an attack is possible but hard to do as well. In addition, such an attack can only cheat vehicles that are on the opposite direction of a roadway and have already passed the places where malicious vehicles are heading to—it is hard to see what significant benefit could these malicious vehicles gain through this attack.

1.5.2. *Denial-of-service (DoS) attacks*

A malicious vehicle can intercept, or drop messages from their transmission to make the network unavailable. In the following, we show how attackers could make denial of service attacks, and how our approaches deal with these attacks.

1.5.2.1. *Two-directional data propagation*

Since we assume a not so sparse traffic for this approach, it is highly possible to have honest vehicles as neighbors of a malicious vehicle. If there is at least a single honest neighboring vehicle, the original message can be successfully forwarded by the honest vehicle as illustrated in Fig. 1.7. According to the message propagation policy described in Section 1.4.1.3, the honest vehicle H will forward RI_B since this message has not been forwarded before.

In the worst case scenario where the traffic is sparse and if a malicious vehicle drops the original data RI_B, the data cannot be propagated at that

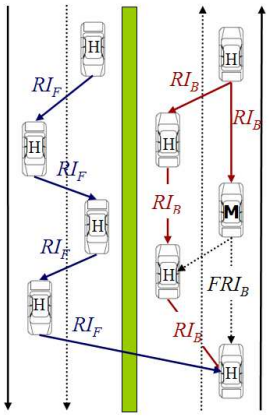

Fig. 1.7. Data propagation with a single malicious vehicle M. The other vehicles labeled H are honest. M can create a forged message FRI_B. If there are honest vehicles around M, the original message RI_B can keep being propagated by those honest vehicles.

moment since no honest vehicle is nearby. If the malicious vehicle creates a forged message FRI_B, any recipient vehicle will get a pair of unmatched regional messages $\langle RI_F, FRI_B \rangle$ (see Fig. 1.7). This is the scenario where a malicious vehicle could cause damage by DoS attack.

However, we can deal with this worst case scenario by adding some time delay for a recipient to accept a regional message. Moments after the above DoS attack happens, it is possible for another source vehicle arriving at the same accident road section to generate a similar regional message and send it (denoted as RI'_F and RI'_B). At this time, due to different vehicle speeds, there could be honest vehicles around the malicious vehicle M to form a new route for the new message RI'_B. Even though the recipient vehicle receives two different messages (RI_F, RI'_B), it will accept the message as long as the content of these two messages are consistent. This scenario shows that although our approach still has a weakness against a particular DoS attack, it limits the impact of such an attack greatly.

1.5.2.2. *Time-based data propagation*

While the two-directional data propagation is relatively vulnerable against the DoS attack when it comes to a sparse traffic, the time-based data propagation is not affected by the traffic density but rather by the population of malicious vehicles in those two delivery vehicle groups. If each deliv-

ery group involves any single honest vehicle, the original message can be delivered to every recipient vehicle by the honest vehicle in each of those two groups. In a very sparse traffic condition, the source can wait for any potential delivery vehicles to send its PKC or RI and the delivery vehicles can adjust their re-broadcasting period according to the traffic condition.

If a delivery group includes only malicious vehicles, the message carried by the group will be lost. As a recipient vehicle cannot obtain a complete message pair, the DoS attack by the malicious group will succeed. However, the probability of each delivery group containing only malicious vehicles is rather low since we assume that the majority of the vehicles are honest. If we want the network to work even under this rare attack scenario, we can let the source vehicle send the same message twice. In other words, the source can wait for another delivery vehicle to re-broadcast the same message in order to increase the chances of the successful delivery of the message.

1.6. Simulation Study

1.6.1. *Simulation environment and metrics*

We evaluated the performance of our proposed schemes using NS-2 network simulator. In the two-directional data verification protocol, the simulation parameters include (i) time delay between RI_F and RI_B for a single recipient vehicle, (ii) propagation delay of the regional message based on distance, and (iii) minimal density of vehicles in order to protect data fragmentation during the propagation. During the simulation of the first two simulation parameters, we assume that vehicles are evenly distributed on the road with a density of 3.4 vehicles per km in order to set up the most sparse distribution while 4 to 52 vehicles per km are evenly distributed in the simulation of the third parameter. In the time-based data verification protocol, we simulated the total time delay to receive both PKC and RI according to variant densities of vehicles on the opposite directional roadway.

We summarize the default values and the range of parameters used in our simulation study in Table 1.2.

Table 1.2. The default values and the range of the parameters in simulation study

Field	**Value**	**Range**
Simulation roadway length	30 km	10 - 30 km
Transmission range	300 m	250 - 350 m
Moving speed	110 km/h	80 - 110 km/h
Message size	100 Kb	
Message bandwidth	1 Mbps	

1.6.2. *Simulation results*

1.6.2.1. *Two-directional data propagation*

Fig. 1.8 shows the time delay between two regional messages RI_F and RI_B in the two-directional data propagation scheme. We assume that 100 vehicles are evenly distributed on each directional roadway and they are moving with a speed of 110 km/h. There is at least 11 ms of time delay between the first and the second arrived messages. According to the network condition, some following vehicles receive RI_B first while some others get RI_F first. The time delay slightly increases as the distance of a vehicle from the target road section becomes farther apart.

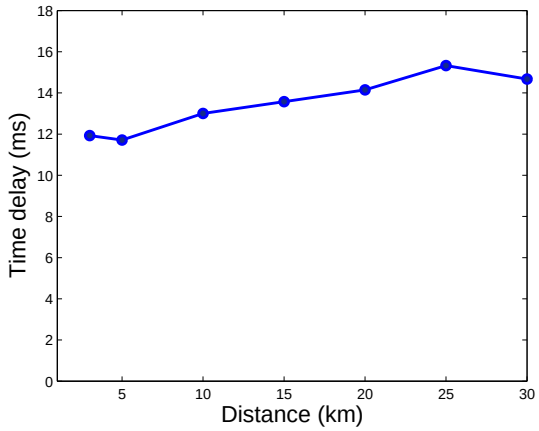

Fig. 1.8. Time delay between RI_F and RI_B in the two-directional data propagation

Fig. 1.9 shows the propagation delay to receive both regional messages. It takes about 25 ms for the regional messages to arrive at vehicles in the

range of 5 km from the target road section while it takes about 156 ms for those messages to arrive at vehicles in the range of 30 km from the target road section. Even though the propagation delay increases proportionally to the distance, it is negligible compared with the time delay for the recipient vehicles to reach the target road section.

We also conducted experiments where vehicles have a speed of 80 km/h. The results were almost the same with a little time difference of tens of nanoseconds. Since the data transmission time is very fast, delays were hardly affected by vehicles' moving speeds.

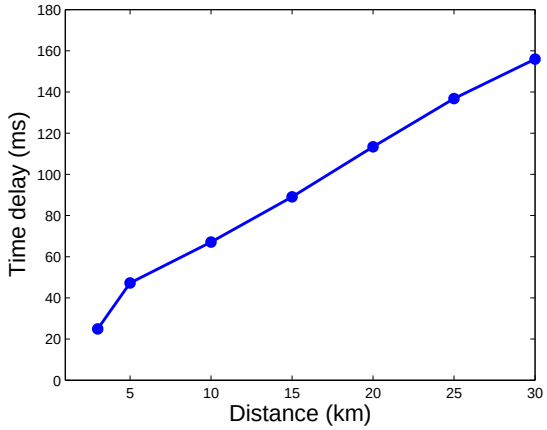

Fig. 1.9. Propagation delay of the regional messages in the two-directional data propagation

Next, we evaluate the minimal density of vehicles to guarantee a full connectivity among vehicles without any data fragmentation in the middle of the data propagation. We assume that the vehicles are randomly distributed on a 10 km long road. The number of vehicles is increased from 40 to 520 to experiment with diverse densities. For each density, the simulation is performed 100 times to generate various traffic situations. For each simulation run, we check for the full connectivity among the entire propagation range. In other words, the full connection is achieved if the data propagation is successfully completed over a set of vehicles without any fragmentation during the propagation. We count the total number of the full connections among 100 runs for each vehicle density.

Fig. 1.10 shows the number of full connections according to density and

data transmission ranges. The data transmission ranges of 250 m, 300 m and 350 m are used. We can see that at least 200 vehicles per 10 km for 350 m transmission range, 240 vehicles for 300m transmission range and 280 vehicles for 250 m transmission range are required to achieve about 80% of full connectivity under the assumption of a single broadcast. Thus, in a sparse traffic, we should allow vehicles to re-broadcast the same regional message a few times to prevent any data fragmentation.

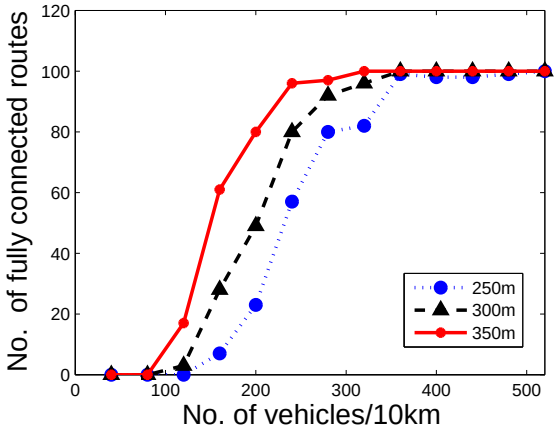

Fig. 1.10. The number of fully connected links among 100 simulation runs according to density and data transmission range in the two-directional data propagation.

1.6.2.2. *Time-based data propagation*

We evaluate the approximate time delay for a recipient vehicle to receive RI according to various densities of delivery vehicles. For this experiment, we assume the vehicle speed of 110 km/h, the distance of a single road section of 600 m, and the road width RW of 50 m. Based on these settings, an approximated minimum delay time between PKC and RI and an approximated re-broadcasting period of a single delivery vehicle would be 20 seconds and 9.6 seconds respectively. Every vehicle is expected to broadcast its typical message periodically in every second. At the beginning of this experiment, the source looks for a delivery vehicle to send the PKC and broadcasts it when the source receives a typical message from a vehicle on its opposite direction. After source waiting for a *delay* amount of time since sending the PKC, the source waits for another delivery vehicle can-

didate to send the RI. As soon as it receives a typical traffic message from a vehicle on its opposite direction, it sends the RI. In order to experiment with the impact of different densities of delivery vehicles, we assume that 5, 10, 20 and 30 vehicles per 10 km are evenly distributed on the source's opposite directional roadway in different simulation runs.

Fig. 1.11 shows incurred time delay for a recipient vehicle (which was at 20 km away from the source initially) to receive the PKC and the RI according to different densities of the delivery vehicles. It will take at least 654 seconds for the recipient vehicle to arrive at the target road section at a speed of 110 km/h. As can be seen in Fig. 1.11, when only 5 vehicles are present in the interval of 10 km, the recipient vehicle receives the PKC and the RI after 353 seconds and 386 seconds respectively upon moving toward the target road section. As the density of delivery vehicles increases up to 20 per 10 km, the recipient vehicle can obtain these messages faster. If there always exist vehicles on the opposite direction within a single data transmission range of a source, a recipient vehicle could receive the RI in almost half time of its arrival time at the target road section. This is because the source does not have to wait for any potential delivery vehicle to send the PKC and the RI. However, denser distribution of the potential delivery vehicles does not increase the speed of the message delivery since it is purely dependent on the moving speed of the delivery vehicles at that moment. Therefore, the message delivery time remains almost the same as the number of the potential delivery vehicles increases from 20 to 30.

1.7. Conclusion

In this chapter, we proposed two novel data verification approaches, two-directional and time-based, for reliable long-existing traffic information propagation on two-way traffic roads. The main idea behind these approaches is to make two different groups of vehicles deliver the same regional traffic message independently. If two messages given from these two groups are either identical or correctly associated with each other, a recipient vehicle accepts that the received regional message is correct. These approaches work effectively because it is either hard or costly for attackers to modify both messages at the same time. Compared with previous VANET security themes that required the support of the complicated and expensive public key infrastructure, the proposed approaches are much simpler and easy to implement, especially during the initial transition stage when a mature VANET network infrastructure does not exist.

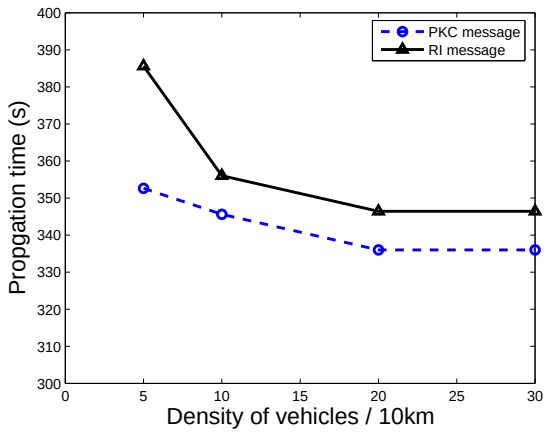

Fig. 1.11. Time delay for delivering PKC and RI according to densities of delivery vehicles in the time-based data propagation.

Acknowledgement

This work was supported by NSF Cyber Trust Grant CNS-0627318 and Intel Research Fund.

References

1. L. Wischhof, A. Ebner, H. Rohling, M. Lott, and R. Halfmann. SOTIS - a self-organizing traffic information system. In *Proceedings of the 57th IEEE Vehicular Technology Conference (VTC)*, pp. 2442–2446, (2003).
2. M. Raya and J. Hubaux. The security of vehicular ad hoc networks. In *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks (SASN)*, pp. 11–21, (2005).
3. P. Papadimitratos, V. Gligor, and J. Hubaux. Securing vehicular communications - assumptions, requirements, and principles. In *Proceedings of the Workshop on Embedded Security in Cars (ESCAR)*, pp. 5–14, (2006).
4. J. Hubaux, S. Capkun, and J. Luo, The security and privacy of smart vehicles, *IEEE Security and Privacy*. **2**(3), 49–55, (2004).
5. K. Plobl, T. Nowey, and C. Mletzko. Towards a security architecture for vehicular ad hoc networks. In *Proceedings of the First International Conference on Availability, Reliability and Security (ARES)*, pp. 374–381, (2006).
6. P. Papadimitratos, A. Kung, J. Hubaux, and F. Kargl. Privacy and identity management for vehicular communication systems: A position paper. In *Proccedings of the Workshop on Standards for Privacy in User-Centric Identity Management*, (2006).

7. F. Dotzer, *Privacy Issues in Vehicular Ad Hoc Networks*. (Springer Berlin/Heidelberg.
8. J. Liu, X. Hong, Q. Zheng, and L. Tang. Privacy-preserving quick authentication in fast roaming networks. In *Proceedings of 31st IEEE conference on Local Computer Networks (LCN)*, pp. 975–982, (2006).
9. B. Parno and A. Perrig. Challenges in securing vehicular networks. In *Proceedings of the Workshop on Hot Topics in Networks (HotNets-IV)*, (2005).
10. F. Picconi, N. Ravi, M. Gruteser, and L. Iftode. Probabilistic validation of aggregated data in vehicular ad-hoc networks. In *Proceedings of the 3rd International Workshop on Vehicular Ad Hoc Networks (VANET)*, pp. 76–85, (2006).
11. M. Raya, A. Aziz, and J. Hubaux. Efficient secure aggregation in vanets. In *Proceedings of the 3rd International Workshop on Vehicular Ad Hoc Networks (VANET)*, pp. 67–75, (2006).
12. P.Golle, D. Greene, and J. Staddon. Detecting and correcting malicious data in vanets. In *Proceedings of the 1st International Workshop on Vehicular Ad Hoc Networks (VANET)*, pp. 29–37, (2004).
13. S. U. Rahman and U. Hengartner. Secure crash reporting in vehicular ad hoc networks. In *Proceedings of the 3rd International Conference on Securing and Privacy in Communication Networks (SecureComm)*, pp. 443–452, (2007).
14. J. Zhao and G. Cao, VADD: Vehicle-assisted data delivery in vehicular ad hoc netowkrs, *IEEE Transactions on Vehicular Technology*. **57**(3), 1910–1922 (May, 2008).
15. Q. Sun and H. Garcia-Molina. Using ad-hoc inter-vehicle networks for regional alerts. In *Technical Report, Stanford University*, (2004).
16. H. Deng, R. Xu, J. Li, F. Zhang, R. Levy, and W. Lee. Agent-based cooperative anomaly detection for wireless ad hoc networks. In *Proceedings of the 12th International Conference on Parallel and Distributed Systems (ICPADS)*, pp. 613–620, (2006).
17. A. Studer, M. Luk, and A. Perrig. Efficient mechanisms to provide convoy member and vehicle sequence authentication in vanets. In *Proceedings of the 3rd International conference on security and privacy in communication networks (SecureComm)*, pp. 422–432, (2007).