Secure traffic data propagation in Vehicular Ad Hoc Networks

Baber Aslam*, Soyoung Park, Cliff C. Zou and Damla Turgut

School of Electrical Engineering and Computer Science,
University of Central Florida,
Orlando, Florida 32816-2362, USA
E-mail: ababer@eecs.ucf.edu
E-mail: park@eecs.ucf.edu
E-mail: czou@eecs.ucf.edu
E-mail: turgut@eecs.ucf.edu
*Corresponding author

Abstract: In vehicular ad hoc network, vehicles can share traffic/emergency information. The information should not be modified/manipulated during transmission without detection. We present two novel approaches to provide reliable traffic information propagation: two-directional data verification, and time-based data verification. The traffic message is sent through two (spatially or temporally spaced) channels. A recipient vehicle verifies the message integrity by checking if data received from both channels are matched. Compared with the popular public-key based security systems, the proposed approaches are much simpler and cheaper to implement, especially during the initial transition stage when a mature VANET network infrastructure does not exist.

Keywords: VANET; vehicular ad hoc network; initial deployment stage; secure data propagation.

Reference to this paper should be made as follows: Aslam, B., Park, S., Zou, C.C. and Turgut, D. (2010) 'Secure traffic data propagation in Vehicular Ad Hoc Networks', *Int. J. Ad Hoc and Ubiquitous Computing*, Vol. 6, No. 1, pp.24–39.

Biographical notes: Baber Aslam received the BE in Telecomm and MS in Information Security from National University of Sciences and Technology, Pakistan, in 1997 and 2006, respectively. Currently, he is a PhD Scholar in School of Electrical Engineering and Computer Science from University of Central Florida. His research interests include computer and networks security.

Soyoung Park received her BS, MS in Computer Science and PhD on Cryptology from Ewha Womans University, Korea in 1998, 2000 and 2006 respectively. Currently, she is a Post-doctoral Researcher at the School of Electrical Engineering and Computer Science, University of Central Florida. Her research interests include cryptography, network security and privacy preserving ubiquitous computing.

Cliff C. Zou received his BS and MS Degree from University of Science and Technology of China in 1996 and 1999, respectively. Then, he received the PhD Degree in Department of Electrical and Computer Engineering from University of Massachusetts, Amherst, MA, in 2005. Currently, he is an Assistant Professor in School of Electrical Engineering and Computer Science, University of Central Florida. His research interests include computer and network security, network modelling and wireless networking.

Damla Turgut is an Associate Professor at the School of Electrical Engineering and Computer Science of University of Central Florida. She received her BS, MS, and PhD Degrees from the Computer Science and Engineering Department of University of Texas at Arlington. Her research interests include wireless networking and mobile computing, wireless communication and coordination in embodied agents, and urban sensing. She serves as a member of the editorial board and the technical program committee of ACM, IEEE journals and international conferences. She is a member of IEEE, ACM, and Upsilon Pi Epsilon honorary society.

1 Introduction

With the significant development of network technologies, VANETs have been emerging as a feasible and critical application for automobile industry. Some existing traffic broadcasting systems, such as traffic radio and road-side electronic bulletin boards, can provide traffic information periodically for specific locations and directions. Compared to these systems, a VANET system could provide much detailed, real-time, and individualised traffic service and also unlimited data services to vehicles.

There are many challenges for achieving a sustainable collaboration and data sharing among vehicles in a VANET (Blum et al., 2004; Yousefi et al., 2006). Security challenges are the critical and indispensable issues to solve in the first place in order to build realistic and practical VANET applications (Yousefi et al., 2006; Parno and Perrig, 2005; Hubaux et al., 2004; Raya et al., 2006b). The existing security research work in VANETs include Self-Organising Traffic Information System (SOTIS) (Wischhof et al., 2003), security and privacy issues (Raya and Hubaux, 2005; Papadimitratos et al., 2006a, 2006b; Hubaux et al., 2004; Plobl et al., 2006; Dotzer, 2006), fast authentication (Liu et al., 2006; Parno and Perrig, 2005), secure data aggregation (Picconi et al., 2006; Raya et al., 2006a), and detecting and correcting malicious data (Raya et al., 2006a; Golle et al., 2004), and so on. Among these security challenges, we focus on the reliable traffic information propagation through multiple vehicles. 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 several minutes or even several hours. We name such an aggregated traffic message as 'regional message' in this paper.

Since regional messages should spread over multiple vehicles through a public wireless network channel, the probability that they can be modified or forged by attackers and malicious drivers during the propagation path greatly increases as these messages propagate further. If the original messages have been altered along the propagation process, the following vehicles should be able to detect the modification and reject these altered messages in order to have a reliable VANET application.

In this paper, we present two novel approaches for vehicle-assisted secure traffic data propagation without any additional roadside infrastructure and special technologies (such as public key infrastructure). The proposed approaches use mobile vehicles on two-way traffic roads to verify the correctness of any delivered regional messages. Since two-way roads are the dominant vehicular environment, our approaches are applicable for most VANET scenarios.[1]

The central design goal of our approaches is to provide *sound* security mechanisms that are simple and economical to implement. The proposed approaches are not attack-proof, but are designed to make any possible successful attacks to be difficult and costly for attackers to conduct. We believe such a design objective is practical and suitable for most vehicular networking applications, especially during the initial deployment stage when the comprehensive VANET support infrastructure has not built up yet. The two proposed approaches are:

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 separate 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:

- have two cooperative vehicles on both driving directions
- 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 pass each other on the opposite direction quickly. If attackers have such two cooperative vehicles, they can only attack our proposed system within a short period of time 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 twice. 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 messages. Because of the time delay between this pair of messages, 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.

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 a VANET. We neither need to use certificates nor its related operations. Our approaches exploit the unique features of bidirectional roadway and high mobility of vehicles to protect traffic information propagation in a VANET.

The remainder of this paper is organised as follows. Section 2 summarises the related work. We provide detailed descriptions for our approaches in Section 3. The security and robustness of our approaches are analysed in Section 4. The simulation results are given in Section 5. We provide a discussion of related issues in Section 6. Finally, we conclude in Section 7.

2 Related work

Many existing work about secure vehicular communication (Raya and Hubaux, 2005; Papadimitratos et al., 2006a, 2006b; Hubaux et al., 2004; Plobl et al., 2006) rely on established vehicular public key infrastructure for providing an Authentication, Authorisation, 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; they may be used in different regions where there could be vastly different legal policies and roadside infrastructure. Thus, designing a robust and scalable key management scheme for the (nation-wide or continent-wide) vehicular public key infrastructure is a big challenge. In addition, it is necessary 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 (2007) 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 (2008) 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, 2004) proposed bidirectional perimeter-based propagation of regional alerts for fast data delivery. This is similar to our concept that it deals with the long-distance propagation of regional alerts, and both vehicles on bidirectional traffic roads forward those messages for fast delivery; however, the authors did not consider the security issue in data propagation. They also presented an efficient message delivery protocol that minimises the number of broadcasts needed for maintaining a regional alert over a period of time, again without consideration to security.

Furthermore, the need to remove compromised, faulty, misbehaving, or illegitimate nodes is essential for designing vehicular security architectures. One such architecture is proposed by Papadimitratos et al. (2007), main objectives including management of the identities and cryptographic keys, the security of communications, and inclusion of privacy enhancing technologies.

A range of security mechanisms have been proposed to evict these problematic nodes from the network (Raya et al., 2007; Moore et al., 2008). Raya et al. (2007) proposed protocols such as Local Eviction of Attackers by Voting Evaluators (LEAVE) which is considered a more comprehensive revocation method. Moore et al. (2008) conducted a performance analysis of the LEAVE and Stinger protocols followed by proposing a hybrid algorithm leveraging the advantages of the previous approaches. The eviction of compromised nodes can be achieved via distribution of Certificate Revocation Lists (CRLs) (Papadimitratos et al., 2008; Laberteaux et al., 2008). Papadimitratos et al. (2008) further investigate the efficient and effective distribution of CRLs which takes advantages of the road-side vehicular infrastructure. Laberteaux et al. (2008) on the other hand, propose an approach for vehicle-to-vehicle epidemic distribution of certificate revocation lists.

Privacy enhancing mechanisms are also critical in vehicular communications. For instance, while vehicles periodically broadcast safety messages, the location of these vehicles become known, risking the drivers' privacy. The CMIX protocol, introduced by Freudiger et al. (2007), to produce cryptographic mix-zones at various locations for instance at the road intersections of the vehicular network where the vehicles are able to change their pseudonyms.

The idea of comparing data from different sources before validating received messages is known in the research community as data trust. Raya et al. (2008) presented how to determine the trust level of received message based on multiple reports, differing from our paper since we focus on how to deliver two reports to a recipient vehicle such that a malicious vehicle cannot modify both reports.

3 Proposed approaches

Before we describe our proposed approaches in detail, we first introduce how vehicles distinguish their driving directions. The vehicles on different driving directions on a two-way road have different roles in regional message

propagation, thus it is necessary for us to provide a simple and practical mechanism for driving direction detection.

Driving direction detection

In this paper, 'driving direction' does not mean that a vehicle needs to know its geographical moving direction. Since we want to treat vehicles on the two driving directions on a two-way road differently, 'driving direction detection' means that a vehicle should be able to determine within its wireless transmission range which of the vehicles are moving in the same direction.

In a VANET, every vehicle periodically broadcasts a short beacon message to detect its neighbouring vehicles and decides when it should send or receive messages. A beacon message contains the sender's Identification number (ID) and other information needed by different VANET applications. If vehicle V receives beacon messages with the same ID repeatedly, it adds the ID to its neighbouring list and keeps it until the vehicle no longer receives beacon messages with that ID.

Each vehicle V dynamically determines the number of same ID beacon messages (denoted by N_b) it requires to receive from a vehicle V' to add V' in its neighbouring list. The value of N_b is determined by the speed of vehicle V (denoted by s), the wireless transmission range of the vehicle (denoted by R), and the broadcasting period of beacon messages (denoted by T_b). We need to make sure that any vehicle on the opposite driving direction can successfully transmit at most $N_b - 1$ beacon messages to the vehicle V. In this way, neighbouring list in vehicle V only contains vehicles that are:

- driving on the same direction
- within vehicle V's transmission range.

This definition of neighbouring vehicles is different from traditional neighbourhood definition where only geographical distance is considered (such as in Studer et al. (2007)).

Suppose vehicle V has a moving speed of s when it conducts driving direction detection. Vehicles on the opposite driving direction have unknown speeds, thus we need to consider the worst scenario where they have moving speed of 0. We can derive the lower bound of N_b:

$$N_b > \left\lfloor \frac{2R}{s \cdot T_b} \right\rfloor. \tag{1}$$

This formula means that if a vehicle moves slowly, it needs a large number of same ID beacon messages for driving direction detection. If the road section is heavily congested, or the road section has a traffic light, the proposed method to detect driving direction may not work. In such situations, vehicles can temporarily freeze their neighbourhood update procedure and keep using the old neighbourhood list for data communication. Since all vehicles are moving slowly or stopped, a vehicle's neighbour will stay as its neighbour for a long time. Therefore, such a practice does not affect data communication.

If we want to prevent malicious vehicles from spoofing a beacon message with another vehicle's ID, we can rely on a simple implementation of public key cryptography (without certificate or public key infrastructure). Each vehicle generates its own public/private key pair (K^+, K^-). The public key K^+ is used as the vehicle's ID. A beacon message contains $\{K^+, K^-(K^+, \text{nonce})\}$ where $K^-(K^+, nonce)$ is used to prevent any other vehicle from spoofing or replaying the beacon message.

Table 1 lists the notations used in this paper.

Table 1 Notations used

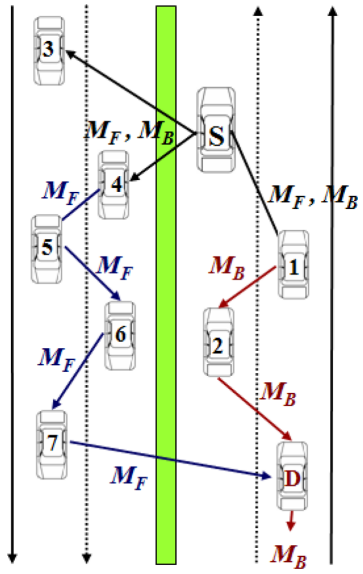
Notation	*Meaning*
M	Regional message
K_i^+, K_i^-	Public key and private key for vehicle i
M_F	Regional message propagating on the opposite direction of the source, $M_F = (M,$ 'forward')
M_B	Regional message propagating on the same direction of the source, $M_B = (M,$ 'backward')
FM_F, FM_B	Fake message of M_F and M_B respectively generated by malicious vehicle
DV	Delivery vehicles – the group of vehicles on the source's opposite driving direction that are within the source's transmission range for time-based approach
DV_1, DV_2	Delivery vehicles in the time-based approach at time $t = T_1, T_2$ respectively
M_1, M_2	Delivered message in the time-based approach at time $t = T_1, T_2$ respectively $M_i = (M, T_i)$, $i = 1, 2$
T_{delay}	Time delay between the two message deliveries in the time-based approach
R	Vehicular wireless transmission range
s	Vehicle moving speed

3.1 Two-directional data verification approach

3.1.1 Data propagation

Figure 1 illustrates the propagation of a regional message M by the two-directional approach. For a regional message M, the source vehicle (denoted by S in the figure) generates two messages to broadcast: $M_F = (M,$ 'forward') and $M_B = (M,$ 'backward'). The source vehicle wants to inform its regional message to the vehicles behind it that will arrive at the source's road segment in the near future. D denotes one of the recipient vehicle who wants to receive the regional message and react accordingly.

Figure 1 Two-directional data propagation on a two-way road. Vehicles on the right side drive upward. S represents a source vehicle who generates regional messages and D represents an arbitrary recipient vehicle. D can receive M_B and M_F from vehicles 2 and 7, respectively. D checks if the two messages are matched. D also relays M_B further (without waiting for M_F to arrive) for vehicles behind it. Vehicles 1 and 2 can possibly receive M_F broadcasted by vehicles 4, 5 or 6 as well; however, they will not forward M_F since this message belongs to the opposite driving direction (see online version for colours)



As shown in Figure 1, the message M_F will be forwarded by vehicles on the opposite driving direction – it propagates towards the moving direction of vehicles on this way. On the other hand, the message M_B will be forwarded by vehicles on the same driving direction of the source. These vehicles are behind the source and relay the message backwards. In other words, a vehicle on the message propagation path forwards either M_F or M_B according to its relative position from the source, even if it may receive the other broadcast message by vehicles on the other driving direction.

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 along the propagation path of M_B can be the destination of the source's regional message if the vehicle wants to read the message. The destination vehicle will forward the given M_B to downstream as long as M_B is still in its defined propagation range.

3.1.2 *Data verification rule*

Once a recipient vehicle D receives both M_F and M_B, it accepts the regional message M if the traffic data contained in M_F is identical to the data contained in M_B. If D only receives one of the two messages, lets say M_F, it treats the regional message as unverified. It can either accept the message with certain security risk or wait for the other message, M_B, sent from vehicles on the other driving direction. It can also wait for further messages generated from other sources to verify the data integrity of the received traffic which will be explained later.

In order for an attacker to alter a propagating regional message without being detected, the attacker needs to:

- have two cooperative vehicles on both driving directions
- both malicious vehicles must be placed between the source of the regional message and the recipient vehicle.

If such two cooperative malicious vehicles exist, they can only cooperate to disrupt data propagation security within a short time period before they move away from each other. Therefore, it is very restrictive and costly to conduct successful attack to the two-directional approach. The two-directional data verification approach, without any certificate authority (Rahman and Hengartner, 2007) or other complicated security protocol, provides a simple yet effective way for reliable traffic data propagation.

3.1.3 *Carry-forward extension to two-directional approach*

Once a complete transmission path exists, the propagation delay in the two-directional approach is very small in the time scale of milliseconds. However, this requires a connected network on both directions for its successful execution. When vehicle density is not high enough, it is possible that there is no complete transmission path between a source and a destination.

In the absence of a fully-connected path in either of the directions, we can extend the two-directional approach by using carry-forward paradigm. In carry-forward paradigm, if a node is unable to forward the message because its downstream nodes are out of its wireless transmission range, it temporarily stores the message until at least one of its downstream node is within its vicinity. In the case of vehicular networks, this approach is suitable since the network topology dynamically changes due to different vehicle speeds. This is especially useful in term of propagating message M_F since the vehicles relaying this message are travelling in the direction of message propagation. In the worst case, the vehicle temporarily storing a message will deliver the message to the destination when it passes by the destination vehicle.

With this carry-forward enhancement, the proposed two-directional approach can be deployed for both high density and low density network scenarios.

3.2 *Time-based data verification approach*

We provide a simple way to verify the integrity of a regional message discussed in the previous section.

The two-directional approach requires a recipient vehicle to receive both M_F and M_B for a road section to verify the validity of a regional message M. If a vehicle gets only one of the messages, 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.

3.2.1 Data propagation

In the time-based approach, a source vehicle only relies on vehicles on the opposite driving direction to carry out the regional message propagation. We define Delivery Vehicles (DV) as the group of vehicles at the source's opposite driving direction that are within the source's transmission range.

The basic idea of this approach is to transmit a regional message via two separated steps where the time delay between these two steps guarantees that a malicious delivery vehicle cannot obtain both transmissions in order to modify the regional message without being detected. The detailed data propagation procedure is as follows:

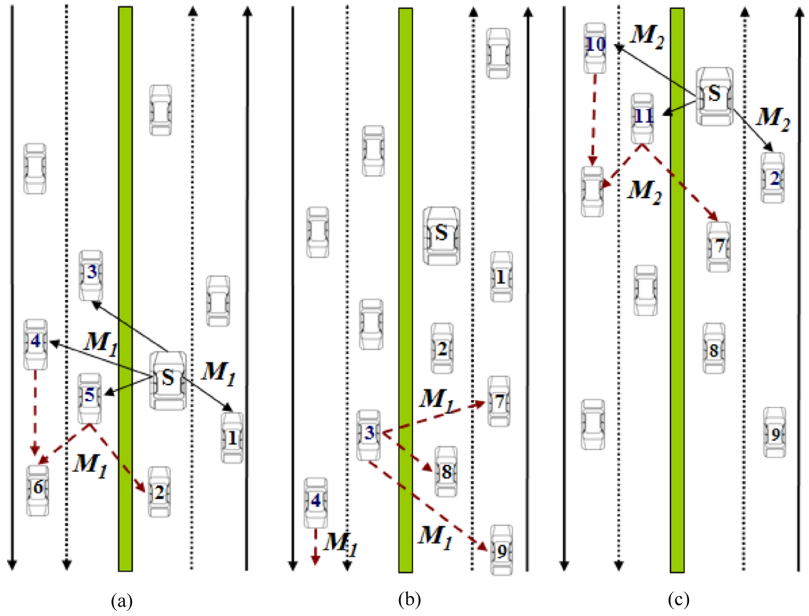
- Once a source has some traffic data to send (such as detecting certain accident or congestion ahead), it creates the first-step regional message $M_1 = (M, T_1)$ and broadcasts the message to its current delivery vehicles in DV_1. T_1 is the time when the source vehicle broadcasts the first message M_1.
- Each vehicle in DV_1 keeps broadcasting M_1 periodically as it drives along the road. In this way, vehicles behind the source that are on the same driving direction of the source will receive message M_1 as they are passed by vehicles in DV_1.
- After a predefined time delay, T_{delay}, from the transmission time T_1 of the first-step message M_1, the source generates the second-step regional message $M_2 = (M, T_2)$ and broadcasts the message to its current delivery vehicles in DV_2. T_2 is the transmission time of M_2 and $T_2 \geq T_1 + T_{\text{delay}}$.
- Each vehicle in DV_2 keeps broadcasting M_2 periodically as it drives along the road.

One distinctive feature of this approach is the fact 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 time delay, T_{delay}, is determined such that DV_1 and DV_2 have no overlapped vehicles.

Figure 2 show the time-based data propagation at three different times. At time $t = T_1$, the source S first broadcasts its M_1 as it has some regional traffic data to send as shown in Figure 2(a). Vehicles numbered 3, 4 and 5 are the delivery vehicles for M_1 at this moment. These three delivery vehicles keep broadcasting M_1 periodically such that upcoming vehicles 7, 8 and 9 behind the source can obtain M_1 from, for example, vehicle 3 as shown in Figure 2(b). After the predefined time delay, S creates M_2 and broadcasts it as shown in Figure 2(c) at time $t = T_2$. The new vehicles numbered 10 and 11 are the delivery vehicles for M_2 at that time. These two vehicles will keep re-broadcasting M_2 periodically as they move. In this way, vehicles 7, 8 and 9 will receive both M_1 and M_2 messages and accept the regional traffic data after verifying that M_1 and M_2 are matched.

Figure 2 Illustration of time-based data propagation at three different times: (a) $t = TS_1$; (b) $TS_1 < t < TS_2$ and (c) $t = TS_2$ (see online version for colours)



Unlike the 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 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 such that a recipient vehicle could obtain a correct message pair.

However, since message delivery speed is determined by the moving speed of the delivery vehicles, message delivery takes longer time than the previously described two-directional approach.

3.2.2 Data verification rule

A recipient vehicle D first receives M_1 at time $t = R_1$. After some time delay, it receives its corresponding second-step message M_2 at time $t = R_2$. M_1 and M_2 are treated as a pair of regional message if they contain the same source's ID. The regional message M will be discarded if $R_2 - R_1 < T_{\text{delay}}$. Otherwise, the recipient vehicle D accepts the regional message M if M_1 and M_2 are matched.

The security of this approach relies on two facts. First, the probability is low for two malicious vehicles that are not within the direct transmission range of each other to collaborate for making a reasonable attack, essentially 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 low. If there are other honest vehicles belonging to DV_1 and DV_2, these honest vehicles can keep broadcasting the original messages, and hence, a recipient vehicle can eventually receive the valid message pair.

3.2.3 Extension to 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.

If a source vehicle receives any beacon messages from vehicles on its opposite driving direction, it broadcasts M_1 to those vehicles. Otherwise, the source broadcasts M_1 when it passes any (smart) delivery vehicle at the opposite direction. After waiting for the predefined time delay, T_{delay}, the source finds the next group of delivery vehicles in the same way and broadcasts the M_2 message.

Likewise, instead of periodic broadcasting, delivery vehicles will carry messages as they move and broadcast the messages whenever they receive any beacon traffic message from vehicles on the same driving direction of the source.

3.3 The combined data verification approach

The 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, the time-based data propagation approach has a higher acceptance rate; however, message delivery in this approach could be slow since it is determined by delivery vehicle's speed. Therefore, we can combine both approaches to overcome these weaknesses. We describe the combined data verification approach in this section.

Once a source vehicle has generated a regional message to send, it conducts the data propagation according to the following steps:

1 The source creates the first-step regional message $M_1 = (M, T_1)$ and broadcasts the message to its current delivery vehicles in DV_1 at time $t = T_1$. In addition, the source creates M_F and M_B as described in Section 3.1.1 and broadcasts these two messages as well.

2 Every vehicle in DV_1 keeps broadcasting M_1 periodically as it drives along the road. The vehicles forward M_F and M_B according to their position and driving direction as described in Section 3.1.1.

3 After a predefined time delay, the source generates $M_2 = (M, T_2)$ and broadcasts the message to its current delivery vehicles in DV_2 at time $t = T_2$.

4 Every vehicle in DV_2 keeps broadcasting M_2 periodically at it drives along the road.

A recipient vehicle D accepts a received regional message M if either M_F and M_B are matched, or M_1 and M_2 are matched.

Since (M_F, M_B) propagate fast by vehicles on both directions, any recipient vehicle can check 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 M_1 and M_2 to determine the validity of received regional message. Consequently, the combined data verification protocol overcomes weaknesses of both approaches and provides a better way for reliable data propagation with a high acceptance rate.

To further increase the chance of receiving and verifying regional messages, a recipient vehicle can also validate a received regional message if one of M_1 and M_2 message is matched with M_B. Since M_B is propagated via a different communication channel from M_1 and M_2, it is also hard and costly for malicious vehicles to modify the messages without being detected.

3.4 Comparison of the 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 summarise 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 computation. 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 is 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, a recipient will receive either only one regional message or unmatched two messages. In that case, 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 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 areas 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 depends on the moving speed of those delivery vehicles. It is in general much slower than the first approach.

The combined Scheme 3.3 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 (M_F, M_B, M_1, M_2), which could possibly increase the communication cost.

To reduce the communication cost, a vehicle could adaptively decide whether it uses the two-directional approach, or the time-based approach, or the combined approach based on the network condition such as vehicle density and vehicle moving speed. For example, if the density of smart vehicles is high such that the probability of having successful data propagation with two-directional approach is above a predefined threshold (as shown in our experiments in Section 5), a source vehicle could choose to use only two-directional approach to minimise the communication cost.

4 Security and robustness study

4.1 Adversary model

In this paper, we focus on malicious attackers who may conduct the following attacks.

- *Alteration attacks*: Upon receiving a regional message, malicious vehicles can modify the message and then forward the false message into the network.
- *Denial-of-Service (DoS) attacks*: Adversaries can drop received regional messages.
- *Bogus message insertion attacks*: Adversaries can generate and broadcast fake regional messages.

4.2 Data integrity

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

4.2.1 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:

- only one of the two roadways has malicious vehicles
- 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 Figure 1. Instead of forwarding M_B after receiving this message from vehicle 1, it can forge M_B to become the forged message, FM_B. Since FM_B is not identical to M_F, any destination vehicle (such as vehicle D) receiving a pair of (M_F, FM_B) will not accept the regional message based on the verification rule. Thus, this attack will not compromise data integrity in VANET communications. The DoS effect caused by this attack is discussed next in Section 4.3.

A malicious vehicle M could also carry out more active attacks such as inserting fake regional message about a road section. For such attacks, we can rely on neighbourhood cooperative detection (similar to approaches presented by Deng et al. (2006)). Suppose M creates a fake pair of messages (FM_F, FM_B) about a road section. There are two possible attack scenarios according to M's current location, which are illustrated in Figure 3.

1 If M tries to generate a fake regional message for a road section ahead of its current location (as shown in Figure 3(a)), the vehicles that directly receive messages from M, (vehicles 6 and 8 in this case), should be able to receive FM_F and FM_B. Based on their current location, vehicles 6 and 8 know that vehicle M is the source; however, vehicle M is not reporting traffic event about its current road section. Thus vehicles 6 and 8 will not forward the fake message.

2 If M generates a fake regional message for its true location (as shown in Figure 3(b)), among the neighbouring vehicles, any vehicle which is at the same road section (such as vehicle 1), or who will move into the road section a moment later (such as vehicle 2), will know that the regional message just received is not accurate based on their own observation of the road section i. Thus, they will not forward the messages, and/or they will immediately generate a warning message to alert others about this fake message attack.

Either way, a fake pair of messages will be either dropped or not 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 FM_F and FM_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.

4.2.2 *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:

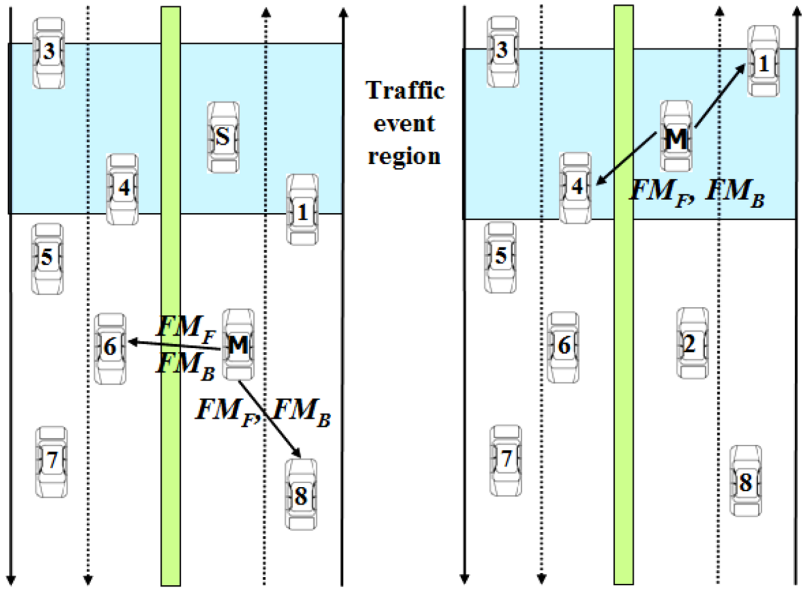
- each group includes a combination of honest and malicious vehicles
- both groups consist of only malicious vehicles.

In the first case, since the group of DV (defined in Section 3.2.1) contains honest vehicles, the original pair of regional message (M_1, M_2) 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 of the communication range of each other (via the time delay between a message pair), thus they can produce a successful attack only if they can generate a valid pair of fake messages by pre-defined rules. In addition, these two groups of malicious vehicles have to be apart from each other with a certain distance – not too short to pass a recipient in less than the predefined time delay, and not too long to make a recipient to discard the first received fake message after timeout.

It is clear that such an attack is possible, but it is hard to realise as well. In addition, for malicious vehicles

Figure 3 Two possible forge attacks by a malicious vehicle M sending fake regional message about a road section for some traffic events: (a) fake message for future-reached road section and (b) fake message for current road section (see online version for colours)



(a) (b)

that conduct this attack, such an attack can only cheat vehicles that are on the opposite direction of a roadway and for an event/accident that has happened at a location where the malicious vehicles have already passed – it is hard to see what significant benefit could these malicious vehicles gain through this attack. Therefore, with the high attack cost and no clear gain, such an attack is only theoretically possible without much real threat to a VANET.

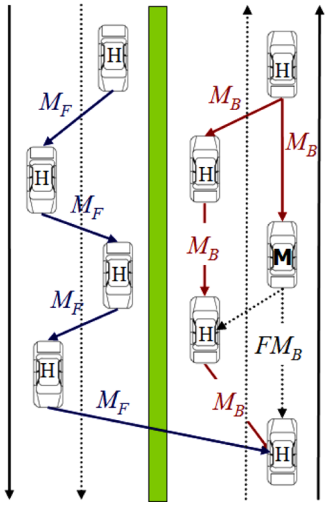
4.3 Denial-of-Service (DoS) attacks

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 DoS attacks, and how our approaches deal with these attacks.

4.3.1 Two-directional data propagation

Since we assume not so sparse traffic for this approach, it is highly possible to have honest vehicles as neighbours of a malicious vehicle. If there is at least a single honest neighbouring vehicle, the original message can be successfully forwarded by the honest vehicle as illustrated in Figure 4. According to the message propagation policy described in Section 3.1.1, the honest vehicle H will forward M_B since this message has not been forwarded before.

Figure 4 Data propagation with a single malicious vehicle M. The other vehicles labelled H are honest. M can create a forged message FM_B. If there are honest vehicles around M, the original message M_B can be successfully propagated by those honest vehicles (see online version for colours)



In the worst case scenario where the traffic is sparse and if a malicious vehicle drops the original data M_B, the data cannot be propagated at that moment since no honest vehicle is nearby. If the malicious vehicle creates a forged message FM_B, any recipient vehicle will get a pair of unmatched regional messages (M_F, FM_B) (see Figure 4). This is the scenario where a malicious vehicle could cause damage by a 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 send a similar regional message (denoted as M'_F and M'_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 M'_B. Even though the recipient vehicle receives two different messages (M_F, M'_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.

4.3.2 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 two delivery vehicle groups DV_1 and DV_2. If each delivery 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.

If a delivery group includes only malicious vehicles, the message carried by the group will be lost. Since 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 delivering the message successfully.

5 Simulation study

5.1 Simulation environment

We simulate traffic message propagation in a two-way road. The distance between the source vehicle and the recipient vehicle varies from 5 km to 30 km. Vehicles enter the road section by following a Poisson process. Vehicles moving speed, if not explicitly mentioned in each experiment, follows normal distribution with a mean speed μ of 100 km/hr and a standard deviation σ of 20/1.96. According to 'confidence interval' introduced in Ross (2006), choosing this σ value can make sure that 95% of simulated vehicle speeds are within 80 km/hr to 120 km/hr range. To simulate vehicles moving with constant speed change, a new moving speed is assigned to each vehicle in every 6 s. We keep track of the vehicle locations in every 300 ms.

The vehicle density varies from 4 vehicles/km to 52 vehicles/km in the simulation of the two-directional data propagation approach. Since time-based approach is mainly used for sparse networks, for this approach vehicle density varies from 0.5 vehicles/km to 20 vehicles/km. Three different wireless transmission ranges were simulated in most experiments: 250 m, 300 m and 350 m. The location of vehicles travelling in different lanes is ignored in our simulation. This is a reasonable assumption since the width of lanes (normally less than 4 m) is negligible compared to the radio transmission range. We conduct 1000 simulation runs for each set of simulation setting in order to obtain an accurate sample average values and smooth curves.

5.2 Two-directional propagation

5.2.1 Impact of vehicle density

The two-directional data propagation approach relies on the vehicles between a source and a destination for relay of the regional messages. The successful relay of messages can only be achieved when a fully-connected path exists between the source and the destination. This requires sufficient number of vehicles on the road. In this section, we first study how does the vehicle density affects the success rate of the two-directional approach.

We assume that the distance between a source vehicle and a destination vehicle is 10 km. The speed with which a vehicle enters the road section is an important parameter. Two separate sets of simulations are carried out to study the effects of vehicle speed. For the first set of simulations all vehicles are assumed to be travelling at the same constant speed. For the second set of simulations vehicle speeds are assumed to follow normal distribution as introduced in Section 5.1.

Figure 5(a) shows the probability of having a fully-connected path between a source and a destination 10 km apart with different vehicle densities for the first set of simulation (with the same constant speed). In order to have a fully-connected path with 90% probability, the required wireless transmission range is 300 m with a vehicle density of 24 vehicles/km.

Figure 5(b) compares simulation results under constant speed and under normal distribution speed for a radio range of 300 m. When vehicles are moving with normal distribution speeds, overall the probability of having a fully-connected path decreases compared to that of constant speeds. This is due to the larger inter-vehicle distances and also reduced effective vehicle density caused by various moving speeds. Since vehicles are moving with different speeds, compared with constant speed scenario, the variability of the distance between two neighbouring vehicles increases. This causes the network to have a large gap between two adjacent vehicles.

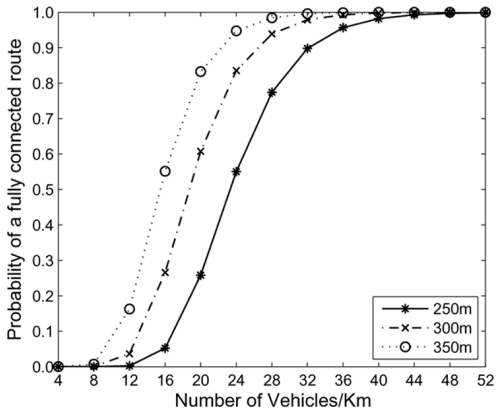
5.2.2 Carry-forward extension of two-directional approach

In Section 3.1.3, we have introduced an extension to the basic two-directional approach by using carry-forward paradigm. Here we study its performance based on simulations by considering two issues:

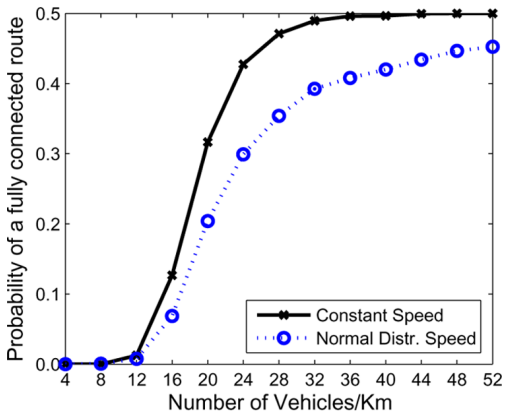
- the probability of successful data propagation
- the data propagation delay.

We simulate a road segment of 30 km. The other simulation parameters have been introduced in Section 5.1. From simulations we measure the average propagation delay for message M_F and M_B, respectively.

Figure 5 Probability of having a fully-connected route from a source to a destination (10 km apart) with different vehicle densities: (a) all vehicles are moving with the same speed under three different wireless transmission ranges (250 m, 300 m, and 350 m) and (b) comparison of the constant speed scenario and the normal distributed speed scenario for radio transmission range of 300 m (see online version for colours)



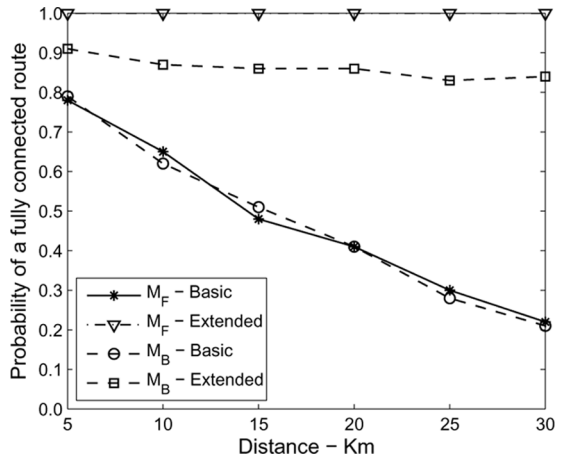
(a)



(b)

Figure 6 shows the probability of achieving a connected route for M_F and M_B for the extended two-directional approach, compared with the original basic approach (no carry-forward). For both M_F and M_B, a significant improvement is achieved by the extended approach. In addition, for the extended approach the probability of successful propagation is not affected by the message propagation distance. Therefore, the extended two-directional approach is especially suitable for long distance traffic data propagation.

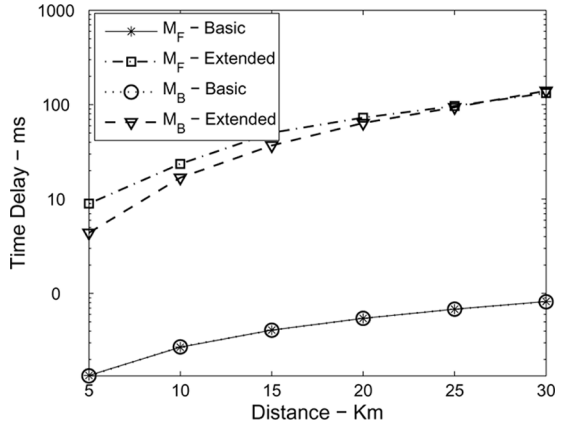
Figure 6 Success probability of message propagation for the basic two-directional data verification approach and the extended approach (introduced in Section 3.1.3 by using carry-forward method) for messages M_F and M_B



In case of M_F, we achieve 100% successful propagation probability. This is due to the fact that vehicles forwarding M_F are also moving in the direction of message propagation, and hence, will eventually deliver the message to the destination even if no connected path is available.

Figure 7 shows the propagation delays for messages M_F and M_B for the basic and extended two-directional approach, respectively. If in a simulation run the message propagation is not successful (as seen in Figure 6), there is no meaning of propagation delay so this simulation run is ignored when calculating the average propagation delay.

Figure 7 Propagation delay of messages for the basic and extended version of two-directional data verification approach. The propagation delays of M_F and M_B in the basic approach are almost the same; and hence, these two curves overlap with each other



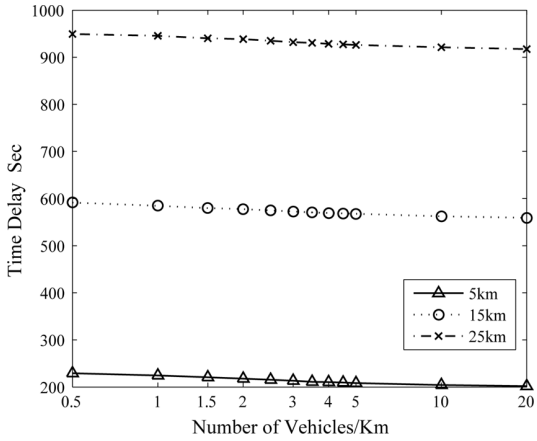
The improved probability of a fully-connected path by the extended approach comes with the cost of increase in message propagation delay; however, we believe that in most scenarios a large propagation delay is better than a message failure. A message failure can be considered as having an infinite propagation delay therefore a finite propagation delay is still better.

5.2.3 *Robustness against Denial-of-Service attacks*

We simulate a road section of 10 km with different vehicle densities. For each simulated network scenario where a fully-connected path exists, a malicious vehicle is picked at random and we check again whether a fully-connected path still exists by removing this malicious vehicle.

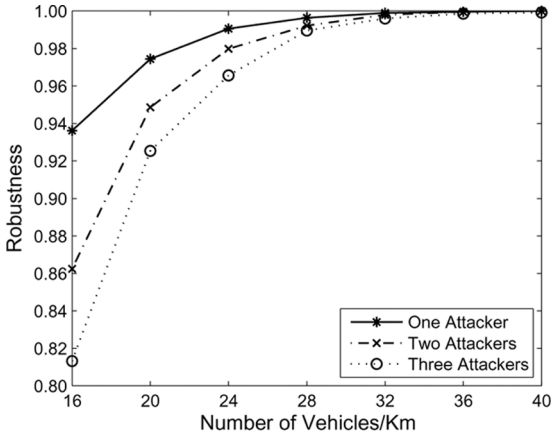
For a single-node DoS attack with different vehicle densities and radio ranges, Figure 8 shows the simulation results. It can be seen that for a radio range of 300 m we can achieve a robustness of 99% if the vehicle density $\geq$24 vehicles/km. Therefore, we can conclude that our two-directional approach is robust against DoS attack.

Figure 8 Robustness against a DoS attack launched by a single malicious vehicle for two different wireless transmission ranges



The simulation is further extended to study the robustness against DoS attacks by multiple non-collaborating malicious vehicles. Figure 9 shows the simulation results under the transmission range of 250 m. The robustness decreases with the increasing number of the malicious vehicles as expected.

Figure 9 Robustness against DoS attack by multiple non-collaborating malicious vehicles



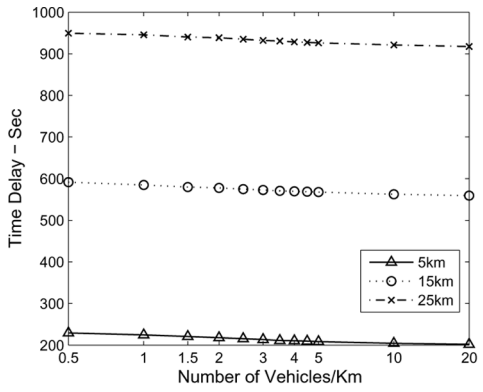
5.3 *Time-based data propagation*

In time-based data propagation, the message propagation delay is defined as the time interval between the time

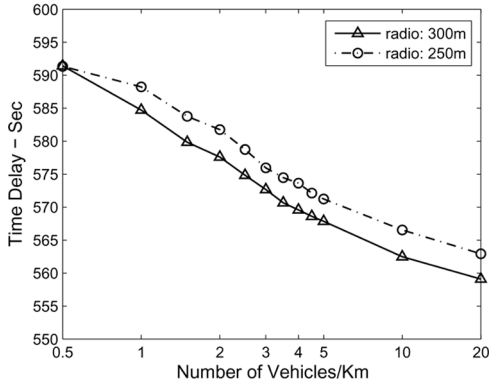
when a source vehicle has a regional message (M_1) to send and the time when both M_1 and M_2 messages reach the destination. In this approach, the propagation delay is essentially determined by the moving speed of the vehicles on the opposite driving direction. On the other hand, vehicle density also affects the propagation delay since the source vehicle can send its message only if there exist vehicles on the opposite driving direction within its transmission range.

In addition, if the source vehicle is unable to send the second M_2 message after a predefined maximum-threshold delay (due to non-availability of any delivery vehicle in the opposite direction), the source discards the M_2 message. This situation is defined as message delivery failure. In this paper, we study both the message propagation delay and the probability of message delivery failure.

Figure 10 Propagation delays for time-based approach under different vehicle densities: (a) 5 km, 15 km, and 25 km propagation distances with the radio transmission range of 300 m and (b) a closer look of the delay for 15 km propagation distance with transmission ranges of 250 m and 300 m



(a)

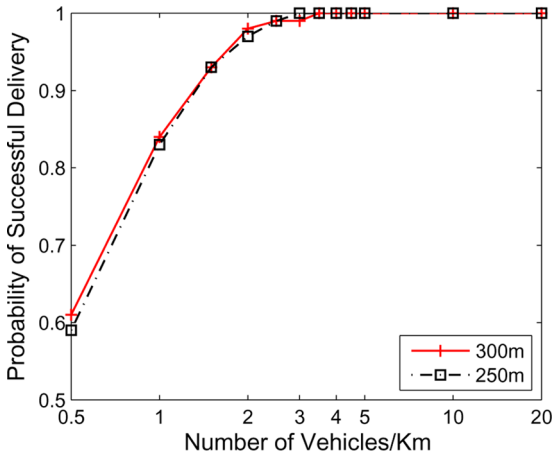


(b)

Figure 10(a) shows the propagation delays for different vehicle densities when the source is 5 km, 15 km, and 25 km away from the destination. It can be seen that the propagation delay is almost independent of vehicular densities and is mostly defined by the distance from the point of incident/origination of the message. Figure 10(b) gives the closer look at the propagation delays at a distance of 15 km with 250 m and 300 m radio transmission ranges, respectively. The results further confirm the earlier finding that vehicle density is not a very important factor in determining the propagation delay. A 40-times increase in vehicle density, i.e., from 0.5 vehicles/km to 20 vehicles/km, causes a reduction in propagation delay by only 30 s, or 5%.

Figure 11 shows the probability of successful transmission of the message to a destination under different vehicle densities. The results show that the vehicle density does affect the data propagation success probability. We can achieve a success probability of more than 90% with a vehicle density of 1.5 vehicles/km. On the other hand, in the two-directional data propagation approach, we require a vehicle density of around 28 vehicles/km to achieve a comparable success probability.

Figure 11 Probability of successful delivery of message at 15 km distance under different vehicle densities (see online version for colours)



6 Discussion

The central design objective of our proposed approaches is to provide *sufficient* security mechanisms which are realistic and economical to implement in the near future. The proposed approaches are not as perfect as attack-proof, rather they are designed to make any possible successful attacks difficult and costly for attackers to conduct.

6.1 Mobility

The time-based data verification approach relies on the mobility of vehicles on the opposite driving direction. Thus, if these vehicles are moving very slowly or do not move due to heavy congestion or traffic light, this approach may not work. In such a scenario, we can only rely on the two-directional approach for secure message propagation.

In the two-directional approach, if vehicles on both directions of a road are stopped (e.g., by a red light) or stuck in a heavy congestion, two malicious vehicles on both directions in the same region may be able to conduct

coordinated data modification attack for an extended period of time and cause substantial damage. However, we believe such an attack is unlikely to be successful. When the road is heavily congested, the density of vehicles becomes much higher. As shown in previous simulation studies in Section 5.2.3, the two-directional approach will have increased robustness when vehicle density becomes larger due to the fact that the original unchanged message has a higher probability to have a full communication path to reach a recipient vehicle.

6.2 Risk assessment

For both proposed approaches, if a recipient vehicle receives only one message instead of a pair of matched message, the recipient treats the message as unverified. This event could happen under the following scenarios:

- The single message received is not altered. The other message has been dropped due to broken wireless link or a malicious vehicle (for the two-directional approach), or due to lack of healthy vehicles passing by when the source sends out the other message (for the time-based approach). In this case, accepting the message has no security risk.
- The received message has been modified by malicious vehicles, and at the same time, the other message has been dropped due to the reasons discussed in the first scenario. In this case, the received message should not be accepted. However, such scenario has a low probability to occur since it requires two events to take place simultaneously.
- A malicious vehicle, either at the incident place or between the incident place and the recipient vehicle, generates only one message instead of a pair of matched message. We have already discussed how to deal with a malicious source in Section 4.2.

A recipient cannot tell under which scenario such an event has occurred. It can either discard or accept the message with certain security risk. The level of security risk is determined by the probabilities of each scenario occurrences. We plan to conduct further research to find additional mechanisms in determining when to accept or discard such a message.

6.3 Malicious source detection and alert message delivery

The two proposed approaches mainly focus on how to provide secure delivery of a generated regional message to other vehicles. We have discussed how to deal with fake regional messages generated by a malicious source in Section 4.2. Basically, we rely on a healthy vehicle near the source to discover the fake message (e.g., by determining that there is no congestion as reported by the fake message), and then immediately sending the alert message.

The alert message itself needs to use the proposed security delivery methods to prevent easy injection of fake alert messages by attackers. Therefore, attackers might generate fake alert messages to cause a DoS attack accordingly. There are still challenges on how to secure the alert message propagation. As our research in this paper focuses on secure message delivery approaches, we plan to continue our research efforts in the direction of how to provide effective and cost-efficient source verification.

6.4 Other extensions

There are still many challenges to tackle before we can deploy a practical and secure vehicular network. Our proposed approaches target two-way roads. We need to develop effective and economical mechanisms to provide secure message delivery for one-way roads, or for two-way roads where the two directions may split far apart in some regions (such as some highways).

In addition, our approaches solely rely on vehicle-to-vehicle communication. When roadside service units are gradually set up, vehicular communication should fully utilise these roadside units to provide efficient and secure communication. For example, roadside units can be used to provide message storing and forwarding when it is difficult to set up vehicle-to-vehicle communication (especially during the VANET initial deployment stage), or be utilised to provide better security services (Aslam et al., 2008). We plan to conduct further research in this direction as well.

7 Conclusion

In this paper, we proposed two novel data verification approaches: two-directional and time-based for reliable traffic information propagation on two-way traffic roads. The novel idea behind these approaches is to make two different groups of vehicles deliver the same regional traffic message independently. If both messages given from these two groups match, a recipient vehicle accepts the received regional message.

The underlying philosophy of our design is to provide sufficient, not necessarily perfect, security mechanisms which are simple and economical to implement in the real world. The proposed approaches are effective and reasonably secure not because they are attack-proof, but because it is difficult and costly for attackers to conduct successful attacks by modifying both copies of a regional message simultaneously. Compared with the previous VANET security themes that require the support of a complicated and expensive public key infrastructure, the proposed approaches are much simpler and easier to implement, especially during the initial transition stage when a mature VANET network infrastructure does not yet fully exist.

Acknowledgement

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

References

Aslam, B., Wang, P. and Zou, C.C. (2008) 'An economical, deployable and secure vehicular ad hoc network', *Proceedings of IEEE Military Communications Conference (MILCOM)*, November, San Diego, California , USA, pp.1–10.

Blum, J.J., Eskandarian, A. and Hoffman, L.J. (2004) 'Challenges of inter-vehicle ad hoc networks', *IEEE Transactions on Intelligent Transportation Systems*, Vol. 5, No. 4, December, pp.347–351.

Deng, H., Xu, R., Li, J., Zhang, F., Levy, R. and Lee, W. (2006) 'Agent-based cooperative anomaly detection for wireless ad hoc networks', *Proceedings of the 12th International Conference on Parallel and Distributed Systems (ICPADS)*, July, Minneapolis, Minnesota, USA, pp.613–620.

Dotzer, F. (2006) 'Privacy issues in vehicular ad hoc networks', *Lecture Notes in Computer Science*, Springer, Berlin, Heidelberg, Vol. 3856, pp.197–209.

Freudiger, J., Raya, M., Félegyházi, M., Papadimitratos, P. and Hubaux, J-P. (2007) 'Mix-zones for location privacy in vehicular networks', *ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS)*, August, Vancouver, British Columbia.

Golle, P., Greene, D. and Staddon, J. (2004) 'Detecting and correcting malicious data in vanets', *Proceedings of the 1st International Workshop on Vehicular Ad Hoc Networks (VANET)*, October, Philadelphia, PA, USA, pp.29–37.

Hubaux, J-P., Capkun, S. and Luo, J. (2004) 'The security and privacy of smart vehicles', *IEEE Security and Privacy Magazine*, Vol. 2, No. 3, May–June, pp.49–55.

Laberteaux, K.P., Hu, Y-C. and Haas, J.J. (2008) 'Security certificate revocation list distribution for VANET', *Proceedings of the 5th International Workshop on Vehicular Ad Hoc Networks (VANET)*, September, San Francisco, California, USA, pp.88–89.

Liu, J., Hong, X., Zheng, Q. and Tang, L. (2006) 'Privacy-preserving quick authentication in fast roaming networks', *Proceedings of 31st IEEE Conference on Local Computer Networks (LCN)*, November, Tampa, Florida, USA, pp.975–982.

Moore, T., Clulow, J., Raya, M., Papadimitratos, P., Anderson, R. and Hubaux, J-P. (2008) 'Fast exclusion of errant devices from vehicular networks', *Proceedings of the IEEE SECON*, June, San Francisco, California, USA, pp.135–143.

Papadimitratos, P., Gligor, V. and Hubaux, J-P. (2006a) 'Securing vehicular communications – assumptions, requirements, and principles', *Proceedings of the Workshop on Embedded Security in Cars (ESCAR)*, November, Berlin, Germany, pp.5–14.

Papadimitratos, P., Kung, A., Hubaux, J-P. and Kargl, F. (2006b) 'Privacy and identity management for vehicular communication systems: a position paper', *Proceedings of the Workshop on Standards for Privacy in User-Centric Identity Management*, July, Zurich, Switzerland.

Papadimitratos, P., Buttyan, L., Hubaux, J-P., Kargl, F., Kung, A. and Raya, M. (2007) 'Architecture for secure and private vehicular communications', *Proceedings of the 7th International Conference on ITS Telecommunications*, June, Sophia Antipolis, France, pp.1–6.

Papadimitratos, P., Mezzour, G. and Hubaux, J-P. (2008) 'Certificate revocation list distribution in vehicular communication systems', *Proceedings of the 5th International Workshop on Vehicular Ad Hoc Networks (VANET)*, September, San Francisco, California, USA, pp.86, 87.

Parno, B. and Perrig, A. (2005) 'Challenges in securing vehicular networks', *Proceedings of the Workshop on Hot Topics in Networks (HotNets-IV)*, November, College Park, Maryland, USA.

Picconi, F., Ravi, N., Gruteser, M. and Iftode, L. (2006) 'Probabilistic validation of aggregated data in vehicular ad-hoc networks', *Proceedings of the 3rd International Workshop on Vehicular Ad Hoc Networks (VANET)*, September, Los Angeles, California, USA, pp.76–85.

Plobl, K., Nowey, T. and Mletzko, C. (2006) 'Towards a security architecture for vehicular ad hoc networks', *Proceedings of the 1st International Conference on Availability, Reliability and Security (ARES)*, April, Vienna, Austria, pp.374–381.

Rahman, S.U. and Hengartner, U. (2007) 'Secure crash reporting in vehicular ad hoc networks', *Proceedings of the 3rd International Conference on Securing and Privacy in Communication Networks (SecureComm)*, September, Nice, France, pp.443–452.

Raya, M. and Hubaux, J. (2005) 'The security of vehicular ad hoc networks', *Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN)*, November, Alexandria, VA, USA, pp.11–21.

Raya, M., Aziz, A. and Hubaux, J. (2006a) 'Efficient secure aggregation in vanets', *Proceedings of the 3rd International Workshop on Vehicular Ad Hoc Networks (VANET)*, September, Los Angeles, California, USA, pp.67–75.

Raya, M., Papadimitratos, P. and Hubaux, J-P. (2006b) 'Securing vehicular communications', *IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications*, Vol. 13, No. 5, May, pp.8–15.

Raya, M., Papadimitratos, P., Aad, I., Jungels, D. and Hubaux, J-P. (2007) 'Eviction of misbehaving and faulty nodes in vehicular networks', *IEEE Journal on Selected Areas in Communications, Special Issue on Vehicular Networks*, Vol. 25, No. 8, pp.1557–1568.

Raya, M., Papadimitratos, P., Gligor, V.D. and Hubaux, J-P. (2008) 'On data-centric trust establishment in ephemeral ad hoc networks', *Proceedings of IEEE Conference on Computer Communications (INFOCOM)*, April, Phoenix, AZ, USA, pp.1238–1246.

Ross, S.M. (2006) *Simulation*, 4th ed., Amsterdam, Elsevier/Academic Press.

Studer, A., Luk, M. and Perrig, A. (2007) 'Efficient mechanisms to provide convoy member and vehicle sequence authentication in vanets', *Proceedings of the 3rd International Conference on Security and Privacy in Communication Networks (SecureComm)*, September, Nice, France, pp.422–432.

Sun, Q. and Garcia-Molina, H. (2004) *Using Ad-Hoc Inter-Vehicle Networks for Regional Alerts*, Technical Report, Stanford University, Stanford, California, USA.

Yousefi, S., Mousavi, M.S. and Fathy, M. (2006) 'Vehicular ad hoc networks (vanets): challenges and perspectives', *Proceedings of the 6th International Conference on ITS Telecommunications*, June, Chengdu, China, pp.761–766.

Wischhof, L., Ebner, A., Rohling, H., Lott, M. and Halfmann, R. (2003) 'SOTIS – a self-organizing traffic information system', *Proceedings of the 57th IEEE Vehicular Technology Conference (VTC)*, April, Jeju, South Korea, pp.2442–2446.

Zhao, J. and Cao, G. (2008) 'VADD: vehicle-assisted data delivery in vehicular ad hoc networks', *IEEE Transactions on Vehicular Technology*, Vol. 57, No. 3, May, pp.1910–1922.

Note

[1]Of course, many cities have one-way roads around their downtown areas. Such a VANET environment has very distinct features such as high density of vehicles and low vehicular mobility. For such an environment we should rely on other security protocols to provide secure data propagation service.