Reliable Traffic Information Propagation in Vehicular Ad-Hoc Networks

Soyoung Park and Cliff C. Zou
University of Central Florida
4000 Central Florida Blvd Orlando FL 32816-2362

***Abstract*-In a Vehicular Ad-Hoc Network (VANET), an important application is to let moving vehicles collaborate with each other by sharing traffic information and alerting others of any emergency or accidental scenarios. To make this application possible, a security mechanism must be designed in the beginning to guarantee that no malicious vehicles or persons can intercept, manipulate, or modify traffic information propagating in a VANET without being detected. In this paper, we present a novel approach to provide reliable traffic information propagation in a VANET: *two-directional data verification*.**

Two-directional data verification approach uses vehicles in both directions of a two-way road as two separated media channels to propagate traffic data. By receiving messages from 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 for an adversary to have two collaborative vehicles on both driving directions in the same region. Even if an adversary can do this, it is costly and attacks can be done only in a short time period. The proposed approach is simple and readily to be implemented, requiring no complicated public-key infrastructure to protect traffic information propagation in VANET.

I. INTRODUCTION

A. *Background and Related Work*

With a significant development of network technologies, vehicular ad-hoc network (VANET) has been emerging as a killing application in a ubiquitous environment. In the VANET environment, vehicles can sense and create their own traffic information then they communicate with each other to collect their local traffic information. Since the traffic messages can be delivered to vehicles faster and further, drivers can react and prepare against sudden traffic events in advance. Finally, vehicles can drive collaboratively to speed up the flow of traffic. The existing traffic broadcasting systems, such as traffic radio, can give traffic information periodically for some specific locations and directions. However drivers only need to know the newest detail information related to their future driving route, which cannot be provided by current broadcasting systems.

Researchers have conducted many researches about self-organizing traffic information system (SOTIS) [1], security and privacy issues [2-7], fast authentication [8-10], secure data aggregation [11-12], and detecting and correcting malicious data [12-13] in VANET. Among these security challenges, we especially concern about reliable traffic information propagating through multiple vehicles over a relatively long distance. Unlike typical traffic messages of each vehicle such as moving direction, location, speed and temporary brake which are useful for neighboring vehicles, aggregated traffic messages obtained in a certain road section such as average speed, density, events like traffic hazard, accident and jam which can affect to the following vehicles for a long time should be delivered to vehicles in a relatively long distance. We name such an aggregated traffic message as "regional message" in this paper.

We focus on the security of the long-existing regional traffic messages. Because those 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 increase. And if the original regional messages have been altered in the propagation, following vehicles should be able to detect the modification and they should not accept those messages.

We define that a given regional message is correct if the message is identical to the original regional message. And we define that the propagation is reliable and secure if any recipient vehicles can receive and detect the correct regional messages. This paper provides an easy way for vehicle-assisted reliable traffic data propagation without any additional road side infrastructure and special technologies. We will 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.

A few of researches about regional alerts delivery [14], crash reporting [15] and vehicle-assisted data delivery [16] in VANET have been suggested. Sun and Garcia-Molina [14] have 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, it does not consider the security of the data propagation. Zhao and Cao [16] have suggested an improved way for fast message routing in more complex roads using information about destination location, vehicle's location and moving direction. Rahman and Hengartner [15] have introduced the concept of cryptographically-verifiable road-worthiness certificates for secure crash reporting. That covers the security problems which can happen in the data propagation. However, it needs to operate additional governmental authorities and road-side access points to manage the certificates.

B. *Contribution*

We provide a new approach for reliable regional traffic data

propagation: *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 vehicle on the propagation path wants to accept the regional message instead of just 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 in the data propagation path.

In order for an attacker to alter a propagating regional message without being detected, the attacker needs two cooperative vehicles on both driving directions between the source of the regional message and the recipient vehicle. Such an attack condition is very hard to be satisfied 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 very short time period when these two vehicles meet or are in a closed range. This is the reason why our proposed simple security approach works.

The biggest advantage of our scheme is that it is simple to setup for reliable data transmission without any additional road-side infrastructure or dedicated public-key infrastructure for VANET. We do not need to use certificates and its related operations as well. Our approach exploits the unique features of bidirectional roadway and fast moving vehicles to protect traffic information propagation in VANET.

We illustrate our VANET model and security issues in section II, and give detail descriptions for our approach in section III. Then we analyze the security in section IV and show some simulated results in section V. In section VI and VII, we discuss about our scheme and then conclude our paper and present future work.

II. VANET MODEL

A. Network Model

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

a. Roads: We basically consider two-way traffic roads which are not too sparse. A bidirectional roadway is logically divided into road sections and each road section has its unique ID number.

b. Car: Each car is equipped with sensors, GPS, a preloaded digital map which has the road segments information, networking device, and computing device which stores private/public key pairs and creates messages and digital signatures. It also has its local traffic analyzer to keep and analyze the regional messages. It senses its own traffic events and communicates with its neighboring vehicles by broadcasting its traffic messages periodically. Also, it forwards the propagated messages to other vehicles.

c. Traffic messages: Traffic messages can be classified into typical messages and regional messages. Typical messages contain 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][12]. These messages are broadcasted in a single data transmission range and not propagated any further.

Regional messages contain its corresponding road section, direction, average speed, density, 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.

B. Attack model

We hypothesize that the majority of vehicles are honest. However, a few malicious attackers can cause damage to the entire VANET. We first show various types of adversaries considered in VANET and describe their possible attacks.

◆ Adversaries and Attacks

In this paper, we mainly concern about malicious attackers who can make the following attacks.

- Denial of service attacks (Message suppressing attacks): Adversaries can intercept and drop packets from the network.
- Fabrication and alteration attacks: Malicious drivers 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.

Notice that we focus on the security for the regional message's propagation. So, the malicious attackers are supposed to make the described attacks in the middle of propagation of the regional messages. In this paper 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 done via some other security mechanisms and it is out of the scope of this paper. If a source vehicle created a wrong regional message, the message will be forwarded to other vehicles as it is. However, since the majority of vehicles are honest, upcoming honest sources can create correct regional-messages for the same road section. Then most of recipient vehicles can accept the correct regional messages through the consistency verification about those regional messages. So we believe our approach can work out even without source authentication mechanism.

◆ Security Requirements

Our goal is to provide a security mechanism against the above adversarial attacks in term of "Data integrity"—Data cannot be modified in transmission; If it was modified, receiver can detect the modification.

III. TWO-DIRECTIONAL DATA VERIFICATION

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 groups. A noticeable advantage in VANET is that every vehicle's trajectory follows the existing roadways. So, it is easy to set a group of vehicles by the geographical road

information. Any roadway can be logically divided into lots of small sections with a certain distance. 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* (see Fig. 1). Every vehicle can easily recognize what road section it is passing through since it has GPS and a digital map which has the road section information.

Vehicles are logically formed into groups based on their road sections that they currently belong to. Unlike the traditional group selection that is based on distance radius regardless of driving direction, in our approach, only vehicles with the same moving direction in each road section are set as a group [12]. Since vehicles need traffic information happened on their moving roadway, vehicles do not need to form a group with vehicles of their opposite moving direction to obtain information occurred on their moving roadway.

A group of vehicles in a single road section collaborate with each other to create a regional message about the road section. The created regional message will be only propagated to cars behind of the road section on the same roadway, since only those vehicles need this message. If a vehicle leaves a road section and gets into a new road section, it becomes a new group member of the new road section automatically.

A. Neighbor Detection

Since our approach regards two-way traffic lanes as two different network channels, vehicles in each directional roadway should forward their selected regional messages which have to be propagated along that roadway. Thus we need a mechanism to prevent a malicious vehicle in a different roadway from inserting a wrong regional message by pretending to drive on its opposite roadway. For this purpose, we allow each vehicle to recognize its neighboring vehicles that drive along the same roadway. Since we assumed that each vehicle broadcasts its typical message periodically, each vehicle can easily construct its neighbor list if the vehicle receives similar typical messages with the same public key from other vehicles more than once. Studer el al. [17] gives more specific ways to find out each vehicle's neighbor group and thus we will not further discuss this issue here.

B. Data Aggregation

In order to aggregate the traffic messages for each road section, we need to elect a source which is treated as a group header of the road section. The source can be elected in a similar way of electing a group leader presented in [11]. The difference is that, in our approach, the closest vehicle to a new road section is selected as a source (or group header). 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. Once a source is elected, the source collects its neighboring vehicles' periodic typical messages by passing through the road section and then creates an aggregated regional message. Any incident events such as sudden brake which can affect just neighboring vehicles for a short time, or abnormal data which are not consistent with other data are ignored in the aggregation.

Since group formation and data aggregation are not our main concern in this paper, we do not consider security vulnerabilities which can happen 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 VANET can be easily applied to deal with such security problems [12][13].

C. Data Propagation

Now we explain our data propagation algorithm. Once a source aggregates a regional message about a road section, vehicles who take charge of delivering the data in both directions forward it. We define several sets of vehicles related to the data propagation. Fig. 1 shows the locations of these vehicles in terms of a source. Let individual vehicle be *V*.

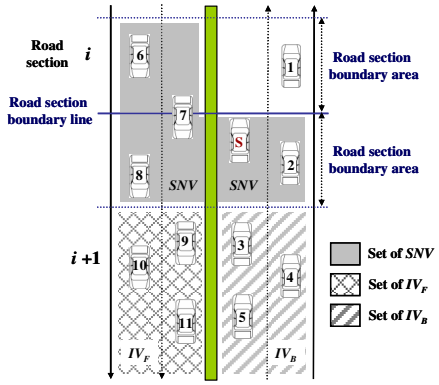

Figure 1. Sets of vehicles on a bidirectional roadway. Each directional roadway has 2 traffic lanes. Vertical arrows represent traffic directions. Horizontal solid line is the road section boundary line between road section *i* and *i*+1. Horizontal dotted line shows the road section boundary area.

- *NV* (Neighbor Vehicle): For a certain vehicle *V*, a set of vehicles which are moving toward the same direction of *V* and in a single data transmission range of *V*. For an example, vehicle 3 and 5 are neighboring vehicles of vehicle 4 in Fig. 1.
- *SNV* (Source's Neighbor Vehicle): A set of vehicles that are in the boundary area of a road section and in a single transmission range of the source excluding vehicles in front of the source at the same driving direction of the source. In Fig.1, vehicle 2, 6, 7 and 8 are *SNV*s of the source *S*.
- *IV* (Intermediate Vehicle): A set of vehicles that is 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 that move toward the same direction of the source and are in backward *Z* distance of the particular road section. *Z* means a propagation range. Vehicle 3, 4 and 5 belong to IV_B in Fig. 1.
  - IV_F: Vehicles that move toward the opposite direction of the source and in forward *Z* distance of the particular road section. Vehicle 9, 10 and 11

belong to IV_F in Fig. 1.

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:

$RI_{PD} = <M, Sig, K^+_S>$

$= <"RID \| PD \| MD \| Value \| SLoc \| TS\text{"}, SIG(K^-_S, M), K^+_S>$, where $PD = \{F, B\}$

RID is an identifier of the road section, *PD* is the propagation direction of the message. If $PD = F$, only vehicles in IV_F forward the message—vehicles in IV_B simply ignore 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 information and *TS* indicates the current time stamp. $SIG(K^-, M)$ represents a digital signature on a message *M* based on the private key K^-. And $< K^-_S, K^+_S >$ denotes a private and public key pair of the source.

2. The source broadcasts these two regional messages.
3. Among vehicles that received both messages from the source, only vehicles in *SNV* rebroadcast both messages.
4. Any vehicle IV_i in *IV* that received the messages from vehicles in *SNV* or vehicles in *IV* chooses its message according to *PD* and forwards it as follows:
   - ① If an intermediate vehicle $IV_i \in IV$ already broadcasted the same RI_F or RI_B before, then IV_i discards the given message.
   - ② Else if $IV_i \in IV_F$ then IV_i broadcasts RI_F given from IV_i's neighboring vehicles.
   - ③ Else if $IV_i \in IV_B$ then IV_i broadcasts RI_B given from IV_i's neighboring vehicles.

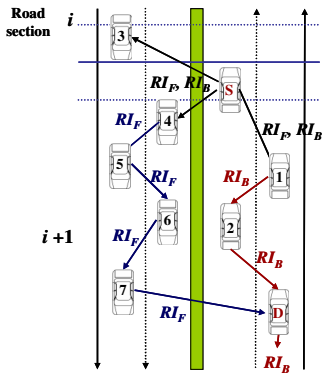

Figure 2. Two-directional data propagation on a bidirectional roadway. S represents a source vehicle and D represents an arbitrary recipient vehicle. D can receive RI_B and RI_F from vehicle 2 and vehicle 7 respectively. D checks if these two messages are matched. D also propagates RI_B for vehicles behind it.

Fig. 2 shows the propagation of the regional messages. Before the source *S* (driving upwards) leaves out the road section *i*+1, *S* first broadcasts RI_F and RI_B about the road section *i*+1. Then vehicles numbered 4, 5, 6 and 7 propagate RI_F and vehicles numbered 1 and 2 propagate RI_B. Finally a destination vehicle *D* receives both RI_F and RI_B from vehicle 7 and vehicle 2 respectively. Of course vehicle 1 and vehicle 2 can receive RI_F from vehicle 4, 5 or 6 as well, even though it is not presented in the figure.

Notice that the source does not specify the destination (or recipient) vehicle in advance but can specify the propagation range of its regional message. Any vehicles in IV_B can be the destination of the source's regional message if the vehicle wants to read it. The destination vehicle will also forward the given RI_B to downstream as long as it belongs to the propagation range.

D. *Data Verification Rule*

After every recipient vehicle *D* receives both RI_F and RI_B, *D* verifies the integrity of the regional message based on the following conditions**:**

- If RI_F equals to RI_B, then *D* accepts the regional message.
- If RI_F does not equal to RI_B, then *D* discards the regional message.
- If *D* gets just one of them, *D* sets the regional message suspect and keeps it.

Therefore, each vehicle only accepts a given regional message if and only if the vehicle receives the same regional message (in the forms of RI_F and RI_B) from both driving directions. Our approach relies on the facts that the probability that arbitrary two cooperative malicious vehicles exist in the same road section but in different directions (move toward each other's opposite direction) is very low. If such two cooperative malicious vehicles exist, they can only cooperate to disrupt data propagation security with a very short time period when they meet each other or in closed range. The two-directional data propagation approach, without any certificate authority [15] or other complicated security protocol, provides a simple but effective way for reliable traffic data propagation.

IV. Security and Robustness

Data integrity: Verification of data integrity is our major task. We show that our scheme can work out well against various malicious attacks. A malicious node cannot forge or modify the given data by pretending that the message is generated by the honest source because the malicious node cannot create the valid digital signature on behalf of the honest source without knowing the source's private key.

If a malicious node tries to forge a message with its own signature, the forged message would be different from the original message. Since RI_F and RI_B are different, a destination vehicle will not accept the forged message based on the verification rule.

Any intermediate malicious vehicle cannot insert wrong regional messages about the original road section. Suppose that a malicious vehicle moves in the source's driving direction and inserts a fake pair of messages $<FRI_F, FRI_B>$. We assumed that any intermediate vehicles will forward a regional message given from their neighboring vehicles in the same moving direction. A following intermediate vehicle *B* in IV_B will forward FRI_B because *B* can have the malicious vehicle on its neighboring list. But an honest intermediate vehicle *F* in IV_F, which received FRI_F from the malicious vehicle, will not forward FRI_F any longer because the message is not given from *F*'s neighboring vehicles. Since the

malicious vehicle is driving in the opposite direction of F, F does not contain the malicious vehicle on its neighboring vehicle list. If the malicious vehicle is driving in the opposite moving direction of the source, an honest intermediate vehicle B in IV_B will stop forwarding FRI_B with the same reason.

Denial of Service: A malicious vehicle can intercept, modify or drop data from their transmission. Since we assumed not too sparse traffic situation, it is possible that honest vehicles are neighboring around a malicious vehicle. If there could be at least a single honest neighboring vehicle around the malicious vehicle, then the original message can be successfully forwarded by the honest vehicle as shown in Fig. 3. According to the message propagation policy described in Section III.C, the honest vehicle H will forward RI_B since this message has not been forwarded before.

Considering the worst scenario where the traffic situation is mostly sparse so vehicles are separated from each other by the maximum data transmission range, if a malicious vehicle dropped the original data RI_B, the data cannot be propagated any longer at that moment. If a malicious vehicle modified or created a forged message FRI_B, any recipient vehicle will get a pair of unmatched regional messages $<RI_F, FRI_B>$ (see Fig. 3). If the recipient vehicle cannot determine which message (RI_F or FRI_B) is forged, it fails to receive and react according to the real message. This is the scenario where a malicious vehicle could cause damage by Denial of Service (DoS) attack.

However, a moment after the above DoS attack event, it is possible that another source car at the same road section will generate a similar regional message and send it out (denoted as RI'_F and RI'_B). At this time, due to vehicles different moving speed, there could be honest cars appearing around the malicious car to form a new route to pass the new message RI'_B. For the recipient vehicle, even though it receives two different messages (RI_F, RI'_B) sent by two sources, as long as the content of these two messages are consistent, the recipient will accept the content. Therefore, our security design is possible to be attacked by a Denial-of-Service attack, but the attack impact is limited.

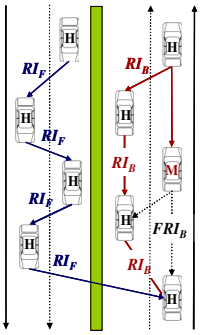

Figure 3. Data propagation with a single malicious vehicle *M*. The other vehicles labeled *H* are honest. *M* can create a forged message FRI_B. If there are honest vehicles around *M*, the original message RI_B can keep being propagated by those honest vehicles.

V. Evaluation

We evaluated the performance of our proposed scheme using NS-2. We assume that data single transmission range is 300m and vehicles are moving with an average speed of 110km/h. In order to set up the simulation scenario where vehicles are sparsely distributed, vehicles are supposed to be evenly on the road with a density of 3.4 vehicles per 1 km.

Fig. 4 shows the time delay between two regional messages RI_F and RI_B in the two-directional data propagation scheme. There is at least 11ms of time delay between the firstly arrived message and the secondly arrived message. According to the network situation, some following vehicles get RI_B first while some others get RI_F first. And the time delay slightly increases as the distance of a vehicle from the target road section goes further.

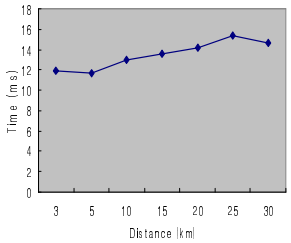

Figure 4. Time delay between RI_F and RI_B

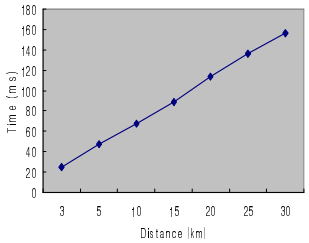

Figure 5. Propagation delay of regional messages

Fig. 5 shows the propagation delay taken to receive both regional messages. It takes about 25ms for both regional messages to arrive at vehicles in the range of 5km from the target road section while it takes about 156ms for those messages to arrive at vehicles at the range of 30km from the target road section. Even though it increases proportionally to the distance, the propagation delay is negligible compared with the time delay for recipient vehicles to reach the target road section. We also conducted experiments where vehicles have a speed of 80km/h, the result was almost the same with a little time difference of tens of nanoseconds. Since the data transmission time is so fast, delays were hardly affected by vehicles' moving speeds.

Lastly, we evaluated the minimal density of vehicles to guarantee a full connection among vehicles without any data fragmentation in the middle of data propagation. To achieve this, every two neighboring vehicles in the propagation range should be located in the data transmission range. We assumed that vehicles propagate the regional message just once, and that vehicles are randomly distributed in an interval of 10 km for this simulation. The number of vehicles is increased from 40 to 520 to give diverse densities. For each density scenario of vehicles, the simulation is performed 100 times to generate various traffic situations. For each simulation run, we checked if the full connection among the entire propagation range occurred. In other words, the full connection happened if the data propagation is successfully completed over the set of vehicles without any fragmentation during the propagation. Then we counted the total number of the full connections among 100 runs for each density scenario of vehicles.

Fig. 6 shows the number of full connections according to density and data transmission range. We simulated it for three data transmission ranges of 250m, 300m and 350m. The figure shows that at least 200 vehicles per 10km for 350m

transmission range, 240 vehicles for 300m transmission range and 280 vehicles for 250m transmission range are required in order to achieve more than 80% of full connections, under the assumption of a single broadcasting. Thus, in a sparse traffic situation, we should allow vehicles to re-broadcast the same regional message a few times to prevent data fragmentation.

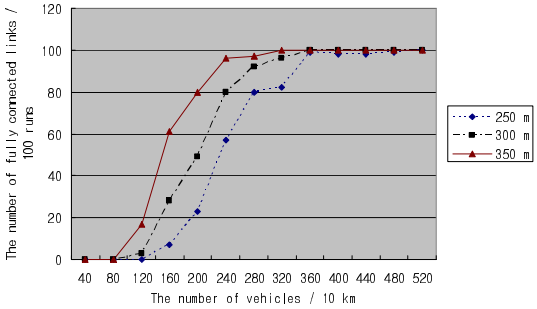

Figure 6. The number of fully connected links among 100 simulation runs according to density and data transmission range

VI. DISCUSSION

Two-directional data verification is simple and easy to verify the correctness of regional messages. However it has a weakness that every recipient vehicle should receive the same regional message twice, each from one direction. If one of RI_F and RI_B is modified during the propagation, a recipient vehicle will discard both regional messages even though one of them could be correct—the recipient vehicle cannot distinguish the correct regional message from the given two messages. If a single correct message is given to a recipient vehicle and the other message is dropped during the transmission, the recipient vehicle can accept the message but with low confidence: the message drop might be caused by wireless transmission problem, not by attackers, and at the same time, the received message might have been forged.

Therefore, we need an additional mechanism to detect a trustable message from the given messages in the above mentioned situations. If a recipient vehicle can know what traffic road is safe, in other words, what traffic road has no malicious attacker, the recipient vehicle can accept the regional message delivered through the safe roadway. An intuitive way to figure out this problem is to use neighboring vehicles. Neighboring vehicles of a malicious vehicle can easily detect the fact that the malicious vehicle modified or forged the original message. Then the neighboring vehicles can send out a malicious-vehicle-detecting message. However, it has still problems such as the malicious vehicle can create a false malicious-vehicle-detecting message for an honest vehicle. So we need further studies to improve the security of our approach against this scenario.

VII. CONCLUSION

We proposed a two-directional data propagation and verification protocol for reliable long-existing traffic information propagation in a two-way traffic road situation. The two-way traffic roads were regarded as two different network channels so a source's original regional message was propagated along two separate roadways. Thus, every recipient vehicle could easily verify if the given regional traffic data are correct by checking if two types of regional messages given from two different roadways are the same or not. The security is based on the fact that arbitrary two malicious vehicles on the two roadways respectively can hardly collaborate with each other to modify or forge the original regional message at the same time. We evaluated the performances about the time delay between two regional messages and the propagation delay of those messages, and it showed that our scheme is a practical security mechanism.

ACKNOWLEDGEMENT

This research was supported by NSF Grant CNS-0627318 and Intel research funds.

REFERENCES

[1] L. Wischhof, A. Ebner, H. Rohling, M. Lott and R. Halfmann, "SOTIS – A Self-Organizing Traffic Information System," Proc. of 57th IEEE Vehicular Technology Conference (VTC'03), 2003.
[2] M. Raya and J. Hubaux, "The security of vehicular ad hoc networks," Proc. of SASN '05, 2005.
[3] P. Papadimitratos, V. Gligor, and J.-P. Hubaux. "Securing Vehicular Communications - Assumptions, Requirements, and Principles." In proceedings of the Workshop on Embedded Security in Cars (ESCAR'06), 2006.
[4] J. Hubaux, S. Čapkun and J. Luo, "The Security and Privacy of Smart Vehicles," Magazine of IEEE Security & Privacy, May/June 2004.
[5] K. Plößl, T. Nowey and C. Mletzko, "Towards a Security Architecture for Vehicular Ad Hoc Networks," Proc. of the First International Conference on Availability, Reliability and Security (ARES'06), 2006.
[6] P. Papadimitratos, A. Kung, J. Hubaux, F. Kargl, "Privacy and Identity Management for Vehicular Communication Systems: A Position Paper," Proc. of Workshop on Standards for Privacy in User-Centric Identity Management, 2006.
[7] F. Dötzet, "Privacy Issues in Vehicular Ad Hoc Networks," Proc. of PET, 2005.
[8] J. Liu, X. Hong, Q. Zheng and L. Tang, "Privacy-Preserving Quick Authentication in Fast Roaming Networks," Proc. of the 31st IEEE conference on Local Computer Networks, pp. 975-982, 2006
[9] B. Parno and A. Perrig, "Challenges in Securing Vehicular Networks," Proc. of Workshop on Hot Topics in Networks (HotNets-IV), 2005
[10] L. Gollan and C. Meinel, "Digital Signatures for Automobiles," Proc. of Systemics, Cybernetics and Informatics (SCI), 2002.
[11] F. Picconi, N. Ravi, M. Gruteser and L. Iftode, "Probabilistic Validation of Aggregated Data in Vehicular Ad-hoc Networks," Proc. of VANET'06, 2006.
[12] M. Raya, A. Aziz and J. Hubaux, "Efficient Secure Aggregation in VANETs," Proc. of the 3rd International Workshop on Vehicular Ad Hoc Networks (VANET'06), 2006
[13] P.Golle, D. Greene and J. Staddon, "Detecting and Correcting Malicious Data in VANETs," Proc. of VANET'04, pp. 29 – 37, 2004.
[14] Q. Sun and H. Garcia-Molina, "Using Ad-hoc Inter-vehicle Networks for Regional Alerts," Technical Report, Stanford University, 2004.
[15] S. U. Rahman and U. Hengartner, "Secure Crash Reporting in Vehicular Ad hoc Networks," Proc. of the 3rd International Conference on Securing and Privacy in Communication Networks (SecureComm'2007), 2007.
[16] J. Zhao and G. Cao, "VADD: Vehicle-Assisted Data Delivery in Vehicular Ad Hoc Netowkrs," Proc. of InfoCom, 2006.
[17] A. Studer, M. Luk and A. Perrig, "Efficient mechanisms to provide convoy member and vehicle sequence authentication in VANETs," Proc. of the 3rd International conference on security and privacy in communication networks (SecureComm '07), 2007.