On Secure, Privacy-aware, and Efficient Beacon Broadcasting among One-hop Neighbors in Vehicular Adhoc Networks

Rasheed Hussain*, Zeinab Rezaeifar*, Donghyun Kim†, Alade O. Tokuta†, and Heekuck Oh*
* Department of Computer Science and Engineering, Hanyang University, ERICA Campus, South Korea
E-mail: {rasheed, hkoh}@hanyang.ac.kr
† Department of Mathematics and Physics, North Carolina Central University, Durham, NC 27707, USA
E-mail: {donghyun.kim, atokuta}@nccu.edu

***Abstract*—Many Vehicular Ad Hoc NETwork (VANET) applications achieve a decent packet delivery ratio using mobility information in the beacon messages broadcasted to the single-hop neighbors. Recently it has been found that if two VANET nodes are not within a line of sight (LoS), the performance of the employed VANET applications can be significantly degraded. Most of the existing VANET researches assume the ideal effective transmission range which does not consider Non-LoS (NLoS) scenario. To fill this gap, this paper provides a new mechanism: (a) to keep the track of the LoS status of individual vehicles on the road (b) to make sure that even in case of NLoS, vehicles maintain their communication with neighbors, and (c) to preserve the location confidentiality and privacy of the users conditionally at all times during communication. We propose a beacons-assisted plausibility-based technique to figure out NLoS status and a cooperative mechanism to guarantee a smooth communication between vehicles in case of NLoS. In case of NLoS, the affected vehicles raise alarms through their beacons and the neighbors with clear LoS to the target vehicles provide the affected vehicle with desired information. Moreover we maintain privacy-aware neighbor lists and location-based encryption for the aforementioned purpose and take the security of privacy of the whole system into account.**

Keywords*—VANET, Nonline-of-sight, Cooperative comm., Effective transmission range, beacons.

I. Introduction

It is believed that Vehicular Ad Hoc NETwork (VANET) will enable a number of emerging applications to make our daily driving safer and more comfortable [1]–[3]. In most cases, those applications rely on a frequent, continuous, and somehow un-interrupted mobility information of the neighbors in the beacon messages [4]. By exchanging the beacons among neighboring vehicles in a timely manner, VANET applications can guarantee the promised quality of service (QoS). Unfortunately, recent experiments conducted on real moving vehicles revealed that, due to obstructed or complete Nonline-of-Sight (NLoS), the effective transmission range can get deteriorated and reduced even up to 10 m [5]. This implies that the connectivity between two neighboring VANET nodes can be compromised by some obstacles such as unresponsive cargo trucks intermittently even though the nodes are geographically close with each other. Surprisingly, this challenging problem is not well-understood yet. To the best of our knowledge, Abumansoor et al. [6] is the only work concerning this issue. However, their strategy is based on an uncontrolled broadcasting and thus suffers from various efficiency and privacy issues. This paper attempts to fill this gap by introducing a new mechanism which can address the NLoS scenarios that affect the QoS of VANET applications. Our main contribution has two folds.

(a) We propose a new method to keep the track of the LoS status of every vehicle. Based on this method, we devise a robust plausibility-based consistency check mechanism to identify NLoS sitaution and deal with it, i.e. guarantee communication between neighbors even if the messages are not received directly. Our routing strategy uses a piggybacking-based alarm/concern-response mechanism and cause significantly less traffics than the uncontrolled broadcasting strategy in [6].

(b) Unlike [6], with the essence of location information from security and privacy standpoint in mind, our new strategy guarantees users location confidentiality and conditional privacy through privacy-aware neighbor lists and location-based encryption. We propose a secure and privacy-aware mechanism to adapt the VANET application to different LoS scenarios and make a smooth transition from normal scenarios to NLoS scenarios. To be more precise, we use a secure location-based encryption scheme to limit the semantics of the message to intended users and to enable the message to be used for the stipulated time duration.

The structure of the rest of the paper is organized as follows: Section II summarizes the related work followed by our proposed scheme for cooperative communication in NLoS scenarios in section III. By quantitatively evaluating our proposed scheme with respect to known solutions in Section IV, we give concluding remarks in Section V.

II. State of the Art

Recently, several efforts have been made to study the VANET scenarios on real vehicles on the road from many perspectives. From the tests, it has been found that an additional received power loss of 10 dB can be caused by the object (for instance a large truck) that obstructs line-of-sight from a transmitter to a receiver [7]. In order to observe the practical effect of the vehicular obstruction on the communication between vehicles, Meireles et al. [5] conducted experimental studies and found out that a single obstacle can cause a drop of over 20 dB in received signal strength when two cars communicate at a distance of 10 m. Similarly, Boban et al. [8] thoroughly studied the effect of the height of a vehicle on the communication between vehicles. In their studies, it was reported that the tall vehicles significantly increase both the effective communication range and the message reachability by more than 50% thereby increasing the message reception rate. From a more generic standpoint, Boban et al. [9] thoroughly studied the impact of vehicles as obstruction in VANET.

From location verification standpoint, Abumansoor et al. [6] proposed a cooperative approach, which is basically a kind of uncontrolled broadcasting, to provide localization, location verification and to make sure the integrity of the localization services in NLoS conditions. They check for inconsistency in the information received from neighbors, which is caused by intermittent NLoS situation, and then trigger location verification function if there is inconsistency. While this work is the first work of its kind, it suffers from several drawbacks. First, this strategy uses a kind of uncontrolled broadcasting and thus suffers from heavy traffic. Another main drawback of this strategy is that a vehicle which is NLoS cannot be distinguished from a vehicle which is too far from the receiver and thus cannot establish a communication channel even without any obstacle. As a result, their strategy keeps looking for a vehicle which is far away and suffers from another efficiency issue. Most of all, [6] does not consider the location privacy of individual vehicles. As a result, during the course of the protocol, all of the protocol participants who are not intended receivers of the mobility packets/beacons, receive the information in plaintext in [6]. Such plaintext information enables adversaries to manipulate the spatiotemporal information in the beacons and it gives rise to profile generation and privacy abuse. It is essential to keep the adversaries at bay to manipulate and/or infringe with location and other vulnerable information. Since there is no distinction in insider or outsider, both kinds of attackers can infringe with identities, spoof them, impersonate other nodes, and generate movement profiles. In their scheme, the adversaries can abuse nodes privacy in many ways.

Opportunistic routing/broadcasting in VANET is another technique that deals with the broadcast efficiency and efficient penetration of messages across the network [10], [11]. However, our NLoS scenario, due to its unique characteristics, cannot be solved through opportunistic broadcast (OB). OB mainly deals with multi-hop transmission where it is used to achieve higher message penetration and minimize the number of hops by selecting the right nodes as candidates for relayers.

Unlike the previous schemes, we encompass the full picture of the vehicular communication in case of NLoS condition by using already established beaconing framework and taking into account the security and privacy of the users and their locations. Our work aims at VANET applications that demand constant PDR and QoS guarantee. Without such mechanism, effective transmission range will be degraded and as a result it will degrade the application performance. Our proposed scheme also considers the mechanism by which we can find out the LoS status of each vehicle. We maintain privacy-aware neighbor lists, and in order to figure out the status of LoS, vehicles perform plausibility-based consistency check on the neighbor lists. Moreover in case of NLoS, the affected vehicles use cooperative mechanism to communicate with the neighbors. The NLoS affected vehicles raise alarm through their beacon messages and the nodes with clear LoS respond through beacon messages as well by using piggybacking. Such approach incurs negligible amount of overhead on the channel and thusforth increases efficiency. For location confidentiality and privacy, we use location-based encryption.

III. Proposed Cooperative Communication in NLoS Conditions

A. System Model

VANET is composed of vehicles equipped with On-Board Unit (OBU) that contains a tamper-resistant module (TRM) which is responsible for secure operations such as cryptography-related operations and storing security keys and certificates. Moreover there are management authorities such as Department of Motor Vehicles (DMV) that sits at the top of the management hierarchy and is responsible for the registration of vehicles and other management roles. Another important entity is the Revocation Authority(s) (RA) that revokes the misbehaving nodes, and judiciary. Without loss of generality, there are heterogeneous types of vehicles on the road ranging from small cars to huge trucks.

B. Adversary Model

We assume the adversaries to be insiders and outsiders and have more resources as compared to a benign nodes. Since we do not use any identities in our scheme, this gives an extra edge to the adversary. In other words the adversary has the capability to abuse users privacy in such environment by correlating spatiotemporal information from beacon messages and construct profiles against users. Adversaries can listen to wireless channel and the excess of resources makes them capable of spoofing or impersonating other vehicles as a result of message manipulation. The users involved in the cooperation are considered to be partially trusted while users that do not participate in VANET activity are not trusted. This is in the sense that, while receiving mobility messages from other users, they may attempt to generate movement profiles against other users and may try to ascertain the real identity of the senders/originators. It is to be noted that, under this adversary model first priority is to minimize the possibilities for outsiders and then deal with the insiders to diminish the privacy abuse.

C. Network Model and Communication Paradigm

The network model of our proposed scheme is illustrated in Fig. 1. The network model, at least in part, resembles with Hussain et al.s [12] and Sun et al.s scheme [13]. We consider the signature VANET framework where DMV controls the whole VANET system along with two other functional entities namely RCAs and RAs. Vehicles on the road communicate with each other and with the roadside infrastructure for service exchange and status updates.

In our proposed scheme, we consider traffic view construction application that requires frequent mobility information from neighbors through beacons. In VANET, every vehicle broadcasts and accumulates beacon messages in the order of milliseconds according to DSRC standard, and use them to

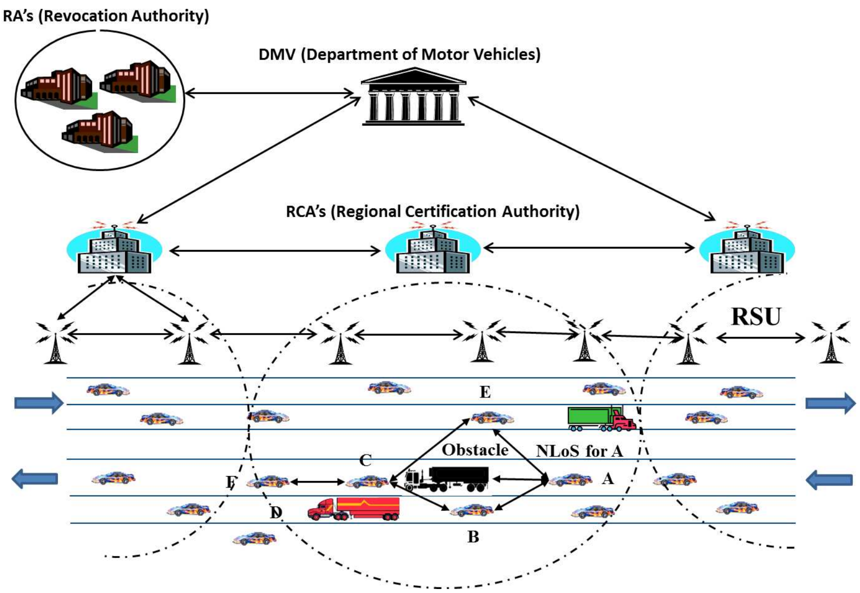
RA's (Revocation Authority)
DMV (Department of Motor Vehicles)
RCA's (Regional Certification Authority)
RSU
E
Obstacle
NLoS for A
C
F
A
D
B

Fig. 1: Proposed Network Model.

construct local traffic view and extended traffic view [14]. As aforementioned, the effective transmission range is affected by the presence of objects that obstructs and/or blocks the line of sight for other vehicles on the road, such as huge trucks. To this end, the NLoS-causing objects are not used as multi-hop relayers because they can be malicious by either not forwarding the messages for malicious reasons or launching any other attacks. Therefore we consider piggybacking on single-hop beacons in our scheme. In order to figure out the LoS status, we leverage both senders and receiver-centric strategies to look for the inconsistency in the neighbor lists. In other words, senders and receivers of the beacons both try to find inconsistency in neighborhood data about the area ahead and behind them, respectively. This way, for the receiver of the beacon, if there is NLoS and there is no neighbor with the clear LoS, then the neighbor who is also the sender of the beacon in the NLoS affected area for this receiver, already knows about the fact that some of its neighbors are experiencing NLoS. In such case, the sender of the beacon actively looks for other sources, e.g. opposite side nodes to provide the information to the vehicles in NLoS affected area.

D. Beacon Messages

The generic format of beacon message aka heart-beat message denoted by M_b is as follows:

$$M_b = (Data\|SecurityParam.\|H_{K_V}(VID)\|CCB)_{K_{geolock}}$$

Where Data is the mobility information including current speed, current location, and other statistics, $SecurityParams.$ are the security parameters included in the beacon message for authentication, confidentiality, non-repudiation, and so forth, K_V is the individual secret key used to calculate the keyed hash and VID is the vehicle ID. It is to be noted that we include the hash value so that the original ID of the vehicle cannot be known. We use additional information in beacons referred to as Communication Control Bytes (CCB). The details of CCB will be discussed in the next subsection. For more details of the security aspects, the readers are referred to [12] and [15]. Since beacons are broadcasted with high frequency, the outsider attackers may find it easy to target these beacons in order to construct the movement profiles against users based on their closed spatiotemporal information. That is why outsiders must be kept at the bay from abusing privacy and constructing movement profiles. We use geolock-based encryption proposed by Hussain et al. [16]. In the geolock-based encryption, location information, validity time, and different security keys are used to construct a geolock value ($K_{geolock}$)to encrypt the whole message with. In order to decrypt the message, the node must be physically present at the location where current $K_{geolock}$ is meant to work, and the node must hold other valid credentials needed for geolock construction. Figure 2 shows the construction process of $K_{geolock}$ that is used to encrypt beacon message. $K_{geolock}$ construction module takes as input, the effective region size, message lifetime, zone key (K_Z), and RSU-level key (K_{RSU}), and then multiplexes these values altogether to calculate the hash value from the multiplexed content. Our proposed location-based encryption mechanism guarantees different levels of confidentiality as follows: GPS coordinates are publically available, K_Z is known to the legitimate VANET users in a specific zone, and K_{RSU} is known to the vehicles currently present within the transmission range of that RSU. That is why the location confidentiality is guaranteed categorically. Moreover We assume that K_Z and K_{RSU} are subject to change on a regular or dynamic interval for security reasons; they have no contribution to security and privacy, otherwise. It is to be noted that in our scheme, user privacy is conditionally preserved through beacon messages and location confidentiality is guaranteed through location-based encryption.

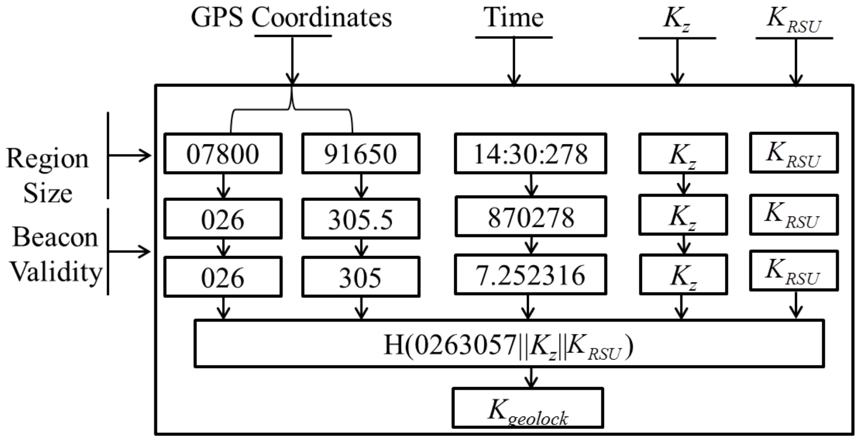

Fig. 2: Geolock-based Encryption key generation.

E. Neighbor Lists

Neighbor list is of prime importance in our proposed scheme because vehicles figure out about the LoS status by checking the consistency in their neighbor lists. Therefore we propose a security and privacy-aware neighbor list maintenance mechanism. From a single user standpoint, we divide the one-hop distance to a fixed size boxes (location slots) in front and behind of the vehicle as given in Fig. 3. The size of each box is an important parameter in our proposed scheme. Having small box size would increase the granularity of the information regarding NLoS, but would raise the privacy concern as well because there would be too few nodes in the single box. That is why we keep the size of the box to be $50m$ for now. That means for the transmission range defined by DSRC, there will be 6 boxes in front of every vehicle and 6 boxes behind it in its theoretical transmission range. These boxes are just the representation of the space in front and behind the vehicle where the vehicle maintains the traffic dynamics. The locations slots (LS) serve as virtual neighbor lists for the vehicles where they maintain the node count at every beacon interval. It is to be noted that in order to find inconsistency, every vehicle stores the immediate two states of neighbor vehicles in the virtual neighbor list. When a message is received from the neighbor, after figuring out whether the node is ahead or behind the receiver; the receiving nodes checks its neighbors list for the previous entry. If the node is already in the neighborhood then the record is updated in the respective box, otherwise it is saved in the respective box. From the above neighbor lists, the receiving nodes have rough idea as at any instant of time, how many nodes are present in each box. It is to be noted that the opposite side vehicles save the information in the same way.

F. Checking for NLoS

As aforementioned, each vehicular node after checking for inconsistency in its neighbor lists, i.e. any box(s), it checks for possible NLoS according to Algorithm 1. In fact, the vehicle compares the immediate previous state of the neighbor list with the newly perceived state through beacons. If there is inconsistency in the neighbor lists, then there can be two scenarios, either inconsistency in the neighborhood ahead or behind the vehicle. These two scenarios exhibit different actions to make sure that the vehicles communicate in case of NLoS. When a vehicle finds inconsistency in the neighborhood ahead, then it confirms NLoS for itself and triggers NLoS-based communication as in Algorithm 2. In case of inconsistency in the neighborhood behind, it concludes that the vehicles behind have NLoS scenario and cannot get its messages. In such case, the current vehicle finds another way, for instance opposite side vehicles to deliver the information to the vehicles behind. In the first case, the receiver raises an alarm against NLoS by triggering NLoS status according to Algorithm 1. At the same time, the node also constructs CCB and piggybacks the NLoS query in the next beacon interval.

G. Piggybacking Parameters

When a node finds out about NLoS in its transmission radius ahead, it constructs CCB. There are two forms of CCB, i.e. CCB-req and CCB-rep. CCB-req is the request from the nodes that experience NLoS and intends to verify the current traffic situation in the respective neighborhood whereas CCB-rep is the reply to the respective query. If a node receives multiple queries regarding an area which is in the closed proximity from the requesters standpoint, then the replier responds collectively to those queries instead of replying individually. For instance two nodes in the neighborhood of each other and driving close to each other and experiencing the same state of NLoS (for instance vehicle A and vehicle B in Fig. 1) may raise an NLoS alarm likely about the same area, which is why only one response will serve the purpose for both of them. The format of both CCBs is given below.

Request:

$$\begin{aligned}(Flag||((req_{id1}, Pos_{start}, status),\\ (req_{id2}, Pos_{start}, status)\\ ,..., (req_{idn}, Pos_{start}, status)))\end{aligned}$$

Reply:

$$\begin{aligned}(Flag||((rep_{req_{id1}}, Pos_{start}, status),\\ (rep_{req_{id2}}, Pos_{start}, status)\\ ,..., (rep_{req_{idn}}, Pos_{start}, status)))\end{aligned}$$

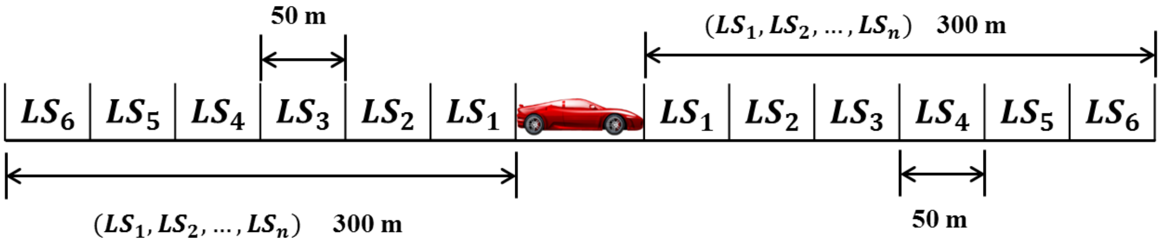

Fig. 3: Neighbor sections of a node (Neighbor Lists).

Algorithm 1 **TriggerNLoS** ($Data_{LS[1\rightarrow n]}$)

```
Assumption: Two immediate statuses for neighbors are saved in any interval $[t_{i-1}, t_i]$
for $k = t_0$ to $k = n$ and $k = k + f_b$ do
    for $LS_1$ to $LS_n$ do and direction ahead
        Check consistency of two consecutive states
        if ($S_{cur} < S_{prev}$)(Abrupt Change) then Construct CCB for respective LS
        Set FLAG
        Break
        else Do nothing
        end if
    end for
    for $LS_1$ to $LS_n$ do and direction behind
        if ($S_{cur} < S_{prev}$)(Abrupt Change) then wait()
        if CCB received then
        Break
        else Send info to opposite side vehicles
        end if
        end if
    end for
    if $FLAG = set$ then Trigger NLoS
    CommNLoS
    end if
end for
return $Status_{NLoS} = TRUE/FALSE$
```

Algorithm 2 **CommNLoS** ($B_1, B_2, B_3, ..., B_n$)

```
Assumption: Two immediate statuses for neighbors are saved in any interval $[t_{i-1}, t_i]$
for $k = t_0$ to $k = n$ and $k = k + f_b$ do
    Beacon received with CCB
    for $LS_1$ to $LS_n$ do
        Extract CCB and check fro the same area for direct comm.
        if report is put up already then Break
        else if (NLoS in the same direction & area in question has consistent node info.) then
        Construct CCB-rep
        Forward the node info. to the requester
        else if (NLoS in the Opposite direction) then
        Forward the available info. with timestamp
        end if
    end for
end for
return /* Communication in NLoS */
```

In the above CCBs, the Flag bit represents the request or response CCB followed by the contents of the request and response. Each request and response is in the form of triplets that contain a unique ID with which the area (slots) under consideration is identified, starting position of that area, and the status of that area in terms of the traffic dynamics, which in our case is the number of nodes. The response is generated in the same way, where the reply is included in CCB for each requested box in the CCP-req.

H. Communication in NLoS

When a vehicular node experiences NLoS in front of it, then it triggers NLoS status as aforementioned and it piggybacks the constructed CCB through next beacon to its one-hop neighbors in both directions. The neighbors upon receiving CCB-req, perform preliminary plausibility checks according to Abumansoor et al.'s scheme [6]. The receiving node also checks for the possible NLoS that it might have for the area in question. In that case, the receiver checks whether it already raised its concern about NLoS, if yes then it needs to wait for the response from another node that has clear line of sight to the area. If the receiver has a clear line of sight and it has consistent information from the current and previous beacon interval, then it constructs CCB-rep and sends it back to the requester(s). It is also possible that the opposite side vehicles receive the request and have clear line of sight towards the area in question. In that case, the opposite side vehicle(s) will forward the information to the requesters with timestamp. The overall scenario is depicted in Algorithm 2.

IV. Quantitative Evaluation

In this section we quantitatively evaluate our proposed scheme from security & privacy, computation & communication overhead, and comparison with known solutions standpoint.

A. Security and Privacy

The requirements of our proposed scheme include location security and user privacy. We assume that the security parameters included in the beacon message already fulfill necessary security requirements such as authentication, non-repudiation, and integrity [15]. Our proposed scheme provides security for M_b against outsiders since the messages are sent in encrypted

TABLE I: Comparison with Known Solutions

Scheme	**Separate Comm. Paradigm**	**Security**	**Conditional Privacy**	**Location Confidentiality against outsiders**	**Multihop Comm.**	**Payload size**	**Revocation Cost**
MHLVP [6]	Yes	No	No	No	Yes	152 *bytes* other than beacons	N/A
Our Scheme	No	Yes	Yes	Yes	No	$148 + \alpha$ *bytes*	$2H$

form. M_b is encrypted with $K_{geolock}$ and only legitimate vehicles and RSUs that hold and/or can construct $K_{geolock}$ can decrypt the message. The security of the message depends upon K_Z, the zone level secret key which is used to construct $K_{geolock}$. $K_{geolock}$ keeps outsiders from manipulating the messages also limits the effect of stale messages in the network, when the validity period of $K_{geolock}$ expires, then it cannot be constructed. Due to high frequency of M_b (in order of milliseconds), we suppose loose authentication for M_b by Hussain et al. [15] where they used keyed HMAC.

Confidentiality and timeliness are provided by $K_{geolock}$. Only legitimate users having K_Z will be able to decrypt the message. However if K_Z is compromised, then outsiders can manipulate messages. Nevertheless they have to be physically present in the effective location. We do not include any identity information in the messages where it leads to link the message to a particular user. However the keyed hash of the VID is included in beacon message that is hard to link to any physical node. For RAs, it is possible to revoke a message, since they store the credentials at the time of vehicle registration and initialization through DMV.

In order to decrypt the message that is encrypted with current $K_{geolock}$, the decrypting node must be physically present in the area where current $K_{geolock}$ is valid and at the right time. Any insider legitimate user that is not currently present in the aforesaid area is considered as insider adversary denoted by A_I. In order for A_I that is not physically present in the area where current $K_{geolock}$ can be used for decryption, must construct all possible combinations of $K_{geolock}$ for the decryption of the message. When A_I receives message encrypted with current $K_{geolock}$ that is constructed with K_Z, K_{RSU}, t_{cur}, and loc_{cur}, it will be hard for A_I to figure out which K_Z and K_{RSU} are used to construct $K_{geolock}$ and that is why A_I has to try all combinations of these two keys and the GPS locations in each zone, in other words try all zones and RSUs therein. Additionally even in the single zone and RSU, the GPS coordinates are also important. If there are n zones, s RSUs in each zone and l locations under the jurisdiction of each RSU, then A_I must try the following number of keys to decrypt the message encrypted with current $K_{geolock}$.

$$\sum_{i=1}^{n}\sum_{j=1}^{s}\sum_{k=1}^{l} K_{ijk}$$

Moreover the time factor is an important issue in such brute force because after the expiry of the validity time denoted by $t_{validity}$ which is also an input to the $K_{geolock}$, the key cannot be constructed and becomes stale.

B. Computation and Communication Overhead

In this subsection, we consider the computation and communication overhead incurred by our proposed scheme. That is why the cost of verification that is incurred by beacon verification is equal to $1E + 2H$ where E is the encryption function and H is the hash operation. However in average cases the overhead is $1E + 1H$ since the revocation maybe needed only occasionally [15].

The communication overhead incurred by our proposed scheme in case of normal beacon is (including security parameters) 148 bytes whereas Abumansoor et al. [6] used 152 bytes of payload in their messages for request that does not include any security parameters. If we consider CCB, then the overhead incurred by our scheme is $148+\alpha$ where α is the size of the CCB. The single entry in CCB is equal to 9 *bytes* and maximum 12 entries can be accommodated in CCB where the effective transmission range is 300 *m*. Therefore the maximum size of the beacon with CCB is equal to 256 *bytes*. However in most of the cases, the communication overhead may not be equal to the maximum.

The storage required incurred by the neighbors list in our proposed scheme is negligibly small. If we consider a 4 lane road, then in a dense traffic regime, a 50 *m* dynamic box of the road can accommodate 28 vehicles of average size, which means there will be 336 vehicles in the transmission range of the vehicle on driving direction and 336 vehicles on the opposite direction at any instant of time. In the beacon storing procedure, we store the current time, $H_{K_V}(VID)$ and the joining time of the vehicle that requires about 34 *bytes*. Hence at maximum a vehicle needs 23 *kilobytes* of storage space.

C. Comparison with Known Solutions

To the best of our knowledge, only Abumansoor et al. [6] addressed the NLoS communication in VANET. However [6] focused more on the location verification. Therefore we compare our proposed scheme with MHLVP [6] from security, privacy, and communication overhead standpoint. It is to be noted that, MHLVP needs a separate communication paradigm with requests and replies in order to verify the location of the questioned vehicles. We take special care of the privacy and location confidentiality in our scheme wherein the neighbor lists are privacy preserved. The unicast communication in MHLVP incurs additional routing overhead to VANET. In contrast, we use the already established infrastructure within the boundary of the DSRC/WAVE standard to cope with the NLoS issues. Moreover colluding attacks are also possible in MHLVP. Additionally the plausibility checks that are suggested in MHLVP may not likely work in case of NLoS because the consistency cannot be checked if there is no communication with the node in the first place. Above all, it is important to know the LoS status beforehand and Abumansoor et al. [6] did not discuss how to find the NLoS scenario on the road. Unlike Abumansoor et al. our proposed scheme does not depend on received signal strength (RSS), because recently it has been found that RSS can easily be manipulated by adversaries. The comparison is outlined in Table 1.

V. Conclusions

In this paper, we put forth a secure and privacy-aware cooperative mechanism to alleviate the effects of Nonline of Sight (NLoS) situation caused by obstacles (e.g. huge vehicles). We aim at VANET applications that need a consistent packet delivery ratio (PDR) to guarantee quality of service (QoS). NLoS phenomenon directly affects such VANET application, therefore we take into account the NLoS factor among communicating vehicles and propose a secure and privacy-aware method to: 1) Figure out the LoS status of the vehicles. 2) Use cooperation-based mechanism to communicate in NLoS scenarios. To figure out LoS status, vehicles check for plausibility-based consistency in the neighbor lists where privacy-aware neighbor lists are maintained through received beacons. For communication in NLoS, the affected vehicles raise an alert about NLoS in its beacons and the vehicles with clear LoS provide them with relevant information. For location confidentiality and privacy, we use location-based encryption. Our proposed scheme is secure and conditional privacy-preserved.

Acknowledgment

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Ministry of Education, Science and Technology (No. 2012-R1A2A2A01046986).

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MEST) (No. 2012-R1A1A2009152).

This work was also supported in part by US National Science Foundation (NSF) CREST No. HRD-1345219.

References

[1] T. Chim, S. Yiu, L. Hui, and V. Li, “Vspn: Vanet-based secure and privacy-preserving navigation,” *Computers, IEEE Transactions on*, vol. 63, no. 2, pp. 510–524, Feb 2014.

[2] T. Chim, S. Yiu, L. C. Hui, and V. O. Li, “Vanet-based secure taxi service,” *Ad Hoc Networks*, vol. 11, no. 8, pp. 2381 – 2390, 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1570870513001261

[3] A. Baiocchi and F. Cuomo, “Infotainment services based on push-mode dissemination in an integrated vanet and 3g architecture,” *Communications and Networks, Journal of*, vol. 15, no. 2, pp. 179–190, April 2013.

[4] Q. Xu, T. Mak, J. Ko, and R. Sengupta, “Vehicle-to-vehicle safety messaging in dsrc,” in *Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks*, ser. VANET ’04. New York, NY, USA: ACM, 2004, pp. 19–28. [Online]. Available: http://doi.acm.org/10.1145/1023875.1023879

[5] R. Meireles, M. Boban, P. Steenkiste, O. Tonguz, and J. Barros, “Experimental study on the impact of vehicular obstructions in vanets,” in *Vehicular Networking Conference (VNC), 2010 IEEE*, Dec 2010, pp. 338–345.

[6] O. Abumansoor and A. Boukerche, “A secure cooperative approach for nonline-of-sight location verification in vanet,” *Vehicular Technology, IEEE Transactions on*, vol. 61, no. 1, pp. 275–285, Jan 2012.

[7] T. Abbas and F. Tufvesson, “Line-of-sight obstruction analysis for vehicle-to-vehicle network simulations in a two-lane highway scenario,” *CoRR*, vol. abs/1308.2574, 2013.

[8] M. Boban, R. Meireles, J. Barros, O. Tonguz, and P. Steenkiste, “Exploiting the height of vehicles in vehicular communication,” in *Vehicular Networking Conference (VNC), 2011 IEEE*, Nov 2011, pp. 163–170.

[9] M. Boban, T. Vinhoza, M. Ferreira, J. Barros, and O. Tonguz, “Impact of vehicles as obstacles in vehicular ad hoc networks,” *Selected Areas in Communications, IEEE Journal on*, vol. 29, no. 1, pp. 15–28, January 2011.

[10] M. Li, W. Lou, and K. Zeng, “Oppcast: Opportunistic broadcast ofwarning messages in vanets with unreliable links,” in *Mobile Adhoc and Sensor Systems, 2009. MASS ’09. IEEE 6th International Conference on*, Oct 2009, pp. 534–543.

[11] B. Blaszczyszyn, A. Laouiti, P. Muhlethaler, and Y. Toor, “Opportunistic broadcast in vanets (ob-van) using active signaling for relays selection,” in *ITS Telecommunications, 2008. ITST 2008. 8th International Conference on*, Oct 2008, pp. 384–389.

[12] R. Hussain, S. Kim, and H. Oh, “Privacy-aware vanet security: Putting data-centric misbehavior and sybil attack detection schemes into practice,” in *Information Security Applications*, ser. Lecture Notes in Computer Science, D. Lee and M. Yung, Eds. Springer Berlin Heidelberg, 2012, vol. 7690, pp. 296–311.

[13] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, “An identity-based security system for user privacy in vehicular ad hoc networks,” *Parallel and Distributed Systems, IEEE Transactions on*, vol. 21, no. 9, pp. 1227–1239, Sept 2010.

[14] R. Hussain, J. Son, H. Eun, S. Kim, and H. Oh, “Traffic information system: A lightweight geocast-based piggybacking strategy for cooperative awareness in vanet,” in *Consumer Electronics (ICCE), 2013 IEEE International Conference on*, Jan 2013, pp. 614–615.

[15] R. Hussain and H. Oh, “On secure and privacy-aware sybil attack detection in vehicular communications,” *Wireless Personal Communications*, pp. 1–25, 2014. [Online]. Available: http://dx.doi.org/10.1007/s11277-014-1659-5

[16] R. Hussain, F. Abbas, J. Son, and H. Oh, “Tiaas: Secure cloud-assisted traffic information dissemination in vehicular ad hoc networks,” in *Cluster, Cloud and Grid Computing (CCGrid), 2013 13th IEEE/ACM International Symposium on*, May 2013, pp. 178–179.