International Journal of Advanced Research in

Computer Science Engineering and Information Technology

Volume: 2 Issue: 3 08-Apr-2014,ISSN_NO: 2321-3337

Non line of Sight Location Verification in EMAP for Vehicular Ad Hoc Networks

M. Kailash[1], Prof. R. Chandrasekaran[2], Dr. J. George Chellin Chandran[3]

Dept of PG CSE, CSI College of Engineering, Ketti, The Nilgiris, India[1]

Dept of ECE, CSI College of Engineering,Ketti, The Nilgiris, India[2]

Dept of CSE, CSI College of Engineering, Ketti, The Nilgiris, India[3]

kmkailash26@gmail.com[1], *chandru_osho@csice.edu.in*[2], chellin1968@gmail.com[3]

ABSTRACT- *The security in VANETs is improvised with the involvement of Public Key Infrastructure (PKI) and Certificate Revocation List (CRL) through message authentication and the data transmissions are improved through NLOS. The direct communications between vehicles are blocked with interference of obstacles like trucks, buildings. These problems are overcome through NLOS conditions such as location verification and misbehavior detection. The neighborhood vehicles are tracked and are authenticated with EMAP. In EMAP, Certificates and signature matches with the CRL are used in checking and verifying the authenticity of any PKI system. Time consumption in checking the CRL is relatively less in EMAP because hash tables are used for searching process. Keys shared with the nonrevoked On-Board Units (OBUs) are used in Hashed Message Authentication Code (HMAC) for revocation checking process. End to end delay and message loss ratio is reduced here and thus the security and efficiency of VANETs are enhanced in EMAP. In EMAP,CRL checking process is improved by an efficient revocation checking process using a fast and secure HMAC function. EMAP is suitable not only for VANETs but also for any network employing a PKI system and also reduces the authentication delay.*

Keywords – VANETs, NLOS, CRL, EMAP, HMAC

1, INTRODUCTION

Vehicular Ad hoc Networks (VANETs) are being developed to provide on-demand wireless communication infrastructure among vehicles and authorities. Such an infrastructure is expected to deliver multiple road safety and driving assistance applications. Vehicles will be equipped with sensors and communication devices that will allow them to cooperate with each other and with authority units to disseminate and exchange various road applications' messages. For example, warning messages and traffic management instructions can be broadcast to increase drivers' awareness of potential travel hazards, allowing them to respond earlier to avoid traffic congestion and collisions or to clear the way for inbound emergency response units.

Other applications pertain to passenger comfort and convenience, such as locating

points of interest, exchanging multimedia assets with other users in the network, or receiving location-based commercial advertisements. VANETs consist of entities including On-Board

Units (OBUs) and infrastructure Road-Side Units (RSUs). Vehicle-to- Vehicle (V2V) and Vehicle-to Infrastructure (V2I) communications are the two basic communication modes, which, respectively, allow OBUs to communicate with each other and with the infrastructure RSUs [1]. The first part of the authentication, which checks the revocation status of the sender in a CRL, may incur long delay depending on the CRL size and the employed mechanism for searching the CRL. Unfortunately, the CRL size in VANETs is expected to be large for the following reasons: 1) to preserve the privacy of the drivers, i.e., to abstain the leakage of the real identities and location information of the drivers from any external eavesdropper each OBU should be preloaded with a set of anonymous digital certificates, where the OBU has to periodically change its anonymous certificate to mislead attackers. Consequently, a revocation of an OBU results in revoking all the certificates carried by that OBU leading to a large increase in the CRL size. 2) The scale of VANET[1,2,3] is very large. Since the number of the OBUs is huge and each OBU has a set of certificates, the CRL size will increase dramatically if only a small portion of the OBUs is revoked. To have an idea of how large the CRL size can be, consider the case where only 100 OBUs are revoked, and each OBU has 25,000 certificates [8]. In this case, the CRL contains 2.5 million revoked certificates.

According to the employed mechanism for searching a CRL, the Wireless Access in Vehicular Environments (WAVE) standard does not state that either a nonoptimized search algorithm, e.g., linear search, or some sort of optimized search algorithm such as binary search, will be used for searching a CRL. In this paper, we consider both nonoptimized and optimized search algorithms. In this paper, we focus on system reliability and location information integrity. We consider two types of attacks: 1) unintentional and 2) intentional. Unintentional attacks on network reliability can occur on roads where large vehicles travel, such as industrial areas. These are locations where safety applications for hazards such as blind spots can help to reduce the number of accidents but where NLOS[3] occurrences might prevent the desired reliability of those applications.

On the other hand, by knowing the limitations of wireless communication signals and possible methods of system exploitation, an attacker could use this technology in his or her favor. For example, a driver might try to avoid being tracked by police by traveling near large vehicles in an attempt to create a barrier. Improving and maintaining drivers' neighborhood awareness are important in VANETs. It is also important in developing a reliable and secure localization service capable of overcoming the obstacles' effects on communication transmissions. In this paper, we propose a cooperative location verification protocol in an NLOS condition. Unlike other verification protocols proposed for VANETs, the NLOS triggers the verification process rather than accepting the error. . Enabling each vehicle to determine its location is necessary in VANETs [2, 3], but it is not enough. Vehicles also need to have information about events in their surroundings and proximal vehicles. This type of information can be exchanged between network members using beaconing, direct messaging, or group updates. Moving objects such as trucks can also interfere with communication between vehicles and could block a driver's visual and communication line of sight, creating a Non Line-of-sight (NLOS) state, which can lead drivers to make poor judgments when changing lanes or merging onto a highway.

2, EXISTING SYSTEM

Most of the VANET simulators do not consider the impact of line-of-sight obstruction, caused by neighboring vehicles, on the packet reception probabilities. to identify and label each vehicle as in LOS [2] or in OLOS situation with respect to TX and RX at each

instant t. The identification of vehicles being in LOS or in OLOS states becomes fairly simple as the TMM discussed earlier provides the instantaneous position of each vehicle on the road. Thus, the position information of each vehicle together with some geometric manipulations gives the state information of each vehicle being in LOS or in OLOS state as follows,

1. Model each vehicle as a screen or a strip with the assumption that each vehicle has the same size.
2. Assumed that the intended communication range is a circle of a certain radius, i.e., Rc. At each instant t the vehicles that are in this circle are considered only.
3. Vehicles in each lane are assumed to be moving along a straight line. Thus only two vehicles in the same, one at the front and one in the back of the TX, will be in the LOS. The rest of the vehicles in the same lane are considered to be in the OLOS state.
4. Draw straight lines starting from the antenna position of the TX vehicle touching the edges of the vehicles in the front and back to the edges of road (see Fig. 2). All vehicles that are bounded by these lines are shadowed by other vehicles thus in the OLOS state.
5. Vehicles that are not bounded by these lines are analyzed individually to see if they are in LOS or in OLOS from the TX.
6. The identification process is repeated for each vehicle and at each time instant t to find out whether the vehicles are in LOS and in OLOS states with respect to every other vehicle. The state information of each vehicle can then be used either for analytical performance evaluations or for packet level VANET simulations.

3, PROPOSED SYSTEM

In VANETs, objects such as buildings, trees, and other features that exist on roadsides can interfere with or block radio signals. In general, the higher the radio signal frequency is, the more vulnerable it is to interference [3]. One particular study showed the vulnerability of high-frequency radio signals to interference. For example, at a frequency of 5.85 GHz, a signal loss of 14 dB is caused by home penetration, and a loss of 11–16 dB is due to tree shadowing, whereas a signal loss of 7.7 dB is caused by penetrating a building at a frequency of 912 MHz. In the U.S., the 5.9-GHz frequency is assigned for VANET communication. In a VANET environment, consideration should be given not only to fixed obstacles and buildings but also to moving objects on the road that can cause signal block. Since vehicles come in different shapes and sizes, they can serve as obstacles between neighbors that are in the same communication range. Unlike with buildings and fixed structures for which interference and signal quality factors can be measured in the field and taken into consideration while traveling in a given area, moving obstacles with different shapes, speed, composition, and density can create an NLOS state that changes on an unpredictable temporospatial basis and could prevent a vehicle from receiving consistent updates and location information from its neighbors.

In Fig. 1, we illustrate what can happen if an obstacle blocks communication signals. Vehicle A detects an event E [2,3], which is an emergency vehicle approaching. In response, A sends a warning message to its neighbors behind it to encourage their operators to slow down and allow the emergency vehicle to pass, which is a sequence of events that could

prevent vehicle operators from needing to brake suddenly or swerve. However, vehicle B might not receive the warning due to the position of the bus C. The bus does not forward the message, assuming that B is within A's communication range. If A has the knowledge that B is still within communication range but obstacle C is blocking direct communication with it, the application should decide to allow C to forward the message to ensure message delivery. We believe that vehicles should have better knowledge about their surroundings to support upper-level applications and services, which do not perform well in NLOS conditions. Our objective in this paper is to present a novel protocol that verifies a vehicle's announced location using a multi hop cooperative approach whenever direct verification and communication are not possible. With such a solution, a vehicle's awareness of its neighbors increases, theoretically improving the reliability and availability of many safety, travel, and traffic management applications and services.

3.1, SAFEGUARDING LOCALIZATION

Due to VANET limitations and the importance of position information, securing localization is a challenging area of research on VANETs. A secure localization can be achieved with the following approaches.

1) **Protected communiqué:** Secure communication channels by enabling receivers to authenticate the sender while maintaining their privacy and checking message integrity. Some researchers have suggested securing VANET communications to authenticate the sender and check the message integrity using digital signatures. In fact, IEEE1609.2 was released as a standard to secure messages in VANET.
2) **Mischievousness exposure and seclusion:** Detect malicious nodes by evaluating the context of messages and the behavior of the sending nodes.
3) **Location verification:** Enable nodes to verify received location information and validate its integrity.

3.2, PROPOSED ALGORITHM

Vehicle VS is the source and it sends a message to the destination VD. The communication could be blocked due to two reasons:

I. **Obstacle Interference**
Buildings, trucks or any other large vehicles could break the signals.

II. **Network Issues**
The signal strength, bandwidth, delay and such network factors could cause communication break.

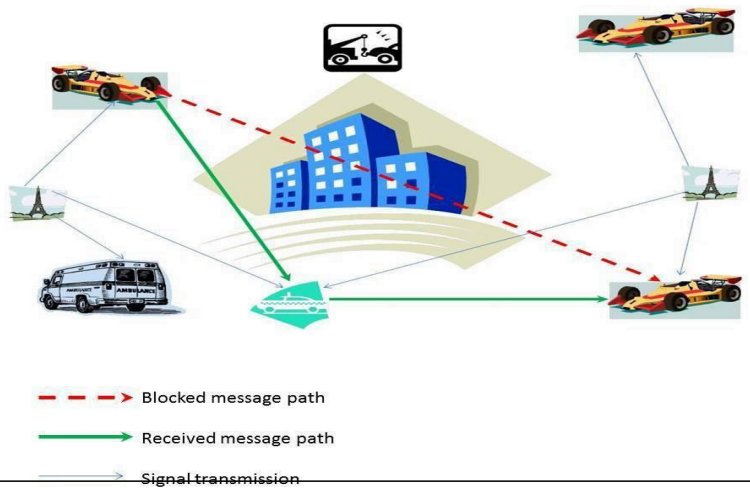

Fig. 1 NLOS Architecture Diagram

The Fig.1 shows the NLOS architecture for the proposed system. On such issues the vehicle takes an alternative path through the neighboring vehicles N [1, 2 … n]. The selected vehicle NV will be the intermediate vehicle to communicate with VD. On each hop EMAP process will be executed, such that every vehicle must be authorized by undergoing:

i. CRL checking process
ii. Message signing
iii. Message verification

3.2.1, ALGORITHM

```
NLOS:VS send_msg→VD
If Msg_blocked(detected)
// Obstacle detection
If obstacle detected
// Position verification
        If neighbour(N[1,2,…n]) == within_range;
//choose neighbour(N[1,2,…n])
        Select neighbor(NV)
        NV =  Min_Dist (VS→VD through N[1,2,…n]);
        Send_msg,VS→ NV(EMAP)||Verify sender;
        Then Send_msg,NV →VD(EMAP) ||Verify sender;
Else
      Stop_connection;
        Else
              Network_Issue;
Else
          Send_msg,VS→VD(EMAP) ||Verify sender;
```

VS→Source vehicle
VD→Destination vehicle
N [1,2,…n]→All neighboring vehicles
NV→selected neighbor
EMAP→Expedite Message Authentication Protocol

3.3, SECURITY

NLOS [3] conditions can affect the integrity of exchanged location information about neighboring vehicles. In this section, we outline the security specifications that are required for the proposed solution that will lead to a secure neighborhood localization information network and validate the integrity of its data.

The proposed solution should do the following:

1. Increase neighborhood awareness and vehicles' knowledge about surrounding nodes under NLOS conditions.
2. Monitor localization information, detect data inconsistencies, and validate data integrity.
3. Ensure that a vehicle avoids total dependency on periodic incoming beacons and update messages.
4. Maintain confidentiality, and employ message or sender authentication.

5. Validate processed information, and eliminate false data before processing.
6. Support availability in a large-scale environment.

4, PERFORMANCE EVALUATION

In comparison with the LOS-EMAP scenario, NLOS-EMAP gives a higher throughput because in LOS if there are obstacles blocking the signal then the message will be quit, where as in NLOS, if obstacle is detected then the message would take the next neighborhood vehicle as its path and then sends the message to the destination through that vehicle. Also the delivery rate would be comparatively high due to the influence of NLOS and the message transfer ratio would increase sufficiently. Authentication Delay, End to End Delay, Message Loss Ratio and Communication Overhead are improved in NLOS compared to that of LOS. Fig. 2 shows the comparison of NLOS with the existing system.

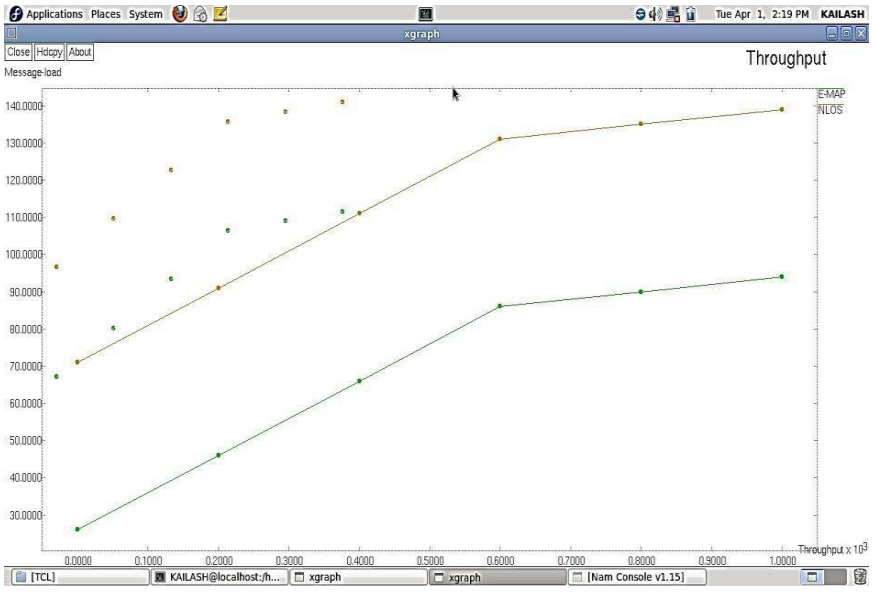

Fig. 2 Comparison of NLOS with Existing system – Throughput

5, CONCLUSION

In NLOS-EMAP, the messages between the vehicles will not fail in any sense because the obstacle detection is ensured here and alternative path is chosen immediately with reference to the position verification. Also the authentication is highly secure through the involvement of EMAP process thereby improving the security, integrity and reliability of the communication. The direction of future enhancement will focus on improving the signal strength of the message transmission.

6, REFERENCES

[1]. Albert Wasef and Xuemin (Sherman) Shen, IEEE, Fellow, EMAP : Expedite Message Authentication protocol for Vehicular Ad hoc Network.

[2]. Taimoor Abbas, and Fredrik Tufvesson, Line-of-Sight Obstruction Analysis for Vehicle-To- Vehicle Network Simulations in a Two- Lane Highway Scenario.

[3]. Osama Abumansoor, Member, IEEE, and Azzedine Boukerche, Senior Member, IEEE, A Secure Cooperative Approach for NonLine- of-Sight Location Verification in VANET.

[4]. P. Papadimitratos, A. Kung, J.P. Hubaux, and F. Kargl, "Privacy and Identity Management for Vehicular Communication Systems: A Position Paper, " Proc. Workshop Standards for privacy In user- centric identity management, july 2006.

[5]. K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, " CARAVAN: Providing Location Privacy for VANET", Proc. Embedded Security in cars (ESCAR) Conf., Nov. 2005.

[6]. A. Wasef, Y. Jiang, and X. Shen, "DCS: An Efficient Distributed Certificate Service Scheme For Vehicular Network," IEEE Trans. Vehicular Technology, vol. 59, no. 2 pp. 533 - 549, Feb.

[7]. A. Boukerche, H. Oliveira, E. Nakamura, and A. Loureiro, "Vehicular ad hoc networks: A new Challenge for localization-based systems," Comput. Commun., vol. 31, no. 12, pp. 2838–2849, July 2008.