An Authenticated Collaborative Grid-Based On-Road Localization Scheme for VANETs

[1]Jayalakshmi L, [2]Ann Nita Netto

[1]PG student, [2]Assistant Professor
[1,2] Dept. of electronics and communication SBCEW Elavumthitta, Pathanamthitta, India

***Abstract*: VANET (Vehicular Ad hoc Network) is an emerging research area. Finding location of a node in VANET is one of the most challenging issues in recent years. GPS receivers equipped inside the vehicles may lose satellite signals and calculate wrong positions due to signal blocking. Grid based scheme is a GPS-free localization method in which vehicles exchange location information and help each other to calculate accurate position for all the vehicles inside the network. However, since VANET is open and wireless in nature, probability for attack is very high. It requires a mechanism to help authenticate messages, identify valid vehicles, and remove malicious vehicles. A Public Key Infrastructure (PKI) can provide this functionality using certificates and public keys with the aid of RSUs (Road Side Units) that act as a gateway between the Certificate Authority (CA) and vehicles. The proposed scheme efficiently prevents eavesdroppers from generating harm to legal users and provides timely revocation of misbehaving participants, thereby contributing towards VANET security.**

***Keywords:* VANET, Grid localization, Attacks, PKI, Certificate authority, CRL, RSU, Revocation.**

I. INTRODUCTION

Vehicular Ad hoc Network (VANET) is a modified form of Mobile Ad hoc Network (MANET) in which the mobile nodes are replaced with vehicular nodes. It has emerged recently as one of the most attractive topics for researchers due to their remarkable ability to improve traffic safety, efficiency and other added services. Nowadays, most of the vehicles use GPS receivers for finding their physical location and to obtain driving direction information. However, the GPS receivers may sometimes lose satellite signals and provide wrong location information due to signal blocking. The problem is found to be more serious in places such as tunnels or multi-floor bridges which may cause various safety and convenience problems. For example, after getting out of a tunnel, a driver may need to make an immediate decision on changing the route without getting enough time to pay attention to other vehicles, resulting in accidents. Grid based localization is a collaborative method to find the accurate location of vehicles with blocked GPS signals with the help of those with good GPS signals. In this method, communication between vehicles employs sharing of location and distance information among them. The sharing is performed by assuming “Trust-Your-Neighbor” relationship among the vehicles which assumes that all neighbors behave properly. However, since VANET is wireless and dynamic in nature, we should not ignore the fact that attackers do exist in real networks. Security is one of the most critical issues in VANETs because their information transmission is propagated in open access environments. There are different varieties of attacks that we cannot enumerate every possible one. The most obvious attack we can imagine may be a node injecting some false information into the network and trying to convince other members of the system. The purpose of the attacker is to cause harm to legal users, and as a result services are not readily available, thus denial of service. It is necessary that all the transmitted data cannot be injected or changed by users who have malicious goals. Moreover, the system must be able to detect the requirement of drivers while still maintaining their privacy.

To address the above challenges, this paper proposes an authentication scheme for vehicles in the network with which the communication between them can be achieved in a secure manner. The proposed scheme is based on the principle of Public Key Infrastructure (PKI) in which the unique ID of each vehicle acts as the public key. The goal of authentication is met using with the aid of road side infrastructure, known as Road Side Units (RSUs). The RSU is responsible for tracking the vehicles and checking whether their identities are valid or not. When a vehicle is found to be problematic, the certificate of that particular vehicle will be revoked and it will be blocked from participating in the network. In the simulations, the communication among multiple nodes has been analyzed, some of which are location-aware and some others are unaware of their location. Then, attack by a malicious node has also been studied and our authenticated localization scheme is applied for the nodes to calculate their location accurately as well as securely.

II. SYSTEM OVERVIEW

A. Assumptions:

It is assumed that each vehicle is equipped with a GPS receiver which is already common nowadays. When the GPS can receive signals from satellites, it provides current location information and driving direction to the drivers. It may sometimes lose satellite signals and when this happens, vehicles calculate their location using grid based scheme. Additionally we assume that each vehicle is equipped with a wireless card so that they can self-organize into an ad hoc network and communicate with each other. Vehicles can find their neighbors through periodical exchange of beacon messages [1]. Also, it is assumed that all vehicles consist of a Tamper Resistant Module (TRM) that performs ID validation.

TABLE 1 NOTATION

Notation	Description
n_i	i^{th} node
(x_i, y_i)	n_i's location
$d_{i,j}$	distance between vehicles n_i and n_j
s_i	possible locations of n_i
$S_{i,j}$	possible locations of n_i determined by $d_{i,j}$

B. Grid-based location evaluation:

In grid based location evaluation, a node n_i obtains the following information: the locations of vehicles n_a, n_b and n_c, distances to the three vehicles and $d_{j,c}$.

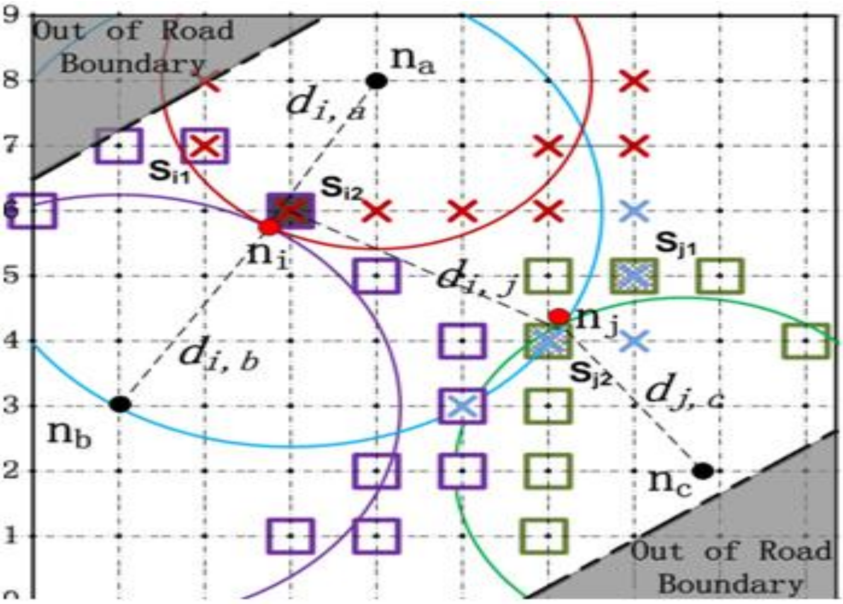

Fig. 1: grid-based localization

To evaluate location in grid based scheme, n_i first divides the map into grids. Then using principles of intersection, the possible grid positions of n_i are calculated in a gridded road map given the grid size r, its neighbor n_j, its position (x_j, y_j), and $d_{i,j}$. Given the input x_j, y_j and $d_{i,j}$, a circle with origin (x_j, y_j) and radius $d_{i,j}$ can be drawn onto the map, and it crosses the map grids at several points. In this way, it marks all the grid intersections closest to these points [1].

III. SECURITY CHALLENGES

There is a huge diversity of VANET services and applications such as road safety, internet access etc. However, efficient data dissemination mechanism is a key challenge to provide successful VANETs applications. Additionally, the problems on VANET security become more challenging due to the distinctive options of the network, like presence of extremely large number of network entities and highly dynamic nature of these entities, specifically, it's essential to make sure that "life-critical safety" information cannot be inserted or modified by an attacker; likewise, the system should be capable of establishing the liability of drivers. At the same time, it should care for the privacy of the drivers and passengers. It is obvious that any malicious behavior of users, like a modification and replay attack with regard to the disseminated messages, might be critical to alternative users.

A. VANET Attacks:

There are a number of probable attacks in VANET. The major idea of the attacker is to generate harms for legal users, and as a outcome services are not easily reached and thus denial of services. Some of these attacks are listed below.

a) Node impersonation:

Every vehicle in VANET has a unique ID and with the help of this ID they exchange information in the network. Each node is identified by this unique ID in the network. In this attack, the attacker changes his/her identity and act as the real message generator. Also, on receiving messages from other nodes, the attacker modifies it for his/her benefit and transmits it into the network.

b) Sending false information:

In this attack, the attacker transmits fake information in the network. As a result of this, other vehicles get diverted from their route and the attacker gets a clear path. The main goal of the attacker is to change the decision of remaining nodes in the network, so that the attacker can get down the network.

c) ID disclosure:

Attacker in this type of attack captures the ID of another node. Then it generates a malicious code to be transmitted to the network and thus collect the required information of other nodes. The privacy of the target node is affected by this type of attack.

d) Sybil attack:

This is one of the most crucial attacks. In this type of the attack, the attacker generates messages which are then transmitted with a different ID. Then the other vehicles in network misinterpret that the message is genuine and it is been transmitted by a legal user of the network. The main task of the attacker is to create an illusion of many vehicles participating in network that are communicating with each other, and force them to change their decision [3].

IV. PROVIDING SECURITY

In this section, the security solution to be deployed in vehicular networks is discussed. The necessary requirement of VANET safety messages is authentication. In this paper, digital signature is chosen as the fundamental building block for providing message authentication. The proposed method is to assign a set of public/private key pairs to each vehicle. Vehicles then use these keys to digitally sign messages and thus authenticate themselves to others. To perform secret operations such as signing the outgoing messages using keys, a Tamper Resistant Module (TRM) is needed inside each vehicle. The module contains a set of sensors that can discover hardware tampering and erase all the stored information to prevent them from being captured [5].

Due to the open environment present in VANETs, a trusted authority is compulsory by which these public keys should be issued and signed. The transportation authority can act as the certification authority (CA) which is responsible for issuing key certificate to vehicles. The requirement for certificates issued by such an authority implies the use of a PKI (Public Key Infrastructure). The advantage of using a PKI for VANETs is certificate revocation, i.e., the certificate of a detected attacker or malfunctioning vehicle can be blocked. After the revocation, it will not be able to use its keys or if it still does, vehicles verifying them will be made aware of their invalidity.

A. *Certificate Revocation:*

Certificate revocation avoids vehicles receiving messages from problematic certificate holders. The most common method to revoke certificates is the distribution of CRLs (Certificate Revocation Lists) that contain the IDs of detected malfunctioning vehicles. In this paper, a Road Side Unit (RSU) based certificate revocation is proposed. RSU is a stationary substance unit configured at roadsides having wireless access point, memory storage and computational capabilities. These units act as a gateway of CA to the vehicular network. The connection of CA to the static RSU infrastructure is over secured wire line links.

B. *Steps in CRL distribution:*

As shown in Fig. 2, following steps are involved in the distribution of certificate revocation list to all vehicles.

1) Vehicles register with RSU with their public keys in order to participate in the network.

2) RSU communicates the acquired keys with CA.

3) CA verifies the keys by checking the validity of corresponding certificates.

4) CA generates the list.

5) The list is distributed to RSU.

6) RSU broadcast the list to vehicles

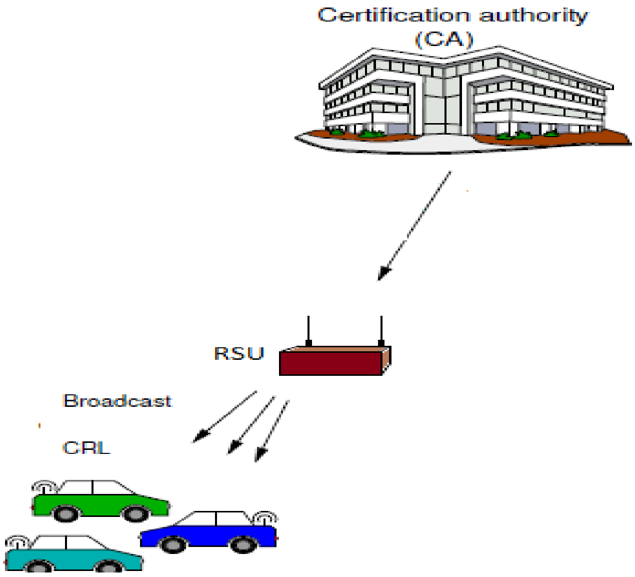

Fig. 2. RSU broadcasts CRL to vehicles

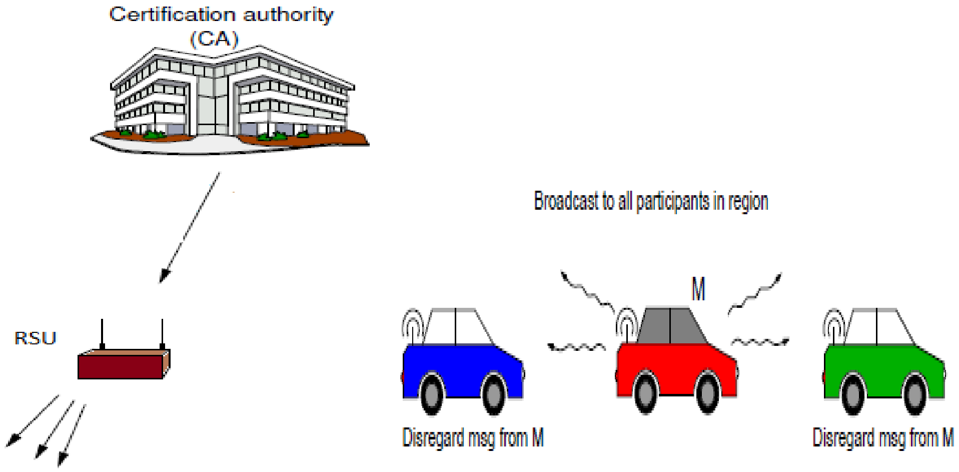

Fig. 3. disregard message from malicious participant

Each vehicle store the CRL in its Tamper Resistant Module with which it checks the ID validation of other vehicles i.e., when a vehicle receives a message, it will check the sender's certificate validity. If the sender does not have a valid certificate, the message will be ignored as shown in Fig. 3. In other words, that particular vehicle will be completely revoked or blocked from the network

V. SECURITY ANALYSIS

In this section, we analyze how the previously proposed solution addresses the security requirements. Authentication of messages is provided by the digital signature of the sender and the corresponding CA certificate. This mechanism offers the guarantee that the message comes from a vehicle that is trusted and outsiders are not able to send messages to network members.

A. Simulation Environment:

Simulation experiments were performed to evaluate the performance of the proposed authenticated localization scheme. The simulation platform used is Network Simulator 2.35 (NS2), an open source event driven simulator. For the simulation purpose, a model of road in an area of dimension 2000×700 was designed using the simulation tool. Then nodes were deployed which actually represent the vehicles on road. Each of these vehicles are assumed to be equipped with a GPS receiver. But due to various reasons, some of these vehicles may suffer from GPS signal blockage and become unable to find their exact location. Hence there were location-aware as well as location-unaware nodes created in the simulation environment.

To meet the goal of authentication, RSUs were deployed on each side of the road. The trusted authority i.e., CA was not shown in the simulation since it has no direct concern in the course of action. However, its functionalities such as ID validation and CRL distribution were presented through its gateway RSU.

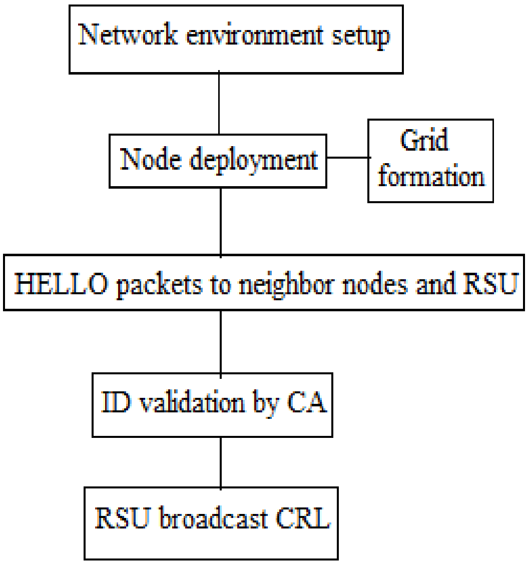

Fig. 4. FLOWCHART-CRL distribution

B. Analysis of Results:

Fig. 4 and 5 shows the flow of execution of simulation. Three cases were considered for the simulation. In the first case, after VANET formation and node configuration, RSUs were deployed. But, ID based verification and certificate revocation were not included. In this case, the network was unable to detect the presence of malfunctioning vehicles. They blindly communicate with each other and believe that whatever information they obtain from others was true.

In the second case, ID verification was performed, but there were no RSUs. Here, detection of malicious ones was found to be possible. However, it was observed that incorrect location information was propagated in the network, which means that timely revocation of malicious nodes is not feasible without RSU. Hence in the final case, both RSUs were deployed and ID based authentication was performed. This scenario was found to be optimal among the three cases.

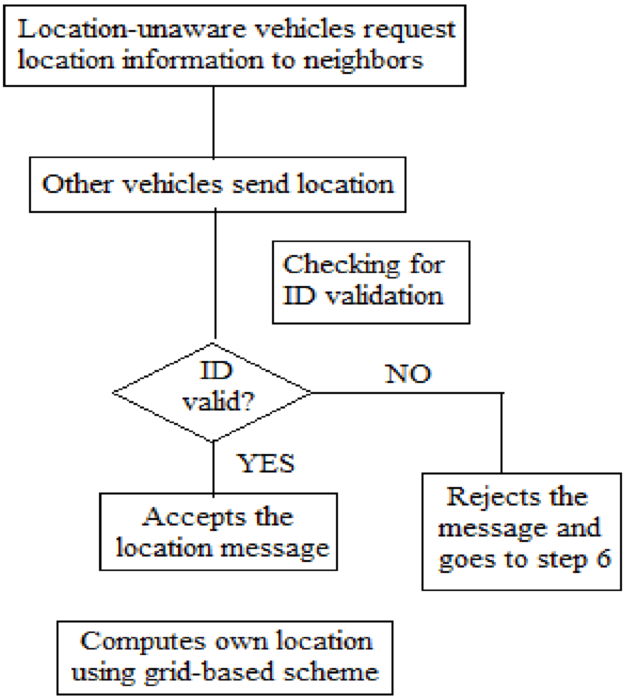
Location-unaware vehicles request location information to neighbors
Other vehicles send location
Checking for ID validation
ID valid?
NO
YES
Accepts the location message
Rejects the message and goes to step 6
Computes own location using grid-based scheme

Fig. 5. FLOWCHART-Authenticated location evaluation

In this case, it was possible to detect malicious nodes as well as to reject information from them. Also, it was observed that the location information that the valid vehicles share among them was more accurate.

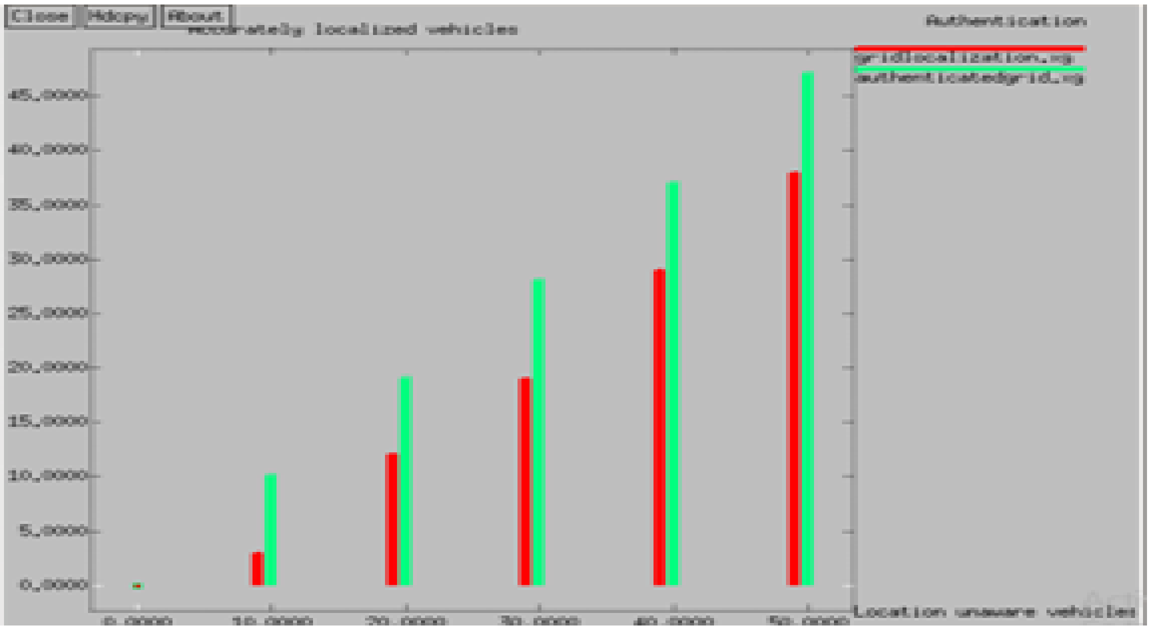

Fig. 6. Localization accuracy

To verify the efficiency of the proposed scheme i.e., to prove that the scheme is able to detect the presence of any malicious node in the network and to reject the message from them, comparative simulations were done between the localization with and without providing authentication. Fig. 6 shows the results of the comparison between authenticated and unauthenticated grid localization. Simulations were performed for various traffic densities by changing the number of vehicles. For a fixed number of location unaware vehicles, it is clear from the graph that more number of vehicles could find their location accurately when the proposed authentication process is carried out. The delay parameter was also compared between the above two cases for various distance between vehicles. The simulation result in Fig. 7 shows that the there is localization delay in authenticated scheme differs from the other in the order of only some milliseconds.

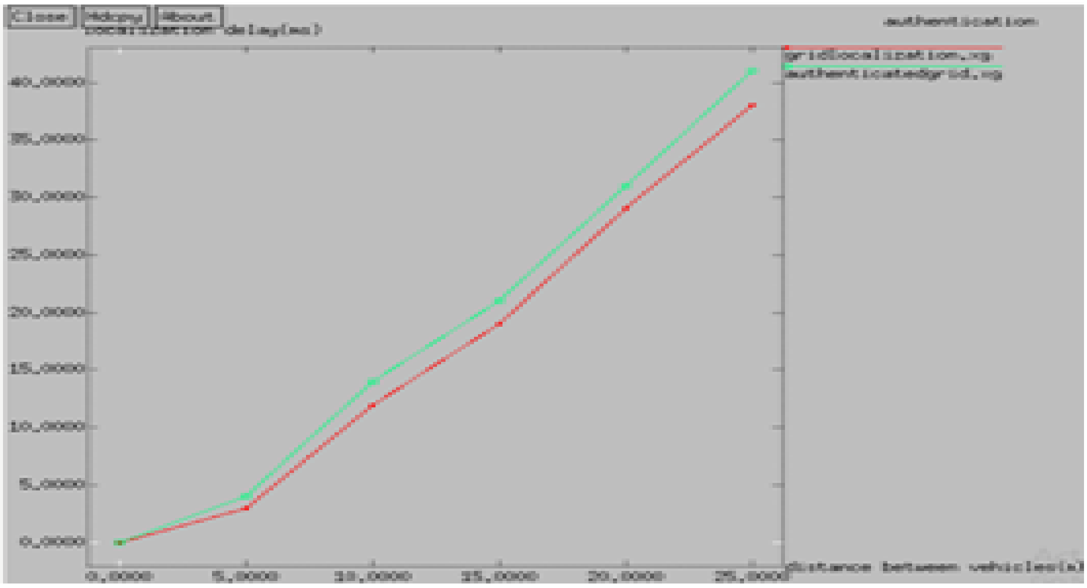

Fig. 7. Localization delay

VI. CONCLUSION

Positioning of a node VANET is one of the most interested research areas in recent years. To have a safe and fast transportation system, all vehicles should be aware of their positions and should know where a traffic problem such as a broken vehicle occurs. A GPS receiver inside the vehicle may not be always able to provide location information. In situations where GPS cannot receive satellite signals properly, the vehicles can use a GPS-free method like grid based localization to find its location. However, while using such a neighbor-dependent localization scheme, it should be ensured that all the data that are sent and received are authenticated. To achieve this, a new security based collaborative localization scheme for VANETs is discussed in this paper. Simulation of the proposed scheme shows that it is an effective solution against harmful attacks due to faulty and dangerous nodes in the network and hence it contributes towards the prevention of various transportation safety issues.

REFERENCES

[1] Tan Yan, Wensheng Zhang and Guiling Wang, "A Grid-Based On-Road Localization System in VANET with Linear Error Propagation",IEEE Transactions on Wirless Communications, Vol. 13, No. 2, February 2014.

[2] Y. Zhang, W. Liu, Y. Fang, and D. Wu, ”Secure localization and authentication in ultra wideband sensor networks”, in IEEE J. Sel. Areas Commun., vol. 24, no. 4, pp. 829835, Apr. 2006.

[3] Mahendra Kumar Jhariya, Piyush Kumar Shukla and Raju Barskhar. ”Assessment of Different Attacks and Security Schemes in Vehicular Ad-hoc Network”, International Journal of Computer Applications, Volume 98 No.22, July 2014, pp- 0975 8887.

[4] Rukaiya Y. Shaikh and Disha Deotale, ”Survey on VSPN: VANET-Based Secure and Privacy-Preserving Navigation”, Rukaiya Y. Shaikh Int. Journal of Engineering Research and Applications , SSN : 2248-9622, Vol. 4, Issue 10(Part - 5), October 2014, pp.01-05

[5] Maxim Raya and Jean-Pierre Hubaux, ”Securing vehicular ad hoc networks”, Journal of Computer Security 15 (2007) 3968, IOS Press.

[6] Syeda Khairunnesa Samantha and K. M. Azharul Hasan, ” An Approach for Alleviating the Starvation Problem in Road Side Units (RSUs)-based Vehicular Ad Hoc Networks (VANETs)”, International journal of communication technology research, Vol. 2, February 2012.

[7] Joo Han Song, Vincent Wong and Victer Leung, ” Poster: Secure Routing with Tamper Resistant Module for Mobile Ad Hoc Networks”, MobiHoc’03, June 1-3, ACM-2003, Copyright 2013 ACM.