International Journal of Security and Its Applications
Vol.9, No.12 (2015), pp.175-196
http://dx.doi.org/10.14257/ijsia.2015.9.12.18

Preserving Location Privacy in Location Based Services against Sybil Attacks

Amit Kumar Tyagi[1] and Dr. N. Sreenath[2]

[1]Research Scholar, [2]Professor
Department of Computer Science and Engineering,
Pondicherry Engineering College, Puducherry-605014, India
amitkrtyagi025@gmail.com, nsreenath@pec.edu

Abstract

With the rapid development of wireless technologies, Privacy of personal location information of a vehicle ad-hoc network (VANET) users is becoming an increasingly important issue. Services provided by Location based services to VANETs users can breached by Sybil attacks i.e. by malicious vehicles claim multiple identities at the same time. The prevention of these attacks, which could occur in or out of the Road Side Units (RSUs) coverage have a challenge to detect, as it should meet a compromise between the ability to identify the real identity of the malicious vehicle, and prevention of vehicle users from being tracked by malicious entities (i.e. unauthorized users). This paper propose a solution to prevent and detect Sybil attacks in VANETs. The identification of attackers is based on two types of authentication techniques. The first uses identification tags (for example: RFID etc.) embedded in the vehicle to authenticate them to the RSU and obtain short lifetime certificates. The second uses certificates to authenticate vehicles to their neighbors. The vehicular network is divided into different zones brought under the control of different certification authorities (CAs), forcing a vehicle to change its certificate when moving from a zone to another. One important characteristic of the proposed solution is that it prevents attackers from tracking the mobility of the vehicles. Avoiding false negatives is also addressed using observers (for example: software components in charge of monitoring) in vehicle nodes. A set of simulation scenarios also are conducted to evaluate the performance of the proposed solution. In last, this paper summarizes the comparison between our proposed approach and other various existed techniques to detect Sybil attacks in LBSs.

Keywords: *Location Based Services, Authentication, Sybil attack, Vehicle Identification Number, Vehicular Ad-hoc Networks, Privacy*

1. Introduction

Recently Vehicular ad hoc networks (VANETs) have emerged as a promising approach to increasing road safety and efficiency, as well as improving the driving experience. Vehicular Ad-hoc Networks have numerous applications, which aim to potentially improve the safety and efficiency of the road traffic systems. The fast advances wireless (mobile) devices and positioning technologies have led to the flourish of Location-Based Services (LBSs), *i.e.,* LBSs deliver information to a vehicle user based on his/her current physical location (for example: directions to a target location or a list of interesting, nearby places *etc.*,). The development of these networks has brought a number of security issues that are especially related to mobile and wireless communication, and user's privacy. Many forms of security attacks (For *e.g.*, Botnet [15], Man in middle attack, Sybil, *etc.*,) against VANETs have emerged which could impair the life safety, or loss of income for the implemented value-added services [4]. Among these attacks, Sybil attack,

ISSN: 1738-9976 IJSIA

which consists in sending messages with multiple forged identities [9]. A Sybil attacker could:

a) disturb the generation of routes when a multipath or geographic routing algorithm is used, by appearing in several places in the generated routes;
b) affect the results of data aggregation by contributing to the process of aggregation several times;
c) evade detection while behaving maliciously by spreading the actions he executes over the forged identities;
d) prevent the network from guaranteeing the fairness of resources by claiming several identities and receiving a high percentage of shared resources[11]. The latter behavior could be used to conduct denial of service (DoS) attacks if the nodes would be prevented from getting the resources they required.

In general, Location-Based Services (LBSs) can classified as; Position-aware and Location-Tracking Applications, Reactive and Proactive LBSs, Location-of-target and Target-at-location LBSs, Sporadic Queries, Self and Cross Referencing LBSs, Single and Multi-target, Content and Application-orientation, Outdoor and Indoor services [17, 27]. Market research firm ABI Research forecasts, the global number of people to enjoy location-based services from 1.2 million in 2006 increases to 31.5 million in 2011.

Location privacy: It is a particular type of information privacy. According to [17, 22], location privacy is defined as the ability to prevent other unauthorized parties from learning one's current or past location. In LBSs, there are conceivably two types of location privacy *personal* subscriber level privacy and corporate enterprise-level privacy. Personal subscriber-level privacy must supply rights and options to individuals to control when, why, and how their location is used by an application. With personal subscriber-level privacy, each individual has liberties to "opt in" and "opt out" of services that take advantage of their mobile location. Corporate enterprise level privacy is fundamentally different in that corporate IT (information technology) managers typically control when, why, and how mobile location capabilities provide application benefits to the organization as a whole.

Several techniques to protect from sybil attacks have been proposed in the literature (Refer: Table 1 and section VI). Some techniques used directional antennas to identify the position/direction from which messages are received [5] and matched the power of the received signal with the position claimed by a node to detect datagrams sent from the same node. Such a technique shows a high degree of inaccuracy and would generate a high ratio of false positives. Resources testing [12] is also used for the detection of sybil attacks, assuming that a single node, which is simulating multiple entities, will exhibit several resources limitation related to computation, storage, and bandwidth, and will be unable to send messages with different forged identities at the same time. Other approaches have based their solutions on the use of public key cryptography (PKI) by authenticating every vehicle with its private key. For authentication purposes use asymmetric key concept in this paper. *Using asymmetric key based authentication because it is widely adopted because of the separate keys used for encryption and decryption.* In this context, authors in [3] assumed that the road side units broadcast a tamper-free digital signatures with timestamp and vehicles have just to analyze the differences of its neighboring nodes' signature vectors with the already received one. In addition, such solution do not preserve the privacy of vehicles. Such solution is hard to use in VANETs because vehicles could be out of coverage of RSUs and will not able to detect Sybil node. In [10], a spatial and temporal correlation, which could be observed when vehicles pass by RSUs and obtain timestamped message, is used to detect Sybil Attacks. The idea is based on the fact that two different nodes, which are requesting certificates from multiple RSUs, could not move across these hotspots RSUs at the same time, unless it is the same vehicle which is generating several requests with different forged identities. However, this solution requires to deploy RSUs beyond road

intersections, to prevent vehicles, which stop there, from forging timely spaced timestamp requests. In [13] a privacy preserving scheme to detect sybil attacks in VANETs is proposed. This solution uses a pool of pseudonyms which are carefully hashed to a common value related to the real identity, and only known by the road side units. This allows RSUs to detect if the same vehicle used forged pseudonyms. However, vehicles should wait to cross RSUs in order to be informed about sybil nodes.

Location privacy protection is the method that sends the false location information or anonymous identity and location information to the server in the location service. These methods can be divided into two categories: one is to protect the user's ID information (conceal anonymity or pseudonym), making the server service does not know the requestor true ID; the other is to protect the location information of the user by submitting a region instead of true location of the user. Existing methods, such as pseudo-location method, pseudonym method, k-anonymity method and other methods based on it, such as personalized k-anonymity, have some defects which will reveal the location privacy [14]. For example: CARAVAN approach [26] from Sampigethaya [16], is another scheme to create user-centric mix zones by using cluster-based communications. Due to vehicle mobility, vehicles tend to form clusters while driving, *i.e.*, several vehicles travel at same speed and keep same distance to each other, especially on highways. The CARAVAN approach exploits this property by grouping vehicles into clusters and letting one of the vehicles in the group act as a proxy for the group members for anonymous communications with entities outside the group. Hence each group forms a virtual moving mix zone. Currently, there is no universal location privacy mechanism that has reached a consensus in the privacy community.

This paper proposed an identification based solution (for example using RFID etc. devices) for the detection of sybil attacks in VANETs. The proposed solution assumes that the network is divided into several zones, where every zone contains several RSUs and one of them is selected to be the controller of the zone (in that case, it will be called a Road Side Controller (RSC)). Every RSC is attached to a certification authority (CA) and vehicles are required to change their certificates from a zone to another. Two types of authentication techniques are used. The first is based on the use of active identification tags embedded in the vehicle to securely authenticate them by RSUs and obtain short lifetime certificates. The second is based on the use of those certificates by vehicles so that they can be authenticated to their neighbors. The solution allows to detect Sybil attacks occurring in or out of the RSU coverage thanks to the use of observer components deployed in the vehicles. To avoid false negatives related to attacks occurring out of the RSU coverage, a set of observers are integrated to the vehicles, RSUs, and RSCs and are in charge of collecting, exchanging, and analyzing history of data related to sensitive events. A set of simulation scenarios are conducted to evaluate the performance of the solution. Figure 1 and Table 1 provides the summary of Sybil attack detection techniques.

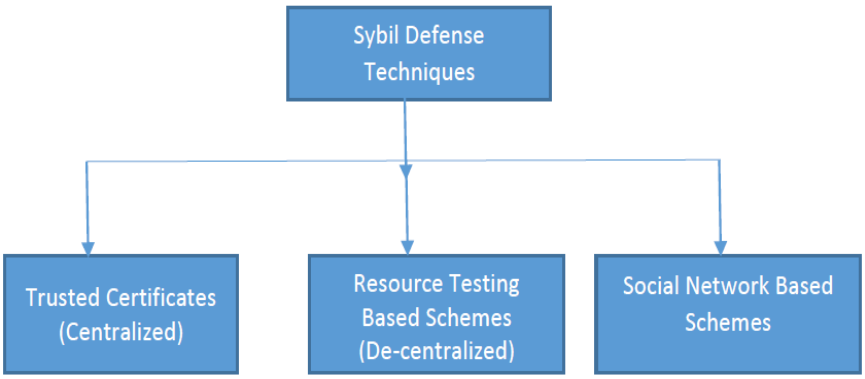

Figure 1. Categorization of Sybil Defense Techniques

The main contribution of this paper is four-fold. First, thanks to the use of identification tags in vehicles, which should contain the Vehicle Identification Number (VIN), RSUs and RSCs can always authenticate, the moving vehicles in the network whenever they go across the hotspots, and prevent unauthorized users from getting access to such an identity. During authentication, the privacy of these vehicles is preserved since the VIN contained in the tag (which is nothing but the Electronic Product Code of the tag) is never transmitted within the vehicular network nor between the identification reader and the vehicle tag. Second, the proposed solution prevents attackers from tracking vehicles as they change their identities from a zone to another and request new certificates from the first crossed RSUs in new entered zone. Third, the proposed detection mechanism is distributed among RSUs and observers in the vehicles, allowing to reduce the overhead in the RSUs and detect attacks beyond its coverage. Fourth, the detection of the sybil attack, as well as the identification the attacker is instantaneous, allowing a quick response to the attack. Now a basic introduction about location privacy is defined in next paragraph.

The rest of this paper is organized as follows. Section II describes the requirements related to an efficient detection of sybil attacks, and the architecture of the proposed VANET. Section III is related to certificates management. It also describes the role of observers. Section IV demonstrates that "How Sybil attacks are detected". Section V presents the simulation results. Then, Section VI discusses about related work about this work. Finally last section VII concludes this work in brief. This paper uses the terms certification authority and trusted authority; mobile users and 'VANET users' or vehicle users; vehicle intruders and malicious users interchangeably.

2. An Efficient Detection of Sybil Attacks in LBSs to Protect Vehicle Users

This section present the requirements to be fulfilled by the solutions proposed to detect sybil attack and the architecture. In addition, this work describe the role and objectives of used observers in the proposed architecture.

A. Requirements for Sybil Attacks detection

In this section, a set of requirements that should be fulfilled to protect VANETs from Sybil attacks.

First, certificate-based solutions and public key infrastructures were proved to be an efficient solution toward the prevention of Sybil attacks in mobile networks. To be efficiently used in VANETs, the certificates should not show the real identity of the vehicles to preserve their privacy. Even if the used certificate would only show the pseudonym of the vehicle instead of its real identity, the latter should be renewed every short-period of time to prevent attackers from tracking the user and compromising the vehicle security. However, as certificates renewal would generate an additional overhead, the solution to develop should come to a compromise between drivers' privacy and protection from Sybil attacks [13].

Second, when renewing their identities by requesting new certificates, vehicles should be accurately and rapidly identified, preventing them from creating several requests at the same time to obtain multiple identities from the same RSU. While such a malicious behavior could be detected if two certificate requests have the same timestamp, false positives could be generated. In fact, if the RSU is deployed in road intersections, it could allow a malicious vehicle, which stops close to the RSU, to generate multiple and timely spaced requests and consequently to receive several valid certificates. Therefore the solution to develop should take into consideration the need for defining the RSU positions and prevent vehicles from obtaining multiple valid certificates to prevent them from generating Sybil attacks. In this context, the use of an accurate localization technique in

addition to vehicles identification could make the solution enough efficient. The use of RFID systems, for example, was proved in the literature to be an efficient solution toward vehicles identification and localization [8].

Third, in several solutions the detection of Sybil attacks is delayed until the user behavior over a period of time is analyzed. Such an analysis could be based on detecting groups of vehicle identities which disappear at the same time when some vehicle goes out of transmission range, or by looking for sets of identities that always go through the RSUs at the same time interval. However, even if the Sybil attack is detected by identifying identities that belong to the same vehicle, the distinction between forged identities and the real identity of the attacker is not always possible. In VANETs, given the sensitivity of the used applications, providing an efficient solution for the protection of VANETs from Sybil attacks, as well as the rapid and accurate identification of the real identity of the malicious vehicles, is a requisite.

Fourth, as in VANETs nodes communicate with each other via multi-hop paths, several important Sybil-related events could not be detected if they occur out of RSUs transmission range. However, These RSUs are typically able to perform an efficient detection of Sybil attacks as they are allowed to track vehicles, generate and maintain voluminous traces of relevant events, and get access to sensitive information (For example: Encrypted certificate requests and their history of generation and use).

While these events could not be detected by intermediate nodes in the network, when the attacker is out of the transmission range of RSUs, the detection of certificate reuse and forged identities (for which no valid certificate is available) could be performed by these intermediate nodes allowing them to complement the activity of the RSUs. Therefore, the security mechanisms to use for the prevention and detection of Sybil attacks should follow a distributed approach by cooperating RSUs and vehicles in the network to allow a rapid and localized detection of malicious vehicles, and a cost-effective reaction against them [2].

B. Proposed Location Privacy Architecture

As discussed in section I, Vehicular Ad-hoc Network using service of location based in real environment. And VANETs have received a great deal of attention for their promises in revolutionizing the intelligent transportation systems and telematics services. In a general setting, a VANETs is composed of three components: on board units (OBUs) equipped in mobile vehicles, fixed roadside units (RSUs), and a central trust authority (TA). Each definition can describe as [17, 22]:

a) *TA (certified trusted authority):* TA is in charge of the registration of immobile RSUs at the road side and mobile OBUs equipped on the vehicles, and can reveal the real OBU identity of a safety message by incorporating with its subordinate RSUs. The TA is assumed powered with sufficient computation and storage capability.
b) *RSU (road side unit):* The RSUs are subordinated by the TA, which hold storage units for storing information coming from the TA and the OBUs. The main tasks of RSUs are (1) issuing a short-time anonymous public key certificate to each OBU when the OBU requests, and (2) assisting the TA to efficiently track the real OBU identity of any safety message.
c) *OBU(on board unit):* The OBUs are installed on the running vehicles, which mainly communicate with each other for sharing local traffic information to improve the whole safety driving conditions, and with RSUs for requesting the short-time anonymous public key certificate.
d) *RSC (road side controller): a RSU only,* but have the different functionality from the RSU. For example in this paper, a VANET‘s user area (for example: a zone to mix the network inside it i.e. provide certificate inside this zone to protect privacy from untrusted vehicle/mobile users) which is divided into a set of zones. A zone

stands for a network area which is covered by a set of RSUs, whose communication ranges do not overlap. In every zone, one of these RSU is elected to generate and deliver security credentials to vehicles, and to collect and analyze observation data regarding security violation in the zone. Such an RSU will be denoted in this paper by a Road Side Controller (RSC).

Generally, a RSC can be elected based, for example, on one of the following criteria: a) the middlemost RSU; b) the most visited RSU when vehicles enter to a new zone; or c) the least overloaded RSU based on statistics generated over a learning period. In this, every vehicle is equipped with one tamper-proof device (for *e.g.*, RFID tag), which includes the Vehicle Identification Number, allowing the RSUs to authenticate vehicles using radio frequency transmission. One or many tamper-proof devices readers are attached to every RSU, and are deployed on roadsides in the positions where the signal sent by the hotspot RSUs starts to be received by the moving vehicles. The tag of every vehicle which enters to a new zone will be read by the deployed identification device readers attached to the RSU of that zone. A reader is attached to a database (DB) from which it extracts useful data to authenticate the tags.

A lightweight privacy preserving authentication protocol is used for that purpose in order to preserve the privacy of the vehicle identity and protect it against any unauthorized tracking and modification by other vehicles. A protocol such as EPCglobal Class 1 Generation 2 could be used [6]. This protocol uses a secure EPCglobal Class-1 Gen-2 RFID System (Refer: section VI). Thanks to the use of 32-bit pseudo-random numbers generated at the RFID tag, the RFID reader and the back-end server, the EPC (Electronic Product Code) of the tag remains hidden. From the read messages, the back end server tries all the pre-configured EPC to compute again the exchanged EPC and identify the used tag. Even if the computation overhead is high, trying all the pre-configured EPCs would protect against eavesdropping and information leakage, since a reader, which is not authenticated by the backend server, is unable to determine the EPC of the tags. In addition, it protects against impersonation and replay attacks as the values emitted by the tags change from a session to another. Moreover, it is secure against tracking unless the attacker knows all EPC of the tags, which represents a hard assumption.

The RSUs provide secure over-the-air services to the remote on-board units (OBUs) in vehicles. Despite the fact that vehicles can be authenticated by RSUs using their tags, digital certificates are also used to authenticate vehicles to their neighbors and RSUs of the same zone. In this context, a Certification Authority (CA) is attached to every RSC, and nodes are forced to change their certificates from a zone to another. The RSUs are in charge of authenticating vehicles and forward the certification requests (generation, renewal, and revocation) they generate to the RSC. Additionally, RSUs collect and send to RSCs observations regarding security events to detect sybil attacks. Each RSU is pre-configured with a certificate generated by the Certificate Authority of its zone. In addition, each vehicle is pre-configured with the set of root certificates related to the different CAs of the network. It is assumed that the growth of the number of vehicles connected to the network will lead to the increase of the number of RSUs and not RSCs. Therefore, the number of certificate authorities will be affected. Since CAs are responsible for the generation of RSUs and vehicles certificates, it is not possible for an attacker to create a rogue RSU and induce vehicles to receive forged certificates.

Every group of RSUs of the same zone are connected through a roadside backbone to the RSC to exchange observation and certificate requests, and distribute reports related to detect sybil attacks. In the same manner the different RSCs are connected together to exchange information related to the generated certificates, and aggregated observations and reports. An RSU sends periodically a WAVE Service Advertisement (WSA) providing assurance that a legitimate service is being announced. Vehicles will use WAVE Short Messages (WSM) to communicate with the RSU. The example provided in

Figure 2 shows a road-map divided into two zones. In the first zone A, there are two RSUs (RSU1A and RSU2A), while in the second zone B, there are two RSUs (RSU1B, RSU2B). RSU2A and RSU2B represent the RSCs of zones A and B, respectively, and each one of them is connected to a certificate authority. In inter-zone roads, vehicles could use certificates of old zone and should check the validity of the certificates of encountered vehicles coming from the new zone. For example, vehicles moving from zone A to zone B toward RSU1A will use the certificate generated by RSCA, while vehicles moving from zone B to zone A toward RSU1B will use the certificate generated by RSCB. Vehicles crossing the road between RSU1A and RSU1B could have certificates generated from two different certificate authorities, and should be able to check the validity of all signed messages.

C. Observing Security-Related Events

To detect security attacks occurring out of RSUs coverage, and collect security related information useful to determine sybil nodes, an observer component is attached to every vehicle, RSU, and RSC.

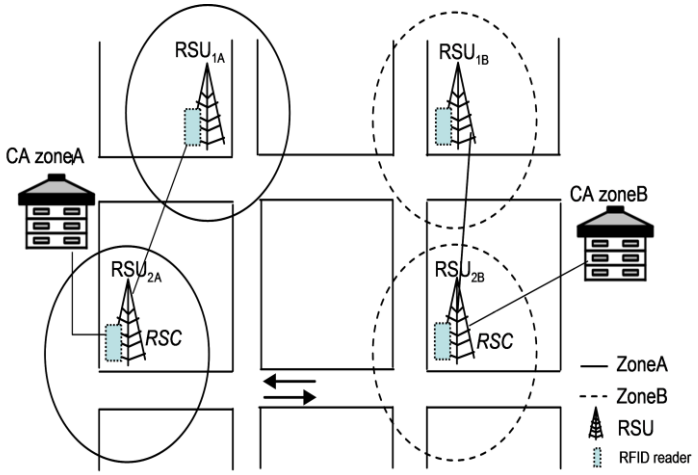

Figure 2. Proposed Architecture

Observers in vehicles are active only in inter-zone roads. They are in charge of following actions:

a) sending certificate generation requests to the first crossed RSU of the same zone;
b) reception of certificate revocation lists from RSUs;
c) authentication of neighbors based on signatures of the received messages;
d) generation of reports about used certificates in inter-zone roads;
e) delivery of the generated reports to RSUs;
f) detection of sybil attacks i.e. multiple request from same vehicle at same time (in same zone or different zone).

Observers at each RSUs are in charge of following actions:

a) collecting the identities of vehicles becoming in the coverage of their hotspots, together with timestamps of entry and exit to the covered area;
b) identifying new vehicles entering to the zone, they belong to, for the first time; b) checking signatures of received messages from the vehicles;
c) collecting messages exchanged between neighbors and checking the validity of their signatures;
d) forwarding to the RSC requests for new certificates, received from new incoming vehicles
e) sending to vehicles the list of revoked certificate;

f) collecting reports generated by vehicles about detected sybil attacks in uncovered area.

Observers in RSCs are in charge of following actions:

a) reception of certificates generation requests sent by vehicles;
b) communication with the certificate authority of the zone to generate, renew, or revoke certificates to vehicles;
c) storage of a timestamped list of generated certificates for each zone;
d) exchange of collected reports forwarded by local RSUs with RSCs of neighbor zones,
e) analysis of vehicles reports to detect Sybil attacks;
f) generation of certificate revocation lists (CRLs);
g) communication of the generated CRLs to the RSUs of the same zone.

When vehicles are in roads interconnecting two different zones, observers collect data history about the certificates used by neighbors in the inter-zone area. These data will be delivered to the RSC through the next crossed RSU. The RSC will correlate the received observations with the certificate data history to detect Sybil attacks. Each entry in this table contains five information:

a) The last used certificate by the vehicle,
b) The last visited zone by the vehicle,
c) The list of neighbor vehicles,
d) The certificates used by neighbor vehicles;
e) The timestamps of all events which were executed by neighbors and required for the use of certificates.

Hence this section dealt with working of observers. Next section discusses about management of certificates among vehicle users.

3. Certificates Management between Vehicle Users, RSUs, RSCs, and TAs

This section presents the certificates delivery, revocation and renewal processes following as:

A. Certificates Delivery

When the vehicle enters to the coverage area of an RSU, the latter authenticates it after securely reading its tag. If the vehicle is visiting the zone to which this RSU is attached for the first time, it generates a temporary identity to be used in the new zone, a pair of private/public key, and the related Certificate Signing Request (CSR), encrypts them together with the vehicle tag's EPC using the public key of the RSU, and sends the obtained content to the RSU. Even if a vehicle tries to perform a man in the middle attack or replay attack *etc.*, the RSU will detect such behavior. In fact, even if the attacker sends a certificate request on behalf of the victim, no certificate will be generated as the claimed EPC is not authenticated by the Identification device (or vehicle's reader) of the crossed RSU (the attacker, which could be a malicious vehicle, is unable to access to the plain content of EPC). In addition, the vehicle is able to verify the signature of authenticated RSU response using the root certificate embedded in the vehicle. To preserve the vehicle privacy and prevent neighbors from tracking the vehicle from a zone to another, each vehicle uses a temporary identity in the generated certificate, and only the RSU is able to find the relationship between the EPC of the vehicle, and this identity.

Consequently, even the attacker possesses stationary radio receivers, places a receiver at each interconnecting crossroads, and tracks a vehicle by its certificate within a zone, it is not able to track the victim in other zones since there are no relationship between temporary identities in the certificates generated to the same vehicle. Hence the attacker

could be able to violate privacy. So to prevent a vehicle from generating several certificate requests, the RSUs expects that each request is followed by an identification device (for *e.g.*, RFID) authentication of the tag. In addition, the RSUs are able to differentiate between the renewal of the same certificate and the request for a second certificate at same time in same zone (this situation will be discuss in Subsection III-C).

After receiving the vehicle certificate request, the RSU decrypts and authenticates it, and checks whether the vehicle identity in that request has been recently read from its tag when it entered the zone. If it is the case, the RSU sends the request to the RSC. The latter creates a new identity to be used by the vehicle in the current zone. After that, it generates an X.509 certificate and sends it back to the vehicle through the RSU. The generated certificate is characterized by a short validity time, which is chosen with respect to the vehicle's mean time of stay in a zone (computed starting from the history data collected by observers in the RSUs), an issuer equal to the certificate authority in the RSC, and a subject corresponding to the vehicle identity generated by the RSU. The Common Name of the issuer of this certificate will also contain the identity of the zone to which the vehicle is attached. The use of the Timestamp field in the certificate request, together with the real vehicle identity, allows the RSUs, which receives two certificate requests, to detect whether it is the same vehicle which is sending these requests at the same time, or these requests are received from two different vehicles that are very close one to other.

Every RSU, which is neighbor to other RSUs of different zones, broadcasts the root certificates of the certification authority of those zones. Before leaving a zone, a vehicle receives the root certificates of potential neighbor zones by the last crossed RSU. In fact, in the roads that interconnect two zones together, a vehicle of the first zone would be required to authenticate a vehicle coming from the second zone. If the latter has not yet reached the RSU of the first zone, it will keep using its current certificate.

B. Certificates Revocation

As a vehicle moves from one RSU to another (and obtains new certificates whenever it enters new zones), it could return back to a visited zone in a short period of time. Consequently, if the certificate that it obtained in the last visit to that zone is still valid (has not expired or revoked yet), and if the new certificate is automatically delivered without checking the expiration time of the last generated certificates, the vehicle becomes a holder of two valid certificates. Consequently, it becomes able to conduct a Sybil attack as it holds the two certificates generated with two different identities. Therefore, to protect the VANET against such a malicious behavior, prior to generation of a new certificate, the old certificate should be revoked if it is still valid, and a new CRL or Delta-CRL (Delta-Certificate Revocation List) should be generated and forwarded to vehicles in the same zone. The use of Delta-CRL is chosen to prevent overloading the network with too large CRLs. (*Note that*- the delta-CRL represents an update of the last generated complete CRL). When a vehicle enters a new zone, or starts to communicate, it may receive a delta-CRL for which it does not already have the last complete CRL. To cope with this situation, the vehicle asks the first encountered RSU to receive an updated version of the CRL.

C. Certificates Renewal

It may happen that a vehicle remains in the same zone for a long period of time exceeding the certificate lifetime. In that case, its certificate should be renewed in the zone to which it is connected. Note that, all generated certificates have the same validity period, which could be pre-defined according to the road map area and the network characteristics (Refer: Subsection V-B). Two situations are distinguished for certificate renewals.

The first situation happens when the current certificate has expired. In that case, the vehicle will request a new certificate after entering under the RSU coverage and authenticating itself using its identification device tag. When choosing the new lifetime period, the RSC should come to a compromise between: a) choosing long lifetime period which avoid renewing the certificate frequently, but may show the need to revoke the certificate if the mobile exists and goes back to the same zone while its certificate is still valid; and b) choosing a short lifetime period which avoids revoking the certificate, but leads the mobile to generate several renewal requests for the same certificate. To settle the validity period of certificates, the RSC should exploit the data history collected from RSUs regarding the vehicles mobility (i.e., entry time and exit time to and from RSU coverage) to compute the mean period of time elapsed by the vehicles in a zone. It should also take into consideration the road map of the zone and the length of uncovered inter zone roads.

The second situation is related to the case where the first certificate has not expired. In that case, the renewal request will be signed by the current private key, it will be sent directly to the RSU, or forwarded through neighbor nodes if the vehicle is out of the RSU coverage. The renewal of the certificate consists in the generation of another certificate which has a new serial number and lifetime period, but contains using the same vehicle identity.

Hence this section dealt with the certificates delivery, revocation and renewal processes. Now next section discusses about detection of Sybil attacks using proposed detection mechanism.

4. Detecting Sybil Attacks

The attacker could perform several forms of sybil attacks, either when it is under the coverage of an RSU or not. The first form of a Sybil attack consists in using a certificate related to another zone. The neighboring vehicles will receive a broadcast message from the attacker which can be authenticated using a certificate related to another zone. Consequently, they detect a potential occurrence of a sybil attack due to a tentative of using another identity. A report containing the temporal identity of the Sybil attacker extracted from vehicle certificate, together with the timestamp of the event occurrence, will be generated and sent to the RSUs. The report is generated each time that a sybil attack occurs and is forwarded to the nearest RSU by the vehicles that detected the event. The number of related reports sent to the RSU is equal to the number of detected attackers.

Although the sybil attack occurs when the vehicle uses several identities in the same time, this behavior could be detected since each vehicle has a certificate. However, since the vehicle could obtain several certificates during navigation, two situations should be distinguished:

a) the vehicle is conducting a sybil attack using a certificate already generated in the current zone together with the certificate generated in another zone;
b) the vehicle has not obtained a new certificate, yet, due to the characteristics of the network (the vehicle went through an uncovered area);
c) the vehicle has not detected the first RSU of the new zone;
d) some communication problems in reading its tag have occurred;
e) intersection of vehicles at different points increase request of certificates from both zone (existed and future one);
f) if same vehicle request for certificate (for authentication) from RSU and neighbour vehicles also;
g) if a vehicle present for a long period in same zone, then it can request of another certificate (after telling a lie about expiration of previous certificates);

h) if the certificate that it obtained in the last visit to that zone is still valid (has not expired or revoked yet), and if the new certificate is automatically delivered without checking the expiration time of the last generated certificates, the vehicle becomes a holder of two valid certificates. Consequently, it becomes able to conduct a sybil attack as it holds the two certificates generated with two different identities.

To avoid false positives, the RSU forwards the alert to the RSC, to check whether the vehicle has already obtained neighboring RSU whether the vehicle has received this new certificate. If yes, the RSU confirms the occurrence of the sybil attack and generates an alert to be broadcast through the attached RSC to all RSUs of the network. The detection of this attack would be instantaneous and easier if the attacker executes this attack under the coverage of an RSU. The second form consists in using a valid certificate in the current zone. In fact, the attacker could exit a zone, say Z1 (from which he has obtained a certificate C1), and obtain a new certificate C2 from the next accessed zone Z2. Later, he returns back to the first zone Z1 before his certificate C1 has expired and obtains again a new certificate C2. Consequently, the vehicle would have two valid certificates C1 and C2 in the same zone. Typically, as the RSU should have generated the revocation request related to C1 before it generated C2 and broadcast the new delta CRL to all vehicles in its zone, if a sybil attack is executed by the vehicle which authenticates itself using certificate C1, all neighbor vehicles would detect the attack and deliver their reports to the next crossed RSUs. However, a example of sybil attack could occur in the road separating the zones Z2 and Z1, in which vehicles may be moving in both directions, and therefore they may authenticate themselves using certificates from zones Z1 and Z2. In this situation, the attacker could communicate with different identities using certificates C2 and C1 and become able to conduct a Sybil attack.

We remind that observers in the vehicles collect the list of used certificates together with the timestamp of the events, and deliver them later to the first crossed RSU. As RSUs forward these reports to the RSC, the latter, which keeps track of all generated certificates, will notice that certificate C1 is used in the network after certificate C2 was generated, and will make sure that these certificates are related to the same vehicle identification number. In that case, an RSU will be able to detect this form of Sybil attack. As a response to the attack, the RSC revokes any valid certificate already delivered to the vehicle. It also generates an alert containing the vehicle identification number, and sends it to the neighboring RSCs in the network, which also forward that information to their RSUs. Each one of the RSU will deny delivering any new certificate to that vehicle once it is authenticated by its identification device tag. It is assumed that the response to the Sybil attacks performed when vehicles enter under the coverage of a new RSU and one false identity at maximum can be used by a Sybil attacker until the revocation process is performed. *Now as a major drawback of pseudonyms changing* (or certificate exchanging) for authentication is that they are vulnerable to attacks by adversaries with background knowledge. Over time as the background knowledge of the adversary increases privacy provided by pseudonyms decreases. For example, consider the situation where an adversary observes that a user visits the same car park at night when there are only a few other cars parked. By colluding with the server, the adversary is able to identify a smaller set of pseudonyms in which the user's pseudonym is included. It is expected that over time the adversary will be able to correctly identify the user's pseudonym. So in order to overcome the degradation of privacy of pseudonyms over time, the pseudonyms (or certificates) need to be changed at regular intervals. A procedure to achieve this problem's solution in explained in our proposed system.

5. Experimental Results via Simulation

This section describe the simulation model and the simulation results.

A. Simulation Model

We used the traffic simulator SUMO (Simulation of Urban MObility) [7] together with NS2 (Network Simulator, version 2.35) in order to generate mobility traces of vehicles and simulate VANETs communication, respectively. The MOVE tool (Motor Vehicle Emission Simulator) [1] was also used to convert SUMO traffic traces into NS2 compatible traces. We enhanced NS2 with new agents dedicated to the simulation of certificates generation, renewal, revocation, and management. We considered a network area of 5*3 km^2, showing a road map composed of a set of urban zones interconnected by freeways.

As shown in Figure 3, each freeway is composed of three way streets for incoming vehicles and three-way streets for outgoing vehicles. In addition, each urban zone is in the form of a grid composed of horizontal and vertical three-way streets, allowing vehicles to move according to the Manhattan mobility model. The length of every urban road is equal to 500 meters. Two RSUs are deployed in every urban zone, each one of them has a coverage radius equal to 250 meters. These RSUs cover all the crossroads used by vehicles to enter or exit the urban zones. The surface covered by RSUs, for each urban zone, does not exceed 25% of the zone area. The simulation period is set to 8000 seconds, using a time slot equal to 1 second. As long as vehicles move inside the same zone, or from a zone to another, certificates are renewed, generated, or removed.

B. Experimental Results

Since the protection against Sybil attack is based on the use of certificates, the aim of the first simulation is to show the ratio of revoked certificates (*i.e.*, Rc), and the ratio of renewed certificates (*i.e.*, Rn), in terms of certificates lifetime. We consider that the total cost (i.e. Cc) associated to the use of certificates is equal to (2 * Rc + Rn) = 3. The Rc value is considered two times the equation, since a certificate revocation requires the generation of a CRL, and in other proposed solution, a revocation is immediately followed by a generation of a new certificate to the mobile that entered the new zone. We only focus on the cost related to the execution of cryptographic functions by which the RSU generates certificates or CRLs.

Even if a CRL requires to be broadcast several times to keep its alive, leading to an additional traffic overhead generated by the RSU, the cost associated to such broadcast is supposed to be negligible with respect to the cost associated to the execution of cryptographic primitives. The chosen maximum speed of vehicles is equal to 13.88 m/s (corresponding to 50 km/h) in urban areas and 25 m/s (corresponding to 90 km/h) in freeways. We conducted the simulation using 100 mobile vehicles, and a certificate lifetime ranging from 500 sec to 5000 sec.

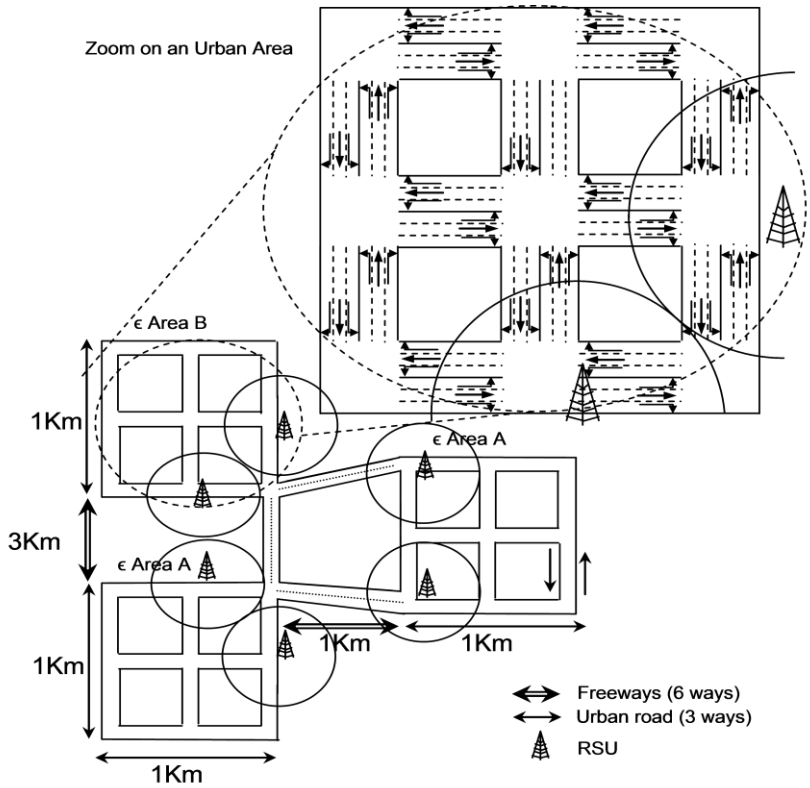

Figure 3. Topology of the Simulated Network

As depicted in Figure 4, the more is the validity period of certificates, the higher will be the ratio of revoked certificates. In fact, as the lifetime of a certificates increases the probability that vehicles go out of a zone and return back to it with a valid certificate in that zone will increase. In addition, as the validity period of certificates increases, there will be a much likelihood of having vehicles which renew their certificates in the same zone. Consequently, the ratio of renewed certificates will decrease. In the opposite case, as long as the certificate lifetime exceeds 1800 seconds the ratio of revoked certificates becomes greater than the ratio of renewed certificates. In fact, using short lifetime certificates, a vehicle would not go out and return back to the same zone while the certificate it previously get in that zone is still valid. In the simulation results depicted by Figure 4, the certificates renewal ratio is equal to the certificates revocation ratio when the certificate lifetime sis equal to1800 seconds, which represents the most convenient value for the considered vehicle speed and network topology.

In the second simulation, we estimated the revocation and renewal ratio of certificates according to number of vehicles and the maximum vehicles speed. The results of this simulation are depicted by Figure 5 and 6, respectively. The lifetime of generated certificates is set to 1800 seconds where the certificate revocation ratio is equal to the certificate renewal ratio. We varied the number of vehicles from 10 to 100. We conducted the simulation for three pairs of urban/freeway speed: 40-80 km/h, 50-90 km/h and 60-100 km/h.

As depicted in Figure 5, the more is the vehicle speed, the higher will be the ratio of revoked certificates as vehicles would cross quickly several zones (*Note here, three pairs of urban/freeway vehicle speeds are considered).* In addition, as the speed in urban area and freeways increases, the peak of revocation ratio will be observed for a smaller number of vehicles. In fact, when we increase the speed and number of vehicles, a congestion will occur quickly in the network and vehicles will progressively stop moving, leading to the decrease of the number of revoked certificates.

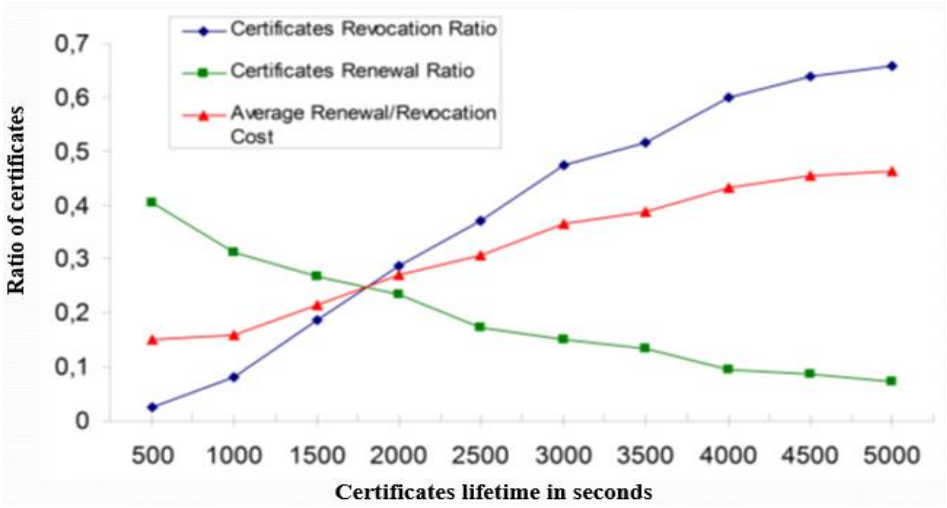

Figure 4. Ratio of Revoked/renewed Certificates and the Related Average Cost vs Lifetime of Certificates

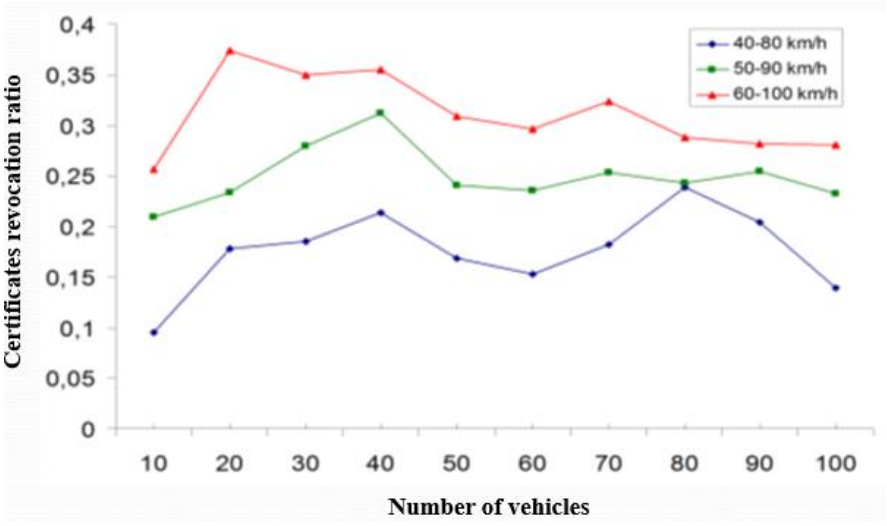

Figure 5. Ratio of Number of Vehicles vs Revoked Certificates

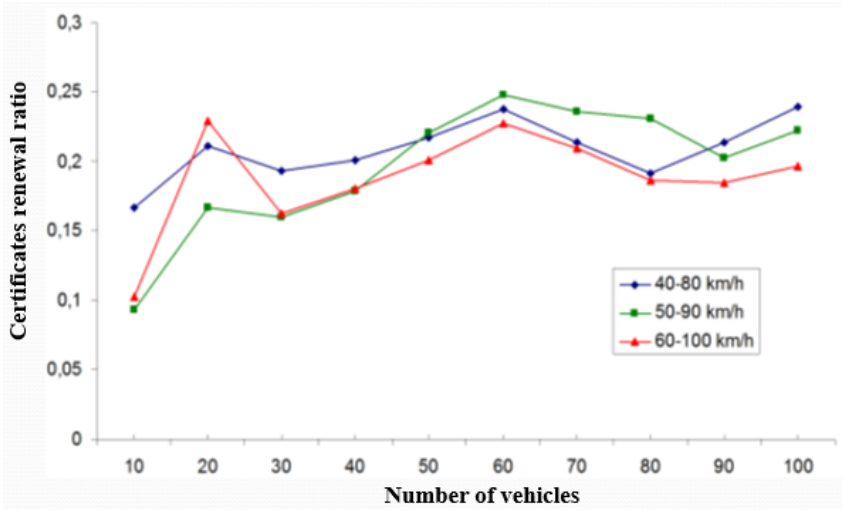

Figure 6. Ratio of Number of Vehicles Renewed Certificates

For a pair of speed equal to 60-100 km/h, starting from 20 vehicles, the network becomes congested, while for a pair of speeds equal to 40-80 km/h, the road congestion starts from 40 vehicles. Note that the road congestion depends only on the architecture of the used road system, and could, for example, be decreased using wide roads. Figure 6 shows the ratio of certificates renewal in terms of number of vehicles, for three pairs of vehicles speed. That ratio increases as the number of vehicles increases from 10 to 60, and starts to decrease after the value 60. In fact, as the density of vehicles in the network increases and the speed of vehicles increases enough, the network becomes congested, leading vehicles to stop moving. If the network area had been totally covered by RSUs, the ratio of renewed certificates would have increased, because the vehicles remain under the coverage of the same RSU. However, we remind that in this simulation only 25% of the network is covered, and vehicles could stop due to congestion in the uncovered zones. This would explain why the ratio of renewed certificates decreases starting from 60 vehicles. In addition, for a high number and speed of vehicles, the revocation ratio decreases considerably due the fact that a congestion will occur quickly in the network.

6. Related Work

Bo Yu *et al.*, [20] presented an integrated scheme to detect Sybil attack in vehicular ad-hoc network. In that detection method they use 1) cooperative detection method in which each node cooperates to detect Sybil node. In this cooperative detection method each node periodically perform three roles a) claimer b) witness c) verifier after performing verification from the verifier, the node is able to detect a Sybil node. In cooperative detection method they estimate the position of the node using Received Signal Strength (RSS).This method did not work well because if witness itself is a Sybil node then result may not be accurate. To overcome this problem they consider that the vehicles coming from opposite direction may be trusty witness, to identify traffic of opposite direction they give 2) presence evidence system for identification of vehicles going on opposite lane, they make use of RSU deployed at uniform distance along the road. When a vehicle passed by an RSU, it issue a position certificate to the vehicle which consists position of RSU with time stamp. When this vehicle encounter with another vehicle on the way they exchange the position certificate and a verifier node can identify a vehicle that it is on the other lane of the road. So by this way verifier can identify traffic which is coming by opposite lane and witnesses are taken from that lane only. Authors in this article integrate the schemes 1 and 2 to detect Sybil nodes [2] in the network; they use statistical detection method to detect Sybil nodes which is based on the radio propagation model.

Hussain *et al.*, [24] presented a scheme in which they detect not only Sybil attack but also privacy is preserved of a node. In this scheme pseudonym-less beaconing is used to preserve privacy of node and for Sybil attack detection a temper resistant module is used to carry out pre-assembly analysis of data, this data is used to assemble beacons. Authors introduced a new term called as Event Reporting Message (ERM). ERMs are supported by RSU to get suspected Sybil nodes in its range and RSU report those nodes to revocation authority. In this scheme RSUs distribute authorized tokens to benign vehicles and by using those tokens node report ERMs. RSUs collect those ERMs for particular event and checks if, more than one ERMs contain the identical token. If RSU found such type of ERMs, it reports those ERMs to revocation authority. In turn revocation authority takes particular action against those nodes.

The network model given in [24] is a good model in which there is centralized trusted authority which is department of motor vehicles (DMV) at the top of the hierarchy, its responsibility is to initialize and generate registration of the vehicles and road-side infrastructure. Below it there are some revocation authorities (RA) and regional certification authorities those are considered as semi-trusted authorities. Main function of revocation authority is to take a particular action when a Sybil node is detected by the

road-side unit and RCAs are responsible for generating certificates for road-side units. In the hierarchy RSUs comes next to RAs and RCAs, main function of a RSUs is to generate tokens to each vehicles in the vicinity and detect unfamiliar behavior of vehicles, if a vehicle is detected malicious then RSU report that vehicle to RA to take particular action. All the vehicles reside at the bottom of the hierarchy.

Bayrem *et al.*, [18] proposed a RFID based solution for detecting Sybil attack in VANETs. In this paper they assume that the network is divided into several zones, in each zone there are several RSUs and one of those RSU is selected as the controller of that zone called as road side controller (RSC). Every RSC is attached to a central certification authority and when vehicles moves from a zone to different zone, vehicles are required to change their certificates. Two types of authentication techniques are used to detect Sybil attack. In first technique they consider that every vehicle embedded with active RFID tags to securely authenticate every vehicle by RSU and obtain short lifetime certificates. Second technique is based on the use of those short lifetime certificates by vehicles to be authenticated by neighboring vehicles. This technique allows detection of Sybil attack in or out of range of RSU; this is because an observer component is deployed in vehicle. Every RSU is equipped with tamper-proof RFID reader to read RFID tag of vehicles. As the vehicle enters in a new zone RFID tag reader reads the RFID of vehicle and authenticate each vehicle by data extracted by database which is attached to reader. Privacy of vehicle is another issue to resolve this issue a lightweight privacy preserving authentication protocol can be used. Problem could be in this scheme is that if malicious node consist a certificate for long period then it can request for new certificates from RSUs or vehicles (if present certificate is not expired then it consisted a valid certificate) at same time in a same zone (or in different zone).

EPCglobal class-1 Gen-2 RFID system [6] is suggested by authors. A 32-bit pseudo random number is generated at RFID tag to hide electronic product code (EPC). A Sybil attack may be that an attacker can use certificate belongs to another zone, this type of attack can be detected as when neighboring vehicles receive broadcast message by attacker, it can be authenticated using certificates of another zone and can easily identified that it is using fake identity. Neighboring vehicle send a report that contain temporal identity of vehicle with timestamp of event to RSU. Some other type of Sybil attack can also be detected in this work. Problem of cost *i.e.*, implementing RFID is a big issue in this work.

Zhou *et al.*, [25] gave a Sybil attack detection scheme for VANET named P^2DAP. In this scheme they assume department of motor vehicle (DMV) as a trusted entity, road side unit (RSU) as a semi trusted entity and vehicles are not considered as trusted entity. DMV maintains vehicle records and issue pseudonyms to the vehicles. In this paper authors gave a privacy preserved solution "P^2DAP" to detect Sybil attack. Privacy of a vehicle is preserved by pseudonyms issued by DMV; and those pseudonyms are also used by vehicular nodes to communicate in secure manner. The problem could be that an attacker can use multiple pseudonyms to pretend to be multiple vehicles. To overcome this problem authors of "P^2DAP" generate pseudonyms for a particular vehicle so that they are hashed to a common value. RSU constantly monitor communication going on among the vehicles and calculate hash value for each pseudonym. In "P^2DAP" both RSU and DMV are able to determine whether pseudonyms belong to same pool or not. In this way scheme is able to detect Sybil attack. Scheme works well and privacy of node is preserved until RSU is trusted, if it is compromised then privacy of a vehicle cannot be preserved. Authors gave variations of P^2DAP as C-P^2DAP for detection of Sybil attack, E-P^2DAP for detecting events instead of Sybil attack, T-P^2DAP for detecting collision. As the traffic density varies according to day time so T-P^2DAP is given to decide threshold for E-P^2DAP and T-P^2DAP while k-P^2DAP is given to distribute different number of pseudonyms for each RSU based on the traffic nearby those RSUs. By combining all

those techniques P^2DAP is an efficient protocol to detect Sybil attack. Only drawback is that the overhead on the DMV.

Mekliche *et al.*, [23] proposed a Sybil attack detection scheme named L-P^2DSA which is very similar to scheme proposed by Tong Zhou *et al.*, [25]. In [23] authors overcome drawback present in [25]. The drawback was that when excessive numbers of vehicles are there on the roads DMV becomes bottleneck. To reduce load at DMV, RSU perform additional role of distinguishing between suspicious nodes. A location based technique is used in which position of suspicious nodes is compared and degree of distinction is measured. Simulation result shows that load at the DMV is decreased and the false positive rate also gone down in this scheme.

Chan *et al.*, [21] proposed a scheme named "Footprint", in which authors not only able to detect Sybil attack but also preserve location privacy of the node. In this detection scheme trajectory of vehicle is used while still preserving anonymity and location privacy of vehicle. In this scheme when a vehicle comes into range of a RSU it requests an authorized message from RSU and message is issued by RSU for that vehicle. This authorized message is a proof that this particular vehicle is present at that particular time in its range. Authorized messages can be used to use to identify a vehicle as message would be different at different location. Authorized messages are not directly used because doing so may leak location information of the vehicle. The messages signed by RSU are signer-ambiguous so anonymity is preserved of the RSU. When a vehicle travels through road it collects all the authorized messages to form a trajectory using a public key. In this scheme a vehicle is free to start a new trajectory using a new public key. This freedom can be abuse by the malicious vehicle by generating multiple trajectories to launch Sybil attack. Some observation shows that multiple trajectories generated by malicious vehicle are very alike. In footprint authors established a relationship between these trajectories to detect Sybil attack. Detailed description is given in this work for generating trajectory, location privacy preserving, and establishing relationship with a pair of trajectories.

Baber. A *et al.*, [10] proposed a scheme to detect Sybil attack which is based on vehicles' geographic information for position based application. This scheme is able to detect common attackers and it also be able to detect smart attacker who are able to adjust their communication range. It is cooperative detection method so every vehicle is cooperating to detect Sybil nodes. The problem of cooperative detection is that the cooperative node should be trustworthy node otherwise result may be deviated. In this method no extra computation devices are needed in detection process because all the communication information are piggybacked in the safety related messages. So this is an efficient detection method. *Protocol design for detection has three phases i.e.* a) **probing:** In this phase when vehicle broadcast their geographic information they also sent index of nearest M vehicle in front of it and nearest M vehicle behind of it. Index could be something by which a vehicle can be uniquely identified. Second phase of this protocol is b) **Confirmation:** Sybil nodes are detected in this phase. Authors mention two type of vehicles as S-vehicle and O-vehicle, S-vehicle are the vehicle which are same side of the suspected vehicle and O-vehicles are the vehicles which are opposite side of the suspected vehicle. If an anomaly is detected, S-vehicle informs this anomaly to others. During this process suspected vehicle is ignored by others. Suspected vehicle is not selected as a verifier in this cooperative message authentication protocol. Authors employ a threshold value on number of S-vehicle and number of O-vehicle for signature protocol. If enough number of S-vehicles are there so that it reaches at threshold signature, O-vehicles are not used. But if there are not enough number of S-vehicles to reach at threshold so O-vehicles are also used to reach at threshold. On the basis of the relative distance between O-vehicle and S-vehicles which detect the anomaly. If a vehicle collects enough partial signatures so it can reach at threshold signature, suspect vehicle is identified. But if it does not reach at threshold signature investigation procedure will stop and the vehicle is treated as a benign

vehicle. Third phase of the protocol is c) **Quarantine:** in this phase all the detected Sybil nodes are quarantine.

Rahbari *et al.*, [11] propose a scheme which is based on cryptography. In this work authors gave a brief introduction to attack which can be performed on VANET and authors also categorize the type of attackers. The schema proposed by the authors cover four security aspects i.e. authentication, non-repudiation, privacy and data integrity. Problem could be in this scheme is that if malicious node uses the identity of node which is in the same domain then this scheme may fail to detect Sybil attack.

Chen *et al.*, [19] proposed a Sybil attack detection technique which is based on difference between normal and abnormal trajectories of vehicle. This scheme can be used at early development of VANET as it require limited support from VANET infrastructure and in this scheme each node can detect Sybil attack locally. Authors consider that when a vehicle come into range of a RSU it issue a digital certificate with time stamp to the vehicle, so sequence of digital signature form a trajectory. A vehicular node can detect a Sybil node by comparing and analyzing motion trajectory of neighboring node. According to authors the scheme given by them is very robust and have lower system requirement. Detection utilizes the properties of traffic under normal condition for example in normal conditions people drive at their own chosen speed, selects their own path and keep a safe distance from other vehicle. So authors consider that every vehicle have trajectory different from other vehicle. When a Sybil node is created by a vehicle the trajectory of Sybil node and malicious node is found to be identical. So in this work authors make use of trajectories to detect Sybil attack. For example: if A and B are the benign vehicle C is malicious vehicle and C' is a Sybil node created by C. When vehicle travels through the road and encountered by different RSU's a trajectory is created by digital certificates issued by RSU's. By comparing trajectories of vehicle Sybil attack can be identified.

Finally as conclude to this section, it covered almost all existed privacy protection techniques proposed by various researchers for LBSs users. But we conclude that, no single privacy preserving techniques (Refer: Table 1) that covers all of the privacy and security requirements to provide certain level of privacy (with maximum security) to mobile users due to some advantages and disadvantages in respective privacy preserving schemes. So our proposed model protect privacy and authenticate to vehicle users to communicate freely inside of LBSs. Hence this section dealt with related work that has been done by various researchers to detect Sybil attacks. Now next section concludes this work in brief.

7. Conclusion

In this real world, Perfect privacy is clearly impossible as long as communication takes place. This paper described a solution for the protection of VANETs users against Sybil attacks only not other types of attacks like reply attack, range query attack, similarity attack, timing attack, transition attack etc. The network is divided into various zones, each one of them is attached to a Certificate Trusted Authority. Each vehicle gets a new certificate in each crossed zone and authenticated by the RSUs using its identification device (for *e.g.*, RFID *etc*.,). The detection of Sybil nodes involves the cooperation between RSUs, RSCs and observers in vehicles, performed using signature verifications scheme. Contrary to other solutions [3, 10, 13, 17, 22, 27] the proposed approach allows the identification of Sybil attackers using RFID tags, even if the attack is performed out of RSUs coverage. In addition, it protects them from being tracked. For that, a set of pseudonyms certificate are used among vehicle users, but the RSUs are the only entities able to determine the real identities of vehicle's users starting from their pseudonyms. Neighbor vehicles are able to inform about Sybil attacks by reporting detected events related to the use of two valid certificates by the same vehicle at the same time. The solution also prevents attackers from tracking the mobility of the vehicles as their

identities change from a zone to another. This work shows a better results against existed techniques (Refer: Table 1) to prevent/detect Sybil attacks.

Appendix(es)

Table 1. Brief Summary of Techniques to Prevent Sybil Attack

Authors	Centralize/ Decentralized	Privacy Preserved of a Node or Not	Certification Authority Used or Not	RSS Based	Location Based	Support of RSU	Propagation Model	Detection Rate
Bo Yu et al. [20]	Decentralized	No	No	Yes	Yes	Yes	Shadowing Model	Good
Hussain et al.[24]	Centralized (DMV is the centralized authority)	Yes	Yes	No	No	Yes	-	Good
Bayrem et al. [18]	Centralized (A centralized certification authority which is connected by Road Side Controllers of each domain is the centralized unit)	Yes	Yes	Yes	Yes	Yes	-	-
Tong Zhou et al. [25]	Centralized (DMV is the centralized authority)	Yes	Yes	No	No	Yes	-	-
Kenza Mekliche et al. [23]	Centralized (DMV is the centralized authority)	Yes	Yes	Yes	Yes	Yes	-	Good
Shan Chang et al. [21]	Decentralized	Yes	No	No	Yes	Yes	-	Good (98 % as mentioned in [21])
Park.S et al. [10]	Decentralized	Yes	No	Yes	Yes	No	-	-
Rahbart et al. [11]	Decentralized	Yes	Yes	No	No	Yes	-	-
Chen et al. [19]	Decentralized	-	No (Only Digital Certificates are Used at RSU)	No	Yes (trajectories contain location information)	Yes	-	Good
Our Proposed Approach	Centralized	Yes	Yes	Yes	Yes	Yes	Manhattan mobility model	Good

Acknowledgment

The authors have declared that they have no acknowledgement.

References

[1] MOVE (mobility model generator for vehicular networks): Rapid generation of realistic simulation for VANET. Available at: http://lens1.csie.ncku.edu.tw/MOVE/index.htm, **(2007)**.
[2] X. Bio, B. Yu and C. Gao, "Detection and localization of Sybil nodes in VANETS", The workshop on Dependability issues in wireless ad-hoc networks and sensor networks of the International Conference on Mobile Computing and Networking, **(2006)**.
[3] C. Chen, W. Xin, H. Weili and Z. Binyu, "A robust detection of the Sybil Attack in urban VANETS", In the Proceedings of the 2009, 29th IEEE International Conference on Distributed Computing Systems Workshops, **(2009)**.
[4] J. Grover, M. S. Gaur, V. Laxmi and N. K. Prajapati, "A Sybil Attack detection approach using neighboring vehicles in VANET", In the Proceedings of the 4th international conference on Security of information and networks, **(2011)**.
[5] G. Guette and B., D., "On the sybil attack detection in VANET", In proceedings of the IEEE International Conference on Mobile Adhoc and Sensor Systems, **(2007)**.
[6] K. H. Kim, E. Y. Choi, S. M. Lee and D. H. Lee, "Secure EPC global class-1 gen-2 RFID system against security and privacy problems", In On the Move (OTM) Workshops, LNCS 4277, **(2006)**, pp. 362-371.
[7] D. Krajzewicz and D. Rossel, "Simulation of urban mobility (SUMO)", German Aerospace Centre, **(2007)**.
[8] E.-K. Lee, S. Yang, S. Y. Oh and M. Gerla, "RF-GPS: RFID assisted localization in VANETS", Mobile Ad-hoc and Sensor Systems, MASS October'09. IEEE 6th International Conference, **(2009)**.
[9] R. Mortazavi and M. Rahbari, "Distributed Sybil Attack detection in VANET", International Journal of Computer Applications, **(2011)**.
[10] S. Park, B. Aslam, D. Turgut and C. C. Zou, "Defense against Sybil Attack in Vehicular Ad-Hoc Network based on roadside unit support", Military Communications Conference, MILCOM, **(2009)**.
[11] M. Rahbari and M. A. J. Jamali, "Efficient detection of Sybil attack based on Cryptography in VANET", International Journal of Network Security & Its Applications (IJNSA), **(2011)** November.
[12] Q. Zhang, P. Wang, D. S. Reeves and P. Ning, "Defending against Sybil Attacks in Sensor Networks", In Proceedings of the Second International Workshop on Security in Distributed Computing Systems (SDCS), **(2005)**.
[13] T. Zhou and R. R. Choudhury, "Privacy-preserving detection of Sybil Attacks in vehicular ad hoc networks", Proceedings of the Fourth IEEE Annual International Conference on Mobile and Ubiquitous Systems, **(2007)**.
[14] A. Kumar Tyagi and Dr. N. Sreenath, "A Robust and Secure Infrastructure to Preserve Privacy for Location Based Services over Road Networks", ICADET, **(2015)** February 21-22.
[15] A. Kumar Tyagi and G. Aghila, "A Wide Scale Survey on Botnet", International Journal of Computer Applications, vol. 34, no. 9, **(2011)** November.
[16] M. Li, K. Sampigethaya, L. Huang and R. Poovendran, "SWING & SWAP: User-centric approaches towards maximizing location privacy", Proceedings of the 5th ACM Workshop on Privacy in Electronic Society, **(2006)**, pp. 19-28.
[17] A. Kumar Tyagi and N. Sreenath, "Location Privacy Preserving Techniques for Location Based Services over road networks", ICCSP, ISBN: 978-1-4799-8080-2, India, **(2015)** April 2-4, pp. 1319-1326.
[18] B. Triki, S. Rekhis and M. Chammem, "A privacy preserving solution for the protection against Sybil attacks in vehicular ad-hoc networks", Wireless and Mobile Networking Conference, **(2013)**.
[19] C. Chen, X. Wang, W. Han and B. Zang, "A robust detection of the Sybil attack in urban VANETs", ICDCS Workshop, **(2009)**.
[20] B. Yu, C.-Z. Xu and B. Xiao, "Detecting Sybil Attacks in VANETs", Journal of Parallel and Distributed Computing, vol. 73, no. 6, **(2013)**, pp. 746-756.
[21] S. Chang, Y. Qi, H. Zhu, J. Zhao and X. (Sherman) Shen, "Footprint: Detecting Sybil Attacks in Urban Vehicular Networks, Parallel and Distributed Systems", IEEE Transactions, vol. 23, no. 6, **(2012)**, pp. 1103-1114.
[22] A. Kumar Tyagi and N. Sreenath, "Future Challenging Issues in Location Based Services", IJCA, vol. 114, no. 5, **(2015)** March.
[23] K. Mekliche and S. Moussaoui, "L-P^2DSA: Location-based Privacy-Preserving Detection of Sybil Attacks, 11th international symposium on programming and systems, April **(2013)**, pp. 187-192.
[24] R. Hussain and H. Oh, "On Secure and Privacy Aware Sybil Attack Detection in Vehicular Communication", In Journal of Wireless Personal Communication, DOI: 10.1007/s11277-014-1659-5, **(2014)**.

[25] T. Zhou, R. R. Choudhury, P. Ning and K. Chakrabarty, "P^{2}DAP- Sybil Attacks Detection in Vehicular Ad-hoc Networks", IEEE Journal on Selected Areas in Communications, vol. 29, no. 3, **(2011)**, pp. 582-594.
[26] K. Sampigethaya and L. Huangy, "CARAVAN: Providing Location Privacy for VANET", In Proc. of Embedded Security in Cars, Germany, **(2005)**.
[27] A. Kumar Tyagi and N. Sreentah, "A Comparative Study on Privacy Preserving Techniques for Location Based Services", BJMCS, 10(4): 1-25, Article no. BJMCS.16995, ISSN: 2231-0851, **(2015)** July.

Authors

Amit Kumar Tyagi is currently working as Ph.D Research Scholar (Full-Time) in Pondicherry Engineering College, Puducherry. He has completed his M.Tech in Computer Science and Engineering from **Pondicherry University, Puducherry**, in 2012. His research interests include Smart and Secure Computing, Network and Information Security, Theoretical Computer Science, Privacy (including Genomic Privacy), Evolvable Hardware, Parallel Algorithms, Cloud Computing.

Dr. N. Sreenath is currently working as Professor in Pondicherry Engineering College, Puducherry. He completed his PhD in Computer Science and Engineering from **Indian Institute of Technology, Madras**, in 2003. His primary research interest lies in WDM Optical Networks. High speed networks.