This regular paper was presented as part of the main technical program at IFIP WMNC'2013

A Privacy Preserving Solution for the Protection Against Sybil Attacks in Vehicular Ad Hoc Networks

Bayrem TRIKI[1], Slim REKHIS[2], Mhamed CHAMMEM[3], and Noureddine BOUDRIGA[4]
Communication Networks and Security Research Lab.
University of Carthage, Tunisia.
Email:[1]bayrem.triki@gmail.com, [2]slim.rekhis@gmail.com, [3]m.chammem@gmail.com, [4]nab@supcom.rnu.tn

***Abstract*—Services provided by vehicular Adhoc Networks (VANETs) would be impaired if faced to sybil attacks, by which 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, is challenging, as it should meet a compromise between the ability to identify the real identity of the malicious vehicle, and prevention of vehicles from being tracked by malicious entities.**

We propose in this paper 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 RFID tags 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 we are considering is divided into different zones brought under the control of different certification authorities, 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 (e.g., software components in charge of monitoring) in vehicle nodes. A set of simulation scenarios are conducted to evaluate the performance of the solution.

***Index Terms*—Sybil attacks detection, RFID, VANET, Observers, Privacy Preserving.**

I. Introduction

Vehicular Adhoc Networks (VANET) have numerous applications, which aim to potentially improve the safety and efficiency of the road traffic systems. The development of these networks has brought a number of security issues, that are especially related to mobile and wireless communication, and users privacy. Many forms of security attacks against VANETs have emerged which could impair the life safety, or loss of income for the implemented value-added services [4]. Among these attacks, we distinguish the Sybil attack, 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; and 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 attacks if the nodes would be prevented from getting the resources they required.

Several techniques to protect from sybil attacks have been proposed in the literature. 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 by authenticating every vehicle with its private key. 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

978-1-4673-5616-9/13/$31.00

used forged pseudonyms. However, vehicles should wait to cross RSUs in order to be informed about sybil nodes.

In this paper we propose an RFID-based solution 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 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 RFID 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.

The main contribution of this paper is four-fold. First, thanks to the use of RFID 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 noting but the Electronic Product Code of the tag) is never transmitted within the vehicular network nor between the RFID 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 detection mechanisms we propose are 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.

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 how sybil attacks are detected. In Section V, we present the simulation results. The last section concludes the work.

II. An efficient detection of Sybil attacks in VANETs

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

A. Requirements for sybil attacks detection

We describe 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 Vehicular Adhoc Networks, 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 multihop 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 (e.g., 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 Architecture

We consider a Vehicular Adhoc Network, 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). The 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.

Every vehicle is equipped with one tamper-proof active RFID tag, which includes the Vehicle Identification Number, allowing the RSUs to authenticate vehicles using radio frequency transmission. One or many tamper-proof RFID 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 RFID readers attached to the RSU of that zone. A reader is attached to a database 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. 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 (OBU) 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 detected 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 1 shows a road-map divided into two zones. In the first zone A, there are two RSUs ($RSU1_A$ and $RSU2_A$), while in the second zone B, there are two RSUs ($RSU1_B$, $RSU2_B$). $RSU2_A$ and $RSU2_B$ 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 $RSU1_A$ will use the certificate generated by RSC_A, while vehicles moving from zone B to zone A toward $RSU1_B$ will use the certificate generated by RSC_B. Vehicles crossing the road between $RSU1_A$ and $RSU1_B$ 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 vehi-

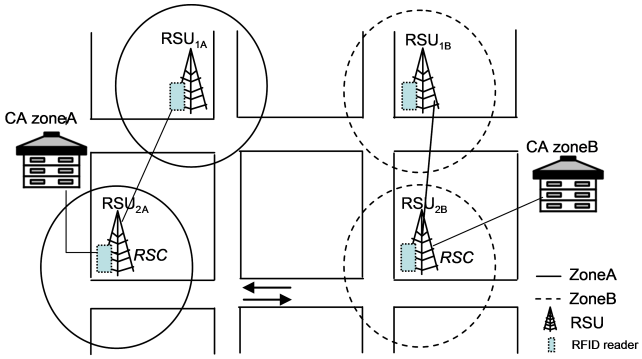

Figure 1. Proposed Architecture

cle, RSU, and RSC. Observers at each RSU are in charge of: 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; and f) collecting reports generated by vehicles about detected sybil attacks in uncovered area.

Observers in RSCs are in charge of:

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

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

- sending certificate generation requests to the first crossed RSU of the same zone;
- reception of certificate revocation lists from RSUs;
- authentication of neighbors based on signatures of the received messages;
- generation of reports about used certificates in inter-zone roads;
- delivery of the generated reports to RSUs;
- detection of sybil attacks.

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 six information:

- The last used certificate,
- The last zone visited by the vehicle,
- The list of neighbor vehicles,
- The certificates used by them;
- The timestamps of all events which were executed by neighbors and required for the use of certificates.

III. Certificates management

In this section we present, the certificates delivery, revocation and renewal processes.

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, 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 RFID 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.To prevent a vehicle from generating several certificate requests, the RSUs expects that each request is followed by an 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 (this situation will be detailed 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 X509 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 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 (we will discuss such issue later in the simulation, described in 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 RFID 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.

IV. 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: either 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; or d) some communication problems in reading its tag have occurred.

To avoid false positives, the RSU forwards the alert to the RSC, to check whether the vehicle has already obtained

another certificate in the current zone. If yes, it checks with 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 Z_1 (from which he has obtained a certificate C_1), obtain a new certificate C_2 from the next accessed zone Z_2. Later, he returns back to the first zone Z_1 before his certificate C_1 has expired and obtains again a new certificate C_2. Consequently, the vehicle would have two valid certificates C_1 and C_2 in the same zone.

Typically, as the RSU should have generated the revocation request related to C_1 before it generated C_2 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 C_1, 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 Z_2 and Z_1, in which vehicles may be moving in both directions, and therefore they may authenticate themselves using certificates from zones Z_1 and Z_2. In this situation, the attacker could communicate with different identities using certificates C_2 and C_1 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 C_1 is used in the network after certificate C_2 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 RFID 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.

V. Simulation

In this section we 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 [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 $5 \times 3\, km^2$, showing a road map composed of a set of urban zones interconnected by freeways.

As shown in Figure 2, 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. Simulation 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, say Rc, and the ratio of renewed certificates, say Rn, in terms of certificates lifetime. We consider that the total cost Cc associated to the use of certificates is equal to $(2 \times Rc + Rn) / 3$. 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 13,88m/s (corresponding to 50km/h) in urban areas and 25 m/s (corresponding to 90km/h) in freeways. We conducted the simulation using 80 mobile vehicles, and a certificate lifetime ranging from 500 sec to 5000 sec.

As depicted in Figure 3, 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,

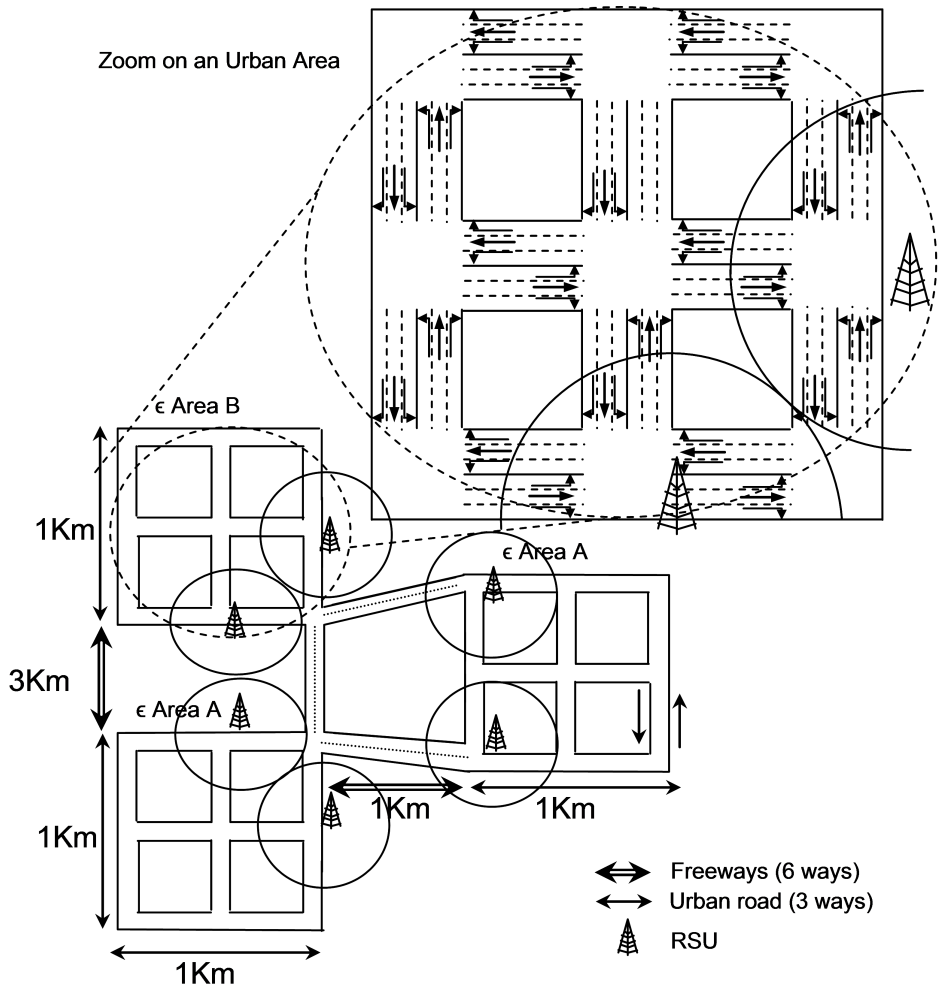

Figure 2. Topology of the simulated network

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 3, the certificates renewal ratio is equal to the certificates revocation ratio when the certificate lifetime is 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 4 and 5, 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 4, the more is the vehicle speed, the higher will be the ratio of revoked certificates as vehicles would cross quickly several zones. In addition, as the speed in urban area and freeways increases, the peak of revocation

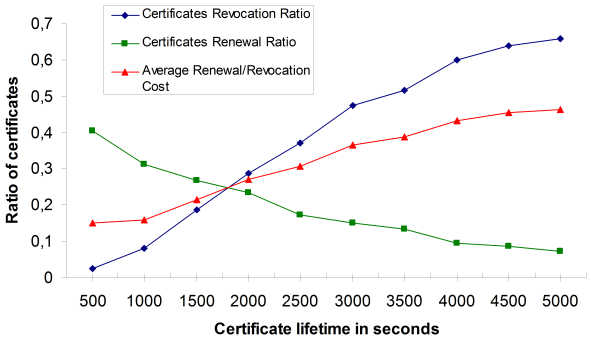

Figure 3. Ratio of revoked/renewed certificates and the related average cost vs lifetime of certificates

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. For a pair of speed equal to

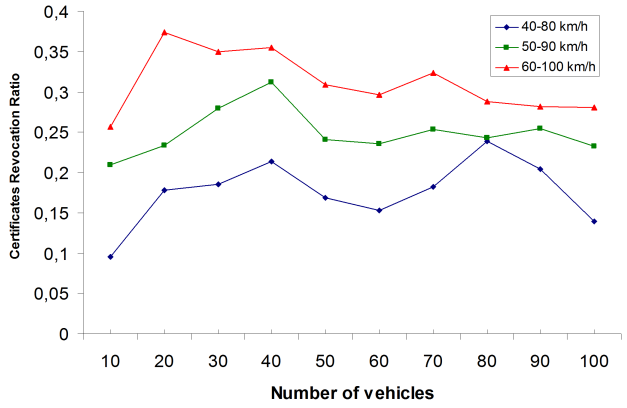

Figure 4. Ratio of revoked certificates vs number of vehicles. Three pairs of urban/freeway vehicle speeds are considered

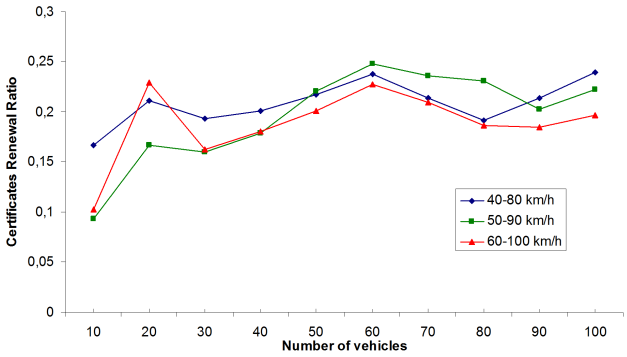

Figure 5. Ratio of renewed certificates vs number of vehicles. Three pairs of urban/freeway vehicle speeds are considered

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 5 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.

VI. Conclusion

In this paper, we described a solution for the protection of VANETs against Sybil attacks. The network is divided into zones, each one of them is attached to a certificate authority. Each vehicle gets a new certificate in each crossed zone and authenticated by the RSUs using its RFID tag. The detection of Sybil nodes involves the cooperation between RSUs, RSCs and observers in vehicles, performed using signature verifications. Contrary to other solutions [3], [13], [10], 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. A set of pseudonyms are used in vehicle certificates, but the RSUs are the only entities able to determine the real identities of vehicles 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.

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] Bio, X., Yu, B., and Gao, C. 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] Chen, C., Xin, W., Weili, H., and Binyu, Z. 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] Grover, J., Gaur, M. S., Laxmi, V., and Prajapati, N. K. 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] Guette, G., 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] Kim, K. H., Choi, E. Y., Lee3, S. M., , and Lee, D. H. Secure epc-global class-1 gen-2 rfid system against security and privacy problems. *In On The Move (OTM) Workshops, LNCS 4277* (2006), 362–371.

[7] Krajzewicz, D., and Rossel, D. Simulation of urban mobility (sumo). *German Aerospace Centre* (2007).

[8] Lee, E.-K., Yang, S., Oh, S. Y., and Gerla, M. Rf-gps: Rfid assisted localization in vanets. *Mobile Adhoc and Sensor Systems, 2009. MASS '09. IEEE 6th International Conference on* (October 2009).

[9] Mortazavi, R., and Rahbari, M. Distributed sybil attack detection in vanet. *International Journal of Computer Applications* (2011).

[10] Park, S., Aslam, B., Turgut, D., and Zou, C. C. Defense against sybil attack in vehicular ad hoc network based on roadside unit support. *Military Communications Conference MILCOM* (2009).

[11] Rahbari, M., and Jamali, M. A. J. Efficient detection of sybil attack based on cryptography in vanet. *International Journal of Network Security & Its Applications (IJNSA)* (November 2011).

[12] Zhang, Qinghua, Wang, Pan, Reeves, S., D., Ning, and Peng. Defending against sybil attacks in sensor networks. *In Proceedings of the Second International Workshop on Security in Distributed Computing Systems (SDCS)* (2005).

[13] Zhou, T., Choudhury, Roy, R., Ning, Peng, Chakrabarty, and Krishnendu. Privacy-preserving detection of sybil attacks in vehicular ad hoc networks. *In Proceedings of the Fourth IEEE Annual International Conference on Mobile and Ubiquitous Systems* (2007).