Detection of Sybil Attacks in Vehicular Ad hoc Networks Based on Road Side Unit Support

Muhammad Saad Naveed, Dr. M Hasan Islam

Abstract— Until recently vehicles and transportation systems were considered as the realm of mechanical engineers, but the need for the road safety and desire to be connected to the world, has broaden the industry scope. In order to do so Intelligent Transport System has been introduced and for few years, Vehicular Ad hoc Networks are getting much attention. The advance developments, wireless communication and life safety point towards to take into consideration the need of security in VANETs. In VANET, many attacks are possible and can cause serious damages to life. One such attack is Sybil attack. Sybil attacks have been regarded as a serious security threat to Ad hoc Networks and Sensor Networks. They may also damage the potential applications of Vehicular Ad hoc Networks (VANETs) by creating a deception of traffic congestion. Here we look on how the Sybil attack works and possible ways that an attacker can cause harm by launching these types of attacks in VANETS, along with the detection schemes that can be used to identify Sybil nodes and prevent the network from various hurtful effects. Later we propose improvements in RSU supported certificate based detection mechanism which may be helpful in solving problems with the current model.

Index Terms— Nodes, road segment, road side units, Sybil attack, Vehicles, Pseudonyms.

1 Introduction

IN In large-scale peer-to-peer systems hostile or defective computing components poses serious security threats. The major defense against these threats is the employment of redundancy. But, one single faulty component or entity can take control of a large part of the system, if it is able to represent itself as multiple identities, which can make the employment of redundancy ineffective, thus executing a Sybil attack.
Lack of physical knowledge of remote entities makes the system to perceive these entities only as informational perception that we refer to as identities. It is the responsibility of the system to make sure that distinct identities refer to distinct entities. Otherwise, the local entity can be fooled into believing a single remote entity as multiple identities and may select a subset of such identities to redundantly perform a remote operation, thereby defeating the redundancy. This forging of multiple identities is known as a Sybil attack on the system.
If there is no proper logical, central and trusted authority that can relate an entity to identity, then it will be easier for one particular entity to present itself as more than one identity. This would allow the particular entity to illegitimately consume major fraction of resources a system offers, which may lead to depletion of resources for other legitimate entities.
One of the most salient method to prevent these Sybil attacks is to have a trusted authority that can endorse identities. Otherwise, there will always be a threat of Sybil attack on the system without a logically centralized authority, except if one makes an unrealistic and extreme assumptions of resource parity and coordination among entities.
It is certainly alluring to visualize a system in which some particular established identities guarantees for other identities, making an entity to accept new identities by trusting the collective assurance of multiple independent guarantors. But, the absence of the trusted identification authority may lead to the initial generation of identities already highly compromised by Sybil attack and therefore can compromise the chain of vouchers.

2 Sybil Attacks In Vehicular Ad hoc Network

Vehicular ad hoc networks are a promising new technology that can provide economically practical solutions and benefits to a variety of applications for the transport system, for example position sensing, traffic monitoring, intelligent transport system etc.
Vehicular Ad hoc Networks are considered to have the potential to not only help in the decision making for the drivers such as route selection to the destination that is the best, less congested route, but also to improve safety of the drivers and passengers by keeping them well-informed about the road and traffic conditions and any disasters ahead. Considering the importance of vehicular ad hoc networks researchers have always been in quest to point out any security threats that VANETs are facing, which may lessen the efficiency of vehicular networks and even cause damage to life safety.
Security is required for a large number of vehicular ad hoc network applications, especially when the vehicular ad hoc networks are responsible for protecting information or monitoring traffic or transmitting critical lifesaving information. Security in vehicular ad hoc networks is complicated by the broadcast nature of the wireless communication and some of the factors related to the nodes' mobility behavior. Apart from these complexities, vehicular nodes have large storage and computational resources which could be helpful in terms of developing security models.
Vehicular ad hoc networks (VANETs) represent complex distributed systems very much similar to that of mobile ad hoc networks consisting of wireless mobile nodes. These nodes can self-organize themselves into various ad hoc network topologies dynamically and freely. This enables and helps the vehicular nodes to communicate with each other in places where there is no communication infrastructure installed.
Generally, communication in wireless networks are carried out based on a unique identifier that is supposed to represents

a network entity which we refer to as a node. In a network these identifiers are used for addressing the network entity during communication, thus forming a one-to-one mapping between an entity and an identity. This is a general assumption many protocol mechanisms assume either implicitly or explicitly. Thus, implying that two identities represents two distinct nodes.

But the lack of such addressing mechanisms in vehicular ad hoc networks creates a vulnerability for Sybil attack. Which means that a malicious vehicle can claim multiple fake identities proving to be harmful to a number of vehicular network applications. In order to understand the attack and its harm in vehicular networks let us consider one of the several scenarios. A driver looking for more resources or traffic-free road to his destination can devise that a large number of vehicles are traveling nearby, thus creating an illusion of traffic congestion. Other vehicles fooled by this illusion chooses an alternate route and withdraw from the road, thus giving the attacker a congestion-free resourceful (in terms of network bandwidth etc.) route. Generally, all these fabricated vehicles remain under the control of attacker, so several other applications or network protocols may also be affected by such attacks depending upon attackers' intention. Some of these include deviation from truth by affecting the results of voting-based protocols using Sybil nodes. Sybil nodes can also be used to launch Denial of Service attacks that can harm the operations of network, leaving other legitimate nodes out of service by affecting data dissemination protocols

In the same way attacker can also use Sybil nodes for blocking life critical information causing serious safety threats. For example, if a vehicle is using an application for early warning, and another vehicle two nodes ahead in the same row reduces its speed significantly or applied breaks, a broadcast message will be generated giving warning to the following vehicles. This message if received by some Sybil node can hinder the forwarding process thus leaving the following vehicles at a great risk or threat. This could result in massive pileup on the highway, potentially causing great loss of life.

Sybil attacks pose a great threat in the absence of centralized identity management in vehicular ad hoc networks. For the security protocol to be effective there is a need for a unique, distinct, and persistent identity per node.

3 Effect of Sybil Attacks In Vehicular Ad hoc Netorks

The major function of vehicular ad hoc network is providing enhanced safety for drivers and passengers. Most of the applications for vehicular networks are developed keeping in mind the safety of users. Any vulnerability and attack pose serious life threats. In the same way a Sybil attack on vehicular ad hoc networks can cause serious damage to the safety of drivers and passengers in several ways.

Some the applications and protocols that can be affected by the Sybil attack in vehicular ad hoc network are discussed as following:

2.1 Routing

Wireless ad hoc networks rely on nodes for multipath routing of data. A Sybil attacker can interrupt the location-based or multipath routing by taking part in the routing using Sybil nodes. Any Sybil node in the routing path can cause disruption and loss of data, as these nodes give the false imprint of being different nodes on distinct locations. Another mechanism that is vulnerable to such attack is geographic routing. A Sybil node can appear more than once, instead of having one set of coordinates at one place at once.

2.2 Misbehavior Detection

Another application in Vehicular ad hoc networks that can be affected by Sybil attack is a reputation and trust-based misbehavior detection applications. These applications are meant to detect particular type of misbehavior of vehicles on the road. It is very likely that such applications have some false positives, hence these applications record several repeated offences by a vehicle before taking any action against the vehicle. An attacker can increase its reputation or trust and decrease others' reputation or trust by using Sybil nodes to disrupt the accuracy of these applications by exploiting virtual identities. For example, an attacker could use Sybil nodes to misbehave many times but not enough to take action against or use these Sybil nodes to take part in blaming or reporting legitimate nodes of misbehavior or false information, thus getting them revoked or blacklisted.

2.3 Data Aggregation

Vehicular ad hoc networks use data aggregation query protocols to compute the sensor reading of the network which will help the network to consume energy instead of returning sensor reading individually. In vehicular ad hoc networks, a Sybil attacker can modify or tamper the aggregated reading results by giving contribution for a number of times as a different node. Normally these computed aggregates are not affected by small number of faulty or malicious nodes sending incorrect readings. But an attacker can create a large number of virtual nodes using Sybil attack and can contribute enough to theses aggregate readings to change the outcome completely.

2.4 Fair Resource Allocation

If the network allocate resources on a per node basis, then the Sybil attacker can use the Sybil nodes to gain unfair share of resources. For example, if in a wireless environment nearby vehicles nodes may be sharing a single radio channel that is allocated to each node for a fraction of time per interval during which they are allowed to communicate or transmit data, the Sybil attacker can use to malicious nodes in order, to obtain an unfair amount of time or any other resources shared using this mechanism. This can also lead to denial of service (DoS) attack by blocking or delaying the access to the services to legitimate nodes by reducing their share of the resources (bandwidth etc.).

2.5 Voting

Vehicular ad hoc networks can use voting for a number of tasks. But, voting-based schemes can be affected by a Sybil attacker who will be able to control the results by rigging the voting or polling process using fabricated Sybil nodes. In any such voting scheme the Sybil attacker can "stuff the ballot

box". The attacker can easily turn the results around by creating a number of identities and also may be able to determine the outcome of any vote. Such type of attack mechanism can be used for blackmailing other legitimate vehicles that have complained about misbehavior of the attacker and attacker using his Sybil nodes can claim that the complaining node is itself misbehaving thus getting it revoked. Similarly, attacker can control or change outcome of any vote against his Sybil nodes.

2.6 False Information

In vehicular ad hoc networks a Sybil attacker can create a random number of virtual non-existent vehicles. These vehicle can then be used transmit false information into the network and give a fake imprint of traffic congestion in order to divert traffic.

Because of these and several other harmful effects, that can have a serious impact on the operations of vehicular ad hoc networks, it is necessary to develop a security model that can detect Sybil attacks and eliminate them from the network.

4 Detecting Sybil Attacks In VANETS

IJSER Considering the security of vehicular ad hoc networks and the threats posed by Sybil attacks. Many efforts have been made and several security models been proposed to detect Sybil nodes and attacks in the vehicular communication. Most of the proposed models are able to detect Sybil attacks but wither they are limited to particular number of vehicular nodes or add too much delay which may lead to the bottleneck in the network communication. Some of these models are discussed below:

Considering the security of vehicular ad hoc networks and the threats posed by Sybil attacks. Many efforts have been made and several security models been proposed to detect Sybil nodes and attacks in the vehicular communication. Most of the proposed models are able to detect Sybil attacks but either they are limited to particular number of vehicular nodes or add too much delay which may lead to the bottleneck in the network communication. Some of these models are discussed below:

4.1 Resource testing detection mechanism

Resource detection mechanism are further divided into following categories

1) Radio Resource testing methods

Radio resource testing [5] uses methods that test the vehicle's radio resources, computational, memory and identification resources. In radio resource testing methods, legitimation of the node is checked by the neighboring node on the basis of the message it sends in response to the neighbors broadcast. The testing node broadcast that message for all its neighbors and randomly chooses a channel for listening of response. If the response is received from the same channel, then the neighbor is legitimate. For the Sybil entities to send the response different channels are used and hence these Sybil nodes are detected.

Problem

The problem with this method is that it assumes or restricts the device that it cannot send and receive at a time. But attackers can have multiple channels and can perform the communication for the Sybil nodes on these channels.

2) Identification Resource Testing

This method proposes that[6], that those vehicles whose MAC and IP addresses are not registered within a list will be considered as fake or false entities. This method demands the vehicles to broadcast the registered IDs which could violate the driver's privacy.

Problem

The method is insufficient for the prevention of Sybil attack as attacker may create multiple identities that are not registered with any of the network. Later these identities can be registered with the network and attacker will be able to have multiple registered Sybil nodes.

3) Computational Resource Testing

This method suggest that if a vehicle is unsuccessful in the completion or solving a task or puzzle will be considered as fake. In Sybil attacks, attacker creates Sybil nodes that are sharing the memory, computational, communication resources. So, by tracking and monitoring the vehicles that are using shared resources for processing communication and sending responses, we can find the malicious vehicles.

Problem

This method requires extensive monitoring and tracking of messages which will require specially designed tools. Resource testing based mechanisms does not actually prevent the attack, in fact, the goal of these mechanisms is to undermine this attack and by restricting fake identities. But considering the fact that attacker can obtain sufficient legitimate IDs (sharing and stealing), there is a strong possibility of a successful attack to occur. Therefore these method may not provide the sufficient level of protection against these attacks [7].

4.2 Position Based Detection

These methods are based on the fact that a vehicle can be only at one point at a time. These techniques propose to use various position based sensors and mechanism for the prevention against Sybil attack. With the advance development in sensors, which are used for various requirements of traffic monitoring purposes, position based detection mechanisms become much easier to implement. But for the effective working of these applications in the real world, the position information must be protected. If this information is not protected attackers can be able to damage the vehicular network by perpetrating attacks e.g. dropping packets, modifying existing packets, inserting bogus packets and replying packets. Based on the coverage range these schemes can be divided into [8], [9]:

- Range-based
- Range free

1) Range-based

Range-based methods estimates the distance between a transmitter and receiver and then try to compute the position of the vehicle by using one of the following estimation methods:

- Received Signal Strength Indicator (RSSI) based

methods [10],

- Time-based methods
- Angle of Arrival based methods.

As these methods tend to have high accuracy in localization, they are used to estimate the distance and verification of position of the vehicle. For position estimations a range-free localization method can be used. Some of the researchers [11] have also put forward an innovative method on the saying of seeing is believing, which also lie in the range-based approaches, but the problem lies there, as any sensor onboard the vehicle will have its range limited. For example a camera or radar can only see or detect the vehicle in its sight or near to it within its range. However the proposed model is to compare what is seen with what is heard by the vehicle, so that the vehicle could confirm definite position of neighbors in order to mark attackers from the others.

Problems

However, there are a few complications in using this method:
(1) The models asks for new additional hardware that at present are not built, adding cost. [12]
(2) Failure of method to identify a malicious vehicle claiming it to be in position of another existing vehicle within the range of verifier vehicle. [12]
(3) Sensors range make the method application impractical.
In order to resolve these problems a method is proposed to assume the radar range to be persistent, such that if a target vehicle is not within the range of radar of verifier vehicle, intermediate vehicles will be used for this model [13].
However using intermediate vehicles could add to the security problems [14]. If a vehicle want to verify the position information about target vehicle, it will have to use more than one vehicle as intermediates. Since the verifier vehicle have no information about the malicious vehicles outside its radar range, it can be easily fooled.

4.3 Verifier based mechanisms

These methods [15], [16] consists of a lightweight approach for detection and localization of Sybil nodes in VANETs. Method uses verifier mechanism to confirm the claimed position by each vehicle using the received signal strengths taken by neighboring vehicles for a time period, which are later analyzed to calculate the position of claimer vehicle.

Problem

The method is simple and have low overhead but also has low accuracy, such as a 10 meters error range in positioning and also neighbor vehicles which can be Sybil entities, then this method is vulnerable against false signal strength measurements.

Improvement

An improved version of the model has been proposed by the researchers which suggests each to vehicle to carry out the role of claimer, witness or verifier according to different events and for different purposes. For the vehicle to verify the claimer vehicle which is periodically broadcasting its position and identity information, the verifier vehicle uses witness vehicles. The witness vehicle must be reliable and therefore for this purpose researchers use road side unit support and traffic pattern establishing the following two rules:
•Vehicles receive a certificate when passes through an road side unit, which contains a time stamp, containing information regarding time, identity and position etc., to prove the presence of the vehicle near the road side unit at a certain time.
•Witness vehicles must be on the other side of the road heading in opposite direction.
Combination of these two rules will ensure that the witness vehicle is physical, legitimate and can be trusted. Rule two helps to make sure that no Sybil entity generated by a malicious vehicle is selected as a witness.

Problems

Some of the problems with the proposed improvements are as follows:
•Lack of precision for detection the position using RSS measurements in city traffic scenario
•Lack of vehicles on the roads (opposite direction) cannot be used for one-way roads
•Violation of privacy by broadcasting identity and position information for distributed position verification

4.4 RSSI Based Detection

This method propose estimation of distance between two entities using received signal strength and theoretical radio propagation models. This approach make this method a low cost method for hardware-constrained systems.

Problems

The reliability of the estimated RSSI cannot be guaranteed because of attenuation in received signal for multipath environments and shadowing effects in the area. There are some techniques that register RSSI values with vehicle identifier for detection of Sybil entities. The following two assumptions used in this approach are not considered to be realistic the assumptions are:
•Malicious vehicles do not collaborate with each other
•Sender vehicles are not allowed increase or decrease their transmission rate
Although the method is sufficient in detection of some of the malicious vehicles in the network but cannot be used as a sole defense [17], [18], [19].

4.5 Authentication and Public key based detection mechanisms

Sybil attacks can be detected using the approach of encryption and authentication. The detection mechanism is based on the authentication of vehicles using Public Key Infrastructure. Detecting Sybil attacks based on this approach have been a focal point of many research works [5], [20], and [21]. It is an understandable that using authentication mechanism and keys are the best and only approach that can fully eliminate Sybil attacks. But since Public Key Infrastructure is heavy and could be complex solution, it is difficult to implement and sometimes considered unrealistic approach towards the detection of Sybil attacks n Vehicular ad hoc networks. More time is consumed and message size is significantly increased Public key encryption or message authentication systems which intern increases the memory requirement for such approach. Therefore, the cost of the resources such as bandwidth and memory usage increases in public key systems. Whereas, symmetric key based systems consume less time and memory and small message sizes as compared to Public Key Infrastruc-

ture. Some of the methods using encryption based approach are as follows:

1) Privacy-preserving Detection of Abuses of Pseudonyms P2DAP

Some researchers [24] have proposed a scheme to detect Sybil attack by focusing on preserving the privacy, which is referred to by the name of Privacy-preserving Detection of Abuses of Pseudonyms P2DAP. This approach uses the role of a governmentally controlled Department of Motor Vehicle (DMV) which can generate a large number of pseudonyms for all vehicles for one year use. The idea is to categorize of group the generated pseudonyms in following two steps.

Step 1: Hashes for each pseudonym are calculated using a global key by the department of motor vehicle. A particular set of bits is selected from the hash result. These Selected bits are referred as "coarse grained hash value" and pseudonyms containing the same coarse grained hash value are known as coarse grained group.

Step 2: DMV separately hashes each pseudonym is separately hashed by department of motor vehicle with another key that is only known to just DMV. Then a set of bits from hash result is selected that is called fine grained hash value. Fined grained hash values that are equal are inserted in a subgroup of the same coarse grained hash value. This will help make sure that all of pseudonyms that have one value of fine grained hash are in a subgroup that belongs to a particular coarse grained group.

Global key that is used for the generation of coarse grained hash values is distributed by the DMV, to all the road side units (RSUs), whereas the key used for generation of fine grained hash values are kept secure and secret. Allocation of the pseudonyms with equal fine grained and coarse grained hash values to the vehicles can start after the department of motor vehicle have generated enough number of fine grained hash values in each subgroup of coarse grained group. At the time of yearly registration for the vehicles, a unique fine grained subgroup of pseudonyms is allocated by the DMV to each vehicle, so, that this unique mapping is a secure plate number for each vehicle.

Now for the Sybil attack detection, the process comprises of two levels. First, Road side units are supposed to be overhearing the messages exchanging between vehicles, each pseudonym that is used for signing a particular traffic event message is stored into a list. Repetitive coarse grained hash values are identified with calculation of coarse grained hash values of these pseudonyms and are marked as suspicious. These suspicious pseudonyms are send to the DMV by the road side units, where fine grained hash values are generated from these pseudonyms. If the generated value is the same value of fine grained hash, attack is inevitable.

In this research the goal preserving privacy is achieved by the use pseudonyms. Road side unit are not able to specify a certain vehicle in a coarse grained group. This will help if the road side unit is compromised, the attacker will not be able to obtain or steal a vehicle privacy and will only be able to get the coarse grained hash key from compromised RSB, as the fine grained hash key is only known to Department of Motor Vehicle. In an effort to reduce the communication overhead, this method suggests that the most of the tasks of DMV are performed by road side units. Whereas, for more security, use of a multi-level hash instead of one-level hash is also suggested.

The results of the simulations for this schema have shown success in initial stages where all of the Sybil vehicles can be detected but, later stages of this schema are dealt with the decrease in communication and computational overhead in exchange for reducing the rate of detection of attack.

Problem

Although in many ways this research holds the edge over other research works as in many of research works done for the Sybil attack detection privacy is not considered but here it is preserved unless the road side unit is compromised. The problem with P2DAP is that first, it's an alternative to use the standard PKI model in a different way, which is still time consuming and secondly it does not deal with the stolen or shared keys or pseudonyms. The communication between the DMV and road infrastructure can lead to the creation of bottleneck as the Department of Motor Vehicle is not able to provide the services for the extreme communication.

2) Foot printing

Foot printing [22] is another proposed approach for the detection of Sybil attacks in vehicular ad hoc networks based on using the authorized event messages as vehicle trajectory by preserving the privacy of vehicles in the network. The detection mechanism is carried out by the vehicle and the road side unit which act as a conversation holder by transmitting the messages among the vehicles. The approach is designed to prove the physical presence of the vehicle by sending an authorized message from the road side unit after the vehicle passing through the unit has made the initial request. These authorized messages are in a consecutive sequence, which help in the unique identification of the vehicle. The researchers have suggested to chain these messages together forming a trajectory of the particular vehicle. But in doing so, the computational overhead and complexity of signing each message increases insignificantly, so, in order to avoid such complexity, it is the responsibility of the last road side unit to sign the vehicle trajectory formed from chained authorized messages. Using a chained message format may help road side units to keep track of vehicles in the network but will be at risk in case the road side unit is compromised. Therefore in order to maintain the privacy and ambiguity of vehicle in the network following two conditions are required to be met:

- Road side units signing the vehicle's trajectory are unknown, which can help maintain the privacy of specific vehicle in case of any eavesdropping.
- Authorized messages can be recognizable if they are issued at the same period of time by the road side unit. Necessary condition as it will not allow the attacker to detect the trajectory of the vehicle even if it tries to gather the road side unit's signed messages over the time. Meaning vehicle trajectories will have a limited use.

The above conditions make sure that the vehicle's position remains hidden and it privacy is maintained. As in this approach road side units are playing the role of conversation holder so whenever a vehicle wants to participate or start a

conversation, it will have to pass the trajectories to the road side unit. Road side unit will check for the similar trajectories and if found similar, then it will be refereed as attack. The mechanism has been evaluated and has shown detection rate of 98% using such attack.

Problems

Although the vehicles privacy is maintained and costs less as vehicles only extra requirement would be a DSRC interface and GPS system. But will have to encounter the following problems.

- Using graphs and identify the similar trajectories inside it makes the approach complex
- Scalability problem caused by attackers with high and dynamic speeds can create complex and longer trajectories and hence the detection probability decreases, as identifying similar trajectories will be much more difficult once the number of road side units involved in the process increases.
- Compromised road side units can be used to issue authorized messages to the attacker

3) Time-stamp certificates

Another way [23] to detect the Sybil entities is issuing certificate to the vehicles. In this approach researches propose to issue the timestamp certificate to the vehicle whenever they pass by a road side unit. This approach does not involve any use of the public key infrastructure and only road side unit are able to generate and issue the certificates. The vehicle after gaining the timestamp certificate can use this for authentication purposes and also to obtains new certificates form the next road side unit. The approach is heavily based in the assumption of varying speed and driver's behavior, such that no two vehicles can pass through the same road side unit at one time. After getting the signed certificates, will be used to authenticate the traffic messages. These certificates are important in two ways

- Indicates the time of issuance to the vehicle by an RSU
- Shows the recent path used by the vehicle by means of the RSU information that issued the timestamp certificates.

The certificates are made unique by using the previously obtained certificates to get the new ones which contains the hash value of the previous, making the timestamp certificates unforgeable and non-transferable. Vehicle that have no certificates will also be regarded as malicious. Two similar timestamp certificates shows a Sybil attack.

Problem

The major problems with the Timestamp series model is that it depends largely on the assumption that based on different behaviors and motion trajectories, two vehicles cannot pass through the same road side unit at one time. This may be true in a highway scenario but fails in cities where congested traffic situations can lead to same vehicles getting same timestamps. This model resolves this problem by forcing each vehicle to request its own pseudonyms for vehicular communication. Even in city scenarios road side units will be able to deal with multiple requests and issue the pseudonyms to respective vehicles. The mechanism could be vulnerable to Sybil attacks in case the road side units are adjacent to each other. For example, in the figure below the vehicle passing through RUS 1 and RSU2 can try to obtain two different certificates from the RSU 3 based on the cert1 and cert2.[23]

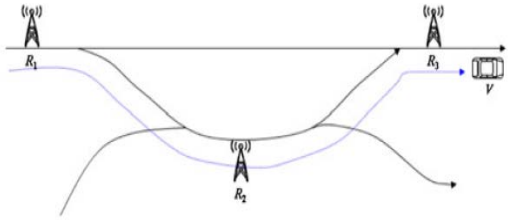

Figure showing the Example of complex roadways. A vehicle V passed through R1 and R2, so it can attempt to obtain at least two different certificates from roadside unit R3, because both R1 and R2 are adjacent to R3. One is based on the certificate from R1 and the other is with the certificate from R2.

5 Proposed Model

As discussed Sybil attacks are harmful for the vehicular ad hoc networks. Therefore in order to defend against these attacks many researchers have proposed several models based on some assumptions of the future of vehicular network model. But these models have some shortcomings in some ways. Here we represent a model for defending against Sybil attack using road side units for distinct identities while protecting the drivers' privacyand try to improve the work done in previous similar techniques [23].

5.1 Assumptions for the Model

Following are the assumptions for the vehicular ad hoc networks. These assumptions are based on the current technologies already installed and used in transport system and considering some of those which would be required for efficient and effective working of vehicular ad hoc networks.

Vehicle

Vehicle is considered as a primary node in the vehicular network model. It has an on-board unit (OBU) for communication purposes and other computing processes, positioning system such as GPS, and digital map including geographical road information, electronic license plates, manufactures unique identity in terms of model number, production date, and color. Other sensor are also installed which are responsible for recording and analyzing data for safety of driver and passengers. Drivers also have the license in the form of smart cards.

All these identities can be read and used by road side units and will help the authorities to hold the particular driver accountable for law violations. All vehicles have to register to the road side units or particular Vehicular network segment i.e. vehicles do not have the choice whether to use the services of VANETs. If vehicles do not register with the road side unit at beginning vehicle will be considered as malicious and no communication will be allowed with other vehicles or access over the internet.

Vehicles are considered malicious so any event information a vehicle desire to send will be through the road side units,

which are responsible for authenticating the event, based on the data gathered through sensors. Other vehicles will only trust an event received from the road side units.

Road Segments

We assume that roads are divided into segments where each segment is defined to be a part of straight road without intersections or diversions. Each segment has its unique set of road side units installed that are connected to each other. Each segment has a registering and deregistering road side unit at the start and end of segment respectively. The model requires the vehicles to register itself with the particular road segment, and in return get a pseudonym. New segment demands vehicle to first register itself with the road side unit. Road segments must be defined in such a way that it can overcome complexity of the road architecture.

Road Side Units

Road side units are the equipment installed along the road to aid in communication. Trusted by all vehicles based on the certificates issued to the road side unit from the Certification authority also trusted by the vehicles. These road side units can be operated by government or private network operators. All road side units are considered to be interconnected through a wired connection.

Road side units are considered to have high computational power, equipped and integrated with certain sensors used along the roads for different purposes.

Two types of road side units are considered

•One, responsible for the issuance of the pseudonym alongside normal purpose communication

•Second, responsible for providing services for authentication and communication. It will overhear the communication messages among vehicles for a particular road segment. To provide redundancy this type of RSU can be used to generate new pseudonym.

The road side units will keep the data updated for the vehicles currently in the road segment. At the end of the segment the road side unit will determine the vehicle leaving the segment so that it can update other road side units along the respective road segment.

Certification Authority

The governmental authority that keeps the records of all vehicles, responsible for certificate management of all the vehicular network nodes. It acts as a trusted third party authority that is both trusted by the vehicles and operators of the road side units.

Sensors

We assume that certain sensors are deployed to assist in vehicular movement. Taking the advantage of data gathered by these sensors we can perform certain verification steps for the enhancing the security of the vehicular networks. The sensors are motion sensors, obstacle sensors, cameras, electronic readers etc.

Vehicular Applications

The user interface applications that are used for receiving and sending traffic messages by the drivers.

5.2 Proposed Framework

When a vehicle is entering a segment of road it is asked about its secret identity or any other ID that can be verified from the governmental authority or network operator (which it has obtained from the MVD) to establish a connection between itself and the road side unit. In return road side unit will assign a unique pseudonym and key pair to the vehicle. Multiple vehicles can perform this step at the same time, but one vehicle can only generate one request based on its ID.

"A unique pseudonym for one connection"

Using this step, attackers would not be able to register multiple vehicles even if they have stolen or shared IDs. Vehicles are required to use this pseudonym in their message body. The deployed sensors will help the road side unit in determining the number of vehicles coming in and requests it received from a section of road at particular coordinates. Since for an attacker to register the multiple identities, multiple requests must be made, which must be verified by the vehicle's coordinates and IDs.

One vehicle with an ID to register issues a request message also containing its coordinates. Road side unit will get the verification of the presence of the vehicle at these particular coordinates (though some form of threshold is to be considered, related to the vehicles movement) using positioning sensors and electronic plate readers. After verification road side unit will generate a key pair and pseudonym for the vehicle which it will use for future purposes of communication.

The verification of the vehicle will require to check the coordinates, the IDs provided by vehicle must match the ID read by the sensors from the electronic plate number. (Combined).

Road side unit will store the credentials provided by vehicle, and pseudonym assigned to it in the form of the table and will send it to the other road side units along the road segment. Road side units along that segment of road will be continuously informed about the newly registered vehicles.

When the vehicle generates an event message it will include the pseudonym, vehicle's current position coordinates in the message body. Road side units will be responsible for the verification that the message generated from the legitimate vehicle. The uniqueness of pseudonym will help the road side units to detect the possible Sybil attack.

If at some point attacker is able to steal the uniquely generated pseudonyms the position coordinates will help determine the Sybil node, with original node at different location. Furthermore the use of digital maps and position detection sensors the physical presence of the vehicle can be verified.

In this model we propose to maintain the vehicles record currently in the road segment or coverage area, upon leaving the road segment, RSUs along that road segment will be informed to revoke the particular pseudonym entries so, the stolen pseudonyms will be useless once the original owner leaves the road segment. The RSUs will use the electronic plates reader for the identification of vehicle leaving the road segment because a malicious vehicle may choose not to inform about its leaving. All pseudonyms related to IDs read at RSU RL will be terminated or revoked.

Upon reaching the next road segment, vehicle will again have

to request registration. In this way Sybil attacks will be prevented with the help of using unique pseudonyms.

5.3 Detailed Process Implementation

Some of the denotation used

- Road Side unit at the start of the road segment = RS
- Road side unit at the last = RL
- Vehicle = V
- Road Segment = Si , i=1,2,3…n
- RSUs within the road segment = RSUM
- Certificate of road side unit = Cert_ RS

Vehicle enters a road segment and receives a beacon message from the front end RSU, which includes the certificate of road side unit RS (Cert_ RS) issued from the CA which contains indication of the type of RSU (to get registered with the road side unit RS) and public key KRS.

$$Cert\_RS = \{Type\ of\ RSU \mid PUB\_KRS, Sig\ (PRI\_KCA, PUB\_KRS)\}$$

Road side unit will gather the information about the passing vehicle from the electronic license plate, which has an ID encoded to it by the motor vehicle department MVD.

Vehicle can validate the RSU by using the public key of RSU with the certificate. After the validation of the RS by the vehicle, the vehicle now trust and knows the type of the RSU to register itself for the new road segment S1. Vehicle in return requests for the pseudonym and send particular credentials which include the IDs issued by the certificate authorities, coordinates of vehicle and a session key.

Message sent by Vehicle V will contain the request for the pseudonym REQP and session key KS and the whole message will be encrypted.

$$ENC\ \{PUB\_KRS, KS, REQP\}$$
$$REQP = \{Request\ for\ the\ Pseudonym \mid Coordinates \mid ID \mid KS\}$$

RSU will process the request and validates the physical presence or existence of the vehicle with the help of integrated sensors, electronic plate readers, digital maps and positioning system deployed.

RSU, after performing the validation process will create a random key pair for the vehicle (PRI_KV, PUB_KV) and a unique pseudonym for the vehicle V. The generated key pairs and certificates will be stored in a tabular form and valid for the respective road segment or coverage area as determined by the motor vehicle department or private operator. The stored pseudonym will be shared by RS among the other road side units within the road segments.

Message sent by RS will be encrypted and contains the unique pseudonym, which includes the issuing time, valid area of use and the certificate content of RS.

$$ENC\_KS\ \{PRI\_KV, REPP\}$$
$$REPP = \{Pseudonym\ PS1, Sig\ (PRI\_KRS, PS1)\}$$
$$PS1 = \{PUB\_KV \mid PUB\_KR \mid Issuing\ Time \mid Valid\ Area \mid Expiration\ Time\}$$

Multiple vehicles can perform this step at the same time, but one vehicle can only generate one request.

"A unique pseudonym for one connection"

This will be insured by the position verification and electronic ID read by the RSU RS. The RSU RS and RL will be responsible for keeping the track of the vehicles currently in the road segment.

When a vehicle V with unique pseudonym will be leaving the particular road segment, it will receive the beacon message from the RSU RL which defines the end of the road segment valid for the particular pseudonym PS1. The purpose of this RSU is only to notify the vehicle and identify the vehicle leaving the road segment. Cert_ RL will help the vehicle regarding the end of road segment while the electronic plate readers and sensors will help the RSU to determine which vehicle is leaving. This will help the revocation of particular pseudonym and vehicle will now know its entering a new segment and need to generate a new request. In this way the road segment S1 will be able to keep the record of the vehicles and revoke pseudonyms of vehicles upon leaving the road segment.

Upon reaching the next road segment similar steps will be performed in order to create a connection between the vehicle and RSU and validation process.

5.4 Using Certificates in Vehicular Communication

Vehicle on the roads observes traffic events occasionally or in some cases periodically. Whenever a vehicle observes a traffic event it generates a traffic event message and broadcasts it. The format for the traffic event message is as follows

$$TEM = \{Event\_Info, Sig\ (PRI\_KV, Data), PS1, Cert\_RS \mid Coordinates\}$$

Event_ Info will include the event occurred, GPS information, speed, time, direction.

The Event_ Info will be signed by the private key of the vehicle V which proves that the traffic data are created by a vehicle that possesses a valid Pseudonym PS1. The receivers of the traffic event message can use the public key PUB_KV to determine the validity of the signed Event_ Info. Also the validity of PS1 can itself be checked with the help of RSU's certificated Cert_ RS. If the receiver vehicle is able to verify all the credentials it will accept the message to perform required task otherwise it will ignore the message. Moreover the overhearing road side unit will look for the any revoked pseudonym being used in the traffic event messages. In case of revoked Pseudonym being used vehicles will be informed to ignore/discard the message.

As it is possible that traffic messages are disseminated through several different multiple hops based on the application in use, the pseudonym PS , RSU certificate Cert_ RS and the signed Event_ Info will prevent any modification or forging of the message.

6 Analysis

Simulations were carried out in NS-2 using the MAC 802.11a module. In order to reduce the packet overhead, we assume elliptic curve cryptosystem for our basic signature scheme. The summary of our simulation parameters is shown in the table below. The key length of elliptic curve digital signature algorithm is 163 bits (21 bytes), and the corresponding signature size is 28 bytes. The estimated signature generation time is 36.82ms, and the verification requires 38.05ms [40], [41], [42].

Parameters	Values
Simulation distance	500m
The number of vehicles	10, 20, 30,40, 50
Average driving speed	50, and 150 km/h
Asymmetric Encryption	ECC with a key of 163 bits
Transmission range	150m
Bandwidth	2MB
Packet size	48 and 94 bytes

6.1 Packet Overhead

Packet Overhead shows how many additional bytes were added in regular traffic messages in order to provide security according to the proposed model.

1) Pseudonym request message

The total length of the request packet generated by the vehicle for the pseudonym is given as follows. The fig 5.2.1b shows that request message contains a request of 8 bytes, ID of the vehicle presumably 8 bytes the coordinates 16 bytes.

= length (request) + length (coordinates) + length (ID) + length (KS)

=8+16+8+16 =48

2) Pseudonym response message

In the same way the response message from the RSU contains the pseudonym which contains the contents: PUB_KV (21bytes), PUB_KR (21 bytes), Issuing Time (8 bytes), Valid Area (8 bytes), Expiration Time (8 bytes). Also the 28 bytes of the signature.

*length (PS1) = 2*length (Key) + 2* length (timestamp) + length (valid area)*

*=2*21 + 2*8 + 8 = 66 bytes*

REPP = 66bytes + 28 bytes of Sig = 94bytes

6.2 Processing time

The temporary pseudonym protocol performs encrypted message communication. For the consistency with signature, we adopt elliptic curve cryptography encryption and decryption with a key of 163 bits for our asymmetric algorithm. The estimated encryption and decryption time are 2.65 and 1.31ms, respectively. Generating a request by a vehicle requires one asymmetric encryption (2.65ms). So the total processing time is 2.65ms. Issuing a new certificate by an RSU requires one asymmetric decryption (1.31ms), one signature generation (36.82ms), and one asymmetric encryption (2.65ms).following figure shows the delay at various speeds with various no. of vehicles. [40], [41], [42].

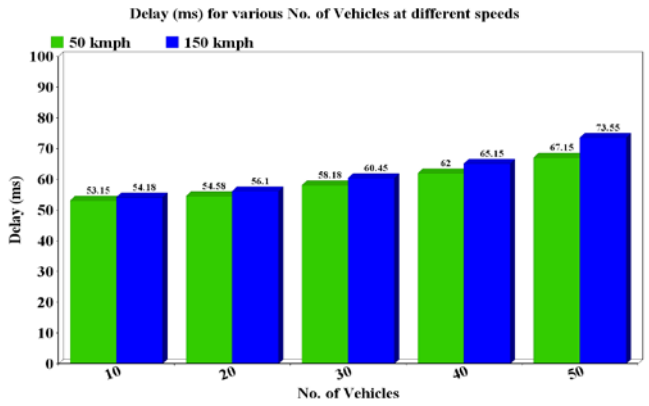

Figure showing the Delay for various no. of vehicles moving at 50 kmph and 150 kmph

6.3 Driver's Privacy

The model is capable keeping the drivers information and route secret, as the record for the vehicles are to be deleted after the revocation of the particular pseudonym moreover the model does not require the new segments to perform the authentication for the incoming vehicle of its own, meaning no complex binding of hash values from previous pseudonyms will be another step in keeping the driver's route privacy as well.

7 Discussion

The above proposed model is capable of limiting certain challenges which we faced in other authentication based schemes. As mentioned that unlike the complex and time consuming scheme of Privacy Preserving detection of Sybil attack, this method is less complex and have short processing time on the other hand the shared or stolen keys cannot be used.

As far as timestamp mechanism is concerned, this model resolves this problem by forcing each vehicle to request its own pseudonyms for vehicular communication. Even in city scenarios road side units will be able to deal with multiple requests and issue the pseudonyms to respective vehicles. For the problems faced by adjacently placed RSUs proper area definition can be helpful to avoid such problems.

Where as in foot printing where problems of RSUs overlapping can lead to the multiple authorization of messages in turn leading to Sybil attack, this method can help in mitigating these vulnerabilities by making the process of authentication and authorization area bound. The complex trajectories and signing of messages by the RSUs can be avoided.

Conclusion

We have explained how Sybil attacks can prove harmful for the vehicular ad hoc networks and what are the various mechanisms and models to prevent such attacks. With the authentication based models considered as one of the most effective, we proposed certain improvements and amend-ments that can

be brought up in order to solve some tech-nical problems face by authentication based mechanisms.

REFERENCES

[1] Lu, R., Security and Privacy Preservation in Vehicular Social Networks, Doctoral dissertation, University of Waterloo, 2012.

[2] J.R Douceur, "The Sybil attack," Proceedings of the International Workshop on Peer to Peer Systems, 251–260, 2002.

[3] Sood, M., & Vasudeva, A., Perspectives of Sybil Attack in Routing Protocols of Mobile Ad Hoc Network. In Computer Networks & Communications (NetCom), Vol. 131, 3-13, 2013.

[4] Karlof, C., Wagner, D., Secure routing in wireless sensor networks: Attacks and countermeasures, Ad hoc Networks Journal (Elsevier,) vol. 1, 293 -315, 2003.

[5] J. Newsome, E. Shi, D. Song, A. Perrig, "The Sybil attack in sensor networks: analysis & defenses," In Proceedings of the 3rd international symposium on Information processing in sensor networks, 259-268, 2004.

[6] G. Yan, S. Olariu, M. C. Weigle, "Providing VANET security through active position detection," Computer Communications, vol. 31, No. 12, 2883-2897, 2008.

[7] B. N. Levine, C. Shields, N. B. Margolin, "A survey of solutions to the Sybil attack," MA, University of Massachusetts: Amherst, 2006.

[8] A. Boukerche, H. A. Oliveira, E. F. Nakamura, A. A. Loureiro, "Vehicular ad hoc networks: A new challenge for localization-based systems," Computer communications, Vol. 31, No. 12, 2838-2849, 2008.

[9] H. Wang, J. Wan, R. Liu, "A novel ranging method based on RSSI," Energy Procedia, Vol. 12, No. 1, 230-235, 2011.

[10] C.-H. Ou, "A roadside unit based localization scheme for vehicular ad hoc networks," Int. J of Communication Systems Wiley, No. 51, 123-130, 2012.

[11] J. T. Isaac,, S. Zeadally, J. S. Camara, "Security attacks and solutions for vehicular ad hoc networks" Communications IET, Vol. 4, No. 7, 894-903, 2010.

[12] K. Ibrahim, "Data aggregation and dissemination in vehicular ad-hoc networks," Doctoral dissertation, Old Dominion University, Norfolk, Virginia, 2011.

[13] P. Y. Shen, "An efficient public key management regime for vehicular ad hoc networks (VANETS)," Masters by Research thesis, Queensland University of Technology, 2011.

[14] G. Yan, W. Yang, J. Li, V. G. Ashok, "Active position security through dynamically tunable radar," In Mobile Ad hoc and Sensor Systems (MASS), IEEE 7th International Conference, 733-738, 2010.

[15] B. Xiao, B. Yu, C. Gao, "Detection and localization of Sybil nodes in VANETs," Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks, 1-8, 2006.

[16] B. Yu, , C. Z. Xu, B. Xiao, "Detecting Sybil attacks in VANETs," Journal of Parallel and Distributed Computing, Vol. 73, No. 6, 746–756, 2013.

[17] M. Demirbas, Y. Song, "An RSSI-based scheme for Sybil attack detection in wireless sensor networks," In Proc. Of International Symposium on a World of Wireless, Mobile and Multimedia Networks, 564–570, 2006.

[18] S. Zhong,, L.E. Li, Y.G. Liu, Y.R. Yang, "Privacy-reserving location based services for mobile users in wireless networks," Technical Report. YALEU/DCS/TR-1297, Department of Computer Science, Yale University, 2004.

[19] S. Abbas,, M. Merabti, , D. Llewellyn-Jones, K. Kifayat, "Lightweight Sybil Attack Detection in MANETs," IEEE, Systems Journal, Vol. 7, No. 2, 236-248, 2013.

[20] B. Dutertre,, S. Cheung, J. Levy, "Lightweight Key Management in Wireless Sensor Networks by Leveraging Initial Trust. Technical Report," SRI-SDL-04-02, SRI Int'l 2004.

[21] S. Capkun,, L. Buttyán, J. P. Hubaux, "Self-Organized Public Key Management for Mobile Ad Hoc Networks," IEEE Trans. Mobile Computing, Vol. 2, No. 1, 52-64, 2003.

[22] S. Chang, , Y. Qi, H. Zhu, J. Zhao, X. Shen, "Footprint: detecting Sybil attacks in urban vehicular networks," IEEE Transactions on Parallel and Distributed Systems, Vol. 23, No. 6, 1103-1114, 2012.

[23] S. Park, B. Aslam, D. Turgut, C. C. Zou, "Defense against Sybil attack in the initial deployment stage of vehicular ad hoc network based on roadside unit support," Security and Communication Networks, Vol. 6, No. 4, 523–538, 2013.

[24] T. Zhou, , R. R. Choudhury, P. Ning, K. Chakrabarty, "P2DAP—Sybil Attacks Detection in Vehicular Ad Hoc Networks," Selected Areas in Communications, IEEE Journal, Vol. 29, No. 3, 582-594, 2011.

[25] M. A. Razzaque, A. Salehi, S. M. Cheraghi, "Security and Privacy in Vehicular Ad-Hoc Networks: Survey and the Road Ahead," Springer Berlin Heidelberg, In Wireless Networks and Securit, 107-132, 2013.

[26] Car 2 Car Communication Consortium Manifesto, work in progress, May 2007.

[27] M. Nekovee, "Sensor networks on the road: the promises and challenges of vehicular ad hoc networks and vehicular grids," In Proc. of the Workshop on Ubiquitous Computing and e-Research, Edinburgh, UK, May 2005.

[28] J. Blum, A. Eskandarian, and L. Hoffmman, "Challenges of inter vehicle ad hoc networks," IEEE Trans. Intelligent Transportation Systems 5(4) (December 2004):347–351.

[29] C2C CC: Car-to-Car Communication Consortium. http://www.car-to-car.org/

[30] NoW: Network on Wheels. http://www.network-on-wheels.de/

[31] PATH: California Partners for Advanced Transit and Highways. http://www.path.berkeley.edu/

[32] FleetNet: Internet on the Road. http://www.et2.tuharburg.de/fleetnet/english/vision.html

[33] GST: A Global System for Telematics enabling on-line safety services. http://www.gstproject.org/

[34] SEVECOM: Secure Vehicular Communications. http://www.sevecom.org

[35] P. Papadimitratos et al., Secure vehicular communications: Design and architecture, IEEE Communications Magazine, 2008, 46(11), 100–109.

[36] M. Raya and J.-P. Hubaux, The security of vehicular ad hoc networks. In: Workshop Security in Ad hoc and Sensor Networks (SASN),Hilton Alexandria Mark Center, Alexandria, VA, USA, November 7, 2005.

[37] B. Parno and A. Perrig, Challenges in securing vehicular networks. In: Workshop Hot Topics in Networks (Hot Nets–IV), 2005.

[38] Car 2 Car Communication Consortium Manifesto, work in progress, May 2007.

[39] F. Kargl, Z.Ma, and E. Schoch, Security engineering for VANETs, in Proceedings of 4th Wksp. Embedded.

[40] J. Blum, A. Eskandarian, and L. Hoffmman, "Challenges of inter vehicle ad hoc networks," IEEE Trans. Intelligent Transportation Systems 5(4) (December 2004):347–351. Sec. in Cars, Berlin, Germany, November 2006, pp. 15–22.

[41] Lv S, Wang X, Zhao X, Zhou X. Detecting the Sybil Attack coopera-

tively in wireless sensor networks. Proc. of International Conference on Computational Intelligence and Security (CIS) 2008; 442–446.

[42] Abdurahmonov T, Yeoh E, Hussain HM. Improving smart card security using elliptic curve cryptography over prime field (Fp), Studies in Computational Intelligence, Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, Springer 2011; 368: 127–140.

[43] Calandriello G, Papadimitratos P, Lloy A, Hubaux J-P. Efficient and robust pseudonymous authentication in VANET. Proc. of the Workshop on Vehicular Ad Hoc Networks (VANET) 2007.