Suresh Gyan Vihar University, Jaipur
International Journal of Converging Technologies and Management (IJCTM)
Volume 2, Issue 1, 2016
ISSN : 2455-7528

A new Secure Framework for Provide the security of VANET network for Secure Communication

[1]Vikash Poonia, 2Dr Dinesh Goyal
Research Scholar[1], Principal [2]
Suresh GyanVihar University, Jaipur

Abstract:-In this paper is a security infrastructure for vehicular Ad Hoc Networks (VANETs) presented by a combination of authentication based on asymmetric cryptography and a subsequent symmetric encryption and authentication system is particularly well adapted to the requirements of a VANETs. The security infrastructure enables the integrity and authenticity of all messages in the VANET to secure without significant loss of performance or violations of privacy to accept. The proposal is based on a detailed requirements analysis and some fundamental considerations with regard to identity and authentication in VANETs.

1 Introduction

Vehicular Ad Hoc Networks (VANETs) can as a subset of the in [2] defined mobile ad hoc networks (MANETs are understood. The data is transmitted wirelessly and each participant (node) messages from other nodes must forward to the functioning of the network to ensure. The characteristic feature of the VANETs is that as a node only vehicles such as cars, trucks or buses will be accepted. The movement of the nodes is not random, but follows the existing roads and traffic rules and partly by the behavior of the other nodes affected. Due to the relatively fixed motion options can at critical points (e.g. busy roads dangerous places etc.) stationary transmitters which are certain services and access to the other (stationary) networks can communicate [5]. Vehicles are also subject to points in the energy supply, available space and the available computing capacity is not the strict restrictions that are usually present in MANETs are adopted [3]. Rather a disadvantage are the potentially very high speeds of the nodes (up to 250 km/h) and the great extension of VANETs.

The main aim of a VANET is to increase traffic safety. This objective is achieved by locally available in the vehicle Telematics data e.g. via current speed, acceleration, position, etc. with the other vehicles and thus be replaced in any vehicle into a global picture of the traffic situation. Abnormal or hazardous road conditions such as accidents, congestion or ice can thus be detected at an early stage and the driver has more time to adequately respond to. In addition to this exchange of Telematics data (and the resulting warnings) should also use signals and instructions for example from the police or fire department via the VANET distributed, the inter alia by influencing the traffic light systems for free travel for the use of vehicles. In addition to theseapplications, the transport safety and the behavior of the participants directly influence many services are also planned in the comfort range, such as location-based services, internet access, remote maintenance of the vehicle etc. [1].

These three categories imply different requirements on the security objectives of confidentiality, integrity and availability. Nevertheless, in order to achieve the goals of the protection is always a security infrastructure needs a basis of trust and creates the use of cryptography. The security infrastructure

Suresh Gyan Vihar University, Jaipur
International Journal of Converging Technologies and Management (IJCTM)
Volume 2, Issue 1, 2016
ISSN : 2455-7528

therefore includes all the technical and organizational measures and facilities to the attainment of the protection objectives are required.

2 Requirements

In this section are the requirements of a security infrastructure for VANETs are explained in more detail. If necessary, according to the three categories of "Telematics Application Messages and Alerts" (A1), "alarm signals and instructions" (A2) and "Comfort Services" (A3). The requirements are listed in Table 1.

2.1 Integrity

the security infrastructure must be mechanisms to make a change to the messages in the transmission in the VANET prevent or recognizable (I1). Malicious between stations can therefore forwarded messages no longer change unnoticed.

For messages from A2, the receiver must in addition the identity or the authorization of the transmitter to send such messages can clearly determine (I2a), since the receiver such messages "blind" must follow. In contrast, messages from A1 plausibility checks are carried out with the help of their own sensors and messages of other traffic participants, allowing the unique identification of the transmitter is not absolutely necessary. The creation of motion or to make it difficult for service usage profiles, it is even desirable that the identity of the sender in the message is not to have to give price (D1). For non-Strafes supplying false information or to prevent unauthorized service usage, it should but also for such messages possible, the identity of the sender - at least - subsequently to prove beyond doubt to be able (I2b). It must therefore also the protection objectives of attribution and non-repudiation can be achieved. Anonymous participation in the VANET should therefore be prevented, pseudonyms participation is desirable.

A subsequent exposure of the identity, but only in the case of serious infringements (e.g. repeated sending false warnings that the transport safety at risk) and under precisely defined conditions possible. An automated monitoring or enforcement, for example on the basis of the sent telematics data - may in accordance with the multilateral security is not possible (D2). Multilateral security means that the interests of all stakeholders are taken into account. In the specific case are the interests of the law enforcement authorities (as far as possible any infringement of the rules of the road with as little expense as possible to pursue the interests of citizens (not suspected independently monitored and automated to be penalized in relation to).Ensure that the inside of the vehicle data collected by sensors are correct, is provided.

The integration of the correct time and location information in the messages for protection against replay and position spoofing attacks is also provided. This data is used by other infrastructure such as Galileo [3].

2.2confidentiality

The confidentiality requirements of confidentiality differ greatly between the three categories of applications. While in the case of alarm signals the confidentiality of user data is negligible, is with the may pay comfort services confidentiality is usually very important to obtain a theft of service or unwanted information profit in between nodes to prevent. The security infrastructure must therefore provide mechanisms with which the confidentiality of user data in various stages (no confidentiality, confidentiality before non-VANET participants, confidentiality especially not direct communication partners) can be achieved (V1).

Because in some circumstances the mere knowledge of an existing communication relationship between two parties unwanted information profit can bring with it, should also include the identity of the sender and receiver are protected in the best possible (D3), but without the above required attribution and non-repudiation to endanger. With regard to the confidentiality of the user data, there is no direct dependencies on accountability and content integrity, it can therefore be implemented largely independently.

In addition to the application and connection data must also be administrative messages, such as the routing protocol messages or messages for the management of the used cryptographic keys are

Suresh Gyan Vihar University, Jaipur
International Journal of Converging Technologies and Management (IJCTM)
Volume 2, Issue 1, 2016
ISSN : 2455-7528

protected against unauthorized monitoring (V2). Also the cryptographic keys that are in the possession of the participants or even central instances must be protected against unauthorized access. In general is also the security infrastructure to protect against attacks (V3).

2.3 Performance

Since many messages in VANET increase transport safety, will hang in the extreme case of human life on the timely processing of messages (availability).But in order for the above mentioned integrity and confidentiality requirements, from the computer units of the VANET participants additional cryptographic operations will be carried out by the preparation of the message time significantly extend. The measures of the integrity assurance increase the message length. For the real-time needs to be able to if the security infrastructure provided mechanisms so as efficiently as possible in regard to the required computing capacity and bandwidth (P1). Measures are also desirable, the Denial-of-Service (DoS) attacks or at least more difficult and thus increase the availability.

2.4 performance

Performance and acceptance ofconstruction and operation of the security infrastructure are connected with costs, particularly with the introduction of VANETs significantly on the rate of equipment of vehicles with VANET technology and thus on the value of this network can have an impact. For this reason, it is important to ensure that the costs of the additionally required vehicle hardware and software (W1) and the costs of the registration of new VANET participants is kept as low as possible (W2). It is important to note that initial costs and possibly also for the build-up of a stationary network and maintenance costs for central instances can accrue. All tasks are on the one hand as cost-effectively as possible to cope with (W3), on the other hand to the operator of the infrastructure the acceptance of all participating VANET enjoy (W4). If necessary, the various tasks to different institutions to distribute.

I1 content integrity of the
I2a unique sender authentication for A2
I2b subsequent accountability for A1 and A3 V1
V2 different levels of confidentiality administrative messages
V3 Protection of the security infrastructure
D1 protection before profile creation
D2 protection against monitoring
D3 Protection of the transmitter and receiver identity P1 efficiency in computing capacity and bandwidth
W1 Low Cost for vehicle hardware and software
W2 little effort for the registration
W3 operating in the most cost-effective
W4 acceptance of the participant

Table 1: Requirements

3 Basic considerations

The following are some of the fundamental issues which the concrete design of the security infrastructure of influence. It will discuss what as the identity of a subscriber are used and how the authentication of the participants.

3.1 Identity

An identity provides the basis for any authentication, i.e. it represents a certain recognition feature against which you e.g. working correctly or cooperative participants to allow VANET and faulty or malicious can exclude. This implies that a node of course neither anonymous occur nor its identity can change any, because otherwise all measures of Regulation into the void. The nature of an identity in VANETs is initially not clearly defined. A VANET-identity can identity characteristics of the vehicle, the current operator or of the holder or of both together.

Vehicle-related identity

In VANETs will apply in addition to any personal data in ground vehicle-related, often automatically sent data (e.g. telematics messages). It is also possible that the current operator is not responsible for any false declarations, but this is a defect of the vehicle or from the manipulation of watches. In this case a vehicle-specific identity appears very suitable.

Be stolen or in criminal activities involved must be tracked vehicles, identity characteristics of the vehicle (such as chassis number, number plate, etc.) as a mandatory part of a VANET-identity. This corresponds to a digital form of the current situation: a number plate pseudonymised the holder of a

vehicle, the driver cannot be determined with certainty. Such a vehicle-related identity would be directly in the vehicle in tamper-resistant hardware to save.

Personal Identity

The second variant are personal VANET identities that are directly related to the operator of the relevant vehicle, since all messages directly to the driving style or theStatus of the truck. This approach also facilitates the reconstruction of accident and driver flight situations in which only the accident vehicle and therefore the holder but not the driver could be determined with certainty if this is the scene of the crime had withdrawn.

This the current legislation to that in principle the vehicle holder accountable. The note on the vehicle holder bars without great effort also clean vehicle-related identities, because the executive is already the holder of documents such as vehicle registration certificate and certificate of approval letter or Part 1 and Part 2 or via your central store.

However it seems that at least for those participants in a VANETs personal identities to use with increased privileges, such asforces of the police, fire department, etc. then there is still the question how can be decided whether a person may use their privileges straight. A policeman should for example, if he is out of his time in the private car is on the road, no instructions to other traffic participants can send. This issue is further discussed below address the joint identities.

The large number of possible driver also raises the question of where personal identities should be saved. A pre-installed on the vehicle itself leaves, because you cannot foresee which persons the car will use. A further variant are also not the vehicle keys: On the one hand, due to cost reasons not for each driver has its own unique key will be provided to the other location the administration and storage of the cryptographic material without alternative option in the hands of the automobile manufacturers.

Electronic driving licenses on the other hand are on offer: each driver must be a valid anyway 2 driving license and prove it if necessary, i.e... The saving of identity on an electronic driving license in the form of a smart card is hardly a loss of comfort for the VANET-user, it should however be exchanged the previous license.

In this solution, synergies can be found in relation to the reorganization of the driving and rest periods (Reg. 3820/85), whose implementation is expected for May 2006 [Ind06]. In consequence of these new rules are so-called driver cards to drivers of motor vehicles is issued under Regulation 3820/85. The driver card is "one of the authorities of the Member State of allocated deliverable, personal transfer and storage device for the purposes of identification of a driver and storage of essential data" (Regulation (EC) No 2135/98 Annex I B). You could use this driver card without major problems as electronic driving license and also remove for identification in VANETs use.

Now one of such electronic driving license from the vehicle is forced to start provided that could give a vehicle holder when his vehicle to another driver against claims from non-secure situations caused by him. It would also give the device precisely define who may travel with the vehicle. Driving without a valid driving license could be contained. One such constraint is now legally but not to enforce and in addition from the following reasons is also not desirable: in the event of a forced through identification of the vehicle could be, for example, problems arise if a vehicle in an emergency, but had to be moved is no demonstrably justified local driver.

Under the circumstances it could also happen that the holder of the rights to accidentally removes his vehicle and then no more to drive them. Apart from these problems, it is

1 the driver of the vehicle is also liable to pay compensation.

2 According to 2 Para. 1 the right "by an official certificate (driving license) to assign." Who he during for the protection of privacy is not desirable that there is in principle before the trip starts at the front of the vehicle cards.

Mixed identity

With this approach, the messages of the vehicle as well as the driver attributable, passenger and vehicle-related identity features combined. To elevate privileges are used, both identities support this. Instructions as to the premises of a road were thus only valid if you from an authorized vehicle (e.g. an ambulance) with an authorized drivers. This can be used to prevent stolen vehicles to send instructions via the VANET abused.

The disadvantage of this variant is that for the creation of movement profiles per se most of the information provided. The identities are exposed in the news, an attacker can cause both certain persons as well as certain vehicles can easily track. The problem of the motion profile creation, but also for the other variants if the identities are unprotected. Under unprotected, it is important to understand that the identities on the one hand, are transferred in plain text and on the other hand also does not need to be changed.

In addition, may cost more by the fact that two identities are required. It is on the one hand the vehicle-related identity produced and in tamper-resistant hardware in the vehicle is stored, as well as on the other hand the personal identity on an electronic driving license.

Conclusion

On the basis of the currently applicable legal basis appears a vehicle-specific identity appropriately with the help of the holder of the vehicle can be determined. For special groups of people such as police officers should however also be used personal identities to which you're special privileges are bound. The privileges are then only in the combination of vehicle-related and personal identity.

For certain situations, such as for the commercial rental of vehicles, it is useful in addition to the vehicle-related also a personal identity for "normal" operator to use to the holder to some extent to protect against third party claims. In this case, however, a subsequent identification of the driver is sufficient. The personal identity must therefore not necessarily in the VANET, but could be used together with the travel time and any other data in tamper-resistant hardware in the vehicle is stored. These data are then however against unauthorized reading to protect. An electronic driving licenses for access control to the truck appears as an option makes sense, however, it should not be forced to VANET identity belong.