International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 2, February - 2014

Secured Communication over VANETs - A Survey

Shazia Sulthana
Assistant professor
Department of electronics & communication
Global Academy of Technology
Bangalore, India

Abstract—**Vehicular Adhoc Networks (VANETs) are emerging mobile ad-hoc network technologies incorporating mobile routing protocols for inter-vehicle data communications to support intelligent transportation systems .Establishment of a secure communication architecture within vehicular ad hoc networks address special challenges, due to the characteristic and high dynamic and mobility of nodes, high rate of topology changes, high variability in nodes density and neighborhood, broadcast/geo-cast communication nature .Vehicular ad hoc networks (VANETs) are therefore target of several malicious attacks (internal or external), in addition to intentional faults and errors. As mobile wireless devices and networks become increasingly important, the demand for Vehicle-to-Vehicle (V2V) and Vehicle to-Roadside (VRC) or Vehicle-to-Infrastructure (V2I) Communication will continue to grow. This paper surveyed on different concept for secure communication over VANET.**

Keywords—VANET, intelligent transport system Security Requirements, ,propagation model, security attacks , simulation parameters. Introduction (*HEADING 1*)

INTRODUCTION

Over the past two decades, vehicular networks have been emerging as a cornerstone of the next generation Intelligent Transportation Systems (ITSs), contributing to safer and more efficient roads by providing timely information to drivers and concerned authorities. In vehicular networks, moving vehicles are enabled to communicate with each other via inter vehicle communications as well as with road-side units (RSUs) in vicinity via roadside-to vehicle communication The required protocols to support MANET are more complex as compared to other non-mobile networks because due to mobility there is no predefined infrastructure or topology of MANET. VANET is a unique type of network which comes under the umbrella of MANET. VANET has transmission mode is often broadcast. (3) The power available is sufficient A vehicular ad hoc network (VANET) is also known as a vehicular sensor network by which driving safety is enhanced through inter-vehicle communications or communications with road-side infrastructure. It is an important element of the Intelligent Transportation Systems (ITSs). In a typical VANET, each vehicle is assumed to have an on-board unit (OBU) and there are road-side units (RSU) installed along the roads. A trusted authority (TA) and maybe some other application servers are installed in the backend. The OBUs and RSUs communicate using the Dedicated Short Range Communications (DSRC) protocol over the wireless channel while the RSUs, TA, and the application servers communicate using a secure fixed network (e.g. the Internet). The basic application of a VANET is to allow arbitrary vehicles to broadcast safety messages (e.g. road condition, traffic accident information) to other nearby vehicles.

In this paper, sections 1 and 2 deal with overview of VANET and basic VANET Network model. Section 3 points out threats to VANET and security requirements. Further sections deal with the different methodologies and propagation models and finally conclusion.

I. ARCHITECTURE OF VANET SYSTEM MODEL

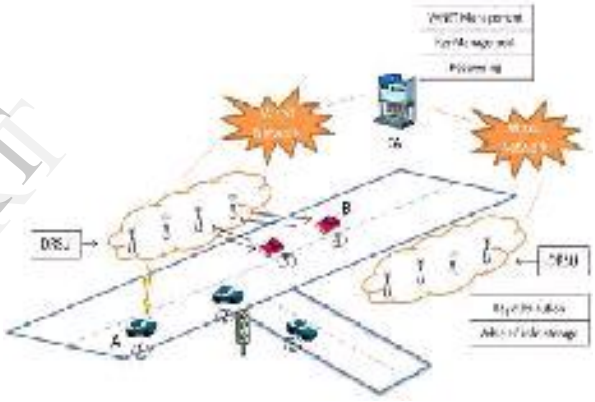

Fig 1. System model

A. Certificate Authorities

Certificate Authorities (CA) are called CA and are responsible as administrate department in VANET. They hold all the secrets and have responsibilities to solve disputes. They are used to do VANET management, key management and recovering. The authority has the highest security level.

B. Distributed Road Side Units (DRSUs)

RSUs are agents of the authority and deployed at the road sides. Distributed Road Side Units (DRSUs) are a set of RSUs. They are used to distribute key and store information from vehicles. However, there is a bottleneck problem of RSU in original VANET. If the RSU is compromised, the message in its coverage cannot be transformed successfully, especially as the message is important and has higher safety requirements. The DRSUs group is semi-trusted with the medium security level. An RSU can be a powerful device or a comparatively simple one. The set of RSUs in a DRSUs group is comparatively simple ones.

C. On Board Units

On Board Units (OBUs) are ordinary vehicles on the road that have ability to communicate with each other through Integrated Intelligent Research (IIR) After registered information on CA as required, an ordinary vehicle can join VANET and be assigned some initial values. OBUs have the lowest security level. Because semi trusted RSU may be compromised

II. OVERVIEW OF VANET

A. Intelligent transportation systems (ITSs)

In intelligent transportation systems, each vehicle takes on the role of sender, receiver, and router to broadcast information to the vehicular network or transportation agency, which then uses the information to ensure safe, free-flow of traffic. For communication to occur between vehicles and Road Side Units (RSUs), vehicles must be equipped with some sort of radio interface or On Board Unit (OBU) that enables short-range wireless ad hoc networks to be formed. Vehicles must also be fitted with hardware that permits detailed position information such as Global Positioning System (GPS) or a Differential Global Positioning System (DGPS) receiver. Fixed RSUs, which are connected to the backbone network, must be in place to facilitate communication. The number and distribution of roadside units is dependent on the communication protocol is to be used. For example, some protocols require roadside units to be distributed evenly throughout the whole road network; some require roadside units only at intersections, while others require roadside units only at region borders. Though it is safe to assume that infrastructure exists to some extent and vehicles have access to it intermittently, it is unrealistic to require that vehicles always have wireless access to roadside units. Figures 2, 3 and 4 depict the possible communication configurations in intelligent transportation systems. These include inter-vehicle, vehicle-to-roadside, and routing-based communications. Inter-vehicle, vehicle-to-roadside, and routing-based communications rely on very accurate and up-to-date information about the surrounding environment, which, in turn, requires the use of accurate positioning systems and smart communication protocols for exchanging information. In a network environment in which the communication medium is shared, highly unreliable, and with limited bandwidth , smart communication protocols must guarantee fast and reliable delivery of information to all vehicles in the vicinity.

a. Inter-vehicle communication

Fig 2: Inter-Vehicle Communication

Inter-vehicle communications allow a mobile vehicle to communicate with its surrounding environment, mobile or fixed networks. More specifically, vehicular nodes can communicate with their peers either via vehicle-to-vehicle communications or through the fixed roadside infrastructure. The communication and the delivery of information may range from motion data (speed, direction, location, etc.) to Internet media content, through the wide variety of supported applications that operate in a vehicular network. The inter-vehicle communication configuration uses multi-hop multicast/broadcast to transmit traffic related information over multiple hops to a group of receivers. In intelligent transportation systems, vehicles need only be concerned with activity on the road ahead and not behind (an example of this would be for emergency message dissemination about an imminent collision or dynamic route scheduling). There are two types of message forwarding in inter-vehicle communications: naïve broadcasting and intelligent broadcasting. In naïve broadcasting, vehicles send broadcast messages periodically and at regular intervals. Upon receipt of the message, the vehicle ignores the vehicle ignores the message if it has come from a vehicle behind it. If the message comes from a vehicle in front, the receiving vehicle sends its own broadcast message to vehicles behind it. This ensures that all enabled vehicles moving in the forward direction get all broadcast messages. The limitations of the naïve broadcasting method is that large numbers of broadcast messages are generated, therefore, increasing the risk of message collision resulting in lower message delivery rates and increased delivery times.

Intelligent broadcasting with implicit acknowledgement addresses the problems inherent
in naïve broadcasting by limiting the number of messages broadcast for a given emergency event. If the event-detecting vehicle receives the same message from behind, it assumes that at least one vehicle in the back has received it and ceases broadcasting. The assumption is that the vehicle in the back will be responsible for moving the message along to the rest of the vehicles. If a vehicle receives a message from more than one source it will act on the first message only.

b. Vehicle-to-roadside communication

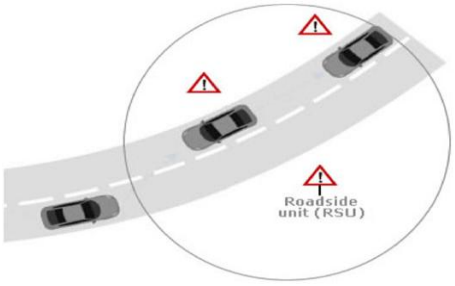

Fig 3. Vehicle to Roadside Communication

The vehicle-to-roadside communication configuration (Fig. 3) represents a single hop broadcast where the roadside unit sends a broadcast message to all equipped vehicles in its vicinity. Vehicle-to-roadside communication configuration provides a high bandwidth link between vehicles and roadside units. The roadside units may be placed every kilometer or less, enabling high data rates to be maintained in heavy traffic. For instance, when broadcasting dynamic speed limits, the roadside unit will determine the appropriate speed limit

according to its internal timetable and traffic conditions. The roadside unit will periodically broadcast a message containing the speed limit and will compare any geographic or directional limits with vehicle data to determine if a speed limit warning applies to any of the vehicles in the vicinity.

C Routing-based communication

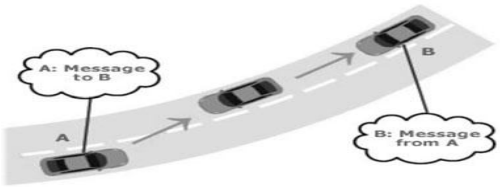

Fig 4. Routing Based Communication

The routing-based communication configuration (Fig. 4) is a multi-hop unicast where a message is propagated in a multihop fashion until the vehicle carrying the desired data is reached. When the query is received by a vehicle owning the desired piece of information, the application at that vehicle immediately sends a unicast message containing the information to the vehicle it received the request from, which is then charged with the task of forwarding it towards the query source.

III. THREATS TO AVAILABILITY

Attackers can be classified according to scope, nature, and behavior of attacks. Some types of attackers are discussed in following paragraph:

1. Some attackers eavesdrop only on the wireless channel to collect traffic information which may be passed onto other attackers. As these attackers do not participate in the communication process of the network, they are called passive attackers. On the other hand, some attackers either generate packets containing wrong information or do not forward the received packets. These are called active attackers.

2. Attacker may be an authentic member of a VANET having authentic public keys and access to other members of the network. Such attackers are called insider. Outside attackers (outsider) are intruders and they can launch attacks of less diversity.

3. Some attackers are not personally benefited from the attack. Their aim is to harm other members of the network or disrupt the functionality of a VANET. These attackers are malicious. On the other hand, rational attacker seeks personal benefit and is more predictable in terms of type and target of the attack.

A Types of Attacks

Several types of attacks have been identified and classified on the basis of layers used by the attacker. At the physical and link layer, an attacker can disturb the network system by overloading the communication channel with useless messages. An attacker can inject false messages or rebroadcast an old message also. Some attackers can tamper with an OBU or destroy an RSU. At network layer, an attacker can insert false routing messages or overload the system with routing information. Privacy of drivers can be disclosed by revealing and tracking the position of drivers. Some of these attacks are briefly explained subsequently.

1) Bogus Information

In this case, attackers are insiders, rational, and active. They can send wrong information in the network so that it can affect the behavior of other drivers. For example, an adversary can inject wrong information about a nonexistent traffic jam or an accident diverting vehicles to other routes and freeing a route for itself.

2) Cheating with Sensor Information

This attack is launched by an attacker who is insider, rational, and active. He uses this attack to alter the perceived position, speed, and direction of other nodes in order to escape liability in case of any mishap.

3) ID Disclosure

An attacker is insider, passive, and malicious. It can monitor trajectories of a target vehicle and can use this information for determining the ID of a vehicle.

4) Denial of Service (DOS)

Attacker is malicious, active, and local in this case. Attacker may want to bring down the network by sending unnecessary messages on the channel. Example of this attack includes channel jamming and injection of dummy messages.

5) Replaying and Dropping Packets

An attacker may drop legitimate packets. For example, an attacker can drop all the alert messages meant for warning vehicles proceeding toward the accident location. Similarly, an attacker can replay the packets after that event has been occurred to create the illusion of accident.

6) Hidden Vehicle

This type of attack is possible in a scenario where vehicles smartly try to reduce the congestion on the wireless channel. For example, a vehicle has sent a warning message to its neighbors and it is awaiting a response. After receiving a response, the vehicle realizes that its neighbor is in a better position to forward the warning message and stops sending this message to other nodes. This is because it assumes that its neighbor will forward the message to other nodes. If this neighbor node is an attacker, it can be fatal for the system.

7) Sybil Attack

In this attack, a vehicle forges the identities of multiple vehicles. These identities can be used to play any type of attack in the system. These false identities also create an illusion that there are additional vehicles on the road. Consequence of this attack is that every type of attack can be played after spoofing the positions or identities of other nodes in the network.

8) Black Hole Attack

A black hole is formed when nodes refuse to participate in the network or when an established node drops out. When the

node drops out, all routes it participated in are broken leading to a failure to propagate messages

IV. PROPAGATION MODELS

The propagation environment in the simulator is used to judge the effects of propagation of electro-magnetic waves through the medium, usually this medium is air. Propagation models can be classified in large scale and fading or small-scale models. From an implementation point of view they can be either deterministic or probabilistic.

A. Deterministic Models

A deterministic model allows computing the received signal strength, based on actual properties of the environment such as the distance between transmitters T and a receiver R. These models range from simple (only account for distance between nodes) to very complex where they also account for multipath propagation in the environment modeled exactly as the area of deployment.

Distance measurement model based on RSSI in WSN.

1) Free Space model

This is the type of RSSI which is suitable for special environment. This model is sometimes also referred to as Friis model. The received power depends only on the transmitted power, the antenna gain and the distance between the sender and the receiver, the idea is that, as a radio wave travels away from an (Omni-directional) antenna, the power decreases with the square of the distance.

$$P_r(d) = P_t G_t G_r \lambda^2 / (4\pi)^2 d^{\alpha} L \qquad (2)$$

Where Pt is the transmitted power, G_t and G_r are the gains of the transmitter and receiver antenna gains and_ is the wavelength. _ is the path loss exponent and is in Free Space. L is the system loss. Often, Gt, Gr and L are set to 1 (matched antennas and no system loss).

1) Ground model:

This is the type of RSSI which is suitable for special environment. The two-ray ground model also accounts for a reflection via the ground, given the dielectric properties of the earth in addition to the direct line of sight (LOS).This model gives more accurate predictions at longer range than the Free Space model and is given as follows:

$$P_r(d) = P_t G_t G_r h_t^{\,2} h_r^{\,2} / d^4 L \qquad (3)$$

Where ht and hr are the heights (in meters) of the transmit and receive antennas respectively. Eq. (3) shows faster power loss than (2), but does not give good results for short distances because of oscillation caused by the constructive and destructive combination of the two separate paths. To cope with this, either (2) or (3) are used based on the magnitude of d, the T-R separation.

2) Log-Normal Shadowing:

This is the type of RSSI which is suitable for general environment. It describes the relationship between the RSSI value and the distance. The Log-Normal Shadow-ing model uses a normal distribution with variance _ to distribute reception power in the logarithmic domain:

$$P_r(d;\sigma^2) \approx LN(P_{r\,\det}(d), \sigma^2) \qquad (5)$$

Where Prdet is a deterministic model such as (2)or (3). As such the received power is given as:

$$P_r(d) = P_t - P_L(d_0) + 10\alpha \log(d/d_0) + x \qquad (6)$$

Here _ is a path loss exponent like the 2 in Eq. (2) and the 4 in Eq. (3). PL(d0) is a reference path loss measured close to the transmitter. Eq. (6) can be rewritten as:

$$P_r = P_r(d_0) * 10^{PL(d)} \qquad (7)$$

This gives a received power by multiplying the deterministic received power with a Power Loss scale factor in dB:

$$P_l(d) = -10\alpha \log_{10}(d/d_0) + x \qquad (8)$$

2) Rayleigh: The Rayleigh propagation model [11] models the situation when there is no LOS, and only multipath components exist. This model incorporates intensive variations in received signal power because multiple paths can either combine constructively or destructively. The amplitude, delay and phase shift of these components greatly depends on the environment.

Typical values for pathloss exponent _

Like the Log-Normal shadowing model in Eq. (5), the Rayleigh model also depends on a deterministic model to which a certain variation is applied:

$$P_{rRayleigh}(d) \cong Rayleigh(P_{r\,\det}(d)) \qquad (9)$$

Where the power factor loss can be defined as

$$P_L(d) = -\alpha \log_{10}(d/d_0) \qquad (10)$$

3) Longley-Rice: The Longley-Rice model (or Rice model) [3] models the reception powers following the Rayleigh distribution but additionally takes into account the positive effects of a LOS path with a certain scale

$$P_r(d) = P_{r\,\det}(d_0) * 10^{pl(d)} \qquad (11)$$

$$P_{rR\sec}(d) = P_r(d) * F(d) \qquad (12)$$

4) Nakagami: The Nakagami model is highly generic. Reception power follows a gamma distribution:

$$P_r(d;m) \approx Gamma(m, P_{r\,\det}(d)/m) \qquad (13)$$

The parameter m specifies the intensity of fading effects. Nakagami includes other models, such as:
_ Rayleigh for m = 1
_ Free Space for $\lim_{m\to\infty}$

V. PARAMETERS FOR SIMULATION

A wireless network simulator used in VANET research often provides a stack of protocols (reacting the ISO OSI reference model) on top of which the protocol or application under test is implemented. A component managing (possible) connections between nodes often works in conjunction with the propagation model in order to evaluate which nodes are affected by a transmission. The results could be that a node correctly receives a message or receives garbled bits due to a collision. A mobility model can be used to move the nodes around as is generally the case in a VANET either based on measured or generated trace traces, an embedded mobility model or a coupling with trace simulation software.

A simulation can have two goals: a) Perform a statistical exploration to gain insight in how a system will work in a generic environment, or b) perform a site-specific evaluation of a system to gain insight in the operational properties in a specific environment. This is a method often used in site planning, which has its roots in cellular technology.

A. Mobility

VANETs are, in fact, a subset of Mobile Ad hoc Networks (MANETs) but with several important differences. Mobility is usually constrained, because the nodes follow roads according to some physical vehicle model. This results in predictable mobility patterns (within certain bounds). Speed is generally high in VANETs, but can differ greatly (e.g. communication between stopped vehicles or vehicles passing in opposite lanes). In contrast to MANETs, nodes in a VANET generally do not have strict weight, size and power consumption limits. The assumption that a mobile device is limited in resources, which is common place in MANETs, does

not necessarily hold for VANET nodes. Furthermore, VANET nodes can safely be assumed to have access to certain peripherals such as positioning and navigation hardware. Another important difference is more of a political nature, because a vehicle may easily travel outside an area covered by a certain legislature.

B. Propagation Environment

Generally, the wireless channel is a highly chaotic and unpredictable system. On its way from transmitter to receiver a signal is being rejected, scattered and absorbed by objects in the propagation environment. As such its magnitude is altered, but due to multiple paths it can also interfere with itself or with signals sent in other frequency ranges. With the context of VANETs comes also a typical radio wave propagation environment. Vehicles generally move on roads, but other scenery can vary from open farmlands to forests to large urban canyons and bridges. Another typical property of the VANET propagation environment is the presence of large metal objects which are continuously changing position in the environment, namely the vehicles themselves. As such the environment is highly dynamic. Large-Scale effects on radio wave propagation are the following three phenomena:

1) Reflection: Reflection occurs when a wave encounter a large surface with certain optical properties. In models reflection is often translated to a path loss exponent

2) Diffraction: This phenomenon is explained by Huy gens' Principle, which states that every point on a wave Simulation front acts as the seed for a secondary wave front. This enables waves to propagate around edges or through holes. This can be modeled with the knife-edge diffraction model which can be used for site-specific modeling of propagation over mountains and large buildings.

3) Scattering: A radio wave scatters when it encounters an object which is small compared to the wavelength, spreading the waves in all directions. This can account for a received signal which is stronger than would have been predicted by reflection and diffraction alone. Small-scale effects on radio wave propagation are often referred to as fading. At the receiver multiple versions of the original signal arrive; they can be reflected and diffracted and arrive with time and phase difference. These multipath waves interfere with each other, which can cause large fluctuations in signal quality with apparently small changes in time or receiver location. This relative motion causes frequency modulation because each multipath will have a different Doppler Shift, there resulting frequency change is derived as follows:

$$F_d = v / \lambda \cos\theta \qquad (1)$$

Here v is the relative velocity, the wavelength and θ the angle between the signal path and the direction of movement.

C. Channel Parameters

A mobile channel can by characterized with channel parameters. The reception of multipath components can be seen as a sample which can be expressed by means of statistical quantities. Delay Spread is the standard deviation of the arrival times. Doppler Spread measures the spectral broadening caused by relative motion of transmitter and receiver.

D. Radio Technologies

Several communication technologies have been used in VANETs in the past, such as infrared and short range radio. The short range radio technologies used is primarily Wi-Fi, although some research is has been done in the 900MHz band and in the millimeter range (60-78GHz). Recently most VANET research converges to IEEE 802.11p [15], a Wi-Fi variety tailored for communication in the vehicular environment as part of the Wireless Access in Vehicular Environments (WAVE) standard [IEEE 802.11p builds upon the proven and mature 802.11 standards, hence providing relatively cheap but powerful and flexible communication devices. It provides low latency access to the medium communication range in the order of 1km.

Single-hop: Most of the identified safety applications are based on direct communication among vehicles within range of one another. So far, there is no need for "networking"

capabilities in the basic DSRC communication design. There are scenarios in which multiple hops of message forwarding is desired (e.g., propagating hazard warning along a roadway). These cases are best served by application level protocols which have contextual knowledge such as a digital map. Additionally, rebroadcast schemes for broadcast performance enhancement are not multihop in the proper sense.

Uncoordinated: Vehicular-safety communication is entirely distributed. There is no coordinator to facilitate orderly channel access. **Broadcast**: Safety communication in generalis targeted at vehicles for where they are rather than who they are exchanged in the control channel. No safety usage in the control channel is limited to occasional advertisements of private applications in the service channels, and is insignificant to overall channel load. Therefore, control channel communication design can and should focus on safety.

E. Signal Parameters

It goes without saying that the frequency at which a radio technology operates greatly impacts its propagation properties. Besides its carrier frequency, other metrics are the transmitted power, the bandwidth and the symbol time, these are results of the modulation scheme used and out of the scope of this paper, but a combination of signal and channel parameters can lead to different kinds of fading. .

F. Implementation in simulators

1) For every node n within a relevant distance, per-form a calculation of the received signal strength.The received signal strength is calculated using a propagation model.

2) For a transmission instance (e.g. the transmission of message x) all signal strengths from concurrent transmissions other than x received at node n are added as noise.

3) Based on the Signal-to-Interference and Noise Ratio (SINR) and Bit Error Rate (BER) a decision is made whether the message is correctly received or has bit errors. If the SINR is below a certain threshold it is impossible to detect the signal in the received noise, and a collision has occurred.

Later, two group-signature-based schemes have been proposed, where a message received from multiple distinct vehicles is considered to be trustworthy. Using group signatures can provide anonymity of vehicles and suppress Sybil attacks by restraining duplicated signatures signed by the same vehicles as One practical issue of these schemes is that different messages with similar semantics may be ignored from making the decision, which leads to a biased or no final decision.

VI. METHODOLOGIES

There are so many methods used in the existing system.

A. Explicit Binding

To eliminate the threat of Sybil attacks, it is straightforward to explicitly bind a distinct authorized identity (e.g., PKI-based signatures) to each vehicle so that each participating vehicle can represent itself only once during all communications. Using explicit identities of vehicles has the potential to completely avoid Sybil attacks but violates the anonymity concern in urban vehicular networks.

B. Resource Testing

As an alternative scheme, resource testing] can be conducted to differentiate between malicious and normal vehicles, where the judgment is made whether a number of identities possess fewer resources (e.g., computational and storage ability) than would be expected if they were distinct. This scheme fails in heterogeneous environments where malicious vehicles can easily have more resources than normal ones.

C. Global Positioning Scheme

Considering the fact that a vehicle can present itself at only one location at a time, localization techniques or other schemes like the Global Positioning System (GPS) aiming to provide location information of vehicles can be exploited to detect hostile identities. However, these schemes often fail in complicated urban settings (e.g., bad GPS signals due to urban canyons, inaccurate localizations due to highly dynamic wireless signal quality).

D. Group Signature Scheme

Later, two group-signature-based schemes have been proposed, where a message received from multiple distinct vehicles is considered to be trustworthy. Using group signatures can provide anonymity of vehicles and suppress Sybil attacks by restraining duplicated signatures signed by the same vehicles as one practical issue of these schemes is that different messages with similar semantics may be ignored from making the decision, which leads to a biased or no final decision.

E. Location Hidden Approach

Recently, Location-hidden authorized message generation scheme have been proposed, where the RSU signatures on messages are signer ambiguous so that the RSU location information is concealed from

The resulted authorized message and two authorized messages signed by the same RSU within the same given period of time are recognizable so that they can be used for identification. The issue of this scheme is that RSU is considered to be trust worthy, which can also be compromised.

CONCLUSION

The establishment of secure communications within wireless networks remain a key issue because of the vulnerabilities of such environment (mobility, dynamicity, wireless links, lack of infrastructure.) The propagation model used in a VANET simulation has large influence on the results. It impacts the selection of nodes that are able to communicate and depicts the probability of correct reception. As a result, it can influence the speed at which messages propagate through the network, directly influencing end-to-end delay in a multi-hop scenario. This paper gives a survey of relevant propagation models and the methodologies for secure communication over the VANET

REFERENCES

1) Aditi Garg, Ankita Agrawal, Niharika Chaudhary, Shivanshu Gupta, Devesh Pandey, Tumpa Roy " New Lightweight Security Protocol for VANET by Using Registration Identity and Group Certificate "*International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970) Volume-3 Number-1 Issue-8 March-2013*

2) Albert wasef and rongxing lu "Complementing public key infrastructure to secure vehicular ad hoc networks" IEEE Wireless Communications October 2010

3) Lei Zhang, Qianhong Wu, Agusti Solanas, and Josep Domingo-Ferrer, *Senior Member, IEEE*A" Scalable Robust Authentication Protocol for Secure Vehicular Communications" IEEE transactions on vehicular technology, vol. 59, no. 4, may 2010.

4) Albert Wasef, *Member, IEEE*, and Xuemin Shen, *fellow,IEEE"EDR:* efficient decentralized revocation protocol for vehicular ad hoc networks" IEEE transactions on vehicular technology, vol. 58, no. 9, november 2009.

5) T.W. Chim a,⇑ , S.M. Yiu a, Lucas C.K. Hui a, Victor O.K. Li "MLAS: Multiple level authentication scheme for VANETs" T.W. Chim et al. / Ad Hoc

Networks 10 (2012) 1445–1456Contents lists available at SciVerse ScienceDirect

6) Lo-Yao Yeh a, Yen-Cheng Chen b,*, Jiun-Long Huang "PAACP: A portable privacy-preserving authentication and access control protocol in vehicular ad hoc networks" L.-Y. Yeh et al. / Computer Communications 34 (2011) 447–456Contents lists available at ScienceDirect

7) Karim El Defrawy, *Student Member*, and Gene Tsudik, *Senior Member"* PRISM: Privacy-friendly Routing In Suspicious MANETs (and VANETs)" Computer Science Department University of California, Irvine, CA, USA

8) T.W. Chim a,*, S.M. Yiu a, Lucas C.K. Hui a, Victor O.K. Li SPECS:Secure and Privacy Enhancing Communications schemes for VANETs "W. Chim et al. / Ad Hoc Networks 9 (2011) 189– 203 available at ScienceDirect

9) Sherali Zeadally · Ray Hunt · Yuh-Shyan Chen
Angela Irwin · Aamir Hassan"Vehicular ad hoc networks (VANETS): status, results, and challenges" Telecommun Syst (2012) 50:217–241 DOI 10.1007/s11235-010-9400-5 available at springer

10) Muhammad Nadeem Majeed, Dr. Shahbaz Pervez Chattha, Dr. Adeel Akram Dr. Mohammad Zafrullah " Vehicular Adhoc Networks History And Future Development Arenas *"Volume 2, Issue 2 April 2013*"International Journal of Information
Technology and Electrical Engineering

11) E.M. van Eenennaam1" A Survey of Propagation
Models used in Vehicular Ad hoc Network (VANET) Research" Design and Analysis of Communication
Systems group,Faculty of EEMCS, University of Twente, The Netherlands

12) S. Cespedes, X. Shen, and C. Lazo, "IP mobility management for vehicular communication networks:
Challenges and solutions," *IEEE CommunMag.*, vol. 49, no. 5, pp. 187–194, May 2011