A Novel Architecture for Authentication and Secure Communication in VANET

Ms. Bhagyashree Dharaskar (Gadekar)
Research Scholar SGB Amravati University and Assistant Professor Department of Computer Science, Priyadarshini Indira Gandhi College of Engineering, Hingna Road, Nagpur,

Dr. R.V. Dharaskar
Director, MPGI Integrated Campus, Nanded, Maharashtra, India

Dr. V. M. Thakare
Professor and Head, Computer Science, Faculty of Engineering & Technology, P G Department of Computer Science, Sant Gadge Baba Amravati University,Amravati

***Abstract*— Authenticate communication model provides secure inter and intra vehicles communication. This architecture uses the concept of distributed database. Every driver has to prove his identity to certified authority to get the communication rights to communicate with other vehicles. Vehicular ad-hoc network for intelligent transport system (ITS) which has become an essential service, provides safety and convenience services like mobile nodes communication, electronic toll collection system, real time audio, collision avoidance, road side safety, traffic jam using cellular phone. In this paper we present a novel architecture for user authentication and communication in Vehicular Ad hoc Networks.**

***Keywords*— Wireless communication network (WSN), VANET, GPS, WLAN, CA (Certifying Authority).**

I. Introduction

Wireless sensor networks (WSN) are easy to develop and used to localization of either devices or people in various environment. For enhancing vehicle, driver security and facilitating inter and intra vehicle communication, VANET consist of various communication patterns and policies based on local securities [1]. Certified authority contains authentication and registration algorithm to provide global communication between vehicles. Among the various wireless technologies for vehicle communication, we can use GPS algorithm [2] to find out the exact location of moving object. Form the wide range of possible use cases, we have chosen accident prevention and post accident investigation. For forensic applications the event logs are maintained for each event at vehicle road side unit and server level. The hybrid WSN architecture uses the concept of unicasting and multicasting for bidirectional communication between node to node and node to server.

II. Related work

Intelligent transport systems are building future cars that smoothly communicate with roadside infrastructure and with each other. It provides various services to improve safety and comfort of driving [11].

Cellular phone can be used as most reliable communication medium in VANET communication [4] [12]. Their fast internet access features provide more feature to VANET communication. We are implementing the authentication and communication architecture using cell phones, which will use the top end architecture for the process.

III. Secure communication

This model consists of two phases to provide authenticate communication which employs vehicles with sensor and mobile phone so that drivers can communication with each other.

Phase 1: Authentication

This phase uses the following algorithm to identify drivers' cell phone on wireless network:-

Algorithm: **User Authentication**

Step 1: Application could be downloaded in driver's cell phone.

Step 2: Fill up the downloaded application with correct and complete details.

Step 3: Return the filled application to certifying authority for approval.

Step 4: If CA found that information is genuine, it send the registration code with specific service to the mobile driver. Otherwise, request will be rejected.

Step 5: Driver, on receiving the code on his cell phone, is authenticated and becomes a part of the secure communication network.

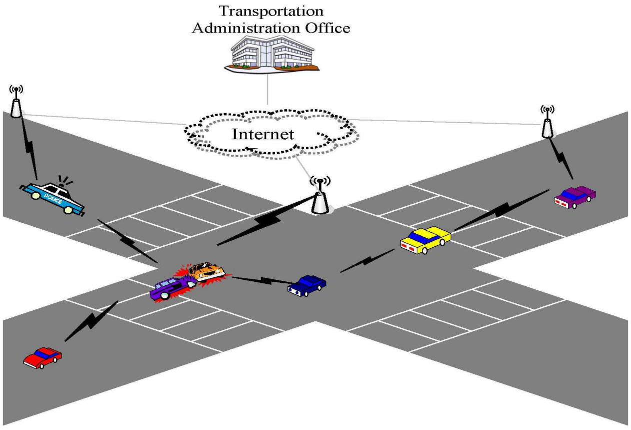

Fig.1 VANET Communication

Phase 2: Authority Privilege Assignment

Depending on type of vehicles, geographical area, and registration code different privileges in the form of communication pattern can be assigning to the drivers. It decide the policy for whom driver are able to communicate.

Phase 3: Secure Communication
The communication is either local or global. Local communication is geographical localization based. It contains bidirectional communication between vehicle-vehicle and vehicle-local server [3]. It is used in pre-accidental prevention. Global Communication called Post- accident investigation covers whole geographical area. It contains bidirectional communication between local server's and main server.
This communication play very important role in forensic investigation because it maintain log history of incoming and outgoing communication of each and every vehicles and local servers. So this concept support hierarchy of name server and main server act as it has centralized control over complete system [5]. Data are stored in local server in distributed fashion. So there are no possibilities of forming bottleneck around main server.

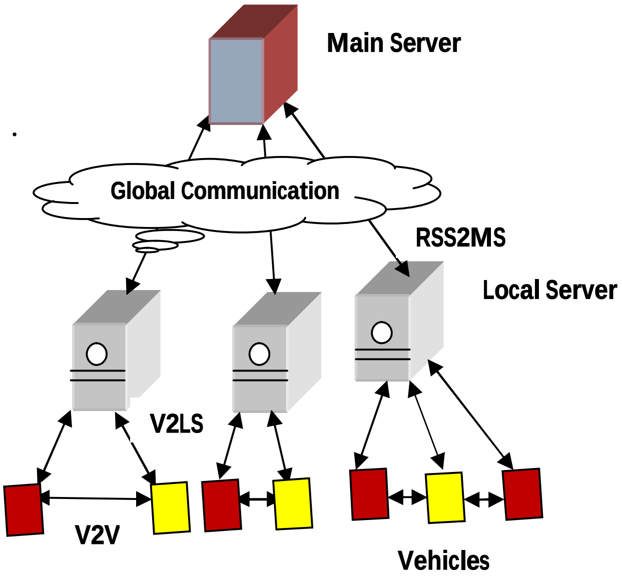

Fig.2 Model of Communication

IV. VEHICLE AUTHENTICATION

Considerable efforts have been devoted to guaranteeing vehicle privacy and quite a number of solutions have been proposed. Among them, for example, pseudonym-based approaches are well-understood. Indeed, the pseudonym of a node is a short-lived public key authenticated by a certificate authority. With these pseudonyms, vehicles can anonymously authenticate their own vehicular reports. This approach is conceptually simple and it is supported by the DSRC standard [13]. However, a major shortcoming of pseudonyms is that each vehicle needs to pre-load a huge pool of anonymous certificates to achieve privacy, and a trusted authority also needs to maintain and manage all the anonymous certificates, which implies a heavy burden of pseudonym management. Note that the number of pseudonyms per vehicle cannot be small, because that would cause each pseudonym to be re-used too often and might lead to vehicle re-identification: indeed, all messages authenticated with the same pseudonym can be linked and, the more messages are linked, the easier is re-identification.

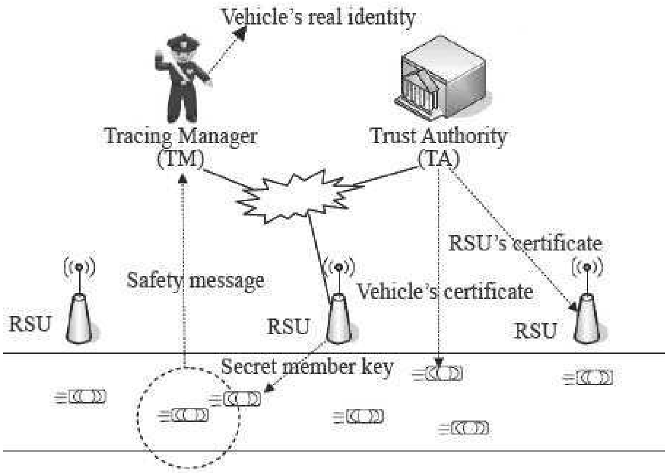

Fig.3 Tracing dishonest vehicles in VANETs

To circumvent the intricate pseudonym management, some proposals suggest using group signatures to anonymously authenticate traffic reports. In this approach [13], each vehicle registers to the transportation administration office and obtains a secret token. With this token, the vehicle can authenticate any message and the authenticated message can be verified by any vehicle getting it. However, the verifying vehicles cannot identify the author of the verified message. Unlike the pseudonym approach, a secret token can be used to anonymously authenticate exponentially many messages until it expires or is revoked, which eliminates the requirement to manage a huge number of pseudonyms. Nevertheless, the group signature approach needs to manage a number of revoked or expired tokens that grows linearly with the time since the system was deployed, and before verifying a traffic report, a verifying vehicle needs to retrieve and verify that the report is not associated with any expired/revoked tokens. This implies that the system performance degrades as the time passes.

Privacy in vehicular communications can only be preserved for honest vehicles. An anonymity revocation mechanism is required "for the prevention, investigation, detection, and prosecution of serious criminal offences" [14]. Both the above pseudonym approach and the group signature approach allow some trusted party to reveal the genuine identities of misbehaving vehicles. By extending the existing law enforcement mechanisms to cover malicious behavior in VANETs that compromises the drivers' safety, this kind of anonymity revocation mechanisms can be viewed as *a* *posteriori* countermeasures that deter abuse of anonymity in VANETs.

With *a posteriori* countermeasures, punitive action is taken against vehicles proven to have originated fraudulent messages however such countermeasures are ineffective against irrational attackers such as terrorists. Even for rational attackers, damage has already occurred when punitive action is taken. To overcome this concern, an option is to employ *a priori* countermeasures [15], which attempt to prevent the generation of fraudulent messages. A report is trusted only if it was endorsed by a number of vehicles in the vicinity greater than or equal to a predefined threshold. The underlying assumption is that most users are honest and will not endorse any message containing false data; the more vehicles endorse a report, the more trustworthy it is.

One may observe that neither *a posteriori* nor *a priori* countermeasures alone are sufficient to secure VANETs. For instance, with *a priori* countermeasures, although the underlying assumption that there is a majority of honest vehicles in VANETs generally holds, it cannot be excluded that a number of malicious vehicles greater than or equal to the threshold be present at specific locations. To address this concern, we presented a proposal [16] incorporating both *a priori* and *a posteriori* countermeasures. This approach can achieve better trustworthiness of traffic reports while preserving privacy for honest vehicles. Time-consuming operations are usually required to preserve privacy in VANETs. This raises the concern of the availability of the system because traffic safety can be improved only if the numerous received reports can be verified and reacted to in time.

V. Communication Pattern

Communications are possible in homogenous and heterogeneous vehicle network without being need to change in underline technology. For that we have specify three types of pattern in which vehicles sharing same geographic or different can communicate with each other smoothly. We can classified this patterns based on local and global communication [6].

There are two types of patterns depend on localization: -

1. Vehicle to Vehicle (V2V)

A. Motivation: - When an emergency is occurred, each vehicle transmit emergency message using V2V pattern to warn other vehicle in the roadway.

B. Way of communication: - This pattern involves communication between vehicles to vehicles.

2. Vehicle to Local Server (Road Side Server):

A. Motivation: - This is only type of communication pattern that involve sending of periodic, information and emergency message. When an unusual situation happen in roadway, this pattern is used by vehicle to send emergency message to other vehicles and local server. Local server will send information message to inform this scenario to other vehicles on road. On other hand, local server will periodically inform each vehicle about nearest hospital, petrol pump, police station and other necessary information by using periodic message.

B. Way of communication: - This pattern involves communication between vehicles to local server and local server to vehicles.

There are only one type of pattern belong to global communication.

1. Local Server to Main Server

A. Motivation: - This communication pattern used in different cases.
Case 1: When vehicle was register on their local network. Local network circulate this information to global server via several local server.
Case 2: When there is any unusual any situation occurred in road way, it is responsibility of local server to give this information to global server. These types of information need in post investigation of accident.
Case 3: To maintain log records of every vehicle, this communication pattern play very important role.

B. Way of communication: - This pattern involves bidirectional communication between road side server and main server.

VI. Algorithm and Applications

In this paper we have proposed an algorithm to find out the exact location of moving vehicle using **Global Positioning System** [8] in local domain.

MOVING_OBJECT_DETECTOR (loc)

1. Each vehicle must equip with various types of sensors and internal camera and GPRS enable MOBILE phone.
2. Every vehicle should register in global server via their local server with their unique city code and vehicle number.
3. When main server want to communicate some message to particular vehicle, it send **query** message to local server based on the location of vehicle [9].
4. Local server then send query message to particular vehicle service provider.
5. This query message contains three fields:
   1. Vehicle registration id:- filled by main server
   2. Position or location of vehicle contains two subfield
      Longitude and altitude filled by service provider.
6. Then **reply** message is sent by local to global server.
7. Reply message contains following fields:-
   - Vehicle registration id: - Same as in query message because it is used by main server in origin authentication phase.

- Position or location of vehicle contains two subfield Longitude and altitude filled by service provider.

In same way vehicle can also find location of each other.

APPLICATIONS

VANET in this context provide following applications:-

A. ***Collision Avoidance:*** Data transmitted from a roadside base station to a vehicle could warn a driver that it's not safe to enter an intersection. In this way, more drivers far behind will get an alarm signal before they see the incident.

B. ***Cooperative Driving:*** Like violation warning, curve warning, lane merging warning etc. These services may greatly reduce the life endangering accidents. In fact, many of the accidents come from the lack of cooperation between drivers. Given more information about the possible conflicts, we can prevent many accidents.

C. ***Payment Services:*** Like toll collection, which is very convenient and desirable to pass a toll collection without having to decelerate your car, waiting in line and searching money?

D. ***Location-based Services:*** Like finding the closest fuel station, restaurant, lodge etc. Some of these applications are life-critical, such as collision avoidance and cooperative driving. Other applications are less safety-related or less specific to the vehicular networks.

E. ***Traffic Optimization:*** Vehicles could serve as data collectors and transmit the traffic condition information for the vehicular network. And transportation agencies could utilize this information to actively relieve traffic congestion. In this way, the vehicles approaching the congestion location will have enough time to choose alternate routes.

VII. Conclusion

The authentication scheme for VANET communication result in smooth wireless sensor network or mobile ad-hoc networks data exchange. It solved the problems of homogenous and heterogeneity network communication in intra and inter domain autonomous vehicle network. In addition of distributed database storage scheme, response time of local server to vehicle gets reduced and hence the throughput of server operation increases. This makes local communication very efficient and reliable. On the other hand, due to centralized nature of main server, it gets complete control over the whole system. Since the main server divide its responsibility between many local servers based on area, region, state and country level, operation of main server significantly prevents itself from overload which in return increase the response time. Use of several protocols and communication patterns make VANET communication more secure and safe.

References

[1] R. Lakshmi Devi, C. Maheswari and Lynette Maria “A Cluster Based Authentic Vehicular Environment for Simple Highway Communication “IPCSIT vol. 37 (2012) IACSIT Press, Singapore

[2] Neng-Wen Wang a, Yueh-Min Huang a, and R. S. Shaji, “An efficient vehicular communication outside the city environments” International Journal of Next-Generation Networks (IJNGN) Vol.2, No.4, December 2010

[3] Wei-Ming Chen “A novel secure communication scheme in vehicular ad hoc networks”, Computer Communications 31 (2008) 2827–2837

[4] Ho-Yeon Kim, Dong-Min Kang, Jun-Ho Lee, Tai-Myoung Chung Myoung Chung “A Performance Evaluation of Cellular Network Suitability for VANET “World Academy of science, Engineering and Technology 64 2012

[5] Mohamed Kafsi, Panos Papadimitratos , Olivier Dousse , Lausanne, “VANET Connectivity Analysis” Switzerland Nokia Research Center, Lausanne, Switzerland T-Labs, Berlin, Germany

[6]Ghassan M. T.,“Current Trends in Vehicular Ad Hoc Networks”AbdallaUniversity of Plymouth School of Computing, Communications & Electronics, UK France Télécom Recherche et Développement CORE, France

[7] Neha Verma, Rakesh Kumar, “Efficient Data Delivery For Secured Communication in Vanet” IOSR Journal of Computer Engineering

[8] P. Salvo, F. Cuomo, A. Baiocchi “Infotainment applications support in VANET” DIET Department - University of Roma, Via Eudossiana 18, 00184 Roma, Italy

[9]Sriram Chellappan and Vamsi Paruchuri,“Integrating Smart Cards with Vehicular Networks: Architecture and Applications”

[10] Emad Eddin A. Gamati, Evitm Peytchev, Richard Germon, Li, Yueyue “Utilization of Broadcast Methods for detection of the road conditions in VANET” Nottingham Trent University - School of Science and Technology - Computing and Informatics Building, Clifton Lane, Nottingham, NG11 8NS, UK.

[11] Andreas Festag, Alban Hessler, Roberto Baldessari,Long Le, Wenhui Zhang, “Vehicle-to-Vehicle and road-side sensor communication for enhanced road safety”

[12] Mario Gerla, Leonard Kleinrock, “Vehicular networks and the future of the mobile internet” Computer Science Dept. UCLA, 405 Hilgard Ave, Los angeles California 90024, USA

[13] C. Boyd and A. Mathuria, Protocols for Authentication and Key Establishment, Springer, 2003.

[14] S. Duri, M. Gruteser, X. Liu, P. Moskowitz, R. Perez, M. Singh and J.-M. Tang, Framework for security and privacy in automotive telematics, in: Proceedings of the 2nd International Workshop on Mobile Commerce, 2002, pp. 25–32.

[15] S. Eichler, J. Billion, R. Maier, H.-J. Voegel and R. Kroh, On providing security for an open telematics platform, in: Proceedings of the 5th International Conference on ITS Telecommunications, 2005.

[16] P. Enge, Retooling the Global Positioning System, Scientific American (May) (2004)

[17] W. Enkelmann, FleetNet – applications for inter-vehicle communication, in: Proceedings of the IEEE Intelligent Vehicles Symposium’03, 2003, pp. 162–167.