ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Review On Improve the Content Delivery and Message Communication Using VANET

K.S.Saravanan[1,] N.Boomathi[2], M.Karthika[3]

Assistant Professor, Department of Computer Science and Applications, Vivekanandha College of Arts and Sciences for Women, Elayampalayam, Tiruchengode, Namakkal, India[1]

Full Time M.Phil Scholar, Department of Computer Science, Vivekanandha College of Arts and Sciences for Women, Elayampalayam, Tiruchengode, Namakkal, India[2,3]

ABSTRACT: Vehicles in a highway are connected to form a vehicular adhoc networks. Vehicular Adhoc Network (VANET) is constructed with vehicles and road side infrastructures. Vehicle location and speed information are continuously collected to manage the VANET communication. A VANET turns every participating vehicle into a wireless router or node. 100 to 300 meter distance is allowed between vehicles to cover a wide network range. Single-hop and multi-hop methods are used for VANET communication. Road Side Unit (RSU) is an infrastructure for communication between the cars for sharing and information from various vehicles. Vehicle to Vehicle (V2V) communication and Vehicle to Infrastructure (V2I)communication methods are used for VANET data transmission. Data replication scheme is used to reduce the data delivery delay. Expedite Message Authentication Protocol (EMAP) is used for VANETs with an efficient revocation checking process.

KEYWORDS: VANET, Message Authentication, Secured Message Communication

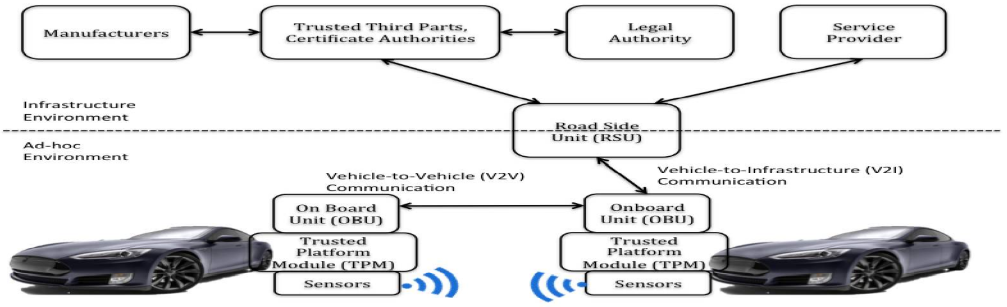
I. INTRODUCTION

A vehicular ad hoc network (VANET) uses cars as mobile nodes in a MANET to create a mobile network. . As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes. Automotive companies like General Motors, Toyota, Nissan, DaimlerChrysler, B MW and Ford promote this term. Most of the concerns of interest to mobile ad hoc networks (MANETs) are of interest in VANETs, but the details differ. Rather than moving at random, vehicles tend to move in an organized fashion. GPS and navigation systems might benefit, as they could be integrated with traffic reports to provide the fastest route to work. vehicles communicate with each other via inter-vehicle communication (IVC) as well as with roadside base stations via roadside-to-vehicle communication (RVC). Within the Communications Society, there is a Technical Subcommittee on Vehicular Networks & Telematics Applications (VNTA). The charter of this committee is to actively promote technical activities in the field of vehicular networks, V2V, V2R and V2I communications, standards, communications-enabled road and vehicle safety, real-time traffic monitoring, intersection management technologies, future telematics applications. Effective measures such as media communication between vehicles can be enabled as well methods to track automotive vehicles. In VANET is not foreseen to replace current mobile communication standards. Automotive vehicular information can be viewed on electronic maps using the Internet or specialized software. InVANET can be used as part of automotive electronics, which has to identify an optimally minimal path for navigation with minimal traffic intensity. The system can also be used as a city guide to locate and identify landmarks in a new city. Vehicular communication is expected to contribute to safer and more efficient roads by providing timely information to drivers, and also to make travel more convenient. The integration of V2V and V2R communication is beneficial because V2R provides better service sparse networks and long distance communication, whereas V2V enables direct communication for small to medium distances/areas and at locations where roadside access points are not available.

DOI: 10.15680/IJIRCCE.2016. 0405023

II. VANET DATA ACCESS

The presence of high-end Internet connected navigation and infotainment systems is becoming a reality that will easily lead to a dramatic growth in bandwidth demand by in vehicle mobile users. Examples of applications of vehicular communication abound, and range from the updating of road maps to the retrieval of nearby points of interest, from the instant learning of traffic conditions to the download of touristic information and media-rich data files. This will induce vehicular users to resort to resource intensive applications, to the same extent as today's cellular customers.

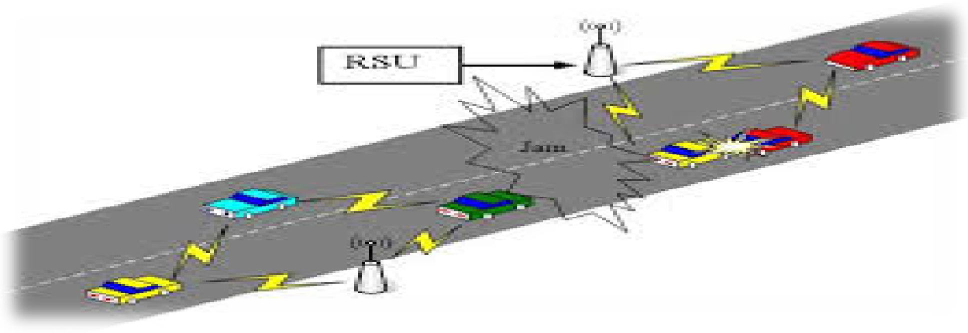

Manufacturers
Trusted Third Parts, Certificate Authorities
Legal Authority
Service Provider
Infrastructure Environment
Road Side Unit (RSU)
Ad-hoc Environment
Vehicle-to-Vehicle (V2V) Communication
Vehicle-to-Infrastructure (V2I) Communication
On Board Unit (OBU)
Onboard Unit (OBU)
Trusted Platform Module (TPM)
Trusted Platform Module (TPM)
Sensors
Sensors

Most observers concur that neither the current nor the upcoming cellular technologies will suffice in the face of such a surge in the utilization of resource demanding applications. Recent network overload episodes incurred in by cellular infrastructures in presence of smart phone users provide a sobering wake-up call. To wit, a recent analysis on the traffic of a large US-based operator showed that smart phone users represent just 1 percent of the total subscribers, yet drain 60 percent of the network resources. To design a network architecture that will scale to support the mass of vehicular users, one possibility is to off load part of the traffic to Dedicated Short Range Communication, through direct infrastructure-to-vehicle transfer, as well as vehicle-to-vehicle data relaying. Such an approach is especially attractive in the case of the download of large amounts of delaytolerant data, a task that is likely to choke 3G/4G operator networks, but that well fits DSRC based I2V and V2V communication paradigms due to its lack of strict time constraints. Within such a context, previous works on content downloading in vehicular networks have dealt with individual aspects of the process, such as the deployment of roadside Access Points (APs) [1], [3], the performance evaluation of I2V communication, or the exploitation of specific V2V transfer paradigms [5]. None of them, however, has tackled the problem as a whole, trying to quantify the actual potential of an I2V/V2V-based content downloading. In this paper, we identify the downloading performance limits achievable through DSRC-based I2V/ V2V communication. To this end, we assume ideal conditions from a system engineering viewpoint, i.e., the availability of preemptive knowledge of vehicular trajectories and perfect scheduling of data transmissions, and we cast the downloading process to a mixed integer linear programming (MILP) max-flow problem. The solution of such a problem yields the optimal AP deployment over a given road layout, and the optimal combination of any possible I2V and V2V data transfer paradigm. It, thus, represents the theoretical upper bound to the downloading throughput, under the aforementioned assumptions. While it is true that the resulting problem is NP complete, we show that, with a careful design of the model, it can be solved in presence of realistic vehicle mobility in a real-world road topology. In addition, we propose a sampling-based technique that efficiently yields a solution even for large-scale instances. Although the problem formulation and the performance figures we derive are interesting per-se, we also exploit our optimal solution to discuss the impact of key factors such as AP deployment, transfer paradigms, and technology penetration rate. As a final remark, we stress that our model, the first of its type to our knowledge, targets the general case of users interested in best-effort downloading of different data content. As a consequence, the goal is not to study information dissemination or cooperative caching, but to investigate the performance of content downloading.

III. VEHICLE AND INFRASTRUCTURE

3.1Management

Road network, vehicles and infrastructure properties are collected for the current status. The vehicle communication is carried out with the On Board Unit (OBU) environment. Data server and replica are provided in the Road Side Infrastructure (RSI). OBU and RSI are used for the data transmission process over the network.



3.2Pattern Analysis

Pattern extraction is performed using the historical vehicle movement details. Apriori algorithm is tuned for the vehicle pattern analysis process. Vehicle flow is analyzed with different time slots. Vehicle location and moving status details are also analyzed in the pattern extraction process .

3.3 Bandwidth Scheduling

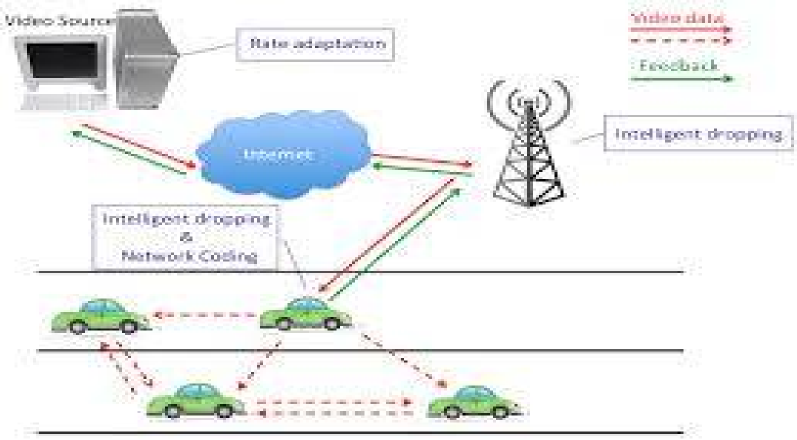
Bandwidth scheduling is used to allocate bandwidth for the vehicles. Density and request level based bandwidth scheduling algorithm is used for the bandwidth allocation process. Request frequency and load level are used in the bandwidth scheduling process. Vehicle traffic level is used for bandwidth assignment process.

3.4 Replica Management

Replica management handles the data distribution process for the replicas. Replica assignment algorithm is used to assign replica contents. Most frequently requested data values are updated to the replicas. Shared data are delivered from the data servers and replicas.

3.5 Content Delivery Process

User requests are processed under the content delivery process. Infrastructure estimation algorithm is used to improve the content delivery process. Dynamic Network Topology Graph (DNTG) is used for the content delivery process. Content delivery is carried out with the support of data servers, replicas and vehicles.



IV. MESSAGE AUTHENTICATION FOR VANETS

Vehicular ad hoc networks (VANETs) have attracted extensive attentions recently as a promising technology for revolutionizing the transportation systems and providing broadband communication services to vehicles. VANETs consist of entities including On-Board Units (OBUs) and infrastructure Road-Side Units (RSUs). Vehicle-to-Vehicle (V2V) and Vehicle-to- Infrastructure (V2I) communications are the two basic communication modes, which, respectively, allow OBUs to communicate with each other and with the infrastructure RSUs. Since vehicles communicate through wireless channels, a variety of attacks such as injecting false information, modifying and replaying the disseminated messages can be easily launched [9]. A security attack on VANETs can have severe harmful or fatal consequences to legitimate users. Consequently, ensuring secure vehicular communications is a must before any VANET application can be put into practice. A well-recognized solution to secure VANETs is to deploy Public Key Infrastructure (PKI), and to use Certificate Revocation Lists (CRLs) for managing the revoked certificates. In PKI, each entity in the network holds an authentic certificate, and every message should be digitally signed before its transmission. A CRL, usually issued by a Trusted Authority (TA), is a list containing all the revoked certificates. In a PKI system, the authentication of any message is performed by first checking if the sender’s certificate is included in the current CRL, i.e., checking its revocation status, then, verifying the sender’s certificate, and finally verifying the sender’s signature on the received message. The first part of the authentication, which checks the revocation status of the sender in a CRL, may incur long delay depending on the CRL size and the employed mechanism for searching the CRL. Unfortunately, the CRL size in VANETs is expected to be large for the following reasons: 1) To preserve the privacy of the drivers, i.e., to abstain the leakage of the real identities and location information of the drivers from any external eavesdropper [3], each OBU should be preloaded with a set of anonymous digital certificates, where the OBU has to periodically change its anonymous certificate to mislead attackers [4], [5], [6]. Consequently, a revocation of an OBU results in revoking all the certificates carried by that OBU leading to a large increase in the CRL size. 2) The scale of VANET is very large. According to the United States Bureau of Transit Statistics, there are approximately 251 million OBUs in the Unites States in 2006 [7]. Since the number of the OBUs is huge and each OBU has a set of certificates, the CRL size will increase dramatically if only a small portion of the OBUs is revoked. To have an idea of how large the CRL size can be, consider the case where only 100 OBUs are revoked, and each OBU has 25,000 certificates [8]. In this case, the CRL contains 2.5 million revoked certificates. According to the employed mechanism for searching a CRL, the Wireless Access in Vehicular Environments (WAVE) standard does not state that either a non optimized search algorithm, e.g., linear search, or some sort of optimized search algorithm such as binary search, will be used for searching a CRL. In this paper, we consider both non optimized and optimized search algorithms. According to the Dedicated Short Range Communication (DSRC) [10], which is part of the WAVE standard, each OBU has to broadcast a message every 300 msec about its location, velocity, and other telematic information. In such scenario, each OBU may receive a large number of messages every 300 msec, and it has to check the current CRL for all the received certificates, which may incur long authentication delay depending on the CRL size and the number of received certificates. The ability to check a CRL for a large number of certificates in a timely manner leads an inevitable challenge to VANETs. To ensure reliable operation of VANETs and increase the amount of authentic information gained from the received messages, each OBU should be able to check the revocation status of all the received certificates in a timely manner. Most of the existing works overlooked the authentication delay resulting from checking the CRL for each received certificate. In this paper, we introduce an expedite message authentication protocol1 (EMAP) which replaces the CRL checking process by an efficient revocation checking process using a fast and secure HMAC function. EMAP is suitable not only for VANETs but also for any network employing a PKI system. To the best of our knowledge, this is the first solution to reduce the authentication delay resulting from checking the CRL in VANETs.

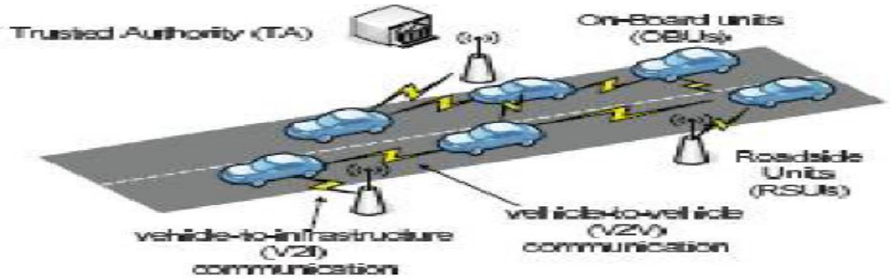
V. ISSUES ON MESSAGE AUTHENTICATION IN VANETS

Vehicular ad hoc networks (VANETs) adopt the Public Key Infrastructure (PKI) and Certificate Revocation Lists (CRLs) for their security. Certification verification is performed with the current CRL and signature values. Expedite Message Authentication Protocol (EMAP) is used for VANETs with an efficient revocation checking process. The revocation check process in EMAP uses a keyed Hash Message Authentication Code (HMAC). The key used in calculating the HMAC is shared only between nonrevoked On-Board Units (OBUs). EMAP uses a novel probabilistic key distribution to enables nonrevoked OBUs to securely share and update a secret key. The following problems are identified in the current VANET security schemes.

- Signature authentication is not provided
- Certificate integrity is not verified
- Key distribution load high

5.1 Expedite Message Authentication Protocol

The proposed EMAP uses a fast HMAC function and novel key sharing scheme employing probabilistic random key distribution. the system model under consideration consists of the following:


Trusted Authority (TA)
On-Board units (OBUs)
Roadside Units (RSUs)
vehicle-to-vehicle (V2V) communication
vehicle-to-infrastructure (V2I) communication

1. A Trusted Authority, which is responsible for providing anonymous certificates and distributing secret keys to all OBUs in the network.
2. Roadside units (RSUs), which are fixed units distributed all over the network. The RSUs can communicate securely with the TA.
3. OBUs, which are embedded in vehicles. OBUs can communicate either with other OBUs through V2V communications or with RSUs through V2I communications.

According to WAVE standard each OBU is equipped with a Hardware materials, e.g., secret keys, certificates, etc., of the OBU. Also, the HSM in each OBU is responsible for performing all the cryptographic operations such as signing messages, verifying certificates, keys updating, etc. We consider that legitimate OBUs cannot collude with the revoked OBUs Security Module (HSM), which a tamper resistant module is used to store the security as it is difficult for legitimate OBUs to extract their security materials from their HSMs. Finally, we consider that a compromised OBU is instantly detected by the TA.

VI. SYSTEM INITIALIZATION

The TA initializes the system it should be noted that: denotes the ith public key for OBUu, where the corresponding secret key is ; denotes the ith pseudoidentity (PID) for OBUu, where the TA is the only entity that can relate to the real identity of OBUu; sigTA(||) denotes the TA signature on the concatenation (k) of and C is the number of certificates loaded in each OBU. Note that the system model under consideration is mainly a PKI system, where each OBUu has a set of anonymous certificates (CERTu) used to secure its communications with other entities in the network. In specific, the public key PKu, included in the certificate certu, and the secret key SKu are used for verifying and signing messages, respectively. Also, each OBUu is preloaded with a set of asymmetric keys (secret keys Ks in RSu and the corresponding public keys K+ s in RPu). Those keys are necessary for generating and maintaining a shared secret key Kg between unrevoked OBUs.

VII. REVOCATION

The revocation is triggered by the TA when there is an OBUu to be revoked. The certificates of OBUu must be revoked. In addition, the secret key set RSu of OBUu and the current secret key Kg are considered revoked. Hence, a new secret key g should be securely distributed to all the nonrevoked OBUs. Also, each nonrevoked OBU should securely update the compromised keys in its key sets RS and RP.

VIII. SECURED CERTIFICATE MANAGEMENT AND MESSAGE COMMUNICATION

The EMAP scheme is enhanced to provide certificate and message signature verification process. Attacks on certificates and messages are detected and controlled by the system. Signature authentication is added with the system. Time boundary based message authentication is used. The VANET communication scheme is secured with enhanced message authentication mechanism. Certificate and message signature verification is performed to control attacks. Data security is also provided with cryptography and digital signatures. The system is divided into five major modules. They are road side unit (RSU), trusted authority, on board unit (OBU), certificate authentication and message communication. The RSU module is designed to perform user authentication module. The trusted authority module is designed to manage certificate authentication process. Client security operations are managed with Since we adopt a generic PKI system, the details of the TA signature on a hardware security module in OBU. Certificate verification and revocation operations are managed under certificate authentication module. The message communication module is designed to manage data transfer between vehicles and RSUs.

IX. CONCLUSION

Vehicular Adhoc Networks (VANET) manages the users with key certificate. Trusted authority is used to handle the certificate issue and verification process. Client and message certificate signature verification scheme is integrated with the system. Data security is provided with dynamic user joint and leaves conditions. Message loss ratio is minimized in the system. Low message verification delay is achieved by the system. The system reduces the key distribution overhead. Vehicular Ad hoc networks (VANET) constructed to manage communication under road networks. Content delivery is managed with vehicles and road side infrastructure. Bandwidth scheduling is performed with vehicle load prediction model. The data replica is used to improve the data delivery rate. The system reduces the infrastructure requirement. Data delivery delay is minimized by the replicas. Pattern based density prediction process is used for the infrastructure estimation process. Reliable data delivery process is supported by the content delivery scheme.

REFERENCES

[1] K.P. Laberteaux, J.J. Haas, and Y. Hu, “Security Certificate Revocation List Distribution for VANET,” Proc. Fifth ACM int’l Workshop VehiculAr Inter-NETworking, 2008.

[2] A. Wasef and X. Shen, “PPGCV: Privacy Preserving Group Communications Protocol for Vehicular Ad Hoc Networks,” Proc. IEEE Int’l Conf. Comm. (ICC ’08), pp. 1458-1463, 2008.

[3] A. Wasef, Y. Jiang, and X. Shen, “DCS: An Efficient Distributed Certificate Service [7] M. Raya and J.-P. Hubaux, “Securing Vehicular Ad Hoc Networks,” J. Computer Security, vol. 15, no. 1, pp. 39-68, 2007.

[4] S. Yoon, D.T. Ha and C. Qiao, “MoPADS: AMobility Profile Aided File Downloading Service inNVehicular Networks,” IEEE Trans. Vehicular Technology, Nov. 2009.

[5] M. Gerla and M. Gruteser, “Vehicular Networks: Applications, Protocols, and Testbeds,” Emerging Wireless Technologies and the Future Mobile Internet, D. Raychaudhuri, M. Gerla, eds., Cambridge Univ., May 2011.

[6] A. Abdrabou and W. Zhuang, “Probabilistic Delay Control and Road Side Unit Placement for Vehicular Ad Hoc Networks with Disrupted Connectivity,” IEEE J. Selected Areas in Comm., vol. 29, no. 1, pp. 129-139, Jan. 2011.

[7] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, “An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications,” IEEE Trans. Vehicular Technology, Sept. 2010

[8] V. Kone, H. Zheng and B.Y. Zhao, “On Infostation Density of Vehicular Networks,” Proc. Fifth Int’l Wireless Internet Conf, 2010.

[9] F. Malandrino and M. Fiore, “Content Downloading in Vehicular Networks: What Really Matters,” Proc. IEEE INFOCOM Mini-Conf., Apr.2011.

[10] Francesco Malandrino and Marco Fiore, “Optimal Content Downloading in Vehicular Networks”, IEEE Transactions On Mobile Computing, Vol. 12, No. 7, July 2013.