ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 10, March 2016

GSPN: GROUP – BASED SECURE AND PRIVACY-PRESERVING NAVIGATION

(M.SUBHAHANAL NUZRATH(AP/ECE), N.BHUVANESHWARI(711212106010), S.JAYALAKSHMI(711212106030), B.KALPANA(711212106035)

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING, JAY SHRIRAM GROUP OF INSTITUTIONS, AVINASHIPALAYAM, TIRUPUR.

ABSTRACT

In this paper, we propose a navigation scheme that utilizes the online road information collected by a vehicular ad hoc network (VANET) to guide the drivers to desired destinations in a real-time and distributed manner. In this paper, we propose a trust based framework for a safe and reliable information dissemination in vehicular networks. Group Based Receiver Driven Protocol divides the network to clusters or groups, where nodes are grouped using the same search query like same direction or same destination route, or so on. Each cluster has a cluster head (Group Leader), its task is to manage communication processes inside, and to outside its cluster. The proposed scheme has the advantage of using real-time road conditions to compute a better route and at the same time, the information source can be properly authenticated. To protect the privacy of the drivers, the query (destination) and the driver who issues the query are guaranteed to be unlinkable to any party including the trusted authority. We make use of the idea of anonymous credential to achieve this goal.

INTRODUCTION

VEHICULAR AD HOC NETWORK

A vehicular ad hoc network (VANET) uses cars as mobile nodes in a MANET to create a mobile network. A VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 meters of each other to connect and, in turn, create a network with a wide range. 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, BMW and Ford promote this term.

STANDARDS

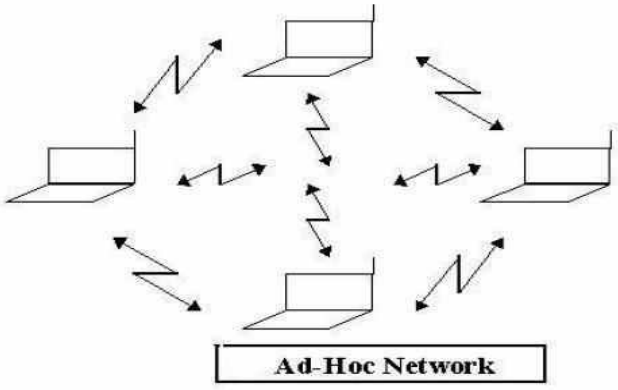


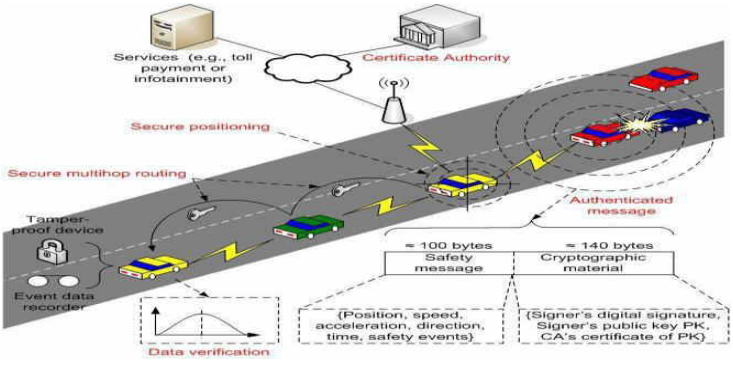
Figure1.2 VANET Application A

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 10, March 2016

Intelligent vehicular ad-hoc network (InVANET) is another term for promoting vehicular networking. InVANET integrates multiple networking technologies such as Wi-Fi IEEE 802.11p, WAVE IEEE 1609, WiMAX IEEE 802.16, Bluetooth, IRA and ZigBee. Vehicular ad hoc networks are expected to implement wireless technologies such as dedicated short-range communications (DSRC) which is a type of Wi-Fi. Other candidate wireless technologies are cellular, satellite, and WiMAX. Vehicular ad hoc networks can be viewed as component of the intelligent transportation systems (ITS).

Vehicle-to-Vehicle (V2V) communication supports services Here, an integrationof VANET and 3G networks using mobile gateways (i.e., vehicles) is introduced. In particular, the integration of IEEE 802.11-based multi-hop VANETs with 3G shall contribute to the evolution of Beyond 3G (B3G) wireless communication systems..

VANET is a special class of MANET to provide communication among nearby vehiclesand between vehicles and nearby roadside equipment's. It is based upon short range wirelesscommunication between vehicles. In these networks, each vehicle is equipped with communication equipment's,computing devices and GPS (Global Positioning Systems)receivers. GPS receiver provides all the information of a vehicle like speed, direction of movement of vehicle, time, location etc.



CHARACTERISTICS OF VANET

- High mobility nodes
- Predictable topology (using digital map)
- Critical latency requirements
- Slow migration rate
- No problem with power
- Security and privacy

WORKING OF VEHICULAR NETWORKS

Vehicular Networks System consists of large number of nodes (for vehicles).Here, each vehicle can communicate with other vehicle using short radio signals DSRC (5.9 GHz), within 1 KM range area. The communication between each vehicle is an Ad Hoc communication that means each connected node can move freely, there is no any wires required, the routers used is called Road Side Unit (RSU), the RSU works as a router between the vehicles on the road and connected to other network devices. Typically, in a VANET each vehicle is assumed to have an onboard unit (OBU) and there are road-side units (RSU) that are installed along the roads. .

Related work

ATTACKS

VANET facing many attacks, some of these attacks are as follows.

Denial of Service Attack (DoS)

Denial of Service attack happens when the hacker or attacker takes control of a all thevehicle's resources or maybe he jams the communication channel that are using by the VehicularNetwork, thus it prevents critical information from arriving.

Message Suppression

In this type of attack, an attacker selectively dropping packets from the network, these packets may hold critical information for the receiver. The attacker suppresses these

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 10, March 2016

packets and he can use that packet again in other time

Alteration Attack

In this type of attack, an attacker simply alters an existing data. It includes delaying the transmission of the information, replaying earlier transmission, or altering the actual entry of the data transmitted

Sybil Attack

Sybil attack is the creation of multiple fake nodes broadcasting false information. In Sybil attack, a vehicle with On Board Unit (OBU) sends multiple copies of messages to other vehicle and each message contains a different fabricated identity.

SECURITY REQUIREMENT FOR VANET

Security is an important issue for ad hoc networks, especially for security sensitive applications. To secure an ad hoc network, need to consider the following attributes as criteria to measure security.

Availability

Availability is a very important factor for VANET. It guarantees that the network is functional, and useful information is available at any functioning time. The availability deals with network services for all nodes comprises of bandwidth and connectivity. Group signature scheme has been introduced in order to encounter the availability issues.

Confidentiality

Confidentiality is an important security requirement for VANETs communications; it ensures that data are only read by authorized parties. It also prevents unauthorized access to confidential information such as name of the driver, plate number and location of the vehicle.

Authentication

Authentication is a major requirement in VANET as it ensures that the messages are sent by the actual nodes and hence attacks done by the attacker can be reduced easily with greater extent. In VANET, authentication is the verification of the identity between vehicles and RSU and the validation of integrity of the information exchange.

Integrity

Data integrity is the assurance that the data received by nodes, RSU and AS is the same as what has been originally generated during the exchanges of the message. In order to protect the integrity of the message, digital signature which is integrated with password access are used.

Non-Repudiation

Non-repudiation in computer security means the ability to verify that the sender and the receiver are the entities who claim to have respectively sent or received the message .

Message integrity and authentication

A vehicle should be authenticated before it can issue a navigation query. On the other hand, an RSU (vehicle) is able to verify that a message is indeed sent and signed by a certain vehicle (RSU) without being modified by anyone.

Identity privacy preserving

The real identity of a vehicle should be kept anonymous from other vehicles as well as from RSUs and a third-party should not be able to reveal a vehicle's real identity by analyzing multiple messages sent by it.

Traceability

Although a vehicle's real identity should be hidden from other vehicles and RSUs, TA should have the ability to obtain a vehicle's real identity so That the vehicle can be charged for using the navigation service. Also TA has the role to maintain liability via non repudiation property of messages when accidents happen on the road.

PROTOCOLS TO ENSURE SECURITY AND PRIVACY

VPKI (Vehicular Public Key Infrastructure)

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 10, March 2016

This scheme required extra communication and it has large storage overhead. To achieve the privacy requirement of vehicle, the authors proposed to use frequently updated anonymous public keys. But, the problem with this solution is that it required large number of key pairs to be stored, hence making the secure distribution of keys, key management, and storage becomes complex; so practically it is not efficient.

Secure Traffic Aggregation

When vehicles are located in a cell, the vehicle that is physically closest to the center of the cell is automatically taken as the group leader of the vehicles in the cell, which is delegated to aggregate messages for the whole group when the message is going to be relayed to the leader of the neighbor groups. The aggregation of messages can achieve a significant reduction in the overhead for vehicle to vehicle communications..

Anonymous-key-based (HAB) security protocol

With the HAB solution, a huge set of anonymous keys are preloaded in each vehicle, and each vehicle randomly takes one of the keys in the set to sign a safety message. The HAB scheme provides an efficient and straightforward way in solving the privacy issues, while the central authority simply keeps all the anonymous certificates of all the vehicles in a certain area in order to maintain the traceability.

RAISE: RSU-aided Message Authentication

In Vehicular Ad-hoc, when the traffic density becomes larger, a vehicle cannot verify all signatures of the messages sent by its neighbors in a timely manner, which results in message loss. Communication overhead as another issue that need to be handle. To deal with these issues, authors have introduced a novel RSU-aided messages authentication scheme called RAISE. With RAISE, roadside units (RSUs) are responsible for verifying the authenticity of the messages sent from vehicles and for notifying the results back to vehicles

IBV: Identity-based Batch Verification Scheme

Identity-based Batch Verification Scheme can achieve conditional privacy preservation that is essential in VSNs, in which each message launched by a vehicle is mapped to a distinct pseudo identity, while a trust authority can always retrieve the real identity of a vehicle from any pseudo identity.

RESEARCH METHODOLOGY

PROBLEM DEFINITION

The communication networks, security issues have been widely addressed in VANETs. Any navigation scheme must also satisfy these security requirements. First, whether or not the service is free, subscription to the service is usually required. A user (note that because the user is usually the driver and it is associated with the vehicle, use these terms interchangeably throughout the paper) must be authenticated to ensure he is a valid subscriber. Messages sent in the system must be authenticated and signed to make sure that they were not modified by anyone. On the other hand, because a vehicle's OBU will continuously communicate with RSUs, the driving habit of a driver as well as the traveling routes can be easily analyzed. So, privacy protection is another basic requirement in VANETs. One common approach to resolve this possible privacy leakage is to use a different authenticable, but unrelated pseudo identity to communicate with a different RSU.

OVERVIEW OF THE PROJECT

EXISTING SYSTEM

We survey the state-of-the-art in trust models/systems and routing protocols in V Nets. Then, as our next contribution, we propose a novel two-layer framework for application-oriented context-aware trust-based communication (FACT) in V Nets, where nodes only use their most trusted neighbours to forward the message otherwise they carry the message by themselves. FACT consists of two modules: Admission and Dissemination. The key distinction of the FACT lies in its space-centric nature. It is a combination of entity-

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 10, March 2016

/data-centric methods in addition to its focus on location. Once a message is received, FACT first applies three safety checks in the admission module to make sure the message: 1) originated from a trusted region and traversed a trusted path; 2) was not under attack on its path; and 3) has a valid content. Then, FACT admits the message and pushes it to the dissemination module to be forwarded through a trusted path. Each vehicle has a trust table where each road segment in the city has its own trust value and this value is constantly updated by the vehicle based on its experience in that segment.

PROPOSED SYSTEM

We propose a new application— Group Based Receiver Driven Protocol (GACVO), divides the network to clusters or groups, where nodes are grouped using the same search query like same direction or same destination route, or so on. Each cluster has a cluster head (Group Leader), its task is to manage communication processes inside, and to outside its cluster. Nodes inside the cluster communicate by direct paths, but their communication with other nodes outside the cluster is achieved by their cluster header, and this creates a virtual infrastructure for networks. In addition of driving guidance, the navigation results can also be used for other purposes. One common approach to resolve possible privacy leakage is to use a different authenticable, but unrelated pseudo identity to communicate with a different RSU. Thus, collecting all messages between a vehicle and all RSUs cannot link the messages together to reconstruct the driving routes or analyze the driving habit of a driver.

MODULE DESCRIPTION

LIST OF MODULES

- VANET Setup
- Navigation Request and Reply
- PropagationVerification of Hop Information
- Guiding to Destination

DESCRIPTION

VANET Setup

Vehicular ad hoc network (VANET) is an important element of the Intelligent Transportation Systems (ITSs). In a typical VANET, each vehicle is assumed to have an onboard unit (OBU) and there are road-side units (RSU) installed along the roads. Each Node formed for VANET setup is considered as vehicle. And nodes are kept in different locations to show that the vehicles are in different locations and they need minimum traveling delay in a distributed manner using the online information of the road condition and the security system.

Navigation Request and Reply

Propagation

Vehicle's navigation query is propagated across the network of RSUs and how the result is sent back to Vehicle. RSU Rk takes up the role of initiating the route searching process by composing the route request message and broadcasts it to all neighbors that are closer to DEST than itself. Each RSU hops along the reverse path Rim repeats the steps done by Rd and includes information corresponding to its hop into the route reply message. Rim also stores the next hop of the forward path (i.e., the identity of the RSU from which it receives the route reply message) into its routing table for guiding Vi later on. Now, let us go back to Rk, the RSU that initiates the route searching process. Upon receiving a navigation reply, Rk will not forward it to vehicle Vi immediately. Instead, it waits for a threshold amount of time for more replies.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 10, March 2016

Verification of Hop Information

Recall that the reply contains a set of identities, a set of locations, a set of certificates, and a set of hop information (average speed and road condition together with signatures), each corresponding to an RSU along the route returned. To verify the average speed and road condition provided by an RSU, its signature is verified using its identity.

As such, this part can be relaxed to be carried out by a conventional car computer device to speed up the process.

Guiding to Destination

Having the returned route, if Vehicle has GPS device installed and it can receive GPS signals for current location, it can simply search for each RSU based on the list of R Li. GPS device is not an assumption of our scheme. Even if Vehicle does not have GPS device installed, our scheme can make use of the VANET to guide Vehicle to the destination. To use the guiding service, Vi first generates a random number rand and sends to Rk. Here, nsn is the navigation session number generated earlier and Rk is the first RSU along the route. Upon receiving the message from Vi. It decrypts the message using its private key to obtain rand and nsn. It then searches its navigation routing table to dig out the session with session number nsn and sends Vi information (e.g., direction) about how to get to the next RSU hop along the forward path (or the destination if it is already the last hop).

ARCHITECTURE DIAGRAM

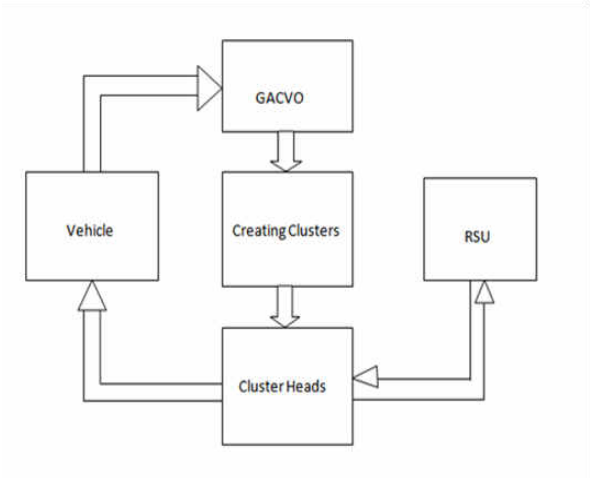


Table c Flag Types New Wireless Trace Format

N	Node Property
I	IP Level Packet Information
H	Next Hop Information
M	Mac Level Packet Information
P	Application Level Packet Information

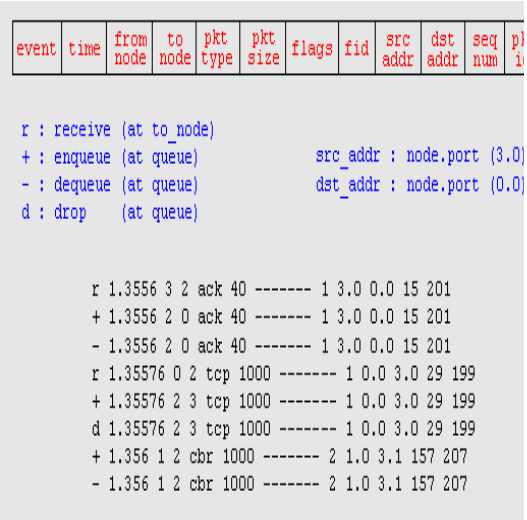
PROGRAMMING STRUCTURE

- Create the event scheduler
- Turn on tracing
- Create network topology
- Create transport connections
- Generate traffic

TURN ON TRACING

on Trace packets individual link Trace file format

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 10, March 2016



SYSTEM IMPLEMENTATION

System implementation is a stage in a stage in the project where the where the theoretical designs turned into working system. The most crucial stage the user confidence that the new system will work effectively and efficiently.The performance of reliability of the system was tested and it gained acceptance. The system was implemented successfully. Implementation is a process that means converting a new system into operation. Proper implementation is essential to provide a reliable system to meet organization requirements.

During the implementation stage a live demon was undertaken and made in front of end-users. Implementation is a stage of project when the system design is turned into a working system. The stage consists of the following steps.

- Testing the developed program with sample data.
- Detection and correction of internal error.
- Testing the system to meet the user requirement.
- Feeding the real time data and retesting.
- Making necessary change as described by the user

SIMULATION MODEL

Simulation done using 63 nodes, made node 0 as source and node 63 as destination, And implemented RSU in node 2, 25 and 37, At first vehicle 1(node 43) sends request to RSU1 then RSU1 forward V1 request to Trusted Authority. TA contains Vehicles Information like Mac ID and master key. TA verifies Mac id and master key of V1 and terminated that node without sending any information, because TA found that V1 issued Pseudo Identity. Then Vehicle 2(node 4) issues request for navigation service to RSU, RSU again forward V2 request to TA then TA verifies the credentials and provides the navigation service to V2.

EXPERIMENTAL RESULT AND DISCUSSION

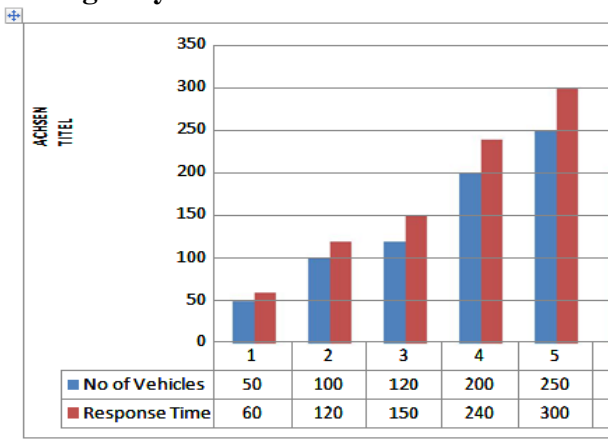
The proposed scheme adopts some security primitives in a nontrivial way to provide a number of security features: 1) Vehicles are authenticated by means of pseudo identities. 2) Navigation queries and results are protected from eavesdroppers. Besides, with the idea of anonymous credential, no one including TA can link up a vehicle's navigation query and its identity. 3) Information provided by RSUs can be properly authenticated before the route is actually being used. Besides satisfying all security and privacy requirements, our solution is efficient in the sense that a vehicle can complete the whole navigation querying process and receive urgent notification in a very short time. On the other hand, the route returned by our scheme can lead to savings of up to 55 percent of traveling time compared with the offline map data searching approach. Note that our VSPN scheme can apply to the situation where the route searching process is done by a central server, which collects and verifies speed data and road conditions from RSUs.

.

Below figure Shows the response time, depends on number **of RSU's implemented**

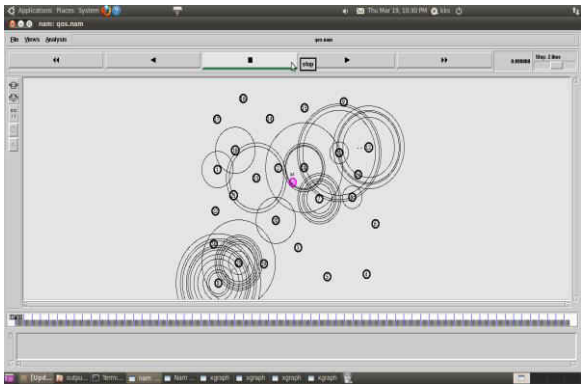
ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 10, March 2016

in a large city.



Result

In the proposed method vehicle can be properly authenticated. Privacy is preserved using the idea of pseudo identity. At the same time, the vehicle's real identity can be traced ifnecessary. Navigation queries and results are protected to preserve user's confidentiality and operator's profit. On the other hand, one's real identity and navigation query are completely delinked using the idea of anonymous credential. Information provided by RSUs can be properly authenticated in an efficient way. The nodes are created with the help of NS 2.34 version and the RSU are chosen from 3 nodes so that the requests from every vehicle are obtained.



SIMULATION OUTPUT

CONCLUSION

A vehicular ad hoc network (VANET) uses cars as Vehicular nodes in a MANET to create a Vehicular network. It is an important element of the Intelligent Transportation Systems (ITSs).In a typical VANET, each vehicle is assumed to have an onboard 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 back end. A VANET can also be interpreted as a sensor network because the traffic control center or some other central servers can collect lots of useful information about road conditions from vehicles. It is natural to investigate how to utilize the collected real-time road conditions to provide useful applications. A new application Group based receiver driven protocol which makes use of the collected data to provide navigation service to drivers.

REFERENCES

[1] F. Wang, D. Zeng, and L. Yang, "Smart Cars on Smart Roads: An IEEE IntelligentTransportation Systems Society Update," IEEE Pervasive Computing,vol. 5, no. 4, pp. 68-69, Oct.-Dec. 2006.

[2] H. Oh, C. Yae, D. Ahn, and H. Cho, "5.8 GHz DSRC PacketCommunication System for ITSServices,"Proc. IEEE VTS 50thVehicular Technology Conf. (VTC '99),pp. 2223-2227, Sept. 1999.

[3] I. Leontiadis, P. Costa, and C. Mascolo, "Extending Access PointConnectivity throughOpportunistic Routing in Vehicular Networks,"Proc. IEEE INFOCOM '10,Mar. 2010.

[4] C. Zhang, R. Lu, X. Lin, P.H. Ho, and X. Shen, "An EfficientIdentity-Based Batch Verification Scheme for Vehicular SensorNetworks,"Proc. IEEE INFOCOM '08,pp. 816-824, Apr. 2008.

[5] R. Lu, X. Lin, H. Zhu, and X. Shen, "SPARK: A New VANETBased Smart Parking Schemefor Large Parking Lots,"Proc. IEEEINFOCOM '09,pp. 14131421, Apr. 2009.

[6] D. Chaum, "Security without Identification: Transaction Systems to Make Big Brother Obsolete," Comm. ACM,vol. 28, pp. 1030-1044, 1985.

[7] E. Aimeur, H. Hage, and F.S.M. Onana, "Anonymous Credentialsfor Privacy-Preserving E-learning," Proc. IEEE MCETECH Conf.e-Technologies (MCETECH'08),pp. 70-80, July 2008.

[8] G. Samara, W. Al-Salihy, and R. Sures, "Security Issues and Challenges Vehicular Ad HocNetworks (VANET),"Proc. IEEEFourth Int'l Conf. New Trends in Information Science and ServiceScience (NISS '10),pp. May 2010.

[9] K.Sampigethaya,M.Li,L.Huang,andR.Poovendran,"AMOEBA:RobustLocation Privacy Scheme for VANET,"IEEEJ. Selected Areas in Comm.,vol. 25, no. 8, pp. 1569-1589, Oct. 2007.

[10] C. Zhang, X. Lin, R. Lu, and P.H. Ho, "RAISE: An Efficient RSUAided Message Authentication Scheme in Vehicular Communication Networks," Proc. IEEE Int'l Conf. Comm.(ICC '08),pp. 1451-1457, May 2008.