Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 1, January 2014, pg.591 – 598

RESEARCH ARTICLE

Appraisal and Analysis on QoS Aware Secured Web Services over VANET Applications

M. Rajeswari
Assistant Professor, Department of IT, SMVEC, Puducherry, India
mrajeswari.smvec@gmail.com

V. Mythili
UG student, Department of IT, SMVEC, Puducherry, India
mythismvec@gmail.com

S. Sridevi
UG student, Department of IT, SMVEC, Puducherry, India
sri93raj@gmail.com

V. Nishanthi
UG student, Department of IT, SMVEC, Puducherry, India
nishavenkat.175@gmail.com

Abstract—Web service will covert user defined application into web application. Vehicular Adhoc network (VANET) provides information about the surrounding to nearby user. It access and provides web services. Here we are using QOS based services to providers. To provide scalability of services, we are using multiple cluster head protocol (MCHP) and our architecture provides both inter and intra cluster security.

Keywords — Clustering, SOA, Web service, VANET, QoS

I. INTRODUCTION

Web service is an internet based application or it is a communication between two electronic devices over a network. It is platform independent. All web services are registered in the Web service registry. Web service is initiated using XML message. It is a scattered application mainly published and accessed for business needs.

Web service composition is a process of combining and provides link to various existing web according to the users requirements. Based on the service provider web service composition is classified into two types

- Atomic service: It is the service provided from a single service provider.
- Composite service: It is the service provided from multiple providers.

The web service calls the procedure that runs on another machine and they exchange information in XML formats. SOAP provides interoperability and it allows the service to pass through HTTP format. SOAP message has three parts

- Envelope: It Wraps entire message contains header and body.
- Header: It is an optional element with additional information such as security and routing.
- Body: It is an application specific data being communicated.

In WSDL the services are self-describing. This WSDL is an XML based language; it provides applications and also the method to access them. WSDL is only read by application. This WSDL link alone is maintained in UDDI.

UDDI are XML based formats and are used to find the web services with the help of messages and operations as long as the data are transmitted. In this the data are used in a UDDI registry.

Eg: UDDI Business Registry (UBR)

- "White pages"-Contact info, description
- "yellow pages categorization of info, details
- "green pages"-Technical data

An ad hoc network is a wireless network that is used to share internet connection with other people temporarily. For that we need to install a wireless network adapter in our system. The wireless links of this network can be used for connecting mobile nodes. These mobile nodes can communicate with other nodes without the help of access point and so they don't have any fixed structure .It doesn't need any router or base station to establish a connection. This network can be configured by itself. Each node is furnished with a transmitter and receiver. They are said to be independent and dynamic. Each node depends on another node to create or begin communication between them, so each and every node act as a router. This network will be deleted automatically when the user disconnects the network. If we need to share files with more than one computer, a multi-hop ad hoc network should be set up, that can transfer files to various nodes.

Vehicular ad hoc networks (VANETs) are a subcategory of mobile ad hoc networks (MANETs) with the unique property that the nodes are vehicles. Because of the controlled node movement it is a realistic notion that the VANET will be maintained by some static structure that supports with some services and can provide access to immobile networks. The main objective of VANET is to increase road safety. It should increase comfort by means of value additional services like position based services or Internet on the road.

II. RELATED WORK

In existing system, Vehicular ad hoc networks (VANETs) enable vehicles to communicate with each other and with roadside units (RSUs). Service oriented vehicular networks are special types of VANETs that support diverse infrastructure-based commercial services, including Internet access, real-time traffic management, video streaming, and content distribution. Many forms of attacks against service-oriented VANETs that attempt to threaten their security have emerged. The success of data acquisition and delivery systems depends on their ability to defend against the different types of security and privacy attacks that exist in service-oriented VANETs.

It introduces a system that takes advantage of the RSUs that are connected to the Internet and that provide various types of information to VANET users. We provide a suite of novel security and privacy mechanisms in our proposed system and evaluate its performance using the ns2 software. We show, by comparing its results to those of another system, its feasibility and efficiency.

III. LITERATURE SURVEY

a) CARAVAN by Krishna Sampigethaya

In vehicular ad hoc networks (VANET), it is possible to locate and track a vehicle based on its transmissions when communicating with other vehicles or the road-side transportation. This kind of tracking leads to threats on the location privacy of the vehicle's client[1]. Here we study the problem given that the location of privacy in VANET by allowing vehicles to prevent tracking of their broadcast communications [2]. First of all identify the distinctive characteristics of VANET that must be considered when designing suitable location time alone solutions. Based on this clarification, we suggest a location privacy method

known as CARAVAN, and calculate the privacy improvement achieved under some presented standard conditions of VANET applications, and in the occurrence of a global adversary.

b) realistic mobility models by Sommer.C Dressler.F et al

Much progress can be observed in the domain of Vehicular Ad Hoc Network (VANET) research. It has to be seen that study of vehicular contact protocols in the context of VANETs are typically based on reproduction models[3]. This approach has two essentials: First, comprehensive network model of each layer of communication protocols is essential as provided by a wide variety of tools by the networking area. And secondly, sensible model of nodes mobility, that is an accurate modeling of road passage, is needed to approximate positions and actions of involved works[4]. The offerings of this critique are dual: First one is, a review of the development of mobility modeling in VANET replication is provided[5]. Secondly, this critique investigates how latest advances in bidirectional combination of road traffic micro simulation and network simulation lead to more realistic results at comparably low computational cost. In conclusion, this article advocates employing such techniques that are openly available for further studies of new communication protocols and mechanisms in the domain of VANET research.

c) Rapid Generation of Realistic Mobility Models by Feliz Kristianto Karnadi et al .

One emerging, new type of ad-hoc network is the Vehicular Ad-Hoc Network (VANET), in which vehicles constitute the mobile nodes in the set of connections. Due to the too expensive cost of deploying and implementing such a system in existing world, most examine in VANET relies on simulations for estimation. A key component for VANET simulations is a realistic vehicular mobility model that ensures conclusions drawn from simulation experiments will carry through to actual deployments[6]. In this effort, we initiate a tool MOVE that allows users to rapidly create realistic mobility models for VANET simulations. MOVE is built on peak of an open resource micro-traffic simulator SUMO. The production of MOVE is a sensible mobility model and can be directly used by popular network simulators such an ns-2 and qualnet[7]. They have evaluated and compared ad-hoc routing performance for vehicular nodes using MOVE to that using the random waypoint model.

d) ABSRP by Brijesh Kadri Mohandas et al

A vehicular ad-hoc network (VANET) is a network of intelligent vehicles that communicate with other vehicles in the network. The main goal of VANET is to provide comfort and safety for passengers. In adding together, various transaction based services, such as information in relation to gas prices, restaurant list of options, and discount sale, can be provided to drivers. To make these services available, there is a need for an well-organized service innovation protocol[8]. Here we propose a new protocol called Address Based Service Resolution Protocol (ABSRP) to discover services in vehicular ad-hoc networks. The majority of the transaction based services are provided by roadside units, we develop their presence to carry out service discovery. We make use of the unique address assigned to each service provider in order to discover a route to that service provider. Our method proactively distributes the service provider's address along with its servicing capabilities to other roadside units within a particular area. Each and every roadside unit will then make use of this information to service the request placed by the vehicles[9]. If the service provider (destination node) is not reachable over the vehicular network, we suggest using a backbone network to service requests. Our approach is self-determining of the network layer routing protocol.

e) A Stable Routing Protocol by Sakhaee.E. et al .

There are numerous research challenges that need to be addressed until a wide deployment of vehicular ad hoc networks (VANETs) becomes feasible. One of the serious issues has the design of scalable routing algorithms that are robust to frequent path disruptions caused by nodes mobility. This paper gives the use of information of all the node movement (e.g., position, direction, speed, and digital mapping of transportation) to predict a possible link-breakage event prior to its happening[10]. All the nodes are grouped according to their velocity vectors. This kind of grouping ensures that nodes that belong to the same group are further likely to establish stable single and multi hop paths as they are moving together. Surrounding routes that involve only vehicles from the same group guarantees a high level of stable communication in VANETs[11].

f) Situation-aware trust architecture by Dijiang Huang et al .

Situation-Aware Trust — to address several important trust issues in vehicular networks. SAT includes three major works: an attribute based policy control model for highly dynamic communication environments, a proactive trust model to construct trust among vehicles, and avoid the fracture of existing trust, and the email based social network trust system to develop trust and to allow the setup of a decentralized trust structure[12]. To deploy SAT, identity-based cryptography to join together entity trust, information trust, safety strategy enforcement, and public network trust, allocating a single identity, and a set of attributes for each and every entity[13]. We conclude by presenting investigate challenges and possible research directions that extend this

g) Dynamic Clustering- by Abderrahim Benslimane et al .

This paper visualizes VANET-UTMS included network planning, high data proportions of IEEE 802.11p-based VANET and the wide coverage area of 3GPP networks are combined[14]. The nodes in the planning are vigorously grouped based on dissimilar metrics. To link VANET with UTMS, a least amount of nodes which are fitted out with UTRAN interfaces and IEEE 802.11p are taken as gateways[15]. An adaptive mobile gateway controlling device has been proposed and problems relating to gateway controlling, service migration between gateways and gateway advertisement are lectured. Using NS2 software the simulations are done to calculate the performance of the planning including the suggested mechanism. Inspiring results are achieved in terms of high data packet delivery proportions and quantity, packet drops proportions and minimized delay.

h) Enhancing IEEE 802.11p/WAVE to provide infotainment applications by Marica Amadeo et al .

To support the wireless access in the vehicular surroundings, IEEE 802.11p/WAVE (Wireless access for vehicular environment) has been emerged. Utmost of the research contributions have intensive on safety based applications[16]. An extension of IEEE 802.11p is proposed in this paper and is protest with the multiple channel process of the WAVE planning and it targets at the non-safety applications. The W-HCF(WAVE based Hybrid coordination function) procedure influences organized access abilities over the conflict based access of the IEEE 802.11p[17]. It adventures nodes location information and management among WAVE providers to increase the performance of cost sensitive and loss delay non safety applications

i) Spatial Distribution and Channel Quality Adaptive Protocol by Slavik.M Mahgoub.I et al .

In vehicular networks, wireless broadcast is an essential module. There are numerous applications which are built on broadcast communications so well-organized routing methods are critical[18]. DADCQ(Distribution adaptive distance with channel quality) protocol is developed to report the needs.[9] To select the forwarding nodes, the distance method is used by the DADCQ protocol. The performance of this process depends on the significance of the decision threshold, but choosing a threshold value is demanding that results in good performance. The optimal rate is affected by wireless channel quality, spatial distribution pattern and node density. Broadcast protocol personalized to vehicular networking should be adaptive to difference of the aspects[19].

j) A Framework for Secure and Efficient Data Acquisition by KhaleelMershad et al

Inter vehicular communication is used in many industries and hypothetical research enterprises that tries to improve security and efficiency of road schemes. VANET(Vehicular ad hoc networks) is used to establish communication between the nodes and with the roadside units. traffic management in real time, access to internet, video streaming and content distribution are supported by the service oriented vehicular network which is a special type of VANET[21]. Many attacks arises against service oriented VANET that tries to impend the safety. A scheme is introduced in this paper to give different information to the VANET users, and it takes the merits of the roadside units which are connected to the internet and which. Novel safety and privacy mechanisms are provided in the proposed system and its performance is calculated using NS2 software[22]. Its efficiency and feasibility are shown by compared the results with the other systems

k) Distributed Multichannel and Mobility Aware Cluster-based MAC Protocol by Khalid Abdel Hafeez et al

Vehicular safety applications require periodic dissemination of status and emergency messages, contention based MAC protocols such as IEEE 802.11p have problems in predictability, fairness, low throughput, latency and high collision rate, especially in high density networks. Therefore, a distributed multichannel and mobility aware cluster-based medium access control (DMMAC) protocol is proposed. Through channel scheduling and an adaptive learning mechanism integrated within the Fuzzy Logic Inference System (FIS), vehicles organize themselves into more stable and non-overlapped clusters. Each cluster will use different sub channel from its neighbors in a distributed manner to eliminate the hidden terminal problem[22]. Increasing the system's reliability, reducing the time delay for vehicular safety applications and efficiently clustering vehicles in highly dynamic and dense networks in a distributed manner are the main contributions of the proposed MAC protocol. The reliability and connectivity of DMMAC are analyzed in terms of the average cluster size, communication range within the cluster and between cluster heads, and the life time of a path. Simulation results show that the proposed protocol can support traffic safety

l) A Multi-hop Authenticated Proxy Mobile IP Scheme for Asymmetric VANET by Sandra C´espedes et al

Vehicular communications networks are used for the access to drive the Internet and IP-based infotainment applications. These services are supported by road-side Access Routers (ARs) that connect the Vehicular Ad hoc Network (VANET) to external IP networks. However, VANETs suffer from asymmetric links due to variable transmission ranges caused by mobility, obstacles, and dissimilar transmission powers, which make them difficult to maintain the bidirectional connections, and to provide the IP mobility required by most IP applications[23]. Moreover, vehicular mobility results in short-lived connections to the AR, affecting the availability of IP services in the VANET. In this paper, we study the secure and timely handover of IP services in the asymmetric VANET, and propose a Multi-hop Authenticated Proxy Mobile IP (MA-PMIP) scheme. MA-PMIP provides an enhanced IP mobility scheme over infrastructure to- vehicle-to-vehicle (I2V2V) communications that uses location and road traffic information. MA-PMIP also reacts depending on the bi directionality of links to improve availability of IP services. Moreover, our scheme ensures the handover signaling is authenticated when V2V paths are employed to reach the infrastructure, so that possible attacks are mitigated without affecting the performance of the ongoing sessions[24]. Both analysis and extensive simulations in are conducted, and the results demonstrate that MA-PMIP improves service availability and provides secure seamless access to IP applications in the asymmetric VANET.

IV. ANALYSIS ON VARIOUS TECHNIQUES

TABLE I- Analysis of Various techniques used in VANET applications

S.no	Author	Title of the Paper	Theme	Advantage	Disadvantage
1	Krishna Sampigethaya *et al* . [2005]	CARAVAN: Providing Location Privacy for VANET	Addressed the location privacy threats due to tracking of vehicles based on their broadcasts.	Forming cluster groups to reduce broadcast for V2I applications such as probe vehicle data.	Realistic mobility for vehicles is less.
2	Sommer.C Dressler.F et al . [2006]	Progressing toward realistic mobility models in VANET simulations	The evolution of mobility modeling in VANET simulations are provided, outlining the simulation strategies typically used.	Vehicular communication protocols are typically based on simulation models.	Advocates employing openly available communication protocols
3	FelizKristiantoKarnadi et al . [2007]	Rapid Generation of Realistic Mobility Models for VANET	New type of ad-hoc network is the Vehicular Ad-Hoc Network (VANET), in which vehicles constitute the mobile nodes in the set of connections	Introduced a tool MOVE that allows users to rapidly generate realistic mobility models for VANET simulations. MOVE is built on top of an open source micro-traffic simulator SUMO.	Realistic mobility model is significantly different from that of the commonly used random waypoint model.
4	BrijeshKadri Mohandas, AmiyaNayak et al . [2008]	ABSRP - A Service Discovery Approach for Vehicular Ad-Hoc Networks	A new protocol called Address Based Service Resolution Protocol (ABSRP) to discover services in vehicular ad-hoc networks	Vehicular ad-hoc networks will play an important role in providing comfort and safety for passengers.	Approach is independent of the network layer routing protocol.
5	Taleb. T, Sakhaee. E. et al . [2009]	A Stable Routing Protocol to Support ITS Services in VANET Networks	This paper argues the use of information on vehicles' movement information to predict a possible link-breakage event prior to its occurrence.	Reduces the overall traffic in highly mobile VANET networks	To prevent broadcast storms that may be intrigued during path discovery operation
6	Dijiang Huang, Arizona et al . [2010]	Situation-aware trust architecture for vehicular networks	SAT includes three main components: an attribute-based policy control model for highly dynamic communication environments, a proactive trust model to build trust among vehicles, and prevent the breakage of existing trust and to allow the setup of a decentralized trust framework	Situation-Aware Trust-to address several important trust issues in vehicular networks.	Security is less.
7	AbderrahimBenslimane et al . [2011]	Dynamic Clustering-Based Adaptive Mobile Gateway Management in Integrated VANET – 3G Heterogeneous Wireless Networks	Coupling the high data rates of IEEE 802.11p-basedVANETs and the wide coverage area of 3GPP networks e.g.,UMTS	High data packet delivery ratio.	QoS for the differentiating the services according to vehicular priorities is less.
8	MaricaAmadeo et al . [2012]	Enhancing IEEE 802.11p/WAVE to provide infotainment applications in VANETs	IEEE 802.11p/WAVE Wireless Access for Vehicular Environment is the emerging standard to enable wireless access in the vehicular environment.	Improve performances of delay	Scalability is less.

9	Slavik.M Mahgoub.I et al .[2013]	Spatial Distribution and Channel Quality Adaptive Protocol for Multihop Wireless Broadcast Routing in VANET	The Distribution-Adaptive Distance with Channel Quality (DADCQ) protocol and it performs well when compared to several existing multi hop broadcast proposals	Adaptive to variation in these factors such as Node density, spatial distribution pattern, and wireless channel quality	The performance of this method depends heavily on the value of the decision threshold, but it is difficult to choose a value that results in good performance across all scenarios

V. PROBLEM DEFINITION

1. VANET

Vehicular ad hoc networks (VANETs) are a subcategory of mobile ad hoc networks (MANETs) with the unique property that the nodes are vehicles. Because of the controlled node movement it is a realistic notion that the VANET will be maintained by some static structure that supports with some services and can provide access to immobile networks. The main objective of VANET is to increase road safety. It should increase comfort by means of value additional services like position based services or Internet on the road.

2. VANET with QoS metrics

Vehicular ad hoc networks (VANET) composes the qos services like

- Performance
- Reliability
- Scalability
- Capacity
- Robustness Exception Handling
- Accuracy
- Accessibility
- Availability
- Operability

a) VANET scalability

Routing protocols are topology-based and Geographic routing is the two major classifications of routing protocols in VANET. Topology-based routing uses the facts about relations that exist in the network to implement packet dispatching. Under topology based routing Proactive and Reactive are present. Geographic routing uses adjacent location information to perform packet dispatching. Proactive routing carries the routing information such as the next forwarding hop is retained in the background irrespective of communication requests. In reactive routing, it opens a route each and every time it is essential for a node to communicate with the other. It keeps only the routes that are currently in use; in this manner it reduces the burden on the network.

The Clustering protocol is appropriate for locations where devices have different competencies with respect to power, data rate, computing resources, or have different parts in an application set-up. The primary goal of the Clustering protocol is to provide a protocol solution that is suitable for a comprehensive variety of networking set-ups where cluster development can be abused. Collection of nodes forms a cluster. The clusters can be formed by the Cluster Protocol which consists of logical connections between a cluster head and its cluster members.

b) VANET security

Diffie Hellman key exchange is a method that provides security for the VANET. This method can be used for secret communication over a public network. Diffie Hellman is a way to interchange cryptographic keys between two parties without any prior knowledge. Public key and private key are the two types of keys used here. The messages can be encrypted and decrypted by the keys.

Intrusion detection provides security for network and computer. It collects and evaluates all the information about computer and the network from various places to identify the security gaps. It is mainly used to avoid the malicious node which tries to enter into

the network. It contains two procedures, host-based and network-base. In host-based procedure, inspection of the configuration files, password files and the other areas of the system are detected.

VI. QoS Requirements

The QoS refer to the high quality of services provided to a web service. These may include performance, scalability, capacity, security, exception handling, accuracy, integrity, robustness, accessibility, reliability, availability, interoperability and network-related QoS requirements. Depending on user's requirement, the qos parameters are classified as follows

i. Performance

The performance of a web service signifies how fast a service request can be finished. It can be measured in terms of response time, execution time, transaction time, throughput, latency and so on.

Throughput is the number of web service requests served in a given amount of time. Response time is the time taken to complete a web service request. Latency is the round-trip delay (RTD) between sending a request and receiving the response. Execution time is defined as the time taken to do its activities one by one in an order. Transaction time defines the time taken for the web service to complete a transaction.

ii. Reliability

Web services should be given with good reliability. Reliability signifies the capability of a web service to achieve its required functions under given terms for a stated time interval. The reliability is the complete measure of a web service to maintain its service quality. Reliability is also associated to the secure data being transmitted and received by service requestors and service providers.

iii. Scalability

Web services should be provided with great scalability. Scalability represents the skill of increasing the computing capacity of service provider's computer system and system has the ability to process more transactions, operations or user's requests in a given time interval .It is also related to performance. In case of count of operations and transaction the web services must be scalable.

iv. Capacity

Web services should be provided with the required capacity. Capacity is the bound of the number of concurrent requests which should be provided with definite performance .Web services should support the required number of concurrent connections.

v. Robustness

Web services should be provided with high robustness. Robustness denotes the degree to which a web service can work correctly even in the presence of invalid or conflicting inputs. Web services should still work even if inadequate parameters are provided to the service request invocation.

vi. Exception Handling

Web services should possess the functionality of exception handling. It is not possible for the service designer to specify all the possible outcomes and alternatives, exceptions should be handled properly. Exception handling is associated with how the service handles these exceptions.

vii. Accuracy

Web services should be provided with high accuracy. Accuracy here is defined as the fault rate generated by the web service The number of faults that the service generates over a time interval should be reduced.

viii. Accessibility

Web services should be provided with high accessibility, here it represents whether the web service is capable of serving the client's requests. High accessibility can be achieved.

ix. Availability

The web service should be ready for instant consumption. Time-to-Repair (TTR) is related with availability. TTR denotes the time it takes to repair the web service .The service should be available instantaneously when it is invoked.

x. Interoperability

Web services should be interoperable in the different platforms to implement services, so the developers using those services should not think about which programming language or operating system the services are presented on.

VII. CONCLUSION

How we can ensure security and privacy in Qos composed services of VANETs represents a challenging issue. In this paper, we have answered this question with our proposed privacy-preserving data acquisition and forwarding scheme by introducing a novel and provable cryptographic algorithm for key generation and powerful encryption. The evaluation of our proposed scheme confirmed its effectiveness compared to a recent security mechanism for VANETs. The ongoing work on REACT focuses on making the proposed system more scalable in terms of the number of users that can connect to an RSU. We are designing an RSU scheduling mechanism in which an RSU builds a schedule that is divided into time slots (TSs). In each TS, all users that are expected to connect to the RSU are specified. Hence, an RSU prepares users' data and caches them during a free TS before the users connect. Using this scheme, the RSU distributes its load among the available TSs.

REFERENCES

[1] Krishna Sampigethaya *et al* ., "CARAVAN: Providing Location Privacy for VANET"

[2] Sommer.C Dressler.F *et al* ., "Progressing toward realistic mobility models in VANET simulations",Communications Magazine, IEEE (Volume: 46, Issue: 11), November 2008.

[3] FelizKristianto Karnadi *et al* ., Rapid Generation of Realistic Mobility Models for VANET

[4] Brijesh Kadri Mohandas *et al* ., "ABSRP - A Service Discovery Approach for Vehicular Ad-Hoc Networks",2008 IEEE Asia-Pacific Services Computing Conference

[5] Taleb. T,Sakhaee. E. *et al* ., "A Stable Routing Protocol to Support ITS Services in VANET Networks",Vehicular Technology, IEEE Transactions on (Volume: 56, Issue: 6), Nov. 2007

[6] Dijiang Huang, Arizona State University *et al* ., "Situation-aware trust architecture for vehicular networks",IEEE Communications Magazine , November 2010.

[7] Abderrahim Benslimane *et al* ., "Dynamic Clustering-Based Adaptive Mobile Gateway Management in Integrated VANET – 3G Heterogeneous Wireless Networks", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 29, NO. 3, MARCH 2011

[8] Marica Amadeo *et al* ., "Enhancing IEEE 802.11p/WAVE to provide infotainment applications in VANETs",www.elsevier.com/locate/adhoc

[9] Slavik.M Mahgoub.I *et al* ., "Spatial Distribution and Channel Quality Adaptive Protocol for Multihop Wireless Broadcast Routing in VANET", Mobile Computing, IEEE Transactions on (Volume:12 , Issue: 4),April 2013

[10] Khaleel Mershad *et al*., "A Framework for Secure and Efficient Data Acquisition in Vehicular Ad Hoc Networks", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 62, NO. 2, FEBRUARY 2013.

[11] Khalid Abdel Hafeez *et al*., "Distributed Multichannel and Mobility Aware Cluster-based MAC Protocol for Vehicular Ad-hoc Networks (VANETs)", unpublished.

[12] Sandra C´espedes *et al*., "A Multi-hop Authenticated Proxy Mobile IP Scheme for Asymmetric VANET", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, 2013.

[13] J. Freudiger, M. Raya,M. Feleghhazi, P. Papadimitratos, and

J. P. Hubaux, "Mix zones for location privacy in vehicular networks," presented at the Int. Workshop Wireless Netw. Intell. Transp. Syst., Vancouver, BC, Canada, Aug. 2007 LCA-CONF-2007-016.

[14] GeoNet Project. [Online].Available:http://www.geonetprojectu.e

[15] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing wireless location privacy using silent period," in *Proc. IEEE WCNC*, New Orleans,

[16]] B.M. Reed and D.A. Jacobs, Quality Function Deployment for Systems. Nat'l Aeronautics and Space Administration, 1993.

[17] [48] P. Runeson and C. Wohlin, ªStatistical LA, 2005, pp. 1187–1192.

[18] J. L. Huang, L. Y. Yeh, and H. Y. Chien, "ABAKA: An anonymous LA, 2005, pp. 1187–1192.

[19] ITSSv Project. [Online]. Available: http://www.lara.prd.fr/projects/itssv6 "Key size," Wikipedia. [Online]. Available: http://en.wikipedia.org/wiki/ Key_size

[20] H. Kido, Y. Yanagisawa, and T. Satoh, "An anonymous communication technique using dummies for location-based services," in *Proc. ICPS*, Santorini, Greece, Jul. 2005, pp. 88–97.

[21] C. Laurendeau and M. Barbeau, "Threats to security in DSRC/WAVE," in *Proc. ADHOC-NOW*, 2006, vol. 4104, pp. 266–279.

[22] C. T. Li, M. S. Hwang, and Y. P. Chu, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks," *Comput. Commun.*, vol. 31, no. 12, pp. 2803–2814, Jul. 2008.

[23] C. Lochert, B. Scheuermann, C. Wewetzer, A. Luebke, and M. Mauve, "Data aggregation and roadside unit placement for a VANET traffic information system," in Proc. 5th ACM Int. Workshop VANET, San Francisco, CA, Sep. 2008, pp. 58–65.

[24] Brijesh Kadri Mohandas *et al* ., "ABSRP - A Service Discovery Approach for Vehicular Ad-Hoc Networks",2008 IEEE Asia-Pacific Services Computing Conference

