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. 4, April 2014, pg.275 – 283

RESEARCH ARTICLE

SAAS – A Gateway to Cost Effective Secure Vehicular Clouds

M.R.Yasmeen, PG Scholar, Karpagam University, Coimbatore Tamil Nadu, India
Email-id: yyasmeen.84@gmail.com
M.Ramya Devi (Ph.D), Assistant Professor, Karpagam University, Coimbatore Tamil Nadu, India
Email-id: ramyamurugadasan@gmail.com

Abstract - Vehicular Cloud Communication (VCC) is the latest buzz in conventional cloud computing. In a Vehicular Cloud (VC), the commuters share resources ranging from storage to computing power to renting it to others over the Internet. The broad horizon calls for covering various aspects of security, social impact, cost effective communication. Much research has been carried over the VC architecture, security challenges and potential threats applicable in the VCs. This paper highlights a cost effective, hassle free, secure communication between the cloud and misshaped vehicles. Communication is established via Software as a Service (SAAS). Additionally, the nearest medical help is made available. Both haversine and GeoAPI distance matrix have been used for the same. The security challenge is addressed with the help of Digital Signature Algorithm (DSA). AES and Blowfish have been evaluated to compute the message processing speed.

Index Terms — Communication, SAAS, DSA, AES, Blowfish, Vehicular Cloud, distance matrix, Web Socket

I. INTRODUCTION

With the advent of cloud computing and fast development of automotive industry and Information and Communication technology, lives have been greatly influenced. There is a paradigm shift in the way vehicles are visualized and utilized. It is no more just a means of commute but an integral part of technology enhancement serving people to make their lives better. VANET was the basic building block. In VANETs, Road Side Units (RSUs) and Vehicles were configured together. The goals of VANET were limited to safety of drivers and their safe journey. This resulted in hardware investments, embedding of units at various locations and registration of vehicles location wise. Each vehicle has to cooperate with its peer via Road Side Infrastructure (RSI) in a vehicle-to-vehicle (V2V) or Vehicle-to-infrastructure (V2I) set up to share messages or resources effectively.

The disadvantages of VANET can be overcome by merging VANET attributes with Cloud. Both are pulled together to reap the benefits at a larger scale.

The vision of Vehicular clouds [2]-[4] has been promoted by Prof. Olariu and his co-workers. The underutilized resources of vehicles, storage and computing power are harnessed to greater extent. Researchers have addressed security issues related to VC. It may look superficially similar to the ones experienced in VANETs. There are challenges involving high mobility vehicles and their accountability via dedicated short range communication (DSRC) transceivers [6]. The communication difficulties pave way for our proposal of a new solution.

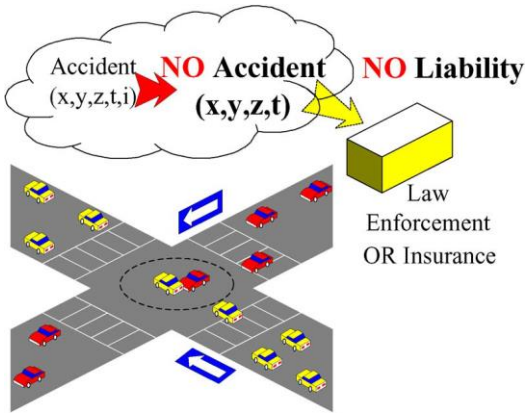


Fig. 1 Security Issue in VCs.

The fig.1.exhibits the possible accident scenario and the way the information could be tampered. Gongjun Yan and his co-workers have proposed security framework for the scenario illustrated in fig.1.

The main contributions of this paper are to strengthen the security framework and establish a faster, reliable communication with the help of SaaS application.

II. STATE OF THE ART

The security challenges are evolving with the growth of Vehicular clouds. The vehicles are pooled as cloud resources for providing services to genuine users. Many real time services are being provided by this cloud such as smart electric power grids, intelligent commuting systems and mobile laboratories. Though the framework has been developed for computing VC and the security challenges are being addressed, there is ample room for creating a near fool proof system. So would be the case of establishing a robust communication system.

Large numbers of papers have addressed security issues related to Vehicular ad hoc network (VANET). Active and Passive location security has been proposed by Yan et al. [10], [11]. The users are authenticated and validated using digital signatures. The messages are encrypted so as not to disclose the message contents. GeoEncrypt has been proposed in VANET by Yan et al. [13].

In the recent times, cloud security problems have been addressed. The solutions were to restrict the hardware accessibility to ensure minimal risks from insiders [15]. New platform was proposed by Santos et al. [16] to have a trustworthy conventional cloud. The Set of virtual machines (VMs) are made available to users by introducing a third party trust coordinator. Garfinkel et al. [17], Berger et.al [18] and Murray et.al [19], adopted similar solution to prevent the interference in the host services by the physical host owner. On system boot up, the system information is recorded and sent to third-party along with hash value. The trust of the cloud would be evaluated by the Trust Center.

III. OVERVIEW OF VEHICULAR CLOUDS

Vehicular Clouds (VCs) utilize the concept of Cloud Computing and VANETs together. There are two types of VCs. *Infrastructure-based* VC and *Autonomous* VC (AVC) [3]. In the Infrastructure based VC, the driver's access roadside infrastructure for services. In AVC, the vehicles are organized in VC to support emergencies and ad hoc events.

The VC services can be categorized into three levels, application, platform and infrastructure. The *Infrastructure as a Service* (IaaS) level offers fundamental services such as sensing, computing, keeping attackers at bay, storage. The next level is *Platform as a Service* (PaaS), where the components and services such as Hyper Text Transfer Protocol Daemon (httpd), ftpd and email server are provided and configured as service. The top most layer is SaaS – *Software as a Service*, where the users pay per their usage.

VCs offer cost-efficient way of services. Smart combinations of storage, price, and communication abilities of VC can be chosen.

A. PROBABLE VC APPLICATIONS

Some of the possible applications of VCs are listed below.

1) *Maintenance of Vehicles*: The new version of software uploaded by the manufacturer is made available to the vehicles.
2) *Management of Traffic*: Traffic status is delivered to the drivers.
3) *Sharing Road Condition*: Drivers are alerted about any blockage of seriousness of the road conditions.
4) *Alert Accidents at road intersections*: In heavily demanding driving conditions, this service is made use of. It lets the drivers know of any accidents that would have occurred at the road intersections. It alerts them of any intersections in the near distance to avoid accidents in case of poor visibility.
5) *Application for safety*: used for preventing collisions or controlling cruise.
6) *Intelligent Parking System*: The vehicles can chose their parking lot by taking the availability into consideration.
7) *Evacuations*: The VCs may come handy in case of any evacuations due to natural hazards.

IV. PREVAILING SECURITY CHALLENGES IN A VEHICULAR CLOUD

Vehicular clouds have challenges that look alike to the difficulties faced in VANET and cloud computing. This section identifies the various challenges associated with a Vehicular cloud.

A. MOBILITY AND LOCALIZATION

The vehicular cloud has to authenticate the highly mobile vehicles. It has to verify the identity of users and check for the integrity of messages received from them. A few authentication metrics that can be adopted [28] are:

1) Ownership: Unique identity like security token, identity card and user owned software token.
2) Knowledge: Security questions, passwords, private identification numbers.
3) Biometrics: Human biometrics like fingerprints, signature, eye scan, voice.

The high mobility makes it difficult to address the authentication needs of vehicles. Their location has to be considered in addition to the associated messages and the time at which they were triggered. With the vehicles constantly changing the location, it becomes tedious to transmit the authentication message to them. Also, the security token is hard to update.

Identifying the drivers' identity in VC is equally challenging. Pseudonyms are used to wade off the privacy issues resulting from simple to complex Sybil attacks [29].

The vehicles location could be traced using radars. This is essential as the VC applications need the exact location details. Hence, it becomes mandatory to validate the location information. Situations wherein the radar detection is not possible, statistical methods could be applied to determine the location of vehicles. [10], [30].

B. SECURITY ATTACKS AND THREATS IN VC.

1) Attacker Model: In traditional security systems, the attackers are prevented from sneaking into the system. However, it is an arduous task when it comes to making the VC more secure. In the current VC environment, the same infrastructure is shared amongst the attacker and their targets, though they may be assigned to different virtual machines. Hence, the modern day attackers outweigh the traditional attackers.

The main targets of an attacker are as listed below:

a) Integrity: executable code, documents and results.
b) Confidentiality: identity of users, location of VMs, valuable data stored on VCs.
c) Availability: services, privileges, machines and applications.

The attackers could try to jam the system with multiple requests there by blocking the availability of resources and services to the needy. It might even try to leak the high privileges to gather the assets [24].

The attackers face many challenges as well. The high mobility has both pros and cons. The attackers will have to make repeated attempts to harm the vehicles. The access to each VM is transitory as the vehicles are bound to move across the states or districts. Moreover, the attackers have to locate the machine on which targets would be lying as it's a distributed environment.

2) Threats: The VC threats can be classified with the help of STRIDE [27]: a system for categorizing the security threats of computer by Microsoft. These categories are briefed as follows:

a) Spoofing user identity: "Man-in-the-middle" attack is the classic example. Here, the attacker enacts himself as a legitimate user to obtain the information intended for the original user.
b) Tampering: The data is altered and forged by the attackers.
c) Repudiation: The identification is forged in case of operations, new data and other actions.
d) Information disclosure: The personally identifiable information is uncovered by the attackers such as finance, identities, residence, medical, political, biological traits.
e) Denial of Service: This results from eating up of available resources by the attackers.
f) Elevation of privilege: The attackers enhance their privileges by intruding into the current system. They alter the configuration or application itself that are meant for normal users.

C. SCALABILITY

The vehicular clouds must be capable of addressing security schemes for dynamically growing number of vehicles. They should not only handle the usual traffic but ought to take care of extra fluctuation that may occur in case of emergencies or natural disasters.

This leads to dynamic security demands. This could be achieved with a careful study of algorithms. It is necessary to choose better algorithms so as to increase the response time along with the maintenance of a highly secure environment that is less prone to vulnerabilities.

D. ESTABLISH TRUST RELATIONSHIPS

It is essential to establish a trust relationship in any secure system. It is one of the important factors. There are many governmental organizations that are trusted. Their relationship with vehicles is governed using legitimacy and uniqueness of identity.

However, establishing a trust relationship becomes cumbersome due to large number of vehicles. In VCs, it's a mammoth task when compared to the traditional VANETs and conventional cloud. Multiple participants push VC on DSRC. The applications need multi hop routes involving multiple nodes in the existing communication. Henceforth, the VC inherits the challenges to establish a trust relationship amongst many vehicles, the available roadside infrastructure, networks, secret key generators and service providers.

V. RESEARCH APPROACH

In this paper, we have addressed two issues in Vehicular clouds.

A. Enhancing security of VC messages

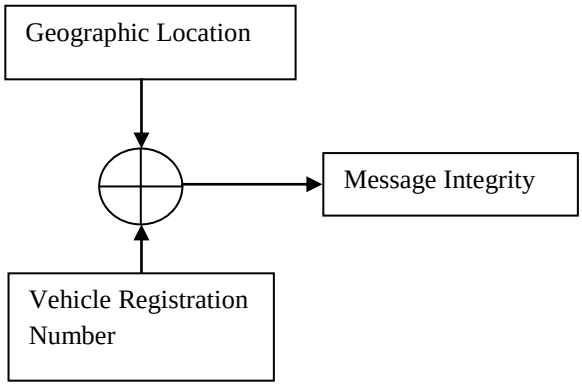


Fig 2. Criteria for Authentication

To enhance the security of VC messages, we have combined two parameters. One is the geographic location and the other is the unique identifier or vehicle registration number.

Digital signature Algorithm is used for the encryption. The geographic location serves as a public key and registration number acts as the private key. This would make it more difficult for the attackers to crack the code. For instance, the message shall be delivered to the vehicles within the geographic location specified and only those vehicles will be able to decrypt the message. Vehicles outside the geographic location would not be able to decrypt it. Thus, it enhances the physical security. As the decryption region is specified dynamically, mounting of attacks is arduous. The server could make out the integrity of message by validating the private key in its legal list of registered vehicles.

We further tried the Blowfish algorithm to fasten up the process of sending the message. Instead of line by line parsing which is followed in the AES algorithm, the Blowfish ciphers the data block wise which in turn reduces the time for processing.

In our experiment of 15 vehicular nodes, we computed the difference between AES and Blowfish which resulted in the following graph.

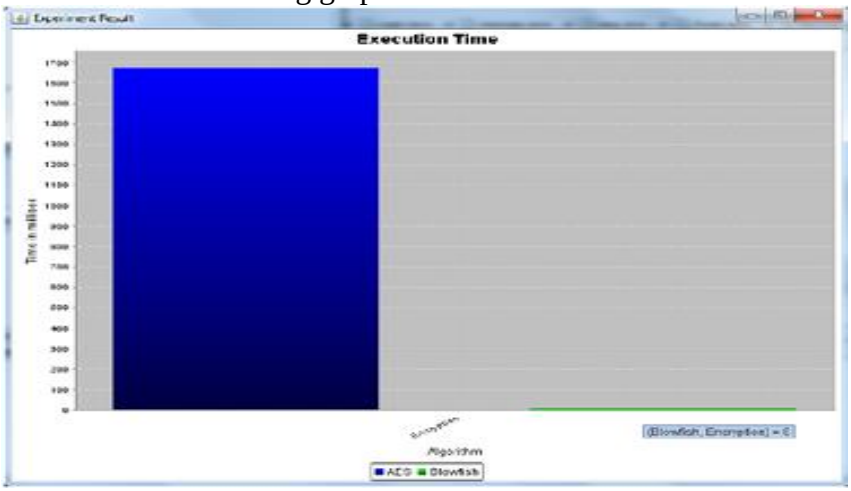


Fig 3. Graph illustrating the difference between AES and Blowfish algorithm usage.

The result of AES is shown in blue color and Blowfish is shown in green color. The AES took 1680 ms to process the message whereas the Blowfish Algorithm took just 8 ms to process it.

B. Ease of communication for highly mobile vehicles

A SaaS application is developed for improvising the way vehicles communicate with the virtual machines. We use the concept of WebSockets. This is to ensure a cost effective, smooth, faster communication between the cloud server and the nodes or vehicles.

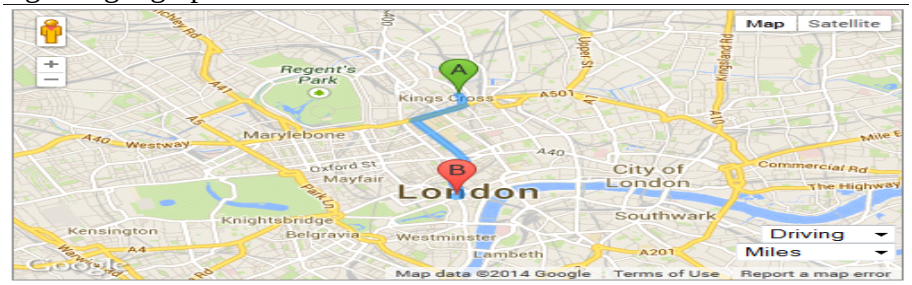
Each Virtual Machine is loaded with the SaaS application to listen to the triggered event. If the VM is overloaded or the service is down due to machine discrepancies, the call could be transferred to other VM that has been configured to act as a backup.

We considered vehicles in few geographic locations. The virtual machines have the information about the ambulance available to respond in case of emergencies and their geographic locations. The vehicles would transmit the longitude, latitude information with the help of WebSockets to the VM. The VM would then compute the nearest available ambulance based on the lat-long information.

To evaluate, we had made use of haversine formula.

$a = \sin^2(\Delta\phi/2) + \cos(\phi1).\cos(\phi2).\sin^2(\Delta\lambda/2)$
$c = 2.\text{atan2}(\sqrt{a}, \sqrt{(1-a)})$
$d = R.c$
where ϕ is latitude, λ is longitude,
R is earth's radius (mean radius = 6,371km)

Apart from haversine formula, we made use of the GeoAPI distance matrix. This way the sever would tradeoff between the time taken by the ambulance to reach the destination in case of an emergency and the driving distance estimate. The same would be communicated to the vehicles in the given geographical location.



Ambulance / Cars	Buckingham Palace	Houses of Parliament	Tower Bridge	Trafalgar Square	Westminster Abbey
Euston	2.4 mi 8 mins	2.3 mi 8 mins	3.9 mi 12 mins	1.8 mi 7 mins	2.4 mi 8 mins
Kings Cross	2.9 mi 9 mins	2.7 mi 9 mins	4.1 mi 12 mins	2.2 mi 8 mins	2.8 mi 9 mins
Liverpool St	3.5 mi 11 mins	3.3 mi 10 mins	2.4 mi 8 mins	2.8 mi 10 mins	3.4 mi 11 mins
Paddington	2.7 mi 8 mins	3.5 mi 11 mins	6.0 mi 18 mins	3.4 mi 10 mins	3.4 mi 10 mins
St. Pancras	2.9 mi 9 mins	2.7 mi 9 mins	4.1 mi 12 mins	2.2 mi 8 mins	2.8 mi 9 mins
Victoria	0.6 mi 2 mins	1.4 mi 5 mins	4.2 mi 13 mins	1.4 mi 5 mins	1.1 mi 4 mins
Waterloo	1.6 mi 5 mins	0.9 mi 3 mins	2.8 mi 8 mins	1.5 mi 5 mins	1.0 mi 3 mins

Fig 4. Experimental result for a set of cars, ambulances, distance matrix, time matrix and the graphical representation of the shortest distance for ambulance.

VI. CONCLUSION

Security and ready reckoning of communication are two priorities of Vehicular clouds. In this paper, we have used the DSA encryption algorithm to restrict the information availability to selected users, thus improvising over Elgamel Signature results. We evaluated and compared both AES and Blowfish algorithm. The real time services are used to determine the vehicles' geographical co-ordinates which are then sent to the cloud server. The SaaS application computes the information and finds the nearest available medical help. The calculation is based on the distance in miles and time taken for each available ambulance to reach the disaster hit area. There is a tradeoff between distance and time. The vehicles are intimated about it.

In future, we would like to overcome the current issues faced with WebSockets and other security issues. Also, the cloud server loads could be configured with the help of elastic load balancing.

ACKNOWLEDGEMENT

The authors are obliged to friends and colleagues for their constructive opinion that have helped us improvise the thought flow and paper organization.

REFERENCES

[1] Gongjun Yan, Ding Wen, Stephan Olariu, and Michele C. Weigle, "Security Challenges in Vehicular Cloud Computing" IEEETransactions on Intelligent Transportation Systems,Vol. 14,No.1, March 2013.

[2] S. Arif, S. Olariu, J. Wang, G. Yan, W. Yang, and I. Khalil, "Datacenter at the airport: Reasoning about time-dependent parking lot occupancy," *IEEE Trans. Parallel Distrib. Syst.*, 2012, [Online]. Available: http://www.computer.org/csdl/trans/td/2012/11/ttd2012112067-abs.html

[3] S. Olariu, M. Eltoweissy, and M. Younis, "Toward autonomous vehicular clouds," *ICST Trans. Mobile Commun. Comput.*, vol. 11, no. 7–9, pp. 1–11, Jul.–Sep. 2011.

[4] S. Olariu, I. Khalil, and M. Abuelela, "Taking VANET to the clouds," *Int.J. Pervasive Comput. Commun.*, vol. 7, no. 1, pp. 7–21, 2011.

[5] Rasheed Hussain, Junggab Son, Hasoo Eun, Sangjin Kim and Heekuck Oh, "Rethinking Vehicular Communications: Merging VANET with Cloud Computing", IEEE 4th International Conference on Cloud Computing Technology and Science, 2012.

[6] L. Li, J. Song, F.-Y. Wang, W. Niehsen, and N. Zheng, "IVS 05: New developments and research trends for intelligent vehicles," *IEEE Intell. Syst.*, vol. 20, no. 4, pp. 10–14, Jul./Aug. 2005.

[7] G. Yan and S. Olariu, "A probabilistic analysis of link duration in vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 4, pp. 1227–1236, Dec. 2011.

[8] H. Xie, L. Kulik, and E. Tanin, "Privacy-aware traffic monitoring," *IEEE Trans. Intell. Transp. Syst.*, vol. 11, no. 1, pp. 61–70, Mar. 2010.

[9] D. Huang, S. Misra, G. Xue, and M. Verma, "PACP: An efficient pseudonymous authentication based conditional privacy protocol for vanets," *IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 3, pp. 736–746, Sep. 2011.

[10] R. Hasan, *Cloud Security*. [Online]. Available:http://www.ragibhasan.com/research/cloudsec.html

[11] G. Yan, S. Olariu, and M. C.Weigle, "Providing VANET security through active position detection," *Comput. Commun.*, vol. 31, no. 12, pp. 2883–2897, Jul. 2008, Special Issue on Mobility Protocols for ITS/VANET.

[12] G. Yan, S. Olariu, and M. Weigle, "Providing location security in vehicular ad hoc networks," *IEEE Wireless Commun.*, vol. 16, no. 6, pp. 48–55,Dec. 2009.

[13] J. Sun, C. Zhang, Y. Zhang, and Y. M. Fang, "An identity-based security system for user privacy in vehicular ad hoc networks,"*IEEE Trans. Parallel Distrib. Syst.*, vol. 21, no. 9, pp. 1227–1239, Sep. 2010.
[14] G. Yan and S. Olariu, "An efficient geographic location-based security mechanism for vehicular ad hoc networks," in *Proc. IEEE Int. Symp. TSP*, Macau SAR, China, Oct. 2009, pp. 804–809.
[15] A. Friedman and D. West, "Privacy and security in cloud computing," *Center for Technology Innovation: Issues in Technology Innovation*, no. 3, pp. 1–11, Oct. 2010.
[16] J. A. Blackley, J. Peltier, and T. R. Peltier, *Information Security Fundamentals*. New York: Auerbach, 2004.
[17] N. Santos, K. P. Gummadi, and R. Rodrigues, "Toward trusted cloud computing," in *Proc. HotCloud*, Jun. 2009.
[18] T. Garfinkel, B. Pfaff, J. Chow, M. Rosenblum, and D. B. Terra, "Virtual machine-based platform for trusted computing," in *Proc. ACM SOSP*, 2003, pp. 193–206.
[19] S. Berger, R. Cáceres, K. A. Goldman, R. Perez, R. Sailer, and L. van Doorn, "VTPM: Virtualizing the trusted platform module," in *Proc. 15th Conf. USENIX Sec. Symp.*, Berkeley, CA, 2006, pp. 305–320.
[20] D. G. Murray, G. Milos, and S. Hand, "Improving XEN security through disaggregation," in *Proc. 4th ACM SIGPLAN/SIGOPS Int. Conf. VEE*, New York, 2008, pp. 151–160.
[21] F. J. Krautheim, "Private virtual infrastructure for cloud computing," in *Proc. Conf. Hot Topics Cloud Comput.*, 2009, pp. 1–5.
[22] M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, "On technical security issues in cloud computing," in *Proc. IEEE Int. Conf. Cloud Comput.*, 2009, pp. 109–116.
[23] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in *Proc. IEEE INFOCOM*, San Diego, CA, 2010, pp.1–9.
[24] Q.Wang, C.Wang, J. Li, K. Ren, andW. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in *Proc.14th ESORICS*, 2009, pp. 355–370.
[25] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds," in *Proc. 16th ACM Conf. CCS*, 2009, pp. 199–212.
[26] SIRIT-Technologies, White paper. DSRC technology and the DSRC industry consortium (DIC) prototype team.
[27] D. Wen, G. Yan, N. Zheng, L. Shen, and L. Li, "Toward cognitive vehicles," *IEEE Intell. Syst. Mag.*, vol. 26, no. 3, pp. 76–80, May–Jun. 2011.
[28] Microsoft, The stride threat model. [Online]. Available: http://msdn.microsoft.com
[29] Fed. Fin. Inst. Examination Council, Authentication in an Internet banking environment 2009. [Online]. Available: http://www.ffiec.gov/pdf/authentication_guidance.pdf
[30] J. Douceur, "The sybil attack," in *Proc. Rev. Papers 1st Int. Workshop Peer-to-Peer Syst.*, 2002, vol. 2429, pp. 251–260.
[31] G. Yan, W. Yang, E. F. Shaner, and D. B. Rawat, "Intrusion-tolerant location information services in intelligent vehicular networks," *Commun.Comput. Inf. Sci.*,, vol. 135, pp. 699–705, 2011.
[32] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inf. Theory*, vol. IT-31, no. 4, pp. 469–472, Jul. 1985.

