Asian Journal of Computer Science and Technology
ISSN: 2249 - 0701 Vol. 3 No. 1, 2014, pp. 12 - 19

Survey on Security Challenges in Warning Message Dissemination and Possible Solutions

Salini Balakrishnan and C. Tripti and Robin Cyriac

Department of Computer Science, Rajagiri School of Engineering and Technology, Cochin, Kerala - 682039, India

E-mail: salini.lunar@gmail.com, tripti.c@rajagiritech.ac.in and robinc@rajagiritech.ac.in

(Received on 12 January 2014 and accepted on 18 March 2014)

***Abstract* – The recent advances in the area of Wireless Communications in Vehicular Ad-hoc Networks (VANET) have brought an emerging platform for both industrialists and for researchers. VANET possess a dynamic topology with multi-hop networks leading to an infrastructure less nature. Communication happens in two ways, one between the moving vehicles and with the Road Side Units (RSU). The usage of wireless medium would surely make it vulnerable to different attacks. By enabling prompt and correct warning messages on road conditions, accident cases etc. VANET can be used to save lives of people, which is the most important application of VANET. Distributing warning messages over a long range is however a very challenging task since message integrity has to be ensured. Also for making the system more reliable non-repudiation should also be included in the security module. A survey of security issues in notification and warning message dissemination is done in this paper.**

Keywords: **Security, Vulnerabilities, Solutions**

I. Introduction

During the last decades, the total number of vehicles around the world is growing enormously. Especially in India traffic is growing four times faster than the population. For a few years road safety has turned out to be a main issue for governments and for car manufacturers as well. So now the focus and effort of companies, researchers and institutions is on improving road safety with the development of new vehicular technologies. Now communication systems has been designed where vehicles can directly take part in the network by making use of the evolved wireless technologies, leading to the creation of networks such as VANETs. Vehicular Ad-hoc Networks is a type of Mobile Ad-hoc Networks (MANET), where the mobile units are vehicles.

The concept being deployed in VANET is the continuously varying vehicular motion. The nodes or vehicles as in VANETS can move around following the road topology with their direction and speed. Vehicular adhoc network (VANET) involves vehicle to vehicle (V2V), vehicle to roadside (V2R) or vehicle to infrastructure (V2I) communication [2] as shown in Fig. 1. This promising technology for future smart vehicle systems and Intelligent Transportation Systems (ITS) has the potential to increase road safety. VANET normally consists of On Board Unit (OBU) and Road Side Units (RSUs). OBU equip a vehicle with short-range wireless capability to form adhoc network between vehicles. Global Positioning System (GPS) can be used to determine the correct location information of each vehicle.

Congestion reduction, accidents prevention, safer roads are some of the benefits of VANETs. The development of an efficient system in VANETs has many important benefits, to the traffic police as well as to the drivers. Proper traffic alerts and updated information about traffic incidents will make safe driving, increase road safety and reduce the traffic jams in the city. It also helps to identify where the traffic rules violations takes place. Furthermore, it also helps in economic ways; real- time traffic alerting will reduce trip time and fuel consumption and therefore decrease pollution as well [18]. There is another important case that does not correspond exactly to a warning of an incident with a determined location, but has also important implications in road safety [5]. That is the case of a warning of the presence of an emergency vehicle like police, ambulance, fire-fighters, etc. So it is definitely beneficial in many ways.

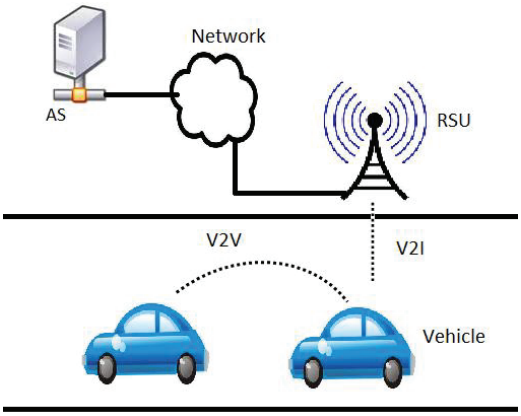

Fig. 1 V2V and V2I Communication

Transportation safety is one of the most important applications of vehicular networks. By providing services like passing traffic information, weather related information, inter-active messages and internet service offerings, user comfort can be enhanced by making use of VANETs. Warning message dissemination such as alert messages to warn other vehicles about potential danger kind of services are used by most of these applications. Vehicles can communicate information on traffic and road conditions with each other, as well as with fixed network nodes. By notifying other vehicles by safety message dissemination in case of an accident can be used to prevent secondary accidents and thereby help in the rescue of people from further collision. So a warning message dissemination scheme which is reliable along with alarm message broadcast system with low delivery delay need to ensured [21].

Security is one of the crucial challenges but only limited attention [8], [4], [21], [11], [5] has been paid for the same. The presence of adversaries or attackers needs to be considered while deploying VANET. Adversaries may inject false or modified messages to the network, repeated messages will be broadcasted again and also impersonation of vehicles will be done. Therefore, the security of communications in VANETs is an essential factor to preventing all these threats. Likewise, non-repudiation should also be enforced but at the same time user privacy need to be protected as well. All these bring forth the importance of various security aspects for VANETs.

Remainder of this paper is organized as follows: Various security vulnerabilities are being showcased in section II, in section III an overview on properties we have to ensure in security mechanisms are being discussed. Followed by a detailed analysis on the importance of Security and Privacy in section IV. Different security schemes and concepts are familiarized in section V and then with a conclusion paper is being completed.

II. Security Vulnerabilities

A rogue version of the vehicular communication protocol stack leads to possible threats for any device in which wireless communication is enabled. Adversaries or attackers possess devices which deviate from such defined protocols. Vehicle manufacturers, by using a variant of the widely deployed IEEE 802.11 protocol makes the attacker's task more easy [23]. The working of a node cannot be concluded as correct even by having proper credentials. The effects of different attackers (internal or external, rational or malicious, independent or colluding, persistent or random) can be different as well. A general exploration on vehicular communication vulnerabilities are being discussed below [7].

A. Jamming

The jammer deliberately generates interfering transmissions that prevent communication within their reception range. Since the network coverage area (along a highway) can be well-defined, at least locally jamming requires only very less effort. As Fig. 2 illustrates, without violating any cryptographic mechanisms and also with very limited power on transmission an attacker can easily partition the network.

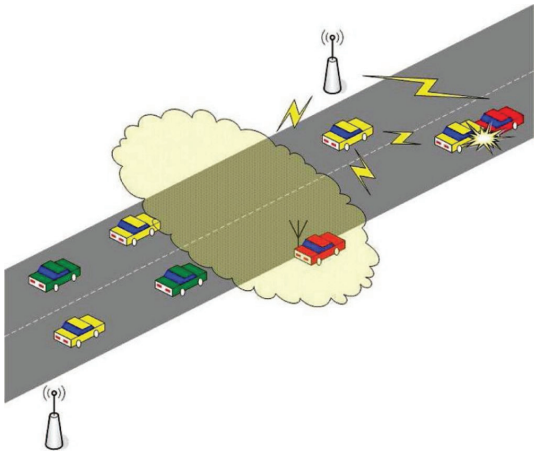

Fig. 2 Spectrum Jamming

B. Forgery

Reception of application data on time and its correctness is a major vulnerability. Fig. 3 illustrates how fast the coverage area of a network can be contaminated by a single attacker by forging and transmitting false warning messages (e.g., ice formation on the pavement), which will be passed to all vehicles in all the traffic streams.

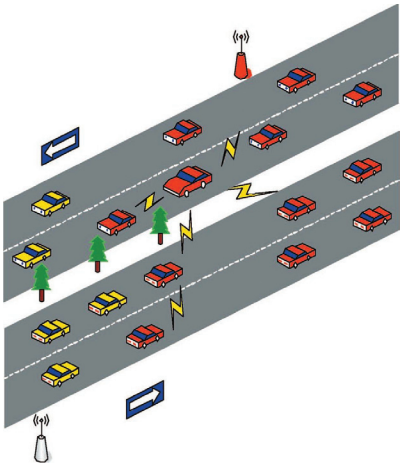

Fig. 3 Message Forgery

C. In-Transit Traffic Tampering

The relay nodes can alter the communication by dropping the messages or by corrupting or by modifying the message meaningfully. So adversaries can manipulate the safety or notification messages in the network. Replay messages can also be done by the attackers. In fact, tampering with in-transit messages may be simpler and more powerful than forgery attacks.

D. Impersonation

Impersonation can be used in message fabrication, modification and while replay attack as well. It is not the primary factor to identify the source of messages. Mainly because the content and the message features is of prime importance rather than its source. An impersonator can be taken as a threat, for example, in order to slow down other vehicles an adversary can masquerade as an emergency vehicle.

E. Privacy Violation

Deployment of vehicular networks made the task of collecting the information specific to a vehicle all easy by overhearing vehicular communication. But then, a concern of privacy preservation is violated since we can infer drivers' personal data easily. In network traffic like safety and traffic related messages, or some control messages, or in transaction-based communications, the messages need to have information like time, vehicle identifier etc. which can be used to identify the source and thereby driver or vehicle details. Control messages include over-the-air registration with local highway authorities etc. Transaction-based communications include automated payments, car diagnostics etc.

III. Overview on Security Characteristic in Warning Message Dissemination

A.Authentication

In a vehicular network, we would like to bind each driver to a single identity to prevent Sybil [6] or other spoong attacks. A congested road scenario can be created by a single vehicle by claiming to be hundreds of vehicles, these needs to be dealt by congestion avoidance scheme. In order to prevent attacks on vehicular networks, we can enforce strong authentication which leads to valuable forensic evidence as well [22].

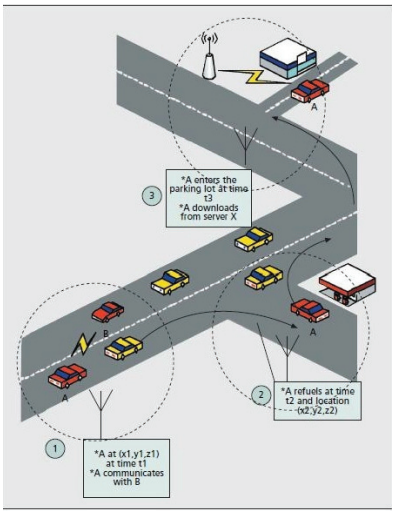

Fig. 4 Privacy Violation

B. Privacy

Users rely on their anonymity or privacy in the network, so a network lacking the same may not be easily adopted by the users. For instance, while preventing spoofing a vehicle's permanent identity may be revealed and this

violates privacy concern of a user. Privacy requirement and security enforcement can be balanced by codifying legal, societal and practical considerations. Privacy preserving law will differ in most countries and since main vehicle manufacturers aim on international market, there should be a system which satisfy most of these diverging laws or need to enable customization in the policies taken.

Users would not accept a system that allows tracking their movements by other vehicles. However, the idea of complete anonymity is practically not feasible now, as for each vehicle there will be a publicly displayed license plate which reveals a tracking a scheme. So a portion of privacy is already being compromised now in the system.

C. Data Integrity

The intended recipients should receive the original data or messages being sent rather than tampered or changed messages by any unauthorized personnel in between. This requirement is crucial when it comes to road safety applications where we cannot afford an integrity violation.

D. Non-Repudiation

Non-Repudiation ensures that vehicles in Vehicular Ad-Hoc Network (VANET) when sending or receiving data-packets should not be able to deny their responsibilities of those actions. This requirement is essential especially when disputes are investigated to determine the entity which misbehaved.

IV. Security and Privacy

Among the major concerns in Vehicular Ad-Hoc Network (VANET) communication, security and privacy protection holds the prime importance. Highly mobile and infrastructure less nature of Inter Vehicular Communication (IVC) makes satisfactory security and privacy solutions to be greatly challenging. Identifying the right level of protection is crucial for security and privacy enforcement. If we enforce too much security then it may adversely affect the system and reduce the benefits in general.

If the security or privacy protection provided is too low, then it will likely result in a reduced trust IVC systems by the driver and might thus severely damage deployment scenario. At the same time, from a manufacturer's point of view, cost also plays a very important role.

In [16] a discussion on the current status of security mechanisms and a study on whether it is ready and sufficient enough for an initial IVC deployment has been carried out. An overview map which is shown in Fig 5 is the outcome of the discussion. If there a number of proposals available and if a general agreement among researchers and standardization bodies is established, those topics are marked in green. These mechanisms need to be included for a first deployment of IVC security and privacy. Yellow indicates topics where there is a large variety of proposed security or privacy protection mechanisms in the literature but where a consensus on how to solve this problem is not yet reached. Topics in red color indicate issues that are still unsolved and where only few works are available so far.

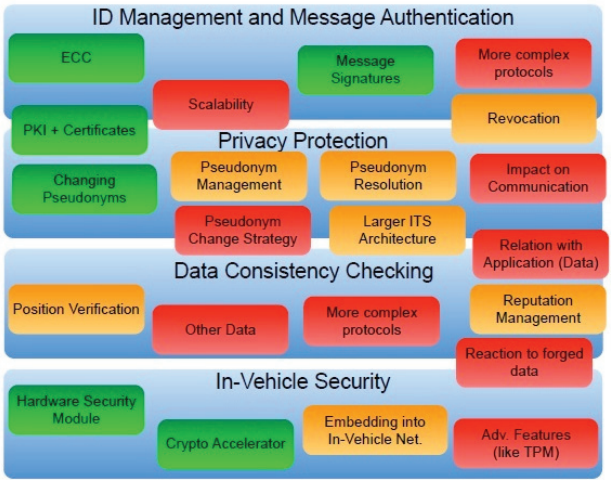

Fig. 5 Research Topics in IVC Security and Privacy

n fact there is no complete solution and agreement in all matters. The big challenge will be to find a right trade-off between strong security and privacy protection on one hand and efficiency and low overhead on the other hand. If researchers and developers fail in either direction, it will inevitably lead to problems with either vulnerable or inefficient and unusable systems.

V. Security Schemes and Concepts

A literature review for the security of Vehicular Ad-Hoc Networks (VANETs) and different classifications used to overcome security challenges are being presented in this section.

A. Symmetric Key System

In symmetric key system, only after sharing and agreeing on a secret key nodes can communicate by sending communication messages. As VANETs are an emerging research area, security aspects are still rising as an important topic. But more attention is directed towards Public Key and Identity Based systems.

A hybrid system which uses both Symmetric and Public Key operations to provide security for VANETs is proposed in [20]. The system provides authentication, confidentiality and privacy preservation. There are two types of communication being considered, pair-wise and group communication. Pair-wise communication occurs when two nodes exchange messages, whereas group communication is involved when more than two nodes needs to be communicated between each other. In order to avoid overhead of using a key pair, they propose symmetric keys for pair-wise communication. But for authentication process it is being mentioned that, symmetric keys should not be used as it might prevent non-repudiation. With a key size of 1024 bits they suggest Advanced Encryption Standard (AES) for the encryption process to make the system secure.

Symmetric key system poses several advantages like being simple, fast, usage, and usage of fewer resources and pre- vents widespread message security compromise. The system is considered to be simple as users just have to specify and share the secret key and can immediately begin to encrypt and decrypt messages. Compared to asymmetric encryption, the speed of the encryption and decryption process is fast and also resource usage is very less. A different secret key is used for communication with every different party. So even if a key is compromised, only the messages between a particular pair of sender and receiver are affected. Communications with other people are still secure.

The disadvantages like the need for a secure channel for secret key exchange, requirement of too many keys and most importantly the origin and authenticity of message cannot be guaranteed makes symmetric key system almost obsolete now. Sharing the secret key in the beginning is a problem in symmetric key encryption. It has to be exchanged in a way that ensures the secrecy of the key. In Vehicular Networks as the topology changes dynamically and the system as a whole is a lot more vulnerable than other system, providing a secure channel leads to a tough requirement [25]. Also a new shared key has to be generated for communication with every different node. This creates a problem with managing and ensuring the security of all these keys. Storage will be challenging for vehicles. As both sender and receiver use the same key for communication, messages cannot be verified to have come from a particular user. This will be a problem if there is a dispute and violates the non-repudiation requirement in safety notification.

When symmetric cryptography has been chosen by a VANET designer key distribution can be done either while manufacturing process or through adhoc mechanisms. Since vehicles have their dynamic nature of having new ones being added up and a need to remove old vehicles from the system, loading keys while manufacturing is not a feasible solution. Relying on ad hoc mechanisms for key distribution without an online trusted third party will introduce security concerns. So in [26] it is concluded to depend on asymmetric cryptography for binding beacon information to vehicles.

B. Public Key System

Prior to the introduction of ID-based (Identity-based) systems, Public key scheme was the most popular scheme for securing Vehicular Ad-Hoc Network (VANET) communication. Basically in Public Key System, each node will be assigned with a pair of keys: a secret key and a public key. By using these keys, nodes are allowed to communicate with each other. However to handle key management operations, a Public Key Infrastructure (PKI) is mandatory.

In [10] public key cryptography is proposed in VANETs in order to allow authorities and vehicles to certify the identities of vehicle. Desirable privacy protocols have also been suggested to preserve drivers' personal information. Solutions for some types of attacks like impersonation are also proposed in it. The problem of location verification is also addressed in the paper. It claims that the usage of GPS-based systems has more weaknesses than strengths and so the uses of distance bounding protocols are proposed for the same.

In [7] another new architecture is proposed on public key cryptosystem which claims to provide authentication, authorization and accountability. They use a practical Public Key Infrastructure (PKI) along with public key cryptography as symmetric key system doesn't provide accountability. Authentication is achieved using digital signatures, and as Elliptic Curve Cryptography reduces the processing requirements they propose that in the article.

C. Privacy Preservation Using Pseudonyms

In [7] a set of anonymous keys are being used for preserving privacy. These keys will be saved in Tamper Proof Device (TPD) and have short life-times. After using a particular key, it will be marked as void so that it cannot be used again. All the key management and distribution is done by the Certificate Authority (CA). The keys being used are traceable only once there are some emergency requirements like a dispute scenario.

A common drawback of using pseudonyms for privacy preservation is the limitation of the pseudonym selection. However, self-generation of pseudonyms comes, at a higher transmission and processing cost. Also it alleviates one of the most significant limitations of the pseudonym-based approach: the need for complex management.

Conditional privacy preservation is being addressed in [15]. So here privacy preservation is made conditional to en- sure senders' personal information protection from recipients. However authorities can still be able to get all the information in case of disputes. It is pointed out here that pseudonym-base approaches are not suitable as it leads to massive searching for the CA in the databases. Schemes like Group Signature and Identity-based Signature (GSIS) is being explained in the article. Short-group signatures are being used for IVC and Identity-Based Signature is being used for communication between vehicles and RSUs. GSIS prevents RSU replication attack, where in a compromised RSU is being relocated to misuse the network and for spreading malicious data.

D. Identity-Based Cryptography

Relative to the properties VANETs possess, IDBC has be- come the mainstream for security framework being used. Earlier Public Key Cryptography (PKC) and/or Symmetric Key Cryptography (SKC) were used for assuring security. Later on, researches made it clear that such schemes are not the best choice for VANET security when relating to its unique characteristics.

When comparison is done between Identity-Based Cryptography (IDBC) and Public key Cryptography [27], once the authentication job is done, the only work a Trusted Third Party (TTP) has is to generate private keys for users. So it does not hold on to any records which binds keys and users relaxing the overhead on the TTP.

Public Key Infrastructure requirement of the Public Key Systems for managing all key operations puts extra burden on the TTP [19] .The infrastructure less nature of VANETs got matched up by eliminating PKI in IDBC. The security activities like encryption, decryption, signing and verifying are all done by the nodes rather imposing it on the TTP. So communication delays are reduced considerably in Identity Based System [17]. As the bandwidth is limited in dynamic wireless environments, key size and certificate size will impose a constraint in the use of PKC.

In IDBC a unique arbitrary string is taken as the public key (like license plate number) so the processing delays in Symmetric Key Systems is avoided effectively. In SKC, the nodes should agree on a shared key for every new communication and it leads to an extensive processing requirements. Considering the dynamicity of the VANET system, SKC is ruled out on the requirement of generating a new key whenever nodes leave/join the group [17]. So eventually SKC is considered to be a bad choice since real-time responses are expected in VANETs and thereby delays cannot be tolerated which makes the use of SKC obsolete in the system. IDBC is considered to be a suitable choice in order to ensure security in vehicular networks as it complied with a large extent to the characteristics of the system.

1. Identity-Based Signature

Identity-based signature is used for secure communication without using public and private key pair [1]. Basically Identity-Based Cryptography (IDBC) is relying on public key cryptosystem. The difference is, rather than generating a key pair, an arbitrary string which uniquely identifies the user is being used as the user's public key and private

key will be generated by a Trusted Third Party (TTP) [1]. However in [1] only Identity-Based Signature was proposed not an encryption scheme.

Even if IDBC is relied on public key cryptosystem, Identity-Based Encryption (IBE) needs two additional requirements, they are: the computation of private keys from a random seed and made it easy and it should be intractable to compute the seed when a public/private key pair is known. Since RSA was being used as the public key cryptosystem [1], it failed to satisfy the extra requirements and it remained as an open problem.

2. Identity-Based Encryption

The open problem with Identity-Based Encryption (IBE) was solved by Boneh and Franklin [3] by Weil Pairing based scheme [12]. The intractability of the Elliptic Curve Discrete Logarithm Problem (ECDLP) is the strength of their proposed scheme. The encryption process in Fig. 6 is performed in 4 steps: [9].

- **Setup:** Master secret key and public key will be generated by Trusted Third Party (TTP) and the public key is distributed to all the users in the network.
- **Extraction:** Upon authentication of a recipient to the TTP it requests for the private key. The private key is generated by the Trusted Third Party (TTP) and provided to the requested recipient.
- **Encryption:** Receivers public key and Trusted Third Party's (TTP) public key is being used by the sender to encrypt the message before sending it.
- **Decryption:** Receiver can decrypt the received message using its private key to retrieve the original message.

3. Identity-Based Approaches

Identity-Based Cryptography (IDBC) has been used for VANET security by quite a few researchers. In [14], the proposed framework achieves privacy and non-repudiation together with basic security features by using an ID-based approach. Privacy preservation has given highlight in it since it attracts vehicles to join the network.

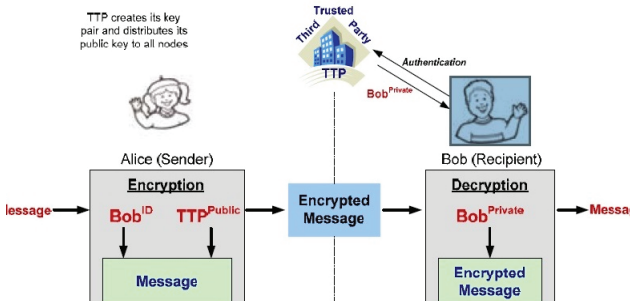

Fig. 6 Identity-Based Encryption

It also provides justification for the failure of previous solutions not to fit in Vehicular Ad-Hoc Network (VANET) because of the unconditional privacy they provide. Identity of vehicles should not be revealed in all circumstances in VANETs. This is fixed by [14] by providing distributed control so as a single authority will not be able to reveal the personal information. Rather than that, multiple authorities can collectively process when identity needs to be revealed.

In [13] another IDBC is proposed for making VANET secure. Highlight in the paper is mainly on the importance of mutual authentication between nodes and the relevance on keeping the identity of nodes from being exposed. The paper specifies the reasons by which IDBC outperforms other traditional cryptographic techniques for the use in VANET scenarios.

VI. Conclusion

Security enforcement is an emerging area of research in Vehicular Ad-Hoc Network (VANET) deployment in order to make the system more reliable and welcoming for the users/vehicles. So the paper starts with the vulnerabilities that Vehicular Network is susceptible to focusing from a Warning Message Dissemination (WMD) perspective. By being more aware on the various attacks or weaknesses we can make the system more strong indeed. Also in this paper unique characteristics that need to be ensured for the effectiveness of WMD are also considered and familiarized. Different security schemes and concepts for countering vulnerabilities and enforcing characteristics are being surveyed and finally a detailed study on the current most viable choice of security mechanism, which is Identity Based Cryptosystem, is carried out, after refreshing both Symmetric Key Cryptosystem (SKC) and Public Key Cryptosystem (PKC).

References

[1] A. Shamir., "Identity-based cryptosystems and signature schemes," Proceedings of Advances in Cryptography-Crypto 84, LNCS, Vol. 196, Springer-Verlag, pp. 47-53, 1984.

[2] H. Kawashima, "Japanese perspective of driver information systems." Transportation 17, pp. 263-284., 1990.

[3] D. Boneh, M. Franklin, "Identity-based encryption from the Weil pairing," Proceedings of Crypto 2001, LNCS, Vol. 2139, pp. 213-229, Springer-Verlag, 2001.

[4] L. Gollan, C. Meinel, "Digital signatures for automobiles, in:Proceedings of Systemics," *Cybernetics and Informatics* (SCI)02, 2002.

[5] M. Zarki, S.Mehrotra, G. Tsudik, N. Venkatasubramanianm, "Security issues in a future vehicular network," in: Proceedings of European Wireless02, 2002.

[6] R. John,R. Douceur, "The Sybil attack," In First International Workshop on Peer-to-Peer Systems (IPTPS), March 2002.

[7] M.Raya, P. Papadimitratos, J. Pierre Hubaux, "Securing Vehicular Communications," Laboratory for computer Communications and Applications (LCA), Switzerland, 2004

[8] J. Blum,A. Eskandarian, "The threat of intelligent collisions," IT Professionals (1), 2429,2004.

[9] J. Baek, J. Newmarch, R. Safavi-Naini, W. Susilo, "A survey of identity-based Cryptography," Proceedings of Australian Unix Users Group Annual Conference, 2004

[10] J. Hubaux, S. Capkun, J. Luo, "The security and privacy of smart vehicles," *IEEE security and Privacy,* Vol. 2, No. 3, pp. 49-55, 2004.

[11] M. Raya, J.P. Hubaux, "The security of vehicular ad hoc networks", in:Proceedings of SASN05, pp. 1121, 2005.

[12] D. R. Stinson, "Cryptography Theory and Practice," 3rd ed., Chapman and Hall/CRC, USA., 2005.

[13] P. Kamat, A. Baliga, W. Trappe, "An Identity-Based security framework for VANTEs," Proceedings of 3rd Int. Workshop on Vehicular Ad-Hoc Networks, pp. 94-95, 2006.

[14] J. Sun, C. Zhang, Y. Fang, "An ID-based framework achieving privacy and non-repudiation in vehicular ad hoc networks," Proceedings of the IEEE Military Communication Conference-MILCOM2007, pp.1-7, 2007.

[15] X. Lin, R. Lu, C. Zhang, H. Zhu, P. Ho, X. Shen, "Security in vehicular ad hoc networks," *IEEE Communications Magazine,* Vol. 46, No. 4, pp. 88-95, 2008.

[16] F. Dressler, F. Kargly, J. Ottz, O. K. Tonguzx, L. Wischh, "Research Challenges in Inter-Vehicular Communication," Lessons of the 2010 Dagstuhl Seminar, Institute of Computer Science, University of Innsbruck, Austria, 2010.

[17] C. Y. Yeun, M. Al-Qutayri, F. Al-Hawi, "Efficient Security Implementation for Emerging VANETs", *Khalifa University of Science Technology and Research,* UAE.

[18] G. Ferrari, S. Busanelli, N. Lotti, Y. Kaplan, "Cross-Network Information Dissemination in VANETs,"11th International Conference on ITS Telecommunications, pp. 351-356, 2011.

[19] X.509: Information technology Open Systems Interconnection, "The Directory: Public-key and attribute certification frameworks", ITU-T, August 2005.

[20] E. Magkos, V. Chrissikopoulos, M. Burmester, "Secure and Privacy-Preserving, Timed Vehicular Communications," Department of Computer Science, Florida State University, Tallahassee, FL 32306-4530, U.S.A.

[21] C.F. Chiasseriniy, E. Fasoloz, R. Furiatoz, R. Gaetax,M. Garettoy, M. Gribaudox, M. Serenox, A. Zanellaz,"Smart Broadcast of Warning Messages in Vehicular Ad Hoc Networks".

[22] B. Parno, A. Perrig, "Challenges in Securing Vehicular Networks", Carnegie Mellon University.

[23] R. Lu, "Security and Privacy Preservation in Vehicular Social Networks", A thesis presented to the University of Waterloo, Ontario, Canada, 2012.

[24] M. Al-Qutayri, C. Yeun, F. F. Al-Hawi, "Security and Privacy of Intelligent VANETs", Khalifa University of Science and Technology, UAE.

[25] P. Sasikumar, C. Vivek, P. Jayakrishnan, "Key-Management Systems in VANETs", *International Journal of Computer Applications* (975-8887), November 2010.

[26] J. Haas, Y.C. Hul, P. K. Laberteaux, "The impact of key assigent on VANET privacy", *Security Comm. Networks.* 2009.

[27] R.L. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communication of the ACM,* Vol. 21, pp. 120-126, 1978.