IJCSN International Journal of Computer Science and Network, Volume 3, Issue 5, October 2014
ISSN (Online) : 2277-5420 www.IJCSN.org
**Impact Factor: 0.274**



# A Survey on Security and Privacy Approaches of Intelligent Vehicular Ad-Hoc Network (InVANET)

**[1] V. N. Sahare, [2] Dr. M. V. Sarode, [3] N. S. Sahare**

Research Scholar, Computer Science & Engineering, GHRCE
Nagpur, Maharashtra, India

**Abstract** - In last few years, Vehicular Ad-Hoc Network (VANET) becomes increasingly popular in many countries. It is an important element of the Intelligent Transportation Systems (ITSs). In a typical VANET, each vehicle is assumed to have an on-board unit (OBU) and there are road-side unit (RSU) installed along the roads. A trusted authority (TA) and application servers could be installed in the backend. As wireless ad-hoc network is also the base technology of Intelligent Vehicular Ad-Hoc Network (InVANET) as that of VANET, almost there is no specific protocol implemented which owing good security strategy. As we know, reason of this issue is most of wireless ad-hoc protocols has suffered from energy consumption problem and the protocols have to focus on reducing resource consumption. Although, it seems InVANET has better situation because energy has not critical position as its predecessor. But security has critical situation in InVANET similar to ad-hoc. Using InVANET is increasing and security architecture must be carefully designed especially when it becomes a worldwide InVANET which give service millions of vehicles in the roads. In this paper we are presenting a survey over security and privacy challenges for InVANET and different approaches used to provide security.

**Keywords -** *InVANET, VANET, Attacks, Security, Privacy, ECC, Identity based Cryptography.*

## 1. Introduction

Now days, for facilitating road safety, traffic management, and infotainment dissemination for drivers and passengers Vehicular Ad-Hoc Network provides a promising network scenario. In VANETs, onboard units (OBUs) frequently broadcast routine traffic-related messages [1] with information about position, current time, direction, speed, acceleration/deceleration, traffic events, etc. By being equipped with communication devices, vehicles can communicate with each other as well as with the roadside units (RSUs) located at critical points of the road, such as intersections or construction sites. As VANETs frequently broadcast and receive traffic-related messages, drivers can get a better awareness of their driving environment. In this way driver can take alternate route and avoid the traffic or abnormal situation in advance. In addition, with a VANET connected with the backbone Internet, local information such as road maps and hotel information can be accessed, passengers sitting in vehicles can go online to enjoy various entertainment-related Internet services with their laptops downloading/uploading data information from the Internet [2]. Before putting the above attractive applications into practice in VANETs, we must resolve security and privacy issues. Particularly, we must guarantee message authenticity and integrity. Moreover, we have to protect user-related privacy information, such as the driver's name, license plate, model, and traveling route.

Although previous studies have addressed the aforementioned issues, they have not taken the scalability and communication overhead into consideration. The basic idea of the previous security schemes for VANETs is to sign each message before sending it and verify each message when receiving it. According to the Dedicated Short-Range Communication (DSRC) protocol [3][8], a vehicle sends each message within a time interval of 100–300 ms. Generating a signature every 100 ms is not an issue for any current signature technique. However, in a high-density traffic scenario, e.g., if 50–200 vehicles are within the communication range, the receiver needs to verify around 500–2000 messages/s, which will lead to a high computation burden to the receivers. Furthermore, traditional public key infrastructure (PKI)-based security schemes require the public key of the sender and the corresponding certificate to be included in the messages. The security overhead is usually bigger than the useful message contents. This issue has to be well addressed due to the limited wireless channel bandwidth available in VANETs.

VANETs are expected to offer tremendous benefits. However, such networks have a number of novel problems that need to be resolved before they get implemented in a practical setting and people have the confidence to use them. Most of the problems are associated with the security and privacy of VANETs. The major challenges to solve these problems are due to the infrastructureless and high dynamic nature of VANETs. A lot of effort has been put recently to resolve these issues in an efficient and robust manner. This paper discusses the security and privacy challenges associated with intelligent VANETs, along with some possible solutions. Next, InVANET security threats and challenges are described. Then possible InVANET security schemes and their underlying concepts.

## 2. Intelligent VANET Concept

Based on the fundamental concepts of WANETs, many other categories have emerged. The most common are: wireless mesh networks, wireless sensor networks and Mobile Ad-hoc Networks (MANETs). The former two categories proved to be useful and are used in some fields like mobile devices' communication and weather monitoring, respectively. Whereas MANETs are those networks that offer high levels of mobility for users and take many forms. One of the most useful forms of MANETs is VANETs, which are also considered the first commercial application of MANETs. InVANET, or Intelligent Vehicular Ad-Hoc Networking, defines an intelligent way of using Vehicular Networking. InVANET integrates on multiple ad-hoc networking technologies such as Wi-Fi IEEE 802.11p, WAVE IEEE 1609, WiMAX IEEE 802.16, Bluetooth, IRA, for easy, accurate, effective and simple communication between vehicles on dynamic mobility. Figure 1 shows the hierarchy of Ad-Hoc networks.

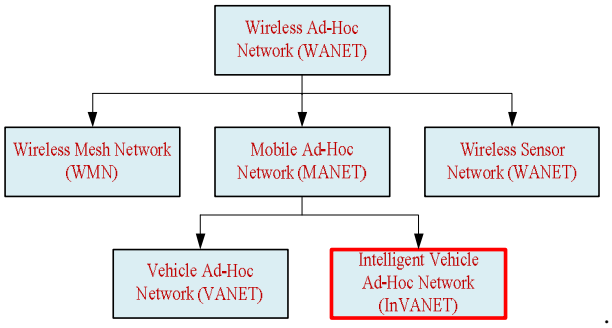


Figure1. Hierarchy of Ad-Hoc Networks

There are security issues in data integrity, privacy, and confidentiality that inherited from the Ad-hoc. In addition of these issues, there are some issues which can impact performance of InVANET such as unpredictable temporary situation (e.g. existence of traffic jam because of an accident). The security of Intelligent VANET is one of the most critical issues because of their transmission information is propagate in open access environments [4]. It is important that all transmitted data cannot be eavesdropped or changed by malicious users. Moreover, the system must be able to detect these malicious users in addition of there is a problem which is legitimate users who do not emphasize their privacy.

It seems these problems in InVANET are difficult to solve because of speed of the vehicles, the randomness of the connectivity between them, increasing network size, and their geographic position [5] [6]. For that purpose there should be direct communication between vehicles to avoid delay, RSU security etc. This type of approach shown in figure 2 where v2v communication overcomes above issues.

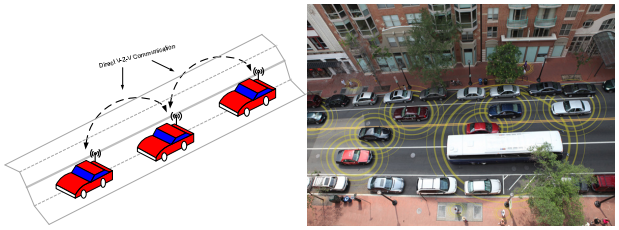

Figure 2. InVANET Direct Vehicle-to vehicle communication

## 3. Security Threats and Challenges

There are various types of security attacks and network adversaries that can pose a threat for Intelligent VANETs. Also we will discuss major security and privacy challenges which it can face. Just like any other wireless network, there are many different catastrophic attacks that can occur in a VANET as well as in InVANET. Before we classify these attacks, it is good to know what exacly the adversary means. A node is considered 'adversary' if it attempts to inject any type of misbehavior in the network that might cause other nodes (i.e. victims), and ultimately the network, to function improperly.

### 3.1 Attacks and Threats

As in other communication networks, there are numerous attacks that can disturb the security of the VANET and the privacy of its nodes.

Each type of attack affects some of the security services in the system; termed 'CIA' which stands for

Confidentiality, Integrity, and Accountability, and Availability. In general, attacks fall into 4 categories as shown in Table 1.

Table 1. Categories of Attacks

| **Type of Attack** | **Definition** | **Affected Characteristic** |
|---|---|---|
| Access | An attempt to obtain unauthorized info. | Confidentiality; because info is exposed to unauthorized parties. |
| Modi-fication | An attempt to alter and change information that is unauthorized to change. | Integrity; because correctness of information is compromised. |
| Denial of Service | An attempt to deny usage or access of information for legitimate users. | Availability ; because the services of a network might not be available for users |
| Repu-diation | An attempt to give incorrect information or deny the occurrence of events. | Accountability; because information is no longer liable. |

Below is a listing of the most common and catastrophic forms of attacks that an InVANET can suffer:

- Denial of Service (DoS): a very simple, but yet lethal attack. In this attack a node might continuously send unwanted data across the network so that it enters a grid-lock state where other nodes are unable to communicate due to channel blocking. This attack can either deny access to information or applications or even the whole VANET.
- Interception: where a node plays the 'man-in-the-middle' role so that information exchanged between two nodes passes by the adversary node. Hence, it gains information that is intended to other destinations.
- Fabrication: where attackers send incorrect information to other nodes for different purposes. For example, a node sending false data about traffic conditions in certain roads. These types of attacks can be very dangerous because they affect the validity of the data received by nodes.
- Impersonation: attackers can pretend to be what they are not in order to gain access to certain information or to aid other attacks by pretending to be a vehicle when in fact it is a stationary adversary.
- Alteration & suppression of data: in these types of attacks, adversary nodes can receive valid data, alter it and resend it to other nodes. Moreover, an adversary can prevent communication between two nodes by dropping certain messages between them. These attacks cause false data and confusion to be distributed among the network nodes and hence it affects performance.
- The Sybil attack: a malicious node attempts to make other nodes [7], which in turn, make other nodes malicious and hence control significant portions of the network and misuse it. This attack is as dangerous as DoS attacks because it can destroy valid communication in the network.

## 3.2 Security and Privacy Challenges

One of the major challenges of securing VANETs is *communication security*. This means secure communication between vehicle to vehicle and vehicle to RSU, i.e. V2V and V2R. For designing security framework the basic security services that are provided in VANETs include: prevention of unauthorized access to information i.e. information confidentiality. Also, in order to detect and prevent malicious intent such as information alteration integrity of exchanged messages must be provided.

Additionally, to prevent impersonation node authentication is important to ensure that all nodes within the network are who they claim to be. Other services include: availability of network services for all users at all times and accountability which aims to associate events with particular nodes for future references in order to prevent attempts to provide false claims or reject true ones. To achieve security in InVANETs various schemes has been used such as encryption and digital signatures as part of cryptography primitives to provide security services discussed above (i.e. confidentiality, integrity, authentication, etc.) in intelligent vehicular networks.

*key management* is another salient challenge that faces the security of InVANETs. To encrypt and decrypt information the key in the security domain is used which

is nothing but the number sequence. While designing security protocols for such networks; various issues of key management must be resolved which has many categories. key revocation is one category which is the process of discarding suspected keys. Traditional methods of revocation such as Certificate Revocation Lists (CRLs) [8] are not suitable for InVANETs due to the large scale of the network. A second category of this challenge is group key management since InVANETs inherit the characteristic of mobility from MANETs.

Furthermore, *detection of malicious nodes and intentions* is considered the most challenging issue in InVANETs so far. The reason for that is because it is easy to access data in the network and hence data validity is compromised. Consequently, it becomes much more difficult to distinguish valid data from malicious data. What makes this even worse is that in Intelligent VANETs there are no guarantees that previously honest nodes do not turn to malicious nodes in the future. Furthermore, in such networks it became desired to prevent the attack before it occurs which really calls for strong security algorithms.

*Location verification* is another challenge for InVANET security. Currently in VANETs, position coordinates can be verified using either a GPS unit [9], a RSU, or via inter-vehicle communication (IVC). All of these methods are considered weak since an attacker can easily fool a GPS unit or manipulate RSUs or even forge data via IVC. Position verification plays a vital role to prevent many attacks like impersonation. It also helps in the data validation process. Therefore, a solid method to verify nodes positions' is required to help improving the security of InVANETs.

These two challenges are quite significant because they intervene with the privacy of the node, i.e. drivers are not willing to reveal their routes and driving habits to be exposed by others. Consequently, they lead to another major challenge in securing InVANETs which is *privacy preservation*.

The privacy issue is concerned with protecting personal information of drivers (name, location, plate number, etc.) within the network. The design of network protocol should hide this information from other nodes; but it should allow information to be extracted in case of accidents. Hence, rather than achieving unconditional privacy which is a major challenge, conditional privacy is desirable for InVANETs. Moreover, the tradeoff between robustness measures, such as the inclusion of personal information during communication which makes the task of malicious node detection easier, and the protection of drivers' information makes the issues of privacy more challenging. The *trade-off between robustness and the level of privacy* a protocol grants is also a key challenge facing InVANETs. Any proposed security algorithm must take into consideration the impact on the users and how well will the public accept it because their privacy is involved in such matters.

This becomes a problem when an algorithm mainly depends on personal data as unique identifiers, in order to be robust enough, that can be traced back to a specific user. For example, the public might consider it intrusive if the algorithm requires the use and exposure of their biometric data. Hence, proposing a security protocol that is robust enough to secure Intelligent VANETs communication, yet be well-accepted by the public is still an open problem.

Other challenges facing InVANETs include *time sensitivity* and *network scale*. The time required to process information in such networks is vital because as mentioned previously, nodes are only within the communication range for short period of time. This forces communication methods to be of real-time processing nature because nodes need to exchange, verify and prevent attacks as they are travelling at high speeds.

So, we need security methods that take this issue into consideration. It is also clear how the issue of network scale can turn to a challenge when talking about such dense networks as VANETs. Huge number of vehicle, of different origins and manufactures, makes it really difficult to manage communication and security in the network [10].

Vehicular communication network that is able to resist malicious activities and attacks and provide the highest possible level of node privacy is the main goal of Intelligent VANET security protocols. Because of some of the unique features of VANETs such as the high mobility and the large network scale it is very challenging design protocols that will provide secure communication and prevent many types of security attacks, as well as protect all personal information of drivers.

## 4. Security Schemes and Concepts

This section presents a literature review for the security of Intelligent VANETs and classifies the approaches used to overcome security challenges. Then it explains in details important cryptographic concepts that are related to security schemes.

## 4.1 Symmetric Key Approaches

To secure the information, Symmetric Key systems were the first type of cryptosystems which are used. In these systems, nodes can only communicate after sharing and agreeing on a secret key [11] that is used to process communication messages. As stated previously, InVANETs are a relatively new research area and the security for such networks is only starting to be a major research topic. Nevertheless, this section discusses existing proposals of using Symmetric Key systems for InVANET security.

In [12] a hybrid system that uses both Symmetric and Public Key operations is proposed to provide security for Vehicular Communication. The hybrid system provides authentication, confidentiality and privacy preservation. To achieve this it defines two types of communication within InVANETs: pair-wise and group communication.

The former type occurs when two nodes require exchanging messages, whereas the latter is established when more than two nodes require communication. They propose the use of symmetric keys when pair-wise communication occurs in order to avoid introducing overhead of using a key pair (i.e. public key systems). However, they point out that symmetric keys should not be used in the authentication process since it might prevent non-repudiation.

## 4.2 Public Key Approaches

Public key schemes were most widely used prior to the introduction of ID-based ones. In Public Key frameworks, each node is granted a pair of keys: a secret key and a public key. These are used in security operations when communicating with other nodes. Is it very important to note that in order to implement this framework; a Public Key Infrastructure (PKI) is required to handle key management operations. Based on such frameworks, the security protocol can also offer desirable features such as certificate revocation and privacy of nodes. Related works in these two fields are discussed in this section.

In [12] security and privacy issues in vehicular communication are addressed. They specified privacy concerns for different methods of tracking vehicles used by authorities. In order to allow authorities and vehicles to certify identities of other vehicles they proposed the use of public key cryptography in vehicular communication. To preserve drivers' personal information, a desirable privacy protocol they have suggested. Solutions are also proposed for some types of attacks like impersonation. In [10], another new architecture is proposed where vehicles equipped with two extra hardware units; the Event Data Recorder (EDR) to record all events and the Tamper-Proof Hardware (TPH) that is capable of performing cryptographic processing. The proposed architecture provides authentication, authorization and accountability. They suggest the use of public key cryptography with a manageable and robust PKI since symmetric key cryptography do not support accountability.

Authentication is performed by digital signatures of communicated messages; they proposed the use of Elliptic Curve Cryptography (ECC) since it reduces the processing requirements.

### 4.2.1 Certificate Revocation

In [10], security architecture for vehicular communication that aims to provide security services for such networks is proposed. They highlight the salient challenges facing vehicular networks such as: the network scale, the privacy issues and the real-time requirements. They also describe the types of security threats and attacks that such network are susceptible to such as: impersonation, information forgery and tempering with traffic.

They also proposed a novel certificate revocation technique through three protocols: the Revocation protocol of Tamper-Proof Device (RTPD) [11], Distributed Revocation Protocol (DRP) and Revocation protocol using Compressed Certificate Revocation Lists (RCCRL). These protocols are introduced since they argue that standard methods of revocation such as Certificate Revocation Lists (CRLs) causes substantial amount of overhead and requires pervasive infrastructure.

Furthermore, [13] discussed the current standards for providing security in vehicular communication. They described how the IEEE 1609 WAVE standards (i.e. DSRC) support security for V2V Communication and V2R communication. The IEEE 1609.2 standard provides security measures that require the use of public key cryptography with ECC support for some applications. However, drivers' privacy preservation issues are not addressed in these standards.

The articles explains the disadvantages that prevent such methods of being suitable for vehicular environments; such as the network scale which is substantial in VANETs and causes the CRL to grow rapidly and hence increase processing requirements when revocation is required. Furthermore, it is highlighted the CRL are considered centralized approaches which do not suit VANETs because of the property of high mobility.

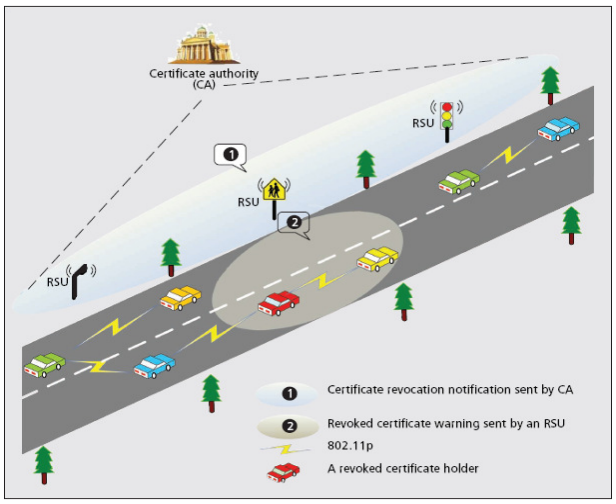


Figure 3. RSU-aided certificate revocation.

A novel certificate revocation scheme as shown in figure 3 termed RSU-aided Certificate Revocation (RCR) is proposed by [13]. In this method, to sign all messages communicated within its range the TTP grants secret keys for each RSU. In order to revoke the particular certificate and stop all communication with node whose certificate is detected to be invalid; the Certification Authority issues a warning message to all RSUs which broadcast messages to all vehicles in respective ranges.

### 4.2.2 Pseudonym Based Approaches for Privacy

In [14] [10], by using a set of anonymous keys an approach for privacy preservation is proposed, which have short life-times, that is in advance stored in the Tamper-Proof-Device for a certain amount of time. Once a key is used it is declared void and cannot be used again and all key distribution and management is performed by the CA of the network. However, the stress is on the point that these keys have to be traceable to the driver only in case of emergencies.

In [15] [13] the 'conditional' privacy preservation in VANETs is addressed. This is a desirable characteristic for VANET because it ensures that recipients are not able to extract senders' personal information; however, authorities are able to do so in cases of accidents or network misuse. They pointed why the pseudonym-based approaches are not suitable for vehicular communication because at each process of revocation, a large database has to be searched by CA. At this point if network scale grows larger, then it is very difficult to manage CRL. They explain the previously proposed scheme for conditional privacy in [16]; the Group Signature and Identity-based Signature (GSIS).

The scheme categorizes the process into two groups: On Board Units (OBS) to OBU and RSU to OBU; which ultimately refers to IVC and RVC. The first group uses short-group signature schemes to ensure the anonymity of communicating nodes, and IBS are used in the second group where all RSU messages are signed and the overall cryptographic overhead is reduced since it is an identity-based approach. A 'RSU replication attack' in which a compromised RSU is relocated in order to misuse the network and spread malicious data, such type of things can also be prevented by GSIS.

### 4.3 Identity-Based Cryptography

Recently, this approach became the mainstream for vehicular communication security frameworks as it is considered a viable choice due to the properties of InVANETs. As mentioned previously, earlier proposed security schemes relied on the use of public key cryptography (PKC) and/or symmetric key cryptography (SKC). However, recent researches discovered that such cryptography methods are not the 'best' choice for security in vehicular communication. One important characteristic of VANETs is that they are of infrastructure-less nature; hence the use of PKC is not suitable since it requires a Public Key Infrastructure (PKI) which deals with issues of key distribution and management. Moreover, sizes of the keys and certificates pose a constraint on the use of PKC in such networks since the bandwidth is limited in such dynamic wireless environments. Also, because vehicular communication requires real-time responses and cannot tolerate delays in communication; SKC is also not considered a good choice [17]. Therefore, IDBC is currently considered a viable choice to provide security in vehicular communication.

### 4.3.1. Identity-Based Signature

The basic idea of identity-based signature is to provide secure communication without the requirement of a public/private key pair. IDBC is based on an underlying public key cryptosystem. However, instead of generating a key pair, an arbitrary string that uniquely identifies the user can be used as his public key. The private key is then generated by a Third Trusted Party (TTP) [19] and issued to the user. As stated previously; IDBC requires an underlying public key cryptosystem, but Identity-Based Encryption (IBE) scheme requires two additional requirements: the ability of easily computing private keys from a random seed and the intractability of the process of computing this seed if a public/private key pair is known. At that time, the proposal used RSA as the underlying public key cryptosystem which did not satisfy the two

additional requirements for an IBE scheme, and hence it was an open problem.

### 4.3.2 Identity-Based Encryption

The IBE open problem was solved by Boneh and Franklin in 2001, with a fully functional scheme. The strength of the scheme they proposed was based on the intractability of the Elliptic Curve Discrete Logarithm Problem (ECDLP). The strength of the security offered by IDBC is based on four key points as stated below:

1. The strength of the underlying public key cryptosystem.
2. The level of secrecy of all information acquired and stored in the TTP.
3. The strength of the authentication methods performed prior to private key issuance.
4. The methods and precautions by which private keys are guaranteed not to be leaked.

### 4.3.3 Identity-Based Approaches

Few researchers proposed the use of IDBC for VANET security. In [10] an ID-based framework is presented to achieve privacy and non-repudiation; along with the fundamental security features, in vehicular communication. The importance of having privacy preserved in such network is highlighted as a key issue to attract vehicles to join such vehicular networks. The proposed framework includes a justification as to why previously proposed ID-based solutions to achieve privacy; such as ring signatures, do not suit VANET environments since it results in 'unconditional privacy'. The framework relies on the pseudonym-based approach to achieve non-repudiation in VANETs. This approach was introduced previously in [14] and it involves a set of short-lived keys which are in advance preloaded with vehicles that cannot be used more than one time, so that no other vehicles are able to track the particular vehicles identity. For this it is necessary to use associate random identifiers (pseudonyms) with the real identity of the vehicle, so they proposed a Pseudonym Lookup Table (PLT).

In [17] [18] another IDBC is proposed for VANET security. It stressed on the indispensability of security and privacy in VANETs in order for them to be well-accepted by the public. They point out that VANET nodes should be able to protect the identity of themselves in order to grant privacy services for that they able to mutually authenticate with other nodes. It explains why IDBC is possibly the 'best' solution to resolve intelligent VANETs security issues and why traditional cryptography techniques cannot be used in VANETs environments.

### 4.4 Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) is considered a public key approach for cryptography that is based on algebraic (Abelian) elliptic curve groups over finite fields. The ECC approach allowed many existing protocols and cryptographic schemes to use it in order to have a variant of the original protocol [19]. For example, ECC can be used to construct the Elliptic Curve Diffie-Hellman (ECDH) key agreement scheme where elliptic curves are used to agree a shared key between two parties [20][21]. As stated previously, the strength of any cryptosystem is based on a computationally infeasible problem. In the case of ECC, this computationally difficult problem is termed the Elliptic Curve Discrete Logarithm Problem (ECDLP). The source of the problem is known as the Scalar Multiplication (SM) of Elliptic Curves.

## Conclusion

Vehicular Ad-Hoc Network technology is a fertile region for attackers who will try to challenge the network with their malicious attacks as it is an emerging and promising technology. This paper gives a wide analysis for the threats and challenges, InVANET security schemes and concepts. Various cryptographic approaches are also defined for ensuring security and privacy.

## References

[1] Chenxi Zhang, Xiaodong Lin, Rongxing Lu, Pin-Han Ho and Xuemin (Sherman) Shen, "An Efficient Message Authentication Scheme for Vehicular Communication", in IEEE Transactions on Vehicular Technology, vol. 57, No. 6, November 2008.

[2] S. Lee, G. Pan, J. Park, M. Gerla, and S. Lu, "Secure incentives for commercial ad dissemination in vehicular networks," in *Proc. ACM Int. Symp. MobiHoc*, 2007, pp. 150–159.

[3] H. Oh, C. Yae, D. Ahn, and H. Cho, "5.8 GHz DSRC Packet Communication System for ITS Services," in *Proceedings of the IEEE VTC '99*, Sept. 1999, pp. 2223 – 2227.

[4] F. Sabahi, "Vehicular Ad-hoc Networks Security Analysis," Presented at International Conf. on Computer Engineering and Applications (ICCEA), 2011.

[5] Khaleel Mershad and Hassan Artail, "A Framework for Secure and Efficient Data Acquisition in Vehicular Ad Hoc Networks", IEEE Transactions On Vehicular Technology, Vol. 62, No. 2, February 2013.

[6] S. Zeadally, R. Hunt, Y. S. Chen, A. Irwin, and A. Hassan, "Vehicular Ad Hoc Networks (VANETS): Status, Results, and Challenges", 2010.

[7] Farzad Sabahi, "The Security of Vehicular Adhoc Networks", Third International Conference on Computational Intelligence, Communication Systems and Networks, 2011, IEEE Computer Society 978-0-7695-4482-3/11.

[8] Mondal, Bilkish. "Measurement of Fluidic Sensitivity of Fluidic Sensor." Cresol 1: 1024. ijcat.org, pg 205-209.

[9] Ghassan Samara, Wafaa A.H. Ali Alsalihy, "A New Security Mechanism for Vehicular Communication Networks", 2012 IEEE 978-1-4673-1677-4

[10] Milos Borenovic, Aleksandar Neskovic, and Natasa Neskovic, "Vehicle Positioning Using GSM and Cascade-Connected ANN Structures", Ieee Transactions On Intelligent Transportation Systems, Vol. 14, No. 1, March 2013

[11] M. Raya, P. Papadimitratos, J. Hubaux, " Securing Vehicular Communication", IEEE Wireless Communication,2006, Vol.13, No.5, pp.8-15.

[12] Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures,"Security Analysis of Vehicular Ad Hoc Networks (VANET)", Second International Conference on Network Applications, Protocols and Services, 2010 IEEE 978-0-7695-4177-8/10

[13] Ren-Junn Hwang, Yu-Kai Hsiao, Yen-Fu Liu, "Secure Communication Scheme of VANET with Privacy Preserving", IEEE 17th International Conference on Parallel and Distributed Systems, 2011

[14] X. Lin, K. Lu, C. Zhang, P. Ho, X. Shen, "Security in Ad-hoc Wireless Networks", IEEE Communication Magazine,2008, Vol.46,No.4,pp-88-95.

[15] G. Calandriello, P. Papadimitratos, J.-P. Hubaux and A. Lioy, "Efficient and robust pseudonymous authentication in VANET," Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks, pp. 19-28, 2007.

[16] C. Lai, H. Chang, C.- C. Lu, "A secure anonymous key mechanism for privacy protection in VANET," Conference on Intelligent Transport Systems Telecommunications, pp. 635-640, 2009.

[17] Thejaswi, D. T. "MART: Multipath-Based Anonymous Routing Protocol in MANETs." ijcat.org, pg 173-178.

[18] X. Lin, X. Sun, P.H.Ho, X. Shen, " GSIS: A Secure & privacy preserving protocol for vehicular communications", IEEE Transactions on Vehicular Technology, Vol-56, No.6, pp.3442-3456.

[19] P. Kamat, A. Baliga, W. Trappe, " An Identity based security framework for VANETs", Procee.dings of 3rd International Workshop on Vehicular Ad-Hoc Networks, pp.94-95.

[20] Nurain Izzati Shuhaimi, Tutun Zuhana, "Security in Vehicular Ad-Hoc Network with Identity-Based Cryptography Approach: A Survey", 7th International Conference on Telecommunication Systems, Services, and Applications (TSSA), 2012, IEEE 978-1-4673-4550-7/12.

[21] R. Peplow, D.S. Dawoud, and J. van der Merwe, "Ensuring privacy in vehicular communication," in Proceedings of the 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology, pp. 610-614, 2009.

[22] D. Hakerson, A. Menezes, and S. Vanston , "Guide to Elliptic Curve Cryptography," Springer-Verlag, NY (2004).

[23] V.S. Miller, "uses of elliptic curves in cryptography," in Advances in Cryptology, CRYPTO'85, ser . Lecture Notes in Computer Science, vol. 218, Springer, 1986. pp. 417-428.

V. N. Sahare received the B.E. degree in Computer Technology from Nagpur University, Maharashtra, India, in July 2004 and the M.E. in Wireless Communications and Computing from Rashtrasant Tukdoji Maharaj University, Nagpur, Maharashtra, India, in 2008. She is currently a Doctoral Researcher with the Department of Computer Science and Engineering, GHR Labs, Nagpur, Maharashtra, India, where she is doing research in Intelligent Vehicular Ad-Hoc Networks. Her research interests include mobile ad-hoc networks, wireless ad-hoc networks.