Detection of Node Impersonation for Emergency Vehicles in VANET

R. S. Raghav[1], R. Danu[2], A Ramalingam[3] ,G. Krishna Kumar[4]
[1]*M.Tech Scholar,* [2]*Assistant Professor,* [3]*Associate Professor,*[4] B.E *Scholar*
[1, 2, 3] *Department of Information Technology, Sri Manakula Vinayagar Engineering College, Puducherry*
[4] *Department Computer Science and Engineering I.F.E.T College of Engineering India*

Abstract

Vehicular networks (VANETs) are an emerging field with large number of constraints. Were it includes traffic efficiency enhancements, infotainment services and safety applications services. (VANETs) require a mechanism .To help authenticate messages, identify valid vehicles, and remove malevolent vehicles. Security and privacy are two major problems in VANETs. Unfortunately, in VANETs, most privacy-preserving schemes are vulnerable to attacks. The most dangerous attack to be noted in VANET is NODE IMPERSONATION attack which makes them more insecure. Now a day's emergency vehicles like (AMBULANCE, SERVICE ORIENTED VEHICLES) need to move quickly in congested area. So there should be a proper path to pass the traffic without any interference .And there is a chance for some attacks. In order to overcome these attacks this paper proposes a secure framework for detection of NODE IMPERSONATION by using the cryptographic techniques for identify the impersonate node and to provide secure and efficient message communication by using CHAP (Challenge – Handshake Authentication Protocol). Here each node is provided with unique ID or pseudonym and this information will be collected by CENTRAL AUTHORITY (CA). The work of CA is to provide privacy, were they can be extended to use many temporary certificates or ID's instead of one permanent certificate. And they use RSU (ROAD-SIDE UNITS) for communication between vehicles. Once they detect any impersonation node with the help of ID, CA used to detect that particular node and trigger an alarm or caution messages to other node in secure and efficient manner.

Keywords— RSU (Road-Side Units), Central Authority (CA), ECDSA (Elliptic Curve Digital Signature Algorithm), CHAP (Challenge – Handshake Authentication Protocol)

1. Introduction

The networks with the absence of any centralized or pre-established infrastructure are called Ad hoc networks and they are said to be collection of self-governing mobile nodes. Vehicular Ad hoc Networks (VANET) is the subclass of Mobile Ad Hoc Networks (MANETs). VANET is one of the influencing areas for the improvement of Intelligent Transportation System (ITS) in order to provide safety and comfort to the road users [1]. VANET directs the vehicle drivers to communicate and to coordinate among themselves in order to avoid any critical situation through Vehicle to Vehicle communication (e.g. speed control ,traffic jams, speed control, road side accidents, free passage of emergency vehicles and unseen obstacles etc. VANET belongs to wireless communication networks area. VANET is the upcoming area of MANETs in which vehicles act as the mobile nodes within the network. The basic motive of VANET is to increase safety of road users and comfort of passengers. VANET uses the wireless network technology in which communication takes place through wireless links mounted on each node (vehicle) [2]. Each node within VANET play as both, the participant and router of the network as the nodes communicates through other intermediate node that lies within their own transmission range. VANET does not depend on any fixed network infrastructure and they are called as self organizing network. Although some fixed nodes act as the roadside units to facilitate the vehicular networks for serving geographical data or a gateway to internet etc. Higher node mobility, speed and rapid pattern movement are the main characteristics of VANET. Vehicular Communication (VC) is an important component of ITS where vehicles communicate with other vehicles and/or road-side infrastructure, analyze and process with the received information, based on the analysis decisions were made. Such a network of self organized vehicles and road-side infrastructure communicating with each other over wireless medium , with a view to improve traffic safety and efficiency forms a VANET. The VANET contains

infrastructure less structure they face some challenges in the design of Topology and Security. Each Vehicles act as a node in a network and they use some routing protocols for message communication [1]. And the main problem occur during the communication is possible of attacks, it either be insider nor be outsider attack where these type of attacks cause problem during the communication and also these attacks are classified into many types and each attack have their own characteristics [3] .Now days transportation system plays a vital role in our daily life and there is possible of occurrence of road side accidents or vehicle collisions where emergency vehicles needs a way to reach the accident spot without any trouble in order to save the life. And here there is occurrence of attacks like threat to driver confidentiality, threat to authenticity, threat to availability and some of miscellaneous attacks.

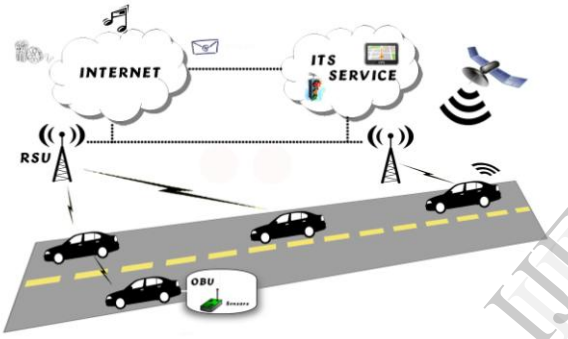

Figure 1.0 Overview of VANET

2. Possible Of Attacks in Vanet

The attack makes the VANET as a more vulnerable network. So these attacks should be detected and several countermeasures should takes place to avoid these attacks

2.1 Threat to Driver Confidentiality

Confidentiality is main type of attack here the messages exchanged between the nodes are vulnerable with some techniques like illogical collection of messages with the help of eavesdropping method and they also gather the node information with the help of broadcast messages [10] .Location privacy and obscurity are consider to be main issues for the vehicles drivers.

2.2 Threat to Availability

Availability refers to the availability of information resources. An information system which does not ready to provide the information when you need it is almost as bad as none at all [8]. These type threats make the nodes more vulnerable which leads to the less availability of the nodes.

2.2.1 Denial of service (DOS) attack

In DOS the main goal is to prevent the legitimate user from accessing the network services and from network resources [12]. And these type of DOS attack can attack the channel system so that no authentic vehicle can access it In VANET it leads to the problem as the user cannot communicate in the network and pass information to other vehicle which could result in miscommunication or drop of packets.

2.2.2 Distributed DOS (DDOS) attack

DDOS attack is more critical than DOS attack as it is distributed in manner. Here the attacker uses different locations to launch the attack were they may user different time slot for sending the message [10]. By using these time slots the nature of the message may be differ from vehicle to vehicle which makes the network not to be available for the users.

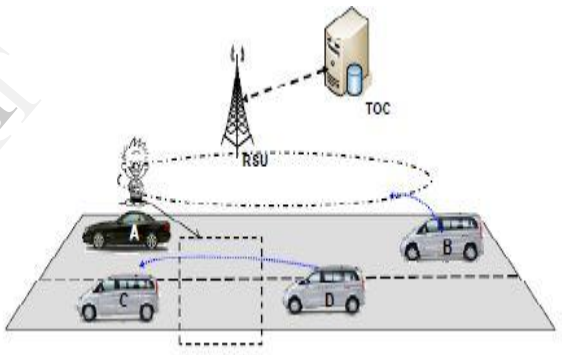

Figure 2.0 Distributed DOS (DDOS) attack

2.3 Miscellaneous threats

These kinds of miscellaneous threats are some of attacks which make the system more vulnerable.

2.3.1 Timing Attack

Time plays a vital role in any application so users need accurate information on right time without any presence of delay. Time is also important issues in Vanet safety applications [10] .Here the attacker without manipulating the original content they add some time slot to create a delay in the message due to this user will not able to receive the message at particular time .

2.3.2 Home attack

Internet is the main component of the VANET. In this attacker can easily attack the user via Internet and can easily control their movements.

2.3.3 Man in the middle attack
As the name tells about the nature of this attack here the attacker sit in the middle of the two communicating vehicle and inject false or modified message between the vehicles.

2.3.4 Traffic analysis
This attack considered to be a serious level threat against the privacy of user in VANET. Here the attacker analyses the traffic packet between the V2V and V2RSU [7]. Attacker uses the information from packet like location of travelling path of the vehicle and Vehicle ID which may be useful for the attacker to extract the required information for its own purpose.

2.3.5 Brute force
Brute force attack is the attacker uses all sets of possible keys for stealing the information from the user [14]. The attacker can use brute force technique to break the cryptography key.

2.3.6 ID Disclosure
It is a passive attack. They get the ID of the target node and its current location. Due to this vehicle's ID will be disclose and their privacy will be viewed easily by the attacker. The attacker can use the RSU (Road Side Unit) [9].

2.4 Threats to Authentication

2.4.1. Sybil attack
It is a critical attack. Here an attacker transmits multiple messages with different ids to the other vehicles. In this way other vehicles thinks that these messages are coming from different vehicles, so there is a occurrence of collision and they are enforced to take alternate route or the attacker provide an illusion of multiple vehicles to other vehicles and to makes them to choose alternate route and leave the rod for the benefits of the attacker [3]. They used to send multiple messages with different ids.

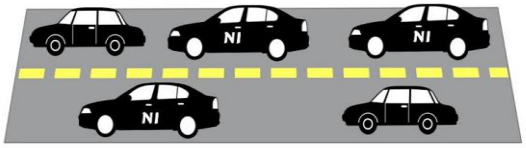

Figure 3.0 Sybil Attack

2.4.2 Node Impersonation attack
The name indicates the nature of the attack were the node will be impersonate by the attacker, so that the attacker can easily changes the identity and act like a original node and pass the false information to other nodes for their benefits. In VANET each node has a unique id and with the help of these ids each vehicle is identified in the VANET network. And these types of attack mostly occur during the time of an accident. In node impersonation attack an attacker can changes his/her identity and acts like a real originator of the message.

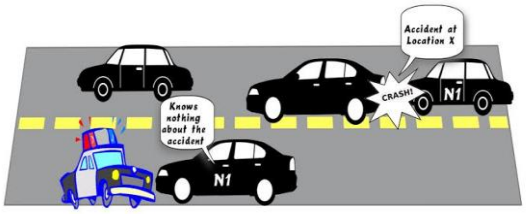

Figure 4.0 Node Impersonation Attack

2.4.3 Message Suppression
In this attacker can selectively drop packets or suppress some important messages from the packet in the network which may contain critical information for the receiver which leads to have improper communication of messages and the attacker may use these packets again later to get the benefits [13].

3. Proposed System
The main threat occurring in a Vanet is attack occurs in Authentication. The emergency vehicles like (AMBULANCE, SERVICE ORIENTED VEHICLES) need to move quickly in congested area .In this situation there is possible of attacks specifically the most dangerous attack to be noted in VANET is NODE IMPERSONATION attack which makes them more insecure [14]. So these emergency vehicles should need a proper path to pass the traffic without any interference. There are some other attacks should be noticed and they should be removed from the network, We have proposed that to provide a secure framework for the emergency vehicles like (AMBULANCE, SERVICE ORIENTED VEHICLES) from NODE IMPERSONATION attack which makes them more insecure. Using the cryptographic techniques for identify the impersonate node and to provide secure and efficient message communication by using some authentication protocol.

3.1 Authentication protocols

Network security plays a major role in network communication privacy, information confidentiality and integrity over network. In VANET every nodes connects with a network for communication of messages between them. So they should have a secure and efficient protocol for communication purpose. For that purpose they should have the AAA technology Authorization, Authentication and Accounting for intelligently controlling access to network resources, enforcing policies, auditing usage and providing the importance of information service. Here in Vanet we are going to use the CHAP (Challenge –Handshake Authentication Protocol).This protocol provides an authentication to each node by validating its identity and they progress with some validating the process each node is provided with unique ID or pseudonym and this information will be collected by CENTRAL AUTHORITY (CA). The work of CA is to provide privacy, were they can be extended to use many temporary certificates or ID's instead of one permanent certificate. And they use RSU (ROAD-SIDE UNITS) for communication between vehicles. Once a new node enters and it will be provide unique ID by CA and if it needs to communicate with other node they should have a handshake with other node and this is achieved by CHAP. Here in CHAP follows 3-way handshake where node sends the call message to CA for entering to the network, (1.CA sends a Challenge message to the node, 2.Node response to the challenge message and 3 CA check its credentials for authentication once they checked the node will be accept else they will be rejected) .The great advantage of using this protocol it is more efficient. Once they detect any impersonation node with the help of ID, CA used to detect that particular node and trigger an alarm or caution messages to other node in secure and efficient manner. Here in CHAP follows 3-way handshake where node sends the call message to CA for entering to the network.

1. CA sends a Challenge message to the node.

2. Node response to the challenge message.

3 CA check its credentials for authentication once they checked the node will be accept else they will be rejected.

The great advantage of using this protocol it is more efficient. Once they detect any impersonation node with the help of ID, CA used to detect that particular node and trigger an alarm or caution messages to other node in secure and efficient manner.

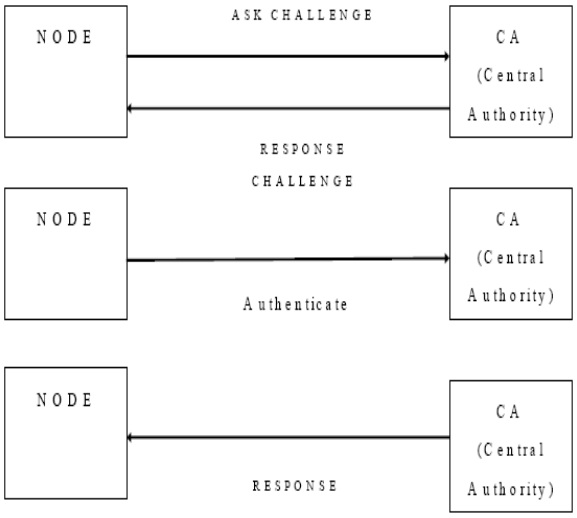

Figure 5.0 Work Flow of CHAP

3.2 ECDSA

The term ECDSA "Elliptic Curve Digital Signature Algorithm" is the combination of Elliptic curve with Digital Signature [12]. Here the ECDSA mainly consist of three concepts like Private Key, Public Key and Signature. The Private Key contains a randomly generated secret number or Id known only to the particular node .If a node needs to send a signed message to the other node they creates a pair of keys in a random manner and they use a signature verification algorithm for verifying the signature of the message .

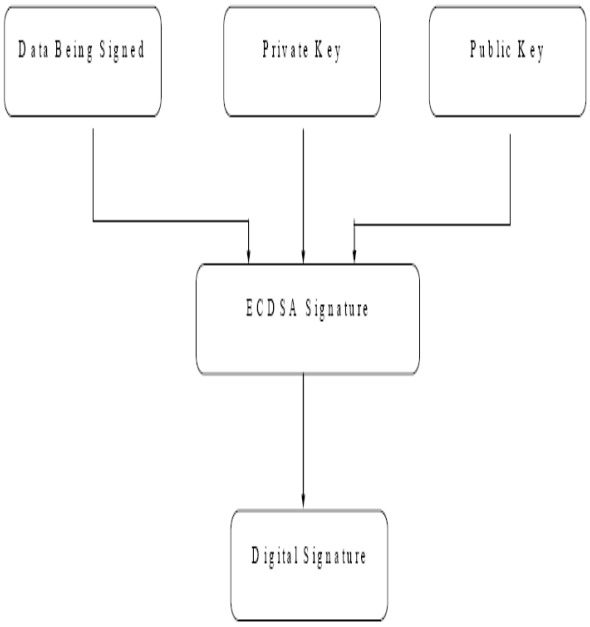

Figure 6.0 Overview of ECDSA

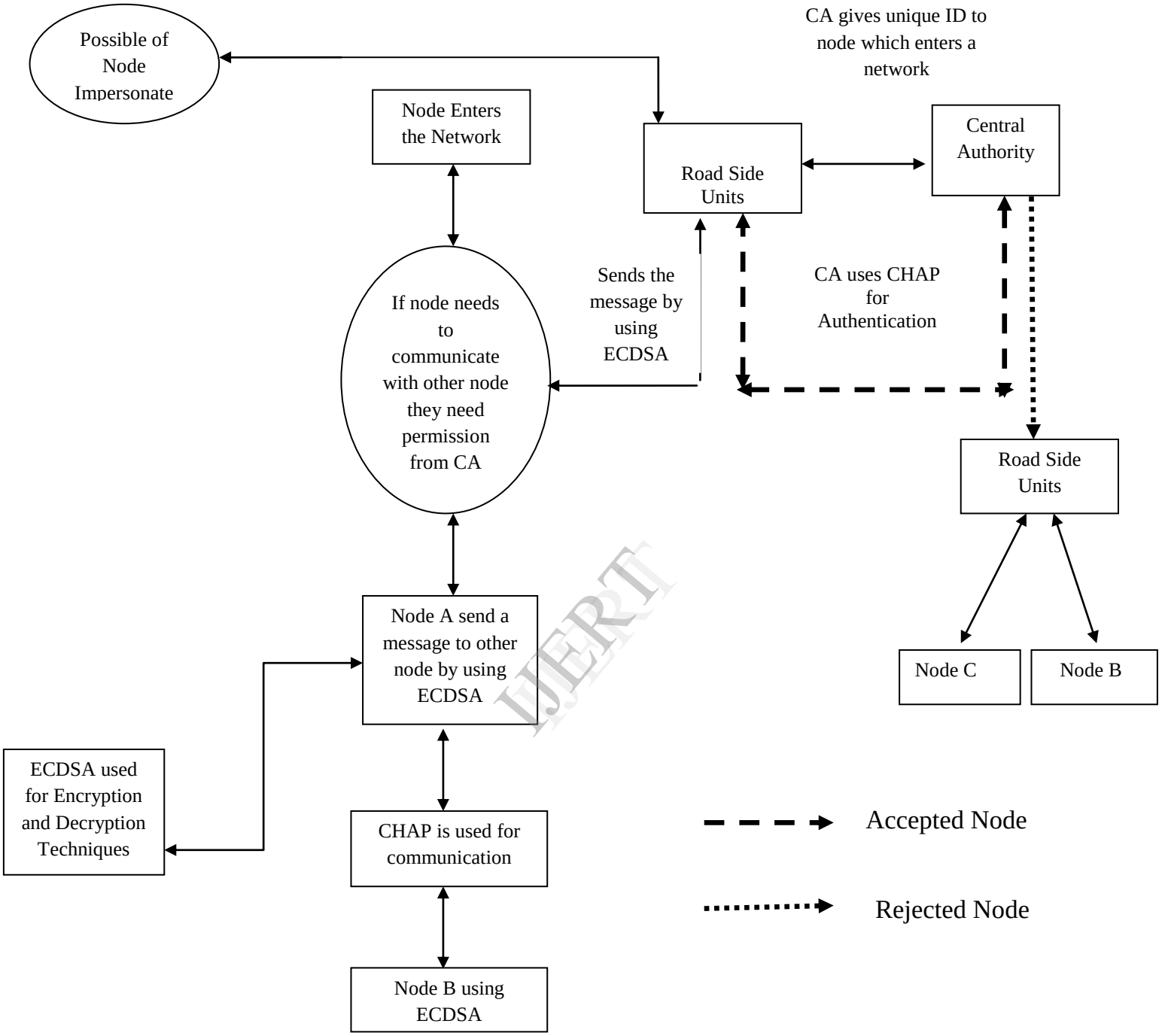

Figure 7.0 Workflow diagram

3.3 Workflow Process

The process flow like this where they use ECDSA and CHAP, to detect node impersonation of nodes for emergency vehicles.

- If a node enters a network it should be register with CA (CENTRAL AUTHORITY) where CA should provide them with unique username and Password with ID and these ID should be randomly generated.
- If a node needs to communicate with other node it should ask permission from CA.
- This permission message should be done by using ECDSA and they need to send to RSU (Road Side Units).
- Where RSU can't able to authenticate they pass the Encrypted message to CA and CHAP is used by CA.
- Node initiates a call by encrypted (ECDSA) message to CA.
- CA sends a challenge message back to the node challenge message contains information about the nodes user name and Password which was given by CA during registration
- Node responses to CA by sending its details.
- CA checks with the details if it gets matched it accept the node to communicate with other nodes , if there is a presence of mismatch in it CA will trigger a alarm message to RSU and other nodes by considering the node have been impersonate and they will be reject for communication.
- They also use same ECDSA for encryption of message and CHAP as authentication protocol for communication between the nodes.

Conclusions

Here we have proposed a secure framework by using ECDSA "Elliptic Curve Digital Signature Algorithm" can be used for creating a message with signature and we can use CHAP (Challenge – Handshake Authentication Protocol) which will provide a secured communication between the nodes. By using these techniques we can provide a secure framework and we can easily provide security for nodes and the detection of node impersonation will become easy and efficient. Our Future work is to provide some extra security in order to avoid the attacks .And this can be done by adding to some new technologies like RFID license plates and Digital signature.

REFERENCES

[1]EMAP: Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks Albert Wasef and Xuemin (Sherman) Shen, IEEE, Fellow

[2]EP2DF: An Efficient Privacy-Preserving Data-Forwarding Scheme for Service-OrientedVehicular Ad Hoc Networks Xiaolei Dong, Lifei Wei, Haojin Zhu, *Member, IEEE*, Zhenfu Cao, *Senior Member, IEEE*, and Licheng Wang

[3]P2DAP – Sybil Attacks Detection in VehicularAd Hoc NetworksTong Zhou, Romit Roy Choudhury, Peng Ning, and Krishnendu Chakrabarty

[4]Efficient Certificate Revocation ListOrganization and DistributionJason J. Haas, Yih-Chun Hu, and Kenneth P. Laberteaux

[5]A Secure Cooperative Approach for Nonline-of-SightLocation Verification in VANETOsama Abumansoor, *Member, IEEE*, and Azzedine Boukerche, *Senior Member, IEEE*

[6]Performance Modeling of Safety Messages Broadcastin Vehicular Ad Hoc NetworksMehdi Khabazian, *Member, IEEE*, Sonia Aïssa, *Senior Member, IEEE*, and Mustafa Mehmet-Ali, *Member, IEEE*

[7]RescueMe: Location-Based Secure and Dependable VANETs for Disaster RescueJinyuan Sun, *Member, IEEE*, Xiaoyan Zhu, Chi Zhang, *Student Member, IEEE*, andYuguang Fang, *Fellow, IEEE*

[8]A Framework for Secure and Efficient DataAcquisition in Vehicular Ad Hoc NetworksKhaleel Mershad and Hassan Artail

[9]Graph-Based Metrics for Insider Attack Detection inVANET Multihop Data Dissemination ProtocolsStefan Dietzel, Jonathan Petit, Geert Heijenk, and Frank Kargl

[10]VANET: SECURITY ATTACKS AND ITS POSSIBLE SOLUTIONS AJAY RAWAT1*, SANTOSH SHARMA2, RAMA SUSHIL3 1Department of Computer Application, University of Petroleum & Energy Studies, Dehradun, India. 2Department of Computer Application, GEU, Dehradun, India. 3Department of Computer Application, Shri Guru Ram Rai Institute of Tech. &

Science, Dehradun, India. *Corresponding Author: Email– 1rawat.ajay@hotmail.com, 2Santosh.sharma.ddn@gmail.com, 3ramasushil@yahoo.co.in

[11]ABACS: An Attribute-Based Access ControlSystem for Emergency Services over VehicularAd Hoc NetworksLo-Yao Yeh, Yen-Cheng Chen, and Jiun-Long Huang

[12]The Elliptic Curve Digital Signature Algorithm (ECDSA) D.on Johnson and Alfred Menezesand Scott VanstoneCerticom Research, Canada _Dept. of Combinatorics & Optimization, University of Waterloo, Canada

[13]Overview of security issues in Vehicular Ad-hoc Networks José María de Fuentes, Ana Isabel González-Tablas, Arturo Ribagorda Department of Computer ScienceUniversity Carlos III of Madrid (Spain) Corresponding author: jfuentes@inf.uc3m.es

[14]Security Issues and Challenges of Vehicular AdHoc Networks (VANET)Ghassan Samara#1, Wafaa A.H. Al-Salihy*2, R. Sures#3#National Advanced IPv6 Center, Universiti Sains MalaysiaPenang, Malaysia1ghassan@nav6.org, 3sures@nav6.org*School of Computer Science, Universiti Sains MalaysiaPenang, Malaysia2wafaa@cs.usm.my