Authentication for security in Vehicular Ad-Hoc Network using Cognitive Radio Technology

G.Bindu[1],S.Sridevi[2],Dr.R.A.Karthika[3]

[1,2]Assistant Professor,[3]Associate Professor,

VISTAS, Chennai

Abstract

Cognitive radio technology works with wireless network and programmed to obtain information from users and authorities from a geographical location, to broadcast the data's between vehicles to vehicles or to road side Infrastructure it is aided by Vehicular Ad-Hoc Network (VANET) which is regulated by Wireless Access Points (WAP) of vehicles. The data's communicated has huge promising possibilities in reducing traffic jam, enhanced road safety, maximum passenger comfort while driving vehicles, and also it serves in reducing fuel consumption. However the data security from Vehicular Ad-Hoc Network considered as a primary treat, because there are some data's communicated might not be certain due to cyber-attack or through signal drop out. This paper identifies the privacy and security issues in communicating data's through Vehicular Ad-Hoc Network and to establish a secured protocol.

Keywords: Cognitive Radio, Data Communication, VANET, Data Security.

Introduction

The tremendous growth of Cognitive radio aided Vehicular Ad-Hoc Network (VANET) in recent years lead to extensive deployment of wireless technology with the large number of wireless gadgets related to motor vehicles in connection with GPS. The main concern in cognitive radio network is to identify available free spectrum and there are various methods adopted to detect availability of a channel like beacons, spectrum sensing, and geo-location database. The coordination of operation in cognitive radio network is mainly governed by the level of security. As cars fall out of the signal range and drop out of the network, other cars can join in to the same network and connects vehicles one to another so that a mobile network is created. It is estimated that the first systems that will be this technology are police and fire vehicles to communicate with each other for the purpose of security. To ensure data integrity, reliability, non- repudiation, preserving privacy of user, it has to be authenticated from authorizedusers or primary users and these data's can be accessed by secondary users to share without making any corrections or interference on received data in a same bandwidth. Cognitive radio technology is planned toshape protocol rules in order to alter and facilitate the user needs efficiently and this will convert the radio nodes from being blindsides of predefined protocols.The data's communicated through Vehicular Ad-Hoc Network (VANET) will be for various reasons in which some messages are Cooperative Awareness Messages (CAMs), may become vulnerable to a listener who can then get the location of that vehicle. Therefore, it is necessary that the messages are secured from giving away the user's location.

Privacy and Security issues

The majortreat in VANET security is to secure location of the vehicle which transmits data to the other users because there should be restriction for somefor the privacy purpose. The location and the personal information of usercan be tracked by attackers and may create harmful results in future, Reliability in communicating data's will be achieved through authentication in order to ensures the purity of the communicated messages, as well as it is difficult to interfere with data's. Another requirement for VANETs is aborting cancellation, hence users are not be able to refuse the message they sent and also they can be identified and penalty is subjected in case of a wrong or fake information[1]. It is achieved by making the data's traceable from the users only by the authorities so that they can cancel or abolish the fake information. This is possible when the tracing should be done by multiple authorities for Individual type of attackers exist in network to enhanceadditional security and more privacy. There are various security schemes can be used to protect privacy in order to achieve anonymity based on the available security system.

Associate vs. Stranger

The attacks can be done by a member node who can communicate with other members of the network here the impact of the attack will be high, otherwise known as insider attack or an associate member can be able to attack in various ways[2]. Whereas, a stranger, who is otherwise called as outsider will not be authenticated to directly communicate with other members of the network, have a limited capacity to perform an attack this will minimize the attacks.

Frequent Attacker vs. RationalAttacker

The frequent attacker uses various methods to damage the member nodes by reducing the band width or drop in network connection by cyber-attack on the network regularly without having any personal gain on attacks. On contrast the rational attacker expects its own benefit from the attacks carried in network and it is easy to establish or figure out the attackers because they are more predictable and follow some patterns that can be scheduled to abort.

Progressive vs. Passive

The progressive attacker can create new packets at periodic intervals to damage the network which is difficult to identify whereas a passive attacker only can screen the packets through wireless channel but cannot generate new packets like a progressive attacker hence it is less harmful[2]. In fact, there is another characteristic of an attacker to make it safe.

Local vs. Extended

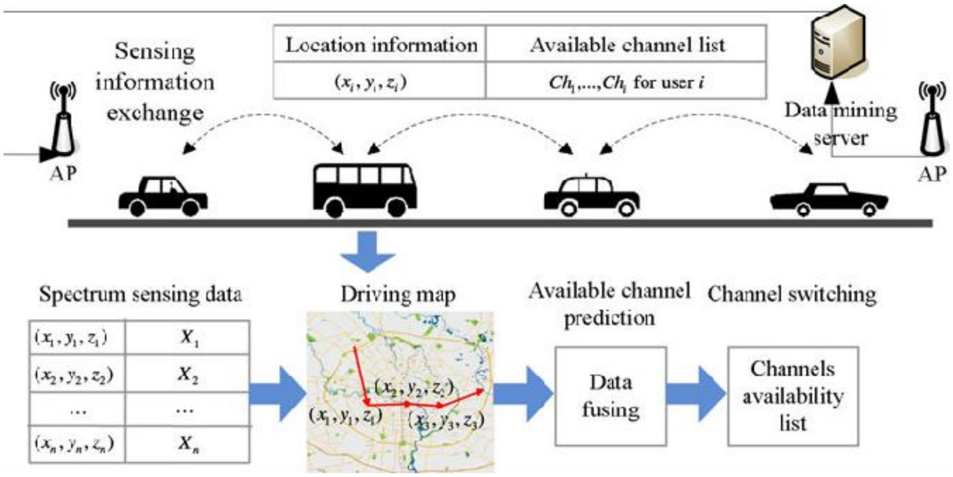
There are attacker focus on a particular geographical area and it is considered as a local attacker it has limited in scope, these attacks can be done by vehicles or by base stations the attacks can be predictable and can be easily sort the issue even if it possesses several entities[3]. In other end the extended attacker can control many entities by widenits scope for long time and the attacks will be continuously disseminated across the network.

Security Requirements

There are three properties in regard withdata security that cannot be ignored and the confidentiality of data’s, integrity, and availability of network for VANETs security, these three properties are essential for managing secured data.

Data Privacy and Confidentiality

Data privacy can be obtained only when the users can access the limited data and the profile or a driver’s personal information must be secured and maintained with authorities. In the following two cases Communications between vehicles and road side units Privacy means that an eavesdropper or a listener is absurd to decide that the two different data’s communicated from the vehicle or a source. Confidentiality and privatizing the data’s to determine if these two different valid messages are delivered from a single source or a vehicle it is strongly difficult to justify by everyone only anappropriate element can Identity and safeguard the privacy of the user and it is similar to Invisibility. Identification of the personal identity of data’s created by user will betotally costly and the confidentiality between a group refers to only a member among the group can able to decrypt the data’sand that are disseminated to all member of a group[6]; and none other can receive or decrypt the data’s except a separate and dedicated receiver can able to decrypt the data’sconcerned to it.



Network availability and Data Integrity

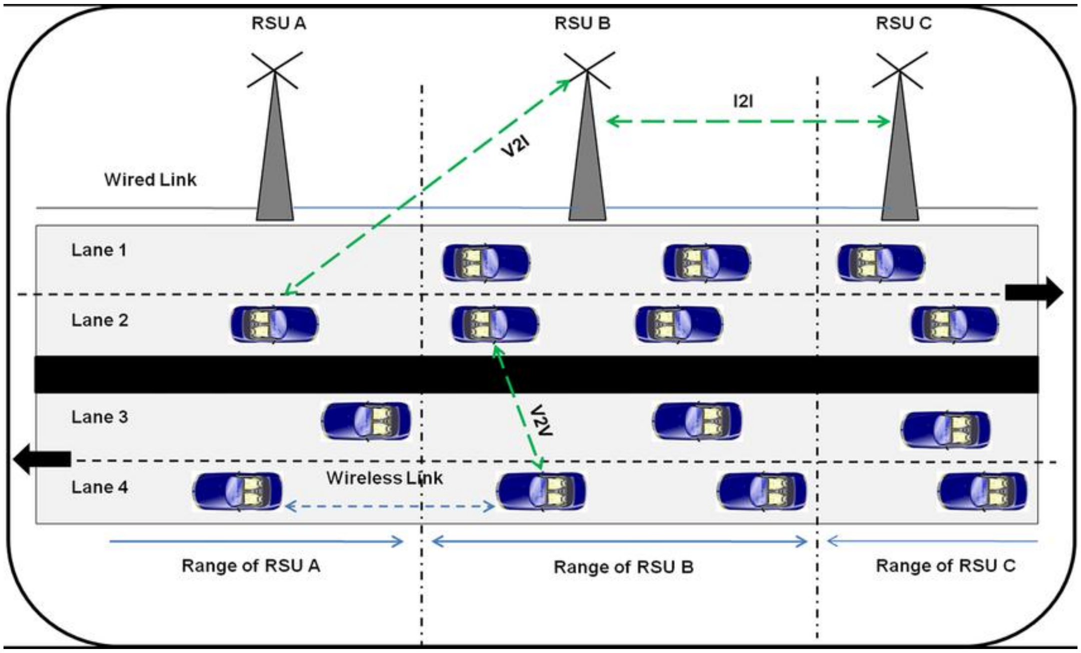
The greater responsibilities goes in maintaining a stable network to transmit data's and that has to be available even if the network the bandwidth and performance should be consistent. This approach of VANETs is not distinct from another networks and it is difficult to establish and assure because of thespeed of vehicles will be varied from each and the distance maintained by vehicles will keep changing. There are some major security requirements and arrangements should be followed satisfy in VANETs data Integrity. This will authenticate that the data's or messages delivered among nodes cannot altered or changed by any attacker in the network. This approach of VANETs generally comprised with data authentication and integrity. The provisionscould be through the node the data's can be verified and the data is absolutely sent and signed by another node without being altered by users and attackers[5]. In order to gain the accomplishment of objective, It is required that the data's need to be verified. The moment when the data is delivered by sender vehicle it has to be authenticated from the receiver's vehicle by executing data verification to analyze if the message bears the corrupted or original data. During the data communication group keys are used by authorities to enhance the security data encryption/decryption, it is a multicast operationsfor the data delivery procedure. TheVehicular Ad-Hoc Network provides data security with an advanced encryption Standard algorithm and Secure Hash Algorithm.

Trajectory Analysis

The route and direction of the vehicles areanalyzed and determined with Global Positioning Services (GPS) enabled navigation systems for the verification in VANET with data forwarder nodes to increase the trust levels. The Direction based Multicast (DMC) exploits vehicle path and direction for efficient multicast in Vehicular Ad-Hoc Network. The data forwarding measurement is predicted to determine the capability of a vehicle node to transmit the message to destination nodes in dissemination procedure.

Data Communication between Vehicles to Vehicle

The data communication of vehicle to vehicle configuration uses multi-hop routing in cognitive radio network and disseminate the information related to traffic like traffic updates to multiple hops for the receivers in the coverage range. As VANET considered as an intelligent transportation systems with the controls, it is convenient for a driver to focus only ahead that is in front no need to have a rear view or not be-hind driver can receive information about the vehicles behind and the distance need to be maintained as well as routes can be rescheduled before the forthcoming collision and the messages will be broadcasted to the users in a particular coverage range.



Communication of Data from Vehicle-To-Roadside Unit

The data’s are communicated between vehicles to roadside unit infrastructure which perform a single hop broadcast from the vehicle to road side unit and the roadside unit disseminate the data or message to all equipped vehicles in the radio coverage or vicinity[7]. The bandwidth of the network will be high during Vehicle communication to a roadside unit infrastructure and the signal strength will be high there are very rare chances of data losswhen it is communicated with roadside units.

Routing-Based Communication

The Cognitive Radio network is the major source forlong distance data communication by linking vehicles and road side units, in some cases the routing-based data communication structure will broadcast in multi-hop fashion where a message is multiplied till the vehicle receives the desired and correct data[6]. There are some cases where the query is raised to the vehicle possessing the desired bit of data and the application of that vehicle immediately sends a single message containing the data to the vehicle which is requested for the information this type of data communication occurs in routing based data communication.

Conclusion

It is compulsory that there should be a coordination maintained and ensured between the licensed and unlicensed users. The communicated data loss will due to different type of attackers and less amount of network bandwidth utilized for data communication in Cognitive Radio technology aided by VANET. Cognitive radio technology with VANET optimize the datato make efficient data communication. Drivers must be reliably identified in case of accidents. It is compulsory that a user should have responsibility in communicating data to other users in network, these data’s will be verified for the future investigation and it will identify the string and content of the data exchanged before an accident or an incident. Despite the vehicles have real existence and identity it could be hidden from other vehicles for security reasons, since the attacks will be predicted it can be resolved by authorities with the aid of trace manager which has the ability to obtain vehicles existence original identities in order to abolish them from future usage.

References:

1. Joanne Mun-Yee Lim1*, YoongChoon Chang2, MohamadYusoff Alias3,and Jonathan Loo4 Cognitive radio network in vehicular ad hoc network (VANET): A survey, Cogent Engineering. 3. 10.1080/23311916.2016.1191114.

2. Zhexiong Wei∗ , F. Richard Yu∗ , Helen Tang† , Chengchao Liang∗ , and Qiao Yan, Security Schemes in Vehicular Ad hoc Networks with Cognitive Radios,Bansal, International Journal of Advanced Research in Computer Science and Software Engineering7(12) ISSN(E): 2277-128X, ISSN(P): 2277-6451, pp. 68-72

3. VinhHoa LA*1, Ana CAVALLI 2, Security Attacks and Solutions in Vehicular Ad Hoc Networks: A Survey, International Journal on Ad Hoc Networking Systems (IJANS) Vol. 4, No. 2, April 2014, DOI : 10.5121/ijans.2014.4201

4. Felipe Domingos da Cunha, Leandro Villas, AzzedineBoukerche, Guilherme Maia, AlineCarneiroViana, Raquel A. F. Mini, Antonio A. F. Loureiro, Data Communication in VANETs: Survey, Applications and Challenges, HAL Id: hal-01369972 https://hal.archives-ouvertes.fr/hal-01369972 Submitted on 23 Sep 2016

5. Yousef Al-Raba'nah, Ghassan Samara* Security Issues in Vehicular Ad Hoc Networks (VANET), International Journal of Sciences & Applied Research, www.ijsar.in IJSAR, 2(4), 2015; 50-55

6. Ms. S. Jeevitha 1, Mr. S.SAMPATH*2, Hybrid Data Transmission Framework with Prediction based Channel Assignment under Cognitive Radio based Vehicular Ad-Hoc Network, International Journal On Engineering Technology and Sciences – IJETS™ ISSN(P): 2349-3968, ISSN (O): 2349-3976 Volume IV, Issue II, February – 2017

7. Ishu Bansal * A Review on Various Approaches of Data Security and Communication in VANET International Journals of Advanced Research in Computer Science and Software Engineering ISSN: 2277-128X (Volume-7, Issue-12) Page 68 www.ijarcsse.com ,December 2017

8. Saurabh Kumar Gaur, S.K.Tyagi, Pushpender Singh, “VANET” System for Vehicular Security Applications International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-6, January 2013 279