International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 6 | Issue 1 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/IJSTCSEIT

Secure Jaunt– Implementation of Honeypot In VANET

Nitha V R
Department of Computer Science, Sree Narayana College , Cherthala, Kerala, India

ABSTRACT

VANET (Vehicular Adhoc Networks) is a technology which is used to implement Intelligent Transport System thereby assuring security. VANET is a car-to car adhoc network in which vehicles can communicate with each other and also with the nearby base stations within a stipulated range. Using VANET technology, drivers would be warned of a potential upcoming crash by the vehicle they are driving because of V2V communication. V2V is a crash avoidance safety system.V2V communication is based on a wireless protocol similar to Wi-Fi which is called DSRC (Dedicated Short Range Communication). The Dedicated short-range communication (DSRC) is a wireless communication technology used in vehicles to implement intelligent transportation system to communicate with other vehicles. This technology operates on 5.9 GHz band of radio frequency spectrum and is effective over short to medium distances. When DSRC is combined with GPS technology, the implementation cost can be minimised.

Keywords : Vehicular Adhoc Networks, Dedicated Short Range Communication, Secure Jaunt

I. INTRODUCTION

In V2V, the transmitted messages common to all vehicles include each vehicle's current GPS position, Vehicle speed, Acceleration and Heading. The Vehicle control information includes Transmission state, brake status, steering wheel angle, Vehicle's path history, Path Prediction.

Path History includes a set of previous positions which provide exact location of the vehicle. Only the points that are necessary to define its path history are transmitted. Straight road need only few data points that represent path history. But when a vehicle enters a curve, more data points need to represent the path history.

Path predictions allow a vehicle to provide its future trajectory and its confidence in this trajectory. With path history and path prediction, vehicle is provided with a dynamic map of the roadway geometry ahead by providing essential information like threat assessment and potential crash prediction.

Sophisticated security system is put in place to ensure that all information is exchanged between vehicles is authentic and can be trusted. By employing common data, security and communication standards, V2V inter-operality among automotive manufacturers has been achieved. Since all vehicles communicate in the same way, each automotive manufacturer is free to develop their own safety application and warning indicators.

When a crash is predicted, the vehicle will provide a warning to the driver either through a seat vibration, tone or visual display or a combination of these indicators. The driver has to remain in controlling the vehicle all the time and the vehicle will not automatically break.

II. METHODS AND MATERIAL

SECUREJAUNT: FEATURES IN V2V TECHNOLOGY

1) Emergency Electronic Brake Lights (EEBL): This application will notify a driver about a sudden braking vehicle in the path ahead before you see the brake light of the vehicle in front of you.

2) Blind Spot Warning Safety Application (BWSA): This application lets a driver know that there's a vehicle that may not be visible to the driver and may be positioned in the driver's blind spot. Because of V2V communication, a blind spot advisory is issued to make you aware of the presence of this vehicle.

3) Lane Change Warning (LCW): If you attempt to change a lane, when there's a vehicle in our blind spot, this will notify a warning which let you know that it's not safe to change lane. Using the data obtained through V2V communication, your vehicle predicts that this vehicle will soon be in your zone.

4) Forward Collision Warning Application (FCW): This application will warn the driver of a potential rear-end crash with a stopped or slower moving vehicle ahead. If there is a slowly moving vehicle ahead your vehicle, the vehicle ahead will provide a warning in the form of wireless signal if you are approaching too quickly.Thereby a potential rear-end crash situation can be avoided. This notification enables you to slow to a safe speed and distance behind the slower moving vehicle. This enables you to slow to a safe speed and distance behind the slower moving vehicle.

If a vehicle is stopped in front of your vehicle, if you can't see it, V2V communication makes you aware of the stopped vehicle so that you can safely slow your vehicle before reaching the stopped vehicle ahead.

5) Do Not Pass Warning (DNPW): This is a safety application, intended to let the driver know that it's not safe to attempt to pass a slower moving vehicle because of oncoming traffic in passing zone. Using V2V, your vehicle is continually looking for cars in your intended passing zone. If a vehicle is detected in the passing zone, a driver advisory is provided, letting you know that the passing situation is potentially unsafe.

6) Intersection Movement Assist (IMA): This safety application is intended to warn the driver when it's not safe to enter an inter section (Junction). If an intersecting vehicle is detected using V2V, a driver warning is provided if it's unsafe for you to enter the intersection. This help you respond in a timely manner and stop rather than continuing through the intersection and potentially getting into a crash.

7) Short Voice Message Broadcasting (SMB): If any driver has to broadcast a message to all vehicles involved in V2V communication, the voice message has to be send through a wireless base station (antenna) placed beside the road. This message can be sent to adjacent wireless antennas and from the antennas the message will be transmitted to a common base station server. Similarly, all broadcasted messages will be received by a common base station server. Based on the majority polling, the common base station server will broadcast a common authorized message to all the vehicles within the range of that base station.

8) Pair up with adjacent cars: Group voice messaging can be implemented if one vehicle is paired with other vehicles. This functionality can be implemented if few cars are travelling in a group. This help in tracking the entire vehicle's who are paired in the same travelling group. Voice messages can be sent from one vehicle which will be broadcasted to all the vehicles which are paired by passing the vehicle Ids. So this help to establish a group voice chat while travelling long distance journeys by a group of vehicles.

SECURITY ISSUES IN VANET

Type of attacks:

1) SYBIL ATTACK: According to this attack,a malicious node attempt to fabricate and manipulate original identity and pretends to be a registered or original source node. The attacker node may create assorted vehicles or nodes of same identity by replication and forces other nodes to leave or move fast from road.
2) DOS (Denial of Service) ATTACK: In this attack, the network availability may get jammed by attacker node or malicious packet

3) DDOS (Distributed Denial of Service)ATTACK: Here attacker perform attack from multiple different locations. As a result there is a chance of multidirectional jamming or blocking. Hence authentic systems can't communicate.

4) TIMING ATTACK: Delay is created in original message by addition of time slots. Content of message is not manipulated or changed but delay is added so that message can be received after validity or importance of message

5) APPLICATION LEVEL ATTACK: Here manipulation is done in the message received & then retransmitted to different nearby nodes or vehicles.

6) NODE IMITATION ATTACK : Here the attacker can send malicious or wrong message to any node hiding or changing its own identity

Establishing security in VANETs is challenging as the network is dynamically changing and has neither fixed boundaries nor a central data management where a firewall or an intrusion detection system (IDS) could be placed.

HONEYPOT

Honeypot is one among the recent innovations in intrusion detection (ID) technique which can be considered as traps designed to attract potential intruders. They are fabricated to look like real systems by putting real looking information into them to make it appear to be a valuable system on the network.

By diverting attackers from valuable systems to honeypots, we can observe what the attackers are trying to do to our systems and networks, and based on this we can develop strategies to respond to attacker.

A honeypot system is instrumented with monitors and event loggers so that hacking activities can be monitored and their methods and patterns can be studied. A honey net is used to deflect hackers from attacking a real network and its resources. Once hackers thought they have got what they need, their attention could be diverted.

An attack against a honeypot is made to be successful. Most importantly, a honeypot is not a real system used by any real user. Therefore any access to honeypot is not legitimate. So we can say that any attempt to communicate with a honeypot is most likely a probe, scan or an attack.

Any inbound connection to honeypot can be considered as a network scan or direct attack. If a honeypot initiates outbound traffic, the system is most likely compromised. Honeypots can be deployed in a variety of locations on a network.

ENHANCED SECURITY IN V2V COMMUNICATION:

By using Aerolink functionality, which is an OnBoard Security in V2V communication, we can protect connected cars from hackers and drivers from being

tracked or hijacked. Aerolink is a software used to enhance Confidentiality, Authenticity and Safety in V2V vehicle transport.

SecureJaunt enhances secure communications by implementing:

- It helps to check the authenticity of all messages coming to it and also helps to secure the crucial data that has been send out from a vehicle.
- Authorities must not use this technique to track vehicle information, speed or location of onboard security of the vehicle.
- With the help of honeypot, the activities of black listed users can be monitored for securing our system.

SECURITY FORMAT USED IN SecureJaunt:

Aerolink is the software which implements V2V security formats by keeping security standard which specified in IEEE 1609.2 standard used in US, Europe etc.

III. RESULTS AND DISCUSSION

WORKING OF SecureJaunt:

SecureJaunt acts as an interface which filters the messages passed in V2V to enhance security such as, filtering for security of messages passing. It encrypts the crucial data sending from the vehicle (such as vehicle details or travelling histories)and It checks the relevance of information, Such as checking the message to find whether the message send is too old or whether the vehicle is too far to pair up.

It also checks the Authenticity of each signing vehicle, by using all the certificate verification .Any vehicle within 300 meters will be authenticated by this service. It is implemented with a set which contains two factors,

The certificate.
The Private Key.

MAINTAINING SEPARATE BLACK LIST AND WHITE LIST IN V2V:

While pairing between the vehicles in V2V, in order to maintain more security and authentication, separate Black List and White list are maintained in the Base station.
Using this Black list and White list, before pairing a vehicle an automatic check can be performed in the two lists such that if the id of any of the pairing vehicle matches with the predetermined blacklisted id, if so, that particular pairing will be blocked.

The Black list and White lists are operating as follows:

BLACK LIST:
The list which is created with the id's of all Vehicles from the pairing history, which were determined as fraudulent or coming from a malicious source.

All those malicious id's will be stored in the blacklist. The Blacklist will be updated frequently with the newly traced malicious id's and thus maintains an updated information about all the id's which are tracked as fraudulent so far.

If two new vehicles are going to pair then a quick check of each of the car id's will be searched in the Black list and if not found, then a message will signal that the id's are safe to be paired and if any of the id's are matched with the Black list entry, then that pairing will be Blocked with a warning message. Hence unwanted paring from a fraudulent or malicious vehicle can be banned.

WHITE LIST:

It contains the id's of all the vehicles which are successfully paired so far in the pairing history .Using this list, we can easily recognise an incoming id as trustworthy and authorised. Hence when a request is coming to a vehicle to be paired, a quick automatic check will be performed in the white list and if a match is found, then immediately a positive signal will be granted to pair up the vehicles for further utilities. Hence, using this combination of black list and White list, the pairing vehicles can enhance security in the pairing process.

REDIRECTING BLACK LISTED USER'S TO HONEYPOT

If a new request is coming from a vehicle to pair, then the id of the requested vehicle will be first checked in the Blacklist and if not found, then it will be checked in the white list. If a match is found in the black list, then immediately the request will be redirected to honeypot so that the user's activity can be monitored. By diverting attackers from valuable system to honeypots, we can observe what the attackers are trying to do to our system and network and based on this, we can develop strategies to respond to attacker. Since the honeypot log all the activities of attacker, the behaviour of attacker and pattern of attack can be analysed for protecting our system.

If a match is not found in the blacklist, then it will be checked in the whitelist and if found then it will be paired with further formalities. Hence Maintaining separate Black lists and White lists enhance the Security feature of V2V communications.

IV. CONCLUSION

V2V communication can be made secure by implementing SecureJaunt features and thereby ensuring a safe and secure communication of vehicles. SecureJaunt features can be implemented to any vehicles which are near to each other V2V technology hopes to dramatically decrease the amount of accidents between vehicles and help keep drivers safe. There is no doubt that complete safety on the road will come in the future and the development of this technology is a step in the right direction.

References:

[1]. https://ieeexplore.ieee.org/document/8376311
[2]. https://emergingtechnology.wordpress.com/2007/10/03/vanet-the-vehicular-ad-hoc-network/
[3]. https://www.ukdiss.com/examples/vanet-technology.php
[4]. https://searchsecurity.techtarget.com/definition/honey-pot

Cite this article as :

Nitha V R, "Secure Jaunt - Implementation of Honeypot In VANET", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 1, pp. 170-174, January-February 2020.
Journal URL : http://ijsrcseit.com/CSEIT206139