AN ANALYSIS OF AUTOMOTIVE CYBER SECURITY MECHANISM FOR INTERNET OF VEHICLES

Sandeep Kr. Yadav[1], Pragati Gupta[2]
[1,2]Rajkiya Engineering College Banda

Abstract

Internet of Vehicles is the domain of futuristic transportation system (FTS) which is used to improve passenger's safety, real-time traffic situation and remotely vehicle control into the emergency cases. Automobile industries have great expectations and want to must ensure that everything possible from the solutions of FTS so they can improve the services. However in this technology, hackers can illegally access FTS networks for individual benefits and interfering into the FTS services which could cause major accident. To provide the solution of this problem several researcher have introduced automotive cyber security algorithms but that have increased the complexity and time during encryption and decryption information. In this paper, we have investigated parameter of automotive networks security and introduced an automotive cyber security algorithm. This algorithm is the fusion of data privacy protection and network protection. The proposed algorithm has capability to detect and concur consequences threats, vulnerability, and suspicious activity. Finally, we have discussed an automotive cyber-security algorithm which is difficult to crack by attacker.

I. INTRODUCTION

Today's, cyber security is a very much debated facet of emerging internet of things. Cyber security plays a very important role in automotive sector to provide a smooth and faster way so that the automotive vehicles can be made secure from the hacker or unauthorized persons. Basically, this paper discusses the vulnerabilities in the automotive industry and the ways or algorithms by which we can resolve all the difficulties coming in the internet of vehicles. Whenever something new connects to the internet, it is bare to the full strength of malicious activity.

Now that we have reviewed very potential threats and vulnerabilities, the next challenge is to design secure automotive system. We know that automotive security field is relatively recent, there are strong technologies and skill in neighboring industries to be leveraged and adopted. Developers can take advantage of obtainable secure development processes to fit in security and privacy into their new vehicles by design. There is a strong relationship between cyber security and automotive security. Automotive computer security is a two-way approach of defenses to detect, protect and correct identifiable or avoidable threats and to protect from previously unknown is unavoidable ones.

One of the most important steps in improving security attitude, whether for a physical location or a computer system understands the motivations, objectives and action of potential attackers or threat agents. There is a characteristic progress of these types of actors in a newly internet connected market. In these types of connected systems, threats can force the lock from outside the next device. Threat agents are quite varied but knowing that who are they and modeling their behavior can help in planning the very much effective lessening strategies. It is very important to fragment the information with a lack of standard agent's definition. This disintegration makes it difficult to quickly and consistently review risks from particular agent.

In this paper we will discuss the potential threats, vulnerabilities and privacy along with these; we will also discuss to design the algorithms for providing a better security in automotive sector.

II. MOTIVATION AND RELATED WORKS

Anything which is newly connected to the internet, it is exposed to the full force of malicious activity. When something as complex as a modern vehicle is connected, assessing the scope of threats is a considerable work, and an attack surface may be left unprotected by probability. Many security risks now widen to vehicles malware, Trojans, buffer flood exploits and improvement escalation.

The vehicles incorporating up to 100 ECUs (Electronic control units), they are approaching the upper boundaries of the wiring connect, which is one of the most important reason that the industry is moving towards greater assimilation and virtualization, reducing the total number of ECUs but increasing the number of functions and complexity of the software. The resulting attack surface is wide, moving most in-vehicles system and an increasingly wide range of external networks, from Wi-Fi, cellular networks and the internet to service garages, toll roads, drive-through windows, gas station and a rapidly growing list of automotive and aftermarket applications. However, effective security cannot be achieved by dealing with individual components, threats or attack points. Unlike traditional computer system, initiation and cost in both the cyber world and physical world are possible over vehicles attack surfaces, making it more challenges to protect the vehicle's systems. In a way of progress of automotive cyber security, the Intel IT Threat Assessment Group has developed a threat agent library and threat agent risk assessment usage model to make a consistent reference to human agents those make-believe threats to computer systems and other information assets.

A. Pranksters and hacktivists

Pranksters, hacktivists and vandals typically represent the dark side of the hobbyist group. They take the opportunity to demonstrate their skill or promote their causes but with negative outcomes for the product owner or manufacturer. In the automotive market, the complexity of the product and requirement for special tools or skills may constrain the number of pranksters and hacktivists able to actually uncover and exploit vulnerabilities, at least until the exploits are developed and made available by criminals or nation-states with greater resources.

B. Vendor and Operations

Many car hacking tools already exists for Vendors, as they do for Smartphone's and other types of electronic devices. These persons are not criminals but they may want to hack their own vehicles for repairing and maintenance in order to improve performance, or disable components to baffle their actions for confidential or false reasons. Since some automotive systems are safety-critical, tampering or modifications can also be forced or forbidden with appropriate security functions even by owners, ensuring that the vehicle operates as intended so that the manufacturer is not subject to additional liability.

C. Organized Crime

Prearranged crime had always been a threat to vehicles and is now a significant threat actor in the cyber security space and possibly in front of researchers in their technical capability.

Cyber threats often follow an evolutionary pattern, beginning with denial-of-service (DoS), followed by malware, ransomware and attacks targeted at specific entities. In this case, DoS or disabling vehicle functions could be aimed at specific models, geographic regions, rental car companies or other corporate fleets. Malware may follow a similar pattern, searching for valuable data to sell or use or tampering with mileage and maintenance data. Ransomware in this case could involve holding individual cars for ransom or troublesome traffic to create disorder for financial or political gain. In cyber security, these tools then become available to other on a cyber-crime as a service model, potentially opening up the automotive market to accurate attacks against individuals, competitors and politicians among others.

D. Nation-states

The motives of nation-states are not often easy to determine. The obvious ones are industrial espionage, surveillance and economic or physical warfare. Other motives may be interference to assist a general manufacturer against distant competitors. If cars are softer targets than corporate or government facilities, they could enable tracking and audio monitoring of high-value subjects. As cyber crime matures and code is shared, complicated code developed by well-funded nation-states finds its way into criminals and pranksters.

E. Infrastructure of transportation

Next generation cars are not only communicating with the internet but they are also talking to each other and to manifold parts of the transportation infrastructure. In addition to attacking the vehicle, security and safety issues can occur through attacks or misbehavior of the nearby infrastructure. A simple example of traffic lights that are by chance or intentionally set to be green in both directions, road trains that allow that cars to be too close together, or message floods that prevent delivery of vehicle-to-vehicle data in time to avoid a collision. Smart vehicles need to be able safety manage through these and other scenarios with appropriate defensive actions.

F. Vehicles Data Protection

To ensure the vehicle data protection it is necessary to encrypt the data exchanged among the vehicles and the RSU. As well as the vehicles needs to verify each other's identity to provide authentication. To achieve the highest level of security the access method to the RSU is designed to be identical to that of a standard WLAN, where mobile device connect to an access point. In our security architecture we used the IEEE 802.11i protocol [5] that will allow the vehicles to access the backbone network. The IEEE 802.11i protocol will ensure the authentication and authorization as well as confidentiality of data for the vehicles. However, this security mechanism will only protect the access link between the vehicle and roadside unit. In the wireless backbone the data is transmitted through multiple hops. As a result, an adversary can eavesdrop in the backbone link when the data is flowed through the vehicles unless there is some security primitives present to protect the backbone link. In a use case scenario, where two vehicles V_a and V_b are communicating with each other over the RSU network. V_a and V_b can communicate securely to the RSU backbone network. If the wireless link established in the backbone network is not protected, then an adversary can eavesdrop the traffic that is forwarded through the backbone network. Therefore, it is necessary to encrypt the data forwarded through the backbone network (RSU) as well to ensure the complete security of the system. In our proposed security architecture, the security of the backbone network (RSU) is ensured by exploiting the public key cryptography.

G. Network Data Protection

As discussed in the previous section, a security solution is necessary to protect the backbone network data provided by the RSU to ensure the complete security of the system. The vehicle data protection provides a secure and authenticated data exchange between the vehicle and the RSU. In this section we propose a security mechanism to ensure the security of the data in the backbone network as well. The proposed backbone network security architecture will use the pre-distributed public key to establish a secure network infrastructure. The main steps associated with the backbone network security architecture are illustrated as follows: *Initialization* – The first step is referred as the initialization phase or key pre-distribution phase. This phase is performed offline before deploying the wireless backbone RSU's. First, a master public key and the corresponding master private key will be generated which will be used for the communication with central Server (Administrator). The master public key will be stored in all the nodes memory and Admin has knowledge about the corresponding private key. Vehicles will use this master public key to establish a secure communication link with the Server. Following this based on some asymmetric key algorithm/public key algorithm the system administrator will generate a random public key and corresponding private key for each of the RSU in the network. Each RSU will store these random pair of keys before deployment. Let, N is the number of RSU in the backbone network. The system manager will generate N number of public keys (PU_1, PU_2, PU_3, …, PU_N) along with the corresponding private key (PR_1, PR_2, PR_3, …, PR_N); where PU_N defines the N-th public key whereas PR_N defines the corresponding private key. After the key generation is performed each pair of keys (PU_N, PR_N) will be assigned to a random RSU in the network. For example, RSU R_1 will be assigned a pair of key (PU_1, PR_1) where PU_1 is the public key and PR_1 is the private key for this node. System administrator will enable each RSU to store the public keys of all other RSU's in the network and the corresponding ids. In V2X, each vehicle can know exactly about its neighboring vehicle identity. Therefore, each vehicle will store the information of their neighbor vehicles identity before the deployment with the help of system administrator. Finally, system administrator will register these entire groups of

RSU's to the Server. The registration needs to be performed in person or by means of some secure communication. After the registration Server will have the information of all authorized RSU's id and their public keys.

Establishing a secure backbone network – In this phase, a secure and authenticated communication through the multi hop wireless backbone network is formed where the vehicles are pre-initialized with some secret information without having any direct contact with each other. The authentication is provided by means of digital signature using the private key of a RSU. When sending data to the next hop RSU, the sending node (RSU) will encrypt the data first by using sending nodes private key and further encrypt it by using the public key of the receiving node. Once the intended receiver receives the message, it will first decrypt the message by using its own private key followed by decrypting it with the public key of sending node. The encryption with the public key ensures the confidentiality of the message since the node for which it is intended for can only decrypt the message; this is because only the intended receiving node has the knowledge of the corresponding private key. On the other side, authentication of the message is ensured by encrypting the message with the sender's private key, this encryption with the private key of sending nodes provide a digital signature which guarantee the origin of data. To support the addition of new vehicles the advantage of digital signature is exploited in the proposed architecture. When the system deploys a new vehicle in the network it will first have to register with the server through the help of system administrator. The administrator will store the information (e.g public key, node id) of the newly deployed vehicle to the memory of the Server through some secure communication. Once the registration process is completed, Server will flood the information of the newly deployed vehicle to the entire network. When flooding the information, the confidentiality of the message will be protected by the use of the receiving nodes public key. The message will be digitally signed by using the master private key to ensure the authenticity of the origin. Each and every other vehicle will store the newly deployed vehicles information and confirm it as an authorized member of the network. The newly deployed vehicle can then communicate with other vehicles in the network once it is recognized as an authorized vehicle.

H. Data Privacy and Secrecy

Personally identifiable information, such as location data, address books and credit card numbers, is now entering and leaving the limits of the vehicles, requiring appropriate privacy controls and anonymization of data. As automakers and third parties create a faultless experience and increase the level of vehicle personalization, cars are becoming an extension of, or addition to, smartphones, home automation systems, entertainment libraries and other components of the digital life, syncing and strong user data.

There are two important aspects of data privacy: confidentiality of personal data and leaking of data outside the consumer's control. To maintain confidentiality, data needs to be protected by encryption inside and outside the vehicle while it is stored, transmitted and by memory protection extensions while it is being processed. Cyber criminals have been known to attack and steal data in all three locations. This includes not only stored personal information, such as address books or credit cards but also style of driving, current location, previous destinations and other metadata. For data leakage, there is a need to validate what data is stored, secure storage of data, destruction of data upon expenses against unauthorized access to ensure observance with information privacy laws.

I. Way of networking for Internet on vehicles

In simple terms, linked car is a road vehicles prepared with three sets of communication system: Internal access, and also an internal network, usually wireless, which enables the car to route its connection access to other devices that are installed inside and possibly outside of the vehicle. Alongside these typically there is Controller Area Network (CAN) bus used to interconnect the scale of ECUs, sensors and actuators that now from part of vehicle's inner electronic workings. Internal access or internal network to provide additional driver benefits: automotive notification of collisions, notification of excessive speeding and other safety alerts. There are two additional communication types that could supplement these. The more mature of these is vehicle-to-vehicle (V2V) technology that enables car to communicate wirelessly and even maintain temporary networks between

vehicles that can inform accident prevention, road hazards and other driving intelligence. A number of automotive OEMs (Original Equipment Manufacturers) are reported to be developing V2V capabilities.

However, there exist a number of cyber-security concerns associated with the V2X. These security concerns are needed to be analyzed in detail in order to design appropriate security mechanisms and overcome security problems that arise in wireless network. In this section addresses the underlying security challenges of V2X, which make the design of new security protocol more complicated. Main constraints in V2X are listed below.

J. Resource Constraints

A V2X network is formed between the vehicles and the road side units (RSU). There is dynamic change of flow of link so ad-hoc network provides varying resources. The client nodes have limited computational power and energy resources, which makes it difficult to implement heavy security infrastructure.

K. Mobility

In V2X, network vehicle nodes can be highly mobile which can produce latency in the convergence of the network. In addition, the mobility of vehicle nodes imposes severe challenge to authenticate the user and to ensure the security of vehicles.

L. Available bandwidth

The vehicles in V2X environment have limited available bandwidth for communication. Security is always a critical step to deploy and manage V2X. However, these constraints of V2X as well as their network architecture pose new challenges in achieving security goals. To provide security it is necessary to encrypt the message sent among communicating nodes. In V2X vehicles need to agree on an encryption key to establish a secure communication. Agreement of the encryption key in a communication network can be viewed as a part of the key management problem, which is one of the most important tasks for network security. However, achieving such key agreement in a resource constrained environment, as V2X is not a trivial task as security protocols always require additional overhead on the computational, storage and energy resources. Moreover, the key management for V2X becomes much more difficult, because there is no central authority, trusted third party or server to manage security keys. Several key agreement schemes have been proposed so far to ensure security in V2X. Some of the schemes are very effective in terms of security, but quite complex to apply in real world environment. Thus, there is a need for a better security system which can combine low operational costs with a high security performance.

III. SECURITY ISSUES IN FTS

In FTS system there are a lots of issues which is related to-

1) *Hardware Security*
2) *Software security*
3) *Network Security*
4) *Cloud Security Services*

In this paper we focus on data security with the help of Network security algorithm where data is affected from unauthorized person.

In FTS network security related to-

- Protecting messages and data over the communication related to location history, Navigation history, call history and microphone records.
- Enforcement of predictably holistic behavior of all devices that means restrict network can communicate to other system in predefined behavior.
- Access control

IV. PROPOSED ALGORITHM

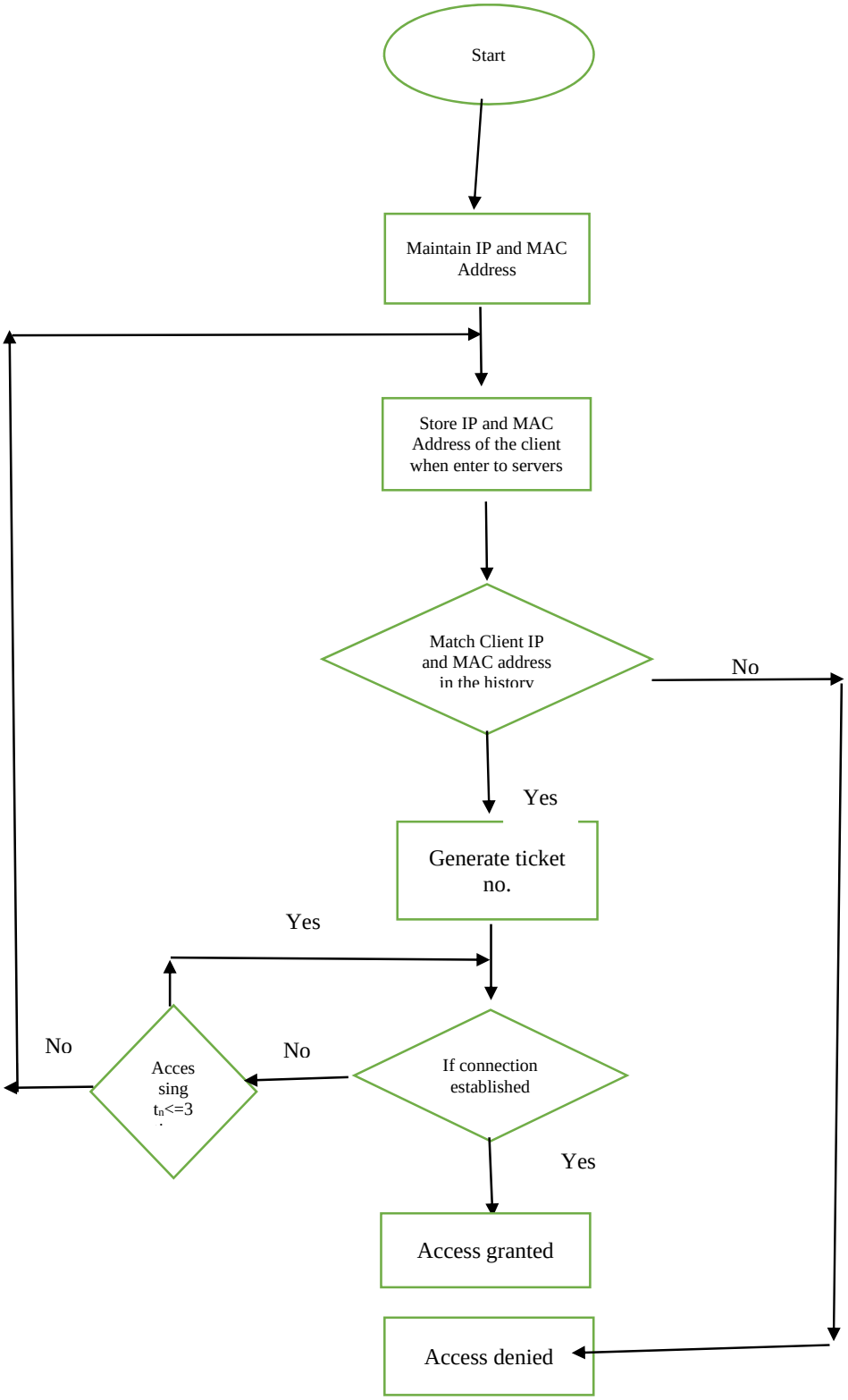
I_H = Maintain IP address History
M_H= Maintain MAC address History
I_U= Store each client IP address
M_U= Store each client MAC address
t_n= ticket number

```
If (IH== IU && MH == MU)
{
Generate Ticket number (tn)
        If (connection==yes)
        {
        Print: (Access granted);
        }
        Else
        If (use tn <=3 times &&
connection== yes)
          {
          Print: (Access granted);
          }
          Else
                {
          Repeat all process.
                }
```

}
Else
{
Print: (Access Denied);
Add the user IP && Mac address to the attacker list
}

V. IMPLEMENTATION

Basic function of proposed algorithm-



VI. FINAL REMARKS

In this paper discuss the prevention of cyber-attack into an automotive network connectivity between vehicles. Therefore, several researcher been introduced several novel mechanism by collecting the necessary information about physical environment, cyber system. Even though, the main problems of automobiles are being attacked by making the automobiles redesigned so that they can operate decisions. By executing such decisions, we can avoid the major consequences of vehicles being attacked.

There are several point which we should consider to design an algorithm and protocol.

A. Advanced Driver assistant systems

Collision avoidance, lane departure warning, adaptive cruise control, smart lighting control and parking assist.

B. Smart transportation

Vehicle sharing, traffic congestion and fuel efficiency are influencing and creating new troubles. Vehicle-to-infrastructure and vehicle-to-vehicle communications, traffic management are the main contributions so that many of the problems can be avoided.

C. Autonomous driving

The main goal of upcoming vehicles in future generation will be a driver less car. This will be a great contribution for modern upcoming vehicle so that a major problem of physical accidents to be avoided. In reality there will be zero collisions, improved sensible traffic and other benefits which were already visible from Google, tesla and others. The innovating automobiles will have an inbuilt security solutions and architectural design so that they make a decision themselves to minimize the emerging threats and accidents.

D. Security in automobiles

For suppose if you are connected to internet, then it is said that you are exposed to a number of malicious activities. When getting into detail your modern vehicle is assured with a scope of being threatened and will be left unprotected unintentionally. When we look into a car in which we have a ECU s of about 100, they are about to reach the upper boundary of the wiring harness. To reduce this, all the upcoming industries and software are hereby with a conclusion that to approach to virtualization along with necessary integration. They are with an idea that with reducing the ECUs along with increasing the functions and complexity of the software which results in the increase in the wide range of external networks and increasing Wi-Fi and cellular network, internet to service garages, troll roads, drive-through-windows, gas stations and rapidly growing list of automobiles and after marketing applications. It is complex that the security which we are going to be done with collaborative effort and should be done with a supply chain and the broader ecosystem. This can be done by hacking cars. This success of hacking cars can be done by depending on three major categories. Which include remote attack, cyber physical features and in-vehicle network architectures. Now a days we can see the CAN bus and the on-board diagnostics, are designed to be robust and are available readily. This is advanced system of a featured car with more potential attack vectors.

E. Cyber security threat agents, models and motivations

Understanding the objectives, motivations and the action to be done by a potential attacker and a threat agent will be a major step in improving the posture of a security if for a physical location of a computer. The Intel IT threat assessment group had developed the threat agent library and threat agent risk assessment usage model just to know the standardized reference and human agents that can be posed to threat the computer systems and much other information which were stored in a particular computer.

F. Researchers and hobbyists

Researchers and hobbyists are the first hackers to attempt an attack with the new device as they are funded by government labs universities and defense advanced research projects agency (DARPA). Their main motivation is initially positive and they access to conduct their research as they have a plenty of time. They will highlight the hacking skills which results in an idea for others to know the amount of hacking in a particular machine.

G. Pranksters and hacktivists

They will stand as a typical represent of a dark side as they take opportunity to demonstrate their skills and complexity of the outcomes and the requirement of special tools and skills and will make available by criminals or nation-states with greater resources.

H. Owners and operators

They use smart phones and other electronics to create a scope for being attacked. Since some automotive systems are safety critical, modifications can be controlled with appropriate security functions.

I. Organized crime and nation states

Organized crime is a major threat to vehicles as their main motivation is financial gain. So this malicious actor always looks for an easy way of stealing cars. Denial-of-service (DOS) followed by malware, ransom ware attacks targeted at specific entities. The individual cars in a disrupting traffic will create havoc for financial or political gain. Whereas, the nation-states' target is not easy to determine. They target a car so that they can track and audio monitoring. So that they can make some financial benefits.

REFERENCES

[1] Hiro Onishi, "Guidelines for Vehicle Cyber Security", 2014 SAE International World Congress, Detroit, Michigan USA, 2014.

[2] Raya M, Aziz A, Hubaux JP. Efficient secure aggregation in VANETs. ACM; 2006a. p. 67-75.

[3] Raya M, Hubaux JP. Securing vehicular ad hoc networks. Journal of Computer Security. 2007;15:39-68.

[4] Fantacci, L. Maccari, T. Pecorella, F. Frosali, A secure and performant token-based authentication for infrastructure and mesh 802.1X networks, in: Infocom'06 Poster Session, April 2006.

[5] D. Singh and M. Singh, "Internet of vehicles for smart and safe driving," 2015 International Conference on Connected Vehicles and Expo (ICCVE), Shenzhen, 2015, pp. 328-329. doi: 10.1109/ICCVE.2015.93

[6] Song J-H, Wong VWS, Leung VCM. A framework of secure location service for position-based ad hoc routing. Proceedings of the 1st ACM international workshop on Performance evaluatio of wireless ad hoc, sensor, and ubiquitous networks. Venezia, Italy: ACM; 2004. p. 99-106.

[7] Szczurek P, Xu B, Wolfson O, Lin J, Rishe N. Learning the relevance of parking information in VANETs.

[8] Proceedings of the seventh ACM international workshop on VehiculAr InterNETworking. Chicago, Illinois, USA: ACM; 2010. p. 81-2.

[9] Zeadally S, Hunt R, Chen YS, Irwin A, Hassan A. Vehicular ad hoc networks (VANETs): status, results, and challenges. Telecommunication Systems. 2010:1-25.

[10] Zhang Y, Lee W, Huang YA. Intrusion detection techniques for mobile wireless networks. Wireless Networks. 2003;9:545-56.

[11] Tang L, Hong X, Bradford P.J.P. Hubaux, B. Levente, and C. Srdjan. "The quest for security in mobile ad hoc networks", Proc of the 2001 ACM International Symposium on Mobile ad hoc networking and computing 2001, Long Beach, CA, USA, pp.146-55, 2001.

[12] C. Srdjan, N. Levente, and J.P. Hubaux. "Self-organized public-key Management for mobile ad hoc networks", IEEE Transactions on mobile computing, vol.2, no.1, pp. 52-64, Jan-Mar. 2003

[13] L. Zhou, and Z. J. Haas. "Securing ad hoc networks", IEEE Networks Special Issue on Network Security, vol.13, no.6, pp.24-30, Nov/Dec. 1999.

[14] J. Dong, K. E. Ackermann and C. Nita-Rotaru, "1)Secure Group Communication in Wireless Mesh Networks," . In Ad Hoc Networks (Elsevier) Journal, Special Issue: Privacy and Security in Wireless Sensor and Ad Hoc Networks, Nov 2009

[15] Y. Sun, W. Trappe, and K. J. R. Liu, "A scalable multicast key management scheme for heterogeneous wireless networks," IEEE/ACM Trans. Network, vol. 12, no. 4, pp. 653-666, 2004

[16] S. Zhu, S. Setia, S. Xu, and S. Jajodia, "GKMPAN: An efficient group rekeying scheme for secure multicast in ad-hoc networks," Mobiquitous, vol. 00, 2004.

[17] M. Singh, D. Singh and A. Jara, "Secure cloud networks for connected & automated vehicles," 2015 International Conference on Connected Vehicles and Expo (ICCVE), Shenzhen, 2015, pp. 330-335. doi: 10.1109/ICCVE.2015.94.

[18] Kim, Kyoung-Dae, and Panganamala R. Kumar, "Cyber–physical systems: A perspective at the centennial." Proceedings of the IEEE 100.Special Centennial Issue (2012): 1287-1308.

[19] V.Priyadharshani,Dr k.Kuppusamy ,"Prevation of DDOS Attack using New Crackingg Algorithm." IJERA Vol. 2, Issue 3, pp.2263-2267, May-Jun 2012 .