ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

Review on Several Kind of Attacks in Vehicular Ad Hoc Networks

Priya Agrawal[1], Dushyant Singh[2]

M. Tech Scholar, Department of CSE, Chandravati Group of Institutions, Bharatpur, Rajsthan, India[1]

Asst. Professor, Department of CSE, Chandravati Group of Institutions, Bharatpur, Rajsthan, India[2]

ABSTRACT: Vehicular Ad-Hoc Networks (VANETs) is an indivisible I.T.S component, where nodes are self-organizing, autonomous and self-managing information in a distributed manner. Its foundation is based on the vehicles co-ordination and/or roadside units by which information is distributed in network in organized manner. In recent years, VANET has been obtained more attention of automotive industries and researchers because of life saving factor. But always coin has two faces, when we know about its life saving factors simultaneously security attacks for VANET is also arises, so now VANET requires security to implement the ad hoc atmosphere and serves subscribers with safety and commercial applications. In this paper, we have performed a review of attack on network existence and its severity levels in VANET atmosphere, which called as Denial of Service (DOS) attack, along with that several type of hybrid Denial of Service attack is also available in it with their available solutions

KEYWORDS: AODV, DSR, MANET, VANET

I. INTRODUCTION

In today's scenario congestion caused by vehicle crashes is assumed to be an issue of great significance on the roads. Due to that, applications associated to driver's safety are the concentration of most researchers, who are working in the field of VANET systems. As a result, efficiency of these applications is enhanced and has a good effect on network to restricting the no. of accidents on road and offers cleaner, comfortable and safer travelling. Drivers on road have no capability to predict the situations on the road coming ahead [1]. But now with the support of computer equipment, sensors and wireless communication devices along with an integration of advanced technically fitted devices it is possible to offer method by which vehicles nodes on the roads can its neighbor vehicles speed and predicts possible risk coming ahead [2]. By the usage of such technique, vehicle could forward alerting messages periodically to its neighboring nodes to predict their speed for avoiding chances of accidents on road [3]. Due to high travelling nodes speed in VANET network; dynamic network configuration and high mobility are unique features of VANET. Because of this some issue is faced by vehicle nodes in a network i.e. restrictions of bandwidth because of the unavailability of central coordinator that maintains and control communication among nodes, signal fading, and disconnection issues because of frequent network fragmentation. Security problems in VANET is a significant prospective in today's scenario due to the rapid development and increasing the usage of VANET. One of the most severe attacks in VANET is Denial-of service (DoS) attack, because it attacks on the network availability which causes life threatening impact on vehicle's drivers, a means of preventing these attacks must be determined as soon as possible because the primary aim of the intruder is to interrupt the communication channel or overwhelms the vehicle's existed services from the original subscribers. Attack builds the system useless and this system uselessness in real-time vehicular networks even for a small time instant is very harmful. Traffic fatalities have been increasing across the world. The National Highway Traffic Safety Administration (NHTSA) statistics presents that in 2012, there were over 30 thousand fatal crashes in which, drivers, passengers and even pedestrians were influenced. The no. is still increasing because of continually issuing driving licenses and more vehicles being bought. In 1994, there was over 190 thousand vehicles registered and 175 thousand licensed drivers. These numbers jumped in 2012 to more than 265 thousand registered vehicles and 211 thousand licensed drivers [15]. These numbers have represented a direct relation with the no. of fatalities. As a result, the requirement to have safer roads began to arise to decrease money and lives losses.

Combining cars with computers was the first step toward decreasing fatalities. Fitting vehicles with computers to scan and control car's components supports drivers to determine problems in their cars, e.g., engine failures and enhances

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

safety by offering an early warning of cars malfunction. Computers in cars first seemed by Chevrolet in 1975. Soon after that, some cars' manufacturers began following the technology and combining new systems to vehicles. Doing so, permitted several systems to be standardized i.e. Electronic Control Unit (ECU). ECU consists of several modules that control different electrical systems or subsystems in motor vehicles: Transmission Control Module (TCM), engine control module (ECM), Brake Control Module (BCM), is systems referred at as car's computer [6] [14].

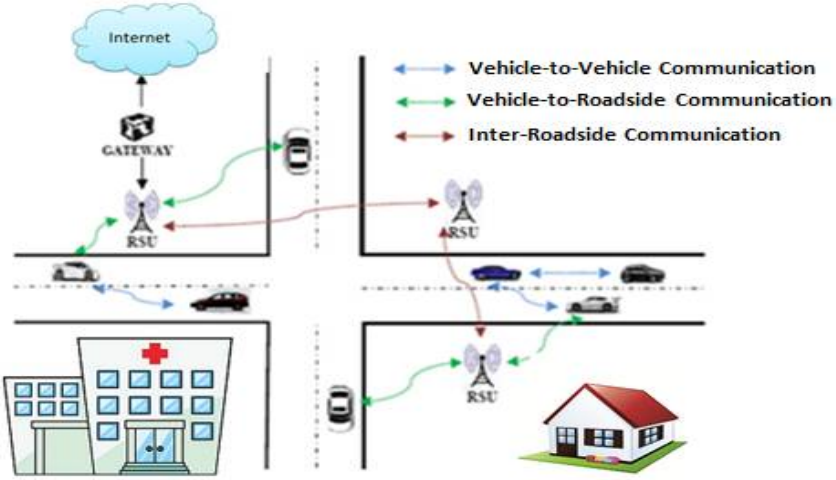

Figure-1 Vehicular Ad-hoc network

While deploying ECU in cars increases the driving safety and quality, it only supports drivers to determine car's internal malfunction. That's because ECU can only offer information related to different cars parts. ECU cannot inform external hazards that are significant to take into counts; weather changes, road hazards and accidents on roads are only some instances of external factors that influence drivers' safety.

VANET promises a secure atmosphere for everyone who shares the road, by warning pedestrians, vehicles and motorcyclists to avoid fatality. The warnings are created by gathering data from VANET nodes and offer alerting messages to nodes that are in impacted areas or routing toward it. In addition, VANET increases comfort by permitting traffic congestion detection, automatic toll collection, emergency dispatch facilities, and electronic inspection of moving trucks through data transmissions with roadside inspection services [11]. VANET proved how useful these alerting messages to avoid crashes, safe lives and improve driving experiences.

Jamming attacks can influence VANET existence, because a jammer can block alerting messages such as road hazard, accident warning, emergency vehicle etc. The consequences of not obtaining these messages can result in failing to slow down, rerouting or stopping the vehicle, which can jeopardize passengers and drivers' safety. It is complex to determine jamming reliably and the effect can be devastating. Thus, Jamming is an open issue. This paper reviews the security problems that VANET may encounter in specific Jamming attack. Simultaneously, it reviews current and different solutions for jamming attack in other kind of networks and represent the specialty of coping jammers in VANET.

II. BACKGROUND

VANET, a kind of ad hoc networks, is an infrastructure-less and self-organized network. In this kind of networks, mobile devices are linked together wirelessly [10]. Every mobile device (known as a node) behaves as both data terminal and router. Nodes in the network utilize the wireless medium to interact with neighboring ones within range. These nodes can be roadside units (RSUs) or vehicles in VANET.

The discovery of VANET seemed after the wireless data networks proliferation because of the recent adoption of the several 802.11. Wireless LANs are broadly deployed and the cost for wireless resources is decreasing. 802.11 adapters or access points (AP) can be bought for next to nothing. As a result of the high acceptance of the 802.11 standards, commercial and academic sectors concentrated on determining other applicable wireless techniques. Thus, Mobile ad-hoc network (MANET) is one field that has obtained considerable care which yield to VANET development. VANET

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

and MANET are very same at the network level yet the details distinguish. They key difference is that MANET nodes move arbitrarily whereas in VANET, vehicles move in an organized way. The benefit of utilizing ad hoc networks is to permit the deployment in fields where it is not possible to install the required infrastructure. It would be costly and unrealistic to install 802.11 access points to cover all the roads in The United States for instance. Another benefit of ad hoc networks is how quickly and easily they can be deployed without administration involvement.

III. VANET REQUIREMENTS AND SECURITY CHALLENGES

So far, VANET security has not achieved enough attention even though it is very essential. The criticality lays on the VANET' packets contents which contains important life information. So it is significant to ensure reliable packets delivery in the network without alteration. To do so, security challenges require be addressing and assuming when designing VANET architecture [7].

VANET must meet the security needs before deployment. In this section, we show the security needs that must be considered. Some attack scenarios will be provided to prove the powerful fatality when attacks are launched by antagonists.

3.1 Availability: Availability needs all facilities that the network provides to be existed when required by legitimate users. One harmful attack is DoS.

3.2 Confidentiality: Confidentiality provides protection for nodes against unauthenticated ones to avoid messages delay attack. A weel-known attack that intends confidentiality is Eavesdropping.

3.3 Authentication and Identification: This need assures that subscribers and messages in the network are legitimate. Impersonation and Sybil attacks are very famous to target and harm this need.

After surveying the security needs that VANET should meet when deployed, we conclude that security is very significant in VANET. Furthermore, securing all communication and ensuring attack-free atmosphere is not an easy job because of the high mobility and the network configuration. Thus, Research is still on going to defend more fields of VANET communications.

IV. SECURITY ATTRIBUTES

In the following subsections, we show security attributes in Vehicular Ad hoc Networks (VANETs) and kinds of malicious vehicles.

A. Security Attributes: There are various significant needs to obtain security in VANETs, which are explained as follows. [17].

Authentication: Vehicles should reply only to the messages transferred by legitimate network members. Therefore, it is very significant to authorize the message sender.

Data Verification: Once the sender vehicle is authorized the obtaining vehicle performs data verifications to examine whether the message contains the correct or disrupted data.

Availability: The network should be existed even if it is under an attack utilizing alternative techniques without influencing its performance.

Data Integrity: It assures that messages or data are not modified by intruders. Else, users are directly influenced by the modified emergency data.

Non-repudiation: A sender must not refuse a message transmission whenever an investigation or vehicle identity is needed.

Privacy: The profile or a driver personal information must be managed against unauthenticated access.

Real-time constraints: however, vehicles are linked to VANETs for a short time interval, real-time restraints should be managed.

B. Types of Malicious Vehicles: In VANETs, malicious vehicles introduce attacks on legitimate vehicles in various ways. Therefore, malicious or intruder vehicles are categorized as follows.

Insiders Vs Outsiders: In a network, a member node which can interact with other network members is called as an Insider and can attack in several ways. Outsiders who cannot interact directly with the network members have a restricted capacity to attack (such as have less variety of attacks).

Malicious Vs Rational A malicious intruder utilizes several methods to destroy the member nodes and the network without seeing for its personal advantage. In opposite, a rational intruder expects personal advantage from the attacks. Therefore, these attacks are more predictable and adopt some patterns.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

Active Vs Passive: An active intruder can create new packets to destroy the network while a passive intruder only eavesdrop the wireless channel but cannot create new packets (such as less harmful).

V. SECURITY ATTACKS AND APPROACES

In this section, we show various security threats on Vehicular Ad hoc Networks (VANETs), and defending approaches of some of these attacks [7, 9, 17, 19, 20, 24].

Bogus Information: Intruders may transfer wrong or bogus information across the network for their benefit. For example, an intruder may transfer incorrect information about the traffic conditions for making its movement easier on the road. This attack is associated to the authentication security needs.

Elliptic Curve Digital Signature Algorithm (ECDSA) [16] is a message authentication technique that utilizes hashing technique to hold messages more protected and offers strong authorization for the destination vehicles. This technique works by creating private and public keys from the source vehicle.

Denial of Service (DoS) Attackers may transfer dummy messages to jam the channel and therefore, decrease the efficiency and network performance. The Distributed DoS (DDoS) is more critical as compared to the DoS where a no. of malicious cars attack on a legitimate car in distributed way from various timeslots and locations. Fig 3 presents that a no. of malicious black cars attack on V1 from several locations and time so that V1 cannot interact with other vehicles.

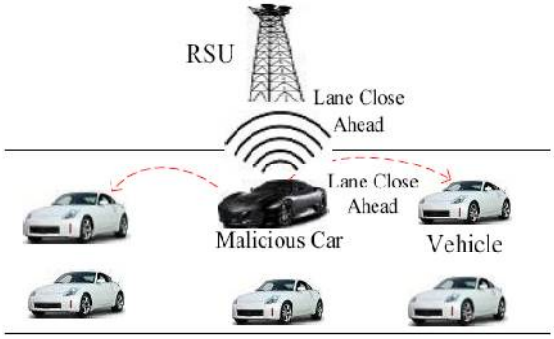

Figure 2: Denial of Service (DOS) Attack

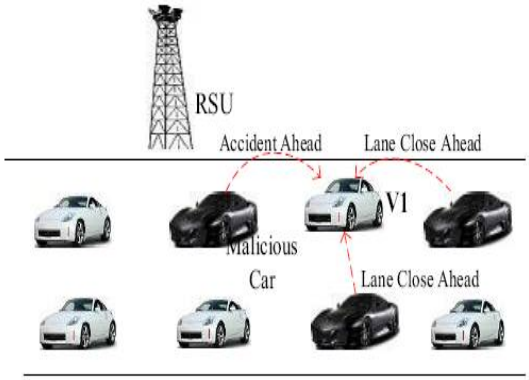

Figure 3: Distributed Denial of Service (DDoS) Attack

Masquerade A vehicle fakes its identity and acts to be another vehicle for its own benefit. It is obtained utilizing message fabrication, alteration, and replay. For example, a malicious vehicle or intruder can act to be an ambulance to defraud other vehicles to slow down and yield.

Black Hole Attack: A black hole is a network area where the network traffic is redirected. Since, either there is no node in that region or the nodes stays in that region deny to participate in the network. This causes data packets to be dropped. Fig 4 shows a black hole attack where the black hole is made by a no. of malicious nodes, which denies to transfer the messages obtained from the legitimate cars C and D to the cars E and F.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

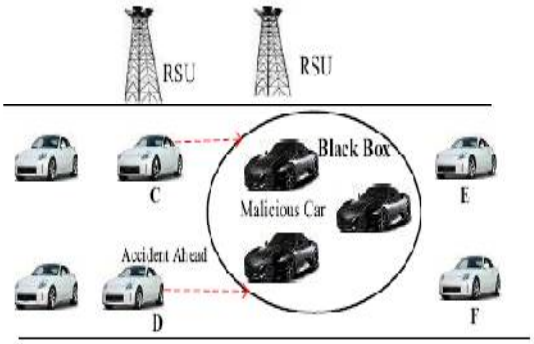

Figure 4: Black hole attack

Malware and Spam Malware and spam attacks i.e. spam and viruses can cause critical interruptions in the normal VANETs operations. Spam and Malware attacks are generally executed by malicious insiders instead of outsiders whenever on board units (OBU) of vehicles and road side units (RSUs) perform software updates. These threats increase transmission latency, which can be reduced by utilizing a centralized administration.

Timing Attack Transferring data at the correct time from one vehicle to another vehicle is importantly significant to obtain data security and integrity. In timing attacks, whenever malicious vehicles obtain any important message they do not send it to the nearby vehicles at the correct time but they add some timeslots to the actual message to generate delay. Therefore, neighboring vehicles of the intruders obtain the message after they really need it.

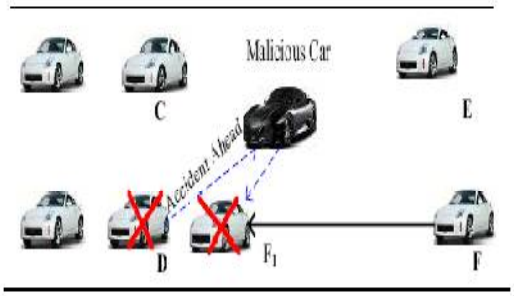

Figure 5: Timing Attack

Man in the Middle Attack (MiMA) In this attack, malicious vehicles hear to the interaction among vehicles and introduce false information among vehicles. Fig 6 shows a MiMA attack where the malicious vehicle C hears to the interaction between vehicles B and D as well as forwards incorrect information to the vehicle E that C obtains from the vehicle A.

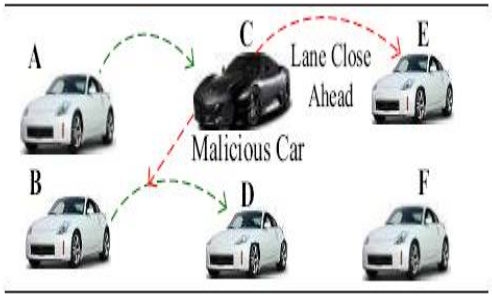

Figure 6: Man-in-the-Middle Attack

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

Sybil Attack: In Sybil attack [4, 25], an intruder creates many identities to simulate multiple nodes. Every node transfers messages with several identities. Therefore, other vehicles feel that there are several vehicles in the network simultaneously. This attack is very harmful however a vehicle can claim to be in different locations simultaneously , thus generating chaos and large security risks in the network.

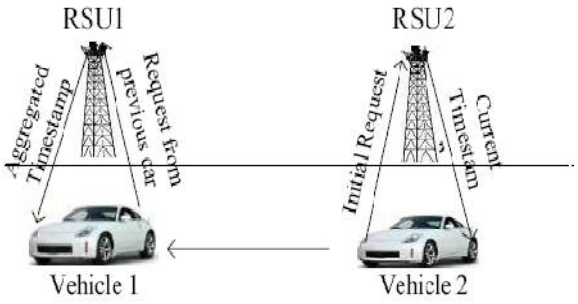

Figure 7: Timestamp series approach

Timestamp series technique is another mechanism to secure VANETs from Sybil attacks [25]. This technique works well for an initial development phase of VANETs with the existence of the RSU infrastructure and only a small no. of vehicles with communication abilities. The RSU issues digital certificates to every vehicle that passes through it and considers that two vehicles cannot pass several RSUs simultaneously. Therefore, a Sybil attacker node is determined if a vehicle obtains multiple messages with the very similar timestamp certificates. This mechanism is also economic however it does not utilize computational expensive public key infrastructure (PKI) or Internet accessible RSUs. Fig 7 shows the working scenario of timestamp series mechanism.

Wormhole Attack: Wormhole is a critical attack in VANETS and other ad hoc networks. In this attack, two or more malicious nodes generate a tunnel to transfer data packets from one network end to the malicious node at the other end and these packets are flooded to the network. The malicious nodes take the control of this short network link or connection, threaten the security of transferring data packets and remove them.

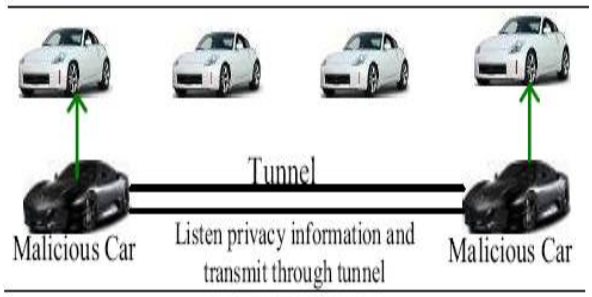

Figure 8: Wormhole Attack

Packet leash [12] is a famous technique to prevent wormhole attacks. For example, TIK is a packet leashes- based protocol for determining and protecting against wormhole attacks. Temporal leashes assure that every packet has an upper bound of distance to travel (which is at most at the light speed). All nodes are tightly synchronized with a clock and the clock difference between any two nodes is known by all other network nodes. The TIK protocol utilizes asymmetric cryptography to offer an instant authorization of the obtained packets where it utilizes n public keys for n nodes and hash functions for holding up-to-date keys information and obtained packets. An attack is determined by computing the differences among the packet travel distance and permitted distance to travel.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

VI. CLASSIFICATION OF SECURITY SCHEMES

Available security and privacy techniques of Vehicular Ad hoc Networks (VANETs) can be categorized into the following classes.

A. Public Key Approaches: In these techniques, every node is offered with a pair of public and secret keys. Public Key Infrastructure (PKI) should effectively handle key management to offer security. A scheme utilizing PKI is suggested whenever a vehicle has two additional hardware units: Event Data Recorder (EDR) to store all events and Tamper Proof Hardware (TPH) to perform cryptographic procedure.

The work performed by Chim, T.W et al. [8] introduces a dynamic key distribution protocol that manages key management without the requirement to save a huge no. of keys for PKI support and therefore, decreases the uses of Tamper Proof Device (TPD). In this technique, vehicles unique information i.e. Electronic license Plate (ELP), chassis no. that generates Vehicle Authentication Code (VAC) is utilized a secret key between vehicle and a certificate authority (CA). A CA is responsible for issuing, distributing, renewing and revoking public key certificates [1].

Efficient Certificate Management Scheme (ECMV) [27] is a PKI-based approach, which offers an effective certificate management among different authorities and thus, the OBU can update its certificates anywhere at any time. Even if the antagonist maintains to get into the network, ECMV has an effective certificate revocation process to remove the antagonist. This scheme decreases the certificate management complexity to a great extent and is very efficient in offering scalability and security.

B. Symmetric and Hybrid Approaches: In these approaches nodes interact after they share and agree on a secret key that is utilized for communication.

Most security techniques of VANETs depend on either symmetric or public keys. Recently, a hybrid system that utilizes both public and symmetric keys has been introduced for security in VANETs. It utilizes two kinds of communications: pair-wise and group communication. Pair-wise communication is utilized when two vehicles require interacting each other while in group communication more than two vehicles interact. Hybrid mechanisms utilize symmetric keys for pair-wise interactions to avoid the overhead of utilizing the key pair. Since, symmetric keys should not be utilized in the authorization procedure however it prevents non repudiation. The key size is 1024 bits and AES is employed for encryption.

C. Certificate Revocation Approaches A public key infrastructure (PKI) is broadly utilized to offer security in VANETs which involves certificate revocation (such as terminating the vehicle membership) [1]. Certificate revocation is done by CA in two ways: centralized or decentralized. In the centralized technique, a central authority is responsible only for taking the decision of revocation while in decentralized technique; a group of vehicles which are neighbours of the revoked vehicle take such a decision.

D. ID-based Cryptography: symmetric key cryptography and Public Key Infrastructure (PKI) are not the best techniques to offer security in VANETs however, they are infrastructure-less. Thus, ID-based cryptography that deals with the best characteristics of other security techniques is also being explored by the research community. For example, ID-based cryptography decreases the computational cost in the ID-based Signature (IBS) procedure for VANETs, and is preferable for authorization utilizing the ID-based Online/Offline Signature (IBOOS) technique. IBOOS increases efficiency by separating signing procedure into an offline (executed initially at vehicles or RSUs) and online phase (executed in vehicles during V2V communications), in which the verification is more effective as compared to IBS.

The work performed by Nafi, N.S.; et al. [20] suggests an ID-based authentication framework that uses both IBOOS and IBS. This framework uses self-defined pseudonyms r ather than real-world IDs without showing vehicles privacy. This framework is effective in term of storage, processing time and communication overhead. This is because this approach preloads a pool of IDs of regional RSUs in every vehicle, which are very small in size and do not change quickly in comparison of other techniques that pre-stores IDs of all RSUs. This technique utilizes IBS for Vehicle-to-Roadside (V2R) and Roadside-to-Vehicle (R2V) authentications while IBOOS is employed for V2V authentications. Evaluation results present that this framework effectively preserves the VANETs privacy.

VII. CONCLUSION

Vehicular Ad hoc Networks (VANETs) are becoming famous in transportation systems however they offer traffic management, road safety and Internet access on highway and disseminate safety information to passengers and drivers. Since, it poses a great challenge to implement VANETs in value-added services because of the attacker vehicles and

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

various security attacks. Therefore, offering privacy and security in VANETs are considered as the most significant research issue in this field.

In addition, vehicles mobility and dynamic behavior of the network impose a significant challenge to remove malicious vehicles and design protected data transmission protocols. Though extensive researches are being performed to offer privacy and security in VANETs most of these techniques consider decreasing computational and communication overhead, and processing delay for authorization between the source and target vehicles.

- Distributing certificates securely, validating them very quick and computationally effective way should be provide more attention while designing protected routing protocols for VANETs.
- Determining the mobility pattern of vehicles and connecting the mobility pattern with malicious vehicles could be taken as a powerful research in offering privacy and security in VANETs.
- Determining and allocating trust values to vehicles and making trust between vehicles are importantly significant to offer the reliability and integrity of applications in VANETs.
- The change of MAC addresses along with the pseudonyms has not obtained enough care. If the IP address changes with the pseudonym the MAC address should also change. Else, antagonists can easily track the target vehicle by its MAC address.

REFERENCES

[1] Himanshu Saini, Rajarshi Mahapatra, “Implementation and Performance Analysis of AODV Routing Protocol in VANETs”, International Journal of Emerging Science and Engineering (IJESE) ISSN: 2319–6378, Volume-2, Issue-3, January 2014.

[2]Kahina Ait Ali, Oumaya Baala, Alexandre Caminada, “Routing Mechanisms Analysis in Vehicular City Environment”,IEEE, 2011.

[3] Radityo Anggoro, Teruaki Kitasuka, Ryoji Nakamura, Masayoshi Aritsugi ,“Performance Evaluation of AODV and AOMDV with Probabilistic Relay in VANET Environments”,IEEE Third International Conference on Networking and Computing, pp. 259-263, 2012.

[4] Haiqing Liu, Licai Yang, Yao Zhang, “Improved AODV routing protocol based on restricted broadcasting by communication zones in large-scale VANET”, Springer, pp. 857-872, 2011

[5] Verma, K.; Hasbullah, H.; Kumar, A., "An efficient defense method against UDP spoofed flooding traffic of denial of service (DoS) attacks in VANET," *Advance Computing Conference (IACC), 2013 IEEE 3rd International* , vol., no., pp.550,555, 22-23 Feb. 2013

[6] Grzybek, A.; Seredynski, M.; Danoy, G.; Bouvry, P., "Aspects and trends in realistic VANET simulations, *Wireless, Mobile and Multimedia Network, 2012 IEEE International Symposium on a* , vol., no., pp.1,6, 25-28 June 2012

[7] Jie Li, Huang Lu, “ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs” , IEEE Transactions on Parallel and Distributed Systems, 2012

[8] Chim, T.W.; Yiu, S.M.; Hui, L.C.K.; Li, V.O.K., "VSPN: VANET-Based Secure and Privacy-Preserving Navigation," *Computers, IEEE* Transactions *on* , vol.63, no.2, pp.510,524, Feb. 2014[9] Yen-Wen Lin; Guo-Tang Huang, "Optimal next hop selection for VANET routing," *Communications and Networking in China (CHINACOM), 2012 7th International ICST Conference on* , vol., no., pp.611,615, 8-10 Aug. 2012

[10] Dalbir Singh and Manjot Kaur, “Mitigation of Sybil Attack Using Location Aware Nodes in VANET”, International Journal of Science and Research (IJSR), Volume 4 Issue 11, November 2015

[11]Jaydip Kamani and Dhaval Parikh, “A Review on Sybil Attack Detection Techniques”, Journal for Research, Volume 01, Issue 01, March 2015

[12] Kewei Sha, Shinan Wang and Weisong Shi, “RD4: Role-Differentiated Cooperative Deceptive Data Detection and Filtering in VANETs”, International Journal of Network Security & its Applications(IJNSA), Vol 3, No.6, 2010.

[13] Hamieh, A.; Ben-othman, J.; Mokdad, L., "Detection of Radio Interference Attacks in VANET," *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE* , vol., no., pp.1,5, Nov. 30 2009-Dec. 4 2009

[14] Lyamin, N.; Vinel, A.; Jonsson, M.; Loo, J., "Real-Time Detection of Denial-of-Service Attacks in IEEE 802.11p Vehicular Networks," *Communications Letters, IEEE* , vol.18, no.1, pp.110,113, January 2014

[15] Yeongkwun Kim; Injoo Kim; Shim, C.Y., "A taxonomy for DOS attacks in VANET," *Communications and Information Technologies (ISCIT), 2014 14th International Symposium on* , vol., no., pp.26,27, 24-26 Sept. 2014

[16] Verma, K.; Hasbullah, H.; Kumar, A., "An efficient defense method against UDP spoofed flooding traffic of denial of service (DoS) attacks in VANET," *Advance Computing Conference (IACC), 2013 IEEE 3rd International* , vol., no., pp.550,555, 22-23 Feb. 2013

[17] Li He; Wen Tao Zhu, "Mitigating DoS attacks against signature-based authentication in VANETs," *Computer Science and Automation Engineering (CSAE), 2012 IEEE International Conference on* , vol.3, no., pp.261,265, 25-27 May 2012

[18] Pooja, B.; Manohara Pai, M.M.; Pai, R.M.; Ajam, N.; Mouzna, J., "Mitigation of insider and outsider DoS attack against signature based authentication in VANETs," *Computer Aided System Engineering (APCASE), 2014 Asia-Pacific Conference on* , vol., no., pp.152,157, 10-12 Feb. 2014

[19] Durech, J.; Franekova, M.; Holecko, P.; Bubenikova, E., "Security analysis of cryptographic constructions used within communications in modern transportation systems on the base of modelling," *ELEKTRO, 2014* , vol., no., pp.424,429, 19-20 May 2014

[20] Nafi, N.S.; Khan, R.H.; Khan, J.Y.; Gregory, M., "A predictive road traffic management system based on vehicular ad-hoc network," *Telecommunication Networks and Applications Conference (ATNAC), 2014 Australasian* , vol., no., pp.135,140, 26-28 Nov. 2014

[21] Kumar, A.; Sinha, M., "Overview on vehicular ad hoc network and its security issues," *Computing for Sustainable Global Development (INDIACom), 2014 International Conference on* , vol., no., pp.792,797, 5-7 March 2014

[22] Mehta, K.; Malik, L.G.; Bajaj, P., "VANET: Challenges, Issues and Solutions," *Emerging Trends in Engineering and Technology (ICETET), 2013 6th International Conference on* , vol., no., pp.78,79, 16-18 Dec. 2013

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

[23] Nafi, N.S.; Khan, J.Y., "A VANET based Intelligent Road Traffic Signalling System," *Telecommunication Networks and Applications Conference (ATNAC), 2012 Australasian* , vol., no., pp.1,6, 7-9 Nov. 2012
[24]Performance Comparison Of AODV and DSDV Routing Protocols in Mobile Ad Hoc Networks, Aditi Sharma,Sonal Rana, Leena Kalia, International Journal of Emerging Research in Management and Technology, ISSN:2278-9359 Volume-3, Issue-7, July 2014.
[25] Ait Ali, K.; Baala, O.; Caminada, A., "Routing Mechanisms Analysis in Vehicular City Environment," *Vehicular Technology Conference, 2011 IEEE 73rd* , vol., no., pp.1,5, 15-18 May 2011
[26] Bhoi, S.K.; Khilar, P.M., "A secure routing protocol for Vehicular Ad Hoc Network to provide ITS services," *Communications and Signal Processing (ICCSP), 2013 International Conference on* , vol., no., pp.1170,1174, 3-5 April 2013
[27] Pathre, A.; Agrawal, C.; Jain, A., "A novel defense scheme against DDOS attack in VANET," *Wireless and Optical Communications Networks (WOCN), 2013 Tenth International Conference on* , vol., no., pp.1,5, 26-28 July 2013