Vehicular Ad-hoc Network (VANET) Challenges, Privacy and Security

[1]Sharda Rani, [2]Anjali
[1]Assistant Professor (Department of Computer Science), R.K.S.D College, Kaithal
duhan.sharda@gmail.com[1], anjali87dagar@gmail.com[2]

Abstract- VANET security shows that there are many mechanisms being developed to ensure that all security concepts are enforced and maintain a standard of efficiency for the operation of vehicular networks. These are an emerging infrastructure that makes use of vehicles as the main objects within a network. These networks use either peer-to-peer communications to communicate with other vehicle objects directly or a more centralized client/server approach to communicate with its road side infrastructures to authenticate, send or receive information. With this added ability implemented into modern and upcoming vehicles, the transportation infrastructure would greatly improve in terms of efficiency, safety and user-friendliness. Although communication introduces better ways of traveling, adding a network infrastructure to vehicles and their environments also introduces the possibility of security breaches inside the vehicles and respective surroundings through internal and external components embedded in Vehicular Ad Hoc Networks. It has been shown that multiple attack surfaces exist and proper defense mechanism must be implemented to properly secure and deploy this type of network.

I. Introduction

Vehicular ad-hoc network (VANET) is an advanced technology that uses vehicles (represented as nodes) to create a self creating network without any infrastructure and has provided an emerging platform for researchers and industrialists. VANET rely only on vehicles themselves in order to provide basic functionality of networks. The security of VANET has drawn a kind attention in today's world, because of wireless medium it is vulnerable to several attacks which affect the operations, so security is one of the main challenging issues and is mandatory for successful deployment of such technology. A robust VANET network strongly depends on secure communication and other privacy features. Vehicular Ad hoc Networks (VANET) is part of Mobile Ad Hoc Networks (MANET), this means that every node can move freely within the network coverage and stay connected.

II. Literature Review

This section presents analysis report of the current existing possible solutions that provides security to the VANET network. In this manner, we will discover the most significant trend and existing solution for each thread. Various securities have been proposed till now and many research articles were introduced to resolve these security problems of VANET discussed in this paper.

Public key Based approach This approach maintains message authentication, where vehicle sign message with the private key and also attached its certificates. At the receiving end, the verification of message takes place where receiver verifies the key that is used to sign the message and after verification it verifies the message.Author [8] discussed this approach and also uses ECC to reduce the network.

VPKI Based approach When vehicle send a message signed with its private key and also attached Certificate authority to it, at the receiving end receiver by using the certificate receiver can obtain the public key and then verify V's signature with the help of its certificate public key. This concept is used by various authors [7, 10, 12, 11, 8]

Certificate Revocation based approach This approach mainly deals with certificate revocation solutions to revoke the certificate using CRLs(Certificate Revocation Lists) which is expired so that other vehicles make aware of their invalidity and author also discussed that using CRLs we cannot get the appropriate solutions but using various protocols such as RTPD (Revocation Protocol of the Tamper-Proof Device), DRP (Distributed Revocation Protocol), and RCCRL (Revocation protocol using Compressed Certificate Revocation Lists) appropriate solutions can be achieved. All listed methods rely on monitoring only, so did not consider for reputation system, every vehicle has to be monitored carefully and also detects its neighbour vehicles.

Anonymous key Based approach In this approach privacy can be maintained by using some set of Anonymous keys that keeps on changing rapidly according to speed of driving. At the time only one key can be used and expires after its usage. Electronic License Plate (ELP) is used to preserve the real identity of driver and this will provide a unique identification number to identify vehicles anywhere [8].

Group signature Based approach There are two major issues of this approach. Firstly, this idea causes a great overhead when a new vehicle enters into the group and secondly, the mobility that prevents a network from making

a group static. Author in [18] discussed about Signcryption and group signature to achieve various security principles. Signcryption is used to encrypt a message and also used to enable a vehicle to join a RSU group. After joining RSU check the validity of the vehicle. Then it applies a group signature using anonymous group certificate so that vehicles in a group can communicate with other group's members and RSU without revealing its identity.

III. Security Threats and Attacks

Denial of service attacks This attack, vehicle resources are controlled by the attackers. This type of attacks also prevents arrival of critical information by jamming the session or communication medium. The author in [10], provide a solution to overcome this type of attack by switching different communication technologies such as DSRC, UTRA-TDD.

Replay attack Previous Information is transmitted again by the attacker in order to get the benefit of current situation at the time of message forwarding. Basic 802.11 provides no securities against this attack due to the absence of unique sequence numbers or timestamp [12]. The main motive of this attack is to avert vehicles identification in hit and run event.

Sybil attack An attacker generates huge amount of pseudonymous and pretends like conveying the information to others that there is heavy jam ahead in the communication medium and also force the vehicles to take an alternative route for their own benefits.

ID Disclosure attack In this attack, there is disclosure of targeted node ID in order to track the current position of that particular vehicle. Generally this tracked information or data is used by car rental companies for tracking of vehicles.

Malicious Attackers An attacker tries to access the particular resources available on the network. To get the resources attackers sometimes damage the VANET's application also [20]. For e.g. a terrorist makes the road congested by generating a warning message before planting a bomb.

Selfish drivers An attacker, in order to get benefit from the vehicles conveys the message to the other vehicles regarding congestion of road. As a result, road will be clear for selfish driver and other vehicles take alternate route.

Pranksters In this attack, hackers get fame via. Their damage and sometimes also convince one vehicle to slow down its speed and then convey a message to the vehicle which is behind to increase the speed.

Snoops Malicious Snoops gather valuable information about users. It takes other person's identity to gain profit or to harm other vehicles and sometimes even track location of a particular vehicle.

IV. Security Issues

Mobility In This network, vehicles can communicate via. making connections with each other but this connection. The use and integration of security mechanisms for warning messages and safety services is absolutely necessary within VANETs. will last only for small amount of time because each vehicle goes in opposing path and never meet again so mobility is one of the major issue in VANET [26].

Network scalability This network is scalable up to millions of nodes app. 7.2 millions and the scale is growing day by day rapidly but there is no global or central authority that governs standard of this type of network [21]. For e.g DSRC of North America and Europe are different not same.

Volatility In case of high mobility of cars connection will be lost, so personal details of user's equipments to a host location requires a long password but this will be unrealistic for securing network.

Efficient Channel Utilization Broadcasting and multicasting are widely used methods in VANETs. But there is limited available bandwidth of nodes and broadcast applications demand high bandwidth [11]. These packets are used for disseminating safety traffic messages or alerts and route discovery.

Authentication In VANET, each vehicle message is assigned with a private key and its certificate. At receiving end vehicle receive the message from sender, it first checks the key and certificate attached with a message and then verification procedure takes place.

Availability Various applications in VANET requires real time environment, so any information must available at any time. This security is essential in time varying environment any delay in a second or a millisecond will make the message meaningless [7].

Non Repudiation When two or more users share the same key then non repudiation occurs [20]. Even after the attack happens this facilitates the ability to identify the attackers and also prevents cheaters from denying their atrocity.

Confidentiality In VANET each driver's privacy is protected by encrypting the message in order to prevent outsiders accessing driver's critical information [2] .Location and anonymity are main issues for vehicular users.

Privacy This type of attacks is identity revealing attack and is related with unauthorized accessing of important data or information about vehicles [8, 21]. In case the car's owner is driver, if the attacker gets the owner's identity then indirectly vehicle may put its privacy at risk. This paper presents a brief survey of VANETs security issues and challenges for ITS system. Although, there are loads of open issues till now in this network [16, 21, 22]. This section provides a brief idea for previous problems for the future work. To overcome the previous problem we provide a concise plan using Electronic License Plate (ELP). ELP are cryptographically verifiable numbers equivalent to conventional license plates issued by govt that help in keeping track of vehicles crossing country edge or boundary lines and also helps in identifying stolen cars. Firstly, CA issued a Digital Certificate using ELP. For this purpose, CA will inspect whether the requested vehicle has ELP or not. In case, if the vehicle has ELP then CA sign on vehicle's Public key and issue the digital certificate. Secondly, after issuing the certificate, verification of certificate is done. Then, RSU and vehicle swap their certificates for more secure communication. There is a little doubt that VANETs offer great potential in the advancement of vehicles and the development of the ITS. The functionality of this network architecture does come at a price since it requires high efficiency with no room for security flaws. Current technologies in authentication, localization, information access and so forth show promise, but better mechanisms must be implemented to ensure that all standards are met. Current research works have shown present alternate solutions with promising potential that will possibly be implemented in future instances of VANETs as its development cycle extends and nears completion. Plenty of vulnerabilities have also been discovered and reported to ensure that none of them are present when VANETs are publicly available to the masses. These vulnerabilities demonstrate to what extent a VANET can be exploited, even to the point of full car control that is unacceptable considering the damage it could cause to the end users. As much as the efficiency of the transportation system would increase if the deployment of VANET was sooner than later, extended research in its security related aspects must be done before being fully implemented.

V. Conclusion

In this paper, we have elaborated on the various challenges, privacy and security issues in vehicular ad-hoc networks (VANETs). The challenges are the factor against the success of the VANET is measured and the area in which further research is needed. The Privacy is also an important factor for the public acceptance and Successful deployment of VANETs. The security of the whole system is very much based on the security of the system platform in the vehicles. Security is one of the important factors for the success of future vehicular networks; hence its integration into the system has to be done very carefully making it an integral part of the system. Future work from the VANET research community must put emphasis not only on developing security mechanisms to counter all potential vulnerabilities, but also on platforms that could be used by researchers to perform further testing on the internal and external components of VANETs. These types of networks are not as readily available as the more standard Internet architecture platforms so it is important that research goes into developing ways for researchers to be able to directly test potential solutions to VANET issues, security related or not. Work must also be put into testing all these proposed solutions unto larger and scalable models to ensure that the mechanisms work as predicted. It also goes to show that future research must be done to test out all the possible security angles of VANETs since room for vulnerabilities cannot be tolerated. The extent of such work would help ensure the protection of VANET users, which is paramount in an architecture that is directly tied to the transportation system.

References

[1] Vehicle Safety Communications Consortium, http://wwwnrd.nhtsa.dot.gov/pdf/nrdl2/CAMP3/pages/VSCC.htm"
[2] Dedicated Short Range Communications Project, "http://www.leearmstrong.comIDSRC/ DSRCHomeset.htm"
[3] The PReVENT Project, " http://www.prevent-ip.org"
[4] The NOW: Network on Wheels Project, "http:twww.network-onwheels.de"
[5] R. Lind et al, "The network vehicle.A glimpse into the future of mobile multimedia", Aerosp. Electron. Syst. Mag., IEEE, 1999.
[6] R. Morris, J. Jannoti, F. Kaashoek, J. Li, and D. Decouto, "Carnet:A scalable ad-hoc wireless network system", Proc. of SIGOPS, 2000.
[7] R. Waghmode, R. Gonsalve, "Security enhancement in group based authentication for VANET",International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), IEEE, January 2017**.**
[8] B. Parno and A. Perrig, "Challenges in Securing Vehicular Networks", Proc. of HotNets-IV, 2005.
[9] M Raya, P Papadimitratos, JP Hubaux, "Securing Vehicular Communications", IEEE Wireless Communications, Vol 13,October 2006 .

[10] M Raya, D Jungels, P Papadimitratos, I Aad, JP Hubaux,"Certificate Revocation in Vehicular Networks", Laboratory forcomputer Communications and Applications (LCA), School of Computer and Communication Science, EPFL, Switzerland, 2006.
[11] GMT Abdalla, SM Senouci, "Current Trends in Vehicular Ad Hoc Networks", Proceedings of UBIROADS workshop, 2007.
[12] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and JP Hubaux,"Eviction of Misbehaving and Faulty Nodes in Vehicular Networks ", IEEE Magazine, vol. 10, October 2007.
[13] P Papadimitratos, L Buttyan, JP Hubaux, F. Kargl, A. Kung, M. Raya, "Architecture for Secure and Private Vehicular Communications", 7th International Conference on ITS, 2007.
[14] Fubler H Schnaufer S, "Vehicular Ad-Hoc Networks: From Vision to Reality and Back", IEEE ,2007.
[15] X Lin, R Lu, C Zhang, H Zhu, PH Ho, "Security in Vehicular Ad Hoc Networks", IEEE Communications Magazine, April 2008.
[16] I Aad, JP Hubaux, EW Knightly, "Impact of Denial of Service Attacks on Ad Hoc Networks", Networking, IEEE/ACM Transactions on Volume 16, August, 2008
[17] W Ren, K Ren, W Lou, Y Zhang, "Efficient user revocation for privacy-aware PKI", In Proceedings of the 5th International ICST Conference, 2008.
[18] R Lu, X Lin, H Zhu, PH Ho, X Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular", In proceeding The 27th Conference on Computer Communications, INFOCOM 2008.
[19] Philipp Wex, Jochen Breuer, Trust Issues for Vehicular Ad Hoc Networks", IEEE, 2008
[20] L.Bariah, D. Shehada, "Recent Advances in VANET Security: A Survey", 82nd International conference on Vehicular Technology Conference (VTC Fall), IEEE, 2015.
[21] R. Mishra A. Singh, "VANET security: Issues, challenges and solutions", International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Nov. 2016
[22] Kenneth P. Laberteaux, J.J. Haas, and Y.C.Hu, ―Security Certificate revocation list distribution for VANET. In VANET ' Proceedings of the fifth ACM international workshop on vehicular Inter-networking, 2008
[23] Yue Liu, Jun Bi, Ju Yang, "Research on Vehicular Ad Hoc Networks", IEEE, 2009
[24] Samara G, Wafaa A.H. Al-Salihy, R. Sures, "Security Issues and Challenges of Vehicular Ad-Hoc Networks (VANET)", IEEE 2010
[25] Z. Lei, W. Qianhong, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," IEEE Transactions on Vehicular Technology, Vol. 59, pp. 1606-17, Mar. 2010
[26] Schweiger, B., Ehnert, P., Schlichter, J.: Simulative Evaluation of the Potential of Car2X-Communication in Terms of Efficiency. In: Strang, T., Festag, A., Vinel, A., Mehmood, R., Rico Garcia, C., Röckl, M. (eds.) Nets4Trains/Nets4Cars 2011. LNCS, vol. 6596, pp. 155–164. Springer, Heidelberg (2011).
[27] Joe, M., M.,Ramakrishnan, " WVANET: Modelling a novel web based communication architecture for vehicular network", Wireless Personal Communications, pp. 1–15, 2015.