ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE
International Journal of Advanced Research in Computer and Communication Engineering

ICACTRP 2017
International Conference on Advances in Computational Techniques and Research Practices
Noida Institute of Engineering & Technology, Greater Noida
Vol. 6, Special Issue 2, February 2017

Vehicular Ad Hoc Networks (VANETs): A Survey on Security issues and challenges

Lavanya Sharma[1], Sunil Kumar Bharti[2], Dileep Kumar Yadav[3]

Department of Computer Science, G B Pant Engineering College Pauri, Uttarakhand, India[1]

Department of Computer Science, NIET, Greater Noida, India[2]

Department of Computer Science, KEC, Mohan Nagar, Ghaziabad, India[3]

Abstract: 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 .This article provides a brief description of various challenging issues in VANET and also presents some existing solutions for these problems. Later, we discussed current status of research and future goals. With this article, researchers and academicians can have more detailed perceptive of VANET and research trends in this emerging field.

Keywords: Vehicular Ad-hoc network, Authentication, threats and attacks, DSRC, OBU, RSU, Ad Hoc networks, Privacy.

I. BACKGROUND

MANET a network with no fixed infrastructure is a very powerful way of communication in various cases where there is no infrastructure or infrastructure is absent such as floods, earthquakes or disaster. VANET is a sub group of mobile Ad-hoc networks (MANETs) and now a day's becomes a very promising approach to support several ITS systems such as traffic monitoring and safety, free and busy routes information, internet services and many more. VANET is one of the important component of ITS in which represented as vehicles can communicate with each other or with the base Station placed across roadside. This network mainly involves three types of communication: vehicle to roadside (V2R), vehicle to vehicle (V2V) or vehicle to infrastructure (V2I) communication and two other units: On Board Unit (OBU) and Roadside Units (RSUs) [1,2]. Among them, OBUs enables short-range wireless ad-hoc network formed between vehicles and Roadside Units (RSUs), placed across the roadside for infrastructure communication. Due to dynamic nature of nodes, they move freely from one position to another within coverage area and any node can becomes a means of transport [4].

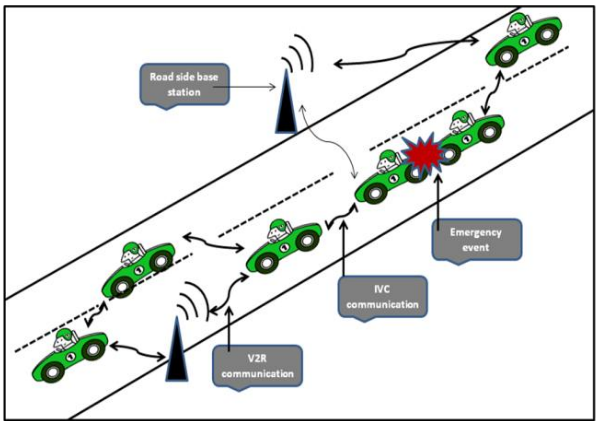

Fig. 1 showing communication pattern: roadside base stations vehicles and acts as a node share safety messages to provide the drivers amount of time to react to emergency event**.**

Recently, various projects have been launched and implemented to support vehicular safety applications such as Network on Wheels (NOW) is a German project started in May 2004 specifically designed for road safety and infotainment applications that is supported by German government and also initiated by leading car manufacturers companies of Europe. This project develops a secure vehicular communication system based on Adhoc network principles and wireless LAN technology for car-to-car communication. Some other projects includes internet ITS consortium (Japan) and prevent project (Europe) [1, 3, 4, 7].

In 2003, ASTM and IEEE adopted dedicated short range communication (DSRC) standard to provide promising infrastructure less communication for transports systems within a range of 1000m and also provides seven 10 MHz channels at the 5.9 GHz licensed band for ITS applications, with different channels, including one specifically reserved for vehicle to vehicle communications (V2V) [2].

The precise features of this network led to the development of several eye-catching services .Some of them are listed below:-

1) Safety Applications: This category mainly concern with the safety of travellers by sharing status information for safety purpose via vehicle to vehicle communication (V2V) or inter vehicle communication (IVC). This information used to activate an actuator of active safety system. Some examples of this category are: travelling on constrained lane or road, signal violation warning, disaster warning, road circumstance information etc. The aim is to enhance road safety by intimating about emergency circumstances such as alert or warning messages. [6].
2) Comfort application: This category mainly focuses on improvement of traveller comfort and traffic efficiency. Some examples of this type of application are: whether forecasting system, gas station, traffic information system and interactive communication such as visual data streaming, web browsing or Internet access to travellers to enjoy the journey.
3) Medical Monitoring application: VANET is an ideal choice for medical monitoring applications in case if patients carries wearable medical devices and outside of wireless access point and need to sent data to the medical centre in case of emergency, in case of disaster where infrastructure is absent there are several individuals with medical issues that needs steady monitoring.

This paper is organised as follows. Section 2, describes various attack and threats and adversaries. Section 3, describes various challenges which are considered as major security issues of this network. Section 4, deals with some security requirements needed to achieve security system. Section 5 discusses current existing solutions presented by several researchers that are needed to achieve a secure. Section 6 we provide our solution for some of the problems.

II. SECURITY ISSUES OF VEHICULAR NETWORK

There are various advances in VANET but still there are several security issues that have to be overcome. These challenges are various attacks and threats that are listed below:

A. VARIOUS ATTACKS AND THREATS IN VANET

This work primarily focuses on various attacks wreak against message itself rather than materialistic security in vehicles.

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.

B. ADVERSARIES

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.

III. CURRENT CHALLENGES IN VEHICULAR NETWORK

Mobility In This network, vehicles can communicate via. making connections with each other but this connection 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.

IV. SECURITY REQUIREMENTS

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.

V. 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 (CA) 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.

Table 1. A Review of Security Aspects in VANET

S. No	Name of the paper	Author	Objective	Drawbacks
1	Security enhancement in group based authentication for VANET	R.Waghmode et al [7]	Use group based V2V communication to prevent vehicle from threat. This scheme can trace malicious vehicle which generates a false message Improved communication & computation cost.	This scheme involves one time authentication process for group and then only V2V communication is done using symmetric key method within group.
2	Eviction of misbehaving and faulty nodes in vehicular networks.	M. Raya et al [10]	Discussed various Revocation protocols (RTPD, RCCRL, and DRP). LEAVE protocol used to make the system operations more secure. Faulty nodes can be detected by using MDS	These methods rely on monitoring only. Not appropriate for reputation system. False positive rate by Bloom filters.
3	Efficient user revocation for privacy-aware PKI	Zhang et al [14]	Idea using the group signature is recommended.	Mobility makes a group dynamic and prevents it from making a static.
4	Security Certificate revocation list distribution for VANET	Kenneth et al. [16]	CRLs distribution by using vehicles in an epidemic manner. Improves distribution speed	Bandwidth and Hardware constraints. Performs approaches that only employ RSUs distribution points
5	Design and analysis of lightweight evocation mechanism for VANET	Jasson et al. [17]	Used lightweight method for exchanging CRL updates Reduction in certificate revocation lists size	Long CRLs due to huge no. of vehicles Low performance in high traffic region
6	A scalable robust authentication protocol for secure vehicular communication	Zhang et al [18]	Discussed Signcryption and group signature mechanism to achieve security principles. Using this protocol specific feature such as mobility, physical road limitations can be exploit efficiently, and properly distributed RSUs.	If any RSU collapsed, than particular network's working gets disturbed. With increase in load ,performance rate decreases

In literature, most of the authors suggested the use of CA for initiating keys storing, managing and broadcasting the CRLs but this requires infrastructure for it. Most of the researchers discussed about CA to tackle generate, renew and revoke certificate operations. For all above operations a large number of CA is required but there is no central administrator or authority that governs the wireless network specially VANET.

VI. DISCUSSION

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.

Verification of certificates is required by all the protocols. We use the $\text{CHECK}_{\text{cert}}$ to verify the certificates. Let us suppose Cert(V) represents a certificate digest or a certificate Cert(V) a truncated output of Hash (cert (V)), where Hash is a hash function and time required to verify the certificates is given by T_{Cert}.

CRL is the certificate revocation list where the certificates are placed after their identification.

Algorithm for verifying the certificate in VANET's is shown below

Algorithm for Certificate Verification

```
VERIFY_CERTIFICATE (V)
    if Cert(V) is a certificate
        then  Verify Cert (V) is authentic or not
            if Cert(V) is authentic
                then Store Cert(V)  with its Digest and Store  flag value to the CRL
            else
                verify the CRL for Cert(V)
    else
        Issue Cert(V)
END
```

VII. CONCLUSION AND FUTURE WORK

This network is an emerging platform for improving road safety on highways and cities traffic scenarios. This is a fertile area for various attackers who keeps on challenging network with their, malevolent behaviour or activities. This work presents a state of art survey of current challenges and their possible solutions. We also present a brief idea on new solution that makes a more secure. In future, we broadly elaborate our concept about certificate of messages, their creation, verification and can simulated by using some tool.

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-on-wheels.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 for computer 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.

BIOGRAPHIES

Lavanya Sharma is pursuing her PhD from GBPEC Pauri, Garhwal, Uttarakhand. She did her M.Tech in Computer Science from MDU Rohtak, Haryana. She has done M.Sc in Information Technology from P.T.U after completing PGDCA. She also did her B.Sc from University of Delhi, India. She has published many international conference, and also papers in reputed journals. Her primary research interests are in image processing and video processing. She has published many research papers as well as journals of repute.

Dr. Dileep Kumar Yadav received his Engineering degree (BTech in Computer Science and Engineering) from Uttar Pradesh Technical University, Lucknow, UP, India in 2006, Master's degree (M.Tech. in Computer Science and Technology) and Ph.D from School of Computer and Systems Sciences, Jawaharlal Nehru University, New Delhi, India. His research interests are in image processing and computer vision. He is a Sun Certified Java Programmer for Platform 1.5 (SCJP 1.5). He has five years of working experience in industry as well as academia. He has published many research papers (in reputed journals, international and national conferences.

Dr. Sunil Kumar Bharti receives Master's degree (Master of Computer Application) and Ph.D from School of Computer and Systems Sciences, Jawaharlal Nehru University, New Delhi, India. His primary research area are in Modeling and Simulation, Computational (Neuroscience), image processing and computer vision. He has published various research papers (in reputed journals, international and national conferences.