A Survey: Security Challenges of Vanet And Their Current Solution

R. Hemalatha[a], Dr J. Abdul Samath [b]

[a] *Research Scholar, Bharathiar University,Coimbatore*
[b] *Department of Computer Science, Chikkanna Government Arts College, Tiruppur*

Article History: Received: 11 January 2021; Accepted: 27 February 2021; Published online: 5 April 2021

Abstract: Vehicles have a very crucial role in our routine life; we use different kinds of transportation in our living world, massive increasing vehicle on the road insisting serious problem such as traffic jam, vehicle congestion, road accidents, the demand for more fuel etc., to subdue the all those problems, the technology has used which is called VANET (Vehicular ad-hoc networks) VANET is self-organized wireless network when it has demanded to make communication between vehicles to vehicles and vehicles to infrastructure. VANET successfully implements the intelligent transportation system (ITS), even the vehicles having short-range networks. Due to the rapid change of network topology, the VANET installation is challengeable on the vehicles. To give a safe drive and reduce car accidents, the communication among drivers of vehicles and roadside devices makes sure that should be authenticated; any wrong modification (or) correction in real-time communication may create system failure and affect road safety. This article provides a brief description of various challenging issues in VANET and presents some existing solutions for these problems. Later, we discussed the current status of research and future goals. With this article, researchers and academicians can have a more detailed VANET and research trends in this emerging field.

Keywords: VANET, Security attacks, ITS, RSU, SEAD

I Introduction

VANET is one type of MANET; VANET is used in ITS (Intelligent Transportation System) to allow people to travel their road safety journey. In VANET, the vehicles able to communicate with another one as well as roadside units (RSU) which are at the edge of the platform of the road, the moving nodes (vehicles) providing unfixed network topology, so VANET do not have any central place to administrate the nodes, the communication established at the time of need depends on wireless range. The VANET is not controlled under of the owner of the node always, nodes could be stolen, and hackers can be tamper on the communication information; various types of cyberattacks happen in VANET, unpredicted and predicted an authorized node drives attacks, unpredicted attacks demarche by authenticated nodes, predicted attacks [3].

We produce and discuss the various kinds of attacks on a wireless network is a detailed manner. This survey will help the forthcoming researchers to categories of security challenges for their work [9].

In VANET, we classify four domain nodes. First, the domain is a node (Vehicle) with a radio system, Bluetooth or wireless device (GPS), I a:- Vehicle --> to --> sensors (lidar and Radar) and Event Data Recorder (DR). I b. Vehicle --> to--> personal devices. Second domain nodes are roadside unit (RSU) to communicate with the base station and vehicle act as gateways. The third domain is the vehicle called VANET on board unit (OBU) fourth domain is a nearby cellular base station [5] [7]. The vehicles are designed with VANET to inform the traffic congestion and road accident around them to nearby base stations and roadside unit (RSU). Besides, inter vehicles communicate with them regarding speed, direction, proximity and other parameters without driver intrusion [6].

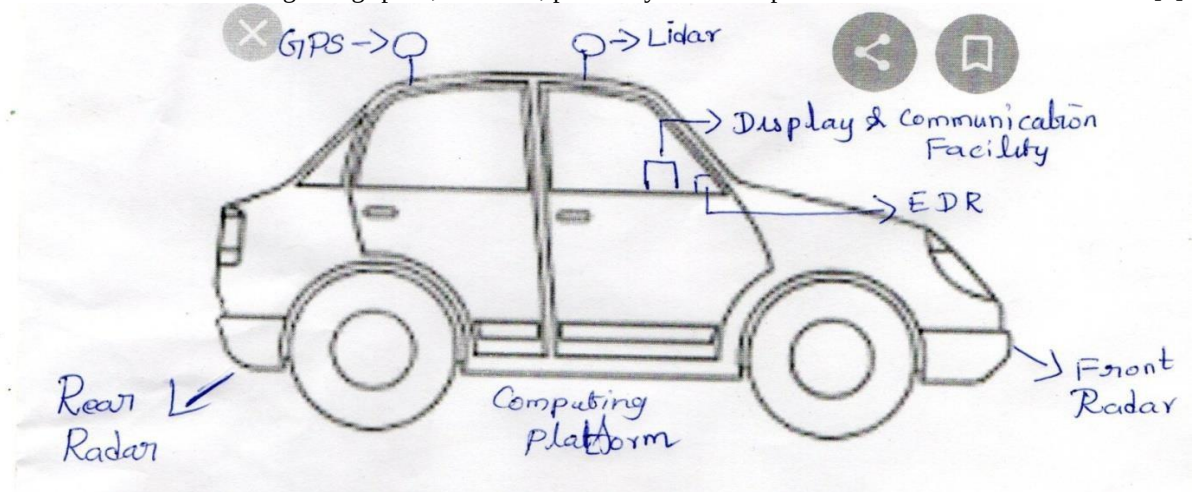

Figure1.Intelligent vehicle architecture

This paper develops a survey on secure vehicular communication system based on Adhoc network principles and wireless LAN technology for car- to-car communication [9].

II BACKGROUND STUDY

This section provides a research report on the latest potential solutions that offer protection to the VANET network. In this way, we can discover the most important pattern and the current solution for each thread. Several securities have been proposed to date, and various analysis papers have been introduced to fix these VANET protection concerns addressed in this document.

Public Key Strategy Based This method retains the security of the post, where the vehicle has a private key sign and its certificates are still attached. The authentication of the message takes place at the receiving end, where the recipient verifies the key used to sign the message and verifies the message during verification. Author [2] addressed this strategy and then used the ECC to minimize the network.

Community Signing Based Strategy There are two key problems with this strategy. Firstly, this concept creates a great deal of overhead as a new car joins the group, and secondly, the versatility that keeps a network from keeping a group static. Author in [12] addressed Signcryption and Community Signature in order to fulfil a range of protection concepts.

III. COMPARATIVE ANALYSIS OF SURVEY

Author	**Objective**	**Drawbacks**
R.Waghmode et al [1]	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.
M. Raya et al [3]	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.
Zhang et al [8]	Idea using the group signature is recommended.	Mobility makes a group dynamic and prevents it from making a static.
Kenneth et al. [10]	CRLs distribution by using vehicles in an epidemic manner. Improves distribution speed	Bandwidth and Hardware constraints. Performs approaches that only employ RSUs distribution points
Jasson et al. [11]	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
Zhang et al [12]	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

Table 1. A Review on Security Aspects in VANET

IV. THE SECURITY CONCERNS TO VANET

Here we classify below the table presents possible cyber-attacks.

Property	Possible attack	Attack effects	Ease of attack
Authentication	Dos	Denial of channel service in the network, the users can't communicate with others	High
	Replay attack	The malicious node received all packets and resent them at different times to all nodes.	medium
	Message spoofing	Lead the wrong direction by the incorrect location information	medium
	Bogus information	Attackers deliver the bogus information to all other vehicles at the same time as well as on all type of wireless networks.	Medium
	Sybil attack	A single compromised node pretend itself as multiple identities	High
Confidentiality	Eavesdropping	Loot the important and personal information from the driver (or) owner of the car.	High
	Blackhole & Grey hole	The information has blocked instead of spread over the network.	Moderate
	Man- in the middle	It happens when a malicious node breaks the relay (or) manipulating the real messages exchanged between the legitimate nodes.	High
	Timing attacks	The real-time content creation has changed.	High
	Injection attack	The attackers inject the wrong information into the automotive bus system.	High
	Location tracking	Attackers can collect and modify the location tracking information for tracking attacks.	High
	Brute force	The attacker, with the help of the technique, crack the key in cryptography	High
	Id disclosure	Obtain the Vehicle's ID and track the route of the vehicle	High
Availability	Flooding attack	Plenty of packets are falling on a node to make the node not available condition.	High
	Jamming attack	The attacker uses the jammer signal to jam the channel.	Medium
	Amalgamation attacks	A group of illegitimate node gathered to start malicious attacks like isolate the legitimate node.	Low

Integrity	Alter the Real message	The compromised node modify and spread the information from what they get.	High
	Forgery attacks	The compromised node changes the actual time and the right location.	High
	Illusion attack	The compromised node deceives the sensors of a car and sends wrong traffic warning messages to the neighbours.	High
	Masquerading	The attackers capture the legitimate identity to obtain confidential information.	High
	Broadcast tampering	The attackers use the vehicle maintenance period to tamper with the hardware of the vehicle.	High

Table 2: possible security challenges, the followings are the most feasible solution for the above attacks.

V PROPOSED TRENDY SOLUTIONS

1. Cryptography style solutions

Cryptography also the best solution for secure communication between users by using protocols that avert an illegitimate person from access. Encryption is one of the cryptography-based techniques where it transforms the data into code by using an advanced algorithm the indented users can only read and prevent outside attackers. In VANET System, each vehicle apply the encryption and digital signature for getting secured message communication with the Vehicle and RSU

Key distributed Encryption technique gives a feasible solution for the attacks such as man – in – the –middle attack, replay attack.

2.SEAD (Secure and efficient ad-hoc distance vector)

Its works are based on the DSDV routing protocol (Discetinanation sequenced distance vector). Some of the Nodes have low CPU processing capability in which attackers try to exploit more network bandwidth SEAD supports that type of nodes by using one way Hash function and Symmetric cryptography.

In Dos Attack, the attackers transmit more traffic information than the CPU capacity to handle, for that one way hash Function is used with that node, which is choosing the Random initial value, then, the List of values are calculated like

$$V_0, V_1, V_2, \ldots\ldots V_n,$$

$V_0=X$, $V_i=H(V_i\text{-}1)$ for) $0 < I \leq n$. for authentication V_i can authenticate $V_i\text{-}4$ By developing $H(H(H(H(v_i\text{-}4))))$. Using destination sequence number easily escape from repeated routing path, and replay attack can identify in the packet using the destination sequence number.

3.ARAN (Authenticate Routing For Adhoc Network)

ARAC (Authenticated routing Ad Hoc Network) is a standard secured Routing Protocol. It works based on cryptographic certificate Authentication; if a Source node finds a route Path to the destination, it broadcast the route discovery request (RDRP) to all nearby neighbours nodes; if a node gets the message from its Neighbor, it sends again to all their neighbour nodes with their signature and owns the authenticated certificate. No intermediate node replay to the sender node even if it knows the destination's route, then the destination node unicasts the replay by reverse mode to the source node. Each node checked own signature of the sender

ARAN is used for spoofing, forgery attackers to detect the malicious node

4.Time stamping

Timestamp with Cryptographic is best to counter measure for a timing attack

5. ARIADNE

Y.Chun Hi et at propose a routing protocol base on DSR on Demand Routing Protocol. Mac, Digital Signature, Symmetric Cryptography and TESLA Techniques used for message authentication. In this, the sender Uses Time Stamp and MAC authentication for secure transmission.

6. VatiCAN

The CAN mechanism is deployed for connected electronic vehicle units inside the car.

The Standard CAN(Controller Area Network) have been 8 bytes only , The are some author try to increasing the capability of CAN By using new protocols. A VatiCAN with Sufficient Bytes to use authentication. Introduce a protocol against masquerading replay attack , injection attacks by sending a partial MAC in each frame.

6a. LIN

There is no need for higher bandwidth, increased capability, higher transmission, and LIN as a CAN choice. LIN is used to control the A/C, steering wheels, seats, lights, engines, doors, air push lock. LIN's master-slave architecture and LIN's master's Synchronization ability are enhanced by adding MAC techniques and a LIN intrusion detection technique.

LIN is one of the best solutions for message spoofing and amalgamation attacks.

6b.Flex Ray

Flex Ray is also used in interconnect automotive bus systems like CAN, VatiCAN, LIN, which is more complex communication protocol. It has a communication rate is 10 Mbps as it compared to CAN, which has 1mbps. It contains 2 sections 1.static, 2.dynamic both efficiently deliver the real messages with secured.

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. This section provides a brief idea for previous problems for the future work. The attackers can be divided as outsiders and insiders, and they used to attack directly or indirectly, even the security protocol to be strong enough the attackers invade into the network security, The cryptographic algorithm method is a feasible solution for security issues categorized as symmetric and asymmetric algorithms. Symmetric algorithm more complex to generate the key, it works by $o(n^2)$ n is a number of nodes. It need more space to store the keys. The asymmetric algorithm works by o(n). It works with only one pair of public and private keys, it does not require a large amount of space, so asymmetric key is best solution for VANET security problems. Next we look at digital signature on cryptography, in this encrypt, decrypt and making signature are need more computation power. This is also good approach to VANET. After that we glance at protocols such as SEAT, SMT, ARAN, ARIADNE, MAC protocols, they are used to encrypt and decrypt the messages; this technique is faster than all other methods. Finally, we discussed the automotive bus system, the communication is run within the in-vehicle system; communication protocols are installed in the system to transmit the messages to each other subsystems. Types of updated methods are CAN, VatiCAN, LIN, FlexRay etc.. This survey paper discusses the trendy security challenge and how to overcome it by the feasible solution. This will help to analyze the right solution for complex security issues.

VII. CONCLUSION

In this survey, VANET is an increasing exploration field with a bright future and, besides, incredible protection difficulties. It provides general security issues to the Adhoc framework and confronts threats, such as espionage, operation investigation and eavesdropping. Moreover, VANET's unique methodology introduces new protection concerns, such as location discovery, illicit tracking and jamming. Conventional cryptographic methodologies used in VANET incorporate public key systems to distribute one-time symmetric session keys for message verification, authentication certificate schemes and randomization of traffic analysis operation designs. The Confidence Grouping System takes a half-and-a-half approach to symmetrical and symmetrical cryptographic plans to obtain both attractive handling rates and protection efficiency. The pseudo-ID-based system is then protected and uses threshold methods for authorization and message signing to strike a compromise between the desire to safeguard client security and the need for traceability for law enforcement forces. The VANETS implementation is graded in terms of protection and comfort and potential usage.

References

1. 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**.**
2. B. Parno and A. Perrig, "Challenges in Securing Vehicular Networks", Proc. of HotNets-IV, 2005.
3. M Raya, P Papadimitratos, JP Hubaux, "Securing Vehicular Communications", IEEE Wireless Communications, Vol 13, October 2006 .
4. 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.
5. GMT Abdalla, SM Senouci, "Current Trends in Vehicular Ad Hoc Networks", Proceedings of UBIROADS workshop, 2007.

6. 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.
7. 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.
8. Vengatesan, K., Kumar, A., Subandh, T., Vincent, R., Sayyad, S., Singhal, A., & Wani, S. (2019). Secure Data Transmission Through Steganography with Blowfish Algorithm. In International Conference on Emerging Current Trends in Computing and Expert Technology (pp. 568–575).
9. Fubler H Schnaufer S, "Vehicular Ad-Hoc Networks: From Vision to Reality and Back", IEEE ,2007.
10. X Lin, R Lu, C Zhang, H Zhu, PH Ho, "Security in Vehicular Ad Hoc Networks", IEEE Communications Magazine, April 2008.
11. 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
12. W Ren, K Ren, W Lou, Y Zhang, "Efficient user revocation for privacy-aware PKI", In Proceedings of the 5th International ICST Conference, 2008.
13. 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.