Proceedings of the International Conference on Artificial Intelligence and Smart Systems (ICAIS-2021)
IEEE Xplore Part Number: CFP21OAB-ART; ISBN: 978-1-7281-9537-7

A Review of Digital signature and hash function based approach for secure routing in VANET

Surender Kumar[1]

[1] Department of CSA Deptt. Choudhary Devi Lal University Sirsa Haryana India

Dr. Vikram Singh[2]

[2] Department of CSA Deptt. Choudhary Devi Lal University Sirsa Haryana India

2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS) | 978-1-7281-9537-7/20/$31.00 ©2021 IEEE | DOI: 10.1109/ICAIS50930.2021.9395882

***Abstract*- Vehicle ad hoc networks (VANETs) have tremendous potential to enhance road and traveler safety through vehicle connectivity to highways and local roads. Vehicle ad hoc networks, also known as Vehicle to Vehicle (V2V) and Vehicle to Roadside (V2R) Unit Connectivity, have gained considerable interest in research over the past few years.Today, every vehicle manufacturing industry tries to implementintelligent technology for drivers' and passengers' safety. They use a variety of Inter-Vehicle Communication technology to boost their safety measures.Various technologies developed for the same, but security and safe message delivery are critical issues. This paper reviews the multiple algorithms available for providing secure communication of information in the network. It demonstrates the methods and limitations of the existing schemes. The challenges of providing data security, reducing data risks, and reliability in data accessibility are also presented. Finally, the proposed research work aims to provide secure routing communication by enhancing authenticity and confidentiality using Digital signature and Hash function based approach for secure routing protocol implementation.**

Keywords: VANET, MANET, Digital Signature, Hash Function, DSRC.

1. INTRODUCTION

"Wireless networks are group of computer networks that use radiofrequency channels of their physical medium for communication"[1]. The node in the transmission range radius can receive information that is broadcasted by any node of the network. Since nodes communicate through the airwaves, they may not need to be connected directly to any network. Therefore, these networks provide data access along with user mobility.

1.1 Adhoc Network

Since its introduction in the 1970s, wireless networks have become widely common in the computing industry. Wireless communication network enables mobility and easiness of communication between numbers of nodes. In this network, nodes are randomly moving and need not fixed Infrastructure to communicate. There are two types of networks in the wireless network. The infrastructure network having stable and wired gateways, is the first. Base stations (BS) are considered the bridges for such kinds of networks. Mobile units connect with the closest base stations that are within the contact range. While the mobile move from the on-base station's radius to another base station radius performs the "Handoff" process by which mobile continues communication smoothly throughout the network.

The second is without mobile network infrastructure, generally known as a mobile ad hoc network (MANET). The infrastructure would not have a base station, fewer networks, no fixed routers, and no unified management. All nodes are able to move randomly and can be connected to each other dynamically.All nodes of these networks perform routers' function, which discovers and maintains routes to other network nodes.

1.2 Vehicular Adhoc Network (VANET)

VANET stands for Vehicular Adhoc Network. In the VANET, vehicles are known to be linked nodes in the form of a "vehicular Adhoc network." The CBR (Constant bit rate) and TCP (Transmission control protocol) are the traffic agents used to transmit data between vehicles [10]. A vehicular Adhoc network is a subgroup of Mobile Ad hoc Network (MANET). "communication of VANET can be classified as two types; a) Vehicle to Vehicle (V2V),b) Vehicle to Infrastructure (V2I), i.e., roadside unit. In general Vehicle communication employs multi-hop or multicast practices. It uses two types of broadcasting: naive broadcasting, in which vehicles send broadcast messages periodically. At regular periods, the vehicle overlooks the message if it has happened from a vehicle at the rear. If the message comes from a vehicle in front, the receiving vehicles send their broadcast message to the vehicle behind it. The limitation of this broadcasting is that a large number of broadcast messages are generated. So there is the riskof message collision" [17].

"Second, Smart broadcasting removes these message collisions risk. By taking an example, if a car positions a dangerous road position such as black ice, it spreads the data or message to the car behind it, which might be heading in the direction of danger. At that time the routing protocols are employed to provide communication of data among vehicles. In the VANET, vehicles (nodes) themselves serve as a router. In the starting very firstly, this VANET technology was integrated into the emergency vehicles to communicate with each other (i.e. police and fire). It is useful in Intelligent Transportation System (ITS) for traffic management that results as saving accidents [17].

VANET is a subcategory of the MANET (Mobile Adhoc Network). As with MANET, VANET has the same characteristics. Both networks' nodes are movable. Both are cell networks, both have no infrastructure, and both use nodes to route traffic between nodes as a network router, or to connect between vehicles by routing the data packet. But certain features distinguish VANET from MANET.

1) Compared to MANET, VANET topology is very dynamically adjusted since the speeds of vehicles are high, so they adjust the position very much [17].

2) MANET nodes can be randomly shifted, but VANET nodes, such as roads and highways, can move in the desired manner [17].

3) To evaluate the location of a node, MANET uses GPS (Global Positioning System), but VANET uses AGPS (Assisted Global Positioning System) or DGPSS (Differential Global Positioning System). There is not enough storage space, poor battery and processing capacity for MANET, and these are not in VANET **[18]**.

1.2.1 VANET architecture

Via collaboration between operators, suppliers, and government officials, VANET can be introduced. A network architecture must allow contact between vehicles and fixed roadside devices [3]**.** Each vehicle consists of two types of units according to this architecture: (1) an on-board unit (OBU) and (2) one or more application units (A.U.s). An OBU is a device with communication features within the car, with a minimum of a little-range wireless communication device committed to road safety. At the same time, an A.U. is a device executing one or a group of applications while usingthe OBU's communication capabilities. AU may be a flexible unit that can be dynamically connected to (and isolated from) an OBU, such as a laptop or PDA. OBUs of multiple vehicles form an mobile Adhoc network (MANET). An ad-hoc network domain can be created by OBUs and roadside units together; roadside units are stationary equipment fixed alongside a route. An RSU can be linked to a network of infrastructure that can be connected to the Internet. RSUs may also connect directly or by multi-hop with one another. RSUs allow OBUs to access the networks and the Internet. [19].

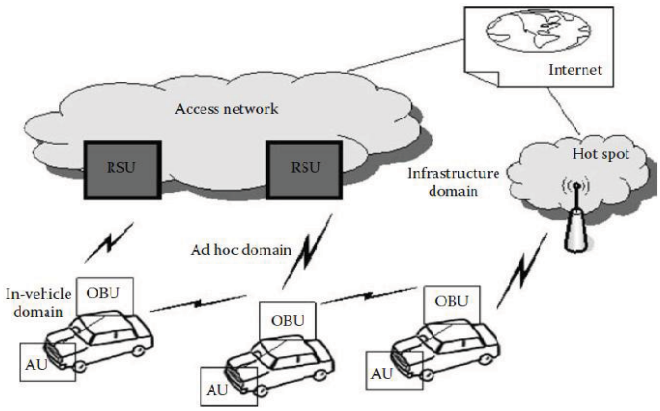

Figure.1: VANET ARCHITECTURE**[19]**

1.3 DigitalSignatures

For verification and honesty, cryptographic signatures and public-key certificates are added to security messages, which can also be used as monitoring tokens. One recommendation suggests that multiple digital licences should be given to vehicle-based units to help anonymity, recognise or track individual vehicles harder. Under the PKI (Public Key Infrastructure), digital signatures primarily support this scheme . Each vehicle is allocated a series of public / private key pairs under the PKI solution. A digital signature and a matching certificate will be included with each message received. Thus, three times the first message will be the resulting message.

To maintain privacy, a car can store an outsized key/certificate package and change keys periodically. In order to avoid being monitored, a vehicle should change its anonymous key within around one minute, as per the study by Raya and Hubaux in [10]. To prevent being tracked, a vehicle should update its anonymous key within approximately one minute. Therefore, if we presume that a median driver uses his vehicle 2 hours a day, the amount of keys needed each year is about 43800, which is about 21 Mbytes. A daunting obstacle for this device would be a way to safely issue and store such a vast number of keys.

1.4 Hash Function

In this function hash value of fixed length is represented by h , it is equal to H(m) of size n which is mapped to an input message m of arbitrary length using a hash function H: $\{0,1\}^* \rightarrow \{0,1\}^n$. It can be used for cryptographic purposes, such as ID-based cryptography, digital signatures and randomization of plaintexts in probabilistic cryptosystems, if such a function satisfies additional specifications [21]:

- The H(x) calculation should be quick and simple, with an approximately linear time.
- Preimage resistance: the search for any message m should be computationally impossible for a given hash value h, resulting in the given hash value H(m) = h.
- Second preimage resistance: looking for a second message m' with m = m' ought to be practically impossible for a defined message m, resulting in the same hash value H(m) = H(m ').
- Collision resistance: the hunt for two messages m and m' with m = m' should be practically infeasible, resulting in the same hash value H(m) = H(m ').

Latest findings have obviously demonstrated that heuristic security claims do not appear sufficient within the cryptanalysis of hash functions. Anything demonstrable is expected. Hashing may be a key idea in cryptography, and

we need powerful hash functions which can be trusted at the same time for their security.

1.5 Routing

Routing within the computer network is a necessary function that influencesnetwork management because of the quality of services in large-scale networks. The traffic flows management must meet the criteria for the degree of traffic to be transferred in order to avoid congestion to eliminate transmitting delays. In addition, these two conditions are incompatible. The optimal control of traffic is a critical problem for the efficiency of services. Network routing, using the shortest path algorithm, is commonly used in WAN[25].

A routing algorithm's efficiency depends on its success during network congestion. The efficiency of the routing algorithm is measured according to network throughput (data transmission quantity) and average packet delay (quality of service).

– The availability of multiple routes is helpful in improving the network's amount of operation.

– Traffic load oscillations must be avoided, but congestion sensitivity is also important. The traffic control center's failure is also risky for a centralised system of route management.

– For the avoidance of congested paths, adaptive routing with frequently updated details is useful.

– The three most important performance metrics for any routing algorithm are service, quality and speed [25].

1.5.1 Secure routing

Without using some pre-existing fixed network structure, a cluster of wireless nodes will dynamically form a network for the exchange of information. To locate routes between nodes, a Routing Protocol (RP) is employed. The primary objective of such an Adhoc Network (RP) is to create a right and effective route between a pair of nodes to transmit a message on time. Protection is a major problem for device designers because of the wireless and dispersed existence of MANETs **[26]**.

Privacy, honesty, authenticity, availability, and non-repudiation should be supported by a safe MANET environment. The vulnerabilities which render MANETs extremely unsafe are discussed as follows[23]:

- Wireless communication's dynamic nature.
- Tampering & Security of node.
- Minimal node strength (Power).
- Infrastructure absence.
- Lack of fixed topology for networks

2. LITERATURE SURVEY

Protocol name	Description	Mechanism/Algorithm	Methodology	Performance
Dual authentication scheme[6]	Improve authentication of data	Hash code and fingerprint of each vehicle used	Two group keys used for data transmission b/w P.U. & S.U.	Improve the authentication
SPBA Scheme[8]	They have used beacons for secure V2V and V2R	It utilizes the potential of the sender vehicle to forecast future beacons in advance.	SPBA is primarily built on symmetric cryptography	Preventing DoS attacks from using memory. SPBA only stores the sign's MACs (rekeyed message authentication codes)without reducing confidentiality.

The novel hybrid mechanism for implementation of security in MANET [26]	The security deals with the authentication and confidentiality of the data packet	Encryption is performed with the RSA based public-key cryptosystem.	Authentication is performed using digital signature algorithm SHA-1	It improves the authentication of the data by associating unique signatures with packets.
Modified ECDSA[28]	The Updated ECDSA contains a WSN sponge-based hash function.	In WSN,Modified ECDSA is containing a sponge based Hash Function.	It provides a WSN sponge-based hash function.	It improves performance like throughput latency, packet delivery ratio.
ECCEA security protocol[27]	ECCEA security framework is built on the bases of AODV protocol to enhance security	ECCEA security framework incorporates security into the AODV protocol to provide data integrity and authentication against adversary effects.	Both the ECCEA and normal AODV protocol simulated and analyzed results.	Their proposed scheme successfully secures the AODV routing protocol in defending against malicious and unauthorized nodes and is more efficient and less power-consuming.
ZgestT Hash Function protocol[21]	This hash function is parallelizable and its collision resistance.	It is based on the Tillich-Zemor hash function. It is a modified version of the Tillich-Zemor hash function.	It is implied by the hardness assumption on a mathematical problem.	It is secure against the known attacks. It is the most secure variant of the Tillich-Zémor hash function until now.
HCPA-GKA [24]	A conditional privacy-preserving authentication and group-key agreement system for VANETs based on a Hash function.	The HCPA-GKA device requires a symmetrical AES algorithm for the community key to encrypt the beacon, where each vehicle has a key that can decrypt the beacon.	In order to allocate the group key for authenticated cars, a group key agreement system based on the Chinese Rest Theorem (CRT) is used.When the car enters and exits the party, the group key is also changed.	Compared to current systems, this device meets the security privacy criteria and has major benefits in terms of computing expense and overhead connectivity.
DMAE [30]	DSRC-based Multi-Channel Emergency Alert Distribution Allocation) algorithm.	DMAE applies the largest channel of bandwidth to the urgent post.	It guarantees QoS in between OBU and RSUvia periodic channel switching.	results using ns-2 shown performance improvement on 1) end-to-end delay and 2) emergency message delivery rate

CONCLUSION

Our research work's main objective is to improve the performance of VANET protocol using digital signature and hash function cryptography algorithm. The Vehicular Adhoc Network (VANET) is a newly created technology for inter-vehicle communications to accomplish traffic safety and productivity purposes. The routing protocols play a critical role in VANETs. However, right now, there is not one that suits all sorts of situations and applications. Insufficient forwarding nodes and network interference can also contribute to serious deterioration of routing protocol efficiency in VANETs. Security and pollution are two of today's main challenges on our highways. Is there a way of mitigating injuries, of saving money, of saving lives? It's considered as Dedicated Short-Range Communication (DSRC). To improve the performance of VANET using a routing protocol, we propose a Secure routing protocol using two strategies of digital signature and hash function for VANET to keep the routing performance from degradation. The proposed research study's specific statement is "Digital signature and hash function-based approach for secure routing in VANET."

REFERENCES

[1] Sarkar S.K., T.G. Basawaraju, and C Puttamadappa (2008),Adhoc Mobile Wireless Networks: Principles , Protocols, and Applications, Auerbach Publications, 2008.

[2] **Toh.C.K. (2002),**Adhoc Mobile Wireless Networks: Protocols and Systems, Prentice Hall PTR, 2002.

[3] **SinghAbhishek, (2013),** Simulation and Analysis of AODV, DSDV, ZRP in VANETs, Masters thesis in computer science and engineering, July 2013.

[4] **Raya M.and J. Hubaux(2005),** The Security of Vehicular Networks. Tech. Rep., EPFL TechnicalReport I.C./2005/009, Mar. 2005.

[5] **FCC(2002)**, Amendment of the commission's rules regarding dedicated short-range communication service in the 5.850-5.925 GHz band, fcc 02-302. Tech. Rep., FCC, November 2002.

[6] **Sayana SS, L.M. Bernald(2018),**Dual Authentication and Key Management for Secure Transmission in Vanet'' International Research Journal of Engineering and Technology (IRJET),Volume: 05 Issue: 04 | Apr-2018.

[7] **Zhou Yousheng, Siling Liu, Min Xiao, Shaojiang Deng (2018),** An Efficient V2I Authentication Scheme for VANETs. Hindawi Mobile Information Systems Volume 2018, Article ID 4070283, 11 pages https://doi.org/10.1155/2018/4070283.

[8] **MathewVinitha, Prof. Leya Elizabeth Sunny(2018),** DSRC: Dedicated short-range communication for improved road safety, *International Journal of Engineering Sciences & Research Technology,* ISSN: 2277-9655, January 2018.

[9] **Sharma Kapil Dev, Sarita Singh Bhadauria(2013),** Implementation of Dedicated short-range communication (DSRC), IEEE802.11p in NS2 and its performance analysis over IEEE802.11, International Journal of Advance Research, IJOAR .org ISSN 2320-9119.

[10] **Kumar Vishal, Shailendra Mishra, Narottam Chand(2013),** Applications of VANETs: Present & Future,Communications, and Network, Volume 5, Published Online February 2013.

[11] **Arora C., K.K. Saini (2014)**,Survey of Various Mobility Models In VANETs published in International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 3 Issue 3 March 2014 Page No. 4073-4080.

[12] **Gayathri S.,S.Nithya, G.Shanthini, R.Janani, R.Ramachandiran (2018)**, ACO-ECDSA BASED SECURE ROUTING IN VANET: A BIO-INSPIRED APPROACH published in International Journal of Pure and Applied Mathematics Volume 119 No. 14 2018, 395-406 ISSN: 1314-3395 (on-line version) URL: http://www.ijpam.eu.

[13] **Kumar Vijaya, P. Inbavalli(2015),**Quantitative analysis on various safety centric based approaches in VANET, (2015) Global Conference on Communication Technologies, GCCT 2015, art. no. 7342778, pp. 834-837.

[14] **Thenmozhi R., P. Karthikeyan,Vijayakumar(2015),** Backtracking performance analysis of Internet protocol for DDoS flooding detection, (2015) IEEE International Conference on Circuit, Power and Computing Technologies, ICCPCT 2015, art. no. 7159474,

[15] **Saravanan D., V. Agalya, J. Amudhavel and S. Janakiraman (2016),** A brief survey on performance analysis and routing strategies on vanets, (2016) Indian Journal of Science and Technology, 9 (11), art. no. 89273.

[16] **Baskaran R.,M.S. Saleem Basha, J. Amudhavel, K. Prem Kumar(2015),** A bio-inspired artificial bee colony approach for dynamic independent connectivity patterns in VANET, (2015) IEEE International Conference on Circuit, Power and Computing Technologies, ICCPCT 2015, art. no. 7159384.

[17] **Agarwal A.,David Starobinski and Thomas D.C. Little (2012),**Phase transition of message propagation speed in delaytolerant vehicular networks,IEEETransactions on Intelligent Transportation Systems, vol. 13, no. 1, pp. 249–263, Mar. 2012.

[18] **Sahu P.,Eric Hsiao-Kuang Wu, Jagruti Sahoo (2013),**Bahg: Back-bone-assisted hop greedy routing for vanet ¸are city environments, IEEE Transactions on Intelligent Transportation Systems, vol. 14, no. 1, pp. 199–213, Mar. 2013.

[19] **Lochert C., Hannes Hartenstein, Jing Tian (2003),** A routing strategy for vehicular Adhoc networks in city environments, in Proc. IEEE IVS, Columbus, USA, Jun. 2003, pp. 156–161.

[20] **Jiang S.,Xiaoyan Zhu, Liangmin(2016),** An efficient anonymous batch authentication scheme based on HMAC for VANETs, IEEE Transactions on Intelligent Transportation Systems, vol. 17, no. 8, pp. 2193–2204, 2016.

[21] **Gaeini A., M. H. Ghaffari and Z. Mostaghim(2018)**, An improved hash function based on the Tillich–Zémor hash function, Researchgate Res. 3 DOI:10.22052/mir.2018.97876.1078 Article June 2018.

[22] **Mohsin Ur Rahman Salfi (2015)**, A study of mobile Adhoc networks – issues and challenges International Journal of Advanced Research in Computer Science, 6 (7), September–October, 2015,93-96.

[23] **Anuj K. Gupta (2009),** Secure Routing Techniques for Mobile Adhoc Networks IEEE International Advance Computing Conference (IACC 2009) Patiala, India, 6–7 March 2009.

[24] **Cui Jie, Zhang Jing(2018)**, HCPA-GKA: A hash function-based conditional privacy-preserving authentication and group-key agreement scheme for VANETs, Vol.14, Sept- 2018, https://doi.org/10.1016/j.vehcom.2018.09.003.

[25] **Stoilov Todor, Krasimira Stoilova (2005),** Routing algorithms in computer networks, Researchgate https://www.researchgate.net/publication/228822491 Article January 2005.

[26] **Solanki Shelbala, Anand Gadwal (2017)**,Evaluation of Hybrid Security Mechanism for AODV in MANET, IJCST Vol. 8, Issue 1, Jan - March 2017.

[27] **Reddy B. Prabhakara and Dr. M.N. Giri Prasad (2014),** Efficient Lightweight Hybrid Cryptography Solution to Secure Mobile Adhoc Networks, International Journal of Research in Computer and Communication Technology, Vol 3, Issue 3, March- 2014.

[28] **Lavanya M., V. Natarajan(2017),** LWDSA: a light-weight digital signature algorithm for wireless sensor Networks, Sadhana Vol. 42, No. 10, October 2017, pp. 1629–1643 DOI 10.1007/s12046-017-0718-5.

[29] **Hafeez Khalid Abdel, Lian Zhao, Bobby Ma, Jon W. Mark (2013),** Performance Analysis and Enhancement of the DSRC for VANET's Safety [30] Applications, IEEE transactions on vehicular technology, VOL. 62, NO. 7, September 2013.

[30] **Ryu Min-Woo, Si-Ho Cha, Kuk-Hyun Cho(2011),**DSRC-Based Channel Allocation Algorithm for Emergency Message Dissemination in VANETs, International Conference on Hybrid Information Technology ICHIT 2011: Convergence and Hybrid Information Technology pp 105-112.