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

International Journal of Innovative Research in Computer and Communication Engineering

*(A High Impact Factor, Monthly, Peer Reviewed Journal)*

*Website: www.ijircce.com*

Vol. 5, Issue 12, December 2017

# Review on Security Protocols in VANET

Yogita A. More [1], Nilima P. Patil[2]

P.G. Student, Department of Computer Engineering, S.S.B.T College of Engineering, Bambhori, Jalgaon, India[1]

Assistant Professor, Department of Computer Engineering, S.S.B.T. College of Engineering, Bambhori, Jalgaon, India[2]

**ABSTRACT**: An ad hoc network is a collction of wireless mobile nodes dynamically forming a temporary network without the use of any existing network infrastructure or centralized administration. There are number of routing protocols developed by researchers. Due to the nature of ad hoc networks, secure routing is an important area of research in developing secured routing protocols. Although researchers have proposed several secure routing protocols, their resistance towards various types of security attacks and efficiency are primary points of concern in implementing these protocols. After the evaluation of these protocols the results refer that they do not give complete protection against possible attacks and have some disadvantages on their performance.In this examined a new routing protocol called Modified Ad hoc On-demand Distance Vector (MAODV) routing protocol which is efficient and superior of the standard Ad hoc On-demand Distance Vector (AODV) routing protocol in performance, but is not secure. So proposed a new secure routing protocol based on MAODV which will be efficient and also immune against the most commonly possible routing attacks. Finally analyzed the proposed protocol against many attacks to ensure its security and also subject it to extensive simulation tests using NS2 simulation tool with the most commonly well-known ad hoc performance metrics to ensure its efficiency.

**KEYWORDS**: VANET, MANET, WANET

## I. INTRODUCTION

Vehicular ad hoc networks (VANETs) have recently attracted extensive attentions as a promising approach to enhancing road safety, as well as improving driving experience. By using a Dedicated Short-Range Communications (DSRC) [1] technique, vehicles equipped with wireless On-Board Units (OBUs) can communicate with other vehicles and fixed infrastructure, e.g., Road-Side Units (RSUs), located at critical points of the road [2]. Therefore, Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications are regarded as two basic types of communications in VANETs.

Once VANETs become available, numerous safe, commercial and convenient services can be deployed through a variety of vehicular applications. These applications mostly rely on vehicles' OBUs to broadcast outgoing beacon messages and validate incoming ones. The broadcast beacons often contain information about position, current time, speed, direction, driving status, etc. For example, by frequently broadcasting and receiving beacons, drivers are better aware of obstacles and collision scenarios. They may act early to avoid any possible damage, or to assign a new route in case of a traffic accident in the existing route. However, before implementing these attractive applications, particularly safety-related ones, we must first address and resolve VANET-related security issues [3], [4], To secure vehicular networks, an authentication scheme is indispensable to ensure messages are sent by legitimate vehicles and not altered during transmissions. Otherwise, an attacker can easily disrupt the normal function of VANETs by injecting bogus messages. Therefore, vehicles should broadcast each message with a digital signature. However, the current VANET signature standard [6] using Elliptic Curve Digital Signature Algorithm (ECDSA) would cause high computational overhead on the standard OBU hardware, which has limited resources for cost constraints. Prior work has shown that one ECDSA signature verification requires 20 milliseconds on a typical OBU with a 400 MHz processor [7]. When a large number of signed messages are received in a short time period, an OBU cannot process them before their dedicated deadline. In this paper, we define this attack as computation-based DoS attacks. Even without any malice, the computation-based DoS attacks can be easily initiated in a high-density traffic scenario. For

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

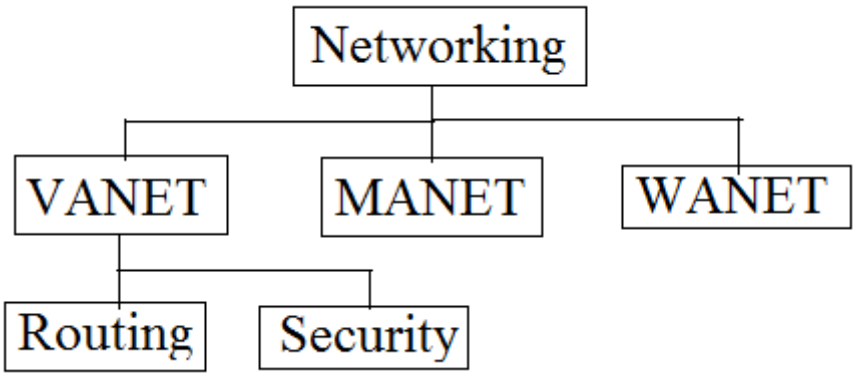
Vol. 5, Issue 12, December 2017

example, when traffic-related messages (beacons) are sent 10 times per second as suggested by the DSRC protocol [1], [6], a vehicle is overwhelmed with more than five neighbors within its radio range. To defend against such attacks, most existing schemes [8], [9], [10] make use of the technology of identity-based batch verification [11] or aggregate signature [12] built on asymmetric cryptography to improve the efficiency of verification. In their schemes, the computational cost is mainly dominated by a few operations of pairing and a number of operations of point multiplication over the elliptic curve [13]. It is affordable for RSUs, but expensive for OBUs to verify the messages [14]. Furthermore, if attackers inject false beacons, the receiver is hard to locate them so that these schemes are also vulnerable to the computationbased DoS attacks [15]. Therefore, designing an effective authentication scheme under high-density traffic scenarios is a big challenge for V2V communications.

In this paper, propose an effective broadcast authentication scheme: Prediction-Based Authentication (PROPOSED) to defend against computation-based DoS attacks for V2V communications. Unlike most of existing schemes based on asymmetric cryptography [8], [9], [10], [15], [16], [17], [18], [19], [20], our PROPOSED is primarily implemented on symmetric cryptography, whose verification is more than 22 times faster than ECDSA. In addition, PROPOSED resists packet losses naturally. Similar to mobile wireless networks, packet losses are common in VANETs. Especially, Bai et al. have shown that the packet loss rate can reach 30 percent in a benign network, and nearly 60 percent in a congestion network [21]. Design PROPOSED on the TESLA scheme [22], which is proposed to secure lossy multicast streams with hash chains. With TESLA signatures piggyback, PROPOSED operates smoothly even when the packet loss rate is high. PROPOSED also aims at improving the efficiency of authentication. Certain vehicular applications may require receivers to verify urgent messages immediately. To support instant verification, we exploit the property of predictability of a future beacon, constructing a Merkle Hash Tree (MHT) to generate a common public key or predication outcome for the beacon. With the prediction outcome known in advance, receivers can instantly verify the incoming beacon. Furthermore, examine the storage overhead brought by our authentication scheme. If a mechanism brings a large storage burden, an attacker would initiate memory-based DoS attacks where an OBU is overwhelmed by storing a large number of unverified signatures. To defend against such attacks, PROPOSED records shortened re-keyed MACs instead of storing all the received signatures. The design PROPOSED with an objective of providing effective, efficient, scalable broadcast authentication and also nonrepudiation in VANETs. To the best of our knowledge, prior authentication schemes for V2V communications either lack non-repudiation, or fail to operate in high packet loss or high-density traffic scenarios.

## II. BACKGROUND

In this section, we provide an overview of the VANET setting and the basic TESLA scheme.



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

International Journal of Innovative Research in Computer and Communication Engineering

*(A High Impact Factor, Monthly, Peer Reviewed Journal)*

*Website: www.ijircce.com*

Vol. 5, Issue 12, December 2017

## III.VANET

**Vehicular Ad Hoc Networks** (**VANETs**) are created by applying the principles of Vehicular Ad hoc Networks (VANETs) - the spontaneous creation of a wireless network for data exchange - to the domain of vehicles[1]. They are a key component of intelligent transportation systems (ITS).

While, in the early 2000s, VANETs were seen as a mere one-to-one application of VANET principles, they have since then developed into a field of research in their own right. By 2015,[1](p3) the term VANET became mostly synonymous with the more generic term **inter-vehicle communication** (**IVC**), although the focus remains on the aspect of spontaneous networking, much less on the use of infrastructure like Road Side Units (RSUs) or cellular networks.

### Vehicular Ad hoc Network

A **Vehicular Ad hoc Network** (**VANET**) is a continuously self-configuring, infrastructure-less network of mobile devices connected wirelessly.[1]

Each device in a VANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a VANET is equipping each device to continuously maintain the information required to properly route traffic[1]. Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology.[2]

VANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network. VANETs consist of a peer-to-peer, self-forming, self-healing network. VANETs circa 2000-2015 typically communicate at radio frequencies (30 MHz - 5 GHz)

The growth of laptops and 802.11/Wi-Fi wireless networking have made VANETs a popular research topic since the mid-1990s. Many academic papers evaluate protocols and their abilities, assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other. Different protocols are then evaluated based on measures such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput, ability to scale, etc.

### Types

- Vehicular ad hoc networks (VANETs) are used for communication between vehicles and roadside equipment. Intelligent vehicular ad hoc networks (InVANETs) are a kind of artificial intelligence that helps vehicles to behave in intelligent manners during vehicle-to-vehicle collisions, accidents.
- Smart phone ad hoc networks (SPANs) leverage the existing hardware (primarily Bluetooth and Wi-Fi) in commercially available smart phones to create peer-to-peer networks without relying on cellular carrier networks, wireless access points, or traditional network infrastructure. SPANs differ from traditional hub and spoke networks, such as Wi-Fi Direct, in that they support multi-hop relays and there is no notion of a group leader so peers can join and leave at will without destroying the network.
- Internet based Vehicular Ad hoc Networks (iVANETs) are ad hoc networks that link mobile nodes and fixed Internet-gateway nodes. For example, multiple sub-VANETs may be connected in a classic Hub-Spoke VPN to create a geographically distributed VANET. In such type of networks normal ad hoc routing algorithms don't apply directly. One implementation of this is Persistent System's CloudRelay.
- Military or tactical VANETs are used by military units with emphasis on security, range, and integration with existing systems. Common waveforms include the US Army's SRW.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

## Pros and cons

**1) Pros**

- No expensive infrastructure must be installed
- Use of unlicensed frequency spectrum
- Quick distribution of information around sender
- No single point of failure.

**2) Cons**

- All network entities may be mobile ⇒ very dynamic topology
- Network functions must have high degree of adaptability
- No central entities ⇒ operation in completely distributed manner.

**Routing:**

**3) 1) Proactive routing**

This type of protocols maintains fresh lists of destinations and their routes by periodically distributing routing tables throughout the network. The main disadvantages of such algorithms are:

1. Respective amount of data for maintenance.
2. Slow reaction on restructuring and failures.

Example: "Optimized Link State Routing Protocol" OLSR

***Distance vector routing***

As in a fix net nodes maintain routing tables. Distance-vector protocols are based on calculating the direction and distance to any link in a network. "Direction" usually means the next hop address and the exit interface. "Distance" is a measure of the cost to reach a certain node. The least cost route between any two nodes is the route with minimum distance. Each node maintains a vector (table) of minimum distance to every node. The cost of reaching a destination is calculated using various route metrics. RIP uses the hop count of the destination whereas IGRP takes into account other information such as node delay and available bandwidth.

**4) 2) Reactive routing**

This type of protocol finds a route on demand by flooding the network with Route Request packets. The main disadvantages of such algorithms are:

1. High latency time in route finding.
2. Excessive flooding can lead to network clogging.[9]

Example: "Ad hoc On-Demand Distance Vector" (AODV)

***Flooding***

Is a simple routing algorithm in which every incoming packet is sent through every outgoing link except the one it arrived on. Flooding is used in bridging and in systems such as Usenet and peer-to-peer file sharing and as part of some routing protocols, including OSPF, DVMRP, and those used in wireless ad hoc networks.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

### 5) Hybrid routing

This type of protocol combines the advantages of *proactive* and *reactive routing*. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding. The choice of one or the other method requires predetermination for typical cases. The main disadvantages of such algorithms are:

1. Advantage depends on number of other nodes activated.
2. Reaction to traffic demand depends on gradient of traffic volume.[10]

Example: "Zone Routing Protocol" (ZRP)

### 6) Position-based routing

Position-based routing methods use information on the exact locations of the nodes. This information is obtained for example via a GPS receiver. Based on the exact location the best path between source and destination nodes can be determined.

Example: "Location-Aided Routing in Vehicular Ad hoc Networks" (LAR)

## IV. SECURITY

Most ad hoc networks do not implement any network access control, leaving these networks vulnerable to resource consumption attacks where a malicious node injects packets into the network with the goal of depleting the resources of the nodes relaying the packets. To thwart or prevent such attacks, it was necessary to employ authentication mechanisms that ensure that only authorized nodes can inject traffic into the network.[16] Even with authentication, these networks are vulnerable to packet dropping or delaying attacks, whereby an intermediate node drops the packet or delays it, rather than promptly sending it to the next hop. Some behavior-based detection techniques have been developed to counter such attacks [17][18] in which a node overhears communication in the wireless neighborhood and determines if a neighbor is behaving correctly, i.e., forwarding the packet toward the intended recipient promptly.

**1.Flooding-Resilient Broadcast Authentication for VANETs**
In this work, we observe that signature flooding can be mitigated by broadcast authentication schemes whose overheads match the *entropy* of the broadcast messages [2]. We study this approach in the context of VANETs and propose two flooding-resilient broadcast authentication schemes, FastAuth and SelAuth, for different VANET applications. Our schemes are based on digital signatures thus providing non-repudiation. To the best of our knowledge, prior work on lightweight broadcast authentication either lacks the non-repudiation property or fails to operate efficiently in dynamic VANET environments. We briefly summarize our schemes.

**2.ABAKA: An Anonymous Batch Authenticated and Key Agreement Scheme for Value-Added Services in Vehicular Ad Hoc Networks** To tackle the aforementioned problems, including security, efficiency, and scalability problems, we proposed an anonymous batch authentication and key agreement (ABAKA) scheme to build a secure environment for value-added services in VANETs [3]. To avoid bottleneck problems, ABAKA is inspired by the concept of batch verification to simultaneously authenticate multiple requests sent from different vehicles using elliptic curve cryptography (ECC), which is adopted by the Trial-Use standard. Meanwhile, multiple session keys for different vehicles can also be negotiated at the same time. To the best of our knowledge, this is the first study that provides batch authenticated and key agreements for value added applications in VANETs

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

International Journal of Innovative Research in Computer and Communication Engineering

*(A High Impact Factor, Monthly, Peer Reviewed Journal)*

*Website: www.ijircce.com*

**Vol. 5, Issue 12, December 2017**

**3. Reconstruction of a Secure Authentication Scheme for Vehicular Ad Hoc Networks Using a Binary Authentication Tree** This necessitates and urges the development of a functional, reliable and efficient security architecture before all other implementation aspects of VANETs. Fundamentally, VANET security design should guarantee source authentication and message integrity. Besides these security requirements, sensitive information such as identities and location privacy should be preserved from the vehicle owner's perspective against unlawful tracing and user profiling. In contrast, traceability is required where the identity information needs to be revealed by law enforcement authorities for liability issues in the event of an accident or crimes[4]. Thus, privacy must be preserved and conditional. To ensure both source authentication and message integrity in VANETs, one appealing solution is to sign each message with a digital signature before the message is sent.
Several schemes have been proposed in the literature and can be mainly divided into the following two categories: traditional public-key-infrastructure (PKI)-based digital signature schemes and group signature-based security schemes. In both categories, each message needs to be signed by the sender using an asymmetric algorithm, and its receiver needs to verify the message that is received. Both of these schemes can effectively ensure secure communication while simultaneously protecting user privacy, but traditional PKI-based schemes may fail to satisfy the stringent time requirements of vehicular communication applications. Particularly as the traffic density increases, a vehicle may become unable to verify the authenticity of the messages sent by its neighbors in a timely manner, which results in message loss and, in turn, an increased risk to public safety.

**4. An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks** Fundamentally, VANET security design should guarantee authentication, nonrepudiation, integrity, and in some specific application scenarios, confidentiality, to protect the network against attackers. Besides the fundamental security requirements, sensitive information such as identity and location privacy should be preserved from the vehicle owner's perspective, against unlawful tracing and user profiling, since otherwise it is difficult to attract vehicles to join the network [6]. On the contrary, traceability is required where the identity information need be revealed by law enforcement authorities for liability issues, once accidents or crimes occur. In addition, privilege revocation is required by network authorities once misbehavior is detected during network access. It is less difficult to prevent misbehavior of unauthorized users since legitimate users and roadside units (RSUs) can simply disregard communication requests from outsiders by means of authentication.

**Disadvantages of Existing System**

- If the receiver misses a beacon, it cannot work in the rest of the current prediction interval.
- It cannot accurately collect the entire beacon message
- Also, it cannot increase the packet delivery ratio.

## V. CONCLUSION

In this paper proposed a new secure routing protocol in VANET which called Secure Modified Ad hoc On-demand Distance Vector (SMAODV) routing protocol. SMAODV is an on-demand routing protocol, but the main difference between SMAODV and other on demand routing protocols is that SMAODV uses the weight-based routing strategy which selects a stable routing path by maximizing the weight among all the feasible paths. The route selection is based on the weight value of each feasible path. In a feasible path, the less weight value represents less reliability. It also represents higher mobility of each node in the path. SMAODV always selects the most stable path for routing which it has the maximum weight value.

## REFERENCES

[1] S. Basagni, M. Conti, S. Giordano, Stojmenovi, and Cacute, in "Vehicular Ad hoc Networking," Wiley-IEEE Press, pp.1-33, 275-300, 330-354, September 2004.
[2] C. Siva, R. Murthy, and B.S. Manoj, in "Ad Hoc Wireless Networks, Architecture and Protocols," Pearson Education, pp. 321-386, 473-526, 2004.
[3] E. M. Royer, and C.K. Toh, "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks," IEEE Personal Communications Magazine, pages 46-55, April 2001.

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

International Journal of Innovative Research in Computer and Communication Engineering

*(A High Impact Factor, Monthly, Peer Reviewed Journal)*

*Website: www.ijircce.com*

**Vol. 5, Issue 12, December 2017**

[4] X. Hong, K. Xu, and M. Gerla, "Scalable Routing Protocols for Vehicular Ad hoc Networks," Computer Science Department, University of California, Los Angeles, August 2002.
[5] T. Lin, S. F. Midkiff, and J.S. Park, "A Framework for Wireless Ad Hoc Routing Protocols," Bradley Department of Electrical and Computer Engineering, Virginia Polytechnic Institute and State University, Blacksburg Virginia, 2003.
[6] V.Sumathy, P. Narayanasamy, J.James and S.Kanimozhi, "THROUGHPUT MAXIMIZATION ROUTING IN MOBILE AD-HOC NETWORK BY LINK BREAK PREDICTION," Academic Open Internet Journal, Volume 16, 2005.
[7] Z. Kai, W. Neng, and L. Ai-fang, "A new AODV based clustering routing protocol," Wireless Communications, Networking and Mobile Computing, on Proceedings of International Conference, IEEE, Volume 2, Issue 23-26, PP. 728 – 731, Sept. 2005.
[8] Wang, N.C., Y.F. Huang and J.C. Chen, "A stable weight-based on-demand routing protocol for Vehicular Ad hoc Networks," Information Sciences Vol. 177, Issue 24, pp. 5522-5537, December 2007.
[9] K. Khamforoosh, A. M. Rahmani, A. Sheikh Ahmadi, "A new multipath AODV routing based on distance of nodes from the network center," Communications, Propagation and Electronics, MIC-CPE, on Mosharaka International Conference, IEEE,
Volume 10, Issue 6-8, pp. 1– 5, March 2008.
[10] S. Tabatabaei, M.A. Jamali, "A stable weight-based Routing Algorithm to Increase Throughput in Vehicular Ad hoc Networks," Mobile computing, IEEE, 2009.
[11] M.G. Zapata, "Secure Ad hoc On-Demand Distance Vector (SAODV) Routing," IETF Internet Draft, draft-guerrero-VANET-saodv-00.txt, August 2001.
[12] L. Jun, L. Zhe, L. Dan, and L. Ye, "A security enhanced AODV routing protocol based on the credence mechanism," Wireless Communications, Networking and Mobile Computing, on Proceedings of International Conference, IEEE, Volume 2, Issue 23-26, pp. 719 – 722, Sept. 2005.
[13] D. Djenouri, O. Mahmoudi, M. Bouamama, D. Llewellyn-Jones, and M. Merabti, "On Securing VANET Routing Protocol Against Control Packet Dropping," on Pervasive Services, IEEE International Conference, Istanbul, ISBN: 1-4244-1325-7, pp. 100-108, 15-20 July 2007.
[14] N. Bhalaji, and A.Shanmugam, "ASSOCIATION BETWEEN NODES TO COMBAT BLACKHOLE ATTACK IN DSR BASED VANET," on Mobile Computing, IEEE, 2009.
[2] M.M. Ibrahim, N. Sadek, and M. El-Banna, "Prevention of Flooding Attack in Wireless Ad-Hoc AODV-based networks using Real-time Host Intrusion Detection," on Mobile Computing, IEEE, 2009.