IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of
Information Technology & Computer Engineering

ISSN 2347–3657

https://doi.org/10.62647/ijitce.2024.v12.i3.pp59-68

Volume 12, Issue 3, 2024

SECURITY ISSUES AND SOLUTIONS IN VEHICLE ADHOC NETWORKS

[1]Kadari Shireesha [2]Burugula Sunitha[3]Mohammad Raziuddin [4]Kummari Vasantha

[1, 2, 3,4]Asst Professor, Vidya Jyothi Institute of Technology, Hyderabad

Abstract:

When it comes to driving safety, vehicular networks are the way to go. As such, it is an integral part of the smart transportation network. While much study has gone into it, the security problem has received comparatively less focus. Here we'll go over some of the technical and security issues with VANET. We also go over some of the most significant assaults and how to counter them. Finally, we go into the mechanisms employed by the solutions and compare them on various metrics.

KEYWORDS: VANET, MANET, VANET defenses, assaults.

I. Introduction:

Since the 1980s, academics have been captivated by the idea of using wireless communication in cars [1]. There has been a dramatic uptick in studies focusing on this topic in recent years. The enormous commitment of major national and regional governments to allot wireless spectrum for vehicular wireless communication, the widespread adoption (and resulting decrease in cost) of IEEE 802.11 technologies, and the embrace of information technology by vehicle manufacturers to address safety, environmental, and comfort issues are all contributing factors. Direct connections between vehicles or between vehicles and infrastructure are not well-suited to cellular networks, despite the fact that these networks allow drivers and passengers to communicate vocally and access basic entertainment features. Nevertheless, real-time traffic updates and danger alerts may be sent and received by vehicular ad hoc networks (VANETs), which allow for direct connection between cars and roadside units (RSUs).

The efficiency and security of the road traffic environment are being compromised by the enormous amount of traffic these days. Annually, traffic accidents claim the lives of almost 1.2

million people. The most difficult problem in traffic management is ensuring the safety of road traffic. Giving cars access to traffic data so they may study their surroundings in relation to traffic is one option. The sharing of traffic environment data between cars may make this happen. A mobile network that can self-organize and function independently of fixed infrastructure is required since all the vehicles are inherently mobile. Microelectronic technology advancements have made ad hoc networks—which combine nodes and network devices into a single unit and allow for wireless interconnection—possible. Mobile ad hoc networks (MANETs) are an advanced form of this network [1]. One use of mobile ad hoc networks is VANET. When drivers and programmers link their vehicles to the internet, they create a self-organizing network called a VANET. The goal of this network is to make driving safer and better manage traffic. In VANET, there are two channels of communication.

A decentralised, wireless network that may run independently of physical infrastructure is known as an ad hoc network. Every node in a wireless ad hoc network acts as a router, directing data packets to other nodes as needed. Wireless ad hoc networks may use personal digital assistants, workstations, or even desktop PCs as its nodes. Depending on the current state of the network, a node is assigned the task of sending data packets to other nodes along the most efficient route. Only with a network connection can this be made feasible. Not only can an ad hoc network route data, it can also forward data using the flooding approach. There are a few different names for wireless ad hoc networks; 802.11 is one of them.

There are 116 fatalities and 7,900 injuries caused by car accidents in the US every single day. There are more than 100 fatalities and 4,600 injuries every day in the European Union, and the yearly cost is €160 billion [6]. In the United States, treating accident victims consumes more health care costs than any other source of disease or injury [3, 4, 5]. As a result, governments and car makers are prioritizing efforts to reduce vehicle deaths [4], [7].

II. Literature survey:

1. A Survey on Mobile Ad Hoc Network (MANET):

Almost everyone these days has a mobile device on them. Using these gadgets to connect with people is something everyone wants to do. Through mobile networks, individuals are able to

transmit mobile connections to one another. An ad-hoc network is the only technology that can make this a reality. Wireless Ad Hoc Networks and MANETs are the extensive topics covered in this study. MANET refers to a network of mobile nodes that can interact with each other and move in any direction. Some of the routing techniques used by MANETs to move data packets throughout the network are covered in this paper, along with the many types of MANETs. In addition, the algorithms' protocols are detailed in this study. The research concludes by comparing the efficiency of various methods.
Mobile Ad-Hoc Network, Algorithms, VANET, MANET, and protocols

2. VEHICLE AD HOC NETWORKS: APPLICATIONS AND RELATED TECHNICAL ISSUES:

The current status of car ad hoc networks is thoroughly examined in this article. We begin by outlining the needs of the two main types of VANET apps—safety applications and user applications—and by examining the potential uses of these applications. We next organize the solutions that have been suggested in the literature based on where they fall in the open system interconnection reference model and how they relate to user applications or safety. We point out their strengths and weaknesses and provide alternatives that we believe would be more effective. Also included are details on the various approaches used to model and assess the solutions put forward. Lastly, we wrap off by proposing a generic design that may serve as the foundation for a functional VANET.

3. STRONG VANET SECURITY ON A BUDGET:

An appropriate security authentication procedure for VANETs is suggested in this article. The technique outperforms existing Public Key Infrastructure (PKI) solutions for VANET authentication in terms of compute and bandwidth efficiency. The plan use the passage of time to generate asymmetric information. A lengthy string of keys is generated by a sender. There is a limited amount of time that each key is utilized to sign messages. A key is made public when it expires and is thereafter never used again. (Further messages are signed by the sender using the key that follows in its chain.) Recipients verify the authenticity of communications they have previously received after obtaining a disclosed key. A certificate issued by an authority specifies the root of the sender's keychain. Numerous approaches of exchanging certificates are detailed in this page. Concerning privacy in VANET, it handles the conflict between anonymity and certificate revocation.

4. The Security of Vehicular Ad Hoc Networks:

As far as mobile ad hoc networks go, vehicular networks are shaping out to be the most important kind. The safety of such systems is the focus of this article. In addition to coming up with a suitable security architecture, we provide a comprehensive threat analysis. Furthermore, we detail a number of important design choices that are still open, some of which have consequences beyond those of a purely technical nature. We provide a suite of security protocols, demonstrate that they safeguard privacy, evaluate their robustness, and do a quantitative evaluation of the suggested remedy.

5. A Tutorial Survey on Vehicular Ad Hoc Networks:

In recent years, the area of vehicle ad hoc networks has seen a lot of attention and development. Communications between vehicles and between vehicles and infrastructure are a part of VANETs, which are based on wireless LAN technology. The dinstinctive set of candidate applications (e.g., collision warning and local traffic information for drivers), resources (licensed spectrum, rechargeable power source), and the environment (e.g., vehicular traffic flow patterns, privacy concerns) make the VANET a unique area of wireless communication. Motives, obstacles, and a brief summary of solutions are all included in this article's review of the area.

6. Guide to Elliptic Curve Cryptography:

Beginning in the mid-nineteenth century, elliptic curves were studied by algebraists, algebraic geometers, and number theorists. There is already a mountain of written material eulogizing the exquisite qualities of these fantastic artifacts. An elegant method for factoring integers based on elliptic curve features was detailed by Hendrik Lenstra in 1984. Scientists looked for more uses of elliptic curves in computational number theory and cryptography after this finding. Whitfield Diffie and Martin Hellman came up with the idea of public-key cryptography in 1976. In 1977, the now-famous RSA cryptosystem—proposed by Ron Rivest, Adi Shamir, and Len Adleman—became the first practical manifestation. This system bases its security on the fact that the integer factorization problem is intractable. In 1985, Neal Koblitz and Victor Miller made the discovery of elliptic curve cryptography (ECC). Similar to RSA systems, elliptic curve cryptography techniques use public keys to encrypt and decrypt data. But another issue, the elliptic curve discrete logarithm problem (ECDLP), provides the basis for its security. Whereas the best methods for the integer factorization problem are known to have subexponential time complexity, the best algorithms for the ECDLP currently have completely exponential time complexity. This implies that elliptic curve systems may provide the appropriate degree of security with far fewer keys compared to their RSA equivalents. For instance, there is consensus that an elliptic curve key with 160 bits of encryption is just as secure as an RSA key with 1024 bits of encryption. Speed and effective use of power, bandwidth, and storage are some of the benefits that may be realized with lower key sizes.

7. A Group-based NTRU-like Public-key Cryptosystem for IoT:

The internet of things has greatly enhanced our everyday lives. Internet of Things (IoT) security relies heavily on public-key cryptosystem. Internet of Things (IoT) applications cannot make use of traditional public-key cryptosystems like RSA and ECC due to the complexity of their encryption and decryption processes. NTRU is a public-key cryptosystem that works well. The study begins by proposing GTRU, a group-based public-key cryptosystem similar to NTRU, and then generalizes NTRU. We next build an Internet of Things (IoT) GTRU with top performance. Lastly, when it comes to lattice-based attacks, our suggested GTRU for IoT is more safe than NTRU, according to the security study.

8. A Survey of Existing Approaches for Secure Ad Hoc Routing and Their Applicability to VANETS:

Intelligent transportation systems of the future will be based on vehicular ad hoc networks, or VANETs. In addition to enhancing road safety and passenger comfort, they have many other potential uses. Data security in a vehicle system is necessary since VANET applications impact safety-of-life. Security solutions for vehicle environments face distinct problems from VANETs due to their unique properties compared to typical mobile ad hoc networks and sensor networks. Several methods exist for safe routing, each tailored to a specific setting and set of security goals; the majority of these methods are extensions of popular ad hoc routing protocols. All of the current solutions are described in this study at a similar degree of abstraction, and they are reviewed methodically. When it comes to the security methods and performance standards that were put into play, the study then compares the solutions. The paper concludes by determining whether the chosen methods' characteristics satisfy VANETs specifications. At a high level, the examined ideas' primary security goals (authentication, integrity, and maybe non-repudiation) align with what may be needed for secure VANET routing. Additional security precautions are necessary since future VANET routing is anticipated to be based on a specialized routing protocol that leverages positions of forwarding. There are safeguards in place to prevent some attacks from taking advantage of the positions included in data packets, as well as safeguards to protect beaconing and location service inside the routing protocol and to guarantee location privacy. Because of these factors, a one-of-a-kind security solution for VANETs must be developed. However, it is also possible to draw conclusions about what makes VANETs secure from analyzing their features. These include things like fewer processing and power limits, centralized registrations, regular technical inspections, and preexisting law enforcement protocols.

9. Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks:

In an ad hoc network, which consists of a collection of mobile wireless computers (called "nodes"), the nodes work together to interact with one another even when their direct wireless transmission range is limited. The routing issue in ad hoc networks has often been investigated in a trusting, non-adversarial situation in earlier studies. We introduce threats to ad hoc network routing and describe Ariadne, a novel secure on-demand routing system for ad hoc networks, along with its design and performance assessment. Ariadne blocks a wide variety of DoS threats and stops attackers or compromised nodes from interfering with routes that are intact and comprised of uncompromised nodes. Ariadne also makes good use of time by sticking to efficient symmetric cryptography primitives. Sorting by Subject and Category: Section C.0 deals with computer-communications network security, while Section C.2.2 is devoted to routing protocols in the realm of network protocols.

III. Existing system:

Here we'll go over some of the technical and security issues with VANET. We also go over some of the most significant assaults and how to counter them. Finally, we go into the mechanisms employed by the solutions and compare them on various metrics.

IV. proposed system:

Here we go over a few technologies that are used in various solutions. Two of VANET's most pressing concerns are user authentication and privacy. Nevertheless, VANET does not need secrecy because, in most cases, network packets do not include sensitive information.

Methodology:

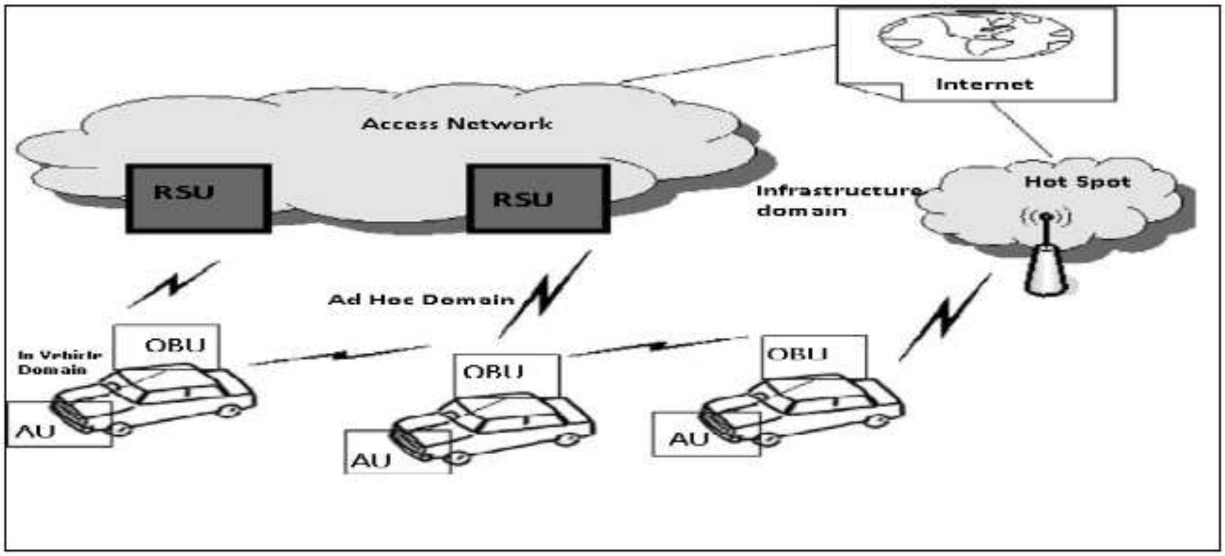
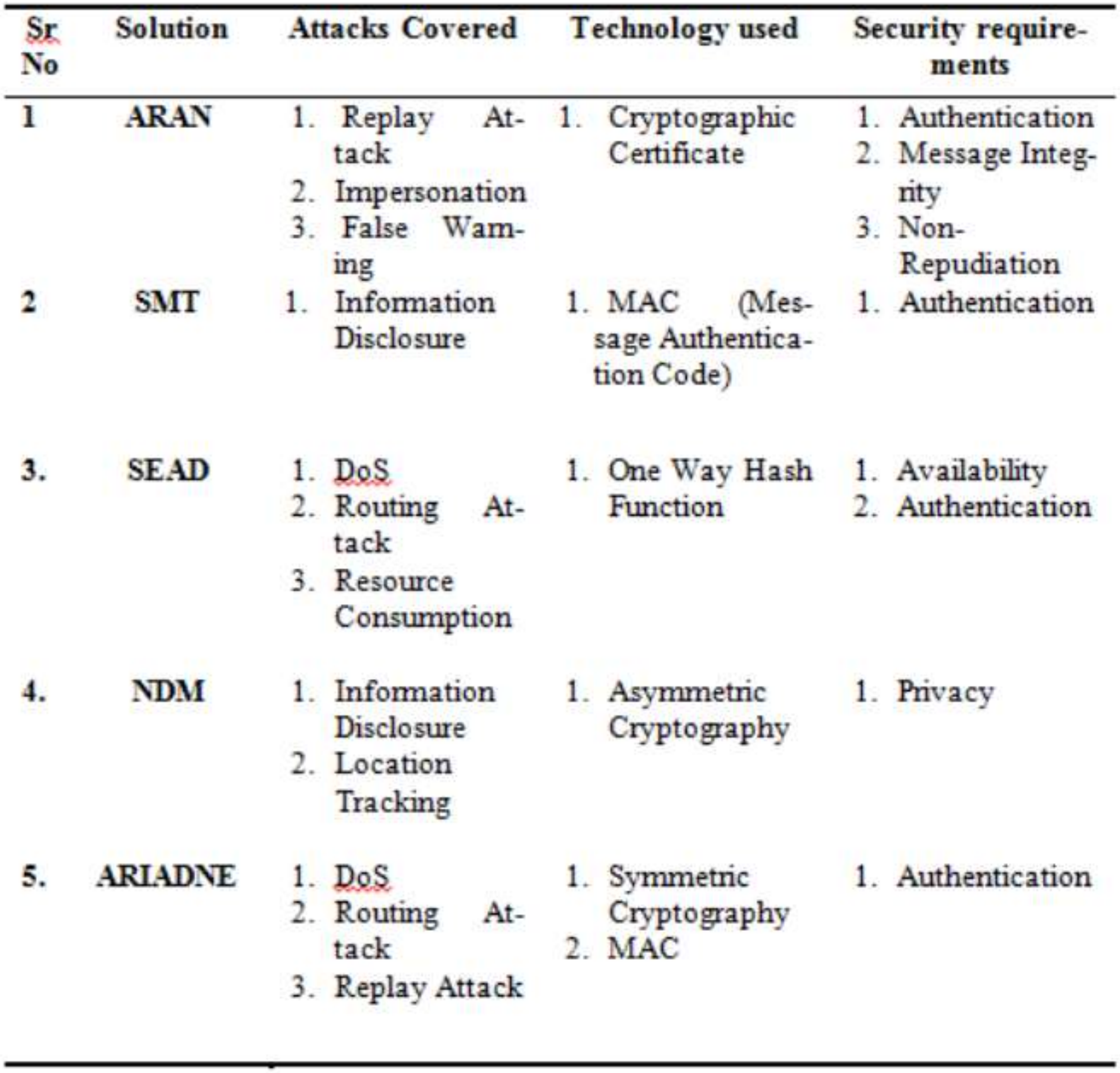


Table 1. Comparison of solutions



Sr No	Solution	Attacks Covered	Technology used	Security requirements
1	ARAN	1. Replay Attack 2. Impersonation 3. False Waming	1. Cryptographic Certificate	1. Authentication 2. Message Integrity 3. Non-Repudiation
2	SMT	1. Infomation Disclosure	1. MAC (Message Authentication Code)	1. Authentication
3.	SEAD	1. DoS 2. Routing Attack 3. Resource Consumption	1. One Way Hash Function	1. Availability 2. Authentication
4.	NDM	1. Infomation Disclosure 2. Location Tracking	1. Asymmetric Cryptography	1. Privacy
5.	ARIADNE	1. DoS 2. Routing Attack 3. Replay Attack	1. Symmetric Cryptography 2. MAC	1. Authentication

Conclusion:

Security is the major issue to implement the VANET. In this article, we study the security requirements and challenges to implement the security measure in the VANET. Different types of attacks and their solutions are also discussed. We discuss some technologies which are used in the different solutions. Among all requirements authentication and privacy are the major issues in VANET. However confidentiality is not required in VANET because generally packets on the network do not contain any confidential data.

References:

[1] S. Sesay, Z Yang and Jianhua He, "A survey on Mobile Ad Hoc Network", Information Technology Journal 3 (2), pp. 168-175, 2004

[2] Moustafa,H., Zhang,Y.: Vehicular networks: Techniques, Standards, and Applications. CRC Press, (2009).

[3] Yaseer Toor et al., "Vehicle Ad Hoc Networks : Applications and Related Technical issues", IEEE Communications surveys & Tutorials , 3rd quarter 2008, vol 10, No 3,pp. 74-88.

[4] Y.- C. Hu and K. Laberteaux, "Strong Security on a Budget," Wksp. Embedded Security for Cars, Nov. 2006;

[5] Maxim Raya e al., "The Security of Vehicular Ad Hoc Networks", SASN'05, Nov 7 2005, Alexandria, Verginia, USA, pp. 11-21

[6] Hannes Hartenstein et al., "A tutorial survey on vehicular Ad Hoc Networks" , IEEE Communication Magazine, June 2008, pp. 164-171

[7] Jose Maria de Fuentes, Ana Isabel Gonzalez-Tablas, and Arturo Ribagorda, "Overview of Security issues in Vehicular Ad Hoc Networks", Handbook of Research on Mobility and Computing, 2010.

[8] Murthy, C. S. R.,Manoj, B. S.: Ad Hoc Wireless Networks: Architectures and Protocols. PEARSON,ISBN 81-317-0688-5, (2011).

[9] Dahill, B. N. Levine, E. Royer and Clay Shields, "A Secure Routing Protocol for Ad Hoc Networks", Proceeding of IEEE ICNP 2002, pp 78-87, Nov 2002.

[10] Y. C. Hu, D. B. Johnson and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks", Elsevier B. V. , pp 175-192, 2003

[11] P. Papadimitratos and Z. J. Haas, "Secure Data Transmission in Mobile Ad Hoc Network", ACM Workshop on Wireless Security, San Diego , CA, September 2003.

[12] Fasbender, D. Kesdogan and O. Kubitz, "Variable and Scalable Security: Protection of Location Information in Mobile IP", IEEE VTS , 46th Vehicular Technology Conference, USA, 1996.

[13] Y. C. Hu, A. Perrig and D. B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", MobiCom'02, pp. 23-26,2002

[14] Fonseca and A. Festag, "A survey of Existing Approaches for Secure Ad Hoc Routing and Their Applicability to VANETS", NEC Network Laboratories, 2006. https://www.researchgate.net/publication/242415320_A_Survey_of_Existing_Approaches_for_Secure_Ad_Hoc_Routing_and_Their_Applicability_to_VANETS

[15] Xiaodong Lin et al., “Security in Vehicular Ad Hoc Network”, IEEE communications magazine , April 2008, pp. 88-95

[16] Menezes, S. Vanstone, and D. Hankerson, "Guide to elliptic curve cryptography", Springer Professional Computing (Springer, New York 2004).

[17] J. Hof fstein, J. Pipher, J. H. Silverman, "NTRU: A ring- based public key cryptosystem", Lecture Notes in Computer Science, Vol. 1423, 1998, pp 267-288.