Journal of Information
2018 Vol. 4, No. 1, pp. 1-9
ISSN(e): 2520-7652
DOI: 10.18488/journal.104.2018.41.1.9
© 2018 Conscientia Beam. All Rights Reserved.

SECURITY THREATS AND PRIVACY ISSUES IN VEHICULAR AD-HOC NETWORK (VANET): SURVEY AND PERSPECTIVE

Emmanuel Bamidele Ajulo[1+]
Raphael Olufemi Akinyede[2]
Olumide Sunday Adewale[3]

[1,2,3]*Department of Computer Science, Federal University of Technology, Akure, Nigeria*
[1]*Email: emmanuelajulo@gmail.com Tel: +2348024607812*
[2]*Email: roakinyede@futa.edu.ng Tel: +2348034702718*
[3]*Email: adewale@futa.edu.ng Tel: 2348033616386*

(+ Corresponding author)

Article History
Received: 1 June 2018
Revised: 19 June 2018
Accepted: 25 June 2018
Published: 29 June 2018

Keywords
Vehicular Ad-Hoc networks (VANETs)
Intelligent Transport System (ITS)
Road-Side Units (RSUs)
OBU
DSRC
WAVE
Node
Bandwidth
Security and privacy threats
Attackers.

ABSTRACT

In Vehicular Ad Hoc Networks (VANETs) Wireless-equipped vehicles are able to communicate with each other as well as Road-Side Units (RSUs) located at strategic places on the road, this enables the formation of self-organized networks connecting the vehicles and RSUs. The (vehicles) nodes are fast mobile causing the network topology to change frequently and unpredictably. Since VANETs do not really rely on any form of central administration or control, nodes in the wireless range dynamically discover each other and establish connection with each other. Due to the pervasive nature of the mobile nodes, it cannot be assumed that VANETs will always be under the control of their owners; nodes could be stolen or tampered with. Each vehicle (node) acts as an independent router and fault detection and network management becomes distributed and more difficult. The shared wireless medium is accessible to both legitimate and illegitimate users; and this has raise formidable research challenges to providing security for this network. This paper take a selective review of the published research work carried out in the security and privacy issue of VANET between 2003 and 2015 and derived a new perspective into the security and privacy attacks in VANET.

Contribution/Originality: This study is one of the very few studies which have investigated security and privacy issues in VANET. We carried out a selective review of published work on this field between 2003 and 2015; and based on our findings, derived a new perspective, and categorized the security attacks on this type of network.

1. INTRODUCTION

Vehicular Ad-Hoc Networks (VANETs) is an extension of Mobile Ad-Hoc Networks (MANETs). In Vehicular Ad-hoc Networks (VANETs), wireless-equipped vehicles form a network spontaneously while traveling along the road. Direct wireless transmission from vehicle to vehicle makes it possible to communicate even where there is no telecommunication infrastructure, such as base stations or access points of wireless dedicated access networks; vehicles can share up-to-date traffic information on the fly [1]. This is an emerging new technology to integrate the capabilities of new generation wireless networks to vehicles. The idea is to provide ubiquitous connectivity to vehicular nodes while on the move, and create efficient vehicle-to-vehicle communications that enable the Intelligent Transportation Systems (ITS) [2].

The network is based on node to node communication. A node can either be a user (vehicle) who desires certain information, or a Road Side Unit (RSU). The node, be it vehicles or RSU, can communicate and exchange data for purposes of information inquiry or distribution. The ultimate goal of VANETs is to enhance the driving experience and increase the level of safety for drivers [3-6]. This is achieved by allowing nodes within certain ranges to connect with each other in order to exchange information. According to Chlamtac, et al. [7] and Tokuda [8] Smart vehicles with the appropriate wireless Information Technology (IT) are able to communicate with each other as well as Road-Side Units (RSUs) located at strategic places on the road, such as junctions. This enables the formation of self-organized networks connecting the vehicles and RSUs [5, 9, 10].

VANET, like every other network is not without security challenges; each vehicle (node) acts as an independent router and generates independent data thus fault detection and network management becomes distributed and more difficult. The nodes are fast mobile causing the network topology to change frequently and unpredictably, nodes in the wireless range dynamically discover each other and establish connection with each other. Due to the pervasive nature of mobile nodes, it cannot be assumed that VANETs will always be under the control of their owners; nodes could be stolen or tampered with because their shared wireless medium is accessible to both legitimate and illegitimate users; making the possibility of eavesdropping, spoofing, and denial-of-service attacks more prevalent [11-13].

Khatri and Malhotra [2] revealed that a number of distinctive factors need to be taken into consideration when designing systems to secure VANET, these factors include: The nature of communication which is based on node-to-node communication, mobility and dynamic-nature in which nodes are constantly changing their locations (except RSUs) with different speeds and directions, frequent exchange of information, and Real time and fast processing of information that should not take time in order to correctly exchange information. This paper take a selective review of the published research work carried out in the security and privacy issues of VANET between 2003 and 2015 and derives a new perspective into security and privacy attack formation in VANET. Section 2 of this paper gives a further overview of VANET; other related works were reviewed in section 3, Section 4 shows the new derived perspective to security and privacy attacks in VANET and section 5 concluded this work.

2. OVERVIEW OF VEHICULAR AD-HOC NETWORK (VANET)

Vehicular Ad-Hoc Networks (VANETs) is a sub-class of Wireless Ad-hoc Networks (WANETs), and an extension of Mobile Ad-Hoc Networks (MANETs). In a VANET, vehicular nodes operate in a peer to peer mode independent of any infrastructure or a centralized administration; to communicate with nodes beyond the range; intermediate nodes forward messages to destination node over multiple hops [10, 14]. Each node acts as an independent router and generates independent data. VANETs do not rely on any form of central administration or control; nodes in the wireless range dynamically discover each other and establish connection. This helps to maintain the ad-hoc network even in situations where nodes keep moving in and out of each other's wireless range [15]. Figure 2.1 shows the general breakdown of the network.

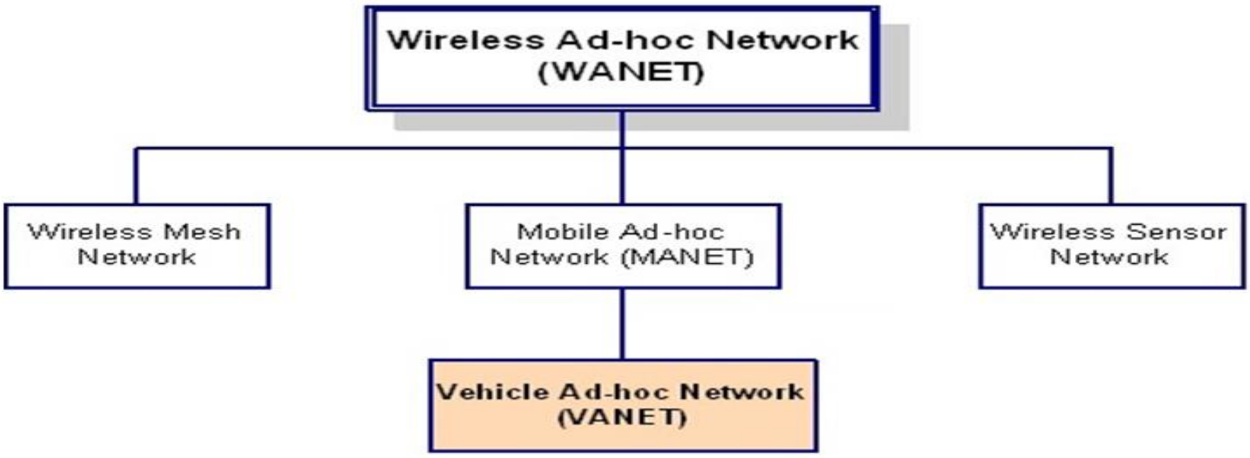
Wireless Ad-hoc Network (WANET)
Wireless Mesh Network
Mobile Ad-hoc Network (MANET)
Wireless Sensor Network
Vehicle Ad-hoc Network (VANET)

Figure-2.1. Hierarchy of Wireless Ad-hoc Networks

(**Source:** La and Cavalli [10])

Figure 2.2 shows the basic structure of VANETs. The vehicles or RSUs nodes in VANETs act both as end points and routers. This network is emerging as the first viable commercial implementation of MANETs (Mobile Ad-hoc Networks) [2, 16-18].

The interest by the automotive manufacturers in the technology has gathered momentum in recent years to the point where new standards called the IEEE 1609 WAVE (Wireless Access in Vehicular Environment) have emerged. The standards basically include enhancements to the IEEE 802.11 in order to support wireless communication among [15, 16, 19]. The IEEE Standard 802.11p and the protocol stack 1609.x together define the foundation for the wireless communications among the different entities –that is, the On-Board Units known as the OBUs which is the transceiver device for vehicles and RSUs which is the transceiver device for road sides' infrastructures of VANETs [20-22].

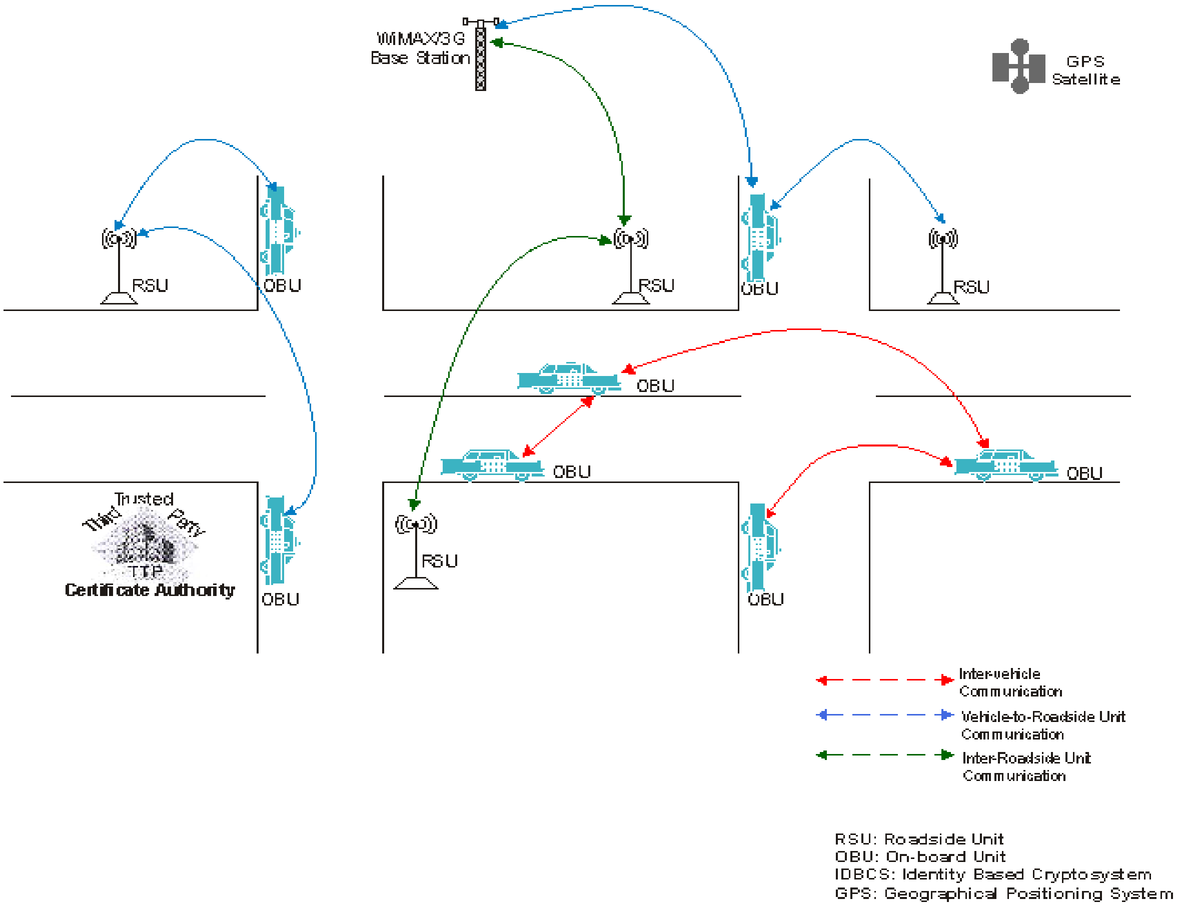

Figure-2.2. The Basic Structure of VANETs

(**Source:** Bhuvaneshwari, et al. [18])

This new paradigm of communication has motivated lots of efforts in academic and standardization communities. The United States of America's (USA's) Federal Communications Commission (FCC) has allocated seven 10MHZ channels in the 5.9GHz band for Dedicated Short Range Communication (DSRC) for the Intelligent Transportation System (ITS) to enhance the safety and productivity of the transportation system [6, 23-25]. The DSRC applications are to be built over OBUs and RSUs. The DSRC provides seven channels with each having 10 MHz of bandwidth. Within the 5.9 GHz spectrum, channel 172 is an unused channel, while channel 184 is the High Availability Low Latency (HALL) channel kept for future use. Channels 174,176, 180, and 182 are defined as Service Channels (SCH), whereas channel 178 is specified as the Control Channel (CCH) for the WAVE communications. During communication, two consecutive DSRC channels can be combined to one when additional bandwidth is required by a VANET. A 10 MHz channel offers the data rate up to 27 Mbps, where 3, 6, and 12

Mbps data rates are mandatory. A 20 MHz combined channel would offers a maximum of 54 Mbps with mandatory data rates of 6, 12, 24 Mbps. However, data transmission rates in WAVE communication also depend on different speed levels of vehicles. A vehicle speeding 0-60 Km/hour can achieve VANET data rates 9, 12, 18, 24, and 27 Mbps, whereas, for 60-120 Km/hour vehicle speed, data rates 3, 4.5, 6, 9, and 12 Mbps are achievable [26].

The DSRC supports a number of different network protocols for interoperability in the hope of gaining widespread adoption. It supports the long-established TCP/IP protocol, which allows IP based routing in DSRC. As a result of supporting TCP/IP, most of the traditional Internet applications are available in the VANET. The communication range of an IEEE 802.11p device using the 5.9 GHz radio is limited to 1 Km at the most, which varies based on the different transmission power of the WAVE transceiver. Vehicles (OBUs) join and exchange information with their nearest RSU's while a vehicle's dwell time may be as short as 3.6 sec [21, 27]. This short dwell time of an OBU allows VANET applications only with low processing time and latency. Figure 2.3 shows the DRSC 5.9 GHz band spectrum.

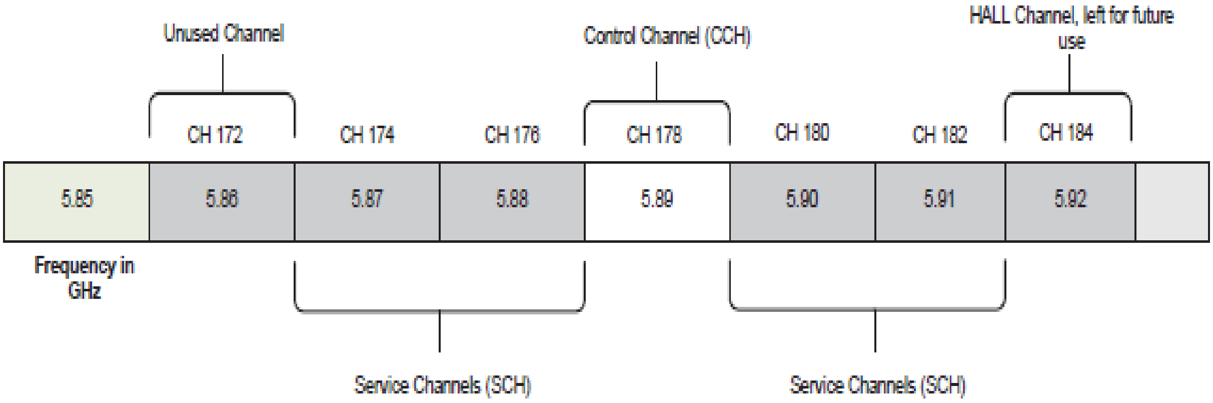

Figure-2.3. Layout of DRSC 5.9 GHz Frequency Band Spectrum

(**Source:** Biswas [26])

VANETs can provide many applications that are safety or entertainment oriented; this include: The provision of road conditions information, traffic conditions, accident reporting which help the authorities to maintain road status, entertainment, internet access and many more [28, 29]. The diversity of these applications is driven by the fact that VANETs are ultimately considered a form of pervasive networks.

3. REVIEW OF LITERATURES

There are different types of security attacks and network adversaries that can pose threat to a VANET. Just like any other wireless network, a VANET is prone to network attack. According to Papadimitratos, et al. [30] attackers can be of several forms each with different levels of impact on the network, some of these are: drivers looking only for their best interest to deceive other nodes that a certain route is blocked in order to clear the path to its (adversary's) destination; users such as robbers might misuse the network trying to extract data from the network to help them locate places with no cars. Malicious attackers are considered the most dangerous category since they can cause severe damage to the network; possible attacks from this category ranges from eavesdropping to terrorism attacks [4, 31].

Parno and Perrig [31]; Raya and Hubaux [4] In their quest described the need to categorize the definition of adversaries as it helps in determining the scope of resources needed to secure a vehicular system. They considered broad classes of adversaries' model categorized as Active versus Passive, Insider versus Outsider, Malicious versus Rational, Independent versus Colluding, and Local versus Extended. A passive attacker is an eavesdropper on the wireless channel, while an active attacker can generate, modify, drop or replay messages in order to give false information to the network vehicles so that attackers can maximize their gain on the network irrespective of the costs. Insider attacker is an authenticated member of the network who can communicate with other members. Being a part of the network, an insider is already in possession of some network credentials, like public keys [4]. An insider can cause more damage to the system by tampering with an OBU, than an outsider who has limited access to the system.

A Malicious attacker seeks no personal benefits from the attacks, and only aims to harm the members or the functionality of the network [4, 31]. Hence, he may employ any means disregarding corresponding costs and consequences. On the contrary, a rational attacker seeks personal profit and hence is more predictable in terms of the attack means and the attack target. Attackers may also act independently or in collusion; where they exchange information and cooperate to make attacks more effective. A colluding vehicle can report an imaginary traffic jam or accident to convince other drivers (since the report comes from multiple vehicles others are likely to believe it) and clear way for the attackers [28].

The effect of attackers' on the network can also be limited in scope, even if he controls several entities (vehicles or RSU), which makes him local. This is because the limited range of OBUs and RSUs make the attack scope limited. An attacker may also be said to be an extended attacker, if he controls several entities that are scattered across the network, thus extending his scope. This distinction is especially important in privacy-violating and wormhole attacks. This made Maiwald [32] categorized each type of attack that affects some of the security services in the VANE; and termed it 'CIA' which stands for Confidentiality, Integrity, Accountability, and Availability.

Aboobaker [33] identified the most common and devastating forms of attacks that a VANET can suffer as Denial of Services (DoS), Fabrication, Alteration and suppression of data, Sybil attack, Masquerading, Privacy violation, and On-board tampering. He described Denial of Services (DoS) as a very simple, but yet lethal attack. In this attack a node might continuously send unwanted data across the network so that it enters a gridlock or deadlock state where other nodes are unable to communicate due to channel blocking. This attack can either deny access to information or applications or even the whole VANET. For a fabrication attack an attacker send incorrect information to other nodes for different purposes. These types of attacks can be very dangerous because they affect the validity of the data received by nodes [34].

In alteration and suppression of data attacks mentioned by Aboobaker [33], adversary nodes can receive valid data, alter it and resend it to other nodes. Moreover, an adversary can prevent communication between two nodes by dropping certain messages between them. These attacks cause false data and confusion to be distributed among the network nodes and hence it affects performance. The Sybil attack is a situation where malicious node attempts to create other nodes, which in turn, make other nodes malicious and hence control significant portions of the network and misused it. Sybil attack is as dangerous as Denial of Service (DoS) attacks because it can destroy valid communication in the network while Masquerading attacker actively pretends (impersonates) to be another vehicle by using false identities, stealing users personal data on the network and by inference violates their privacy [1, 10, 33].

4. OUR PERSPECTIVE ON SECURITY REQUIREMENTS FOR VANET

The derived perspective on security and privacy attacks on VANETs by this research are succinctly categorize into four types namely: Interruption, Interception, Modification and Fabrication attackers.

4.1. Interruption Attack

This is attack on availability. information from the Source Vehicle (SV) is unable to get to the Destination Vehicle (DV) as a result of intrusion activity such as junks packets denying information flow and service availability. Figure 4.1 shows interruption attack between Source Vehicle (SV) and Destination Vehicle (DV).

4.2. Interception Attack

This is attack on confidentiality. The Source Vehicle (SV) is sending message to Destination Vehicle (DV), but the Intruder (I) is reading the message being transmitted. This occur when Intruder (I) have access into intermediate network like router, and passively listening to the message. This can also be described as an attack on Privacy. Figure 4.2 shows interception attack between Source Vehicle (SV) and Destination Vehicle (DV).

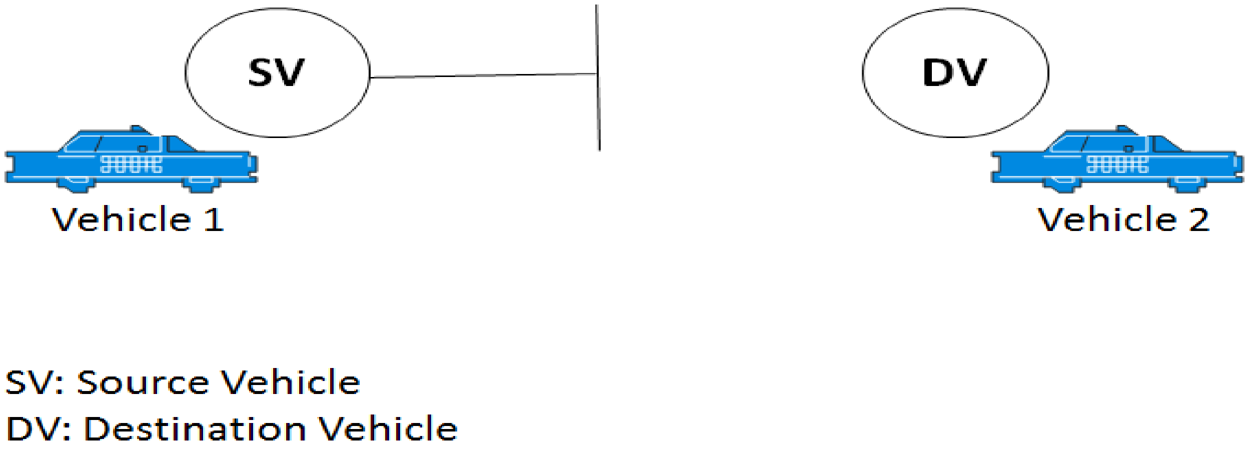

Figure-4.1. Interruption Attack between Source Vehicle and Destination Vehicle

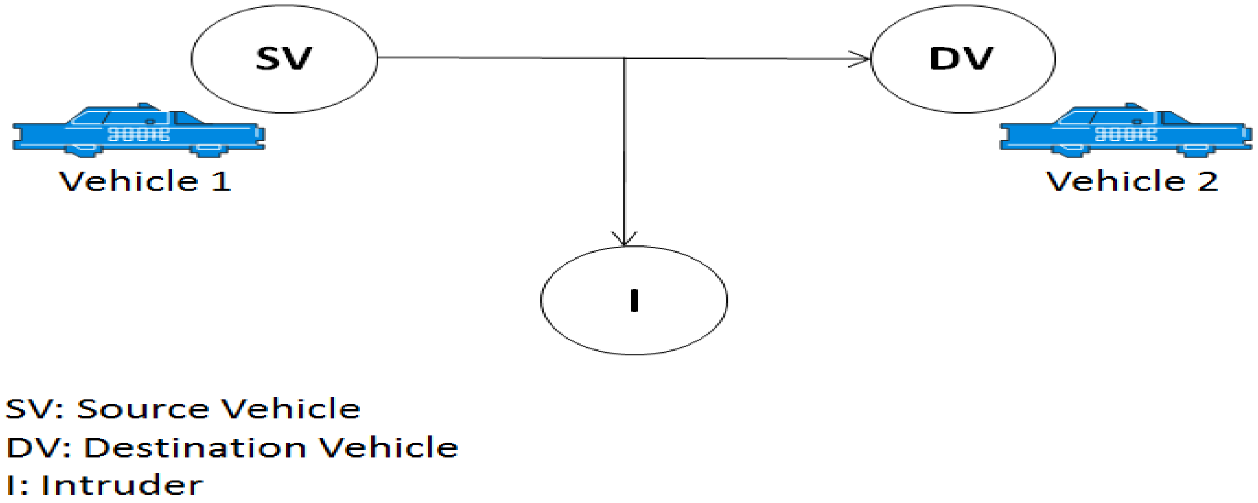

Figure-4.2. Interception Attack between Source Vehicle and Destination Vehicle

4.3. Modification Attack

This is attack on integrity. The Intruder (I) has access to intermediate network like the router, but beyond passively listening to the message, the Intruder (I) tampers and modifies the message. This is a Read-Modify-Send scenario attack. Figure 4.3 shows modification attack between Source Vehicle (SV) and Destination Vehicle (DV).

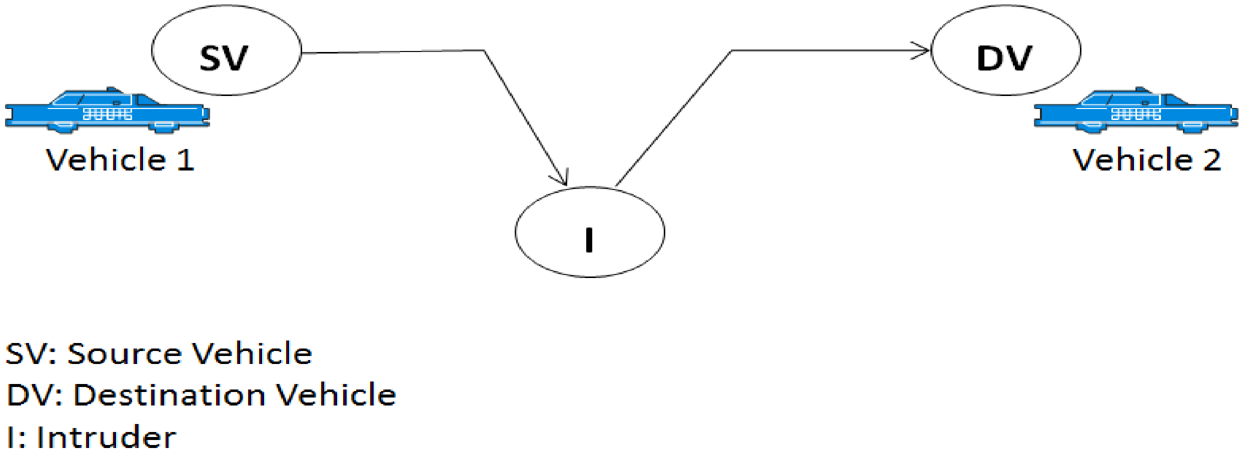

Figure-4.3. Modification Attack between Source Vehicle and Destination Vehicle

4.4. Fabrication Attack

This is attack on authenticity. A situation where the Intruder (I) probably studying and analyzing the Source Vehicle (SV) for some time and then fabricate the message to make the Destination Vehicle (DV) thinks the message is coming from the Source Vehicle (SV). In this type of attack, the Destination Vehicle (DV) finds it difficult to know if the message is coming from the Source Vehicle (SV), thus misleading the Destination Vehicle (DV). Figure 4.4 shows fabrication attack between Source Vehicle (SV) and Destination Vehicle (DV).

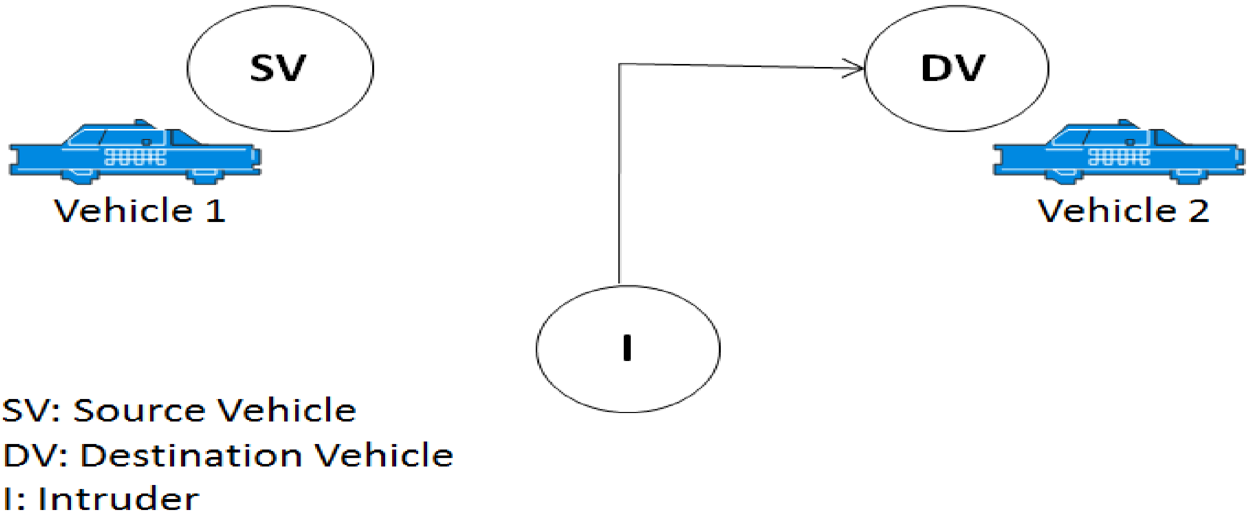

Figure-4.4. Fabrication Attack between Source Vehicle and Destination Vehicle

Based on this categorization, it is observed that any forms of attack on VANET be it attacks such as illegal listening and obtaining of information on the network, modifications of message content and traffic analysis to identify vulnerable points on the network, masquerading, replay attack and Denial of Service (DoS) fall under any of this category regardless of their mode of operations.

5. CONCLUSION

Security is a component factor that needs to be fully and efficiently realized if VANET will get its users confidence. This review has shown that due to the pervasive nature of the mobile nodes in VANET, it cannot be assumed that the networks will always be under the control of their owners as nodes could be stolen or tampered with; various forms of attacks were reviewed and succinctly categorized based on our research perspective, that any form of security and privacy attacks on VANET can be viewed from four basic forms of attack: interruption interception, modification and fabrication attacks regardless of the mode of operations used by the attackers.

Funding: This study received no specific financial support.
Competing Interests: The authors declare that they have no competing interests.
Contributors/Acknowledgement: All authors contributed equally to the conception and design of the study.

REFERENCES

[1] G. Samara, W. A. H. Al-Salihy, and R. Sures, "Security analysis of vehicular ad hoc networks (VANET)," presented at the Second International Conference on Network Applications, Protocols and Services, 2010.

[2] M. Khatri and S. Malhotra, "An insight overview of issues and challenges in vehicular adhoc network," *Journal of Global Research In Computer Science*, vol. 2, pp. 8-13, 2011.

[3] M. Raya and J. P. Hubaux, "The security of VANETs," in *Proceedings of the 2nd ACM International workshop on Vehicular ad Hoc Networks.*, 2005.

[4] M. Raya and J. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, pp. 39-68, 2007. View at Google Scholar

[5] R. Dass, R. Sangwan, and I. Girdhar, "Vehicular ad hoc networks," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 1, pp. 1-4, 2012.

[6] T. Foss, "Safe and secure intelligent transport systems (ITS)," presented at the SINTEF Transport Research Arena, 2014.

[7] I. Chlamtac, M. Conti, and J. J. Liu, "Mobile ad hoc networking: Imperatives and challenges," presented at the Ad Hoc Networks Conference, 2003.

[8] K. Tokuda, "DSRC type communication system for realizing telematics services," *Oki Technical Review*, vol. 71, pp. 64-67, 2004. View at Google Scholar

[9] J. Hoebeke, I. Moerman, B. Dhoedt, and P. Demeester, "An overview of mobile ad hoc networks: Applications and challenges," *Journal of Communications Network*, vol. 3, pp. 60-66, 2004. View at Google Scholar

[10] V. H. La and A. Cavalli, "Security attacks and solutions in vehicular ad hoc networks: A survey," *International Journal on Ad-hoc Networking Systems*, vol. 4, pp. 1-20, 2014. View at Google Scholar | View at Publisher

[11] P. Papadimitratos and J. Hubaux, "Secure vehicular communications: Results and challenges ahead," presented at the Workshop on Mobile Computing and Communications Review (MC2R), 2008.

[12] A. Khan, "Minimization of denial of services attacks in vehicular adhoc networking by applying different constraints," *International Journal of Academic Research in Business and Social Sciences*, vol. 3, pp. 662-684, 2013. View at Google Scholar | View at Publisher

[13] Girish and H. D. Phaneendra, "Identity-based cryptography and comparison with traditional public key encryption: A survey," *International Journal of Computer Science and Information Technologies*, vol. 5, pp. 5521-5525, 2014. View at Google Scholar | View at Publisher

[14] Raya, Papadimitratos, Gligor, and Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," presented at the 28th IEEE Conference on Computer Communications (INFOCOM), 2008.

[15] S. U. Rehman, M. A. Khan, T. A. Zia, and L. Zheng, "Vehicular ad-hoc networks (VANETs) - an overview and challenges," *Journal of Wireless Networking and Communications*, vol. 3, pp. 29-38, 2013. View at Google Scholar

[16] X. Lin, R. Lu, C. Zhang, H. Zhu, P. Ho, and X. Shen, "Security in vehicular ad hoc networks," *IEEE communication Magazine*, vol. 46, pp. 88-95, 2008. View at Google Scholar

[17] S. Zhao, "Issues and solutions of applying identity-based cryptography to mobile ad-hoc networks," Electronic Theses and Dissertations, 2012.

[18] Bhuvaneshwari, Divya, Kirithika, and Nithya, "A survey on vehicular ad-hoc network," *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, vol. 2, pp. 3-4, 2013.

[19] D. Jiang, V. Taliwal, A. Meier, W. Holfelder, and R. Herrtwich, "Design of 5.9 GHz DSRC-based vehicular safety communication. *IEEE Wireless Communications*, vol. 13, pp. 36-43, 2006. View at Google Scholar | View at Publisher

[20] IEEE, *IEEE wireless LAN medium access control (MAC) and physical layer (PHY) specifications amendment 8: Medium access control (MAC) quality of service enhancements, IEEE computer society*. New York: IEEE Std 802.11e, 2005.

[21] IEEE, *IEEE trial-use standard for wireless access in vehicular environments - security services for applications and management messages*: IEEE Std 1609.2-2006, 2006.

[22] IEEE, *IEEE trial-use standard for wireless access in vehicular environments (WAVE) networking services IEEE*. New York: IEEE Std 1609.3, 2007.

[23] FEC, "Federal communications commission," FCC Report and Order2004.

[24] K. Bilstrup, "A survey regarding wireless communication standards intended for a high-speed vehicle environment," Technical Report of School of Information Science Computer and Electrical Engineering, Halmstad University, Sweden, 2007.

[25] M. T. A. Ghassan, A. A. Mosa, and M. S. Sidi, "Vehicular ad-hoc network," *University of Plymouth – School of Computing, Communications & Electronics Publications*, vol. 1, pp. 8-10, 2014.

[26] S. Biswas, "Establishing security and privacy in WAVE-enabled vehicular Ad hoc networks," Ph.D. Thesis Submitted to The Department of Computer Science, Faculty of Graduate Studies of The University of Manitoba, Winnipeg, Manitoba, Canada, 2012.

[27] Y. L. Morgan, "Novel issues in DSRC vehicular communication radios," *IEEE Canadian Review*, vol. 63, pp. 7–10, 2010.

[28] M. Raya, P. Papadimitratos, and J. Hubaux, "Securing vehicular communication," *IEEE wireless communication*, vol. 13, pp. 8-15, 2006. *View at Google Scholar*

[29] A. Boukerche, H. Oliveira, E. Nakamura, and A. Loureiro, "Vehicular ad-hoc networks: A new challenge for localization-based systems," *Computer Communications*, vol. 31, pp. 2838-2849, 2008. *View at Google Scholar* | *View at Publisher*

[30] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J. P. Hubaux, "Secure vehicular communication systems: Design and architecture," *IEEE Communications Magazine*, vol. 46, pp. 100-109, 2008. *View at Google Scholar*

[31] B. Parno and A. Perrig, "Challenges in securing vehicular networks," in *Proceedings of the Fourth Workshop on Hot Topics in Networks (HotNets-IV)*, 2005, pp. 1-8.

[32] E. Maiwald, *Fundamentals of network security*, 1st ed. USA: McGraw Hill, 2003.

[33] A. K. Aboobaker, "Performance analysis of authentication protocols in vehicular ad hoc networks (VANET)," Technical Report RHUL MA2010.

[34] J. M. de Fuentes, L. Gonzalez-Manzano, A. I. Gonzalez-Tablas, and J. Blasco, "Security models in vehicular ad-hoc networks: A survey," *IETE Technical Review*, vol. 31, pp. 47-64, 2013. *View at Google Scholar*

Views and opinions expressed in this article are the views and opinions of the author(s), Journal of Information shall not be responsible or answerable for any loss, damage or liability etc. caused in relation to/arising out of the use of the content.