Review of VANET (Vehicular Ad Hoc Network) and Countermeasure against DOS Attack

Muhammad Ananda Fauzan[1], Selo Sulistyo[1] and I Wayan Mustika[1]
[1]*Department of Electrical Engineering and Information Technology, Universitas Gadjah Mada, Yogyakarta, Indonesia*

Keywords: VANET, MANET, Security, Node, Communication, Autonomous Vehicles, ITS.

Abstract: VANET technology is a sub-domain of MANET that being used in vehicles. This technology able to improve the security for drivers because it provides communication features between vehicles. Vehicles will act as a nodes and supporting infrastructure. VANET is susceptible to various types of attacks such as Denial of Service (DoS) because it is still on the development phase, increasing security for this technology will guarantee the implementation on actual conditions. Various attacks that occurs will be classified and determined which ones gives the heaviest impact and disrupt the performance of VANET. The use of VANET technology will help to create traffic that are able to improve the security and comforting users on the road. Thus, applied the Intelligent Transport System (ITS) can ensuring a friendly environment for safety traffic.

1 INTRODUCTION

Vehicular Ad hoc Network (VANET) is a development of Mobile Ad Hoc Network (MANET), VANET is a combination of vehicles equipped with wireless devices. Communication occurs on the highway between vehicles with other vehicles, vehicles with infrastructure, namely the Road Side Unit (RSU). Communication between vehicles and RSU is referred to as the Intelligent Transport System (ITS). The aim of VANET is to help people avoid vehicle accidents, according to the US Department of Transportation (USDOT). ITS is intended to describe how vehicles can be connected to overcome some problems such as safety and the environment.

VANET has several possible attacks, Sybil attacks, timing attacks, replay attacks, routing attacks, DOS attacks are a few examples. This can be seen from the motives of the perpetrators, as well as the use of security holes in accordance with the security requirements that are targeted.

2 DATA COLLECTION

Literature process begins with finding reference paper from several sources like IEEE and Scopus jounal database. Filtering selection of the paper that will be reviewed in this study based on the date the paper was published (range of years: from 2010-2018) and the quality of journal based on the number of citations. The data used in this review related to the technology, and research journals on computer science and engineering, IEEE Review in Engineering.

Keywords that are being used to find an appropriate paper such as "Autonomous Vehicles", "VANET", and "DOS Attack". The main focus in the analysis of a paper is in the parts of the method and discussion. The obtained information from the sources paper then recorded and will present on discussion and finding part. We will discuss the objectives and methods that being used on each paper. In total, there are 11 reference paper related with attack on VANET that obtained by filtering process.

3 RESULTS

3.1 VANET Architecture

The architecture of VANET consists of: On Board Unit (OBU), Application Unit (AU) which is part of the OBU, RSU and network access.

a. On Board Unit (OBU): in the form of a Global Positioning System (GPS) module, wireless communication module, Central Control Module (CCM), and user interface. CCM acts as a serial port processor, memory, and transceiver data. Supporting Dedicated Short range Communication (DSRC)

Fauzan, M., Sulistyo, S. and Mustika, I.
Review of VANET (Vehicular Ad Hoc Network) and Countermeasure against DoS Attack.
DOI: 10.5220/0009865901270132
In *Proceedings of the International Conference on Creative Economics, Tourism and Information Management (ICCETIM 2019) - Creativity and Innovation Developments for Global Competitiveness and Sustainability*, pages 127-132
ISBN: 978-989-758-451-0

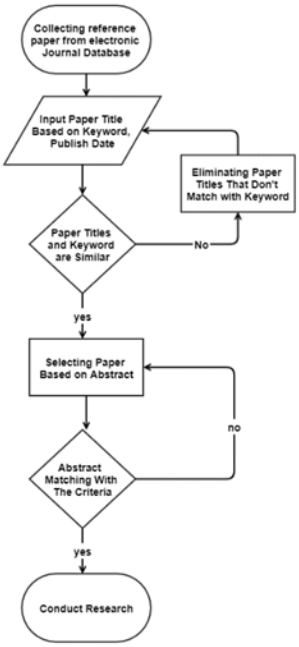

Figure 1: Literature process.

is also a function of OBU. DSRC regulates the sender of security and status between vehicles within a certain range (Kumar et al., 2017).

b. Application Unit (AU): additional components in the OBU to facilitate communication using the program, in the form of a physical component connected to the OBU. AU only deals with networks through OBU and performs tasks related to safety applications related to vehicle mobility and network functions (Krishna, 2017).

c. Road Side Unit (RSU): network support devices, usually physical and permanent, are placed at the end of the road or around the intersection, supporting devices that are equated with traffic lights, serve to increase signal coverage and inter-OBU data distribution and communication between RSU to reach OBU in the other region (Kumar et al., 2017).

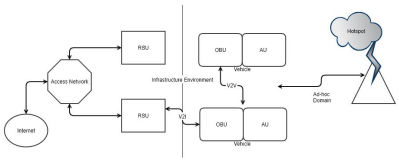

Figure 2: VANET architecture

3.2 Security Requirements and Potential Attack

Authentication, ensuring that messages sent by vehicles are authentic and genuine, those messages coming from clients that have been recognized and registered on the network are used to prevent the spread of messages that are not authentic and aim to disrupt the network and affect user safety. Integrity, the message sent is not changed by the sender to the recipient. Non- repudiation, the transmission of messages that have been sent cannot be denied by the sender. Availability, the system must always be available and accessible under any circumstances. Confidentiality, guarantees that message transmission can only be accessed by users who have been authenticated and closely related to user privacy, if it comes from another user who is not authenticated then the message can be ignored (Sumra et al., 2011)(Luckshetty et al., 2016).

Some examples of threat attacks that can occur in accordance with security requirements:

Table 1: Security Requirements and Potential Attack

Security Requirements	Potential Attack
Availability	DoS, DDoS, black hole, spamming malware
Confidentiality	Timing attack, home attack, man-in-the-middle attack, traffic Analysis, brute force attack, bogus information, ID closure
Authentication and Integrity	Node impersonation, replay attack, tunneling, GPS spoofing, message suppression, sybil attack

3.3 Type of Attacker

Determining the attacker's motives for carrying out attacks on VANET is difficult because it is unpredictable. In order to prevent and help anticipate this, the motives and reasons for the attackers are grouped into several types.

Some of these types are insider, active, extended, and malicious, independent, dependent, outsider, passive, local, and rational, intentional, and unintentional. This is done to better understand the habits

of attackers so that attacks can be more easily anticipated. These types are also used as markers and priority giving (Sumra et al., 2013).

a. Insider & Outsider: Insider is a network user who has been authenticated and has access to the network. Outsiders are individuals or groups of attackers whose capacity to attack is limited.

b. Malicious & rational: malicious is an attacker type that only has the motive to damage and disrupt the functions of network services. Nationally, attackers who have a goal to gain profits, in practice, are more predictable.

c. Active & Passive: active attacks with the aim of changing content, signals, and packages. Passive attacks that aim to analyze information on the network.

d. Independent: the attacker has an independent nature of the network, so it does not depend on other things in the attack process.

e. Intentional: is the personal purpose of an attacker who intentionally interferes with the work of the network in order to create problems for the user when accessing the network.

f. Dependent: is a group of attackers that are interdependent with one another intentionally carrying out specific attacks. Coordinate in groups when carrying out attacks.

g. Unintentional: accidentally involved in network damage that occurs and causes various network problems to users. Usually occurs in the process of operation and transmission on the network.

(Malla and Sahu, 2013) the types of attacks that can be carried out are grouped into five attack classes. This types of attack determine which one gives most impact based on their classes.

3.3.1 1st Class Network Attack

Directly affects communication whether the media is used such as infrastructure or other vehicles, some examples of attacks are as follows :

a. Denial of Service (DOS Attack)
Attacks carried out on communication media cause interference to the node in accessing the network. Blocking nodes (vehicles) that have authentication to access network services, as well as infrastructure in the form of RSU (as access points). There are three level of DoS Attack the attacker use to disrupt communication (Pathre, 2013)(Rampaul et al., 2016):

(1) Overwhelm the node resources
This level attacker focuses on nodes to disrupt communication, to overwhelm the resources so nodes become busy, by sending unique messages continuously so they are not able to do their job in verifying messages to be sent or received. Make the victim unable to access the network.
In other cases the attacker attacks the RSU, causing a busy condition when verifying the message from the attacker so that other nodes will not be able to get reply from the RSU, resulting in the service becoming unavailable.

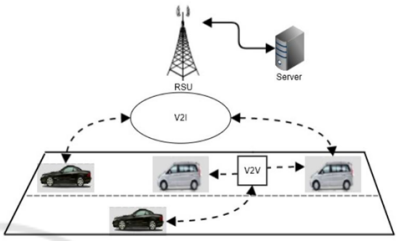

Figure 3: Overwhelm the resources node and infrastructure.

(2) Jamming the channel
At this level the attack is carried out by directly jamming the channel, make the users unable to access the network. The attacker sends frequencies to a particular domain, so that the domain and its surroundings cannot access the network, users can re-use the service when leaving the domain.
In other cases the attacker attacks using certain frequencies to jam the infrastructure. At this stage sending and receiving messages from and or to other nodes is not possible because it make the network inacessible.

(3) Distributed Denial of Service (DDoS)
Execute DoS attacks from various locations. The attack will take place at different times, the attacker's habits will be different for each object of attack (vehicle). The purpose of an attack is the same as DoS, but it is done at different locations and times on the same target. The attack can also be done on V2I Communication.

b. Node Impersonation
On VANET each vehicle has its own unique identity that is used to verify the message sent, in a critical case such as an accident the message sent will be crucial make this unique identity is needed so that the wrong message is not sent

to other users. This attack aims to change the message from the original node by modifying the attacker's identity and when received by other users it remains detected as a message from the original sender.

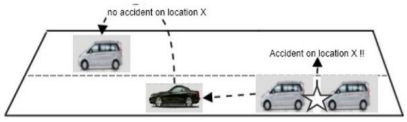

Figure 4: Node impersonation

c. Sybil Attack
This type of attack manipulates the attacker's vehicle, creating the identity of the attacker's vehicle to have the same identity as the others, each vehicle seeing the attacker at a different location at the same time. In Figure 5 Vehicle A duplicates its identity so that it is detected to fill the road. The main goal of an attacker is the ability to control the direction of the other vehicle's (Pathre, 2013).

Figure 5: Sybil attack

3.3.2 2nd class Application Attack

The attacker's main motive for this attack is to change the content on the application (safety and non-safety) that is used for its own purposes. Types of safety applications such as warning information on the road, the attacker will change the warning content into false info that can result in an accident.

Figure 6: Safety application attack

In non-safety applications the information provided is in the form of conditions outside the traffic so that if changed it will not cause dangerous conditions.

3.3.3 3rd Class Timing Attack

Gives delay to the message / information sent, so the message will be late until it enters the expiration time.

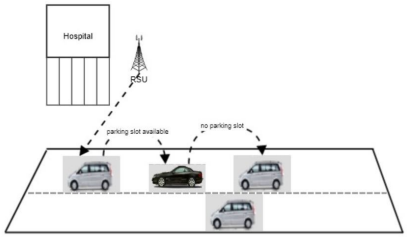

Figure 7: Non-safety application attack

The first information (1) is conveyed to the closest vehicle that is to the attacker's vehicle, then because the information was not delivered on time there was a second accident (2) involving the vehicle behind it. In the safety application, time is the most crucial thing because the message must be received directly at that time if not the main function of the application will be lost.

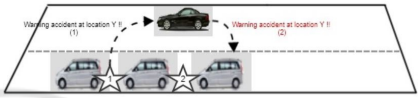

Figure 8: Timing attack

3.3.4 4th Class Social Attack

An attack intended to influence the emotions of the user. Through the messages aiming to generate angry behavior from the user when the message is received by the user.

3.3.5 5th Class Monitoring Attack

The attacker will monitor the communication that occurs on V2I and V2V, when the information needed has been obtained it will be channeled to the other attackers who need it.

3.4 Solution to Prevent Attack

In its application there are several models to prevent certain types of attacks that can occur on the VANET.

(Hasbullah et al., 2010). This first model relies on the OBU's ability in each vehicle to make a decision to block DoS attacks, in its application the processing unit is able to recommend OBU to select anticipation, according to the type of attack OBU has 4 options that can be done; Channel switching, Technology switching, Frequency hopping spread spectrum (FHSS), Multiple Radio Transceiver. New information can be received and forwarded to users by OBU after going through the process and selecting the most appropriate technology.

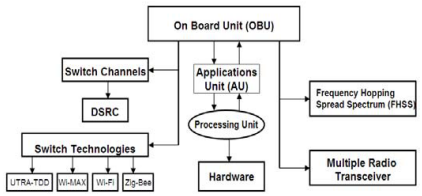

Figure 9: Model of OBU features

(VIPIN and Chhillar, 2018). The Group Controlled Analysis Model is analyzing the types of nodes that are dangerous and harmless based on several parameters compared namely the direction, position, and speed of the vehicle. As shown on Table 2 is the result of the model.

Table 2: Result of the method

Measure Performance	Existing Technique	Proposed Model
Throughput	517.48	743.47
PDR	83.16	87.27
Communication Loss	4.87	0.83

The results of the analysis of these parameters detect communication carried out by nodes that do no harm to produce communication that does not affect delay, response time, and communication loss. It is an observation of communication problems at an early stage. Being able to ensure communication occurs more effectively to the small scope of the vehicle, in blocking the occurrence of DDoS attacks.

(Kolandaisamy et al., 2018). Multivariant Stream Analysis, MVSA consists of several stages in detecting DDoS attacks on the network. There are 3 algorithms used in detecting the attack of the first algorithm for classification, the second algorithm is a set of rules generated from calculations, algorithm 3 will give the final result.

a. Preprocessing Stage
Begin the classification phase of safety and non-safety applications in traffic by collecting logs on packages containing information.

b. Multivariant Stream Weight Stage
The algorithm is used at this stage to calculate weights to detect DDoS attacks.

$$MASV = \frac{Ap}{Apf'} x \frac{Ahc}{Attl} \quad (1)$$

The payload value (Ap), is the value of bandwidth that is affected by the frequency of the package (Apf). hop count (Ahc) depends on TTL (Attl). As shown in equations (1).

$$Masw = \Sigma \frac{MASV}{24} \quad (2)$$

Time divided by number of time windows (24) as per hour count into one time window assume this calculation to detect in one day make it 24 time windows. As shown in equations (2).

c. DDoS Mitigation Stage
It is the final stage of the MVSA method, doing a trace on the first node then preprocessing it in the log, the preprocessing stage generates a rule / standard and produces a value / weight that will be used to detect the problematic packet. Using algorithm 3, the detection results from the package will be known.

$$MASM = \frac{Dist(Ri.Pl, P.Pl)}{\Sigma packet recieved in Tix \frac{Dist(Ri.hc, P.hc)}{P.ttl}} \quad (3)$$

The value calculated for the package received must be of a certain size (σ) at a certain time window (Ti). The algorithm must calculate the distance (Dist) between the rules and features (Ri) extracted for the packet received. The value calculated for the package received must be of a certain size (σ) at a certain time window (Ti). The algorithm must calculate the distance (Dist) between the rules and features (Ri) extracted for the packet received. As shown in equation (3).

$$IF MASM < MASW \&\& MASM <> Ri.Features \quad (4)$$

Comparison between MASM and (MASW and MASM) is the end result in computational algorithms to detect DDoS attacks.

After observing the communication in traffic against various different situations such as network trace, payload, the amount of data generated by the packet, then hop count (a number of messages from the node that must be sent to reach the destination), time to live (duration of data transmission on the network). Four (4) features are calculated to produce a rule and weight which can classify an authentic or dangerous a package is.

The result show that MVSA outperform the other 3 methods (H-IDS, Multi Filter, Trilateral trust) in term of throughput, detection accuracy, detection time, delivery ratio, packet delay, packet drop ratio. Figure 11 shows result on delivery ratio.

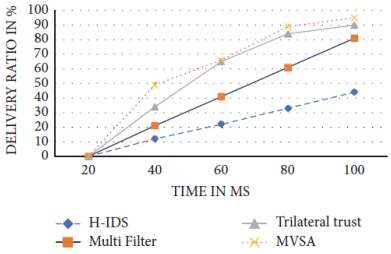

Figure 10: Delivery ratio

4 CONCLUSIONS

From the research that has been done, it can be concluded that based on the security requirements and types of attacks that can occur in vanet, network availability is the first and most important thing because it is related to network services, if not available, users will lose the benefits of safety and non-safety applications.

In order to be used properly, network services must be available at all times, but attacks on DoS that are carried out can result in availability being disrupted. This attack is categorized as the first class because it diverts services from the start and prevents sending information between nodes and infrastructure.

In this paper, we describe the vanet architecture, attack type, type of attack, several methods and models to cancel and reduce the risk of attacks, not only DoS also includes DDoS. The most important thing is to maintain availability on the network, messages generated by VANET services must be guaranteed and provide benefits to users.

REFERENCES

Hasbullah, H., Soomro, I. A., et al. (2010). Denial of service (dos) attack and its possible solutions in vanet. *International Journal of Electronics and Communication Engineering*, 4(5):813–817.

Kolandaisamy, R., Md Noor, R., Ahmedy, I., Ahmad, I., Reza Z'aba, M., Imran, M., and Alnuem, M. (2018). A multivariant stream analysis approach to detect and mitigate ddos attacks in vehicular ad hoc networks. *Wireless Communications and Mobile Computing*, 2018.

Krishna, B. H. (2017). Study of ad hoc network with reference to manet vanet fanet. *International Journal of Advanced Research in Computer Science and Software Engineering*, 7(7):390–394.

Kumar, A., Bansal, M., et al. (2017). A review on vanet security attacks and their countermeasure. In *2017 4th International Conference on Signal Processing, Computing and Control (ISPCC)*, pages 580–585. IEEE.

Luckshetty, A., Dontal, S., Tangade, S., and Manvi, S. S. (2016). A survey: comparative study of applications, attacks, security and privacy in vanets. In *2016 International Conference on Communication and Signal Processing (ICCSP)*, pages 1594–1598. IEEE.

Malla, A. M. and Sahu, R. K. (2013). Security attacks with an effective solution for dos attacks in vanet. *International Journal of Computer Applications*, 66(22).

Pathre, A. (2013). Identification of malicious vehicle in vanet environment from ddos attack. *Journal of Global Research in Computer Science*, 4(6):30–34.

Rampaul, D., Patial, R. K., and Kumar, D. (2016). Detection of dos attack in vanets. *Indian Journal of Science and Technology*, 9(47).

Sumra, I. A., Ahmad, I., Hasbullah, H., et al. (2011). Behavior of attacker and some new possible attacks in vehicular ad hoc network (vanet). In *2011 3rd International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, pages 1–8. IEEE.

Sumra, I. A., Hasbullah, H. B., Ahmad, I., Alghazzawi, D. M., et al. (2013). Classification of attacks in vehicular ad hoc network (vanet). *International Information Institute (Tokyo). Information*, 16(5):2995.

VIPIN, D. and Chhillar, R. S. (2018). The ddos attack detection and prevention in vanet by group controlled analysis model.