Penerbit Akademia Baru

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 1, No. 1. Pages 16-32, 2015

Analyze the VANET Performance in Presence of Timing Attack and Sinkhole Attack using OMNeT++

F. N. Bhatti[*,1,a], *R. B. Ahmad*[1,b], *M. A. Shahbani Bakar*[2,c], *S. Daud*[1,d], *S. J. Elias*[1,e] *and M. N. M. Warip*[1,f]

[1]School of Computer and Communication Engineering, University of Malaysia Perlis, Malaysia
[2]Universiti Utara Malaysia, 06010 Sintok, Kedah, Malaysia
[a,*]*fahadnazirbhatti@gmail.com*, [b]*badli@unimap.edu.my*, [c]*shahbani@uum.edu.my*,
[d]*shuhaizar@unimap.edu.my*, [e]*sjamel@gmail.com*, [f]*nazriwarip@unimap.edu.my*

Abstract – *The growth in research advancement of vehicular Adhoc Network (VANET) has seen a significant rise in the security attack. In this paper, we give the simulation for quantitative investigate of VANET in the presence of Timing attack and Sinkhole attack. We described the performance metrics and discover the effect and harm caused by Timing attack and Sinkhole attack, which directly affect the network Quality of Service (QoS). Our assessment results show that the impact on VANET under Timing attack and Sinkhole attack varies potentially depending on a number of vehicles, the number of attacker vehicles. The impact of a Timing attack and Sinkhole attack increased significantly by increasing the number of attacker vehicles in several of the situations. While the number of attacks impact level continually effect on network performance with varying the number of vehicles. The contribution in this paper has used the OMNeT++ simulators to quantify analysis of the VANET performance in the presence of attacks by comparison with a non-malicious network and a network which enclosed malicious behavior. It has been investigated in two types of attacks, namely 1. Sinkhole attack 2. Timing attack.*

Keywords: VANET, Security, Timing attack, Sinkhole attack, OMNeT++.

1.0 INTRODUCTION

VANET offers a frivolous infra-structure less to administrate the variations sensory in aggressive situations. Inappropriately, the open nature of such situations, VANET is predominantly prone to letdowns as well as, it is essential to handle with several procedures of interferences, alternating from power outages to malicious. Moreover, these malicious can simply spread the wrong info and silently meaningfully influence network administration. Hence, it is necessary to quantify the threats caused by Timing attack and Sinkhole attack on VANET.

For instance, the huge set of vehicles in VANET are established on the assembly of a tree-based routing topology originated by a sink [1-4]. Individually, these protocols procedure promoted info such as hop count from a sink to shape a routing topology. Systematic and quantitative protected process of protocols is necessary for strength and life of the network. Reflect the attack, recognized as the Sinkhole attack [5], where attacker vehicle imaginary to be nearer to the sinks than all its surroundings, appealing additional traffic, these Vehicles can whichever choicely drop the received packet. For instance selective-forwarding attack or receive complex info.

The main drawback for security challenges is considered that the routing protocols not designed itself for security measurement [6]. VANET facing a lack of security issues because of it is an open nature network, so any vehicle can join and leave [7-8] the network without any restriction or any condition, therefore it is concluded that overhead can simply attack the communication of VANET. The most common attacks namely Timing attack [9] Sinkhole attack, Denial of Service (DoS), Sybil attack, etc. In [10] the authors gave the comparisons of several routing protocols like DSDV, AODV, and DSR in the presence of attacks, as well the detail of detection the few attacks is present in [11-13].

In this paper, we used Dynamic Mobile Ad-hoc Network On-demand (DYMO), which is on-demand routing protocol. We quantify the impact of Timing attack and Sinkhole attack on VANET by using various network attributes. To meet above-mentioned security issues we executed the simulation to capably quantify the analysis of Timing attack and Sinkhole attack in VANET.

To evaluate performance evaluation of VANET in presence of attacks, we used the number of vehicles and number of attackers vehicles to analyze the different behavior by compare the network performance in presence of Timing attack and Sinkhole attack, our simulation shows the outcome of number of vehicles in presence of attacks, such as increase and decrease in the number of attackers vehicles effect on the network performance.

The simulation of the non-malicious and malicious network used the OMNeT++ simulator and investigated on DYMO routing protocol, for further investigation it can be examined on other routing protocols to see the impact on VANET performance, for future research, the simulation of this work can be used to investigate other attacks on VANET, the attacks on confidentiality, integrity, availability and non-repudiation, such as, Sybil attack, dropping attack, Blackhole attack, flooding attack, DoS, and worms.

The work in this article is systematized as follows. We discuss protocol and attack in section 2, in section 3, quantify the impact on VANET with simulation experiment as well present all results by comparison of normal network and network under sinkhole attack, finally, conclude the result of this paper is summarized in the last section.

1.1 Practical Requirements of Vanet

The governmental and the vehicular industries are considering to achieve the improvement in the road safety, which has been included few of most useful applications, such as US-DoT applications, while commercial applications contribute a huge number of applications, which

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 1, No. 1. Pages 16-32, 2015

triggered serious issues in VANET, such as, less availability of storage, transaction control, network administration, and so on. Some detail of requirements has been presented in [14-16]. The practical requirements compacts with the practical complications must be addressed to the deployment of VANET to regulate the VANET. The practical requirements of VANET describe as following.

1.1.1 Network Administration

According to huge mobility, the routing protocols, the channel situation meet with alteration rapidly. The ad-hoc network is such an open nature network and the VANET is the one of the ad-hoc network, which is infrastructure less nature, so each vehicle can be leave and join at any time, which are connected through their access point which is called RSU, and the range of RSU which is limited and to give coverage to the RSU.
United States implemented the DSRC routing protocol while another ad-hoc routing protocols can be also employed. The research of VANET is in progress in this current era some of the authors presented the network administration requirements [14], and some of the problems facing the network administration due to infrastructure less nature, the more issues are security related, it has been many of routing protocols are proposed for the VANET. The author [17] compared the performance of different routing protocols and mentioned the limitations of infrastructure less network as well as challenges.

1.1.2 Social and Economic

There are many of social networks participate in the VANET, in the shape of information sharing, advertising and social grouping to alert and to circulate the information regarding the city and highway conditions. The information about the collisions and congestions [18] done by alert or warn to its neighbor or broadcast message to its neighbor, the message received from any vehicle and after receiving it might be received a message from a malicious so the verification of these types of information is a challenging task. And economical applications side, it brings many challenges to satisfy vehicular industries. In the area of manufacturing of vehicle industries, it is challenging to assemble a structure that carries the common application [19].For instance, the road's signal control, which abuse from an end user may discard such kind of administration. The end user must accept the violation warning of police traps, for instance, traffic police. So to inspire the manufacturer to regulate the VANET.

1.1.3 Congestion and Collision

According to limitless the network scope possibly introduce the great challenges, and the transportation capacity is short in the city regions as well at some particular times. For instance, in the morning and evening times the flow of traffic is higher than other times even highway regions. Because of these different transportations flows the network barriers often arises while in hurry periods of time. Hence, the transportation weight is very heavy resultant the network face the crowd and might be the collision arises.
The author [18] discussed congestion control as well as provided the comparison of congestion control algorithms. The congestion control is complicated due to increase in

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 1, No. 1. Pages 16-32, 2015

traffic and data exchange. Plenty of application exchange the data from one user to multiple users, resultant the congestion control became complicated.

1.1.4 Ecological Influence

Due to the usage of electromagnetic waves, to broadcast the messages and joins the VANET, it is studied in the literature that electromagnetic waves highly influenced by the atmosphere. Therefore, to regulate the VANET, the ecological influence should take a serious note, before regulating the VANET. It has been studied [15, 17] some of the challenges related to ecological influence.

1.1.5 MAC Design

The VANET normally has been employed the public medium which regulates the communication among the V21 and I2V. Therefore, the MAC scheme considered as a key issue by literature, as well as various methods has been assumed and designed such as TDMA, SDMA, CSMA and so on. The IEEE802.11 is assumed the CSMA created Mac for VANET [20].

1.1.6 Security

Beside safety applications, the main challenge arises in comfort applications. The comfort applications are designed for to provide all possible type of application to make the drive comfortable and enjoyable. For instance, entertainment, multimedia, gaming, vehicle maintenance, fuel refill etc. The VANET has been designed with consideration and assumption to save lives of people and provide some tools such as applications of VANET that helps to avoid the collisions by communicating to neighbor vehicles.

It is studied in literature the exchange such kind of information depend on behavior. The behavior that can be selfish behavior or normal behavior. The malicious can be considered as selfish behavior, which try to modify such kind of information. Therefore, the integrity of communication must be satisfied. The detailed survey of security issues is presented in [14, 15, 21, 22, 23].

1.1.7 Commercial

There is plenty set of applications has been employed for the VANET. The detail of some of these commercial applications is presented in [20, 24]. In general, when the credit card transaction involved with any application, it considered providing the high-level security, such as cryptographic techniques to make the secure transactions. As well as the maintenance of engine the parts, the VANET should consider commercial applications with data integrity, availability, since DoS is a serious attack to the availability, so the usage of these plenty applications, it is needed to consider with their requirements.

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 1, No. 1. Pages 16-32, 2015

1.2 DYMO Routing Protocol

DYMO [25] is known as reactive routing protocol that creates a path on demand basis desires to transmit the data to the required destination. It can be used as a replacement of AODV protocol with a path accretion feature, it uses hop-by-hop routing model of the order number and link setback. Each vehicle upholds its own order number. The order number is increased each of time the vehicle transmit a route request message. This permits other vehicles to decide the order of discovery message to evade stale routing info, to notify the duplicate message, as well to confirm loop freedom.

This protocol works as twofold, 1.Route discovery and 2.Route maintenance. The Route discovery is a process of generating a route to a required endpoint when a vehicle desires a route to it. When P wants to interconnect with a Vehicle Q, it switches a route request (RREQ) message. The order number is increased earlier it is added to the RREQ. The message is transmitted into the network. Every vehicle forward an RREQ join its particular address, order digit, and gateway info to the RREQ parallel to the initiator vehicle.
Upon transmitting the RREQ, the initiating vehicle awaits the greeting of an RREP message from the board. If no RREP is established within RREQ WAIT TIME, the vehicle may over try to discover a route by issuing another RREQ. And the Route maintenance is the process of replying to differences in topology that occurs after a route has initially been shaped.

1.3 OMNeT++ Simulator

OMNeT++ can be extended, linked, module-based C++ simulation public library largely for network structure which can either be MANET or VANET, optical fiber etc. In general, OMNeT++ can construct the wireless and wired communication network. The basic frameworks of OMNeT++ are presented in real life scenarios, for instance, OMNeT++ have been widely used by researchers. The Domain-specific processes, e.g. the maintenance of ad hoc networks, internet protocols, network modeling is available in its model category of frameworks. It can also be designed by other specific available modules.

OMNeT++ provides the freedom for users to create their own assumptions. OMNeT++ employed an Eclipse-based IDE, a graphical runtime background, as well as other tools. OMNeT++ can only be used for academic and research purpose and not for commercial use. There is an allowance for real-time simulation, network imitation, other programming languages, database addition, and several other processes. A pyramid of small characteristic situations in OMNeT++ and recyclable modules has been designed in C++. The OMNeT++ maintains communicative modeling of the modules by fixed state topologies and communication patterns. The modules are largely based on message forwarding. All the functions of the modules are in open source, which are designed by using C++ and admits for a prompt prototyping method of modular design.

OMNeT++ allows the designed simulation to run by command line or graphical background executed by the user and can tune the run time duration base on written command line. Some parameters have been written into the initialization file while some parameters which are the required parameters appear in the graphical background and it will request for missing parameters.

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 1, No. 1. Pages 16-32, 2015

1.4 Attack Module

The attack module consists of two attacks, first Sinkhole attack and second Timing attack, which add the behavior of attack accordingly Sinkhole attack nature and Timing attack nature. In this attack module also have normal behavior vehicles, which act like a normal behavior vehicles. Initially, start with message send and it check the behavior either normal behavior or abnormal behavior if the behavior is normal it will be labeled as normal behavior and for attacker behavior run up for further processes, such as change the behavior accordingly attack type. After changing the behavior it checks furthermore attack type. If attack type is Sinkhole attack it stop the routing discovery and if Timing attack it add some delay in the time slot. The flow chart of attack module for the simulation of Sinkhole attack and Timing attack is shown in Figure 1. The detailed discussion of each of these attacks in the simulation process is following;

1.4.1 Timing Attack

The timing attack triggers the delay in data packets for an assigned amount of time. The timing attack can disturb the various QoS parameters, for instance, delay, PDR, and throughput. The overall network performance is affected by the Timing attack. The parameters of Timing attack used in the simulation process is following;

- Delay Attack Probability (double): the probability of delaying a data packet was chosen between 0 and 1.Zero (0) is set for the normal behavior while one (1) is set for the timing attack vehicle.
- Delay Attack Value (double): This is the specific delay time applied to the packet. It should be noted that the parameters can be stated in a statistical distribution pattern. Thus, it is modified every time it is assessed. By default, it follows a normal distribution with mean by 1 second and the standard deviation by 0.1 seconds.

1.4.2 Sinkhole Attack

The sinkhole attack is defined as a sinkhole attacker vehicle which sends fake routing information, attracting or declaring that it knows the best route and causing other vehicles to route data packets over itself. The sinkhole attacker vehicle triggers as attacker fake routing reply RREP to attract traffic. The parameters of sinkhole attack used in the simulation are following;

- Sinkhole Attack Probability (double): the probability of responding an RREQ with a fake route RREP is assigned among 0 and 1. By default, 0 is set for the normal behavior of DYMO protocol and 1 is set for Sinkhole attack.
- Sink Only When Route in Table (bool): if set to true, the sinkhole attacker vehicle sends fake RREP to RREQ for those attacker vehicles which have a valid route, that is, routes present in its routing table. On the other hand, the else false value is vehicles that send fake RREP to any RREQ message incoming.

- Sequence number Added (double): This is the fake sequence number produced by the attacker vehicle which is added to the sequence number noticed in the RREQ. It can be altered every time when stated as a statistical distribution. By default, it follows a uniform distribution.

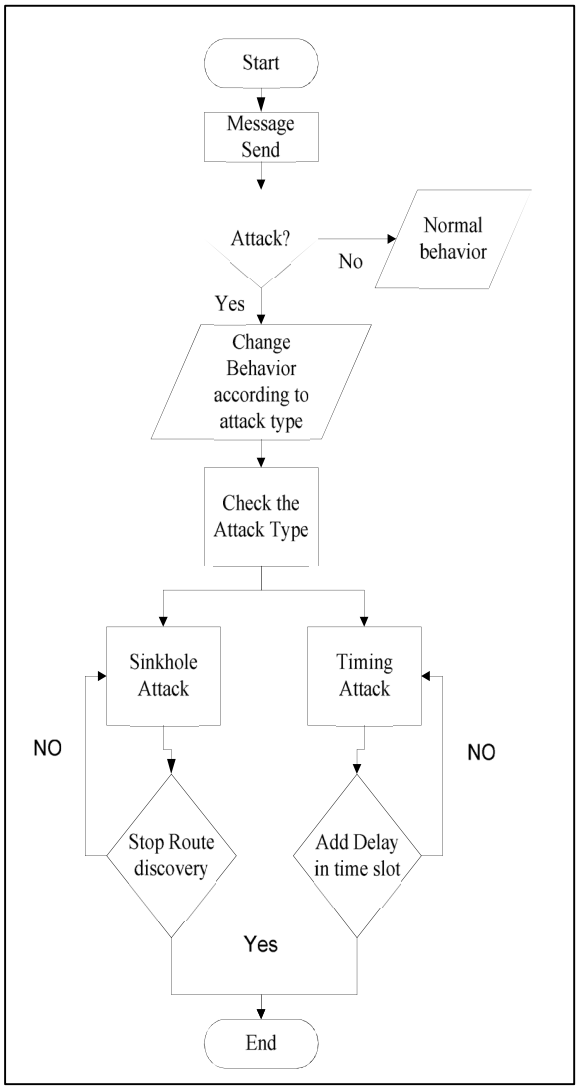

Figure 1: Flow chart describing simulation process of the Sinkhole attack and Timing attack

To overcome the issue above mentioned, it was considered to use the Discrete Event Simulator OMNeT++. It was carried out the simulation parameters based on Timing attack and Sinkhole attack, which are needed to perform the experiments to quantify the impact on VANET performance with Timing attack and Sinkhole attack by comparing with non-malicious network and malicious network. OMNeT++ is an authoritative network simulator which is widely used by the researchers of this area. Proposed outline has been executed for

determination of quantifying the network performance by performing the experiments. The overall performed experiments consist on the number of normal behavior vehicles, a number of malicious behavior vehicles, the number of RSU and send intervals time.

It was used the parameters to perform the each experiment based on Timing attack and Sinkhole attack. The codes for Timing attack and Sinkhole attack was used to simulate the network and each time simulation was run for each attack by changing some codes of attacks, such as based on attacks which is essential to get the satisfactory result for analysis the network performance by comparing non-malicious network and malicious network.

It was written the simulation codes in a .cc file which is present in OMNeT++, in the .cc file it can write the simulation codes. The initialization file which is called .ini file in OMNeT++, in .ini file it can write the initialization parameters based on .cc file codes. Overall the simulation was ran based on .cc file written codes and parameters given in the .ini file both files representing the network modeling, the network modeling can be done in the .ned file, in .ned it was described the network modeling which was based on network performance by comparing the non-malicious and malicious network. The modeling of the non-malicious and malicious network has been used DYMO routing protocol in this research.

Overall experiments have been used the DYMO-based network grounded on the experimental result. Table 1 has been used for modeling the network, such as, non-malicious network and malicious network, the malicious network based on Timing attack and Sinkhole attack which was used in this research.

Table 1: Simulation Parameters for VANET performance in presence of attacks

Parameter	Description
Simulator	OMNet++
Simulation Time	250s
Number of Vehicles	10, 20, 30, 40, 50
Number of Attacker	1, 2, 3, 4
Number of RSU	10
Simulation Area	2000m*2000m
Routing protocol	DYMO
MAC Layer	802.11
Packet Size	512
Inspected Methods	Normal and Attack
Mobility Speed	Uniform (2mps, 4mps)
Mobility Wait Time	3s, 8s
Send Interval	0.1s, 0.15s, 0.2s, 0.25s
Mobility Angle	+180deg, -180deg
Repeat Simulation	Average (5 Times)
Transport Agent	UDP

Penerbit Akademia Baru

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 1, No. 1. Pages 16-32, 2015

2.0 METHODOLOGY

2.1 Simulation Modeling

The simulation of VANET is consists of two parts, the first simulation of a non-malicious network and second is a simulation of a malicious network. Non-malicious network and malicious network contained the number of vehicles and the number of attackers. The malicious network is based on Sinkhole attack and Timing attack. Figure 2 shown the simulation of the network. DYMO routing protocol is used to simulate the network and two kinds of attacks Sinkhole attack, and Timing attack.

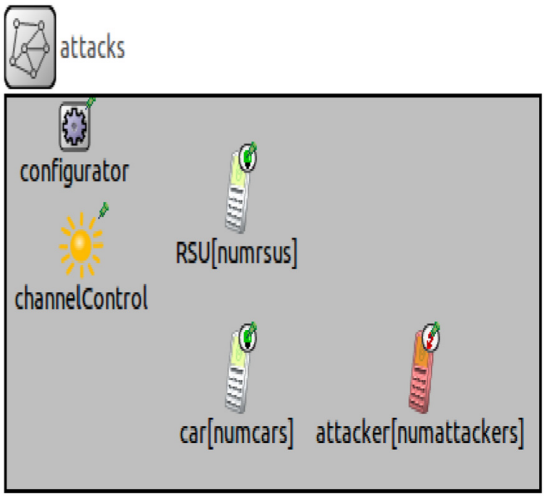

Figure 2: Simulation the Network Structure of VANET

2.2 Performance Evaluation

This research has been designed based on the non-malicious and malicious network which was assumed to compare for achieving the network performance in the presence of attacks, such as, Timing attack and Sinkhole attack. In general analysis is depends on the parameters, for instance, what kind of parameters are needed to examine the network performance which are based on analysis or based on the comparison.

To analyze the VANET performance, it concludes the delay to look forward impact in the presence of attacks. The delay is defined as; the average duration occupied for a data packet to reach the assigned destination. In general, the delay comprises delay which triggered by route discovery procedure and queue on data packet broadcast. To calculate the delay, it uses the Equation 1 is following;

$$\text{Delay} = \frac{\sum(\text{Arrival time} - \text{Send time})}{\sum \text{Number of Connections}} \quad (1)$$

Penerbit Akademia Baru

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 1, No. 1. Pages 16-32, 2015

3.0 RESULTS AND DISCUSSION

3.1 Network Delay in Presence of Timing Attack

To evaluate the delay in presence of Timing attack, it is needed to compute the delay by using the Equation 1. It has been compared with a non-malicious behavioral network, which contained no Timing attacker vehicle in the network and a network with a malicious behavior which contained the Timing attack in VANET. It has been observed by comparing the nonmalicious and a malicious network, the delay was triggered up in a malicious network due to the presence of Timing attack. On the other hand, the network performance of a non-malicious network which was observed is normal.

It is observed that the delay in the network is increasing the presence of Timing attack. The analysis which is based on comparisons of a non-malicious network and a network that contained Timing attack is shown in Figures 3a, 3b, 3c, and 3d. It shows in Figure 3a, it has attained the analysis by experiments with the send interval 0.10s which is increased. In general, the send interval 0.1s is used to considered as the high value of data transmission. Delay increased the more when the data transmission in the network is high than other send intervals, such as 0.25s, 0.20s, and 0.15s.

In the Figures 3, 4, 5 and 6, the number of Timing attacker vehicles representing as 1 attack, 2 attacks, 3 attacks and 4 attacks, 0 represent a non-malicious network. The numbers of vehicles considered were 50, such as 10 vehicles, 20 vehicles, 30 vehicles, 40 vehicles, and 50 vehicles.

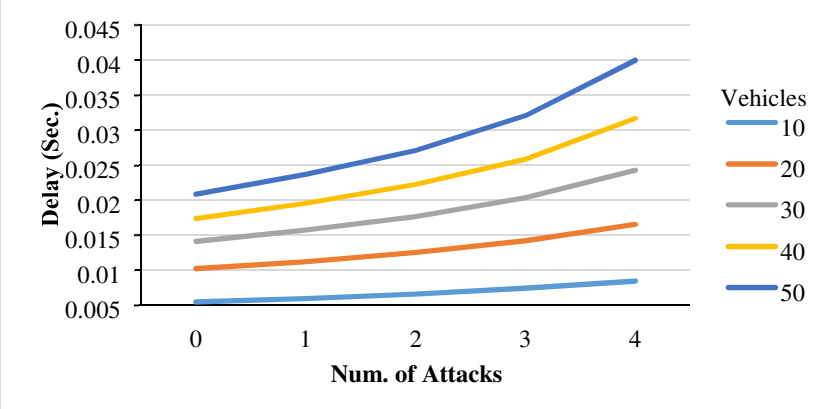

Figure 3: Analysis Delay of VANET in the presence of Timing attack with send interval 0.10s

It was observed through attained results that in the presence of Timing attack, it increased the delay in the network which is affecting the overall network performance. The vehicles are moving faster on the road such that delay might be the main reason of the accident physically, in the presence of Timing attack.

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 1, No. 1. Pages 16-32, 2015

In general delay should not be increase in VANET, but due to the malicious behavioral vehicle's participation in the network which is Timing attack, makes the overall performance of the network degrade, and it is due to when the numbers of vehicles are increasing in the network, and when the traffic flow is increasing such as send interval 0.1s.

The delay has been increased with send interval 0.10s in the network in the presence of Timing attack and the participation of 50 vehicles as well as delay has been increased with lower send intervals, such as 0.25. The analysis based on delay computed is presented by comparing with other send intervals as following.

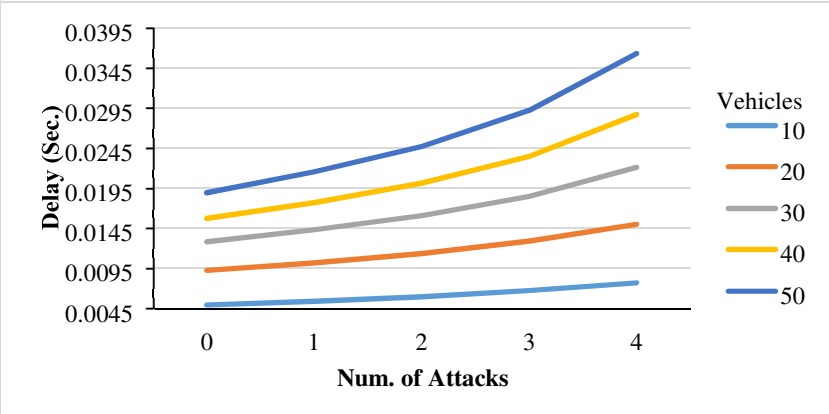

Figure 4: Analysis Delay of VANET in the presence of timing attack with send interval 0.15s

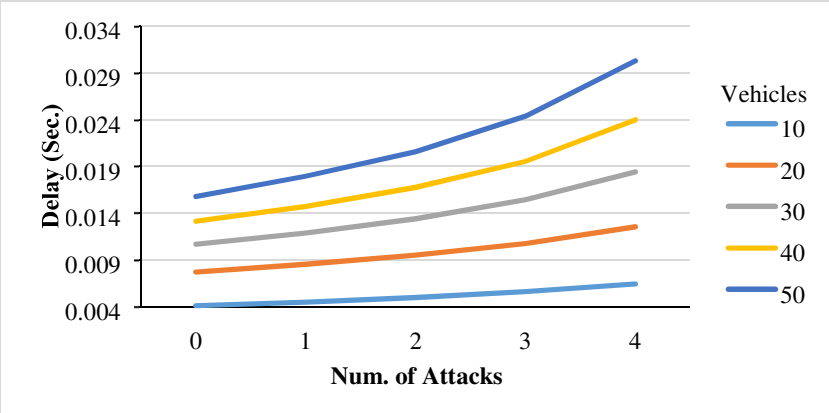

Figure 5: Analysis Delay of VANET in the presence of timing attack with send interval 0.20s

The analysis attained the average of overall delay of Timing attack is shown in Figure 7 which observed the delay by increasing approximately 80% with the participation of 50 vehicles in

a network in the presence of Timing attack. On the other hand, it examined the delay increasing rapidly when the 50 vehicles join the network in the presence of Timing attack other than 20 vehicles joins in the network in the presence of Timing attack.

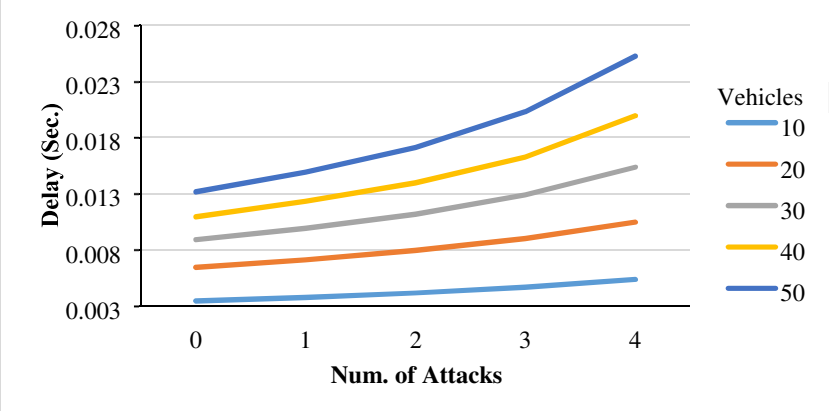

Figure 6: Analysis Delay of VANET in the presence of timing attack with send interval 0.25s

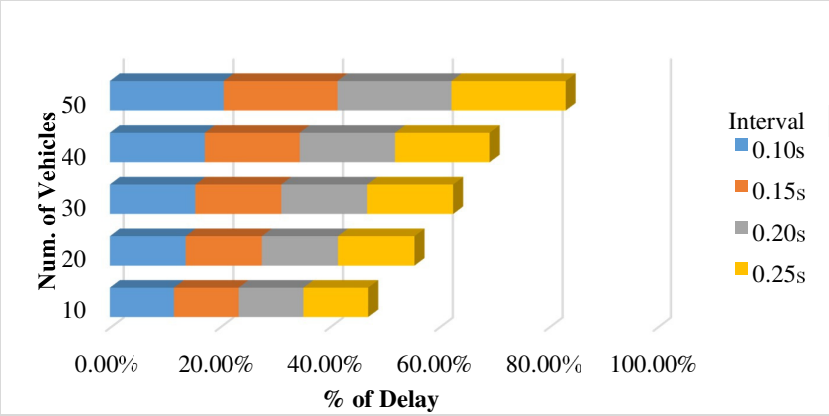

Figure 7: Analysis the Average Delay of VANET in the presence of Timing attack

Network Delay in Presence of Sinkhole Attack

The delay is compared with non-malicious network and a network in the presence of Sinkhole attack. A network was simulated in the presence of Sinkhole attacks and it computed the delay by using the Equation 1. It is observed based on the result; the number of the Sinkhole attacks is increasing the delay which is a serious threat to VANET performance. It is studied in the previous section that to get the data or warning message which contained the delay, either useless or worthless.

The delay is triggered down the life of the network and degrades the network performance.

Penerbit Akademia Baru
Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 1, No. 1. Pages 16-32, 2015

Quantitative examination of network performance which contained the delay is shown in Figure 4a, 4b, 4c, and 4e with send interval, which was considered as 0.1s, 0.15s, 0.20s and 0.25s and the number of vehicles, which was considered 50. In Figure 8, 9, 10, and 11 which represents the number of vehicles, 10 vehicles, 20 vehicles, 30 vehicles, 40 vehicles, and 50 vehicles respectively. Sinkhole attacker vehicles were considered 4 which are 1 attack, 2 attacks, 3 attacks, and 4 attacks, and 0 is representing the non-malicious behavior network, which shows the performance of the network with no attack. It is observed that when the number of Sinkhole attacker vehicles joins in the network, the delay is triggered to increase the overall performance and it is also observed that when the send interval is 0.1s in the network transaction, the delay is more increased than another send interval such as 0.25s, 0.20s, and 0.15s. It has been perceived with send interval 0.25s in network operation performance. In general, send interval 0.25s contained low data flow in the network, so the delay is higher in 0.1s than 0.25s, but because the Sinkhole attack joins in the network when the send interval is 0.25s, it also increased the delay in the network. The delay is higher when the numbers of vehicles are 50 in the network. It is not very effective in the network when the network contained 10 and 20 vehicles, but with more than 20 vehicles in the network, the delay is increased and it affect the overall network performance.

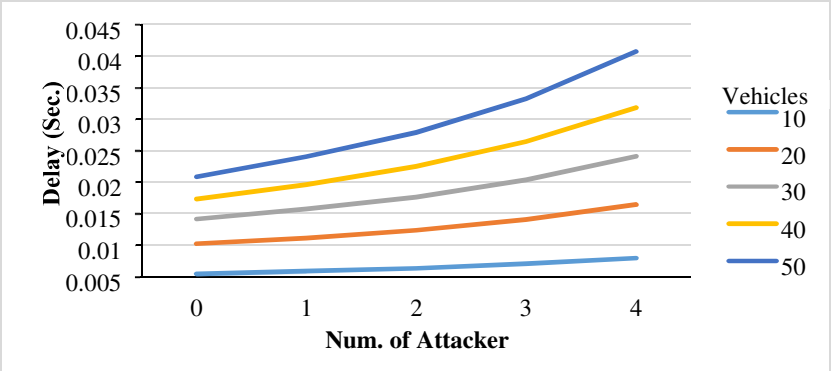

Figure 8: Analysis the Delay of VANET in the presence of Sinkhole attack with send interval 0.10s

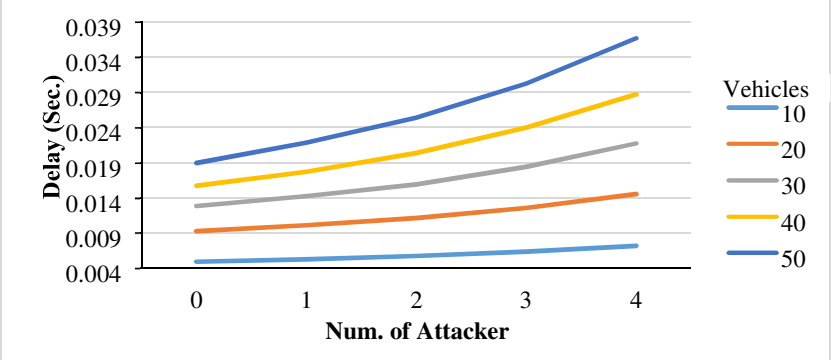

Figure 9: Analysis the Delay of VANET in the presence of Sinkhole attack with send interval 0.15s

Penerbit Akademia Baru
Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 1, No. 1. Pages 16-32, 2015

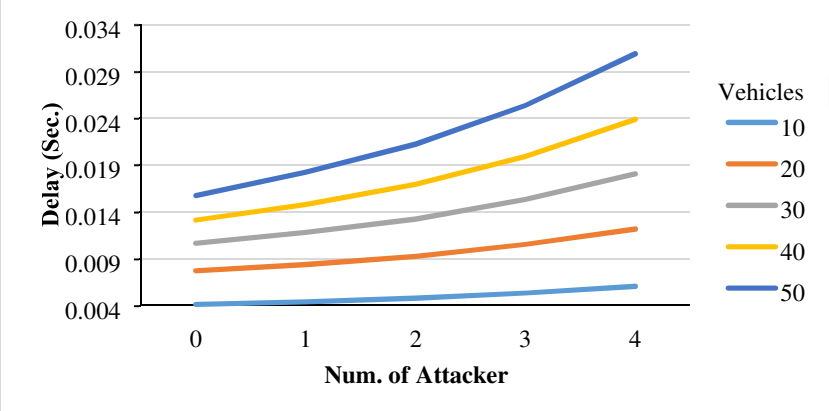

Figure 10: Analysis the Delay of VANET in the presence of Sinkhole attack with send interval 0.20s

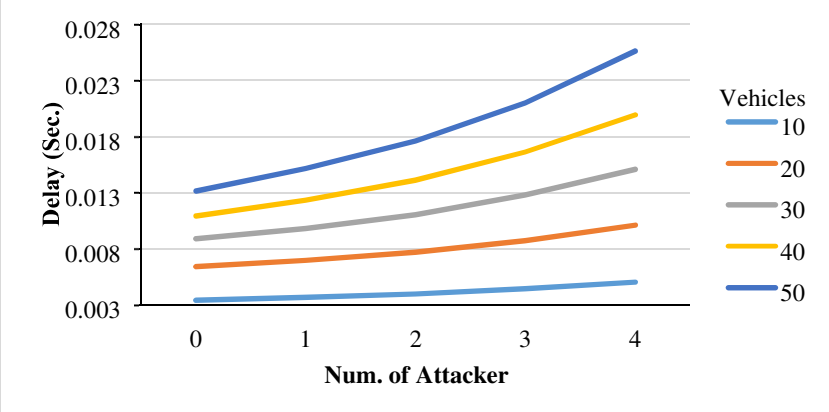

Figure 11: Analysis the Delay of VANET in the presence of Sinkhole attack with send interval 0.25s

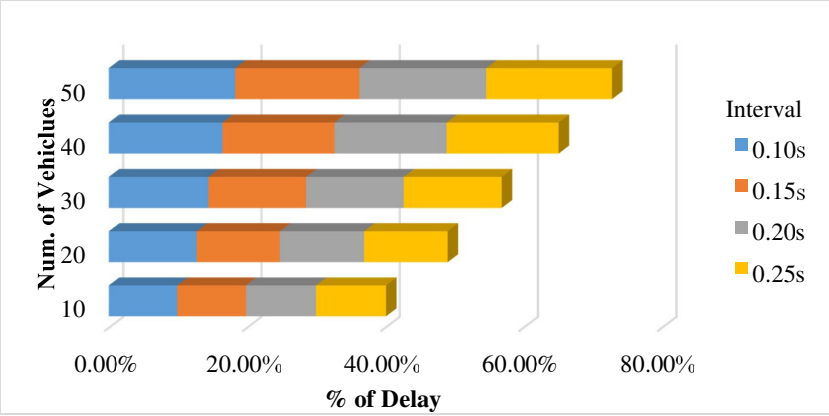

Figure 12: Analysis the average Delay of VANET in the presence of Sinkhole attack

Figure 12 shown the overall scrutinization of average delay with different send intervals in the presence of Sinkhole attacker vehicles. Hence, overall sum-up when the send interval 0.10s, or when the traffic flow is higher in the presence of 50 vehicles participation then delay is increased approximately 72%. It has been observed that when the number of vehicles is increasing in the network with the presence of Sinkhole attack, the delay is increasing rapidly, however, when the number of vehicles is less than 20 in the network, the delay is also increased, but more than 20vehicles participation in the network increased the delay rapidly.

CONCLUSIONS

The simulation result shows that the ratio of impact for sinkhole attack and timing attack varies significantly depending on the number of vehicles in the network, number of attacker vehicles (sinkhole attack and timing attack) and different number of send interval such as high data flow and low data flow in the network, it is shown that performance reduces when the number of attacker vehicles (sinkhole attack and timing attack) increases significantly with the increase in the number of vehicles in the network such as it compared with low number of vehicles less than 20 and big number of vehicles in network such as 50 vehicles, and it evaluated that when the number of vehicles is less than 20 in the network then the overall network performance is less under harm. On the other hand, when the number of vehicles is more than 20 in the presence of Timing attack and Sinkhole attack. Delay increased approximately 80% in the presence of Timing attack while the delay is increased approximately 72% in the presence of Sinkhole attack.

REFERENCE

[1] F. Ye, A. Chen, S. Lu, L. Zhang, A scalable solution to min: cost forwarding in large sensor networks, Tenth International Conference on Computer Communications and Networks, IEEE, Scottsdale, AZ, 2001, pp. 304-309.

[2] B. Krishnamachari, D. Estrin, S. Wicker, The impact of data aggregation in WSN, 22nd International Conference on Distributed Computing Systems Workshops, IEEE, Washington, USA, 2002, pp. 575–578.

[3] U. Cetintemel, A. Flinders, Y. Sun, Power-efficient data dissemination in WSN, MobiDE, CA, USA, ACM, 2003.

[4] Y.J. Zhao, R. Govindan, D. Estrin, Residual energy scans for monitoring WSN, Wireless Communications and Networking Conference, IEEE, 2002, pp. 356-362.

[5] C. Karlof, D. Wagner, Secure routing in WSN: Attacks and countermeasures, Workshop on Sensor Network Protocols and Applications (SNPA), IEEE, Anchorage, Alaska, USA, 2003.

[6] N. Milanovic, M. Malek, A. Davidson, V. Milutinovic, Routing and Security in MANET, Computer 37 (2004) 61-65.

[7] J. Cai, P. Yi, J. Chen, Z. Wang, N. Liu, An adaptive approach to detecting black and gray hole attacks in ad hoc network, 24th IEEE International Conference on Advanced Information Networking and Applications (AINA), IEEE, Perth, WA, 2010, pp. 775-780.

[8] X. Zhang, Y. Sekiya, Y. Wakahara, Proposal of a method to detect black hole attack in MANET, International Symposium on Autonomous Decentralized Systems, IEEE, Athens, 2009, pp. 1-6.

[9] I.A. Sumra, J.A. Manan, H. Hasbullah, Timing Attack in Vehicular Network, Recent Researches in Computer Science (2011) 15th World Scientific and Engineering Academy and Society (WSEAS), at Corfu Island, Greece pp. 151-155.

[10] S.M. Bo, H. Xiao, A. Adereti, J.A. Malcom, C. Bruce, A performance comparison of wireless ad hoc network routing protocols under security attack, Third International Symposium on Information Assurance and Security, IEEE, Manchester, 2007, pp. 50-55.

[11] W. Chen, L. Xiang, G. Xiaopeng, A new solution for resisting gray hole attack in MANET, Second International Conference on Communications and Networking, IEEE, Shanghai, 2007, pp. 366–370.

[12] M.S. Al Mazrouei, S. Narayanaswami, Mobile adhoc networks: A simulation based security evaluation and intrusion prevention, International Conference for Internet Technology and Secured Transactions (ICITST), IEEE, Abu Dhabi, 2011, pp. 308- 313.

[13] O. Adaobi, E. Igbesoko, M. Ghassemian, Evaluation of Security Problems and IDS for Routing Attacks in Wireless Self-Organized Networks, 5th International Conference on New Technologies, Mobility and Security (NTMS), IEEE, Istanbul, 2012, pp. 1-5.

[14] I.A. Sumra, H. Hasbullah, J.A. Manan, Effects of attackers and attacks on availability requirement in vehicular network: a survey, International Conference on Computer and Information Sciences (ICCOINS), IEEE, Malaysia, 2014, pp. 1-6.

[15] A. Rawat, S. Sharma, R. Sushil, VANET: security attacks and its possible solutions, Journal of Information and Operations Management 3 (2012) 301-304.

[16] T.W. Chim, S.M. Yiu, L.C.K. Hui, V.O.K. Li, Security and privacy issues for intervehicle communications in VANETs, Sensor, 6th Annual IEEE Communications Society Conference on Mesh and Ad Hoc Communications and Networks Workshops, IEEE, Rome, 2009, pp. 1-3.

[17] H. Liu, Z. Shang, Comparing the performance of the ad hoc network under attacks on different routing protocol, International Journal of Security and Its Applications 9 (2015) 196-208.

[18] L. Long, R. Baldessari, Performance evaluation of beacon congestion control algorithms for VANETs, Proceeding of IEEE Globecom, IEEE, Houston, TX, 2011, pp. 1-6.

[19] H. Hartenstein, P.L. Kenneth, A tutorial survey on vehicular ad hoc networks, IEEE Communications Magazine 46 (2008) 164-171.

[20] The CAMP Vehicle Safety Communications Consortium, Vehicle Safety Communications Project Task 3 Final Report, Sponsored by USDOT. Available through National Technical Information Service, Spring_eld, Virginia 22161, 2005.

[21] H.L. Vinh, C. Ana, Security attacks and solutions in vanet: a survey, International Journal on AdHoc Networking Systems 4 (2014) 1-20.

[22] M.S. Al-Kahtani, Survey on security attacks in Vehicular Ad hoc Networks (VANETs), 6th International Conference on Signal Processing and Communication Systems (ICSPCS), IEEE, Gold Coast, QLD, 2012, pp. 1-9.

[23] B. Mishra, P. Nayak, S. Bahera, D. Jena, Security in vehicular adhoc networks: a survey, ICCCS, ACM, Rourkela, 2011, pp. 590-595.

[24] Y. Wang, F. Li, VANET, Springer-Verlag, London, 2009.

[25] I. Chakeres, C. Perkins, Dynamic MANET On-demand (DYMO) Routing draft-ietfmanetdymo-17, Internet Engineering Task Force, 2007, Available: https://tools.ietf.org/html/draft-ietf-manet-dymo-26.