Identifying the Impacts of Node Mobility on Network Layer Based Active and Passive Attacks in Mobile Ad Hoc Networks: A Simulation Perspective

Uthumansa Ahamed[1(✉)] and Shantha Fernando[2]

[1] Department of Physical Sciences, Faculty of Applied Sciences, Rajarata University of Sri Lanka, Mihintale, Sri Lanka
[2] Department of Computer Science and Engineering, Faculty of Engineering, University of Moratuwa, Colombo, Sri Lanka
shantha@cse.mrt.ac.lk

Abstract. Ad hoc On-demand Distance Vector Routing (AODV) is a routing protocol that is used in Mobile Ad hoc Network (MANET). Pure AODV protocol is failed to handle the security. In this research, we try to find the answers for the following research questions to upgrade AODV protocol in security concern. I). Does node mobility in a MANET impact the behavior of a malicious node? II). Is node mobility need to be considered when designing appropriate security countermeasures? We used Network Simulator 2 (NS2) for simulations and AODV as routing protocol. Blackhole and Grayhole attacks are selected to study the network layer based Active attacks and Wormhole attack is used for Passive attack. We observed the impacts of each attacks by changing the speed of nodes and the numbers of connected node in the network. We changed the directions of node mobility randomly during the simulation. Though node speed is constant for all nodes. Number of nodes and nodes speed are changed to collect more accurate results. We compared the performances of each network with a controller. Few Performance Matrices (PM) (Packet Delivery Ratio (PDR), End to End Delay (EED) and Throughput) are used to evaluate the network performances. Mobile nodes degrade the network performances. Node mobility either leads to break the links between nodes nor to create new links. Therefore it creates an opportunity to break the link with malicious node. We can screen the malicious node at routing if a routing protocol is equipped with an initial screening mechanism for malicious nodes.

Keywords: Node mobility · Active attacks · Passive attacks · Simulation study

1 Introduction

MANET is a type of Ad hoc Network [1] that is formed by self configurable wireless mobile devices: mobile phones, laptops and other mobile devices. These devices

N. Chaubey et al. (Eds.): COMS2 2021, CCIS 1416, pp. 262–275, 2021.
https://doi.org/10.1007/978-3-030-76776-1_18

are called as nodes. The main character of a MANET is mobile nodes. Source, destination and intermediate nodes are available in MANET [1]. The limited wireless radio range makes source node to depend on number of intermediate nodes to communicate with destination which is not in its‘ radio range. This nature is called as multi-hop routing. Relatively Low cost of network deployment and opportunistic nature enables MANET into many applications. For instance disaster situations, hostile environments and military operations when infrastructure networks are unavailable [1].

Basically routing protocols are categorized into two: Proactive and Reactive. AODV [2] is an example for reactive routing protocol that is more suitable for MANET [1]. Fundamental characters of MANET are dynamic network topology, open network boundary and infrastructure-less nature. These characters are the reasons for the security threats in a MANET [1]. Therefore pure AODV protocol is insecure for data communications. In order to propose a security mechanism following research questions should be answered. I). Does node mobility in a MANET impact the behavior of a malicious node? II). Is node mobility need to be considered when designing appropriate security countermeasures?

Rest of the paper is organized as follows. Related literature are reviewed in Sect. 2 to identify research gap. State of the art of the node mobility related researches are presented on Sect. 3 to point-out the importance of this study. Section 4 describes about the research methodology. Section 5 expresses the results and discussions in our study. Section 6 explains about the conclusion and proposed future works.

2 Literature Review

Camp, T. et al. [3] presented simulation results by using synthetic mobility models which are used in ad hoc network simulation. The data traffic pattern of the mobility model greatly influences the protocol performances. Moreover they [3] argued that Random Way-point Mobility Model (RWMM) is flexible and it creates a realistic mobility patterns and Random Direction Mobility Model (RDMM) is unrealistic than RWMM. The Boundless Simulation Area Mobility, Gauss–Markov Mobility, Probabilistic Random Walk Mobility Models provide movement patterns that one might expect in the real world. Sharma, G. et al. [4] constructed movement paths using the Voronoi diagram of obstacle vertices that is more realistic movement model through the incorporation of obstacles. Connectivity of the nodes, network density, packet delivery and overhead of the routing protocol are effected because of the mobility model. Bai, F et al. [5] did a study and analyze various mobility models and their effects on MANET protocols. Furthermore they [5] attempted to provide current research status of mobility modeling and analysis. They concluded that a requirement method is needed to select a suitable set of mobility models. Lin, G. et al. [6] proposed a technique that enables accurate derivation of steady state distribution functions for node distance and speed to analyze mobility model based on the renewal theory. This theoretical solution is suitable for speed decay problem of nodes in

RWMM. Atsan, E. et al. [7] provided a hybrid classification for mobility models. They used Random Walk Model (RWM) and RWMM during their simulation study. Simulation results are discussed based on the simulation settings and parameters. They simulated based on the varying number of nodes and size of the simulation area. RDMM and RWM showed worst performance. AODV protocol performed well for boundless simulation area mobility model.

Sharma, G. et al. [4] designed a research to answer three research questions based on the different mobility models and delay capacity relationship. Their study results showed that the mobility models are considered in the literature are in some sense extreme: they either exhibit the smallest critical delays or the largest critical delays among the mobility models. They introduced an idea of critical delay that is studied to identify the tolerated value to enhance the network capacity. They showed that the critical delay is inversely proportional to the length of the node traveled path in same direction [4]. Radha, S. et al. [8] discussed the survey of about different mobility models that are independent and dependent node mobility. They stated that exponential model performs well than the uniform models for expanded speeds and traffic loads. They stated that best performance is possible with the combination of different mobility models. Ting, Z. et al. [9] studied about node mobility model in vehicular communication system. They suggested to use RWMM and RDMM in a simple environment because of its less computational overhead compared to Vehicular mobility model.

Ciullo, D. et al. [10] analyzed the correlated node movement based on the real mobility process. They enforced the Group Mobility model for better network performances than independent node movements. Through the study, they revealed the wide range of correlated node movements help to better performance than the independent nodes movements. Khairnar, V. et al. [11] evaluated the RWMM through a simulation study in a VANET. They stated that MOVE allows to customize the RWMM in a realistic manner. Vasanthi, V. et al. [12] analyzed some mobility models. Their simulation study is based on the RWMM in DSR routing protocol. The study aims to prove the affect of mobility model on the network performances of the simulation. Finally they concluded that simulation results highly dependent on the node mobility model used in the simulation. Zarifneshat, M. et al. [13] attempted to propose modification on the random mobility models and Levy walk mobility model to enhance the simulation node mobility into realistic ones. Their simulation study is based on random mobility model. Through the simulations results they exposed the correlation between occurrence of an accelerated movement and event of mobile node's direction change. Han, G. et al. [14] tried to measure the influences of mobility of the selected nodes in an Mobile Wireless Sensor Network on the DV-hop localization algorithm. RWMM, RDMM and Reference Point Group Mobility models are used for the simulation study [14]. They conclude that RD and RWP mobility models perform well in DV-hop localization algorithm. Moreover, mobility models greatly affect the DV-hop localization algorithm. Othman, N. et al. [15] investigate about the node mobility on node cooperation in MANET. In their

study they observed that RWMM and Steady-state RWMM impact similarly on the cooperative nodes. Furthermore Self Similar Least Action Walk Mobility model significantly differ from other two models. Finally they concluded that different mobility models produce different impacts on the network.

Though researchers conducted different studies on the node mobility of the network and different mobility models there are no any study considering on the impacts of node mobility of malicious node.

3 State of the Art

As discussed under literature review section, in 2002, Camp, T. et al. [3] surveyed different mobility models for ad hoc network to illustrate the importance of selecting a mobility model for a simulation. Furthermore relationship between mobility model and the network performances is exposed. In 2003, Jardosh, A. et al. [16] proposed a realistic mobility model by introducing obstacles on the route of node movement. Bai, F. et al. [5] surveyed and examined different mobility models that has unique characters such as temporal dependency, spatial dependency or geographic restriction. In 2004, Lin, G. et al. [6] proposed a new methodology to simulate mobility of nodes with a guaranteed steady state for node movement distribution from the beginning. In 2006, Atsan, E. et al. [7] surveyed and proposed a hybrid classification on existing mobility models. In 2006, Radaha, S. et al. [8] presented a survey which helps researchers to select a research model for the simulation study based on the performance evaluation. Furthermore, they concluded that combination of different mobility model may be more effective for simulations. Sharma, G. et al. [4] analyzed different mobility models by using a framework which evaluates a mobility model by critical delay. In 2009, Ting, Z. et al., [9] presented a comparative study of mobility models on VANET. In 2011, Ciullo, D. et al. [10] concluded from their research study that correlated nodes movements lead to better performance than independent node movement mobility models. In 2012, Vasanthi, V. et al. [12] analyzed different mobility models including entity models. In 2013, Zarifneshat, M. et al. [13] mobility trace produced by a mobility trace generator tool. They used association rule mining concept to find possible correlation between mobile nodes. In 2014, Othman, N. et al. [15] investigated the impacts of few mobility models. In the same year, Han, G. et al. [14] quantified the influence of mobility of a node that moved based on three different mobility models by using DV hop based localization model.

4 Methodology

Computer simulation is considered as the research instrument to collect empirical data such as field experiment do [16]. Table 1 shows parameters that are maintained during the simulations. Attacks are introduced individually to the network to check the impacts separately. Impacts on the network is expressed

through the PDR, EED and Throughput. PDR is a ratio between total number of received packets from destination node and total number of packets sent by the source node [1]. EED is a time that is taken by a packet to reach the destination node [1]. Units are in seconds. Throughput is a ratio between total number of successfully received packets by destination node and total time taken to receive all the packets [1]. Units are in bytes per second (bps). The attacks are introduced to the network by modifying the functions of AODV protocol [1]. Grayhole attacks is configured as to drop all packets after a certain period of time. Transmission range in between wormhole nodes are maintained as twice the range of the normal node during the wormhole attack simulations. We considered following assumptions.

- Nodes are identical.
- Configurations are unique for all nodes except wormhole nodes.
- Malicious nodes show abnormal behavior during the communication.

Table 1. NS2 parameters

Parameter	Value
Simulator	NS2 (v.2.35) [17]
Frequency	9.14×10^8 Hz
Bandwidth	2.0×10^6 bps
Antenna/OmniAntenna X, Y, Z	0, 0, 1.5 m
Radio-propagation model	TwoRayGround
Network interface type	Phy/WirelessPhy
Traffic type	Constant bit rate (CBR)
Max packets in Interface Queue	50
Nodes Transmitter range	250 m
Number of nodes	10, 15, 20, 25, 30
Node Speed	0, 5, 10, 15, 20 ms^{-1}
Simulation Area X, Y	1500 m, 2500 m
Simulation time	10 s

5 Results and Discussion

Table 2 contains the average values of each PM of the networks which are affected by different security attacks. In this experiment, node mobility is maintained as zero ms^{-1} in each network. Average values of PM are obtained by averaging each corresponding PM values. Average PDR, EED and Throughput values of the controller network are 50.58%, 0.76 s and 6746.51 bps. According to the results PDR value is decreased on increasing the number of connected nodes in the network. Though, PDR value is increased at last. EED value is increased

for increasing the connected nodes amount. Furthermore Throughput value is decreased gradually on increasing number of connected nodes in the network. The reason is, the packets needed to travel through many nodes while increasing the nodes amount.

Due to the effect of Blackhole attack PDR, EED and Throughput of the network are 0.28%, ∞ and 0.33% compared to the controller network. Blackhole node does not allow any data packets but routing packets. PDR and Throughput values are not zero because Blackhole node allows only routing packets. Therefore the Blackhole attack degraded the network performances than all the other network performances.

Wormhole attack enhanced the network performances than other networks including controller network. Because of the higher speed data transferring wormhole tunnel between wormhole nodes. Therefore data packets quickly transfer through the tunnel. Furthermore, wormhole attack is a passive attack which shows no harm or undetectable harm to the network [1]. PDR, EED and Throughput values are 151.60%, 1.31% and 178.41% compared to the controller network.

The network shows intermediate performances in the presence of Grayhole attack. The performances are lower than controller network and higher than the network with Blackhole attack. PDR, EED and Throughput values are 51.30%, 92.67% and 57.23% compared to the controller network.

Table 2. Network performances in zero node mobility

Performance matrices	Controller	Blackhole	Grayhole	Wormhole
PDR	50.58	0.14	25.95	76.68
EED	0.76	∞	0.71	0.01
Throughput	6746.51	22.34	3861.28	12036.26

Figure 1 shows the graph plotted between PDR of different number of connected nodes in the network vs node speed in the presence of Blackhole attack. According to the simulations results, the link between source and Blackhole node is broken and established again at lower number of nodes with higher speed of node mobility. Therefore graph shows slight increase at that point. In the other cases, link breakages did not occur along with the Blackhole node or no any new links are established after a link breakage with Blackhole node.

Figure 2 shows the graph plotted between PDR of different number of connected nodes in the network vs speed of node mobility in the presence of Grayhole attack. According to the simulations results, when the number of connected nodes and the speed are increased the link between the source and Grayhole node breaks. Then a new route is established between source and destination node. Therefore PDR is increased. When the speed of node mobility is very high, PDR values are decreased due to the breakage of the existing links among the nodes.

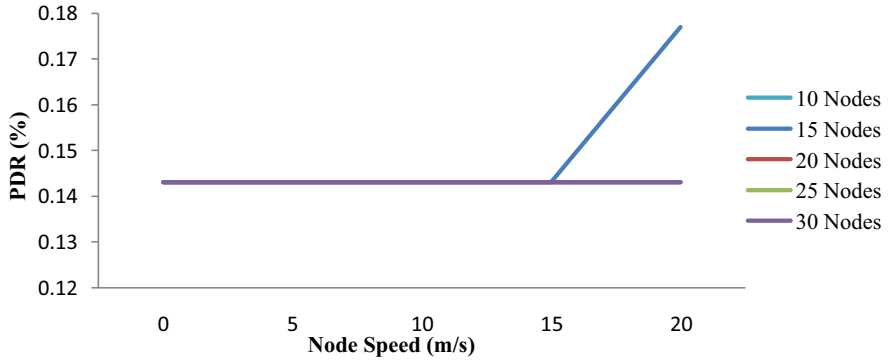

Fig. 1. PDR of the network with Blackhole attack vs node speed

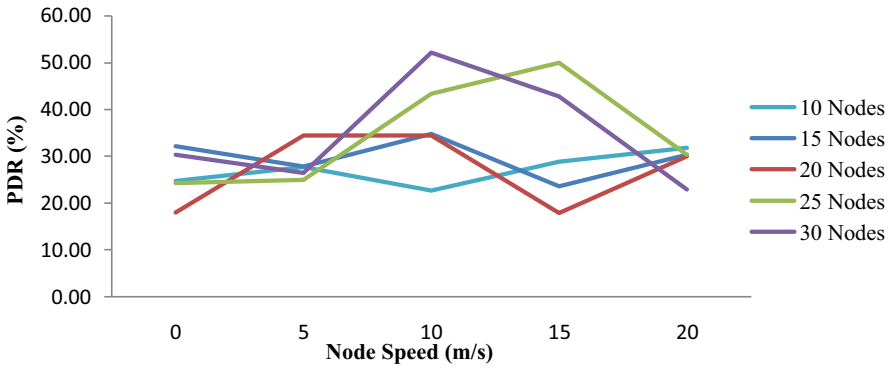

Fig. 2. PDR of the network with Grayhole attack vs node speed

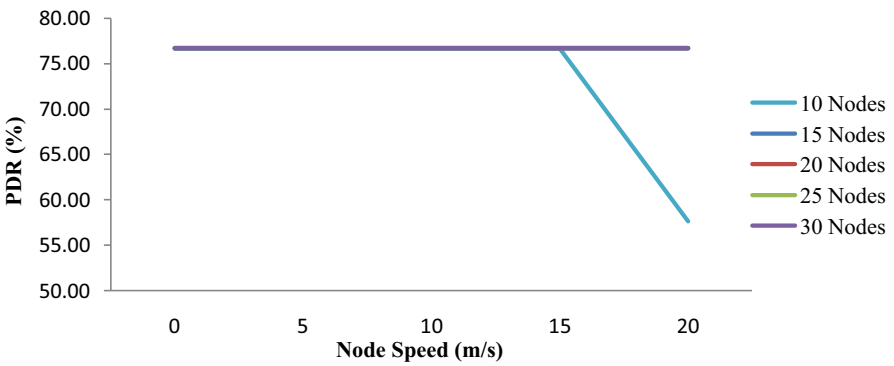

Fig. 3. PDR of the network with Wormhole attack vs node speed

Figure 3 is the graph of PDR value of different number of connected nodes in the network vs speed of node mobility in the presence of Wormhole attack. According to the simulations results when the number of connected nodes and speed of nodes are increased PDR value remains same because of the wormhole tunnel. Though when number of node is low and speed of the node is high the link between the source node and the wormhole node breaks. Therefore PDR value is decreased.

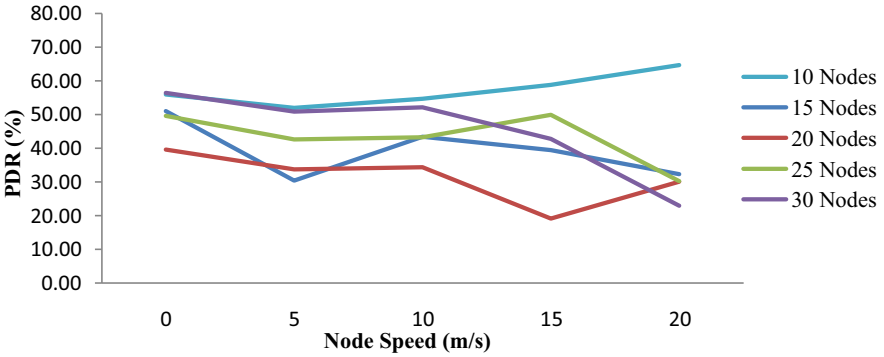

Fig. 4. PDR of controller network vs node speed

Graph between PDR of different number connected of nodes in the network vs speed of node mobility of the controller network is shown in Fig. 4. According to the Fig. 4, though the number of connected nodes are increased, PDR value is decreased. This is because of the higher speed of node mobility increases the links breakage. Therefore amount of data received by destination is decreased. Even when the number of connected nodes are decreased, destination can receive data by new links which are created by higher speed of node mobility.

Figure 5 shows the graph plotted between EED of different number of connected nodes in the network vs speed of node mobility in the presence of Blackhole attack. According to the simulation results, destination node did not receive any data packets either number of connected nodes in the network is increased or speed of node mobility is increased. Therefore all the graphs are lie on zero.

Figure 6 shows the graph plotted between EED of different number of connected nodes in the network vs speed of node mobility in the presence of Grayhole attack. According to the results, when the speed of the node mobility and number of connected nodes in the network are increased links are broken including the link between Grayhole node and the source node. Therefore source node is able to communicate with destination with lowest hop count. Therefore EED is decreased when number of connected node and speed of the nodes mobility are increased.

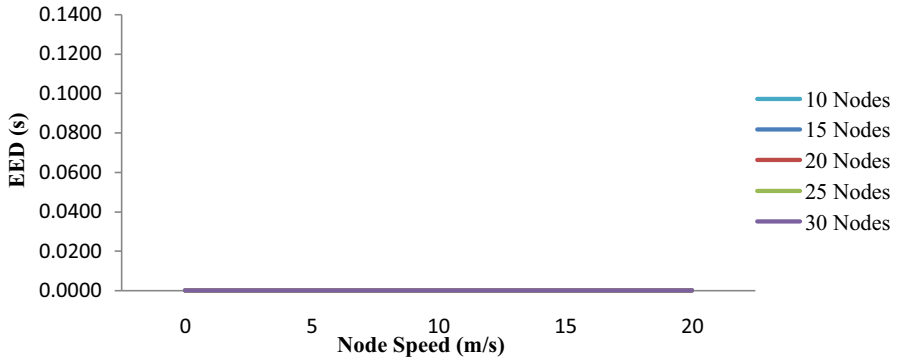

Fig. 5. EED of the network with Blackhole attack vs node speed

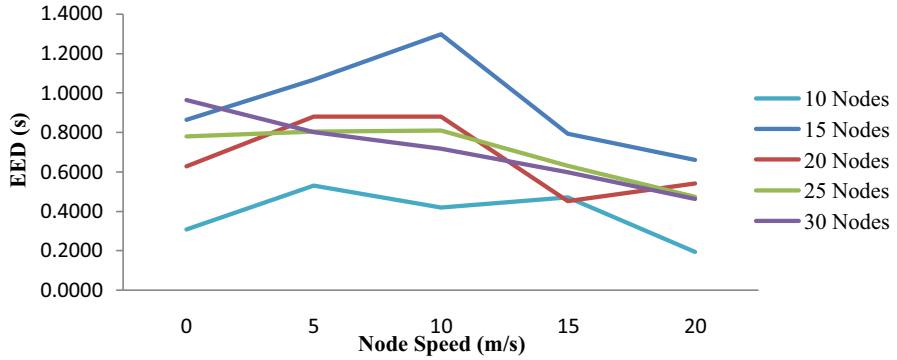

Fig. 6. EED of the network with Grayhole attack vs node speed

Figure 7 shows the graph plotted between EED of different number of connected nodes in the network vs speed of node mobility in the presence of Wormhole attack. According to the results, when the speed of nodes mobility and number of connected nodes in the network are increased links are broken including the link between Grayhole node and the source node. Therefore source node is able to communicate with the destination with lowest hop count. Therefore EED is decreased when number of connected nodes and speed of the nodes mobility are increased.

Figure 8 is the graph between EED of different number of connected nodes in the network vs speed of node mobility of the controller network. According to the results, when the number of connected nodes and the speed of the node mobility are increased the EED value is decreased. This is because with higher number of node and higher node speed existing links are broken and new links are created. Furthermore data packets are reached the destination through newly created shortest route.

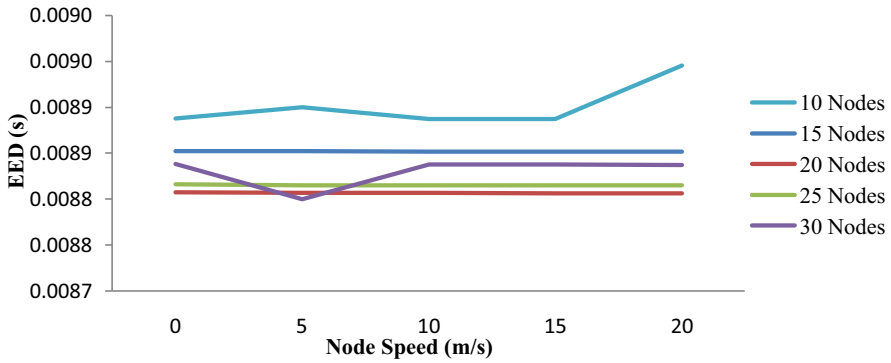

Fig. 7. EED of the network with Wormhole attack vs node speed

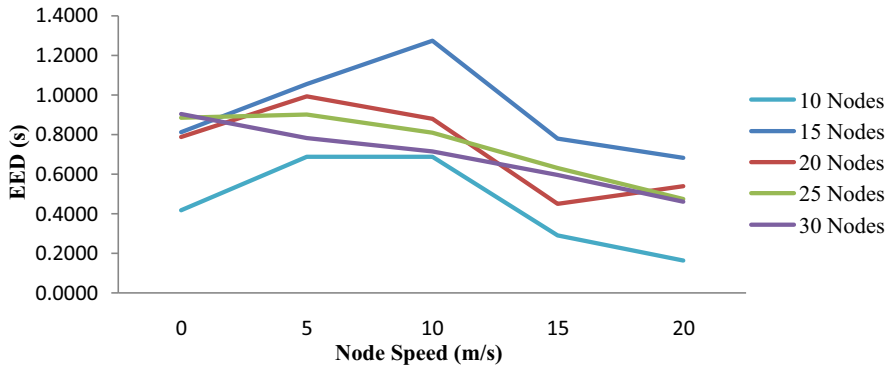

Fig. 8. EED of controller network vs node speed

Figure 9 shows the graph plotted between Throughput of different number of connected nodes in the network vs speed of node mobility in the presence of Blackhole attack. According to the Fig. 9, when the number of connected nodes and the speed of the node mobility are increased the Throughput value remains same. This is because of Throughput of RREQ packets. Furthermore There was no any link breakage between source node and Blackhole node or no any new links are created due to the node mobility. Graph between Throughput of different number of connected nodes in the network vs speed of node mobility of the network which is affected by Grayhole attack is shown in Fig. 10. According to the Fig. 10, when the number of connected nodes and the speed of the node mobility are increased the Throughput value is decreased. This is because of the link between the source and Grayhole node is broken and new links are not formed between source and destination node. Furthermore in lower number of

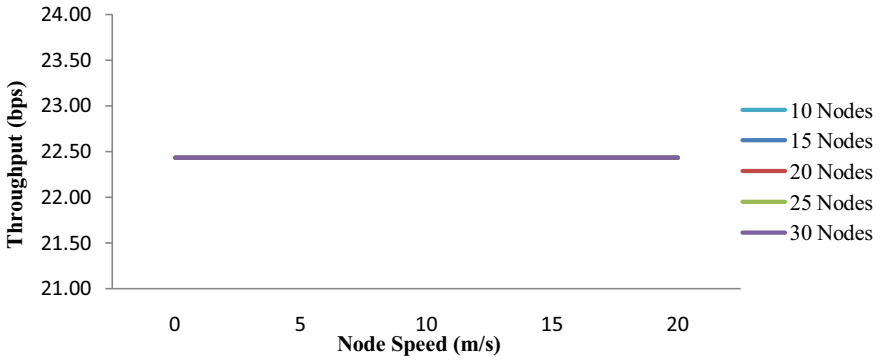

Fig. 9. Throughput of the network with Blackhole attack vs node speed

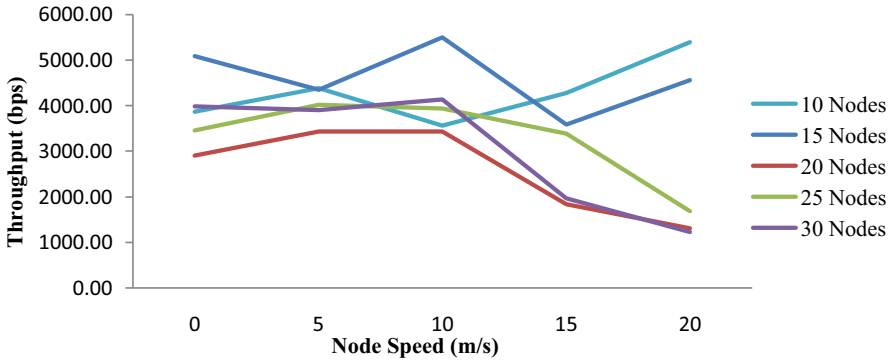

Fig. 10. Throughput of the network with Grayhole attack vs node speed

connected nodes in the network with higher speed of node mobility new links are established between source and the destination node. Therefore Throughput value is increased.

Figure 11 shows the graph plotted between Throughput of different number of connected nodes in the network vs speed of node mobility in the presence of Wormhole attack. Though number of connected nodes in the network is increased and speed of the node mobility is increased Throughput remains same. The reason is Wormhole node are able to maintain the link with source node. Furthermore the link between source node and Wormhole node is broken with the lower number of connected nodes in the network and with the higher speed of node mobility. Therefore Throughput value is decreased. Figure 12 shows the graph plotted between Throughput of different number of connected nodes in the network vs speed of node mobility of the controller network. According to the simulation results, when the number of connected node in the network and the speed of node mobility are increased, Throughput value is decreased. The reason is the link breakage between nodes. Though in the lower number of connected

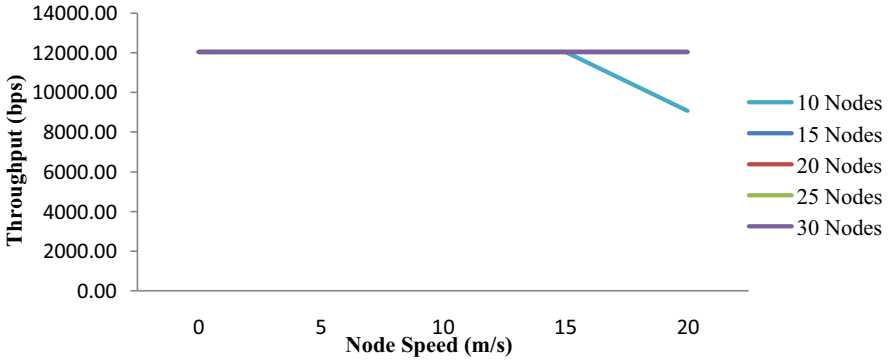

Fig. 11. Throughput of the network with Wormhole attack vs node speed

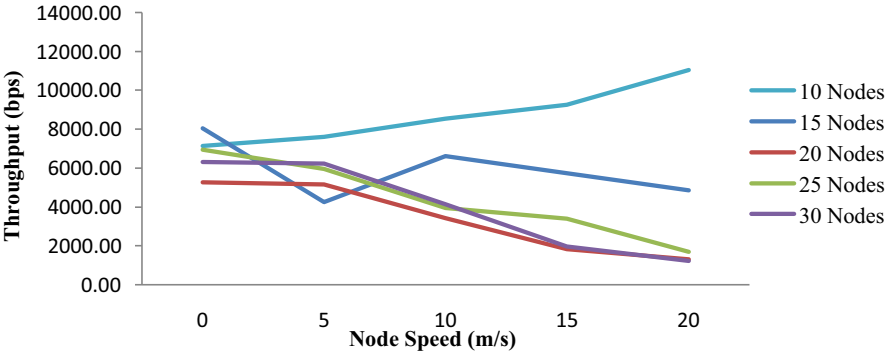

Fig. 12. Throughput of Controller network vs node speed

nodes in the network and higher speed of node mobility Throughput value is increased. Because source node is able to create new and shortest path between destination node.

6 Conclusion and Future Works

Node mobility in the network degrades the MANET performances that differ from one another based on the node speed and direction of the movement. Node mobility leads to occasional link breakage between nodes in the MANET. Therefore link breakage affects the activity of a malicious node. All the nodes including malicious node need to under go for route establishment between source and destination nodes after a link breakage. Therefore node mobility need to be considered when designing appropriate security countermeasures. Because if a routing protocol is equipped with malicious screening mechanisms on route discovery stage then malicious nodes can be screened. Link breakage is favorable for security. Because, It is possible to identify Black hole nodes from the initial

screening mechanisms on the routing process. Furthermore, it is helpful to find new shortest path to destination node after the nodes movements. During the simulation we observed that initial route links are maintained in AODV until it breaks. Though, destination node is very close to source node. Therefore, this is opened to another research regarding the existing route verification for shortest path for communication during the communication.

References

1. Ahamed, U., Fernando S.: Identifying the impacts of active and passive attacks on network layer in a mobile ad-hoc network: a simulation perspective. Int. J. Adv. Comput. Sci. Appl. **11**(11) (2020). https://doi.org/10.14569/IJACSA.2020.0111173
2. Perking, C. Royer, E.: Ad-hoc on-demand distance vector routing. In: 2nd IEEE Workshop on Mobile Computing Systems and Applications, LA, USA, pp. 90–100. IEEE (1999)
3. Camp, T., Boleng, J.D., Davies, V., et al.: A survey of mobility models for ad hoc network research. Wireless Commun. Mob. Comput. **2**(5), 483–502 (2002)
4. Sharma, G., Mazumdar, R., Shroff, N.: Delay and capacity trade-offs in mobile ad hoc networks: a global perspective. IEEEs ACM Trans. Netw. **15**(5), 981–992 (2007). https://doi.org/10.1109/TNET.2007.905154
5. F. Bai, F. Helmy, A.: A survey of mobility models. In: Wireless Ad-hoc Networks. University of Southern, California (2004)
6. Lin, G. Noubir, G. Rajaraman, R.: Mobility models for ad hoc network simulation. In: IEEE INFOCOM 2004, Hong Kong, pp. 454–463 (2004). https://doi.org/10.1109/INFCOM.2004.1354517
7. Atsan, E. Özkasap, Ö.: A classification and performance comparison of mobility models for ad hoc networks. In: Kunz, T., Ravi, S. (eds.) ADHOC-NOW 2006, LNCS, pp. 444–457. Springer, Heidelberg (2016). https://doi.org/10.10007/1234567890
8. Radha, A., Shanmugavel, S.: Mobility models in mobile ad hoc network. IETE J. Res. **53**(1), 3–12 (2007)
9. Ting, Z. Jianjun, H. Li, S. Jianfeng, L. Yan, M.: Study on mobility models in vehicular communication system. In: 2009 2nd IEEE International Conference on Broadband Network & Multimedia Technology, Beijing, pp. 57–61 (2009). https://doi.org/10.1109ICBNMT.2009.5347824
10. Ciullo, D. Martina, V. Garetto, M. Leonardi, E.: Impact of correlated mobility on delay-throughput performance in mobile ad-hoc networks. In:2010 Proceedings IEEE INFOCOM, CA, San Diego, pp. 1–9 (2010). https://doi.org/10.1109/INFCOM.2010.5461993
11. Khairnar, V. Pradhan, S.: Mobility models for vehicular ad-hoc network simulation. In: 2011 IEEE Symposium on Computers & Informatics, Kuala Lumpur, pp. 460–465 (2011). https://doi.org/10.1109/ISCI.2011.5958959
12. Vasanthi, V., Hemalatha, M.: Simulation and evaluation of different mobility models in ad-hoc sensor network over DSR protocol using Bonnmotion tool. In: Thampi, S.M., Zomaya, A.Y., Strufe, T., Alcaraz Calero, J.M., Thomas, T. (eds.) SNDS 2012. CCIS, vol. 335, pp. 157–167. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-34135-9_16

13. Zarifneshat, M., Khadivi, P.: Using mobile node speed changes for movement direction change prediction in a realistic category of mobility models. J. Netw. Comput. Appl. **36**(3), 1078–1090 (2013)
14. Han, G., Chao, J., Zhang, C., Shu, L., Li, Q.: The impacts of mobility models on DV-hop based localization in Mobile Wireless Sensor Networks. J. Netw. Comput. Appl. **42**, 70–79 (2014)
15. Othman, N. Hassan, R. Hasan, S.: The impact of mobility models on nodes cooperation in mobile ad hoc networks. In: 2014 IEEE Student Conference on Research and Development, Batu Ferringhi, pp. 1–5 (2014). https://doi.org/10.1109SCORED.2014.7072943
16. Barberousse, A. Franceschelli, S. Imbert, C.: Computer simulations as experiments. Synthese **169**(2012). https://doi.org/10.1007/s11229-008-9430-7
17. Issariyakul, T. Hossain, E.: Introduction to Network Simulator NS2, 2nd edn. Springer, Heidelberg (2012). https://doi.org/10.1007/978-1-4614-1406-3