www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 6 Issue 10 October 2017, Page No. 22602-22611
Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i10.09

Analytical Approach on Routing Protocols in Wireless Ad-Hoc Networks under Security Attacks

IR Saidu[1], MZ Haruna[2], MM Isa[3]

[1]Nigerian Defence Academy Kaduna
[2]Nigerian Defence Academy Kaduna, Nigeria
[3]Nigerian Defence Academy Kaduna, Nigeria

Abstract
Wireless networks have certainly been a revolution in today's technologically as one of the most vital and active fields in the communication industries. These wireless ad-hoc networks consists of independent nodes with decentralized administration and physical infrastructures, with a dynamic topology in which nodes can easily leave or join the network at all time and also move freely. In other not to compromise the confidentiality, and integrity of network services, the safety of packets data can only be achieved by guaranteeing that the problem of security has met the requisite standard. The performance analyses of routing protocols for Ad-Hoc wireless networks, DSDV, DSR and AODV were investigated using network parameters such as averages throughput, packet delivery ratio and End-to-end delay using various scenarios of mobile node and size of the network. Awk script was used to analyze the trace file and produce the average throughput, packet delivery ratio and end-to-end delay as the result of the simulation. The simulation was run by implementing codes in DSDV, DSR and AODV CC class files to accommodate the behavioral pattern of attacks. The results analysis of routing protocols under the security attacks, it was observed that the DSDV significantly has lower performance as a result of frequent link changes and connection failures which led to heavy overload and congestion problems. Furthermore, when comparing the two reactive routing protocols, AODV performs better than DSR.

Keywords: Ad-Hoc wireless networks, DSDV, DSR, AODV, Averages Throughput, Packet Delivery Ratio and End-to-end delay

1.0 Introduction

Wireless networks have certainly been a revolution for communication technique in today's technologically as one of the most vital and active fields in the communication industries in the world (Almarimi *et. al*, 2014). Wireless ad-hoc networks are consists of independent nodes with decentralized administration and physical infrastructures, with a dynamic topology in which nodes can easily leave or join the network at all time and also move freely (Arya 2013). Today the principal application of Ad-Hoc networks are used during the military tactical operations. For example, military formations (such as ships, troops, or aircraft) are equipped with wireless network communication devices, usually form an Ad-Hoc network when they are deployed in a war zone.

In wireless Ad-Hoc networks, routing protocols are one of the normally interesting and research areas. There are several routing protocols for Ad-Hoc network, i.e. Dynamic Sequence Distance Victor (DSDV), Ad-Hoc On-Demand Distance Vector (AODV) Dynamic Source Routing (DSR), etc. These routing protocols are essential to the operations in Ad-Hoc networks and for any successful security breach for the routing would severely affects the performance of the entire network, this is the main purpose why the routing protocols form the attacker target (Bader et al. 2011). Security has always become the challenges for Wireless Ad-Hoc networks. It had been the most important concerns for the fundamental practicality of Ad-Hoc network due to it nature of decentralized administration access point and management.

2.0 Related Works

Most works on these Ad-Hoc wireless networks do not take mobility and security attacks into account in their comparison. The papers vary mobility but do not consider varying the number of nodes which impacts on the routing performance of the Ad-Hoc protocols. However, only few papers have made a comprehensive analysis over it. According to the study by (Bertocchi et al., 2003) a performance comparison of the routing protocols OLSR, DSR and AODV for Ad-Hoc networks without any security attack using a fixed number of nodes and then compare the standard Djikstra algorithm and concluded that protocols like AODV and DSR are the better choice if the network load is moderate and can achieve remarkable energy saving compared to OLSR protocol. (Wren 2006) reviewed the black hole and grey hole attack in wireless mesh network, the proposal was based on the analyzing of the two attacks in the network environment, with aim of prevent the network layer from these attack in which false node act as regular node and calculate the delay in both attack, and how they affect the network delay. Comparative investigation on the performance of the three routing protocols DSDV, DSR and AODV is done by (Jakhar & Speed 2013). The paper includes speed and mobility into account which is a prime contribution and studied the effects of changing node mobility rate, scalability and maximum speed on the performance of DSDV, DSR and AODV. The simulations result indicates that reactive routing protocols DSR and AODV perform better than proactive routing protocol DSDV. However, the paper strictly adheres to the performance of the routing protocols with a fixed number of nodes without under security attacks.

The present research focused on the different network sizes with security attacks which are implemented and a comprehensive performance evaluation of all the routing protocols DSDV, DSR and AODV without and with security attacks carried out. Contrary to the study by Sharma & Sengupta, (2010) who compare the performance of the routing protocols without the security attacks. Similarly, study by Nitika Lochab & and Priti Narwal, (2014) analyses the performance of the routing protocols of DSDV, DSR and AODV based on mobility model without the security. The routing performances are analysed with respect to throughput, end to end delay and packet delivery ratio.

According to another study by (Adam et al, 2011) made a comparison between DSDV, DSR and AODV and increased the network load by 5 nodes for every simulation. They likewise compared only performance of the three protocols with varying change in network load with a maximum of 20 nodes and found that the performance of DSR is quiet better than both AODV and OLSR, in terms of End-to-end delay and packet delay variation's and seemed to be the most efficient in the simulated environment. Additionally, a comparative investigation on the performance of the three routing protocols DSDV, DSR and AODV is done by (Jakhar & Speed, 2013). The paper includes speed and mobility into account which is a prime contribution and studied the effects of changing node mobility rate, scalability and maximum speed on the performance of DSDV, DSR and AODV. The simulations result indicates that reactive routing protocols DSR and AODV perform better than proactive routing protocol DSDV. However, the paper strictly adheres to the performance of the routing protocols with a fixed number of nodes without taking into consideration of security attacks.

3.0 Research Questions

The project seeks to investigate the performance of three routing protocols in Wireless Ad-Hoc networks under the security attacks and to address the gaps identified in evaluating these protocols. In order to achieve this, the following questions need to be addressed and answered:

Q1: What are the consequences of each of these attacks on wireless Ad-Hoc networks? The performance impact of routing protocols in Ad-Hoc networks under normal operation as well as under the attacks will also be measured.

Q2: Which of the protocols are more exposed to the attacks in Wireless Ad-Hoc networks? Investigations would be conducted by comparing the results from both types of protocols under the attack

and to analyze the routing protocols that are affected by the attacks.

Q2: Which of the proposed plans can be used to help in curbing the effect of attack in the performance of routing protocols in Ad-Hoc networks? Theoretically, the proposed plans will be analyzed and on the basis of the analysis, suggestions will be made on which plans are likely to be used in mitigating the attacks.

4.0 Methodology

The conduct of this research was to simulate the performance of routing protocols in wireless Ad-Hoc network. Conveniently, computer simulation software Network Simulation version 2 (NS-2) was employed. The various described modules based on the implementation and experiment in a network simulation environment were designed and programmed using C++ and were implemented to work with existing NS-2.34 modules simulation environment (Marti et al. 2000). The NS-2 was considered as simulation tool as it has the capability to simulate many features such as: traffic source behavior constant bitrate (CBR); Transport Control Protocol (TCP); routing packet flow; network topology; multicasting and mobile nodes (Meeneghan & Delaney 2004). In this research, the three routing protocols DSDV, DSR and AODV were implemented in NS-2 simulation environment using CBR on two 2 scenario files (scen and scen1).

The simulation with the routing protocols were run to create the performance of these routing and to compare its performance without the security attacks. The next step was to run these routing protocols in malicious environments using the four attacks scenarios (black hole, grey hole, selfish node and DoS attacks) and were compared with their performance in previous step in order to expose the weaknesses of these routing protocols caused by attacks. Based on performance analysis, results of these routing protocols was then used to propose a solution to improve the performance of routing protocols. In this work, the NS 2.35 was installed and Ubuntu 14.04 was used as the operating system. Simulations were carried out with tcl scripts generated to simulate various networks scenarios which were executed to produce a network animator (nam) and a trace (trc) files. The trace file contains the information of the entire simulation details like different time slots, communication between the different nodes, packet size and name, source and destination address details and various other details of the environment (Tomar et al., 2012).

4.1 Experimental Environment

To setup and run NS-2 simulation network, an OTcl script was generated in the network topology using the network objects. The tcl file generated for each of the scenario files to produce the desire trace and nam files for the simulation when the tcl file of each of the routing protocol is created. The network object tcl file can be made by running a new file from the object library and plumb the data through the trace files (Meeneghan & Delaney, 2004).

Basic simulation and network configuration in NS-2 takes place in the tcl script, the network to NS-2 using the tcl script was run and the output files were generated. This experiment was analyzed using the awk programming language in order to analyze the Average Throughput, Packet delivery ratio and End-to-end delay. The network main feature was then illustrated as a chart in Microsoft Excel.

4.1.2 Implementation and Simulation Platforms

The simulation tools described in NS-2, nam, trace files and awk are some of the tools used to extract data from details of the simulation and result analysis of this experiment. The performance of three routing protocols in Ad-Hoc wireless networks (DSDV, DSR and AODV) were investigated using the averages throughput, packet delivery ratio's and

End-to-end delay with various scenarios of mobile node and size of the network. The simulation began by preparing the framework used to simulate the networks by changing the settings and the number of nodes and the number of data flows in different types of network simulation scenario. Awk script was used to analyze the trace file as stated before and produce the Average Throughput, Packet delivery ratio and End-to-end delay as the result of the simulation. The simulation was run by implementing codes in DSDV, DSR and AODV

CC class files to accommodate the behavioral pattern of the attacks.
This file is generated by a setdest command, the CRB type of traffic connection is used for connections between the nodes. To enable thorough and reasonable evaluations, the routing protocols are simulated with different scenario files which are pre-generated with changing movement patterns and traffic and mobile node. The graphs are analyzed and rational conclusions are drawn to investigate the performance of the three protocols in the absence and presence of the security attacks in an Ad-Hoc network.

4.2: Performance Matrix

This research evaluated the performance comparison of average throughput, packet delivery ratio and end-to-end delay of the three protocols DSDV, DSR and AODV to study the effects on the whole network. Throughput determines the stability of the network in different traffic conditions, packet delivery ratio accounts to the percentage of packets delivered when the network is subjected to different traffic conditions and end-to-end delay is considered to be the estimated time it takes for a data packet to reach the destination node.

4.2.1: Throughput

It is the fraction used for transmission of data packets and correctly delivered to the destination nodes. Throughput is also defined as the total number of packets received by the destination (Al-maashri 2006). It is in fact a measure of the effectiveness of a routing protocol measured in bits/second and can be determined by dividing the total number of delivered data packets by the total duration of simulation time. It is also computed as:

$$\text{Throughput} = \frac{\text{Data size x Received}}{\text{Bandwidth x SimTime}}$$

Where Data size is the size of the data packets, Received is the number of data packets correctly received by the destination nodes, Bandwidth is the nominal channel bandwidth and SimTime is the total simulation time (Bertocchi et al., 2003).

4.2.2 Packet Delivery Ratio

The total number of data packets received divided by the packets sent. It expresses the fraction of the data packet delivered from source node to destination when the network is subjected to different traffic conditions (Al-maashri 2006). It also provides the information about the number of packets dropped or forwarded by the routing protocol. The packet delivery ratio can be expressed in equation below:

Packet Delivery Ratio's

$$= \frac{\text{Total Data packets received}}{\text{Total Data packets sent}}$$

4.2.3 End-to-End Delay

The end-to-end delay is the transmission require for a data packet to be transmitted on a network from source to destination nodes. This parameter only indicates the rough estimated time it takes for a data packet to be sent over the network (Adam et al. 2011). End-to-end delay does not give network stability because the substitute routes may have longer or shorter delays before it becomes perfectly stable.

4.3 Traffic Scenario Performance

NS-2 supports two different types of traffic scenario performance for wireless ad-hoc networks; Constant Bit Rate (CBR) and Transmission Control protocol (TCP). In this research, CBR was used as the traffic pattern for the simulation. To create CBR connections the user should run: type –nn –seed –mc –rate > cbrfile name. Where type cbr traffic is set in accordance with the desire node for the simulation. The start times for the CBR connections are randomly chosen with a maximum time value set to 450 secs.

5.0 Simulation Results

The NS 2.35 was selected to carry out the simulations. The simulations were run and the performance of the three routing protocols DSDV, DSR and AODV in the absence of the security attacks and with the presence of the four security attacks (i.e black hole, grey hole, selfish node and DoS attacks). Various comparison were made regarding the network parameters: average throughput, packet delivery ratio and end-to-end delay. The simulation in this research was

DOI: 10.18535/ijecs/v6i10.09

basically divided into three phases. In the first phase, the performance analysis of DSDV, DSR, and AODV was performed by increasing network nodes in the absence of any attack, then the second phase; by incerasing the network nodes in the presence of attacks and by comparing the routing protocols without and with attacks in the third phase. While increasing the network nodes and mobility for accuracy and validation, the results were simulated and expected results were seen.

5.1 Performance analysis of routing protocols without security attacks

The research findings are such that Figure 1 below, shows the average throughput of the ad-hoc routing protocols under varying network nodes. It was observed that AODV performs best compared to the other protocols with a peak throughput of 247.07 kbps. Furthermore, DSR performed credibly good at the low network load but could not sustain the performance at higher network nodes. However, the DSDV significantly had lower performance as a result of frequent link changes and connection failures which led to heavy overload and congestion problems as the DSDV required extra time to set up routing tables before delivering packets.

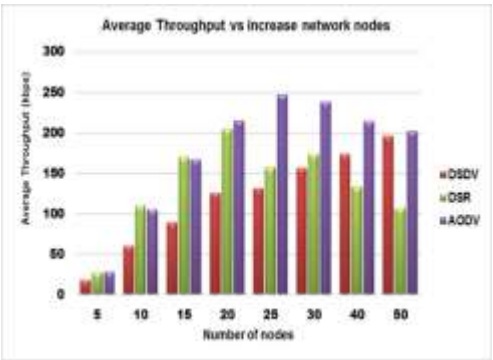

Figure 1: Throughput plot by increase network nodes

From the results presented in Figure 2, the average end-to-end delay of all 3 routing protocols with increased network node is shown. It was observed that reactive routing protocols (DSR and AODV) had higher end-to-end delay than DSDV proactive routing protocols. AODV again outperforms DSR when the network node density increases, and in this scenario, DSR appears to have suffered more and thus has more end-to-end delay than other routing protocols. DSDV being proactive in nature, was observed to have less end-to-end delay than both the DSR and AODV on average. Furthermore, when comparing the two reactive routing protocols, AODV performs better than DSR. The reason for this could be that DSR internally sets a large value for route delete timeout or the routes learnt to neighbouring nodes through path accumulation became quickly obsolete. This may be because routes took left or right turns and moved away from sending node as the routes were moving constantly, DSR had to initiate path discovery multiple times.

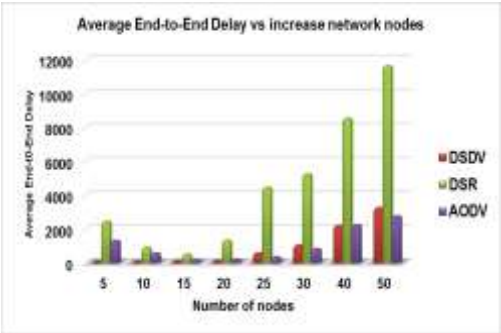

Figure 2 End-to-end delay plot by increase in number of nodes

5.2 Performance analysis of routing protocols under security Attacks

The following are the simulation results that show the effects of an increase in the presence black hole, grey hole, totally and periodically selfish nodes in routing protocols of the Ad-Hoc wireless networks. The number of black hole, grey hole, totally and periodically selfish nodes is presented by 20 percentage from each of the number of network nodes. The remaining were assumed to be well behaved nodes.

5.2.1 Result Analysis of Average Throughput

Figure 3, below shows the results obtained from licentious average throughput activities of black hole nodes in the DSDV, DSR and AODV. The throughput of all the three protocols declines when the network nodes decrease at low number of network nodes and then gradually increases. At high increase network node, the impact of black hole nodes in DSDV throughput is not very strong with a quite constant increase value. On the other hand, the average throughput of DSR and AODV drops quickly with DSR performing better than AODV.

DOI: 10.18535/ijecs/v6i10.09

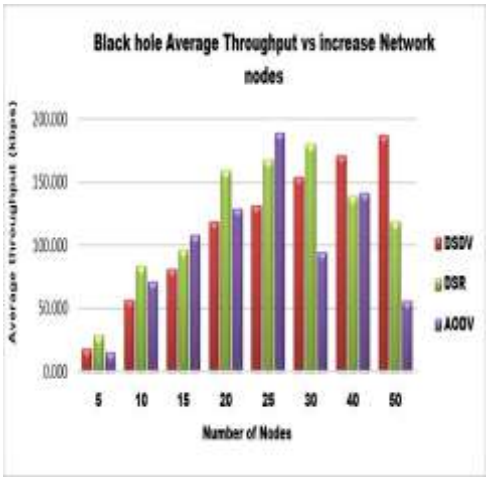

Figure 3: Average Throughput for routing protocols networks experiencing black hole nodes.

From the result observed in Figure 4, present the result obtained from licentious average throughput activities of grey hole nodes in the DSDV, DSR and AODV. The throughput of all the three protocols decreases as the network node be at low number of network nodes and gradually increase. At high increase network node, the impact of grey hole nodes in DSDV average throughput is not very strong with a quite constant increase value. On the other hand, the average throughput of DSR and AODV drops quickly, with AODV suffer much drop at 50 nodes compare to DSR.

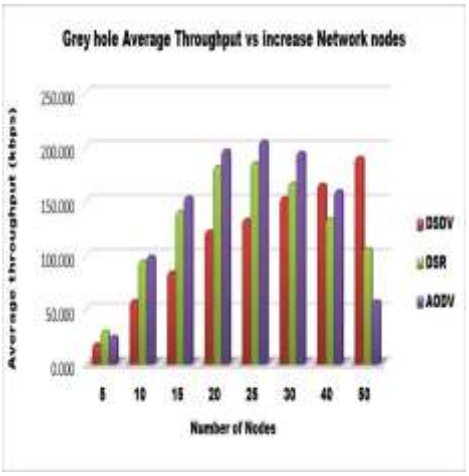

Figure 4: Average Throughput for routing protocols networks experiencing grey hole nodes.

5.2.3 Result Analysis of End-to-End Delay

Figure 5, shows End-to-End delay of DSDV, DSR and AODV with black hole nodes and increasing network nodes. The impacts of black hole nodes on End-to-End delay for three routing protocols under 5 nodes and from 30 to 50 nodes network are high. What is observed is that DSR has a higher End-to-End delay among the three protocols and AODV and DSDV the lowest with black hole nodes. This is as a result that DSR needs time to find a route on demand of the source, or when the link breakage occurs. Whereas DSDV is a proactive routing protocol it therefore finds route sporadically, thereby a route is always available and ready when a packet is required to be sent, reducing the end-to- end delay.

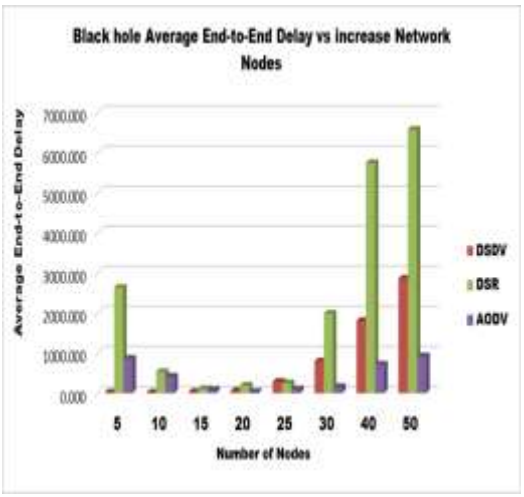

Figure 5: End-to-End for routing protocols networks experiencing black hole nodes.

5.3 Comparison of Routing Protocols with and without Security Attack

The security in Wireless Ad-Hoc networks is always the major constraint due to lack of centralized administration. The misbehaving nodes which occur due the present of the attack in the network, consumes data packets and degrades routing performance in Wireless Ad-Hoc network. This research simulates the scenario of attack, security and normal routing in Ad-Hoc networks and analysis its effects. In this study, the routing protocols DSDV, DSR and AODV using three network metric parameters of Average throughput and end-to-end ratio would be use to compare the results.

5.3.1 Result Analysis of DSDV without and with Impact of Attack on Average Throughput:

DOI: 10.18535/ijecs/v6i10.09

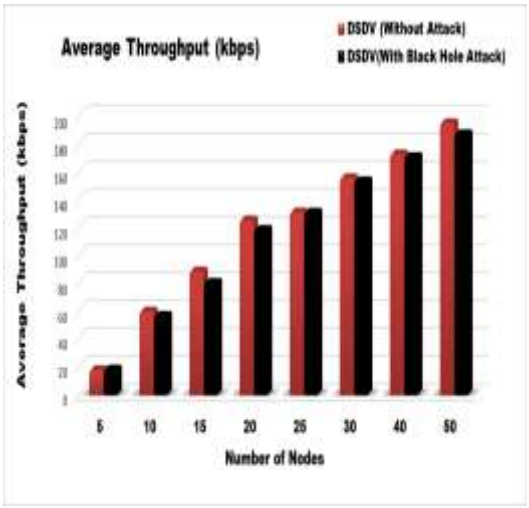

Figure 6: Comparison of DSDV without & with black hole nodes on average throughput.

5.3.2 Result Analysis of DSR without and with Impact of Attack on Average Throughput

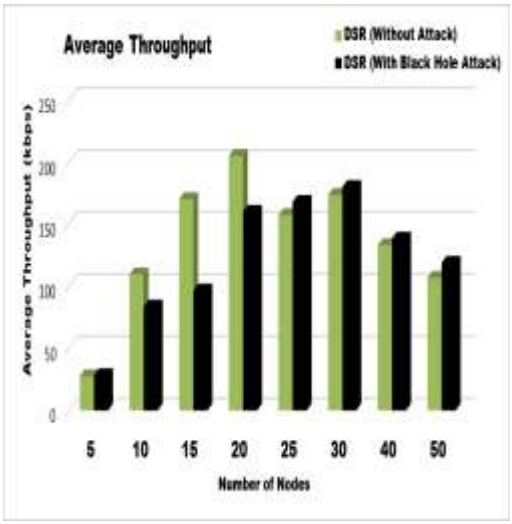

Figure 7: Comparison of DSR without & with black hole nodes attack on average throughput.

5.3.3 Result Analysis of AODV without and with Impact of Attack on Average Throughput

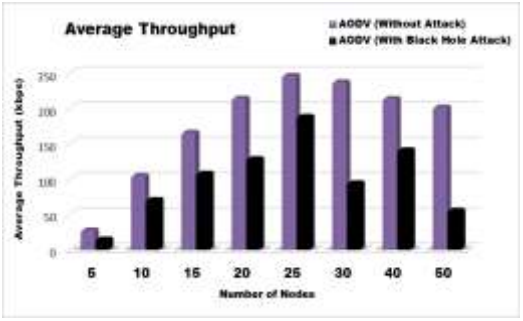

Figure 8. Comparison of AODV without & with black hole nodes attack on average throughput.

5.3.4 Result Analysis of DSDV

Without and with Impact of Attack on End-to-End Delay

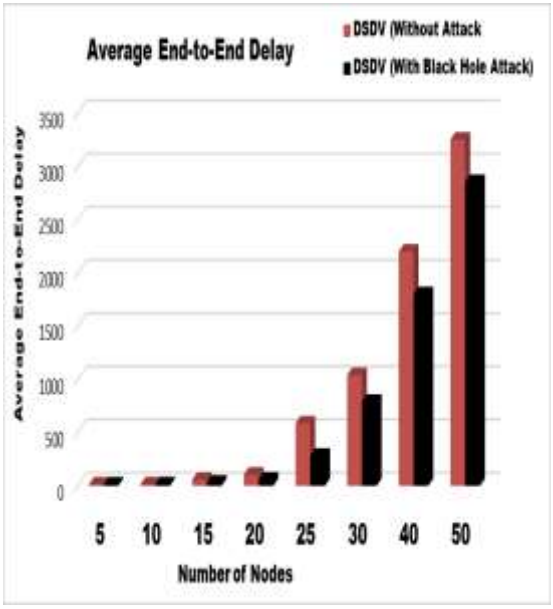

Figure 9: Comparison of DSDV without & with black hole nodes attack on end-to-end delay

5.3.5 Result Analysis of DSR without and with Impact of Attack on End-to-End Ratio Delay.

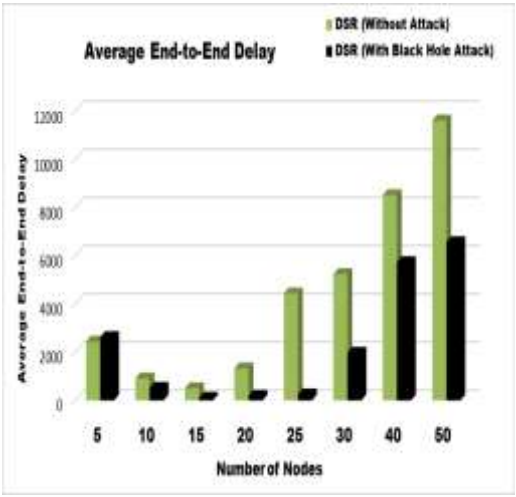

Figure 10: Comparison of DSR without & with black hole nodes attack on end-to-end delay.

5.3.6 Result Analysis of AODV without and with Impact of Attack on End-to-End Delay.

DOI: 10.18535/ijecs/v6i10.09

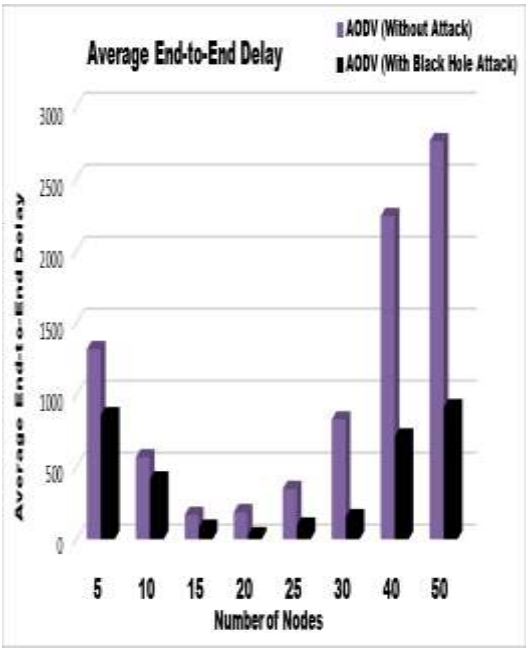

Figure 11. Comparison of AODV without & with black hole nodes attack on end-to-end delay.

6.0 Conclusion

This research provided a detailed investigation of the performance of three routing protocols DSDV, DSR and AODV without and with security attacks such as black hole. It is obvious from this research that no any protocol in Ad-Hoc network is exempted for security attacks and therefore, the needs to provide measure such monitoring the misbehaving node in the network in order to curb the menace of security attacks for all Wireless Ad-Hoc routing is necessary for optimal performance. Although must of the routing protocols under certain attacks lives up to their protocol standard as their still protocols performs well in a highly dense network even under attacks conditions.

When considering the impact of black hole attack on DSDV, DSR and AODV routing to the networks average throughput it is observed that the throughput is high with increase in number of nodes but the trend of throughput with black hole attack and without black hole attack remains the same with little slight increased. As a result of the immediate reply from the malicious node of the black hole as the nature of malicious node here is it would not check its routing table. The results of the analyses of the three protocols indicate that there is need for improvement performance and securing the routing protocols. The observations from simulation results have discovered that reactive protocols perform even with the security attacks, but still requires security measure to coattail the effect of the security predicament for better performance. The protocols discussed do not address security issues; it would be interesting to observe the effects of security additions to the performance of these protocols. The simulation can be extended to any future routing protocols to facilitate comparison of the protocol to the existing ones investigated in this research.

6.1: Future Work

In future research plan would be made to accommodate the hybrid routing protocols in the comparison to extend the simulations for more challenging scenarios. Also, increase the number of scenarios, simulation time and network topology including the number of network node from maximum of 50 nodes to a large number to present a more complex network Ad-Hoc networks. Also, the monitoring would be extended with other attacks (black hole and selfish nodes attacks to mitigate the malicious node behaviour.

References

1. Abu-thuraia, H.M.M., 2010. Secure Zone Routing Protocol in Ad-Hoc etworks.
2. Adam, G., Bouras, C. & Tavoularis, N., 2011. Performance Evaluation of Routing
3. Protocols for multimedia transmission over Mobile Ad hoc Networks.
4. Al-maashri, A., 2006. Performance Analysis of MANET Routing Protocols in the Presence of Self-Similar Traffic. , pp.801–807.
5. Amjad, K., 2012. The Performance of MANET Routing Protocols with Different Mobility and Propagation Models. , (October).
6. Arya, V., 2013. A S URVEY O F E NHANCED R OUTING P ROTOCOLS F OR M ANETs. *IEEE Communications Magazine*, 3, pp.1–9.
7. Azzedine Boukerche, 2001. A Performance Comparison of Routing Protocols for Ad Hoc Networks. , 00(C), pp.1033–1037.
8. Bader, A., Mardini, W. & Baniyasein, M., 2011. A New Protocol for Detecting Black Hole Nodes in Ad Hoc Networks. , 3(1), pp.36–47.

9. Bertocchi, F. et al., 2003. Performance Comparison of Routing Protocols for Ad Hoc Networks. , pp.1033–1037.
10. Broch, J. et al., 1998. A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols. *4th annual ACM/IEEE international conference on Mobile computing and networking*, pp.85–97.
11. Chiejina, E., Xiao, H. & Christianson, B., 2015. A Dynamic Reputation Management System for Mobile Ad Hoc Networks. *Computers*, 4(2), pp.87–112. Available at: http://www.mdpi.com/2073-431X/4/2/87\nhttp://www.mdpi.com/2073-431X/4/2/87/.
12. Deng, H., Li, W. & Agrawal, D.P., 2002. Routing security in wireless ad hoc networks. *IEEE Communications Magazine*, 40(10), pp.70–75.
13. Djenouri, D., Khelladi, L. & Badache, N., 2005. A survey of security issues in mobile ad hoc networks. *IEEE communications surveys*, (April 2009), pp.559–572.
14. E. Perkins, C. & Bhagwat, P., 1994. Highly Dynamic (DSDV) for Mobile Computers Routing. *Proceedings of the ACM SIGCOMM94, London, UK*, pp.234–244.
15. Ghaffari, A.L.I., 2006. Vulnerability and Security of Mobile Ad hoc Networks. , pp.124–129.
16. Haas, Z.J., 1999. Securing ad hoc networks. *IEEE Network*, 13, pp.24–30. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=806983.
17. Hubaux, J., 2003. Equilibrium Analysis of Packet Forwarding Strategies in Wireless Ad Hoc Networks – the Dynamic Case. , pp.1–12.
18. Jakhar, S.K. & Speed, M., 2013. TCP Traffic Based Performance Investigations of DSDV , DSR and AODV Routing Protocols for MANET Using NS2 Parameter.
19. (2), pp.154–158.
20. Kamboj, E. & Rohil, H., 2011. Detection of Black Hole Attack on AODV in MANET Using Fuzzy Logic. , 1(6), pp.316–318.
21. Khemariya, P., Purohit, U.K. & Barahdiya, P.U., 2016. Performance analysis of Improved on demand routing under the black hole attack in MANET. , (03), pp.1899–1903.
22. Kurkowski, S., Camp, T. & Colagrosso, M., 2004. A Visualization and Animation Tool for NS-2 wireless
23. Simulations : iNSpect ∗. , pp.1–16.
24. Liu, P. et al., 2011. Analyzing the TCP Performance on Mobile Ad-Hoc Networks. , pp.143–148.
25. Marti, S. et al., 2000. Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. , pp.255–265.
26. Meeneghan, P. & Delaney, D., 2004. An Introduction to NS , Nam and OTcl scripting.
27. Murthy, S., 1807. An E cient Routing Protocol for Wireless Networks.
28. Nitika Lochab & and Priti Narwal, 2014. Study and Analysis of Routing Protocol in Manet\n. *IOSR Journal of Computer Engineering (IOSR-JCE)*, 16(5), pp.116–120.
29. Papadimitratos, P. & Haas, Z.J., 2002. Secure Routing for Mobile Ad Hoc Networks. *Mobile Computing and Communications Review*, 6(4), pp.79–80. Paper, P. & Topologies, D., 2002. Security within Ad hoc Networks.
30. Rashid Hafeez Khokhar, M.A.N.& S.M., 2015. A Review of Current Routing Attacks in Mobile Ad Hoc Networks. *International Journal of Computer Science and Security*, volume (2)(issue (3)), pp.18–29.
31. Sarmah, N., 2014. Performance Analysis of Mobile Ad-Hoc Routing Protocols by Varying Mobility , Speed and Network Load.
32. Senenkov, G., 2003. Georgiy Senenkov PROTOCOLS COMPARISON IN AD HOC NETWORKS Department of Mathematical Information Technology.
33. Sharma, Y., Sharma, A. & Sengupta, J., 2010. Performance evaluation of Mobile Ad hoc Network routing protocols under various security attacks. *Methods and Models in Computer Science (ICM2CS), 2010 International Conference on*, 42(18), pp.1–6.
34. Stajano, F. & Anderson, R.J., 2000. The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks. *Proceedings of the 7th International Workshop on Security Protocols*, pp.172–194.

35. Tomar, G.S. et al., 2012. Performance comparision of AODV, DSR and DSDV under various network conditions: A survey. *Proceedings - 2011 International Conference on Ubiquitous Computing and Multimedia Applications, UCMA*
a. *2011*, pp.3–7.
36. Tripathi, M., Gaur, M.S. & Laxmi, V., 2013. Comparing the Impact of Black Hole and Gray Hole Attack on LEACH in WSN. *Procedia - Procedia Computer Science*, 19, pp.1101–1107.
37. Ullah, I. & Rehman, S., 2010. Analysis of Black Hole attack on MANETs Using different MANET routing protocols. *School of Computing Blekinge Institute of Technology*, *...*.
38. Velloso, P.B. et al., 2010. Trust Management in Mobile Ad Hoc Networks Using a Scalable Maturity-Based Model. , 7(3), pp.172–185. Wren, M., 2006. H Ealth S Pending and the BLack H Ole. , 2006(6), pp.1–23.
39. Zafar, S., 2016. Throughput and Delay Analysis of AODV , DSDV and DSR Routing Protocols in Mobile Ad Hoc Networks. , 3(2), pp.25–31.
40. Zhao, H., 2003. Security in Ad Hoc Networks. *Security*, pp.756–775.
41. Zolfaghari, M. et al., 2016. Methods for Detection and Removal of Grayhole Attack in Mobile Adhoc Network (MANET). , 5, pp.15–19.