Performance Analysis of AODV MANET under Black Hole Attack

Johnpaul Nwagwu

Simon Fraser University

April 2023

Outline

1 Introduction
- Motivation
- Related Work

2 Overview of Routing Protocols
- AODV Protocol

3 Overview of Attacks on MANETs
- Black Hole Attack

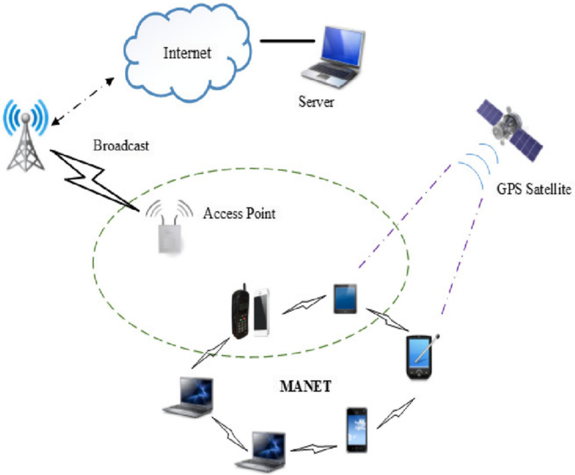
4 Network Simulation Setup
- Simulation Set up
- Simulation Scenario

5 Results and Discussion
- Time Evolution of Delay and Throughput
- Constant Position Mobility Model
- Random Walk 2D Mobility Model

6 Conclusion and Future Work
- Conclusion
- Future Work

7 Bibliography

Introduction



A Mobile Ad Hoc Network [1]

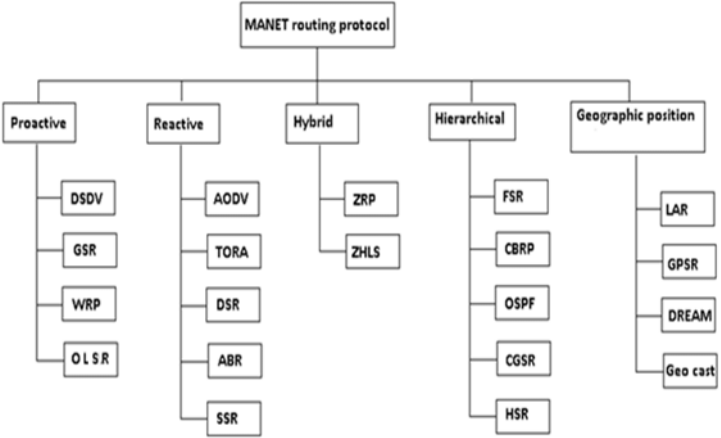
Motivation

- Tactical Networks, PANs, BANs, Wireless Sensor Networks
- Extended Network Connections, Education, Entertainment
- Emergency Services, Smart Cities, FANETs, IMANETs
- Commercial and Civilian Environment, IOT, Mobile Conferencing

Related Work

- Konagala Pavani and Damodaram Avula: used NS-2.29 to simulate the performance of AODV routing protocol in MANETs under black hole attack. Results showed that the throughput of the network is reduced when under black hole attack with increased packet loss and lower packet delivery ratio[2]
- Sakshi Jain and Ajay Khueta: Detecting and Overcoming black hole attack in AODV MANETs using a base node. Results showed an increase in packet delivery ratio with improved throughput but with higher delays[3]
- Latha Tamilselvan and V. Sankaranarayanan: Prevention of black hole attack in MANET. The results showed that their modified ODV protocol performed better than the basic AODV protocol[4]

Overview of Routing Protocols



An Overview of Routing Protocols [5]

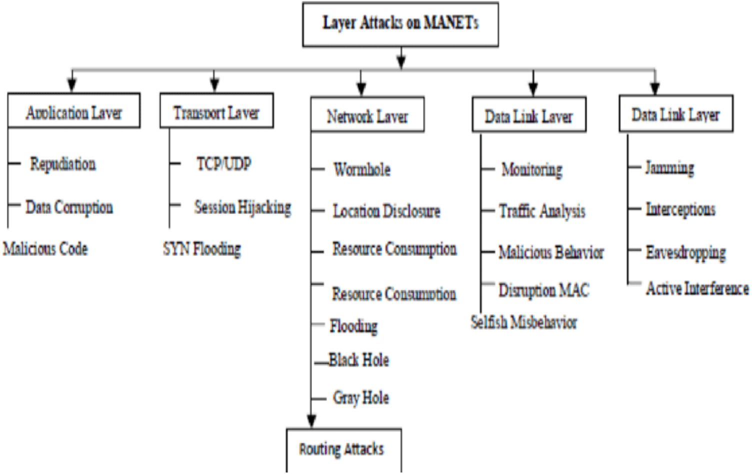
AODV Protocol

Overview: Works on Open Shortest Path First (OSPF) concept and Dijkstra's Algorithm. Uses both concepts for establishing a route or path in MANETs

Key Terminologies

- Route Request Message (RREQ) - broadcast
- Route Reply Message (RREP) - unicast
- Route Error Message (RERR) - broadcast

Attacks on MANETs

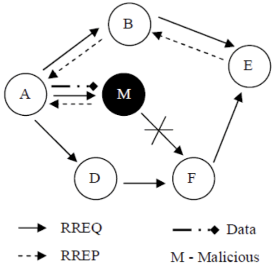


An Overview of Attacks on MANETs [6]

Black Hole Attack

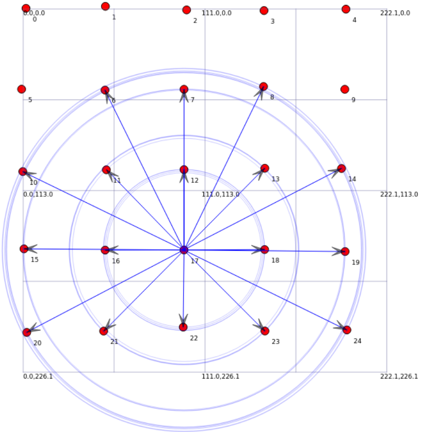
Key idea

- Malicious Node
- Advertises itself as the least cost path
- Drops or sends packets to non-existent IP address



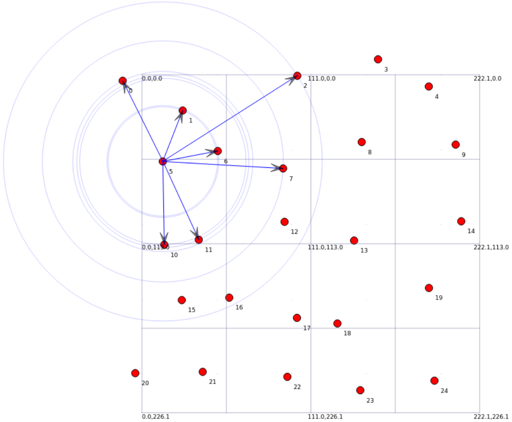
Black Hole Attack Setup[4]

Overall Simulation Set up



NS3.33 NetAnim view of the 25 node MANET

Overall Simulation Set up: Mobile Nodes



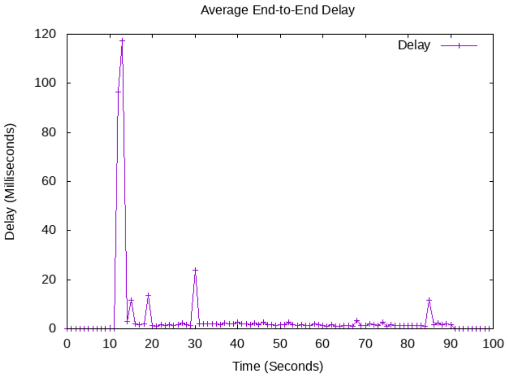
NS3.33 Net Animation view of the 25 node MANET when nodes are mobile

Simulation Scenario: More details in report

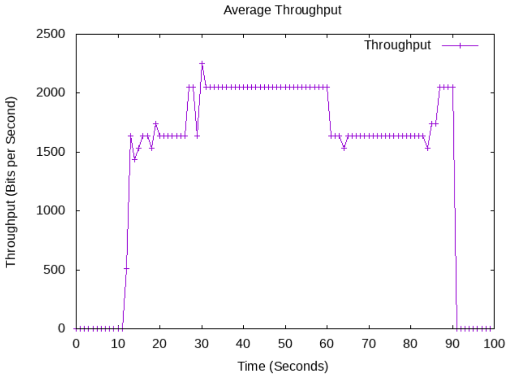
Parameter	Definition
Protocol	AODV
Simulation time	100 s
Traffic Source	Constant Bit Rate
Number of nodes	25,49
Number of Sinks	1,3,5
Mobility Model	Constant, RandomWalk2D
Propagation Model	Constant Speed
Node Speed	20 m/s, 100 m/s
Node Pause time	0 s
Position Allocator	Grid
Propagation Loss Model	Friis

Table: Simulation Parameters

Time Evolution of Delay and Throughput



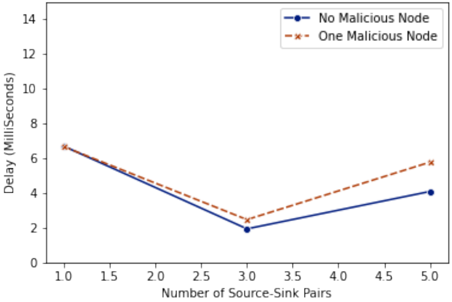
(a)



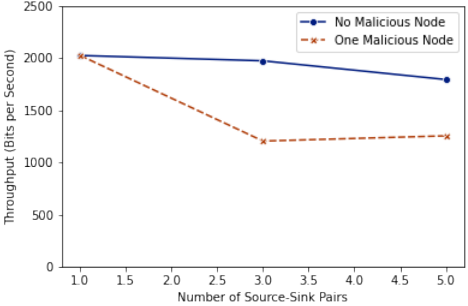
(b)

Figure: Time graph of Average End-to-End Delay (a) and Average Throughput (b) between 5 Source-Sink Pairs with Static Nodes, Normal Density and ConstantPositionMobility

Constant Position Mobility Model: Normal Density



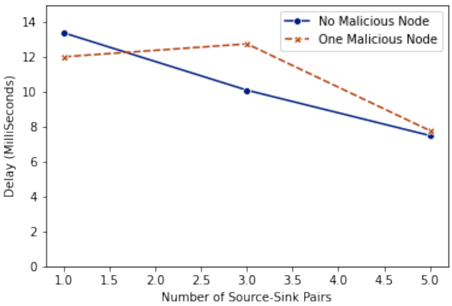
(a)



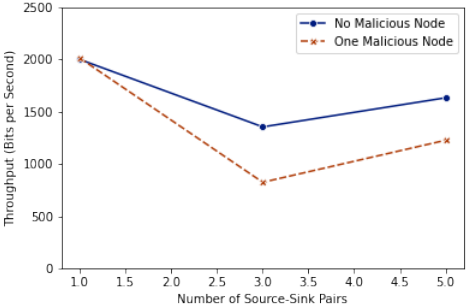
(b)

Figure: Average End-to-End Delay (a) and Average Throughput (b) between One, Three and Five Source-Sink Pairs with Static Nodes, Normal Density and Constant Position Mobility Model

Constant Position Mobility Model: High Density



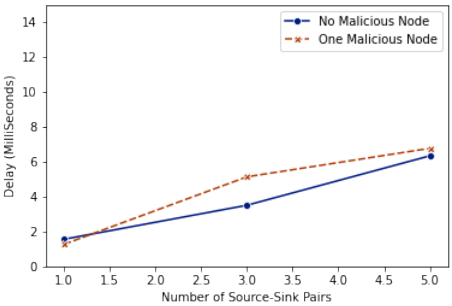
(a)



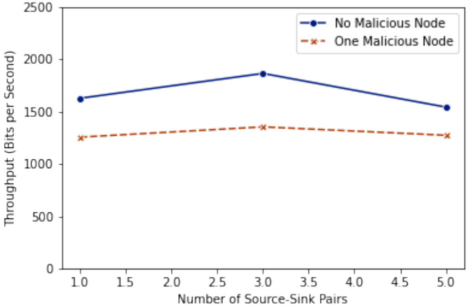
(b)

Figure: Average End-to-End Delay (a) and Average Throughput (b) between One, Three and Five Source-Sink Pairs with Static Nodes, High Density and Constant Position Mobility Model

Random Walk 2D Mobility Model: Normal Speed



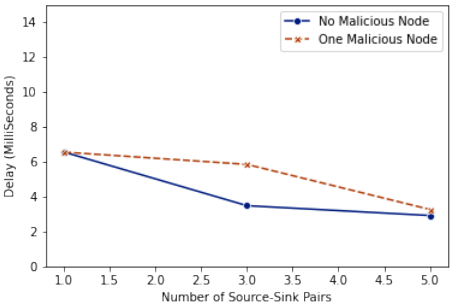
(a)



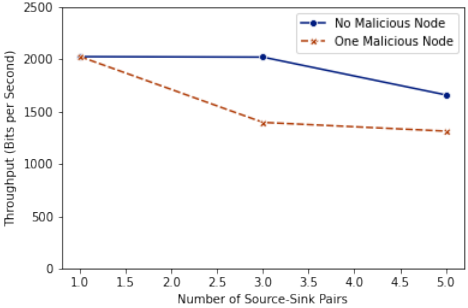
(b)

Figure: Average End-to-End Delay (a) and Average Throughput (b) between One, Three and Five Source-Sink Pairs with Mobile Nodes, Normal Density, Normal Speed and Random Walk 2D Mobility Model

Random Walk 2D Mobility Model: High Speed



(a)



(b)

Figure: Average End-to-End Delay (a) and Average Throughput (b) between One, Three and Five Source-Sink Pairs with Mobile Nodes, Normal Density, High Speed and Random Walk 2D Mobility Model

Conclusion

Conclusion

- A Black hole can reduce Throughput and increase Delay
- Mobility of nodes can reduce the effect of black Hole Attack
- The Mobility model, Density and Speed of nodes can affect Throughput and Delay
- Increasing node density can affect Throughput

Future Work

Future Work

- Compare Black Hole Attack in AODV protocol to OLSR, DSDV
- Test the simulation for other mobility models such as Random Direction 2D Mobility Model
- Consider other performance metrics such as packet delivery ratio, Receive Rate
- Investigate the effect of parameters such as data rate, bit rate, loss model
- Run the simulation for a longer time and compare metrics

Acronyms and Abbreviations

MANET	Mobile Ad Hoc Network
AODV	Ad Hoc on-Demand Distance vector
OLSR	Optimized Link State Routing
PANs	Personal Area Networks
BANs	Body Area Networks
FANETs	Flying Ad hoc Networks
IOT	Internet of Things
IMANETs	Internet Mobile Adhoc Networks
DSDV	Destination Sequenced Distance Vector
GSR	Global State Routing
WRP	Wireless Routing Protocol
TORA	Temporally Ordered Routing Protocol
DSR	Dynamic Source Routing
ZRP	Zone Routing Protocol

Thank You!

References

[1] S. Senthilkumar, W. Johnson, and K. Subramaniyan, "A distributed framework for detecting selfish nodes in manet using record- and trust-based detection (rtbd) technique," *EURASIP Journal on Wireless Communications and Networking*, vol. 2014, p. 205, Nov. 2014. DOI: 10.1186/1687-1499-2014-205.

[2] K. Pavani and D. Avula, "Performance evaluation of mobile adhoc network under black hole attack," in *International Conference on Software Engineering and Mobile Application Modelling and Development (ICSEMA 2012)*, 2012, pp. 1–6. DOI: 10.1049/ic.2012.0155.

[3] S. Jain and A. Khuteta, "Detecting and overcoming blackhole attack in mobile adhoc network," in *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, 2015, pp. 225–229. DOI: 10.1109/ICGCIoT.2015.7380462.

[4] L. Tamilselvan and V. Sankaranarayanan, "Prevention of blackhole attack in manet," in *The 2nd International Conference on Wireless Broadband and Ultra*

Wideband Communications (AusWireless 2007), 2007, pp. 21–21. DOI: 10.1109/AUSWIRELESS.2007.61.

[5] Priyanshu and A. K. Maurya, "Survey: Comparison estimation of various routing protocols in mobile ad-hoc network," *International Journal of Distributed and Parallel Systems*, vol. 5, Jun. 2014. DOI: 10.5121/ijdps.2014.5309.

[6] M. Ichaba, "Security threats and solutions in mobile ad hoc networks; a review," *Universal Journal of Communications and Network*, vol. 6, pp. 7–17, Jan. 2019. DOI: 10.13189/ujcn.2018.060201.

[7] o. O. K. Diaa Eldein Mustafa Ahmed, "An overview of manets: Applications, characteristics, challenges and recent issues," *International Journal of Engineering and Advanced Technology(IJEAT)*, vol. 6, Apr. 2017.

[8] R. H. Khokhar, M. Ngadi, and S. Mandala, "A review of current routing attacks in mobile ad hoc networks," *International Journal of Computer Science and Security*, vol. 2, Nov. 2008.

[9] g. Pankajini Panda Khitish Ku. and P. Niranjan, "Manet attacks and their countermeasures: A survey," *International Journal of Computer Science and Mobile Computing*, vol. 2, pp. 319–330, Nov. 2013.

[10] O. Sbai and M. Elboukhari, "Simulation of manet's single and multiple blackhole attack with ns-3," in *2018 IEEE 5th International Congress on Information Science and Technology (CiSt)*, 2018, pp. 612–617. DOI: 10.1109/CIST.2018.8596606.

[11] H. Singh, G. Singh, and M. Singh, "Article: Performance evaluation of mobile ad hoc network routing protocols under black hole attack," *International Journal of Computer Applications*, vol. 42, no. 18, pp. 1–6, 2012, Full text available.

[12] C. Jamadagni, "[ns-3] blackhole attack simulation in ns-3,". DOI: https://mohittahiliani.blogspot.com/2014/12/ns-3-blackhole-attack-simulation-in-ns-3.html.