

# Blackhole Attack in Mobile Ad-Hoc Network

Simon Fraser University  
Communication Networks  
ENSC 427

Group 4  
Paul Chen  
SeungJun (John) Lee

# Roadmap

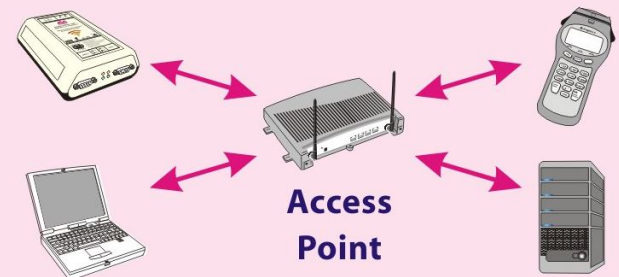
- Introduction
  - *Ad-hoc Network & Blackhole Attack*
- Implementation and Topology
  - *Network Simulator - 2.35*
- Result Analysis
  - *NS-2 Visual Trace Analyzer & Perl Scripts*
- Conclusion
- Things We Have Learned From This Project

# Introduction - MANET

## ● Mobile Ad-hoc Network (MANET)

- > “For This Purpose Only”
- > Self-forming
- > No central controller
- > Dynamic topology
- > Light-weight terminals
- > Anywhere & anytime
  
- > Security threats

### Infrastructure Network



### Ad Hoc Network



# Blackhole Attack

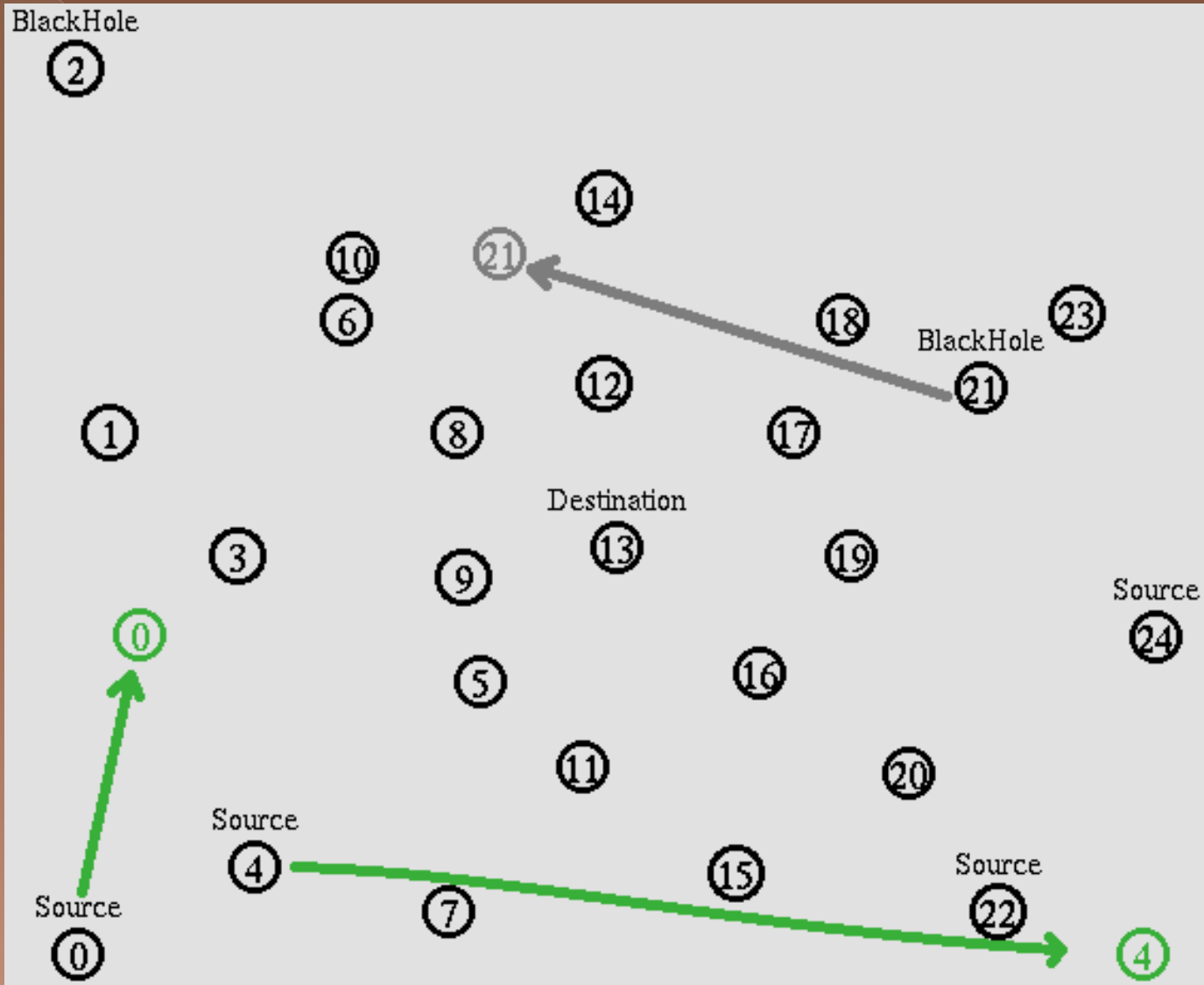
- Blackhole attack (Packet drop attack)
  - > A type of denial-of-service (DDoS) attack
  - > Nodes in MANET are vulnerable
  - > Occurs from a node becoming compromised
  - > Hard to detect and prevent
  - > Can be easily deployed to attack MANET

# Implementation

- Simulation Tools
  - Network Simulator 2.35 (NS-2.35) Mac Version
- Simulation Parameters

<b>Routing Protocol</b>	<b>AODV</b>
<b>Agent</b>	<b>UDP</b>
<b>Application</b>	<b>CBR</b>
<b># of nodes in total</b>	<b>25</b>
<b># of blackhole</b>	<b>2</b>
<b># of source node</b>	<b>4</b>
<b># of destination node</b>	<b>1</b>
<b># of medium node</b>	<b>18</b>

# Topology



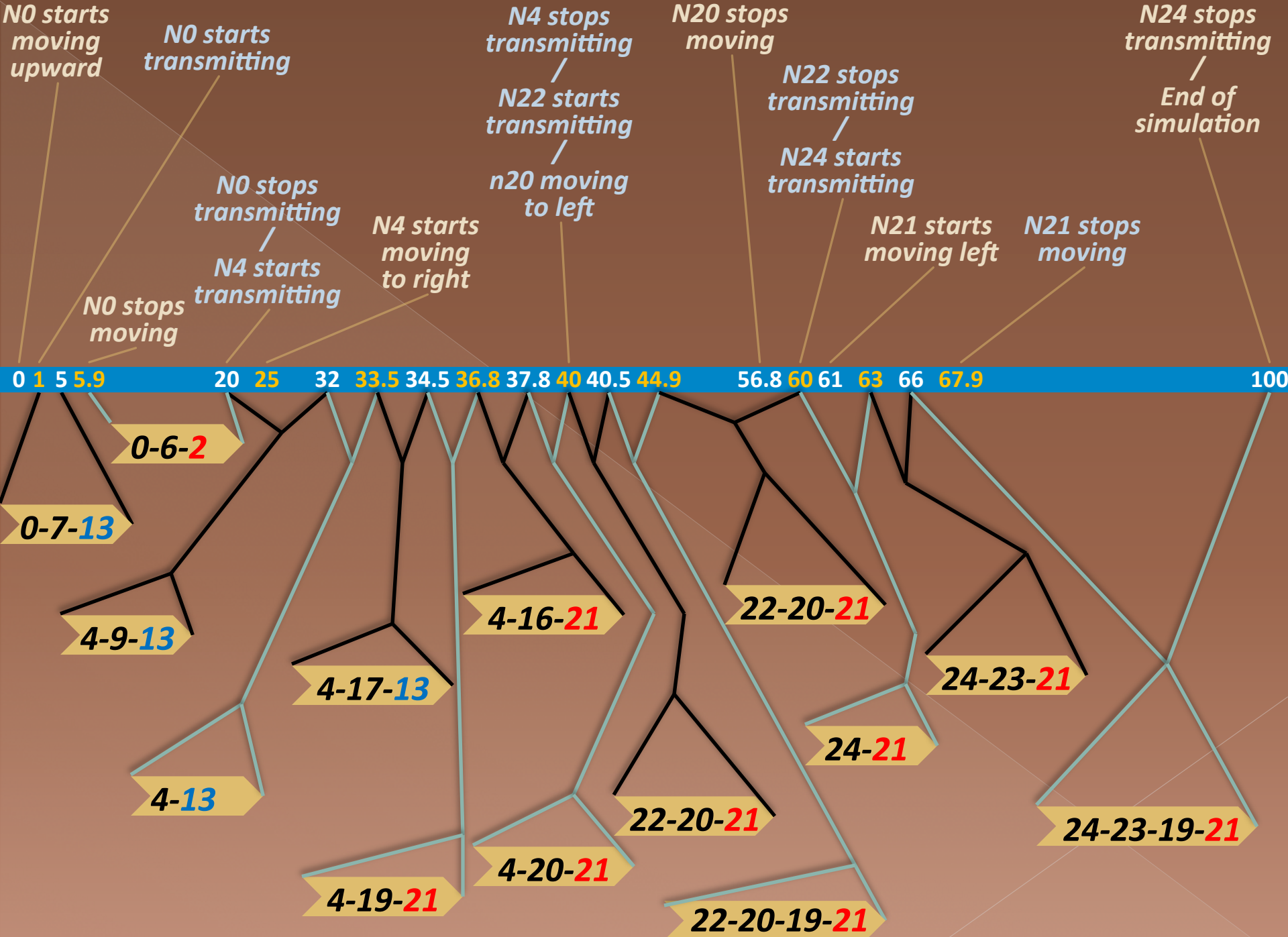
# Simulation Event Table

<b>Time (Second)</b>	<b>Event</b>	<b>Transmission Route</b>
0	N0 moving upward	N/A
1	N0 sending packets	0-7-13
5.90	N0 stops moving	0-6-2
20	N0 stops sending pkt/ N4 starts sending pkt	4-9-13
25	N4 moving right	4-9-13
32	N4 still moving	4-13
33.50	N4 still moving	4-7-13
34.45	N4 still moving	4-19-21
36.80	N4 still moving	4-16-21
37.80	N4 still moving	4-20-21

# Simulation Event Table – Cont.

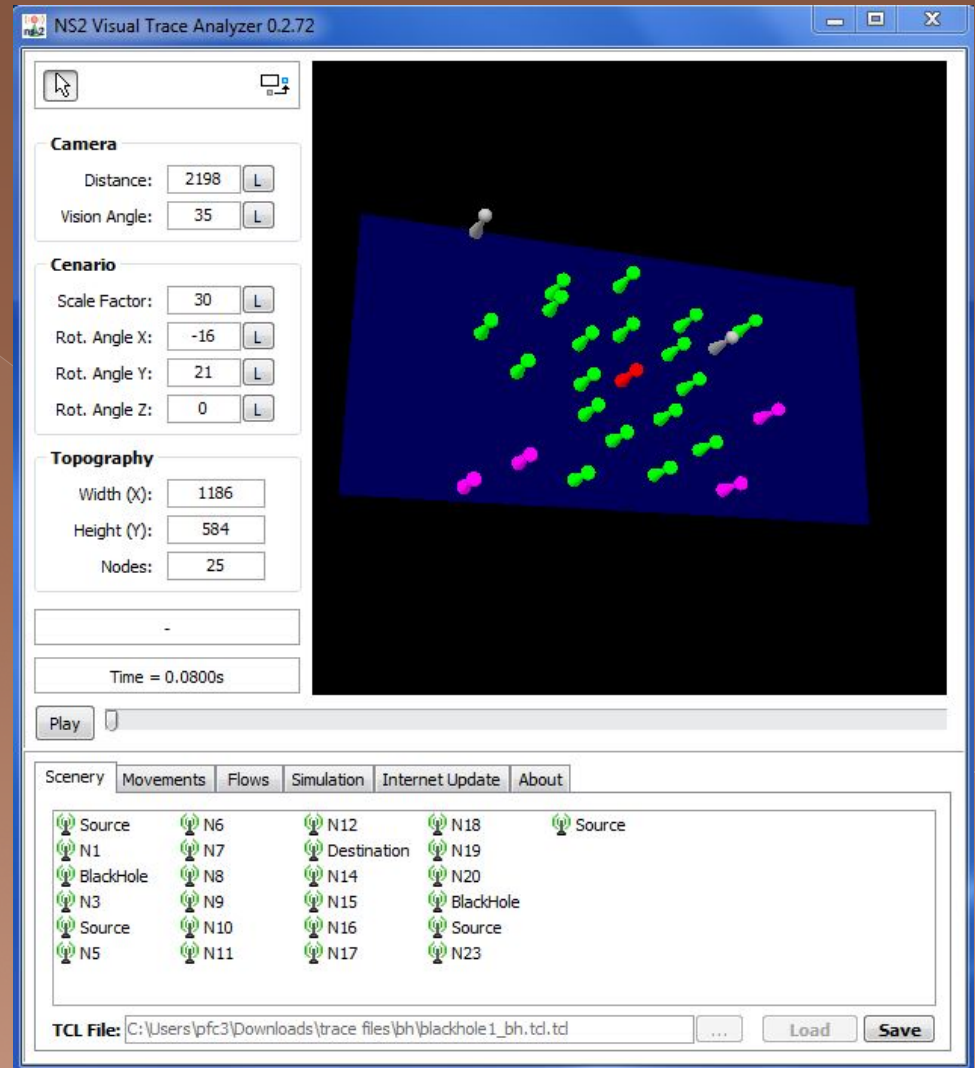
Time (Second)	Event	Transmission Route
40	N4 stops moving/ N4 stops sending pkt/ N22 sending pkt/ N20 moving left	22-20-21
40.5	N20 still moving	22-20-19-21
44.9	N20 still moving	22-16-21
56.80	N20 stops moving	22-16-21
60	N22 stops sending pkt/ N24 starts sending pkt	24-21
61	N21 moving left	24-21
63	N21 still moving	24-23-21
66	N21 still moving	24-23-19-21
67.9	N21 stops moving	24-23-19-21
100	N24 stops sending pkt	N/A





# Result Analysis

- Tool used
  - > NS-2
  - Visual Trace Analyzer
  - 0.2.72
  - > Perl scripts

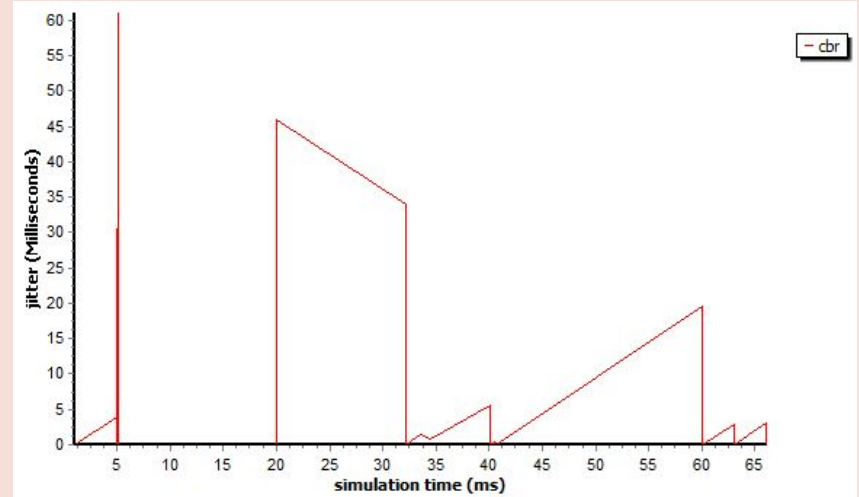
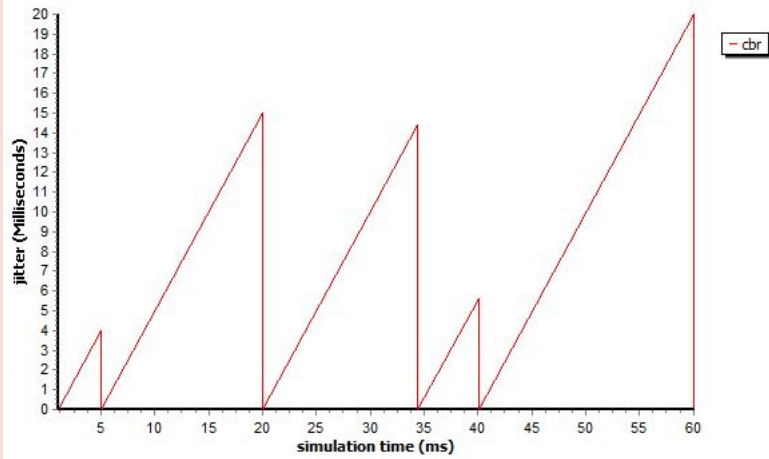


# Result Analysis – Jitter at N2 & N21

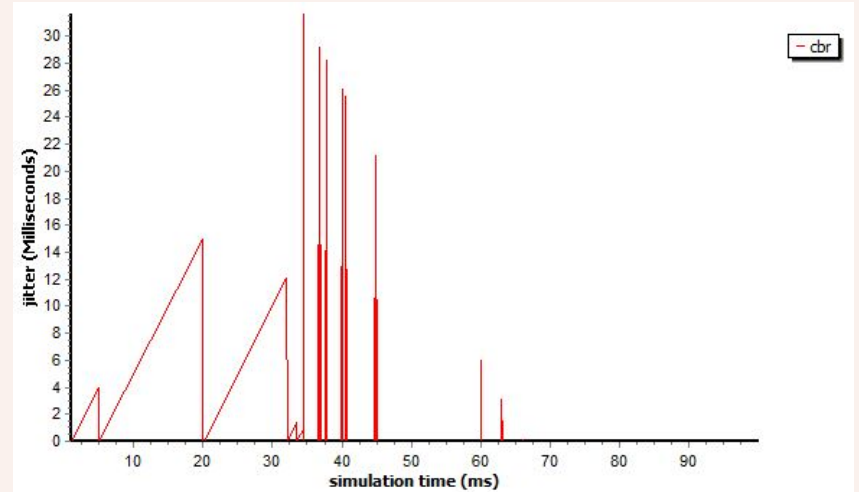
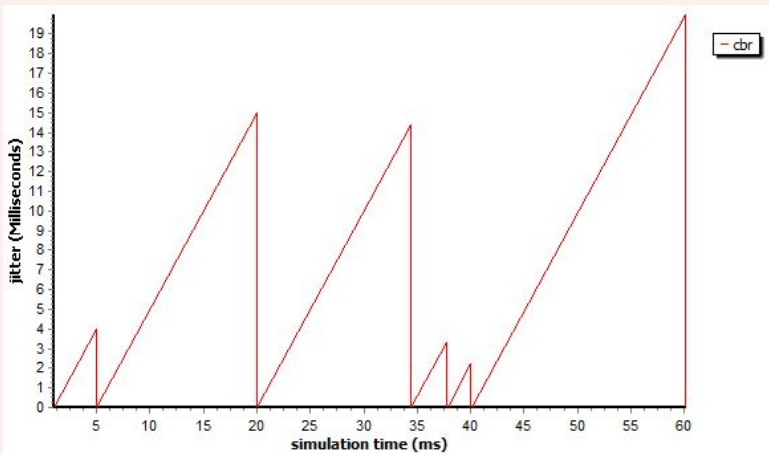
Blackhole disabled

Blackhole enabled

N 2



N 21

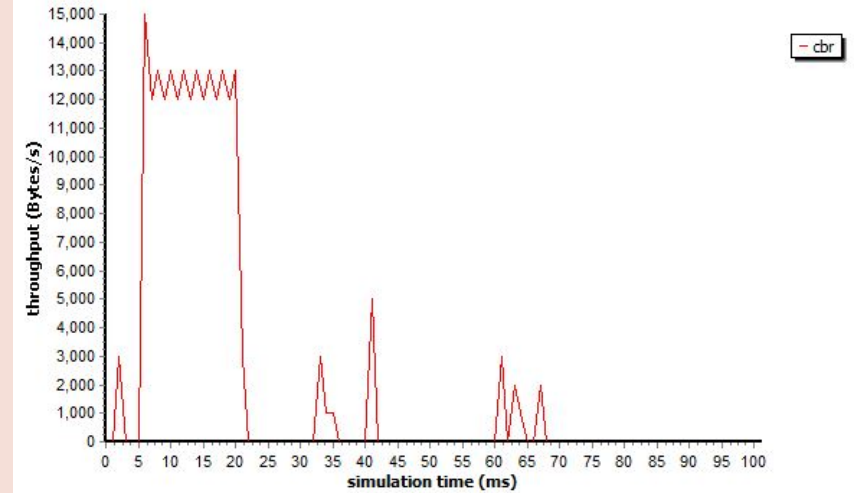
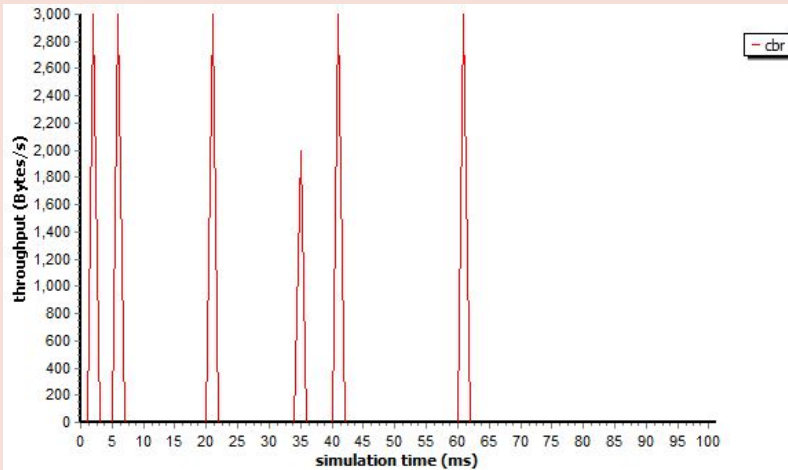


# Result Analysis – Throughput Received at N2 & N21

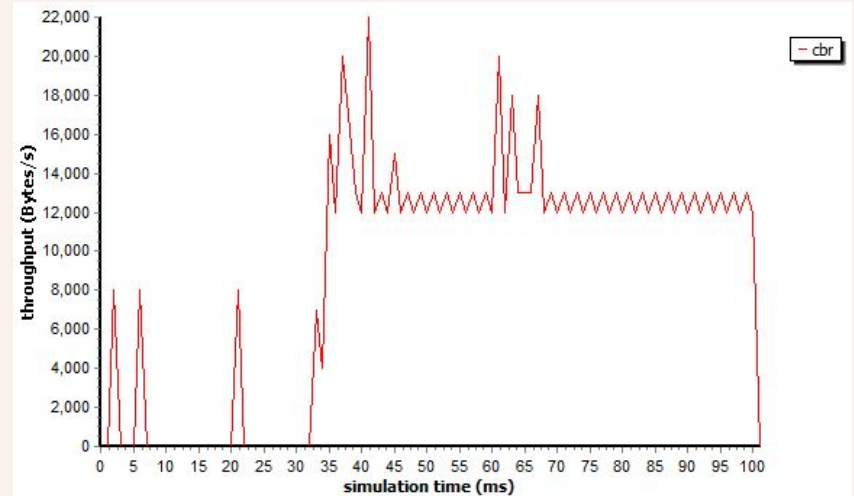
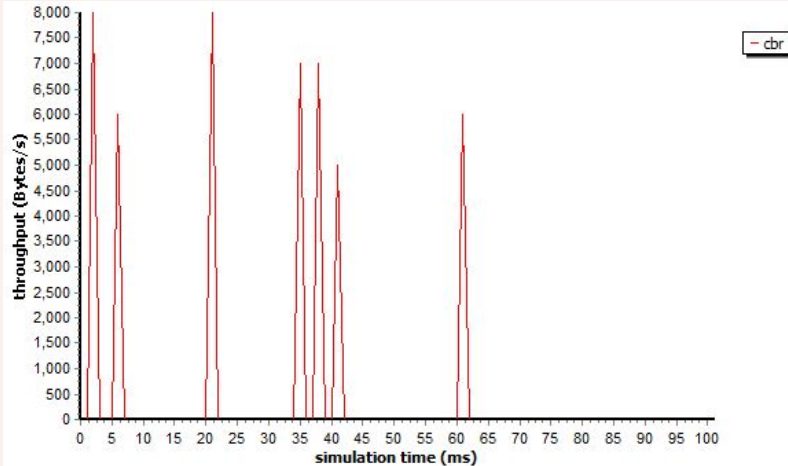
## Blackhole disabled

## Blackhole enabled

N2



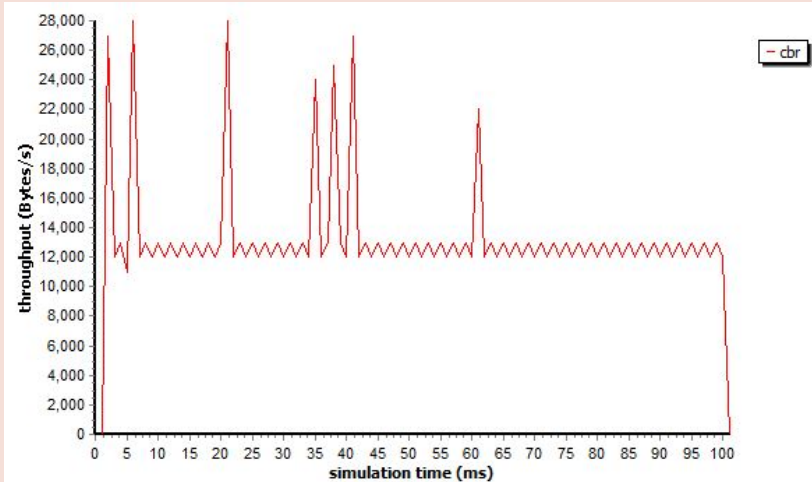
N21



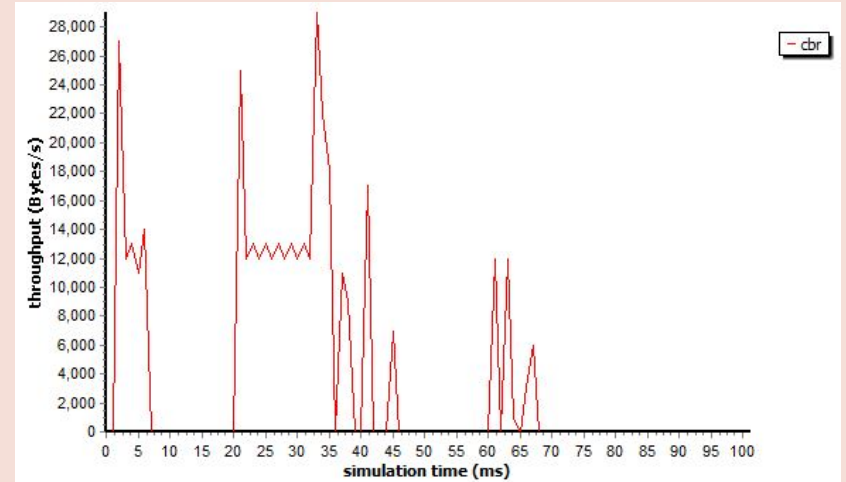
# Result Analysis – Throughput received at dest. node

N13

## Blackhole disabled



## Blackhole enabled



# Result Analysis – Perl Script

Information of the overall simulation model in two scenarios:

	<b>Blackhole disabled</b>	<b>Blackhole enabled</b>
Sent Packets	1241	1241
Received Packets	1237	226
Packets Dropped	4	1015
PDR	99.6777 %	18.2111 %
Average Path Length	2.007276	8.584071

# Conclusion

- Potential of MANET based applications
- Blackholes have significant impact on the MANET
- Black holes are invisible in large topology of the network
- Can only be detected by monitoring the lost traffic

# Things We Have Learned From This Project

## ◎ **SeungJun (John) Lee:**

- › *Concept of Communication Networks*
- › *Understand the Black-Hole attack in network*
- › *Routing Protocol in Mobile Network*

## ◎ **Paul Chen:**

- › *Wireshark, NS related softwares and perl scripts*
- › *Time management is critical and always prepare a backup plan*
- › *Don't be afraid of what might go wrong*
- › *Communication within the group is the key*



# References:

- ◉ [1] A. Leon-Garcia and I. Widjaja, *Communication Networks: Fundamental Concepts and Key Architectures*, 2nd Ed. New York: McGraw-Hill, 2004.
- ◉ [2] Anita, EA Mary, and V. Vasudevan, *Black hole attack prevention in multicast routing protocols for mobile ad hoc networks using certificate chaining*, *International Journal of Computer Applications*, 2010 , no, 1-12, pp 21-28.
- ◉ [3] C.E. Perkins, E.M. Royer, *Ad-hoc on-demand distance vector routing*, *Mobile Computing Systems and Applications*, 1999. Proceedings, WMCSA '99. Second IEEE Workshop on, pp. 90-100, 25-26 Feb 1999.
- ◉ [4] E. H. Teerawat Issariyakul. *Introduction to Network Simulator NS2*. Springer US, Springer.com, 2009.
- ◉ [5] G. I. Papadimitriou, A. S. Pomportsis, P. Nicopolitidis, and M. S. Obaidat *Wireless Networks* pg 291-292, John Wiley and Sons Ltd, December 2002
- ◉ [6] H. Deng, W. Li, Agrawal, D.P., "Routing security in wireless ad hoc networks," Cincinnati Univ., OH, USA; *IEEE Communications Magazine*, Oct. 2002, Volume: 40, page(s): 70- 75, ISSN: 0163-6804.
- ◉ [7] K. Lakshmi, S.Manju Priya, A. Jeevarathinam K.Rama, K.Thilagam, "Modified AODV Protocol against Blackhole Attacks in MANET", *International Journal of Engineering and Technology*.
- ◉ [8] M. Al-Shurman, S. Yoo, and S. Park, *BlackHole Attack in Mobile Ad hoc Networks*, *ACM Southeast Regional Conference*, pp. 96-97, 2004(ACM-Se' 42), Huntsville, Alabama, 2-3 April 2004.
- ◉ [9] M. Greis, *Marc Greis Tutorial for the Network Simulator NS-2*.
- ◉ [10] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J.Dixon and K. Nygard, *Prevention of Cooperative BlackHole Attack in Wireless Ad hoc Networks*. Paper presented at the International Conference on Wireless Networks, Las Vegas, Nevada, USA, 23-26 June 2003.