MIT World Peace University

Wireless Devices and Mobile Security
Third Year B. Tech, Semester 5

Simulation of Routing in Mobile Ad Hoc Networks with Multiple Nodes

---

Lab Assignment 3

Prepared By

Krishnaraj Thadesar
Cyber Security and Forensics
Batch A1, PA 10

November 26, 2023

Contents

1 Aim **1**

2 Objectives **1**

3 Theory **1**
3.1 What are Mobile Ad-hoc Networks? 1
3.2 MANET Applications 2
3.3 Challenges and Issues in MANET 2
3.4 Types of ADHOC Routing Protocols 3
3.5 Routing Protocols in MANET 3

4 Platform **3**

5 Screenshots **3**

6 Code and Algorithm **3**
6.1 Algorithm 3
6.2 Code 4

7 Conclusion **6**

8 FAQ **7**

1 Aim

Write a program to simulate routing in mobile Ad-Hoc network with multiple nodes. You may use NetSim or NS2 or QualNet for this experiment.

2 Objectives

1. Understand about the basics of Mobile Ad-hoc Networks (MANETs) and different routing protocols
2. Setup a network with wireless nodes using ns2
3. Get familiar with the different characteristics of MANET through simulations

3 Theory

3.1 What are Mobile Ad-hoc Networks?

Mobile Ad-hoc Networks (MANETs) are decentralized networks formed by a collection of mobile devices that communicate with each other without relying on a pre-existing infrastructure or centralized administration. In MANETs, nodes act both as data sources and routers, dynamically establishing connections to relay information. This self-configuring and adaptive nature makes MANETs suitable for scenarios where traditional network infrastructure is impractical or unavailable, such as military operations, disaster response, and collaborative sensor networks. The topology of a MANET is dynamic, continually changing as nodes move, join, or leave the network.

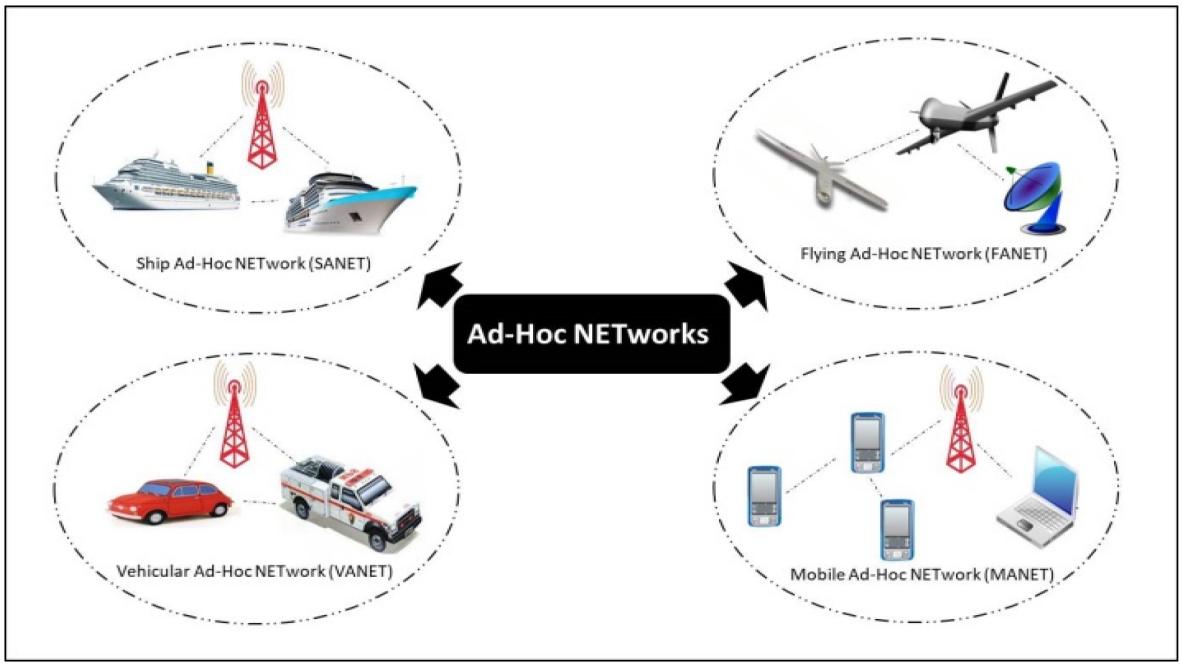

Figure 1: Different Ad Hoc Networks

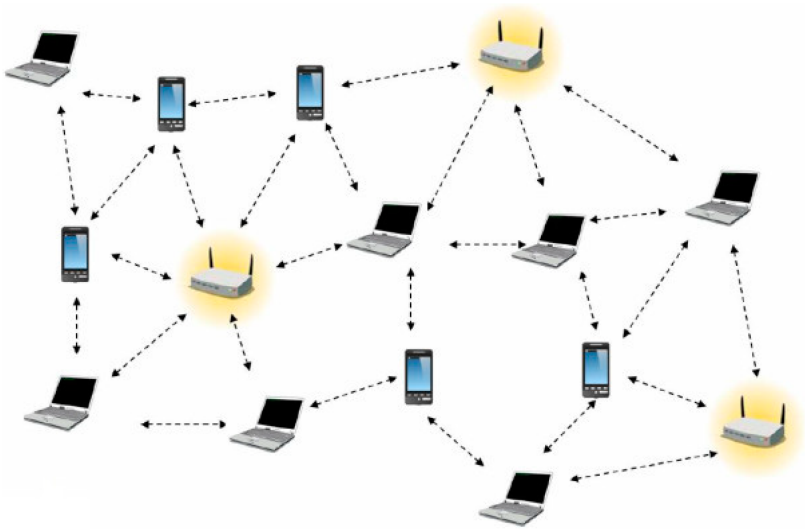

Figure 2: A Wireless Ad Hoc Network

3.2 MANET Applications

MANETs find applications in various domains, including:

- **Military Operations:** MANETs provide an effective means of communication for soldiers and vehicles on the battlefield where a fixed infrastructure is not feasible.
- **Disaster Response:** In disaster-stricken areas with damaged or nonexistent communication infrastructure, MANETs enable rescue teams to establish communication networks on the fly.
- **Sensor Networks:** Collaborative sensor networks leverage MANETs, allowing sensors to dynamically form networks for collecting and transmitting data.
- **Mobile Conferencing:** MANETs support spontaneous and mobile communication in conferences or meetings without the need for predefined infrastructure.

3.3 Challenges and Issues in MANET

MANETs face several challenges and issues, including:

- **Dynamic Topology:** Rapid changes in network topology due to the mobility of nodes make routing complex.
- **Limited Resources:** Devices in MANETs often have constraints on power, processing capabilities, and memory, requiring energy-efficient protocols.
- **Security Concerns:** MANETs are vulnerable to various security threats, such as eavesdropping, unauthorized access, and malicious attacks, due to the absence of a centralized authority.
- **Routing Complexity:** Designing efficient routing protocols is challenging in the absence of a fixed infrastructure, requiring adaptability to dynamic conditions.

3.4 Types of ADHOC Routing Protocols

Various types of ad-hoc routing protocols serve different purposes:

1. **Proactive (Table-Driven) Protocols:** These protocols, like Optimized Link State Routing (OLSR), maintain consistent routing information through periodic updates. Nodes continuously update their routing tables, allowing for quick route selection when needed.
2. **Reactive (On-Demand) Protocols:** Protocols such as Ad Hoc On-Demand Distance Vector (AODV) establish routes only when necessary, reducing routing overhead. Route discovery occurs reactively in response to data transmission requirements.
3. **Hybrid Protocols:** Hybrid protocols combine features of both proactive and reactive protocols, providing adaptability to changing network conditions. They strike a balance between maintaining current routing information and on-demand route discovery.

3.5 Routing Protocols in MANET

Routing protocols in MANETs play a critical role in establishing and maintaining communication paths:

- **AODV (Ad Hoc On-Demand Distance Vector):** A reactive protocol that establishes routes on demand. When a node needs to communicate with another, it initiates a route discovery process, and a route is established as a response.
- **DSR (Dynamic Source Routing):** Another reactive protocol where nodes dynamically discover and maintain routes. Nodes maintain a route cache, and route discovery occurs when a route is not present in the cache.
- **OLSR (Optimized Link State Routing):** A proactive protocol that efficiently maintains a topology table for optimized route selection. Nodes periodically exchange link state information, allowing for quicker route convergence.

These routing protocols address the challenges of MANETs by adapting to the dynamic nature of the network and varying resource constraints.

4 Platform

Operating System: Ubuntu 22.04 x86-64
IDEs or Text Editors Used: Visual Studio Code
Compilers or Interpreters: NS2, NAM 1.4

5 Screenshots

6 Code and Algorithm

6.1 Algorithm

1. Set network parameters such as channel, propagation, network interface, MAC, queue, antenna, etc.

2. Create a new simulator object.
3. Open trace and nam files for network visualization.
4. Load a flat grid topology.
5. Configure nodes in the network with various parameters.
6. Create nodes in the network and set their positions randomly.
7. Schedule nodes to move randomly.
8. Attach agents to nodes in the network.
9. Create a CBR traffic generator and attach it to a UDP agent.
10. Start the CBR traffic generator.
11. Schedule the end of the simulation.
12. Run the simulation.

6.2 Code

```
set val(chan) Channel/WirelessChannel;
set val(prop) Propagation/TwoRayGround;
set val(netif) Phy/WirelessPhy;
set val(mac) Mac/802_11;
set val(ifq) Queue/DropTail/PriQueue;
set val(ll) LL;
set val(ant) Antenna/OmniAntenna;
set val(ifqlen) 50;
set val(rp) AODV;
set val(nn) 11;
set val(x) 500;
set val(y) 400;
set val(stop) 3;

set val(energymodel) EnergyModel;
set val(initialenergy) 1000;

set ns [new Simulator]

set tf [open AODV.tr w]
$ns trace-all $tf

set nf [open AODV.nam w]
$ns namtrace-all-wireless $nf $val(x) $val(y)

set topo [new Topography]
$topo load_flatgrid $val(x) $val(y)

create-god $val(nn)

set chan_1_ [new $val(chan)]

$ns node-config -adhocRouting $val(rp) \
  -llType $val(ll) \
```

```
  -macType $val(mac) \
  -ifqType $val(ifq) \
  -ifqLen $val(ifqlen) \
  -antType $val(ant) \
  -propType $val(prop) \
  -phyType $val(netif) \
  -channel $chan_1_ \
  -topoInstance $topo \
  -agentTrace ON \
  -routerTrace ON \
  -macTrace OFF \
  -movementTrace ON \
  -energyModel $val(energymodel) \
  -initialEnergy $val(initialenergy) \
  -rxPower 0.4 \
  -txPower 1.0 \
  -idlePower 0.6 \
  -sleepPower 0.1 \
  -transitionPower 0.4 \
  -transitionTime 0.1


for {set i 0} {$i < $val(nn)} {incr i} {
  set node_($i) [$ns node]
  $node_($i) set X_ [ expr 10+round(rand()*480) ]
  $node_($i) set Y_ [ expr 10+round(rand()*380) ]
  $node_($i) set Z_ 0.0
}

for {set i 0} {$i < $val(nn)} {incr i} {
  $ns at [ expr 0.2+round(rand()) ] "$node_($i) setdest [ expr 10+round(rand()
    *480) ] [expr 10+round(rand()*380) ] [expr 60+round(rand()*30) ]"
}

#$ns duplex-link $node_(5) $node_(2) 2Mb 10ms DropTail

set udp [new Agent/UDP]
$ns attach-agent $node_(5) $udp
set null [new Agent/Null]
$ns attach-agent $node_(2) $null
set cbr [new Application/Traffic/CBR]
$cbr attach-agent $udp
$cbr set packetSize_ 512
$cbr set interval_ 0.1
$cbr set rate_ 1mb
$cbr set maxpkts_ 10000
$ns connect $udp $null
$ns at 0.4 "$cbr start"

for {set i 0} {$i < $val(nn)} {incr i} {
        $ns initial_node_pos $node_($i) 30
}

for {set i 0} {$i < $val(nn)} {incr i} {
  $ns at $val(stop) "$node_($i) reset";
}

#$ns at $val(stop) "$ns nam-end-wireless $val(stop)"
$ns at $val(stop) "finish"
```

```
$ns at 3.1  "puts \"end simulation\"; $ns halt"

proc finish {} {
        global ns tf nf
        $ns flush-trace
        close $tf
        close $nf
        exec nam AODV.nam &
        exit 0
}

puts "CBR packet size = [$cbr set packetSize_]"
puts "CBR interval = [$cbr set interval_]"

$ns run
```

Listing 1: AODV.tcl

7 Conclusion

Thus, implemented a TCL script to simulate routing in mobile Ad-Hoc network with multiple nodes using NS2.

8 FAQ

1. *What are the main features of routing protocols?*

   Routing protocols in networking possess several key features:

   - **Path Determination:** Routing protocols determine the optimal path for data transmission.
   - **Dynamic Adaptability:** They adapt to changes in network topology and conditions.
   - **Scalability:** Capable of handling networks of varying sizes.
   - **Robustness:** Resilient to network failures and able to recover quickly.
   - **Security:** Incorporate measures to secure routing information and prevent attacks.

2. *Why is routing in an ad hoc network so difficult, and why is this network more vulnerable as compared to conventional networks?*

   Ad hoc networks pose challenges due to their dynamic and self-configuring nature, making routing difficult. They are more vulnerable because:

   - **Dynamic Topology:** Constantly changing network topology requires adaptive routing algorithms.
   - **Limited Resources:** Devices in ad hoc networks often have limited power and processing capabilities.
   - **Open Medium:** Wireless communication is susceptible to eavesdropping and unauthorized access.
   - **Lack of Centralized Authority:** Absence of a centralized control makes it challenging to enforce security policies.

3. *Can ad hoc networks be used by multiple devices, and why?*

   Yes, ad hoc networks can be used by multiple devices. The self-configuring nature of ad hoc networks allows devices to dynamically form connections without relying on a centralized infrastructure. This flexibility makes them suitable for scenarios where multiple devices need to communicate without the need for pre-existing network infrastructure.

4. *What are common Attacks on Routing Protocols? Explain in detail.*

   Common attacks on routing protocols include:

   (a) **Spoofing:** Impersonating a trusted node to inject false routing information.
   (b) **Routing Table Overflow:** Flooding a router's routing table to disrupt normal operations.
   (c) **Denial of Service (DoS):** Overloading the network to make it unavailable to legitimate users.
   (d) **Replay Attacks:** Capturing and retransmitting data to gain unauthorized access.
   (e) **Selective Forwarding:** Malicious nodes selectively forward packets to disrupt communication.

5. *How is Route maintenance carried out in the AODV protocol? Give advantages and disadvantages of AODV.*

   Route maintenance in AODV involves:

   - Periodic HELLO messages to verify the status of neighbor nodes.
   - Route Error (RERR) messages to notify about broken links.
   - Route Requests (RREQ) for new routes when needed.

   Advantages of AODV:

   - **Adaptability:** Adapts well to dynamic network conditions.
   - **Reduced Overhead:** Minimizes routing overhead by using on-demand route establishment.

   Disadvantages of AODV:

   - **Latency:** Introduces latency in route discovery.
   - **Route Rediscovery:** May lead to frequent route rediscovery in dynamic environments.

6. *What is the main vulnerability of routing protocols?*

   The main vulnerability of routing protocols is the susceptibility to various attacks, including:

   - **Spoofing:** Impersonation of trusted nodes.
   - **Eavesdropping:** Unauthorized interception of communication.
   - **Denial of Service (DoS):** Overloading the network to disrupt service.
   - **Routing Information Manipulation:** Altering routing information to misdirect traffic.