Bucknell

A Study of On-Off Attack Models for Wireless Ad Hoc Networks

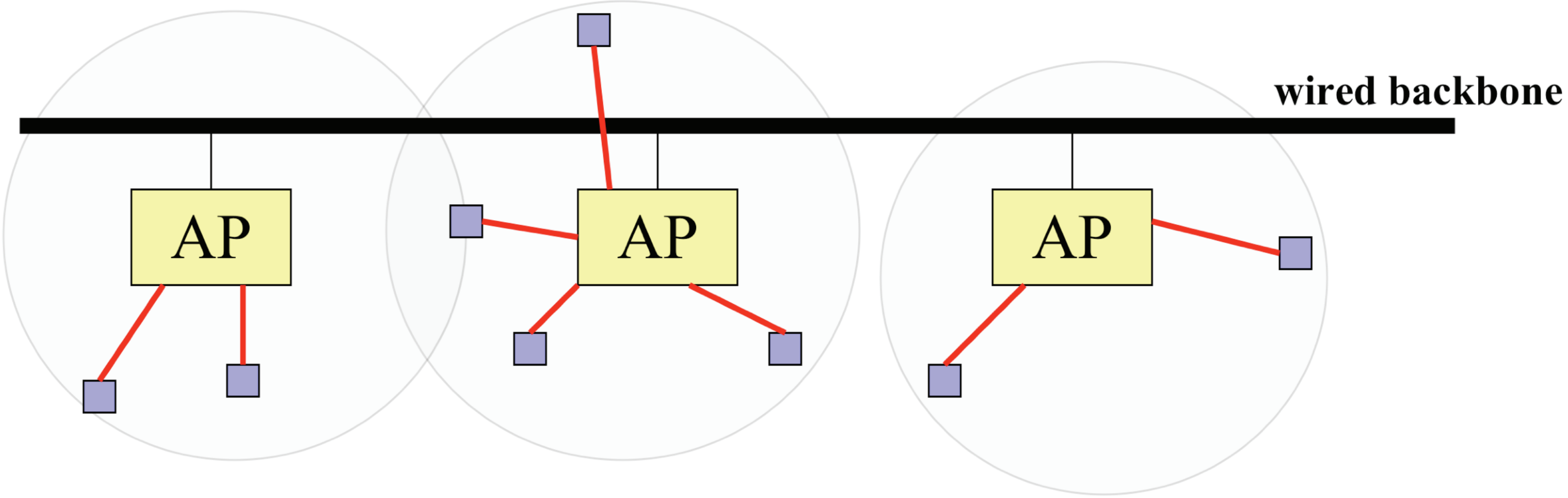
L. Felipe Perrone <perrone@bucknell.edu>

Dept. of Computer Science

Bucknell University, Lewisburg, PA, U.S.A.

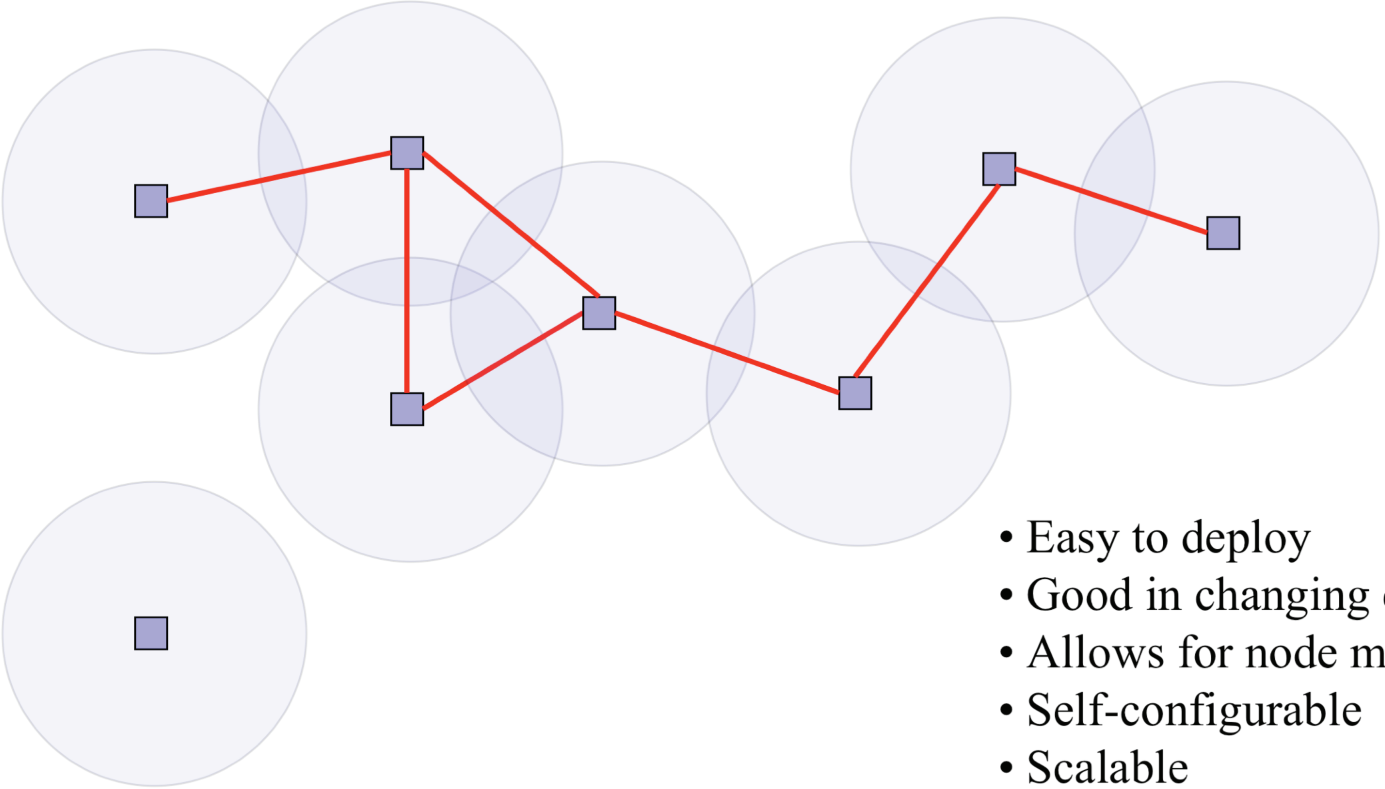
Wireless Networks (1)

Wireless Hot Spot or Fixed Infrastructure (IEEE 802.11 PCF)



Wireless Networks (2)

Wireless Ad Hoc Network (IEEE 802.11 DCF)



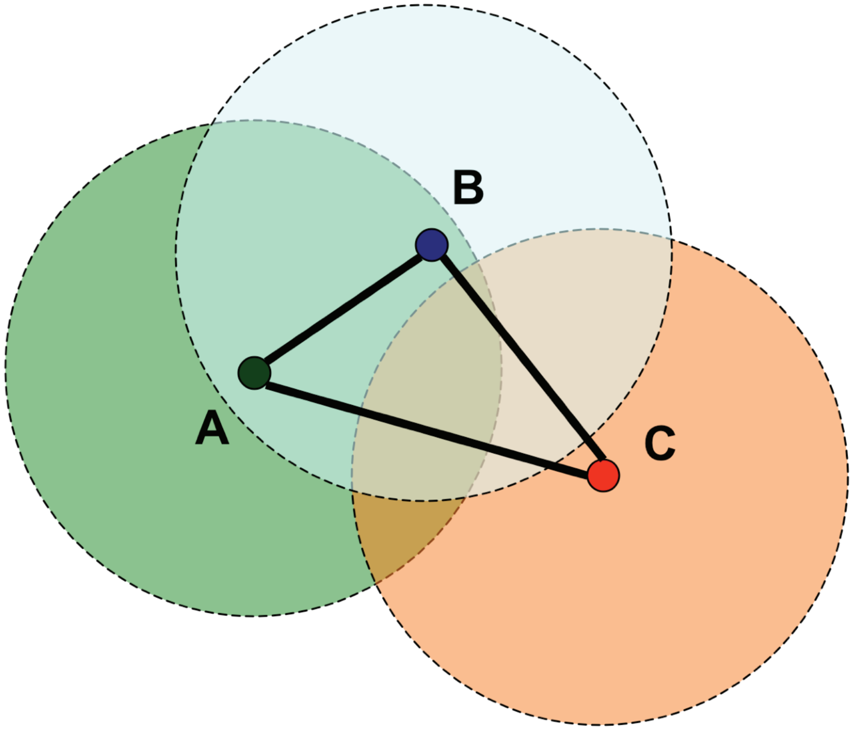
- Easy to deploy
- Good in changing environments
- Allows for node mobility
- Self-configurable
- Scalable

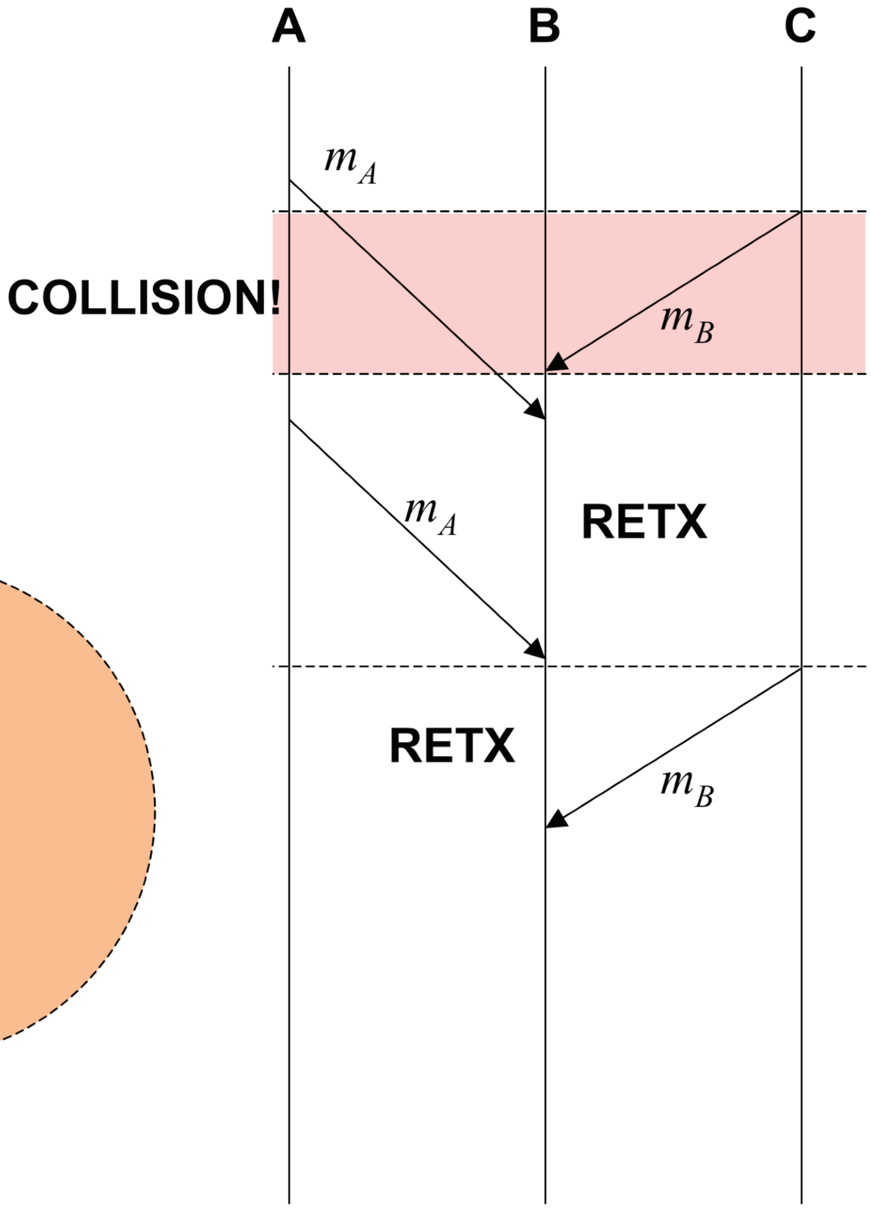
Medium Access Control

<u>Goal:</u> To coordinate access to the shared medium in a way that:

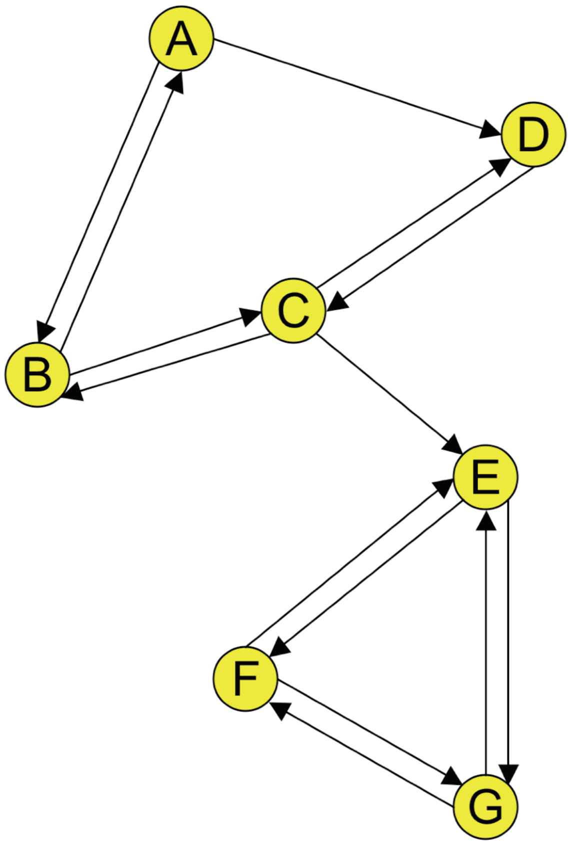
- Maximizes throughput,
- Minimizes collisions, and
- Avoid hidden and exposed node problems.

Collisions





Routing

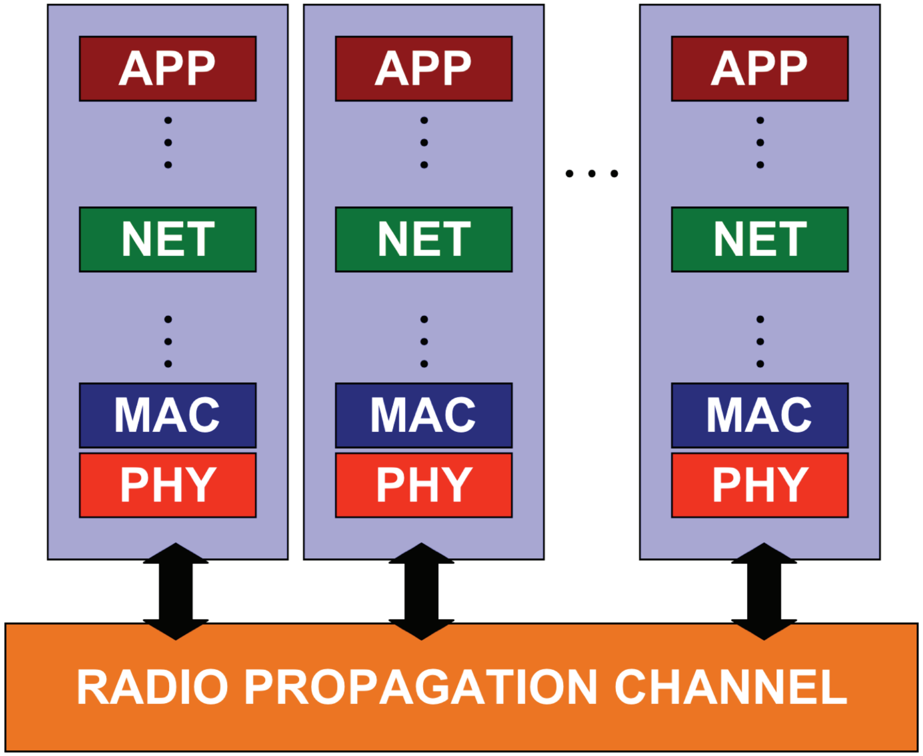


All-pairs shortest path problem:

Find paths connecting every node to every other node in the graph.

- Use a distributed algorithm that uses control messages to discover neighbors and to share knowledge of routes.
- Find paths only on demand.
- Deal with channel asymmetries and cycles.
- Deal with reliability problems associated with links and with nodes.
- Deal with malicious interventions.
- Should be scalable.

Network Model



Physical Layer:
radio sensing, bit transmission

MAC Layer:
retransmissions, contention, collisions, error-detection and correction

Network Layer:
routing

Application Layer:
traffic generation

Vulnerabilities in Wireless Ad Hoc Networks

Extensive research has been done to evaluate the effects of attacks on the protocol algorithms (protocols have design and implementation faults).

Our research has been on attacks that deal with the physical integrity of the nodes and the conditions in their surrounding environment.

Motivation

We need to understand the risks of the technology before we can rely on it for mission-critical applications.

Risks can be quantified/estimated with computer simulation, but for that we need a model.

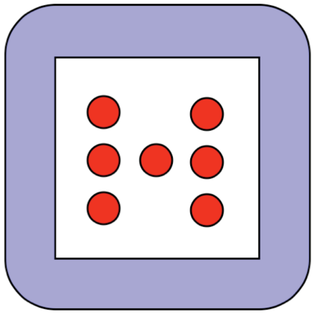
Random Variables

Definition: Let Ω be a sample space. A random variable X is a function with domain Ω and range the real numbers R or a subset of R.

F. Solomon, Probability and Stochastic Processes, 1987, Prentice-Hall

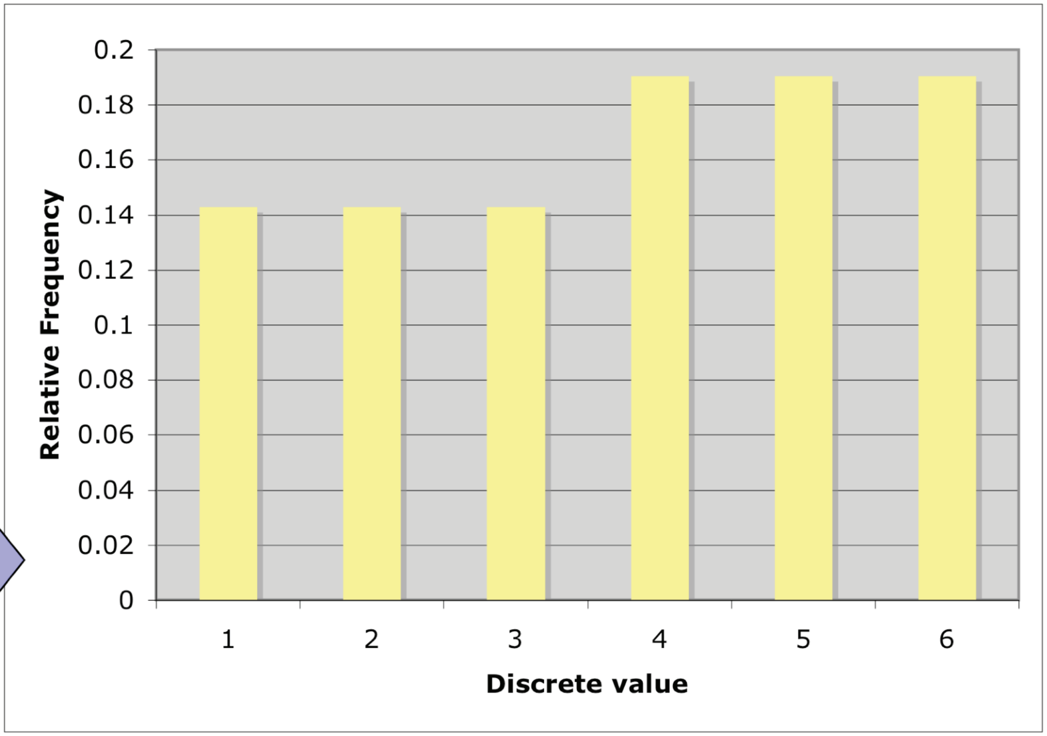
Random variables can be discrete (countable range) or continuous (uncountable range) and are described by a probability mass function or a probability density function, respectively.

Example: Electronic 6-Sided Die

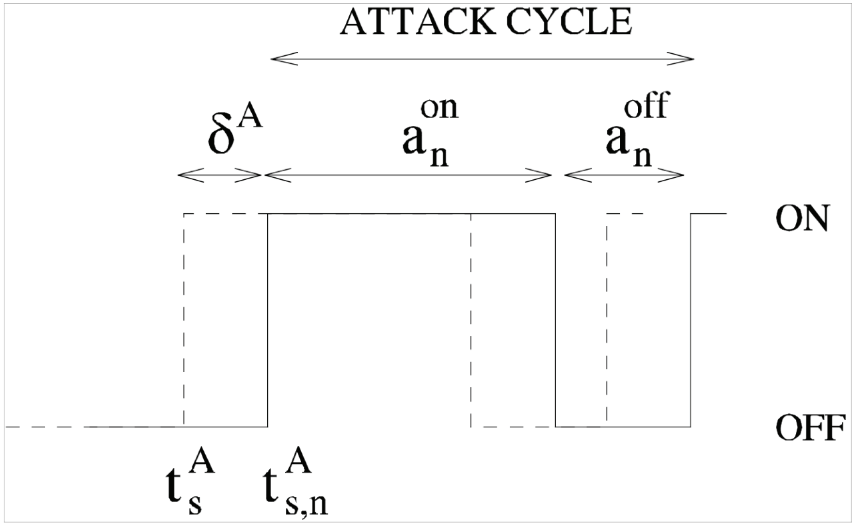


$\Omega = \{1,2,3,4,5,6\}$

For some i in Ω, what is the $\Pr\{X=i\}$?



On-Off Attack Model



$\delta^A \sim \Delta^A$: jitter for attack A

$t_s^A \sim T_s^A$: start time for attack A

$T_{s,n}^A = T_s^A + \Delta^A$

$t_{s,n}^A \sim T_{s,n}^A$: start time for attack A on node n

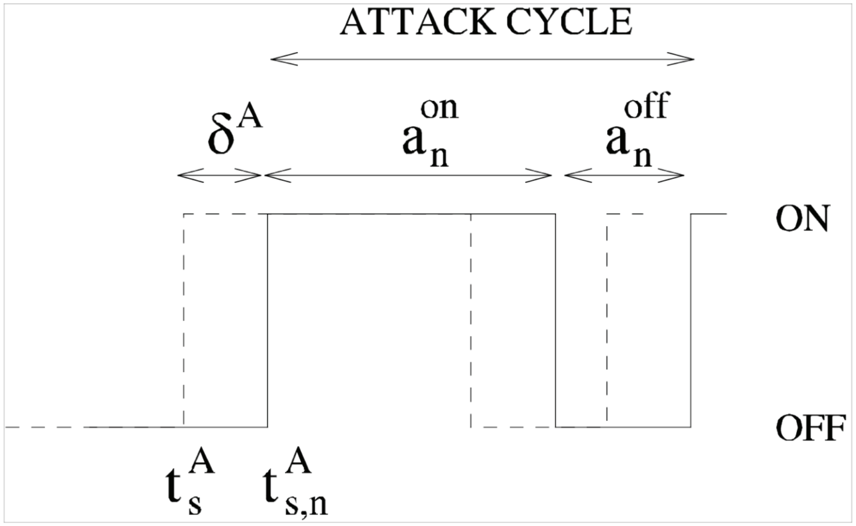
$a_n^{on} \sim A_n^{on}, a_n^{off} \sim A_n^{off}$

A_n^{on} : length of on-period

A_n^{off} : length of off-period

p : prob. that some node n is attacked or launches an attack

On-Off Attack Model



p : prob. that some node n is attacked or launches an attack

$\delta^A \sim \Delta^A$: jitter for attack A

$t_s^A \sim T_s^A$: start time for attack A

$T_{s,n}^A = T_s^A + \Delta^A$

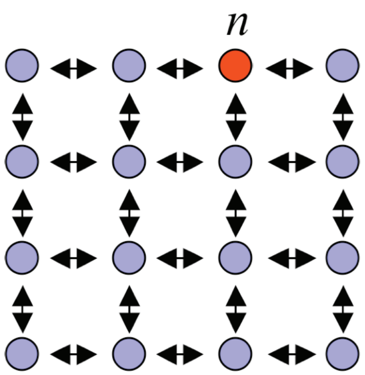
$t_{s,n}^A \sim T_{s,n}^A$: start time for attack A on node n

$a_n^{on} \sim A_n^{on}, a_n^{off} \sim A_n^{off}$

A_n^{on} : length of on-period

A_n^{off} : length of off-period

The *Reboot* Attack

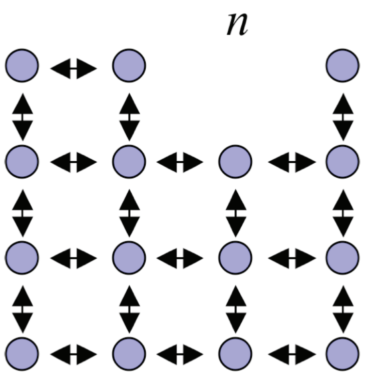


Node n is attacked

```
while (simulation not finished) do
  if Bernoulli(REBOOT PROBABILITY)==1 then
    $t_{s,n} \leftarrow U\,[t_s, t_s + \delta]$
    at time $t_{s,n}$ do:
    while (true) do
      power down and stay offline for $a^{on}$ sec.
      bootup and stay online for $a^{off}$ sec.
    end while
  end if
end while
```

The periodic rebooting of node n causes the routing protocol to send out messages to re-establish routes. A physical action against the node (e.g., removing and reinstalling batteries) is able to create additional control traffic in the network.

The *Reboot* Attack

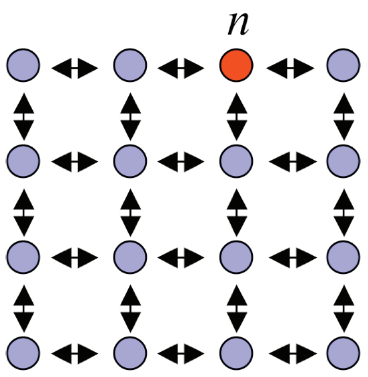


Node n is attacked

```
while (simulation not finished) do
  if Bernoulli(REBOOT PROBABILITY)==1 then
    $t_{s,n} \leftarrow U\,[t_s, t_s + \delta]$
    at time $t_{s,n}$ do:
    while (true) do
      power down and stay offline for $a^{on}$ sec.
      bootup and stay online for $a^{off}$ sec.
    end while
  end if
end while
```

The periodic rebooting of node n causes the routing protocol to send out messages to re-establish routes. A physical action against the node (e.g., removing and reinstalling batteries) is able to create additional control traffic in the network.

The *Reboot* Attack

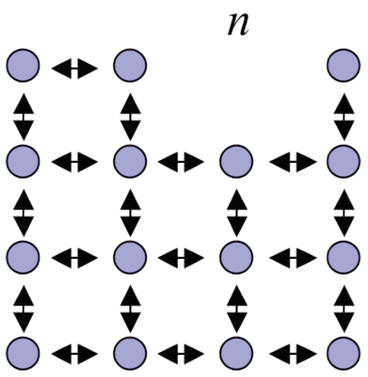


Node n is attacked

```
while (simulation not finished) do
  if Bernoulli(REBOOT PROBABILITY)==1 then
    $t_{s,n} \leftarrow U\,[t_s, t_s + \delta]$
    at time $t_{s,n}$ do:
    while (true) do
      power down and stay offline for $a^{on}$ sec.
      bootup and stay online for $a^{off}$ sec.
    end while
  end if
end while
```

The periodic rebooting of node n causes the routing protocol to send out messages to re-establish routes. A physical action against the node (e.g., removing and reinstalling batteries) is able to create additional control traffic in the network.

The *Reboot* Attack

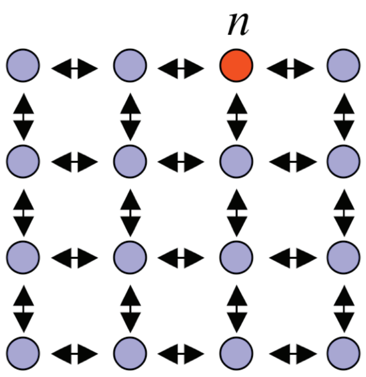


Node n is attacked

```
while (simulation not finished) do
  if Bernoulli(REBOOT PROBABILITY)==1 then
    $t_{s,n} \leftarrow U\,[t_s, t_s + \delta]$
    at time $t_{s,n}$ do:
    while (true) do
      power down and stay offline for $a^{on}$ sec.
      bootup and stay online for $a^{off}$ sec.
    end while
  end if
end while
```

The periodic rebooting of node *n* causes the routing protocol to send out messages to re-establish routes. A physical action against the node (e.g., removing and reinstalling batteries) is able to create additional control traffic in the network.

The *Range* Attack

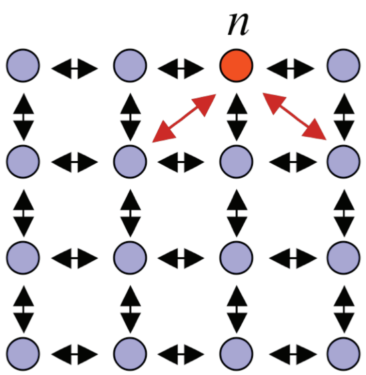


Node n is attacked

```
while (simulation not finished) do
  if Bernoulli(REBOOT PROBABILITY)==1 then
    $t_{s,n} \leftarrow U\,[t_s, t_s + \delta]$
    at time $t_{s,n}$ do:
    while (true) do
      decrease TX range for $a^{on}$ sec.
      restore original TX range for $a^{off}$ sec.
    end while
  end if
end while
```

The periodic changes in the transmission power of node n cause the routing protocol to send out messages to update shortest routes. A physical action against the node (e.g., obstructing the node’s antenna) is able to create additional control traffic in the network.

The *Range* Attack

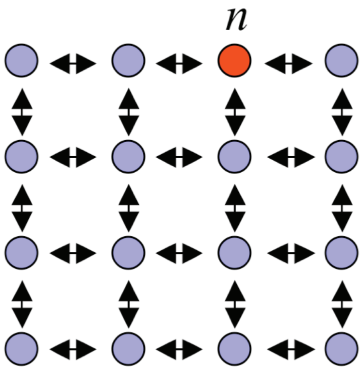


Node n is attacked

```
while (simulation not finished) do
  if Bernoulli(REBOOT PROBABILITY)==1 then
    $t_{s,n} \leftarrow U\,[t_s, t_s + \delta]$
    at time $t_{s,n}$ do:
    while (true) do
      decrease TX range for $a^{on}$ sec.
      restore original TX range for $a^{off}$ sec.
    end while
  end if
end while
```

The periodic changes in the transmission power of node *n* cause the routing protocol to send out messages to update shortest routes. A physical action against the node (e.g., obstructing the node’s antenna) is able to create additional control traffic in the network.

The *Range* Attack

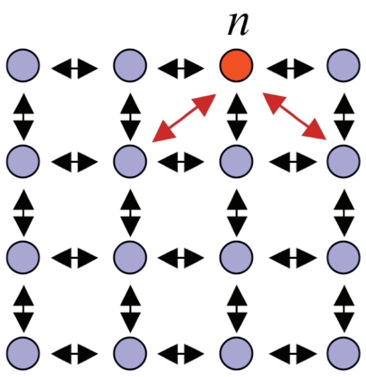


Node n is attacked

```
while (simulation not finished) do
  if Bernoulli(REBOOT PROBABILITY)==1 then
    $t_{s,n} \leftarrow U\,[t_s, t_s + \delta]$
    at time $t_{s,n}$ do:
    while (true) do
      decrease TX range for $a^{on}$ sec.
      restore original TX range for $a^{off}$ sec.
    end while
  end if
end while
```

The periodic changes in the transmission power of node n cause the routing protocol to send out messages to update shortest routes. A physical action against the node (e.g., obstructing the node’s antenna) is able to create additional control traffic in the network.

The *Range* Attack

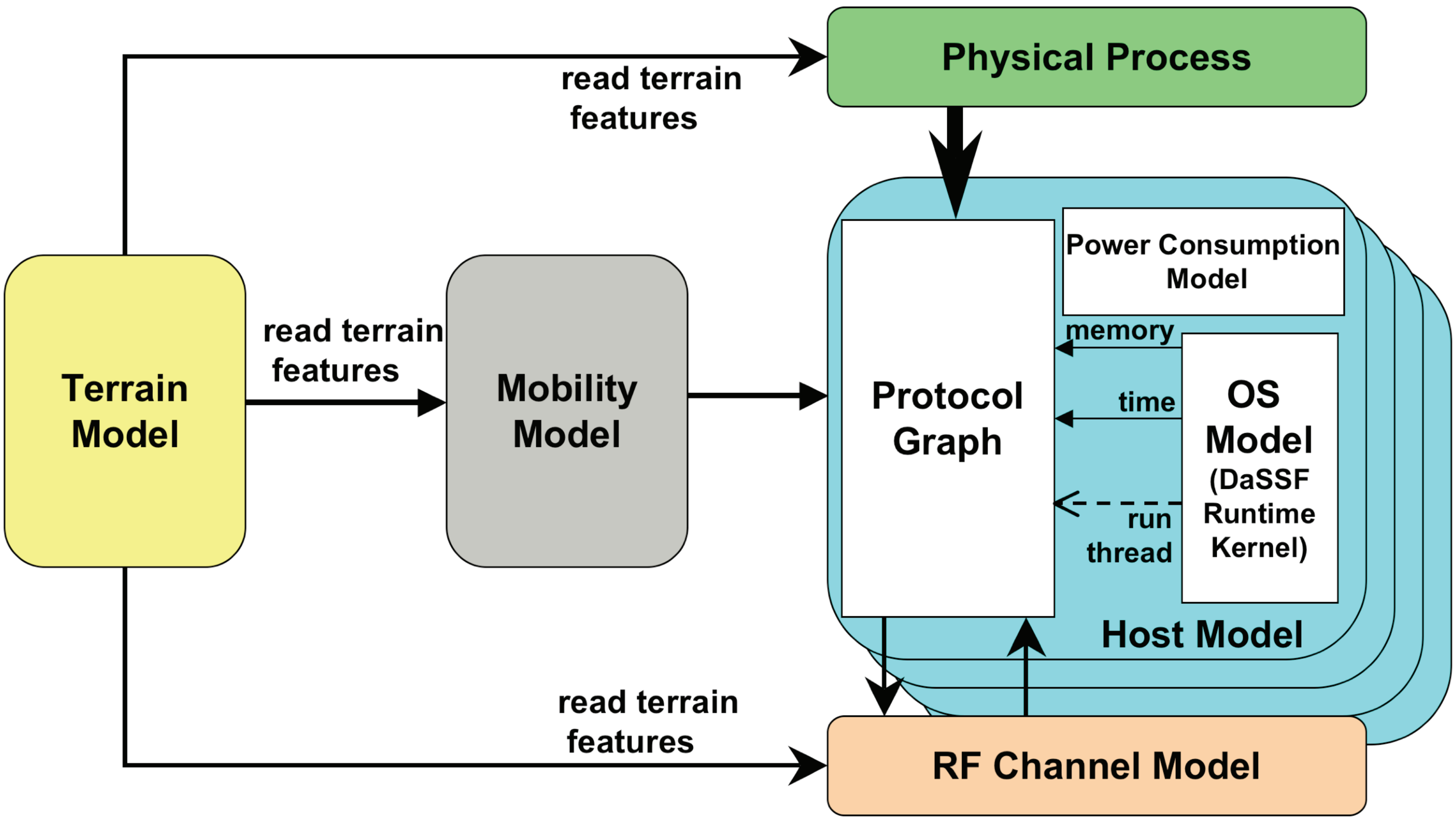


Node n is attacked

```
while (simulation not finished) do
  if Bernoulli(REBOOT PROBABILITY)==1 then
    $t_{s,n} \leftarrow U[t_s, t_s + \delta]$
    at time $t_{s,n}$ do:
    while (true) do
      decrease TX range for $a^{on}$ sec.
      restore original TX range for $a^{off}$ sec.
    end while
  end if
end while
```

The periodic changes in the transmission power of node *n* cause the routing protocol to send out messages to update shortest routes. A physical action against the node (e.g., obstructing the node’s antenna) is able to create additional control traffic in the network.

SWAN: a Simulation Tool



Experimental Scenario

RF propagation: 2-ray ground reflection, antenna height 1.5m, tx power 15dBm, SNR threshold packet reception.

Mobility: stationary; grid deployment.

Traffic generation: variation of CBR; session length=60|120, destination is random for each session, CBR 3072 bytes/s for each session.

Network: 36 nodes in a 6x6 regular grid (150 m spacing).

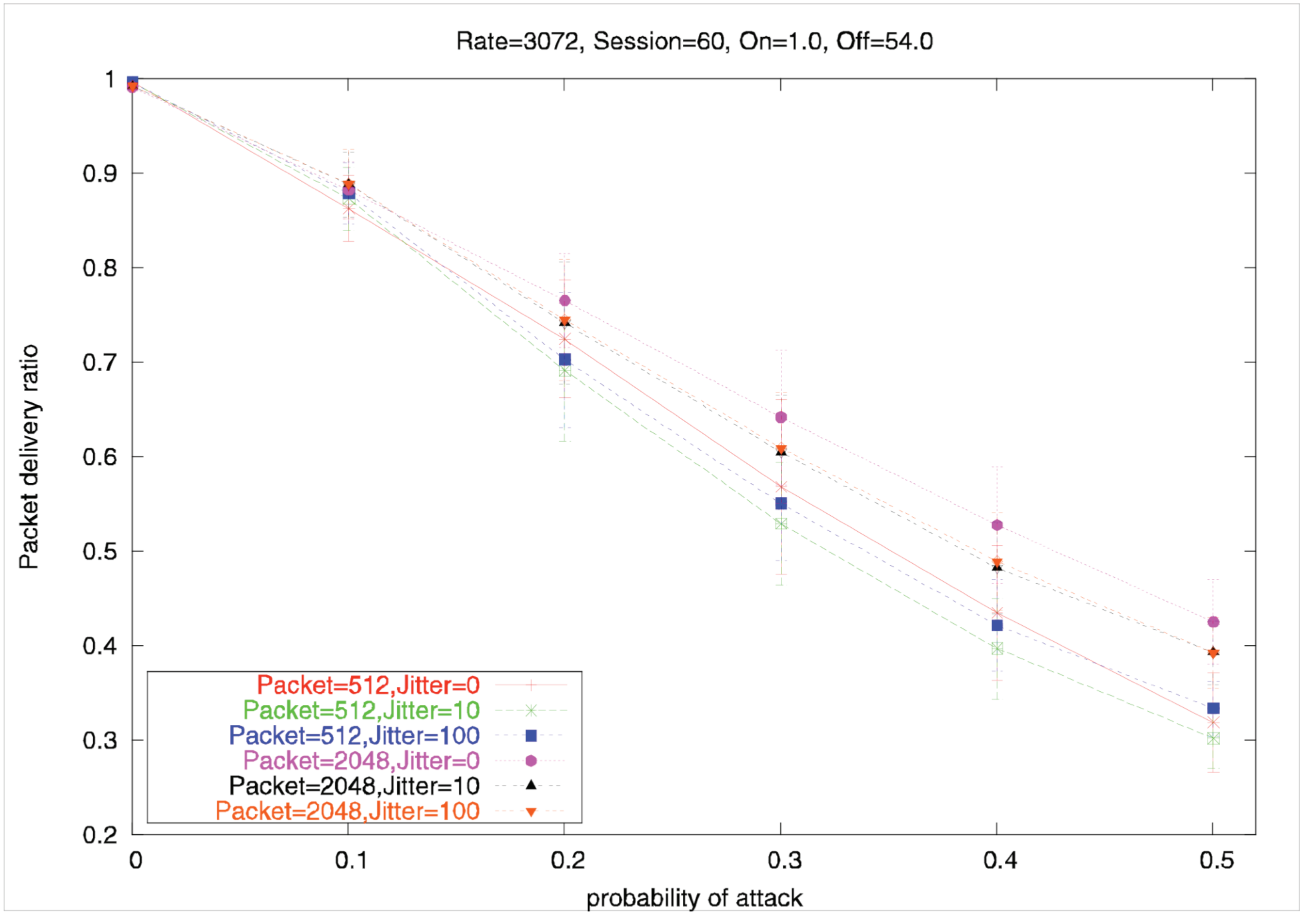
Transient avoidance: statistics collected after 100 sec.

Protocol stack: IEEE 802.11b PHY (message retraining modem capture, 11 Mbit/s), IEEE 802.11b MAC (DCF), ARP, IP, AODV routing (no local route repair, MAC acknowledgements, expanding ring search, active route time out of 10 sec., max two retries for RREQs).

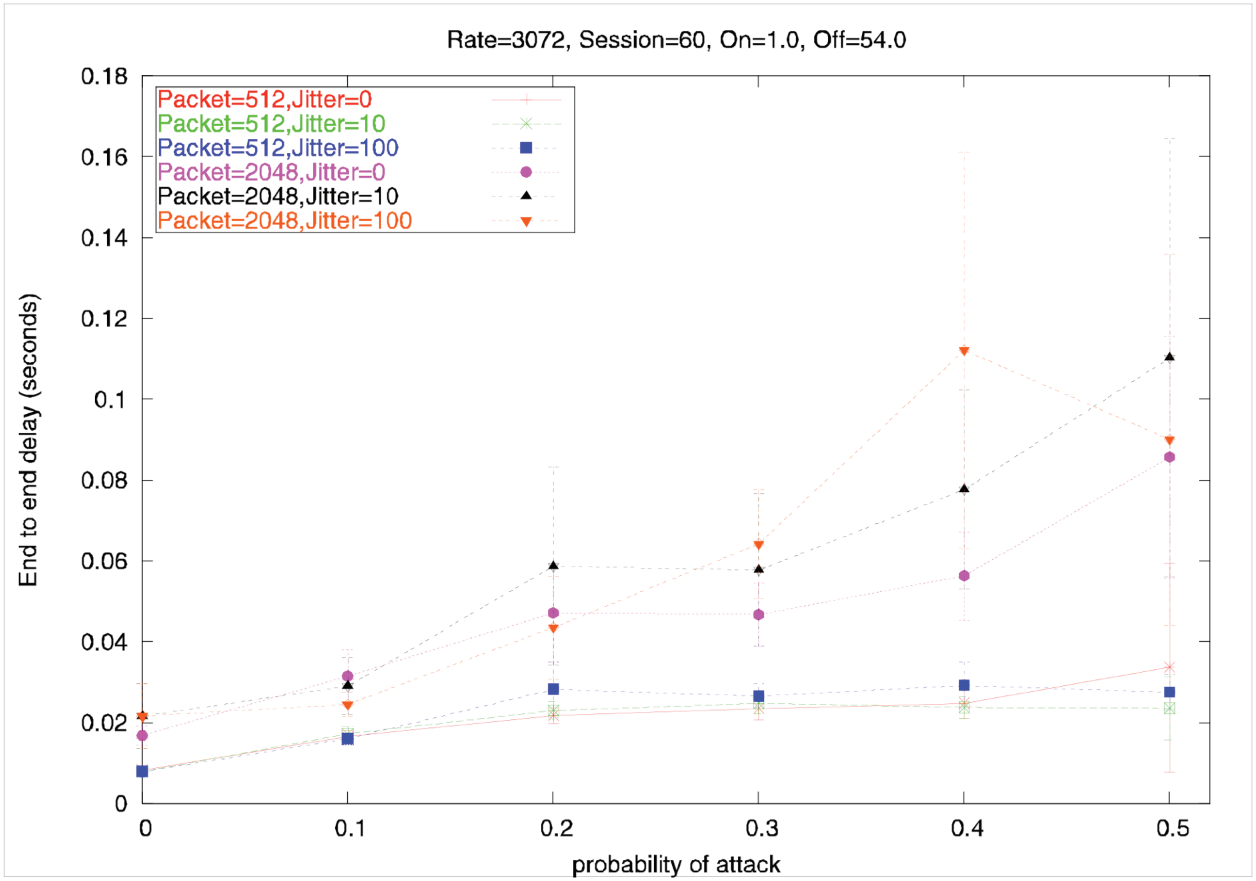
Arena size: 900 m x 900 m.

Replications: 20 runs with different seeds for every random stream in the model. For all metrics estimated, we produced 95% confidence intervals.

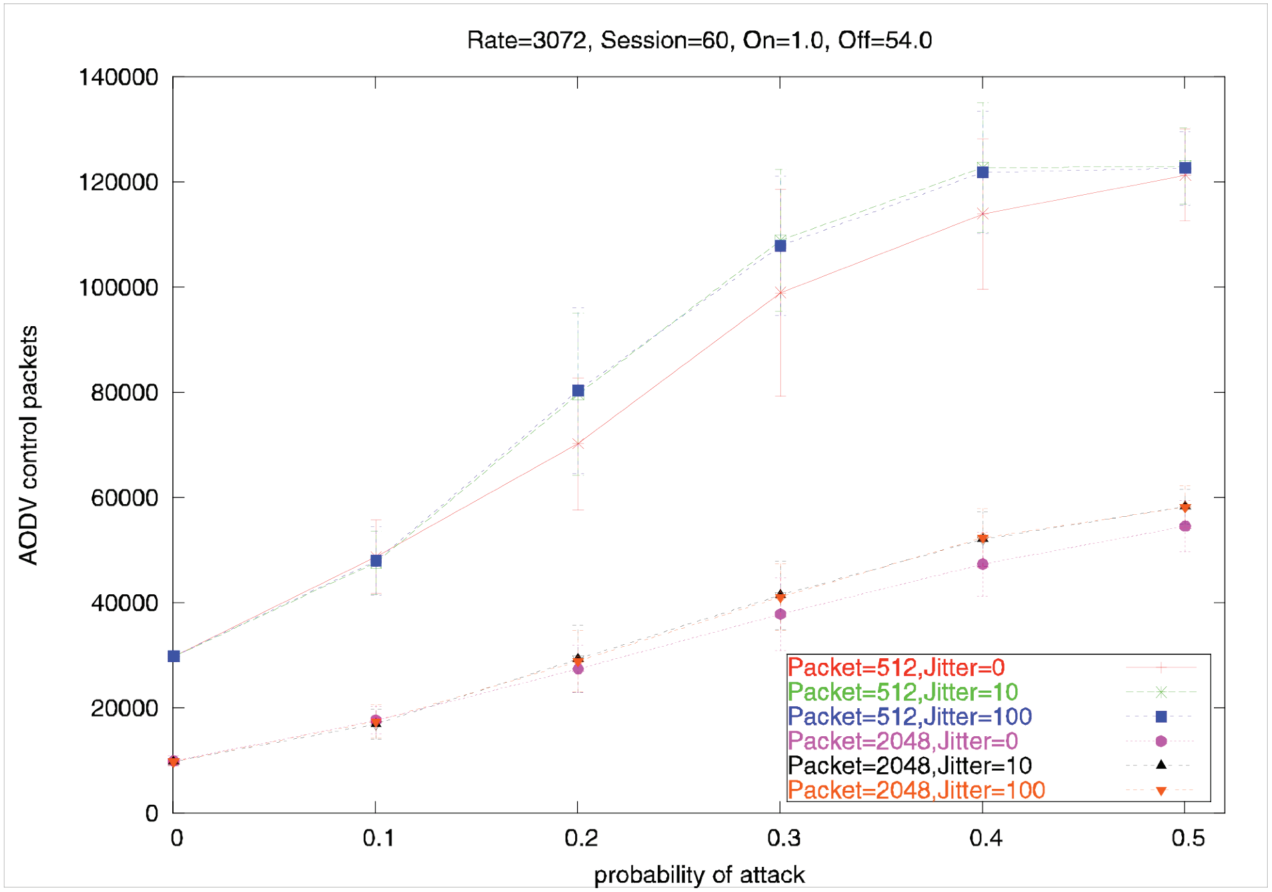
Effect of Reboot Attack Jitter on PDR



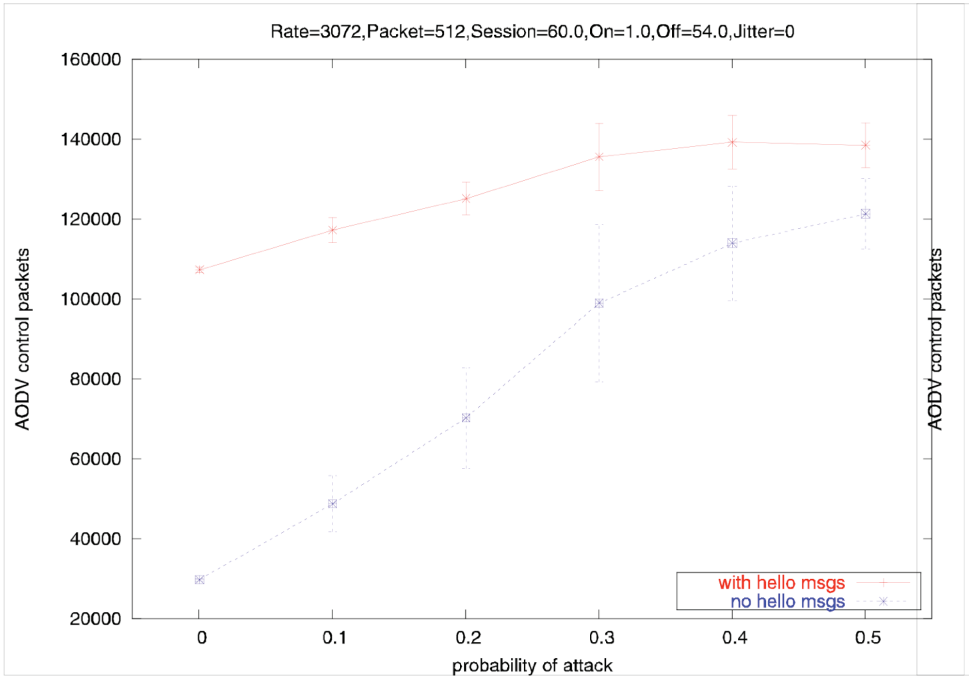
Effect of Reboot Attack on End-to-End Delay

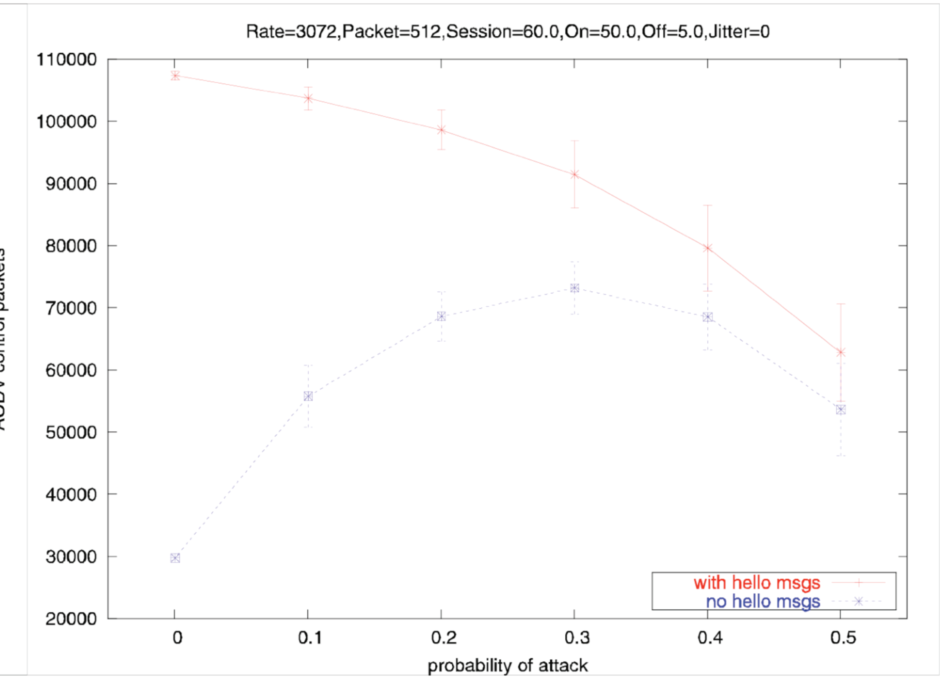


Effect of Reboot Attack Jitter on AODV Control Packets

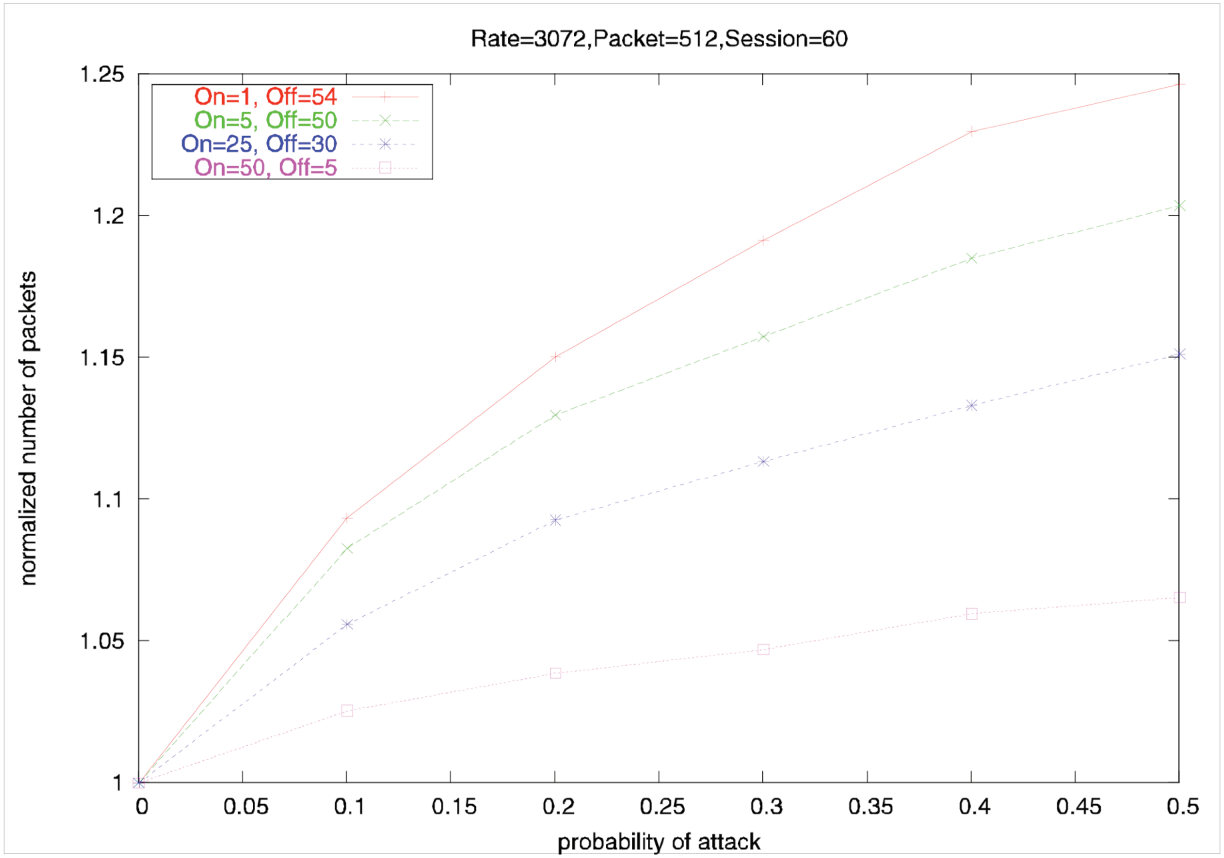


Effect of Length of Attack Cycles on AODV Control Packets

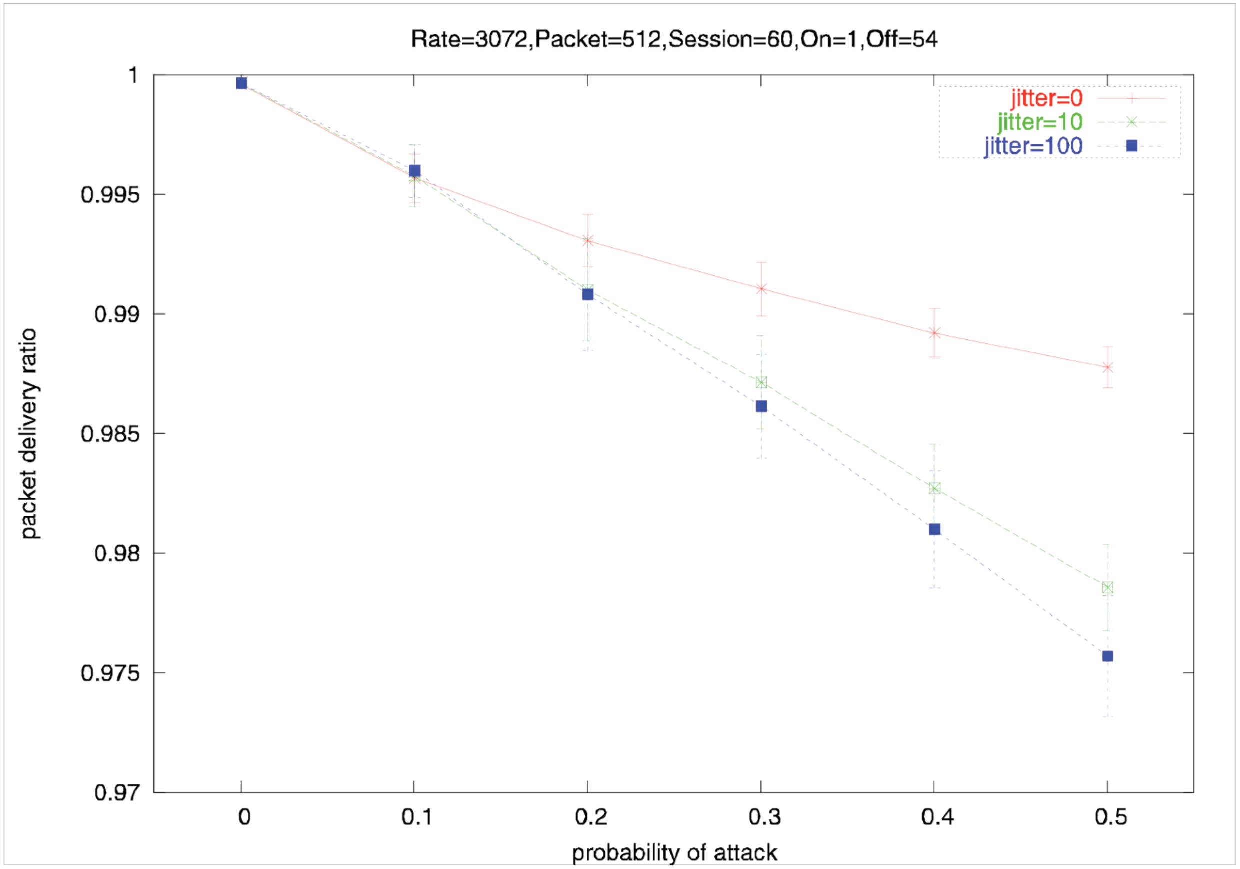




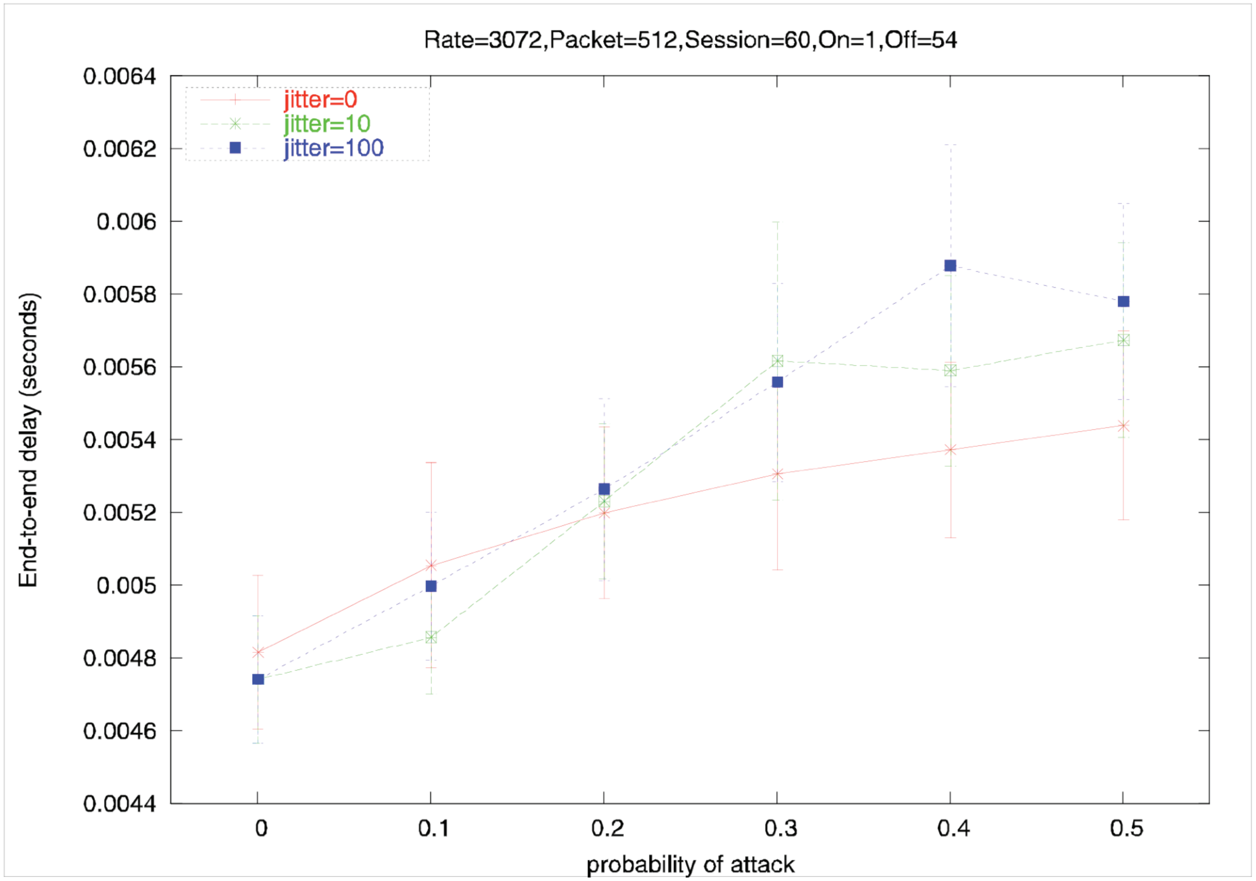
Effect of Range Attack AODV Control Packets (Jitter=0)



Effect of Range Attack on PDR



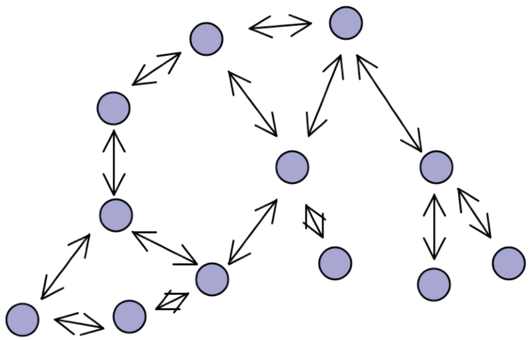
Effect of Range Attack on End-to-End Delay



Summary

- We presented a model that is general within the category of on-off attack processes.
- Our experimental results quantify the effects of two simple attack models on a wireless grid using ad hoc routing (AODV).

Current and Future Work



- Determine the impact of the attacks on other metrics of “network health”. We have investigated the effects on different metrics to quantify connectivity. (on going)
- Determine the length of the transients experienced by different metrics when there’s an attack state transition. (on going)
- Evaluate the impact of the attacks when the network topology is a random graph. The choice of analysis methodology will be important.
- Construct a framework that automates the construction and the execution of simulation experiments. (Chris Kenna)
- Evaluate the impact of the attacks when cycle lengths are given by more complex probability distributions. (Bryan Ward)