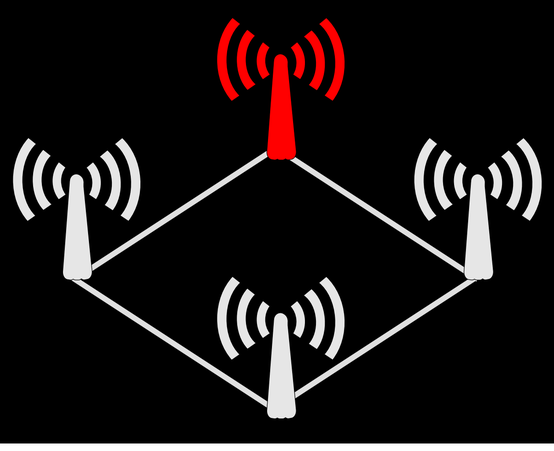
CERIAS

The Center for Education and Research in Information Assurance and Security

Adversarial Testing of Wireless Routing Implementations



Endadul Hoque[*], Hyojeong Lee[*], Rahul Potharaju[*], Charles Killian[‡*], and Cristina Nita-Rotaru[*]

[*] *Department of Computer Science, Purdue University.*

[‡] *Google, Inc.*

{ ROUTING IN WIRELESS NETWORKS }

Routing protocols

- Fundamental component of wireless networks
- Different from traditional routing protocols
  - Proactive: *DSDV*
  - Reactive: *AODV*
  - Secure: *ARAN*

Robustness and security

- Traditional efforts
  - Model checking
  - Simulation

Limitations

- Real-world implementations bring new vulnerabilities
  - Model checking and/or simulation not enough
- Adversarial testings discover critical vulnerabilities
  - Simulator-based implementation may not cover all

{ GOAL / CONTRIBUTIONS }

Goal: Automate adversarial testing of real-world implementation of wireless routing protocols

Design platform for wireless routing protocols

- Extension of an existing platform (Turret)
- Leverage network emulation and virtualizations
- Support special features for wireless protocols

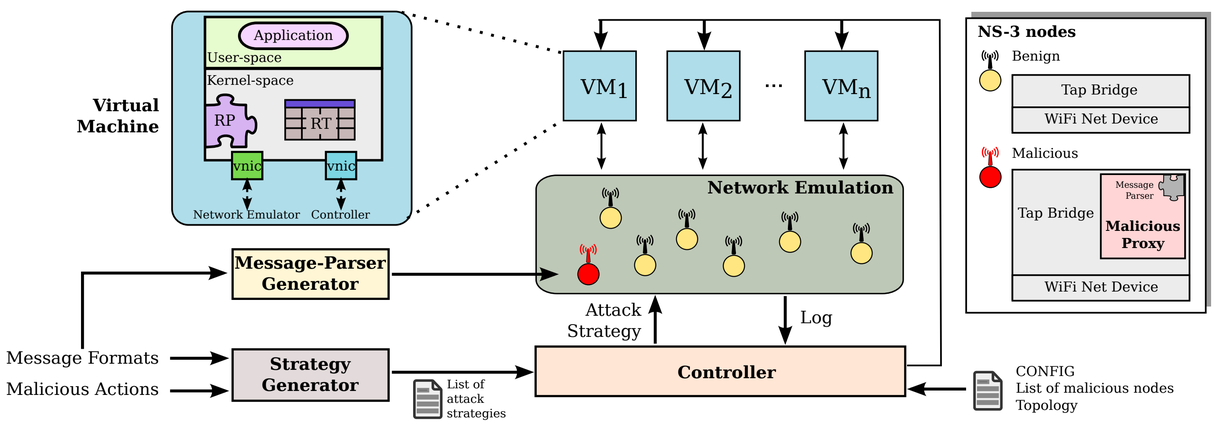
Demonstrate attack/bug discovery

- Case studies: AODV and ARAN
- (Re-)discover 14 attacks
- Discover 3 bugs

Turret

- For general distributed systems
- Use target system's binary
- Support manipulation of protocol messages

{ TURRET-W PLATFORM }



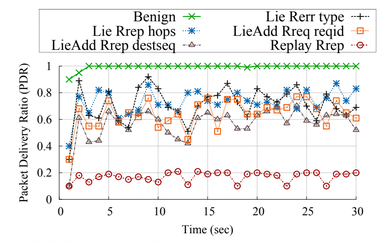
Turret-W

- Wireless network emulation
  - to support wireless routing protocols
- Separation of control plane and data plane
  - to support basic attacks such as blackhole attacks
- Side channels among malicious nodes
  - to support colluding attacks such as wormhole attacks
- Replay packets

{ CASE STUDY }

Evaluation methodology

- 12 VMs, vary # of malicious nodes
- Routing: AODV, ARAN
- Application: iperf
- Performance metric: PDR
- Combine blackhole/wormhole attacks
- Baseline performance from benign test



PDR for AODV with 4 adversaries

AODV

- 1 new implementation-level attack
  - Lie RREQ type 2 - cause neighbors to crash
- 7 known protocol-level attacks
  - Reply RREP
  - LieAdd RREP destsq.
  - Blackhole/wormhole attacks
- 2 bugs
  - Kernel interaction order
  - Route packet harder

```
1. void NS_CLASS rrep_process(..., int rreplen, ...){
2.     unsigned int extlen = 0;
3.     AodvExtension *ext = rrep + RREP_SIZE;
       ...
4.     while ((rreplen - extlen) > RREP_SIZE) { // RREP_SIZE: 20
         ... // process extention according to the type
5.       /* read ext length from packet */
6.       extlen += EXT_HDR_SIZE + ext->length;  // EXT_HDR_SIZE: 2
7.       ext = ext + EXT_HDR_SIZE + ext->length;
8.     }
       ...
9.  }
```

ARAN

- 6 known protocol-level attacks
  - Divert REP
  - Drop RDP
  - Blackhole/wormhole attacks
- 1 bug
  - Wrong postal address

CERIAS

PURDUE UNIVERSITY