# A Platform for Finding Attacks in Unmodified Implementations of Intrusion Tolerant Systems

**Hyojeong Lee*, Jeff Seibert+, Charles Killian* and Cristina Nita-Rotaru***
Department of Computer Science, Purdue University*, MIT Lincoln Laboratory+

## Intrusion Tolerant Systems

•Correct operation and make progress even when a fraction of nodes are compromised
•Previous work found attacks that can degrade performance severely so that the system is no longer practically usable
•Finding such attacks is extremely difficult

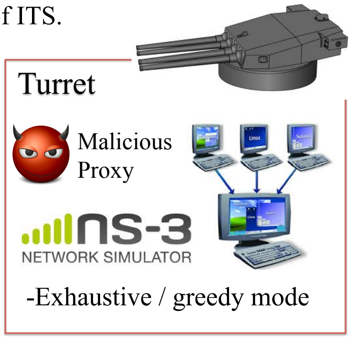
## Related work

• "Gatling: Automatic Attack Discovery in Large-Scale Distributed Systems " NDSS`12
 - Automatically injects malicious actions and greedily search performance attacks
 - Only works with special environments (Mace)

## Turret

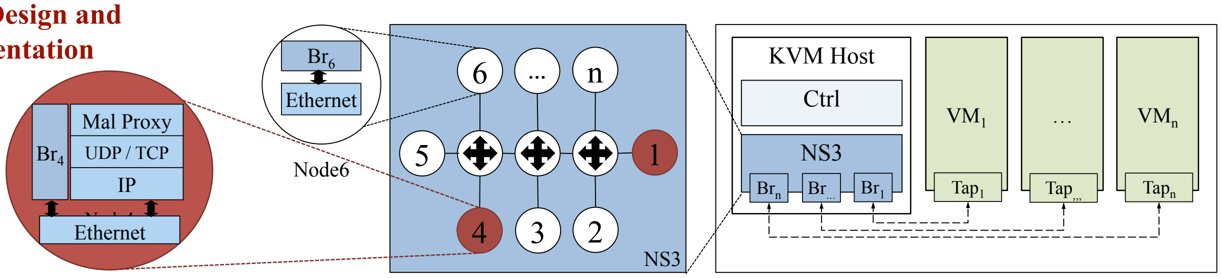
•A platform for automatically finding performance attacks in **unmodified** implementations of ITS.

- Realistic environment: Virtualization + network emulation
- User provides: Binary + Message Format
- Automated malicious proxy: Deviates protocol
- Snapshot/rollback the entire distributed system



-Exhaustive / greedy mode

## Turret Design and Implementation

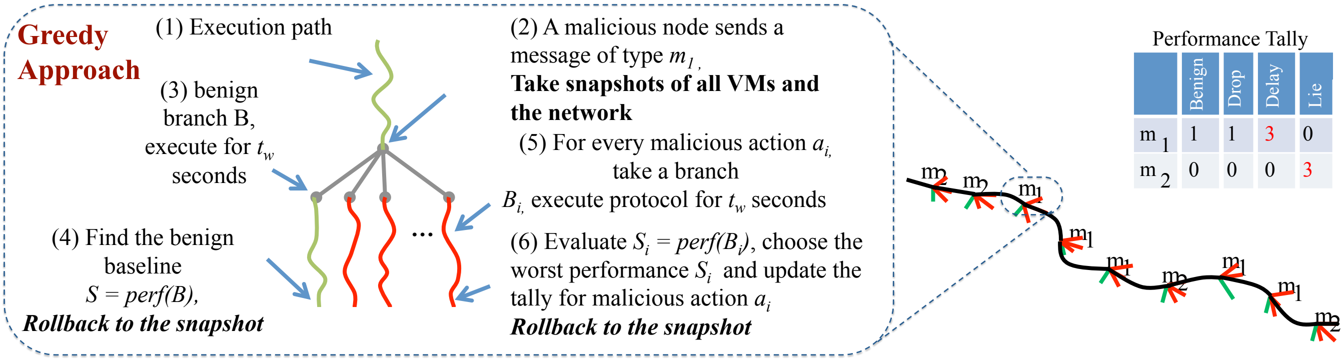


-Malicious proxy: intercept and manipulate message delivery and contents
-Implemented network emulator snapshot
-Controller can take snapshots of all VMs and the network together

### Exhaustive Search:

-Generate all possible list of single actions and combination of actions
- Try each action and see the results

### Greedy Approach



(1) Execution path

(3) benign branch B, execute for $t_w$ seconds

(4) Find the benign baseline $S = perf(B)$, ***Rollback to the snapshot***

(2) A malicious node sends a message of type $m_1$ , **Take snapshots of all VMs and the network**

(5) For every malicious action $a_i$, take a branch $B_i$, execute protocol for $t_w$ seconds

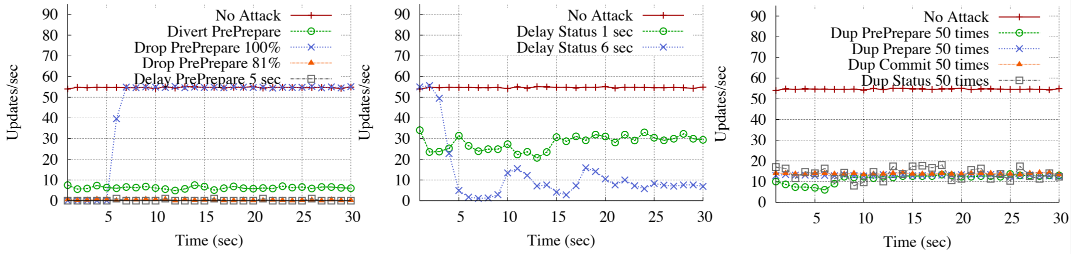
(6) Evaluate $S_i = perf(B_i)$, choose the worst performance $S_i$ and update the tally for malicious action $a_i$
***Rollback to the snapshot***

Performance Tally

| | Benign | Drop | Delay | Lie |
|---|---|---|---|---|
| $m_1$ | 1 | 1 | 3 | 0 |
| $m_2$ | 0 | 0 | 0 | 3 |

## Results

• Applied Turret on three ITS
 - PBFT
 - Prime
 - Steward
• Total 18 attacks found,16 previously undocumented



(a) Attacks that limit progress in PBFT

(b) Delay attacks that cause DoS in PBFT

(b) Dup attacks that cause DoS in PBFT