Information Assurance of LTE-Advanced Self-Organizing Networks

Munawwar M. Sohul
Raghuprasad Bettadapura
Aman Singhal
Jeffery H. Reed
Virginia Polytechnic Institute and State University

Outline

- Motivation of the work
- Security aspect of SON
- Impact of SON security vulnerabilities
- Focused analysis on one attack
- Simulation results
- Summary and Conclusion

Motivation

- Motivation for Self Organizing Network (SON)
  - Demand for improved user experience
  - Heterogeneous Network (Het-Net) increases network complexity
  - Cost of Network management
- SON is one of the key features of LTE and LTE-A
  - Benefits: Reduced cost and improved network performance
  - Challenges: New and unique security vulnerabilities
- Very little research work exists
  - Outside of standard bodies or proprietary works
  - One of first known information assurance of LTE-A SON study
- Goal:
  - Encourage consideration of security aspect in the development and implementation phase of SON functionalities.

Security Aspect of SON (1/4)

- SON functionalities introduce new network vulnerabilities
  - Network intelligence and behavior characterization
    - Results in reduced throughput
  - Node emulation attack
    - Decreases cell coverage
    - Affects scheduling algorithms and serving node preference
  - Automation requires measuring the environment through sensing
    - An intruder can modify the UE, eNB, OA&M measurements, and radio resource control reports

Security Aspect of SON (2/4)

- Initial setup of a network element (NE) and configuration
  - The security environment of NE setup should not impair the level of automation reached
  - Setting up secure connectivity between a NE and its OAM system (as well as other NEs) is crucial
    - Increasingly physical security is replaced by virtual security

**Physical security: dedicated physical backhaul links, (macro) base stations installed in dedicated, locked cabinet

**Virtual security: virtual backhaul links, pico/micro base stations installed in a public environment

Security Aspect of SON (3/4)

- Automation means inherently reducing human interaction
  - Reduce human monitoring of security related aspects of the system
  - It is important to analyze if this reduction is acceptable.
- The new threat scenarios incurred by SON functionality
  - Needs to be analyzed and addressed by security mechanisms
- Literature review of SON security aspect
  - No published prior work on SON security

Security Aspect of SON (4/4)

- Analysis of SON architecture and characteristics revealed
  - *Point of vulnerabilities for intrusion*
    - Measurements from network entities
    - Location and interface involved
    - Learning algorithms
    - Interdependency of SON functionalities
  - *Types of security threats*
    - Network intelligence and behavior characterization
    - Node emulation attack
    - Faltered device association and route integrity
    - Denial of service attack
    - Jamming attacks on reference and synchronization signals

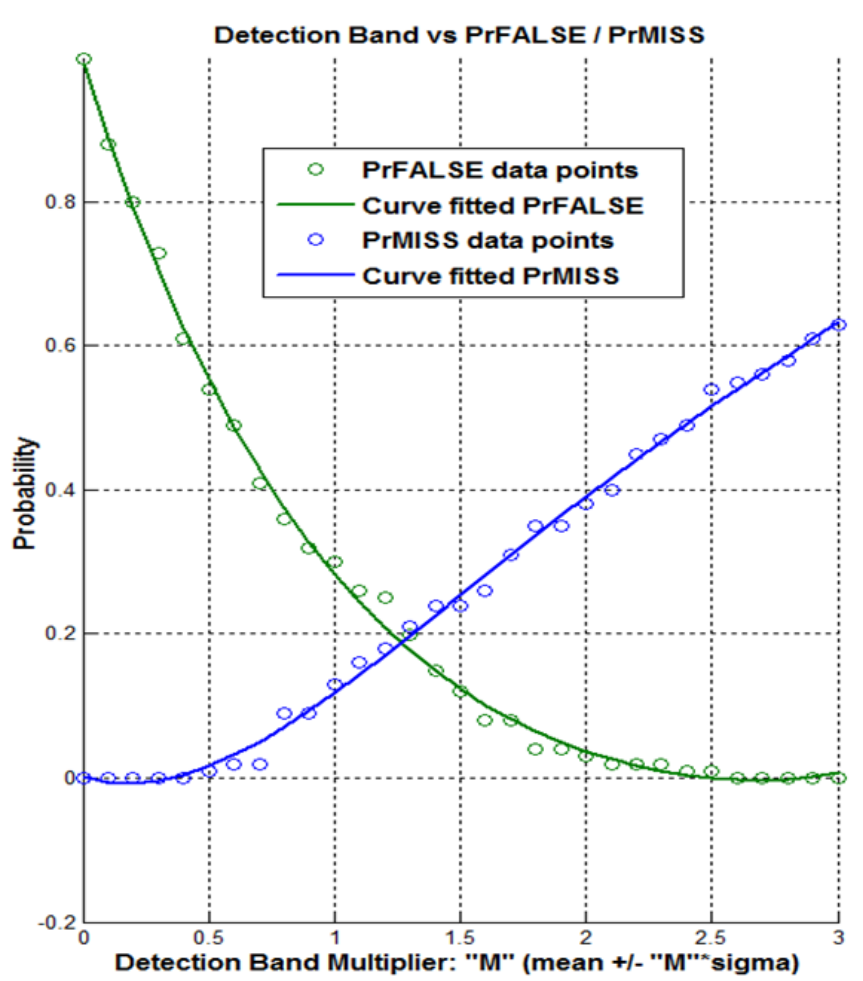
Impact on System Performance

- Expected impact of attack on system performance
  - Poor cell coverage
  - Degraded cell edge performance
  - Traffic load imbalance
  - Scheduling malfunction
  - Poor HO performance
  - Radio link failure
- Metrics for analyzing effectiveness of attack
  - RSRP, SINR
  - Radio link failure (RLF)
  - Hand over parameters
  - Cell edge throughput
  - Call setup time
  - Traffic load distribution
- Initial recommendation on potential defense
  - Anomaly Detection
  - Firewall to restrict the propagation of intrusion and localize the impact
  - Authentication for device association

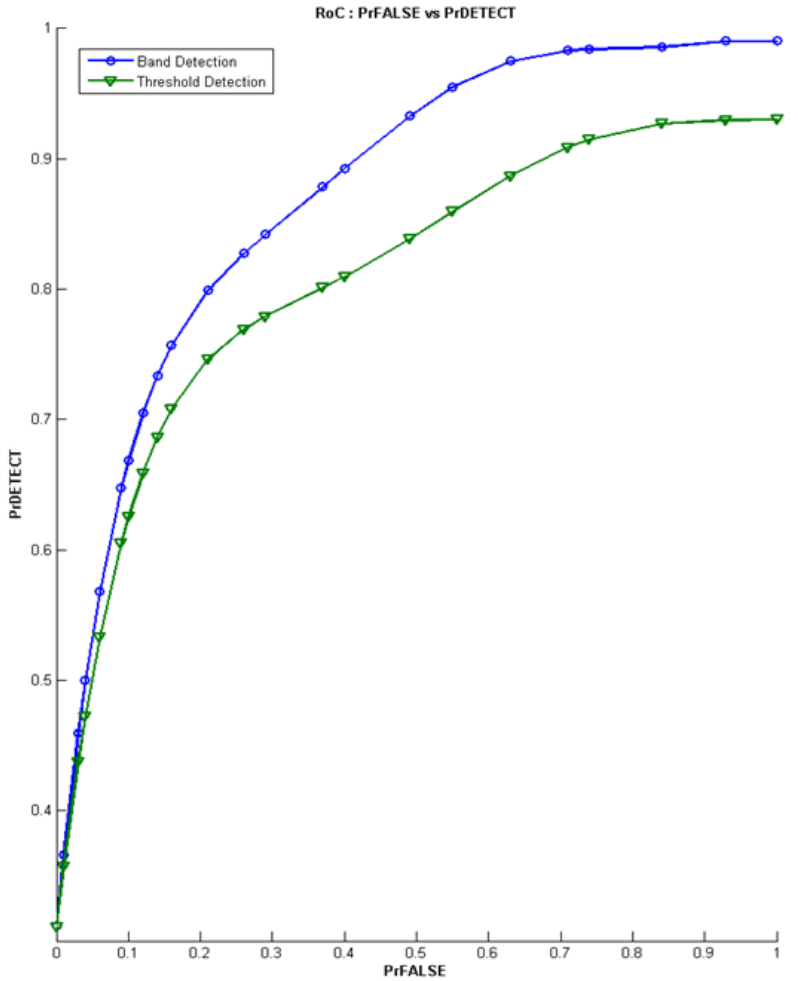
Focused Analysis for one Attack

- Use case: Inter Cell Interference Coordination (ICIC)
- Intrusion detection technique: Anomaly detection
- Context:
  - LTE (Rel-8) spec., Uniform traffic, Okumura-Hata mode
  - Threat type: node emulation, measurement modification
  - Observation phases: before and after attack, and after recovery
  - Frequency reuse policy: Fractional Frequency Reuse – 3 (FFR-3)
  - Triggering metric: SIR, RSRP
- Observations:
  - SIR for cell edge users for
  - Throughput for the cell edge users

Simulation Results: Detection Approaches

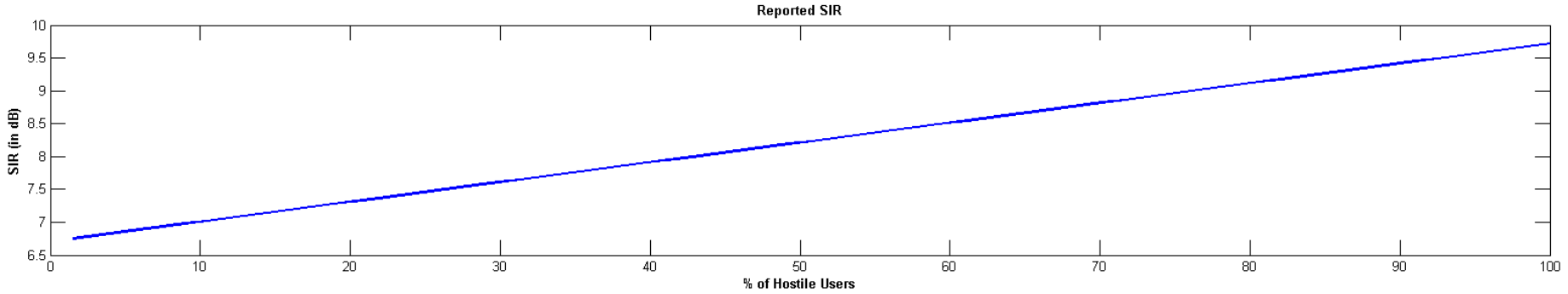


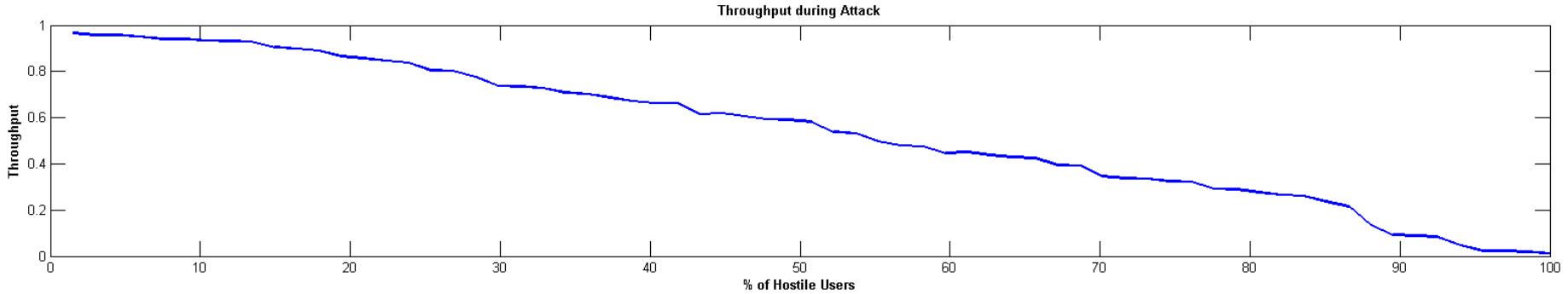
*Detection Band = mean ± 'M' * standard deviation*

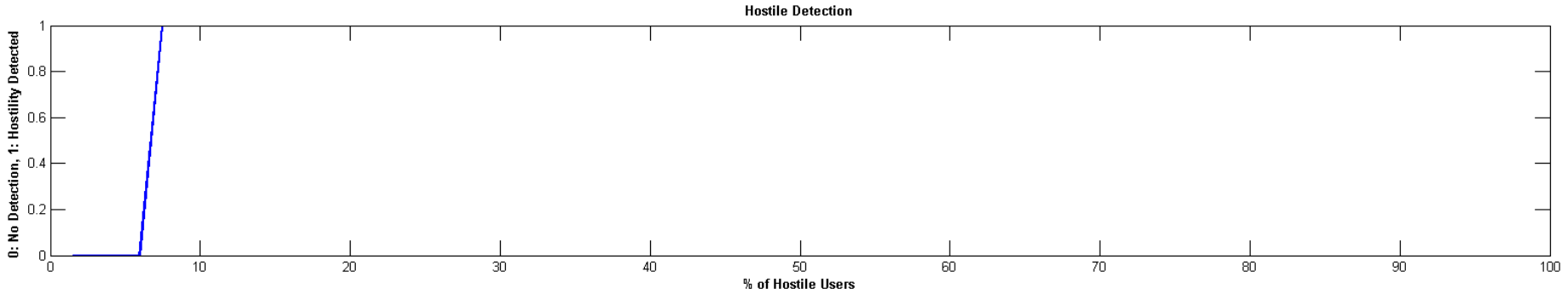


Comparison of 'Threshold' and 'Band' approaches

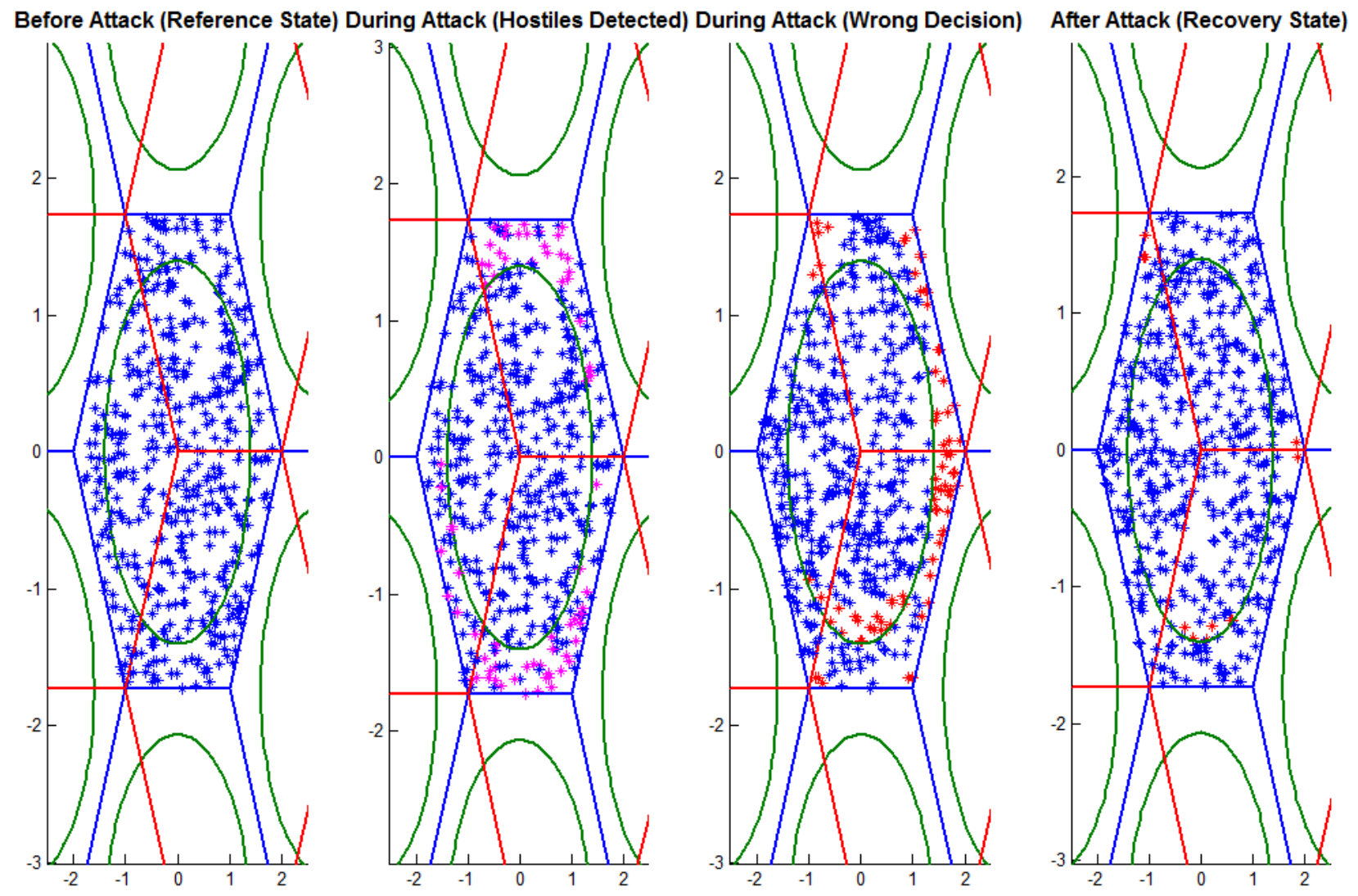
Simulation Results: Response Time



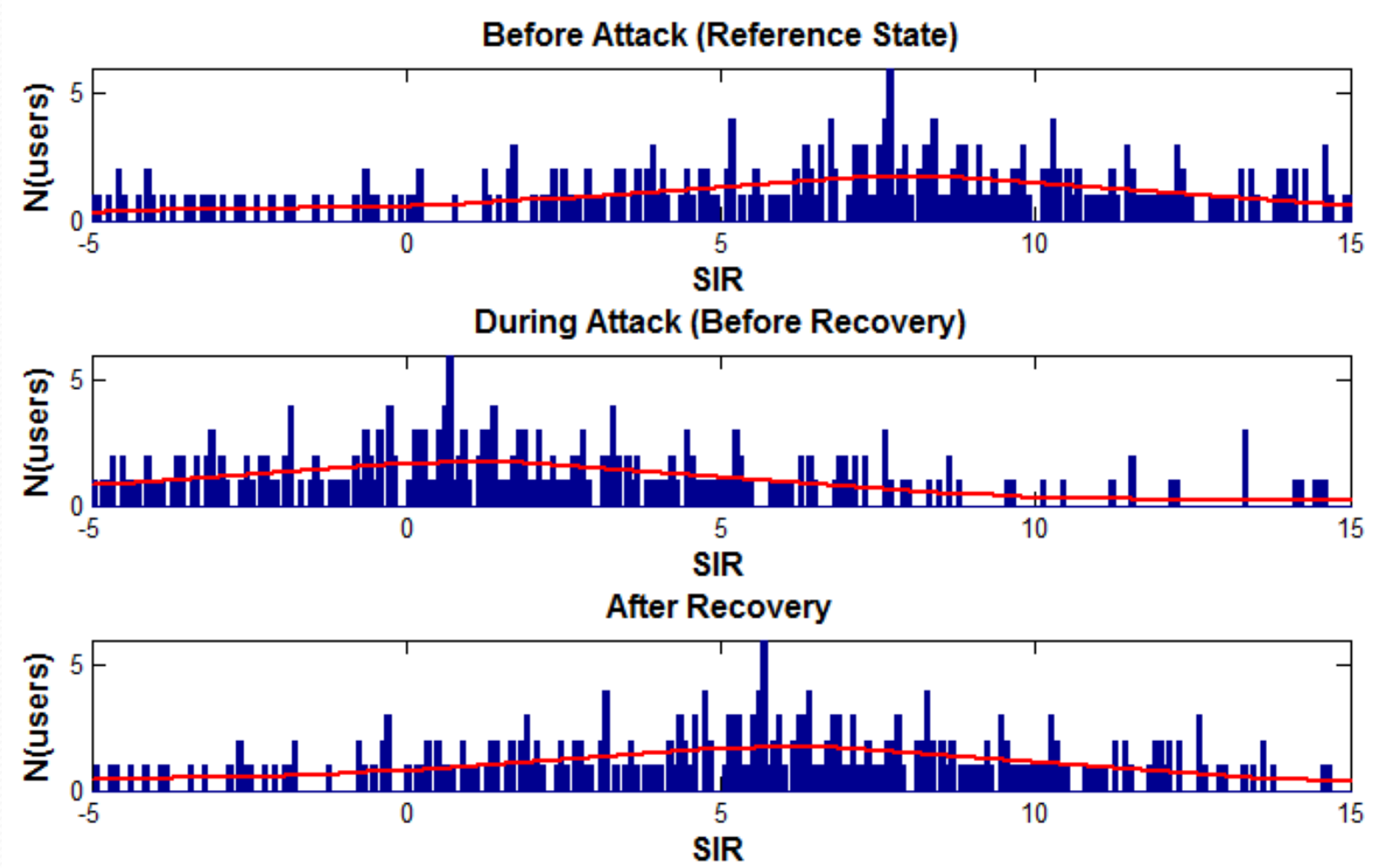




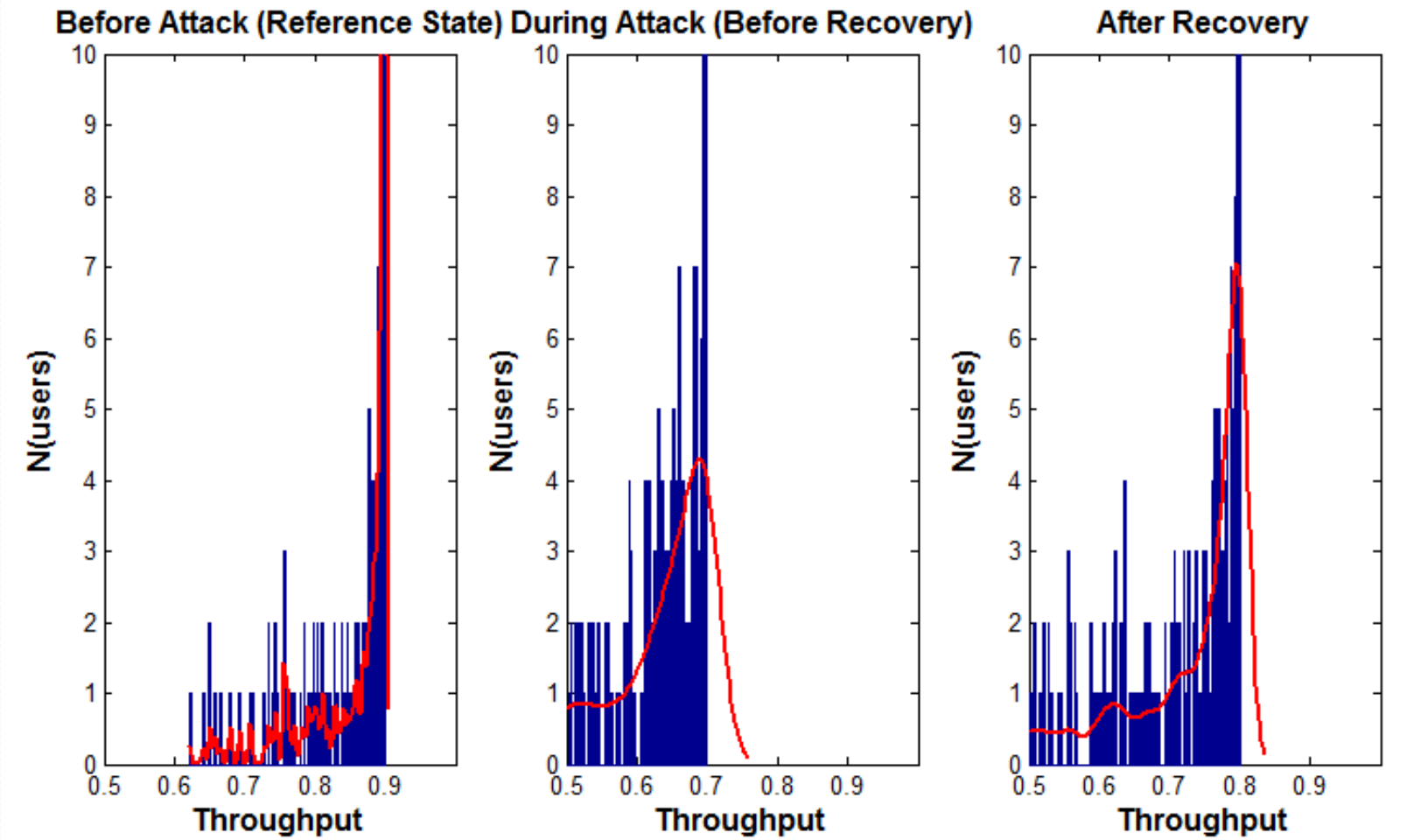
Simulation Results: System Performance



Simulation Results: System Performance (SIR)



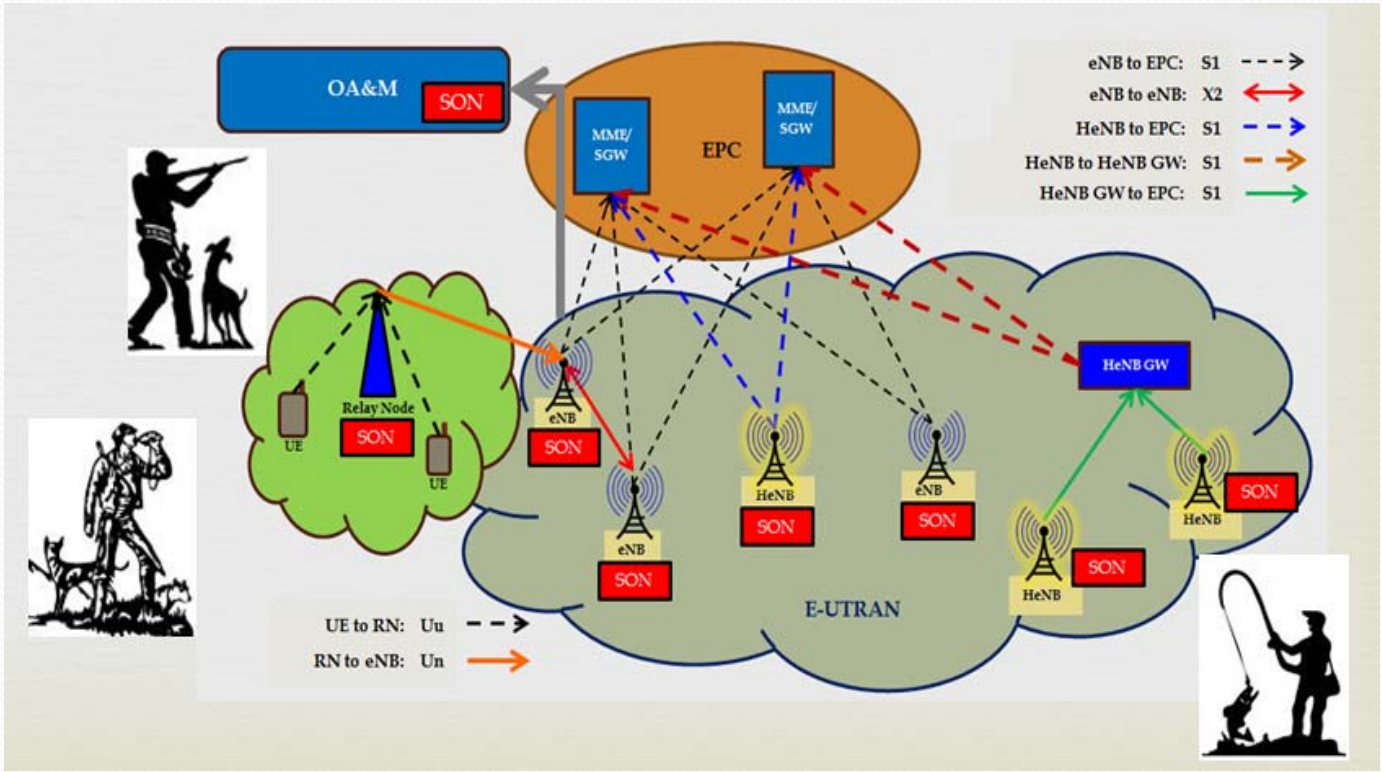
Simulation Results: System Performance (Throughput of the cell-edge users)



Summary and Conclusion

- This initial work presents security aspect of SON
  - Point of vulnerabilities for intrusion and Possible security threats
  - Simple analysis of one SON use case (ICIC) to justify the initiative.
- Future work might include
  - Extend the current work to other SON use cases
  - Theoretical analysis of SON vulnerabilities
  - Response time/recovery time analysis
  - Explore other possible counter measures
- To realize the potential of SON, it is important to
  - Address the security concerns of SON
  - Consider security aspect in the development and implementation phase of SON algorithms

Thank You


OA&M
SON
MME/
SGW
EPC
MME/
SGW
eNB to EPC: S1
eNB to eNB: X2
HeNB to EPC: S1
HeNB to HeNB GW: S1
HeNB GW to EPC: S1
HeNB GW
Relay Node
SON
UE
UE
eNB
SON
eNB
SON
HeNB
SON
eNB
SON
HeNB
SON
HeNB
SON
SON
E-UTRAN
UE to RN: Uu
RN to eNB: Un