Combating Insider Attacks in IEEE 802.11 Wireless Networks with Broadcast Encryption

Joseph Soryal, Irippuge Milinda Perera, Ihab Darwish,
Nelly Fazio, Rosario Gennaro, Tarek Saadawi

The City University of New York

AINA 2014

Outline

① Motivation

② Attack Impact

③ Our Solution

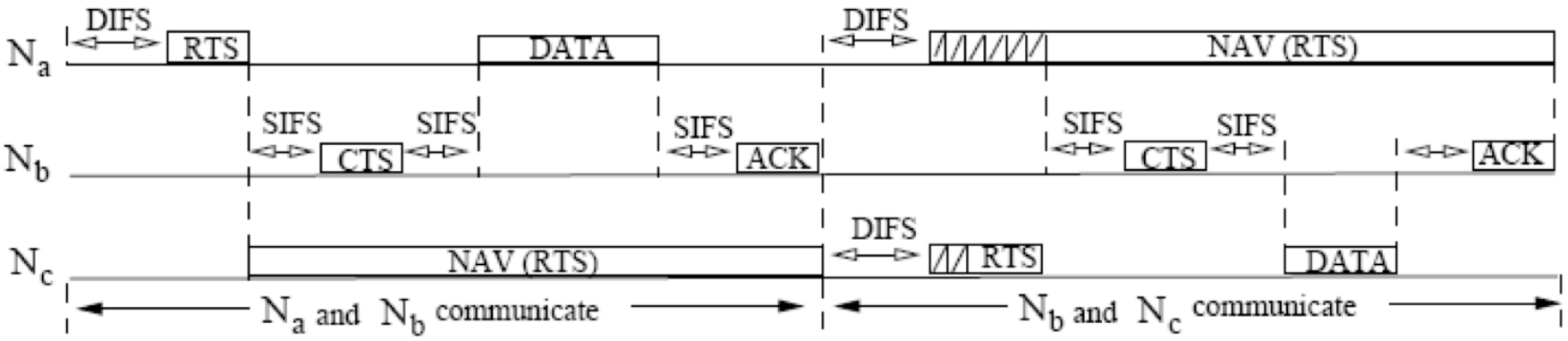
④ Simulation Results

⑤ Summary and Future Work

① Motivation

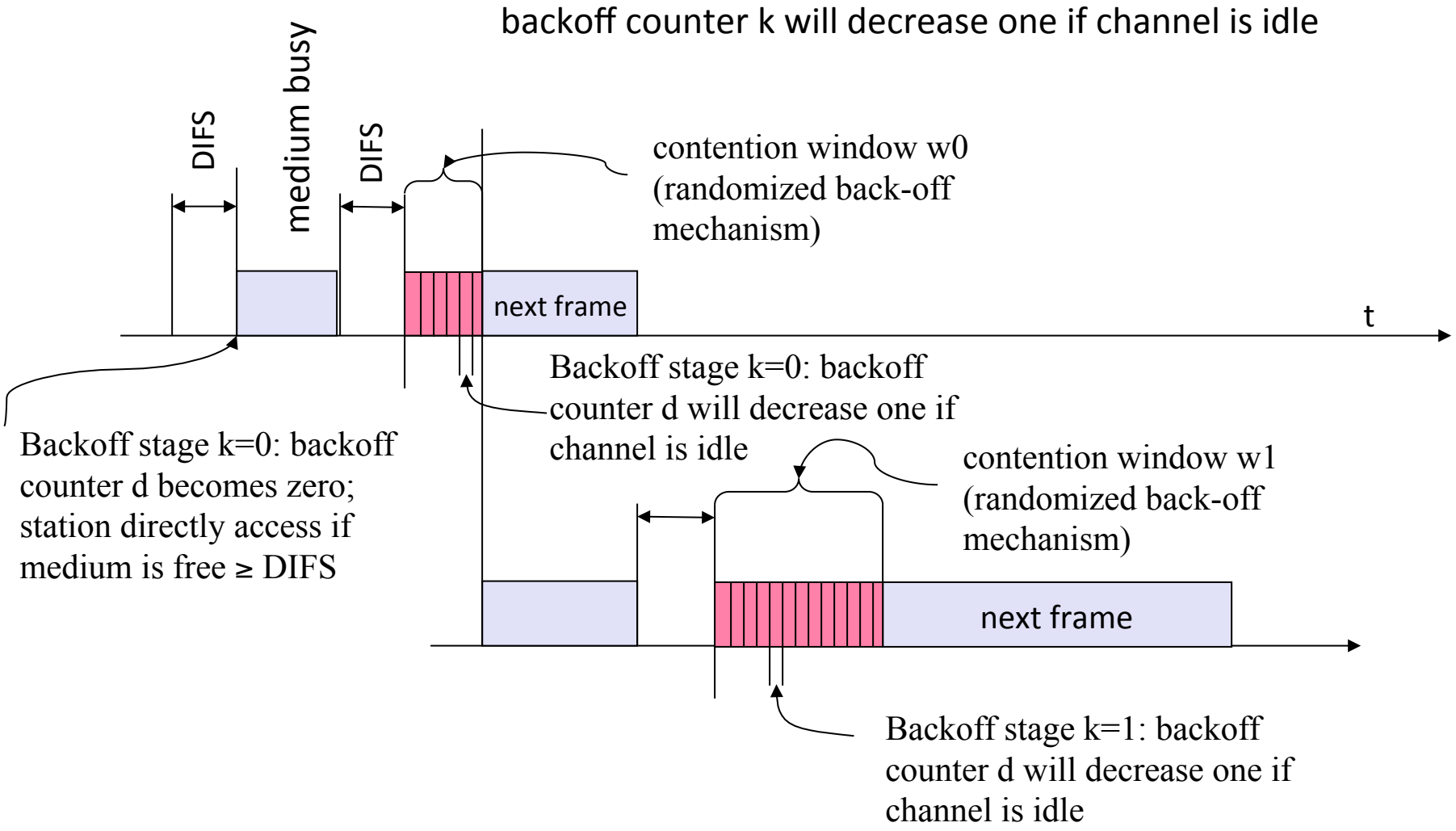
IEEE 802.11 Wireless Networks

- Shared wireless medium → inevitable collisions
- Request-to-Send/Clear-to-Send (RTS-CTS) protocol preserves fairness



- Nodes expected to follow Binary Exponential Back-off (BEB) algorithm in case of collision

IEEE 802.11 Wireless Networks



Insider Attack in IEEE 802.11 Wireless Networks

- Manipulating the Back-off Timer in the MAC layer for IEEE 802.11 can be done by a malicious user to achieve the following:

1. A legitimate user that wants to illegally increase his own throughput on the expense of other honest nodes. (Greedy User)
   - Example: a WiFi user in a café.

2. An attacker (malicious user) that wants to disrupt the whole network and prevent legitimate users from utilizing the available resources (Bandwidth) and drain their internal resources (Power, CPU usage, etc.) – DoS attack

- In this case the attacker will disrupt the network's performance and will go undetected. Intelligent attackers will follow the MAC protocol (RTS - CTS - ACK) and will appear to be legitimate node

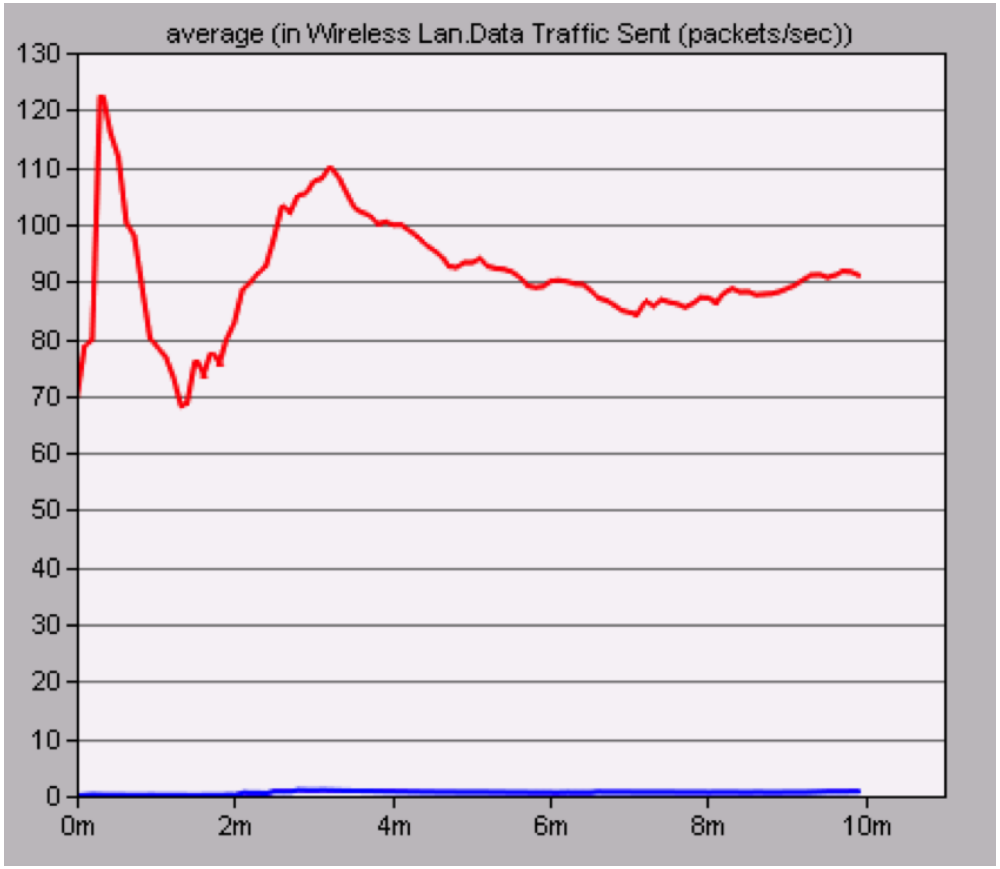
Insider Attack in IEEE 802.11 Wireless Networks

3. An untrusted vendor might manufacture NIC cards violating the MAC protocol to create an improved performance of their products

4. Most of the security researches focus on networks that have centralized coordination (i.e., Access Point scheme), but few take the challenge to investigate security issues in distributed environment.

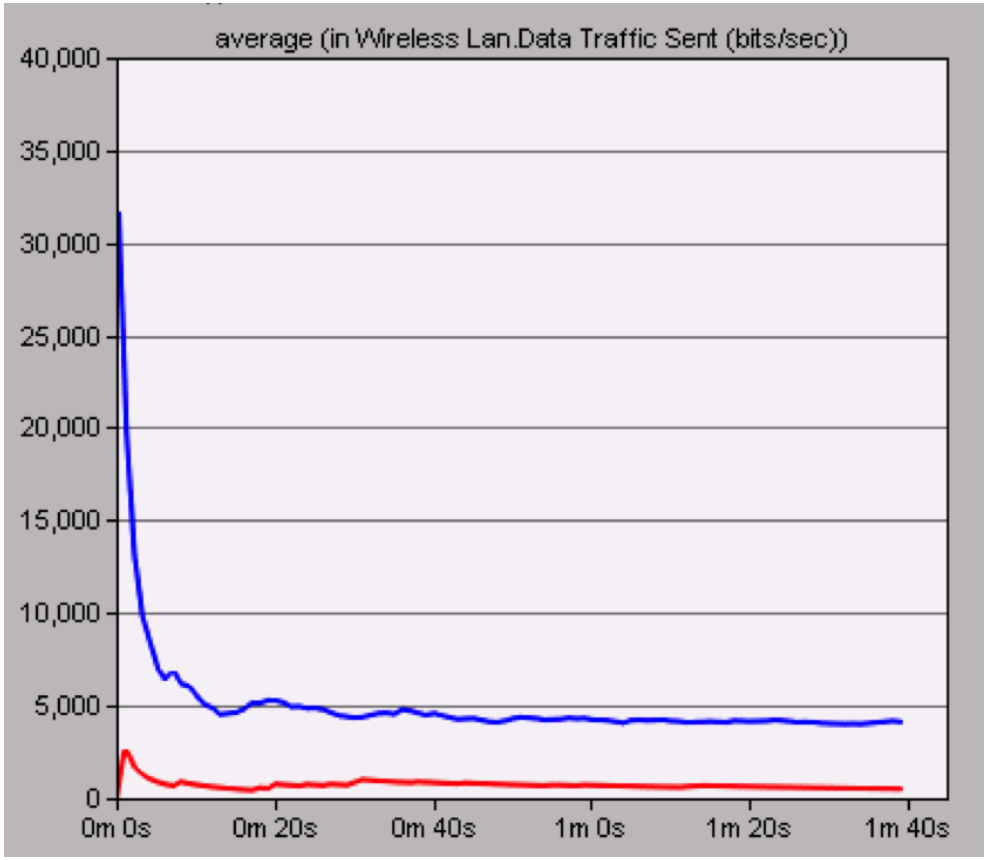
② Attack Impact

Attack Impact



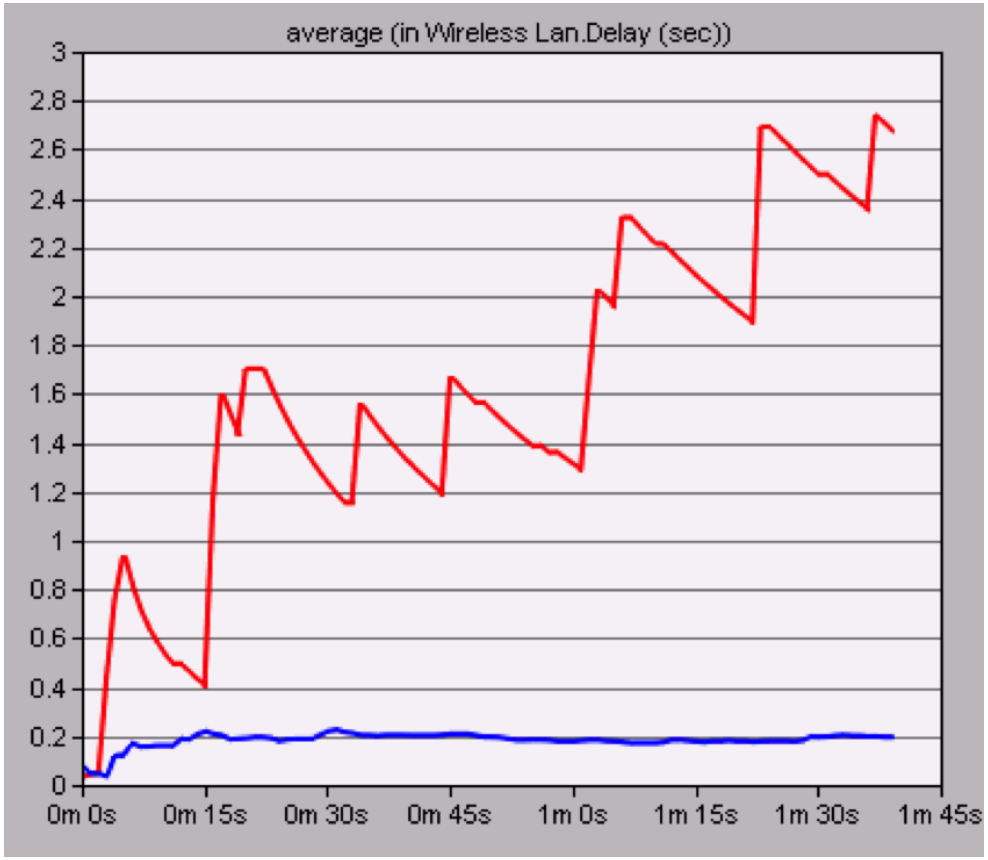
Traffic Sent (packets/second) by a node when following the standards (blue) vs. when mounting the attack (red)

Attack Impact (cont.)



Traffic Sent (bits/second) by an honest node under normal conditions (blue) vs. when an attacker is present (red)

Attack Impact (cont.)



Packet transmission delay (seconds) under normal conditions (blue) vs. when an attacker is present (red)

③ Our Solution

Goals

1. To Detect the Attacker node under saturation condition:
   - ✧ Applying Markov Chain to analyze the behavior of the MAC Layer and obtain theoretical results
   - ✧ Utilize the theoretical results as a baseline for detection threshold

2. To Mitigate the impact of the attack:
   - ✧ The Network has to recover with minimal impact
   - ✧ The attacker should continue to have the impression that the attack is still carried on.
   - ✧ Using multiple Asymmetric Broadcast Encryption techniques to exchange control information to exclude the attacker.

3. Compare the Mitigation results techniques (Series (Chain Method) Vs Broadcast Encryption techniques)

Detection Phase (Using Markov Chain Analysis)

$b_{j,k}$: stationary distribution probability of being in state (j,k), $j \in [0,L]$ is the backoff stage $k \in [0, w_j - 1]$ is the backoff counter

$b_{0,k,e}$: probability of being in stationary distribution of state $(0,k,e)$, when a transmission is completed, but has no packet waiting in the transmission queue

w_j: contention window size at backoff stage j.

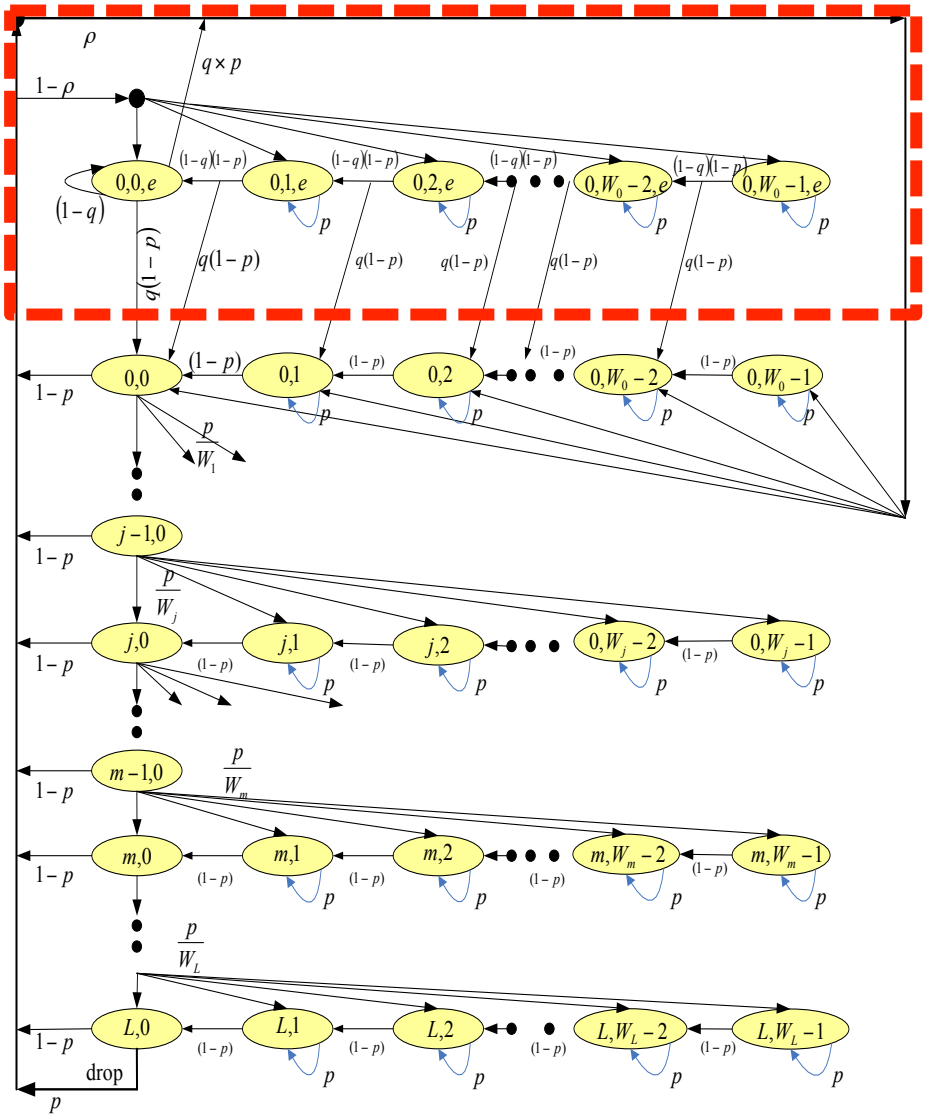
$$w_j = \begin{cases} 2^j w_0 & j \le m \\ 2^m w_0 & m < j \le L \end{cases}$$

p : probability that the node senses the channel in a random slot and finds the channel is busy.

τ : transmission probability that a node attempts to transmit a packet in a randomly chosen slot time.

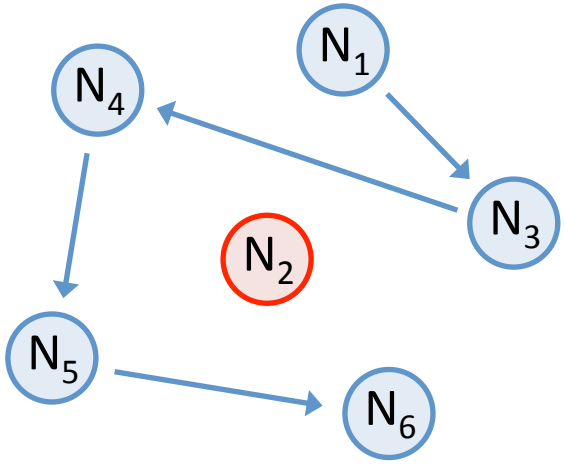
ρ : probability that there is at least one packet waiting in the transmission queue at the time when a transmission is completed.

q : probability of at least one packet waiting in the transmission queue

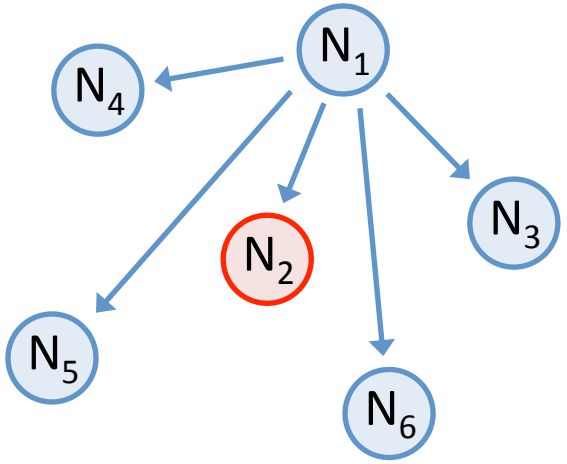


Mitigation Phase (Using Broadcast Encryption)

- Broadcast Encryption allows faster recovery after attack



Chain Method



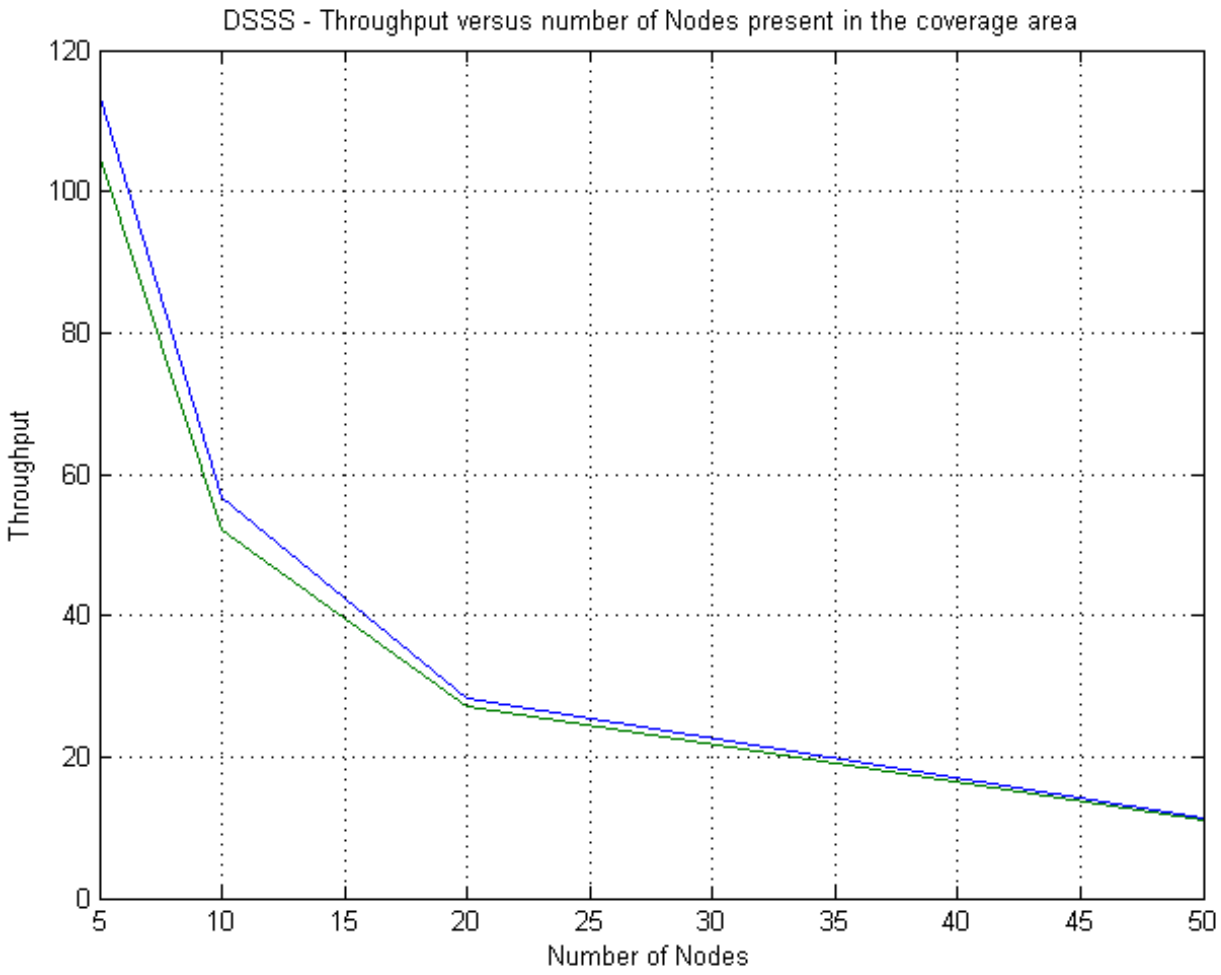
Broadcast Method

④ Simulation Results

Theoretical Results Vs. Simulation

- Three IEEE 802.11 technologies were studied
- IEEE 802.11a – IEEE 802.11b
- DSSS – OFDM

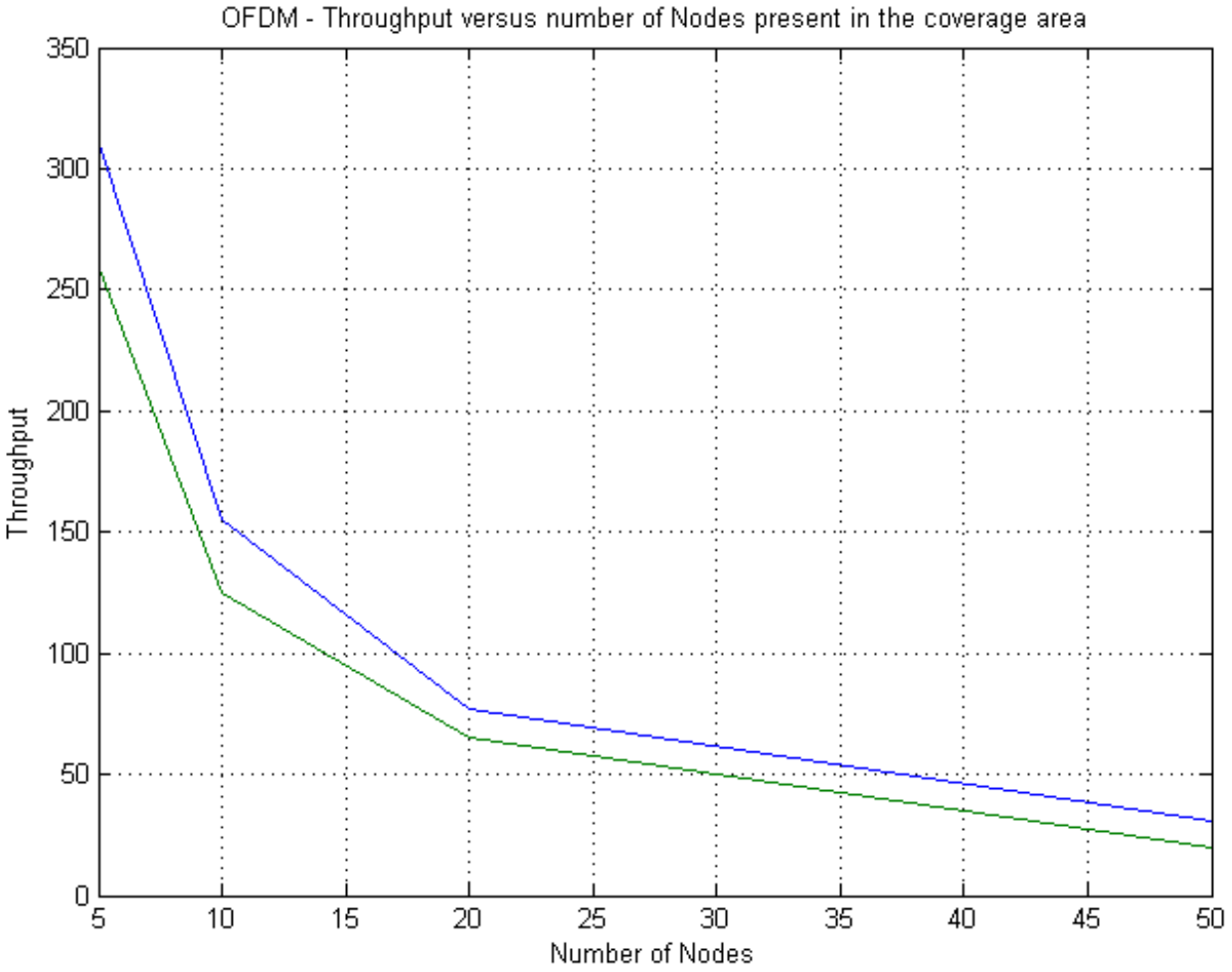
DSSS



Theoretical Throughput

Simulation Throughput

OFDM



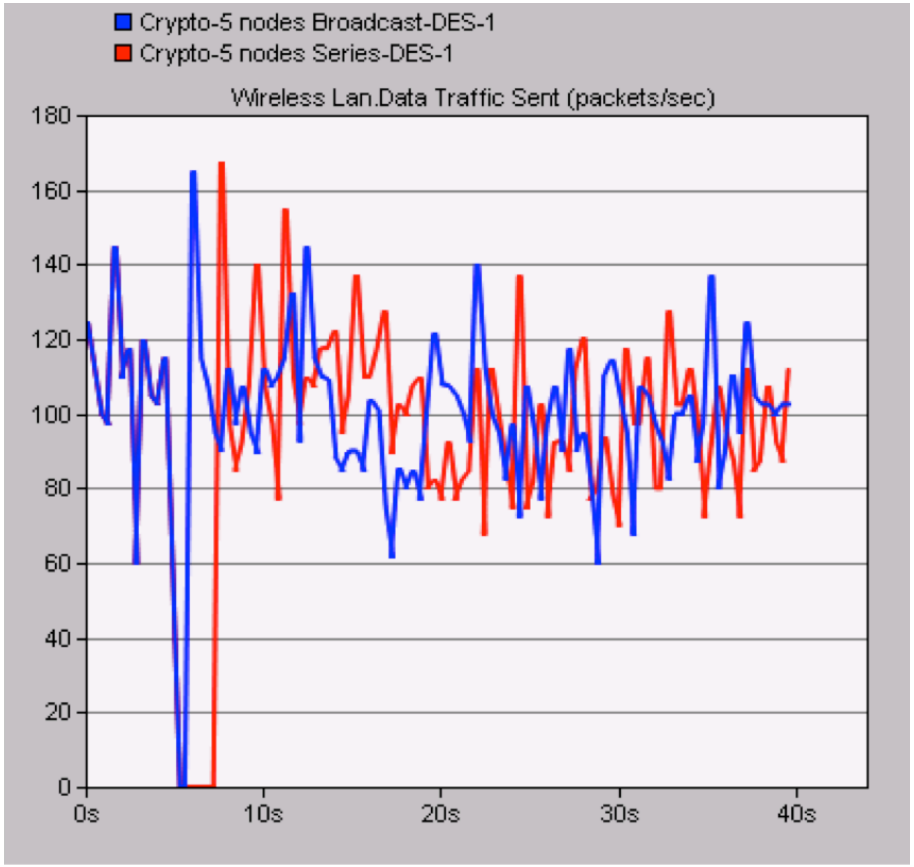
Theoretical Throughput

Simulation Throughput

OPNET Simulation

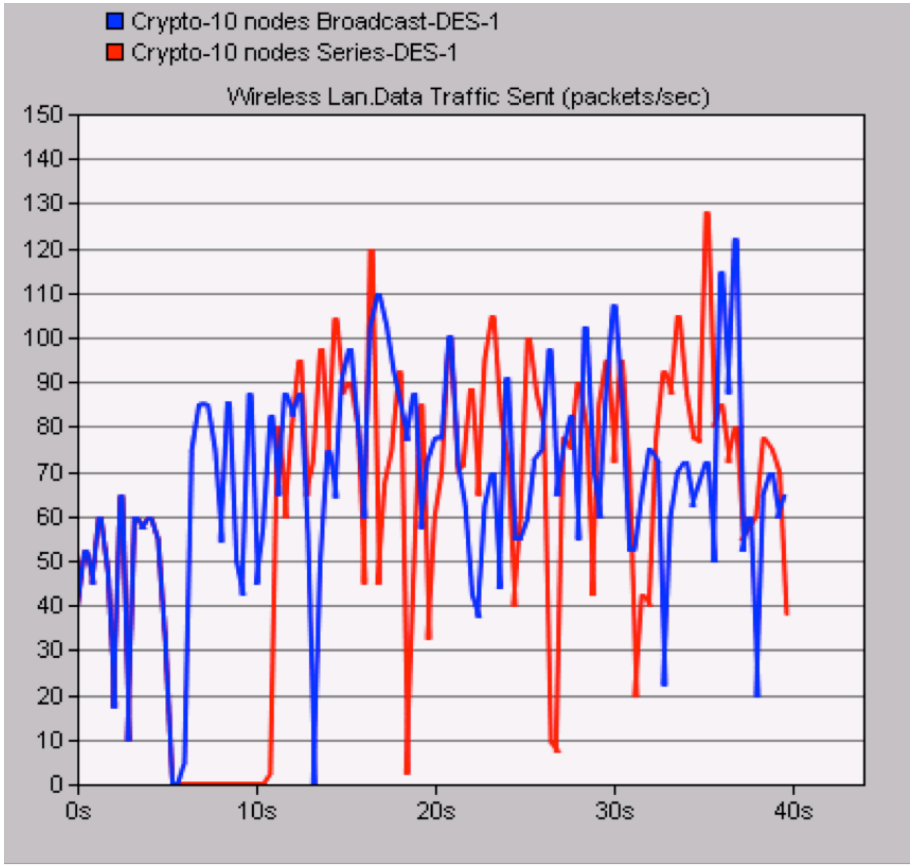
- Models in the OPNET Simulator was developed to validate the algorithms:
  - Attacker Model was created.
  - Markov Chain function was embedded into the MAC layer in a Mobile workstation (IEEE 802.11) via Matlab link.
  - Mobile workstation (IEEE 802.11) was modified to perform the detection.
  - Mobile workstation (IEEE 802.11) was modified to perform the channel hopping via controlling the PHY layer.

Simulation Results



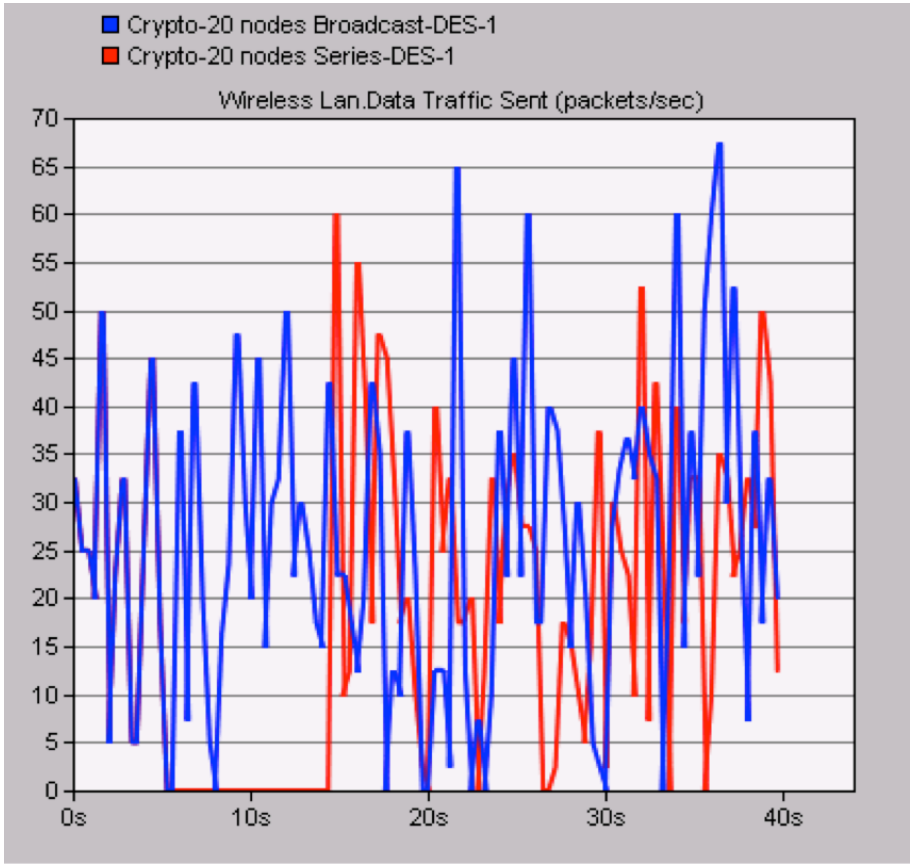
Traffic Sent (packets/second) using DSSS for 5 nodes in chain method (red line) vs. broadcast method (blue line).

Simulation Results



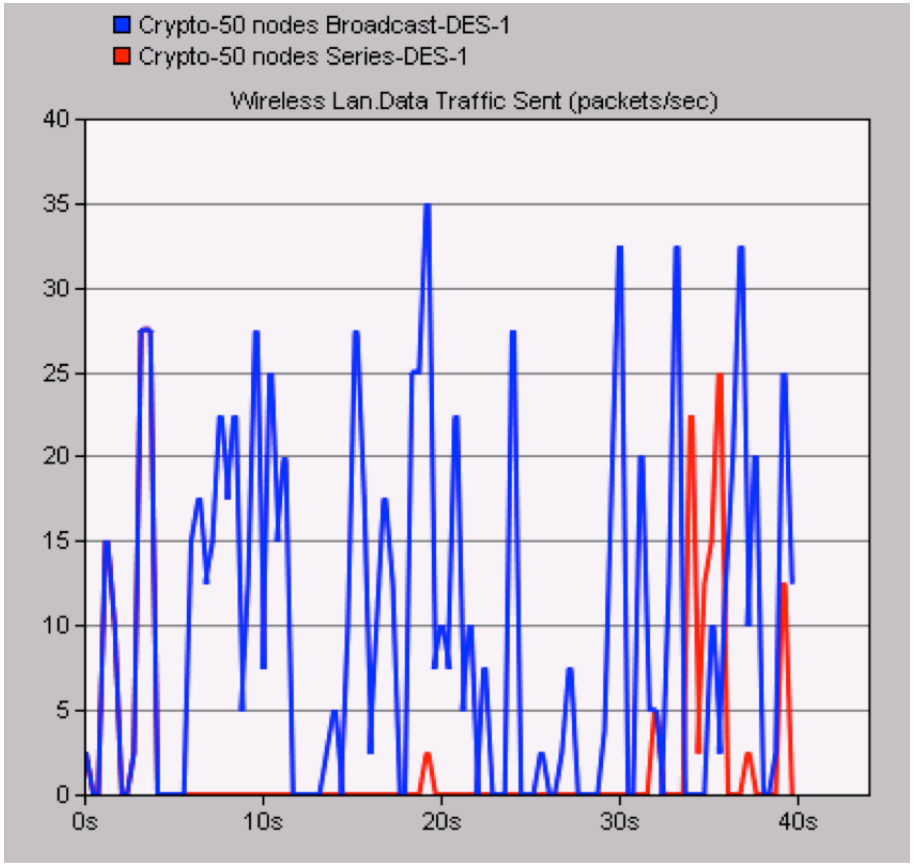
Traffic Sent (packets/second) using DSSS for 10 nodes in chain method (red line) vs. broadcast method (blue line).

Simulation Results



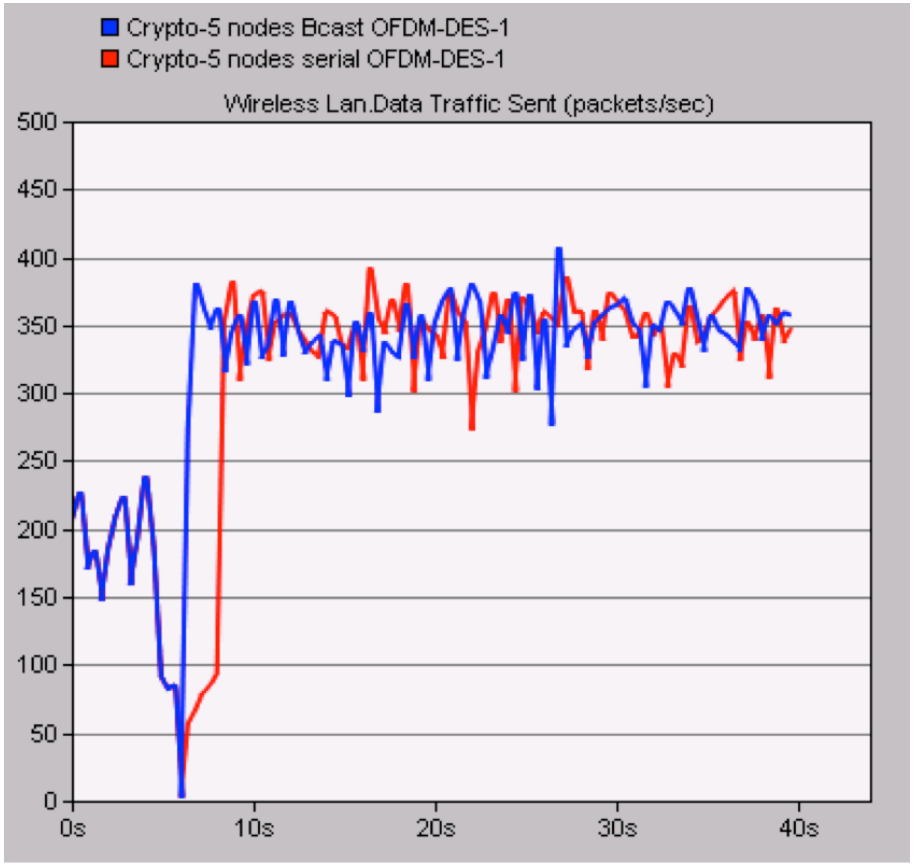
Traffic Sent (packets/second) using DSSS for 20 nodes in chain method (red line) vs. broadcast method (blue line).

Simulation Results



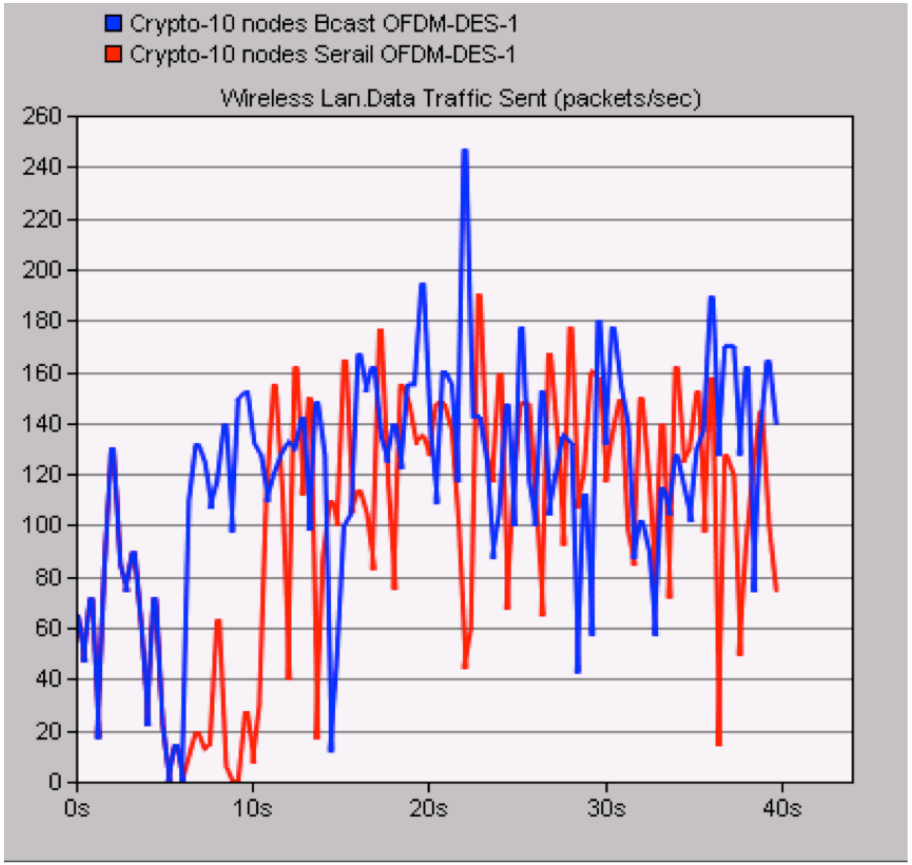
Traffic Sent (packets/second) using DSSS for 50 nodes in chain method (red line) vs. broadcast method (blue line).

Simulation Results



Traffic Sent (packets/second) using OFDM for 5 nodes in chain method (red line) vs. broadcast method (blue line).

Simulation Results



Traffic Sent (packets/second) using OFDM for 10 nodes in chain method (red line) vs. broadcast method (blue line).

⑤ Summary and Future Work

Summary

- The Broadcast Encryption technique outperformed the Series (Chain Method) technique.
- We have presented a Detection and Mitigation technique to detect Attacker nodes in a distributed wireless network.
- The key contribution is using Markov Chain model to predict the behavior of the network under saturation and using Broadcast Encryption to implement the mitigation technique.
- The Algorithm is fully distributed and scalable.

Future Work

- Explore Game Theoretic approaches to better model the network under attacks and develop more resilient architectures to reduce the impact on the network

Thank You!