Resilience of LTE Networks against Smart Jamming Attacks

Farhan Aziz, Jeff Shamma & Gordon Stuber
School of Electrical & Computer Engineering
Georgia Institute of Technology, Atlanta, GA

2014 ARO-MURI Cyber Situation Awareness Review
University of California at Santa Barbara,
November 19, 2014
Real World Enterprise Network

Mission

Sensor Alerts

Correlation Engine

Impact Analysis

Data

Data

Data

Create semantically-rich view of cyber-mission status

Mission Model

Cyber-Assets Model

Cyber-Assets

Analysis to get up-to-date view of cyber-assets

Analysis to determine dependencies between assets and missions

Simulation/Live Security Exercises

COAs

Predict Future Actions

Analyze and Characterize Attackers

Data

Real World Enterprise Network
BACKGROUND:
How does an LTE Subscriber (UE) get access to the network (eNB)?

*LTE is a commercial WWAN standard but has been lately suggested to be used for Critical Infrastructure like Public Safety and Smart Grid communications!!!
Subscriber’s Initial Acquisition Procedure

- Switched On
  - Searches for strong cell
- Acquires PSS
- Acquires SSS
  - Exact carrier freq, cell ID index, subframe timing, CP
  - Frame timing, physical Cell ID
- Reads PBCH
  - MIB (BW, SFN, PHICH config)
- Reads PDSCH
  - SIB 1 (cell suitability, PLMN, cell access info, SIB scheduling) & SIB 2 (paging, PRACH, BCCH, PDSCH, PUSCH, PUCCH scheduling)

An LTE network is composed of multiple Control and Data Channels, each designed to perform a specific task/service.

Every UE has to follow a specific sequential procedure to access the network or get (or send) user data!

Sends Attach Request on PRACH/PUCCH

Vulnerable to Smart Jamming attacks
Subscriber’s DL/UL Data Transfer Procedure

Decodes PCFICH every subframe

PDCCH-config

Decodes PDCCH every subframe

DCI & PDSCH DL/UL Resource Assignments

UE decodes DL data

Sends UL data, BSR and PHR on PUSCH

Initial access and UL sync request

Sends UCI on PUCCH/PRACH

eNB sends UL resource assignments on PDCCH

UE gets UL resource assignments

eNB Sends UL data ACK/NAK on PHICH

eNB decodes UL data

Vulnerable to Smart Jamming attacks

Random Access on PRACH

Sends DL data ACK/NAK on PUCCH/PUSCH
SMART JAMMING ATTACKS & COUNTERMEASURES

*Smart jammer* can be easily implemented with the help of an *LTE-UE* or SDR like *USRP*, and can jam specific *Channels* unlike a *barrage jammer*, without any need to hack the network or *attach* to it!!!
# Some Possible Jamming Actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Possible Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inactive</td>
<td>When jamming is not played for detection avoidance or other purposes.</td>
</tr>
<tr>
<td>Jam DL-RS</td>
<td>Affects both Idle and Connected mode UEs - may prevent users from demodulating data channels, degrade cell quality measurements for reselection and handover, and block initial cell acquisition.</td>
</tr>
<tr>
<td>Jam DL-RS + PUCCH</td>
<td>PUCCH jamming may cause eNB to lose track of critical feedback information from UEs, which in turn affects both DL and UL active data sessions.</td>
</tr>
<tr>
<td>Jam DL-RS + PBCH + PRACH</td>
<td>All incoming UEs may be blocked and Idle mode UEs may not be able to transition to Connected state.</td>
</tr>
<tr>
<td>Jam DL-RS + PCFICH + PUCCH + PRACH</td>
<td>All DL and UL resource grants may be lost caused by PCFICH jamming, in addition to effects of DL-RS, PUCCH and PRACH jamming</td>
</tr>
</tbody>
</table>

*Smart Jammer* focuses its limited power and resources to jam specific *critical Control Channels* to disrupt a number of services and functionalities offered by the network.
# Suggested Network Countermeasures

<table>
<thead>
<tr>
<th>Action</th>
<th>Possible Remedy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td>Default action – corresponds to regular operation of the network when jamming is not detected. Co-channel interference is managed by the network automatically.</td>
</tr>
<tr>
<td>Increase DL-RS Tx Power</td>
<td>May alleviate DL-RS jamming effects at the expense of lower Tx power for remaining channels.</td>
</tr>
<tr>
<td>Throttling</td>
<td>Throttling of all UEs’ throughput in fear of jamming – may be used as a threat or jamming test mechanism.</td>
</tr>
<tr>
<td>Carrier f + SIB 2 Change</td>
<td>Interference avoidance mechanism by “relocating” eNB’s center frequency (hence PSS/SSS and PBCH) to a different frequency and moving all of active data sessions to different channels chosen randomly within occupied BW (e.g. a 20 MHz network can transform itself into 15 MHz or less) – this may avoid Control Channels jamming. Changing SIB 2 parameters may avoid PRACH jamming.</td>
</tr>
<tr>
<td>Timing Change</td>
<td>Interference avoidance mechanism by “rebooting” frame/subframe/slot/symbol timing. This may help alleviate Control Channels jamming by moving it to Data Channels i.e. PDSCH and PUSCH. Active data sessions need to be handed over to neighboring cells for this transition.</td>
</tr>
</tbody>
</table>

**Countermeasures** are based on *Pilot boosting, threat mechanism* or *Interference avoidance* to (possibly) alleviate certain jamming effects.

Until now, *jamming* is dealt by physical *neutralization* of the jammer.
Game-Theoretic Framework

- Two Jammer Types:
  - Cheater
    - Jams the network with the intent of getting more resources for itself as a result of reduced competition among UEs
    - A *Cheating UE* is always present in the network with an active data session
  - Saboteur
    - Jams the network with the intent of causing highest possible damage to the network’s utility
    - *Sabotaging UE* does not have any interest in getting more network resource and may not even have an active data session

- Modeled as matrix games with eNB as the row player and jammer as the column player

- *eNB Utility*: *Weighted* linear function of *normalized averages* of the following as compared to baseline jamming-free scenario:
  - Overall throughput
  - Number of active users
  - DL-RS SINR difference
  - PUCCH SINR difference
  - PRACH failure rate

- *Fixed Cost* associated with a particular eNB action

*Jammer type* is based on its intent and capabilities. *Utility* is a function of performance metrics.
SINGLE-SHOT vs. REPEATED GAMES

Non-zero-sum games – both players are utility maximizers.
### Single-Shot Games Simulation Results

#### eNB vs. Cheater

<table>
<thead>
<tr>
<th>Strategy</th>
<th>eNB</th>
<th>Cheater</th>
<th>eNB vs. Cheater</th>
<th>eNB vs. Cheater</th>
<th>eNB vs. Cheater</th>
</tr>
</thead>
<tbody>
<tr>
<td>0,0</td>
<td>-190,10</td>
<td>-526,260</td>
<td>-180,3</td>
<td>-520,260</td>
<td></td>
</tr>
<tr>
<td>-4,-14</td>
<td>-180,3</td>
<td>-528,245</td>
<td>-172,15</td>
<td>-526,251</td>
<td></td>
</tr>
<tr>
<td>-431,-431</td>
<td>-642,-431</td>
<td>-1118,-443</td>
<td>-629,-441</td>
<td>-1116,-442</td>
<td></td>
</tr>
<tr>
<td>-84,-57</td>
<td>-282,-47</td>
<td>-620,199</td>
<td>-273,-59</td>
<td>-618,199</td>
<td></td>
</tr>
<tr>
<td>-80,0</td>
<td>-270,10</td>
<td>-606,260</td>
<td>-260,-3</td>
<td>-600,260</td>
<td></td>
</tr>
</tbody>
</table>

#### eNB vs. Saboteur

<table>
<thead>
<tr>
<th>Strategy</th>
<th>eNB</th>
<th>Saboteur</th>
<th>eNB vs. Saboteur</th>
<th>eNB vs. Saboteur</th>
<th>eNB vs. Saboteur</th>
</tr>
</thead>
<tbody>
<tr>
<td>0,0</td>
<td>-193,40</td>
<td>-539,226</td>
<td>-183,22</td>
<td>-532,220</td>
<td></td>
</tr>
<tr>
<td>-4,14</td>
<td>-182,39</td>
<td>-541,238</td>
<td>-175,24</td>
<td>-539,236</td>
<td></td>
</tr>
<tr>
<td>-431,431</td>
<td>-646,492</td>
<td>-1134,821</td>
<td>-633,471</td>
<td>-1132,820</td>
<td></td>
</tr>
<tr>
<td>-84,57</td>
<td>-88,53</td>
<td>-88,35</td>
<td>-91,45</td>
<td>-88,36</td>
<td></td>
</tr>
<tr>
<td>-80,0</td>
<td>-84,-3</td>
<td>-83,22</td>
<td>-87,-11</td>
<td>-84,-21</td>
<td></td>
</tr>
</tbody>
</table>

*eNB utility* is severely compromised at *NE* and *Strategy* may depend on both the *Jammer type* and its actions.
At most only one type of Jammer is present in the network – no mixed or dual personality types. Robust performance in our simulations.
Proposed Network Strategy Algorithm for Repeated Bayesian Game

Incomplete and asymmetric information about opponent’s state and actions. eNB triggers Jammer type determination algorithm if it senses jamming and plays according to its estimate.
**Proposed Cheater and Saboteur Strategy Algorithms for Repeated Bayesian Games**

**Cheater** can follow network timing and re-direction but **Saboteur** cannot, hence **Cheater** might be able to estimate network actions more reliably. **Saboteur** keeps re-synchronizing itself with the network periodically to launch jamming attacks effectively.
Repeated Game’s Simulation Results

- **Simulation Parameters:**
  - Prob. of Cheater’s occurrence: 9.33%
  - Prob. of Saboteur’s occurrence: 5.67%
  - Other parameters are the same as single-shot games.

- **Repeated Game Utility Results:**
  - eNB Utility: -23.2
  - Cheater’s Utility: 466.2
  - Saboteur’s Utility: -511.3

- **eNB Utility Improvement over Single-shot games:**
  - **Relative Utility Improvement:** 57%

Network may recover most of its performance loss in *Repeated game* using our proposed algorithms and may even force an adversary to retract!!!
Conclusions

- LTE networks are vulnerable to Denial-of-Service (DOS) and loss of service attacks from smart jammers.
- *Smart jammers* can launch network-wide jamming attacks without hacking the network or using excessive Tx power or jamming BW.
- Network may suffer huge performance loss and may not be able to recover itself using current protocols.
- Network’s strategy depends both on the *jammer type* and its actions.
- Our proposed repeated game learning and strategy algorithm can help the network recover most of its performance loss and may even force an adversary to retract!!!
Thank you!!!

Questions?
BACKUP
INTRODUCTION TO LTE
What is LTE/LTE-A?

- 3GPP’s evolution path towards 4G (4th Generation) Wireless Wide Area Networks (WWANs)
- LTE: (UMTS) Long Term Evolution
- LTE-A: LTE-Advanced

Key Benefits:
- Higher peak data rates (DL ~300 Mbps, UL ~ 75 Mbps)
- Improved end-user throughput
- Reduced latency
- Scalable bandwidth
- FDD/TDD options
- Economies of scale
- Easier roaming
- Worldwide availability of devices, infrastructure and test equipment
- Flat All-IP network architecture
LTE Air Interface

- **Downlink (DL) Waveform:** OFDMA
- **Uplink (UL) Waveform:** SC-FDMA
- **Flexible Bandwidth Support:** 1.4 – 20 MHz (single-carrier)
- **Air Interface Nodes:**
  - eNB: Evolved Node B (radio network)
  - UE: User Equipment (end user)
- **Spectrum Versatility:**
  - Frequency Division Duplex (FDD)
  - Time Division Duplex (TDD)
  - Half-Duplex
- **DL/UL MIMO Support**
  - Single (and same) communication link for DL and UL
  - Hard handover-based mobility
  - QPSK, 16-QAM and 64-QAM data modulation schemes
  - System Information (SI) is broadcasted in Master Information Block (MIB) and System Information Blocks (SIBs)
Frequency-domain Organization

- Subcarrier spacing: 15 KHz (Normal Operation)
- 1 Resource block (RB): 12 subcarriers = 180 KHz
- Channel BW and corresponding RBs:

<table>
<thead>
<tr>
<th>Channel BW</th>
<th>1.4 MHz</th>
<th>3 MHz</th>
<th>5 MHz</th>
<th>10 MHz</th>
<th>15 MHz</th>
<th>20 MHz</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Subcarriers</td>
<td>73</td>
<td>181</td>
<td>301</td>
<td>601</td>
<td>901</td>
<td>1201</td>
</tr>
<tr>
<td>Number of RBs</td>
<td>6</td>
<td>15</td>
<td>25</td>
<td>50</td>
<td>75</td>
<td>100</td>
</tr>
</tbody>
</table>
Time-domain Organization (FDD)

- Radio Frame: 10 ms
- Half Radio Frame: 5 ms
- Subframe: 1 ms
- Slot: 0.5 ms
- OFDM Symbols/slot: 7 (Normal CP)
- Basic Unit of Time Ts: 32.55 ns
- Resource Element (RE): 1 subcarrier x 1 symbol
  - Smallest time-frequency resource unit
- Resource Block (RB): 12 subcarriers x 1 slot
  - Time-frequency resource unit for user scheduling
Time-Frequency Resource Grid

1 subcarrier = 15 KHz
1 slot = 0.5 ms
### DL Channels & Signals

<table>
<thead>
<tr>
<th>Channel/Signal</th>
<th>Acronym</th>
<th>Type</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary/Secondary Synchronization Signals</td>
<td>PSS/SSS</td>
<td>Sync. Signal</td>
<td>Time/frequency synchronization, unique Cell ID</td>
</tr>
<tr>
<td>Physical Broadcast Channel</td>
<td>PBCH</td>
<td>Physical</td>
<td>MIB (DL BW, PHICH config, SFN, Tx antennas)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Channel</td>
<td></td>
</tr>
<tr>
<td>Downlink Reference Signals</td>
<td>DL-RS</td>
<td>Physical</td>
<td>DL channel estimation for coherent demodulation, DL signal strength</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Signal</td>
<td>measurements</td>
</tr>
<tr>
<td>Physical Control Format Indicator Channel</td>
<td>PCFICH</td>
<td>Control</td>
<td>Control Format Information (CFI) for control channel region</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Channel</td>
<td></td>
</tr>
<tr>
<td>Physical Downlink Control Channel</td>
<td>PDCCH</td>
<td>Control</td>
<td>DL/UL resource allocation, DL Control Information (DCI)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Channel</td>
<td></td>
</tr>
<tr>
<td>Physical Hybrid ARQ Indicator Channel</td>
<td>PHICH</td>
<td>Control</td>
<td>HARQ ACK/NAK for UL data transmission</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Channel</td>
<td></td>
</tr>
<tr>
<td>Physical Data Shared Channel</td>
<td>PDSCH</td>
<td>Data Channel</td>
<td>DL user data, SIB transmission, upper-layer signaling</td>
</tr>
</tbody>
</table>
# UL Channels & Signals

<table>
<thead>
<tr>
<th>Channel/Signal</th>
<th>Acronym</th>
<th>Type</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sounding Reference Signals</td>
<td>SRS</td>
<td>Ref. Signal</td>
<td>UL channel quality estimation independent of PUSCH/PUCCH</td>
</tr>
<tr>
<td>Demodulation Reference Signals</td>
<td>DM-RS</td>
<td>Ref. Signal</td>
<td>Coherent demodulation of PUSCH &amp; PUCCH</td>
</tr>
<tr>
<td>Physical Uplink Control Channel</td>
<td>PUCCH</td>
<td>Control Channel</td>
<td>UL Control Information (UCI) for DL/UL resource scheduling</td>
</tr>
<tr>
<td>Physical Uplink Shared Channel</td>
<td>PUSCH</td>
<td>Data Channel</td>
<td>Dedicated UL user data, UCI on UL, upper-layer signaling</td>
</tr>
<tr>
<td>Physical Random Access Channel</td>
<td>PRACH</td>
<td>Random Access</td>
<td>Random access for registration, resource requests, call setup, UL timing sync, handover, RLF recovery</td>
</tr>
</tbody>
</table>
LTE PROCEDURES & SCHEDULING
UE’s Initial Acquisition Procedure

Switched On

Searches for strong cell

Acquires PSS

Acquires SSS

Reads PBCH

Frame timing, physical Cell ID

Reads PDSCH

MIB (BW, SFN, PHICH config)

SIB 1 (cell suitability, PLMN, cell access info, SIB scheduling) & SIB 2 (paging, PRACH, BCCH, PDSCH, PUSCH, PUCCH scheduling)

Vulnerable to Smart Jamming attacks

Sends Attach Request on PRACH/PUCCH
UE’s DL/UL Data Transfer Procedure

- Decodes PCFICH every subframe
- Decodes PDCCH every subframe
- Sends DL data
- Ack/NAK on PUCCH/PUSCH
- Random Access on PRACH
- Sends UCI on PUCCH/PRACH
- Decodes PDCCH
- Sends UL data, BSR and PHR on PUSCH
- eNB Sends UL data, ACK/NAK on PHICH
- eNB decodes UL data
- UE gets UL resource assignments
- UE decodes DL data
- Initial access and UL sync request
- Sends UCI on PUCCH/PRACH
- Decodes PDCCH
- DCI & PDSCH DL/UL Resource Assignments
- vulnerable to Smart Jamming attacks
PSS/SSS  and DL PBCH Scheduling

- **PSS/SSS**
  - Time-domain:
    - Subframe # 0 and 5 of every frame
    - Last 2 OFDM symbols of slot # 0
  - Frequency-domain:
    - 6 RBs (1.08 MHz) in the middle of channel BW irrespective of overall system BW
  - Quite robust design

- **PBCH**
  - Time-domain:
    - Subframe # 0 in every frame
    - First 4 OFDM symbols of slot # 1
  - Frequency-domain:
    - 6 RBs (1.08 MHz) in the middle of channel BW
  - TTI = 40 ms (same information is repeated in 4 frames)
DL-RS Scheduling

- Antenna Ports 0 and 1:
  - Time-domain:
    - The 1st and 3rd last OFDM symbols of each slot
  - Frequency-domain:
    - 6 subcarrier spacing and 2x staggering (45 KHz frequency sampling)

- Antenna Ports 2 and 3:
  - Time-domain:
    - The 2nd OFDM symbol of each slot
  - Frequency-domain:
    - 6 subcarrier spacing with 2x staggering

- Optional Frequency-hopping:
  - Each pattern corresponds to one Cell ID group
  - Period 10 ms
DL PCFICH and DL PDCCH Scheduling

- **PCFICH**
  - **Time-domain:**
    - 1st OFDM symbol of all subframes
  - **Frequency-domain:**
    - Spans entire system BW
    - But, mapping depends on Cell ID
    - 1 REG = 4 Res

- **PDCCH**
  - Aggregation of contiguous Control Channel Elements (CCEs)
  - **CCE:**
    - Time-domain: 1 – 4 OFDM symbols/subframe
    - Frequency-domain: 9 Resource Element Groups (REGs) = 36 REs
UL PUCCH Scheduling

- **Time-domain:**
  - Spans entire subframe in which it is scheduled

- **Frequency-domain:**
  - Always mapped to the outside edges of the system BW
  - Employs frequency-hopping in consecutive slots

- Cannot be transmitted simultaneously with PUSCH
- Resources assigned by higher layers
- Multiple UEs can be assigned the same PUCCH resources
UL PRACH Scheduling

- Two types:
  - Contention-based
  - Contention-free
- Common resource
- Restricted to certain time/frequency resources
  - May or may not be present in every subframe and frame
- Each RA preamble occupies 6 consecutive RBs
  - Purely a random sequence
- Starting frequency is specified in SIB 2
- No frequency-hopping
- 64 PRACH configurations
- 4 preamble formats in FDD depending on cell size
What is A Smart Jammer?

- LTE resources (specifications, devices, test equipment, expertise etc.) are publicly/commercially available
- Any LTE-capable UE can “learn” network parameters (SIBs) and synchronize itself with the network without even sending an Attach Request!!!
- A *Smart Jammer* can jam specific parts/channels on an LTE network unlike a *barrage jammer***!!
- There is no need to hack the network or its users
- This can be implemented in SDR like USRPs as well
ENVIRONMENT MODEL
Channel Model

- **Simplified Path Loss Model:** \( P_r = P_t K d^{-\gamma} \)
  - \( P_r \) is the Received Power (in dBm)
  - \( P_t \) is the Transmitted Power (in dBm)
  - \( K(dB) = 20 \log_{10} \left( \frac{\lambda}{4\pi d_0} \right) \) is a Constant
  - \( \gamma \) is the *Path Loss Exponent* (typical values: 2.7 – 3.5 for urban microcells)

- **SINR Model:**
  \[ \Gamma = \frac{|h_0|^2 R_0^{-\gamma}}{\sigma^2 + |h_j|^2 R_j^{-\gamma}} \]
  - \(|h_0|^2\) and \(|h_j|^2\) are *exponentially-distributed channel gains* (due to small-scale *Rayleigh fading*) from desired transmitter and jammer respectively
  - \(R_0 \) and \( R_j \) are *distances* from corresponding transmitters
  - \(\sigma^2\) is the *noise variance* at each receiver
DL Data Throughput Model

- **PDSCH Data Throughput:**
  \[ T_{\text{put}} = \frac{RB_{\text{scheduled}} \log_2 (1 + \Gamma_{PDSCH})}{\Gamma_{PDSCH}} \]

- **Proportional Fair Scheduling (PFS)** is used for resource scheduler.

- It is assumed that both UE and eNB are unable to decode Control Channels below a certain **Block Error Rate (BLER)** threshold.
  - Failure to decode any critical Control Channel would result in **Radio Link Failure (RLF)**.
  - Required **SINR threshold** computation:
    - For coded channels (like PBCH, PCFICH and PUCCH) **Union Bound** and equally-likely error probability across all symbols is used.
    - For un-coded signals (like DL-RS) closed-form expression for QPSK **Symbol Error Rate (SER)** in Rayleigh fading is used.
GAME-THEORETIC MODELING
Game-Theoretic Framework

- Two Jammer Types:
  - Cheater
    - Jams the network with the intent of getting more resources for itself as a result of reduced competition among UEs
    - A *Cheating UE* is always present in the network with an active data session
  - Saboteur
    - Jams the network with the intent of causing highest possible damage to the network’s utility
    - *Sabotaging UE* does not have any interest in getting more network resource and may not even have an active data session

- Modeled as two-player matrix games with eNB as the row player and jammer as the column player

- UEs arrive in the cell according to a *homogeneous 2D Stationary Spatial Poisson Point Process (SPPP)*
- Jammer keeps changing its location randomly and launches jamming attacks probabilistically
- UEs have little or no mobility
Utility Models

- **eNB Utility:**
  - Weighted linear function of normalized averages of the following as compared to baseline jamming-free scenario:
    - Overall throughput (in dBs)
    - Number of active users (in dBs)
    - DL-RS SINR difference (in dBs)
    - PUCCH SINR difference (in dBs)
    - PRACH failure rate
  - Fixed Cost associated with a particular eNB action

- **Cheater’s Utility:**
  - Weighted linear function of normalized average throughput (in dBs) and average duty cycle as compared to baseline scenario

- **Saboteur’s Utility:**
  - Weighted linear function of normalized eNB overall average throughput (in dBs), average number of eNB active users (in dBs) and jammer’s average duty cycle
Discussion on Single-Shot Games’ Simulation Results

- eNB’s utility is severely compromised in case of a jamming attack
- eNB’s strategy depends on both the jammer type and its actions
- NE:
  - eNB vs. Cheater
    - Two pure strategy NE at (Normal, Jam DL-RS+PUCCH) and (Normal, Jam DL-RS + PCFICH + PUCCH + PRACH)
    - Expected payoff of (-526,260) and (-520,260)
  - eNB vs. Saboteur
    - Mixed strategy NE with probability distribution of (0.04, 0.05, 0, 0, 0.91) and (0.67, 0.28, 0, 0, 0.05) for eNB and Saboteur
    - May be loosely translated to pure strategy (Change Timing, Inactive) and (Change Timing, Jam DL-RS) NE
    - Expected payoff of (-81.32, 0.68)
- Simulation Parameters:
  - Carrier-to-Jammer power ratio \((C/J)\): 20 dB
  - Probability of jamming \((P_j)\): 0.7
  - BLER threshold: 10%
  - Utility and other parameters can be found in the paper.
Repeated Bayesian Games: Why?

- Single-shot games:
  - Not much appealing for implementation and convergence

- Repeated games:
  - More opportunities for network utility improvement via learning and utilizing game dynamics

- Bayesian games:
  - Incomplete and asymmetric information of other player’s state and actions

- Assumptions:
  - At most only one type of adversary can be present in the network
  - Cheater can follow dynamic resource allocation of eNB but not the Saboteur
  - All the players form an estimate of opponent’s actions and strategize accordingly

- All proposed algorithms can be implemented with current LTE technology