

## Abgabe PHYSEC 2

### 1. FM-Empfänger

### 2. Funkfernbedienungen

### 3. Spectrum Sensing

### 4. Reading assignment

#### 4..1 a)

Siehe Seite 36 des Papers sollen damit *resource depletion attacks* und *masquerade attacks* abgewehrt werden.

#### 4..2 b)

Siehe Seite 37 des Papers haben Signalprints die folgenden Eigenschaften:

- Sie sind schwer zu *spoofen*
- Sie weisen eine starke Korrelation in Hinblick auf ihre physikalische Umgebung auf
- Über mittlere Zeitdauern variieren sie nur leicht

#### 4..3 c)

##### Node Induction

Da der Sender nur mithilfe des empfangenen Signalprints, welches mit dem Referenz-Signalprints verglichen wird, identifiziert werden kann, muss das voraussetzen, dass das Referenz-Signalprint existiert. Falls jedoch eine Node zum ersten mal mit dem Netzwerk interagiert, fehlt logischerweise dieses Referenz-Signalprint, was das Identifizieren dieser Node nicht möglich macht. Wenn eine Node sich dem Netzwerk anschließen will, legt sie offen auf welchen Kanälen sie die restlichen Übertragungen senden wird. Die Empfänger stellen sich darauf ein und messen ihre jeweiligen RSSI Werte, die daraufhin über das Netzwerk verteilt werden.

##### Frequent Hello Messages

Aufgrund der kontinuierlichen Batterieentladung sinkt die Übertragungsstärke zunehmend, was zur Folge hat, dass die RSSI-Werte mit der Zeit abnehmen. Als Konsequenz wird der Vergleich der RSSI-Werte mit dem Signalprint nach einer gewissen Zeit beeinträchtigt und somit die Identifikation. Im

Allgemeinen kann die Entladungsrate nicht ohne Weiteres vom Empfänger vorausgesagt werden, da es von der Ladung des Senders abhängt. Deshalb wird das regelmäßige Versenden von „hello“-Paketten empfohlen. Immer wenn ein Empfänger eine Übertragung eines Senders erhält, vergleicht dieser dann den empfangenen RSSI-Wert mit dem des Referenz-Signalprints. Erreicht die Differenz eine gewisse Größe, wird die Generierung eines neuen Referenz-Signalprints angefordert. Oft reicht der Verkehr von genuinen Übertragungen aus, aber ist das nicht der Fall müssen „hello“-Pakete übertragen werden zur erfolgreichen Verifizierung der RSSI-Werte.

## **Data Transmission**

Nicht jede Datenübertragung wird mithilfe eines Signalprints verifiziert. Je mehr Empfänger zusammenarbeiten um ein Signalprint zu generieren, desto höher die Verlässlichkeit des Signalprints. Es kann passieren, dass zu einem Zeitpunkt nicht genug Empfänger auf einen bestimmten Kanal eingestimmt sind um einen ausreichend verlässlichen Signalprint zu erhalten. Deshalb wird eine Methodik bestehend aus zwei Schritten verwendet:

- Das Netzwerk hält Ausschau nach verdächtiger Aktivität
- Falls so eine Aktivität bemerkt wurde, stimmt das Netzwe eine ausreichende Anzahl an Empfängern auf die entsprechenden Kanäle ein und ein Signalprint wird erzeugt