Design of LPI Signals Using Optimal Families of Perfect Polyphase Sequences

CSDL

Inseon Kim, Ki-Hyeon Park, Min Kyu Song and **Hong-Yeop Song**

Yonsei University

Jang Yong Lee

Agency for Defense Development

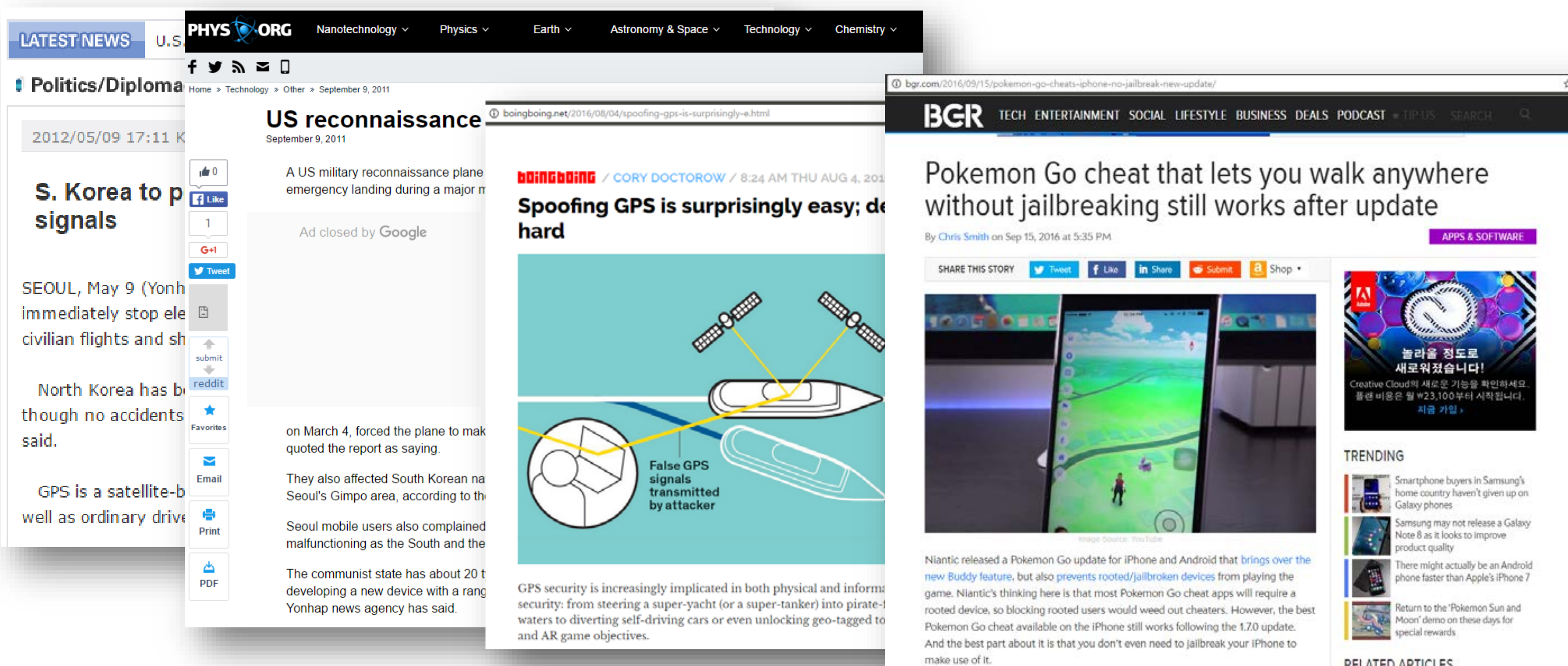
ISITA 2016, October 30- November 2

Contents

- Introduction
  - Motivation
  - Low-Probability Interception(LPI)
  - Direct Sequence Spread Spectrm(DSSS)
- Construction of Sequence Family
- Proposed LPI Communication System
- Summary

Motivation

Modern physical attack are considered to be jamming attack or spoofing attack. Many attacks for GPS are reported. Even some people use GPS spoofing for Pokemon Go!



Low-Probability of Interception(LPI)

An LPI signal is a communication signal having the following characteristics:

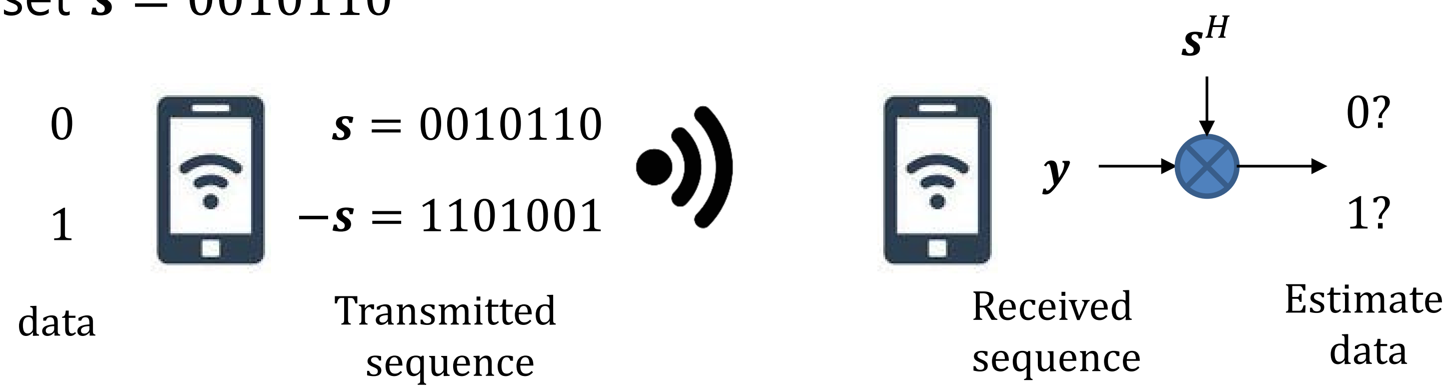
1) It is hard to understand (or capture) the meaning of the communication with LPI signals by any invalid users.
2) It is hard to disturb (or interrupt) the communication with LPI signals by any invalid users.
3) It is hard to determine (or detect) whether the communication with LPI signals is operated in specific time/frequencies by any invalid users. In other words, an invalid user cannot decide the existence of LPI signals in the air.

Direct-Sequence Spread Spectrum(DSSS)

A sequence $\boldsymbol{s}$ of sufficient length is shared with both transmitter and receiver

The system is performed by encoding the messages with $\boldsymbol{s}$ and decoding with matched filter

Ex) set $\boldsymbol{s} = 0010110$



- In this system, the performance is determined by the correlation of sequences
- If unintended users know the information of sequence $\boldsymbol{s}$, then we can say LPI characteristic is broken
- GPS P(Y) or GPS M codes use these technique for LPI characteristics

Construction of Sequence Family

Definition 1

1) Two sequences $\boldsymbol{u} = \{u(t) | t \in \mathbb{Z}\}$ and $\boldsymbol{v} = \{v(t) | t \in \mathbb{Z}\}$ are ***cyclically equivalent*** if there exists an integer τ that satisfies $u(t) = v(t + \tau)$
2) Two families of sequences $\mathcal{F} = \{f_1, f_2, \cdots, f_n\}$ and $\mathcal{G} = \{g_1, g_2, \cdots, g_n\}$ are ***cyclically equivalent*** if $g_i \in \mathcal{G}$ is cyclically equivalent with some $f_j \in \mathcal{F}$
3) Two families of sequences $\mathcal{F} = \{f_1, f_2, \cdots, f_n\}$ and $\mathcal{G} = \{g_1, g_2, \cdots, g_n\}$ are ***completely distinct*** if there is no cyclically equivalent sequence pair f_i and g_j

Example

$$\mathcal{F} = \{(0,0,0,1), (1,1,2,3), (0,1,2,1)\}$$
$$\mathcal{G} = \{(0,1,0,0), (1,2,1,0), (2,3,1,1)\}$$
$$\mathcal{H} = \{(0,1,0,0), (1,2,1,0), (2,3,3,3)\}$$
$$\mathcal{I} = \{(0,1,0,1), (1,1,1,1), (2,1,0,0)\}$$

cyclically equivalent

cyclically inequivalent & not completely distinct

completely distinct

Construction of Sequence Family

Let $\boldsymbol{g} = \{g(t) | t \in \mathbb{Z}\}$ be a p-ary sequence of length p

$\mathcal{S}(\boldsymbol{g})$: set of all p-ary sequence of length p^2 s.t. any sequence $\boldsymbol{s} = \{s(t) | t \in \mathbb{Z}\} \in \mathcal{S}(\boldsymbol{g})$ satisfies $s(t) = s(j + pi) \equiv s(j) + i \cdot g(j) \pmod{p}$ for given $s(j)$ for $j = 0,1,\cdots,p-1$

Theorem (Park16)

If $\boldsymbol{g}$ is a permutation, then all the sequences in $\mathcal{S}(\boldsymbol{g})$ have the perfect auto-correlation property

Let's consider an example when $p = 3$. If we set $\boldsymbol{g} = (0,1,2)$, then $\mathcal{S}(\boldsymbol{g})$ is

$$\begin{pmatrix}0&0&0\\0&1&2\\0&2&1\end{pmatrix},\begin{pmatrix}0&0&1\\0&1&0\\0&2&2\end{pmatrix},\begin{pmatrix}0&0&2\\0&1&1\\0&2&0\end{pmatrix},\begin{pmatrix}0&1&0\\0&2&2\\0&0&1\end{pmatrix},\begin{pmatrix}0&1&1\\0&2&0\\0&0&2\end{pmatrix},\begin{pmatrix}0&1&2\\0&2&1\\0&0&0\end{pmatrix},\begin{pmatrix}0&2&0\\0&0&2\\0&1&1\end{pmatrix},\begin{pmatrix}0&2&1\\0&0&0\\0&1&2\end{pmatrix},\begin{pmatrix}0&2&2\\0&0&1\\0&1&0\end{pmatrix},$$

$$\begin{pmatrix}1&0&0\\1&1&2\\1&2&1\end{pmatrix},\begin{pmatrix}1&0&1\\1&1&0\\1&2&2\end{pmatrix},\begin{pmatrix}1&0&2\\1&1&1\\1&2&0\end{pmatrix},\begin{pmatrix}1&1&0\\1&2&2\\1&0&1\end{pmatrix},\begin{pmatrix}1&1&1\\1&2&0\\1&0&2\end{pmatrix},\begin{pmatrix}1&1&2\\1&2&1\\1&0&0\end{pmatrix},\begin{pmatrix}1&2&0\\1&0&2\\1&1&1\end{pmatrix},\begin{pmatrix}1&2&1\\1&0&0\\1&1&2\end{pmatrix},\begin{pmatrix}1&2&2\\1&0&1\\1&1&0\end{pmatrix},$$

$$\begin{pmatrix}2&0&0\\2&1&2\\2&2&1\end{pmatrix},\begin{pmatrix}2&0&1\\2&1&0\\2&2&2\end{pmatrix},\begin{pmatrix}2&0&2\\2&1&1\\2&2&0\end{pmatrix},\begin{pmatrix}2&1&0\\2&2&2\\2&0&1\end{pmatrix},\begin{pmatrix}2&1&1\\2&2&0\\2&0&2\end{pmatrix},\begin{pmatrix}2&1&2\\2&2&1\\2&0&0\end{pmatrix},\begin{pmatrix}2&2&0\\2&0&2\\2&1&1\end{pmatrix},\begin{pmatrix}2&2&1\\2&0&0\\2&1&2\end{pmatrix},\begin{pmatrix}2&2&2\\2&0&1\\2&1&0\end{pmatrix}.$$

These 9 sequences are cyclically inequivalent with each other

Construction of Sequence Family

Theorem (Park16)

If $\boldsymbol{g}(\kappa, m, \tau) = \{g(t; \kappa, m, \tau) | t \in \mathbb{Z}\}$ satisfies

$$g(t; \kappa, m, \tau) \equiv m(t+\tau)^{\kappa} \quad (mod\ p)$$

for an integer τ, an integer $m(\not\equiv 0)$, and an integer κ that is relatively prime to $p-1$, then the family $\mathcal{F}$ of size $p-1$ made by picking up any one member $\boldsymbol{s}_m$ from $\mathcal{S}(\boldsymbol{g}(\kappa, m, \tau))$ for each $m = 1, 2, \cdots, p-1$ has optimum cross-correlation property

Let's consider an example when $p = 3$. The possible parameters are $\kappa = 1$, $m = 1\ or\ 2$, and $\tau = 0, 1\ or\ 2$. Now, choose $\kappa = 1$, $m = 1$ and $\tau = 0$

$$g(t; 1, 1, 0) \equiv t \quad (mod\ 3)$$

We have $\boldsymbol{g}(1,1,0) = (0, 1, 2)$

$\mathcal{S}(\boldsymbol{g}(1,1,0))$

$$\begin{pmatrix}0&0&0\\0&1&2\\0&2&1\end{pmatrix}, \begin{pmatrix}0&0&1\\0&1&0\\0&2&2\end{pmatrix}, \begin{pmatrix}0&0&2\\0&1&1\\0&2&0\end{pmatrix},$$
$$\begin{pmatrix}1&0&0\\1&1&2\\1&2&1\end{pmatrix}, \begin{pmatrix}1&0&1\\1&1&0\\1&2&2\end{pmatrix}, \begin{pmatrix}1&0&2\\1&1&1\\1&2&0\end{pmatrix},$$
$$\begin{pmatrix}2&0&0\\2&1&2\\2&2&1\end{pmatrix}, \begin{pmatrix}2&0&1\\2&1&0\\2&2&2\end{pmatrix}, \begin{pmatrix}2&0&2\\2&1&1\\2&2&0\end{pmatrix}.$$

$\longleftrightarrow$ Optimum Cross-correlation

$\mathcal{S}(\boldsymbol{g}(1,2,0))$

$$\begin{pmatrix}0&0&0\\0&2&1\\0&1&2\end{pmatrix}, \begin{pmatrix}0&0&1\\0&2&2\\0&1&0\end{pmatrix}, \begin{pmatrix}0&0&2\\0&2&0\\0&1&1\end{pmatrix},$$
$$\begin{pmatrix}1&0&0\\1&2&1\\1&1&2\end{pmatrix}, \begin{pmatrix}1&0&1\\1&2&2\\1&1&0\end{pmatrix}, \begin{pmatrix}1&0&2\\1&2&0\\1&1&1\end{pmatrix},$$
$$\begin{pmatrix}2&0&0\\2&2&1\\2&1&2\end{pmatrix}, \begin{pmatrix}2&0&1\\2&2&2\\2&1&0\end{pmatrix}, \begin{pmatrix}2&0&2\\2&2&0\\2&1&1\end{pmatrix}.$$

Construction of Sequence Family

Definition 2

Let p be an odd prime. Then, for any $m = 1, 2, \cdots, p-1$, the family $\mathcal{S}_m$ is defined to be $\mathcal{S}\big(\boldsymbol{g}(\kappa, m, \tau)\big)$ for an integer τ and an integer κ that is relatively prime to $p-1$. Define a family $\mathcal{F}$ of size $p-1$ by picking up any one member from each $\mathcal{S}_m$ for $m = 1, 2, \cdots, p-1$. The family $\mathcal{F}$ can be simply written as

$$\mathcal{F} = \{\boldsymbol{s}_m | m = 1, 2, \cdots, p-1\}$$

Theorem 1(Park16)

Let p be an odd prime. Then, for any $m = 1, 2, \cdots, p-1$, the family $\mathcal{S}_m$ in *Definition 2* contains p^p sequences of period p^2. The family $\mathcal{F}$ of size $p-1$ in *Definition 2* is an optimum family in the sense that every sequence has the perfect auto-correlation and any pair has the optimum cross-correlation.

Construction of Sequence Family

Theorem 2

Let p be an odd prime. Then, for any $m = 1, 2, \cdots, p-1$, the family $\mathcal{S}_m$ in *Definition 2* contains only p^{p-1} cyclically inequivalent members with each other. Total number of ways of constructing "**completely distinct**" $\mathcal{F}$'s in *Definition 2* is at least $\varphi(p-1)p^{p-1}$ where $\varphi(\cdot)$ denotes the Euler's phi function

Proof of Theorem 2)

Ways of choosing κ is $\varphi(p-1)$ since κ is relatively prime to $p-1$

For given κ, each $\mathcal{S}_m$ contains p^p sequences by Theorem 1.

Total numbers of constructing the family $\mathcal{F}$ is $\varphi(p-1)p^{p(p-1)}$

Now, consider two families

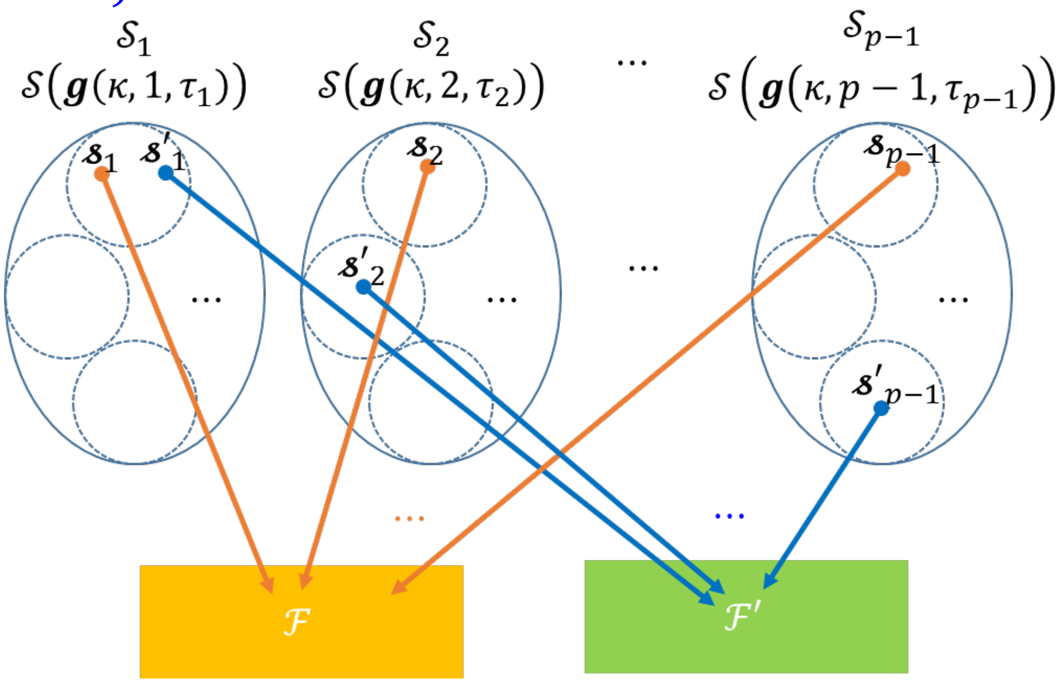
$$\mathcal{F} = \{\boldsymbol{s}_m | m = 1, 2, \cdots, p-1\} \text{ and } \mathcal{F}' = \{\boldsymbol{s}'_m | m = 1, 2, \cdots, p-1\}$$

are not completely distinct.

It happens when any one pair of $\mathcal{F}$ and $\mathcal{F}'$ are cyclically equivalent

Construction of Sequence Family

Proof of Theorem 2)



Given $\mathcal{F}$, the number of constructing $\mathcal{F}'$s is at most $p \cdot p^{p(p-2)} = p^{(p-1)^2}$

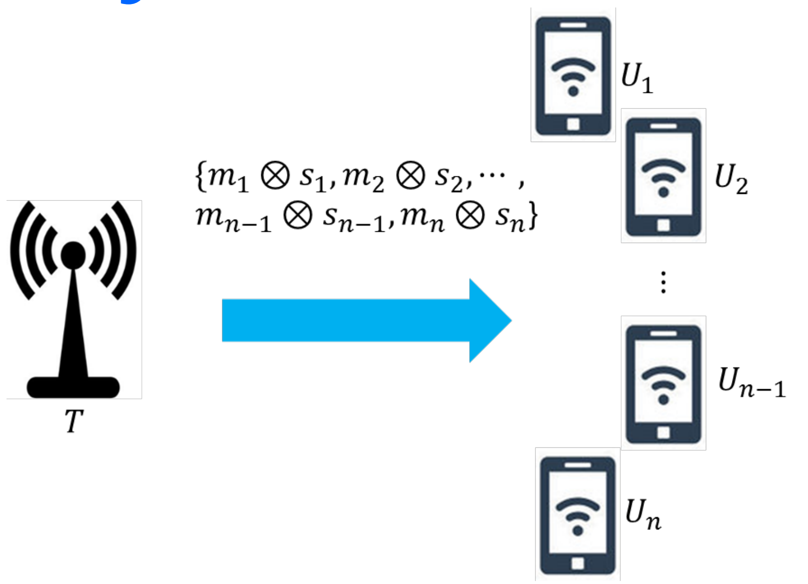
The number of completely distinct families is at least

$$\frac{\varphi(p-1)p^{p(p-1)}}{p^{(p-1)^2}} = \varphi(p-1)p^{p-1}$$

Proposed LPI Communication System

Assumptions

- Transmitter T and n receivers
- Transmit messages m_i to each receiver U_i
- Each user U_i has a private key k_i shared only with transmitter
- S_i : set of p-ary sequence of period p^2 ($p(\gg n)$ be an odd prime)
- S_i and S_j $(i \neq j)$ have perfect auto- and cross correlation property



System Design

- Transmitter T and all users make an agreement for prime p
- Each user U_i selects a sequence $s_i \in S_i$ according to key k_i and the selection method must be shared only with transmitter
- Transmitter has $\mathcal{F} = \{s_1, s_2, \cdots, s_n\}$ and each user U_i has s_i and none of other s_j's
- Transmitter sends signals $\{m_1 \otimes s_1, m_2 \otimes s_2, \cdots, m_n \otimes s_n\}$

Proposed LPI Communication System

Remark 1

For proposed LPI communication system, an attacker must guess $\boldsymbol{s}$ from $\varphi(p-1)p^{p-1}$ candidates to transmit information successfully to valid user U_i even if he have knowledge of prime p. If someone select $p = 31$, one has $\varphi(30) \cdot 31^{30} \approx 2^{152}$ candidates of "completely distinct" families of sequences with period $31^2 = 961$ and size 30. The number of candidates is far larger than the key space of AES-128, that is 2^{128}. This means that the brute-force attack of guessing s is almost impossible in this case, since it is harder than the brute-force attack against AES-128.

Summary

- In this talk, we propose a communication system with multiple users requiring LPI properties using the optimal families of polyphase sequences

- We discuss and prove the bound on the key space for candidates, and conclude that our system is more secure than those employing encrypted sequences using AES-128 against brute-force attack.

Question?