다중위상수열의 최적수열집합을 이용한 저피탐 신호 설계

김인선, 송민규, 송홍엽, 이장용*

연세대학교, *국방과학연구소

2016년도 한국통신학회 하계종합학술대회

▪ 저피탐 신호[1] 특성

- 허가 되지 않은 사용자는 저피탐 신호를 획득할 수는 있지만 신호를 해독할 수는 없어야 함
- 허가되지 않은 사용자는 저피탐 신호를 방해하기 어려워야 한다. 즉, 재밍 상황에서도 저피탐 신호는 적합한 사용자에게 정보를 성공적으로 전탈 할 수 있어야 함.
- 허가되지 않은 사용자는 저피탐 시스템이 운용되는 특정 시간이나 주파수를 알기 어려워야 한다.
  허가되지 않은 사용자는 저피탐 신호의 존재조차도 알 수 없어야 함

▪ 저피탐 시스템

- 충분한 길이의 수열 s로 메시지를 부호화
- 정합 필터 s^H를 이용하여 메시지를 복호화

$$SIR = \frac{C(s,0)}{\max\limits_{\bar{s},\tau} C(s,\bar{s},\tau)}$$

- SIR를 가능한 낮게 유지
- s를 충분히 큰 수열집합으로부터 선택

▪ 최적수열집합 생성[3]

- p가 2보다 큰 소수
- 주어진 수열 $s(j)$ $(j = 0,1,\cdots,p-1)$에 대해서, 주기 p^2인 p진 수열집합 $S(\boldsymbol{g}) = \{s(t)|t \in \mathbb{Z}\}$

$$s(t) = s(j+pi) \equiv s(j) + ig(i) \pmod{p}$$

- $S(\boldsymbol{g})$는 p^p개의 수열을 갖는다
- 주기 p인 p진 수열 $\boldsymbol{g}$가 순열 (permutation)이라면 $S(\boldsymbol{g})$는 완전상관특성을 갖는다.
- τ가 임의의 정수, $m \not\equiv 0 \pmod{p}$인 정수, κ 가 $p-1$과 서로소인 정수일 때

$$\boldsymbol{g}(\kappa,m,\tau) = \{m(t+\tau)^{\kappa} \pmod{p} | t \in \mathbb{Z}\}$$

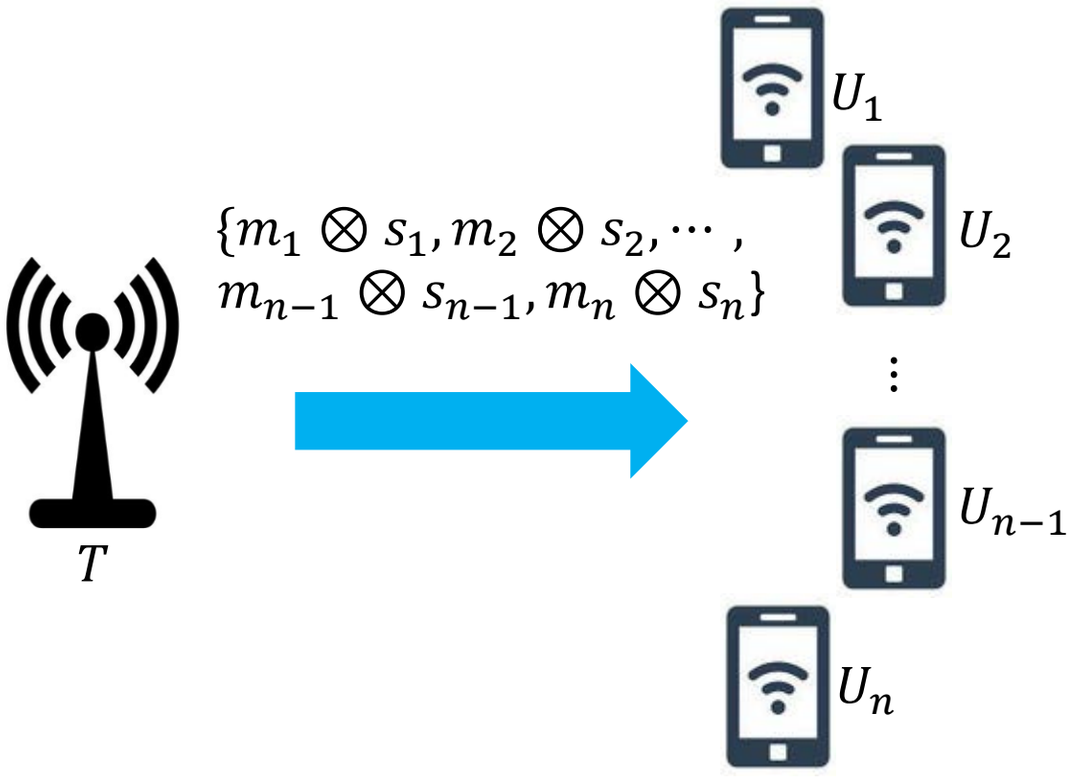
- 수열집합 F

$$F = \left\{\boldsymbol{s}_m \in S\left(\boldsymbol{g}(\kappa,m,\tau)\right) \middle| m = 1,2,\cdots,p-1\right\}$$

▪ 정리 1 [3]

임의의 정수 $m = 1,2,\cdots,p-1$에 대해 $S\left(\boldsymbol{g}(\kappa,m,\tau)\right)$은 p^p개의 주기 p^2인 수열을 갖는다. 수열집합 F는 다음 2개의 성질을 만족한다. 1) 모든 수열이 완전자기상관 특성을 갖고 2)모든 수열 쌍은 최적상호상관 특성을 갖는다.

- **제안하는 저피탐 통신 시스템**
  - 송신기 T, n개의 수신기 $U_1, U_2, \cdots, U_n$
  - 수신기 U_i는 개인키 k_i를 가지고 오직 송신기와 공유
  - 소수 $p(\gg n)$에 대하여 주기 p^2인 p진 수열의 집합: $S_i \ \ (i = 1,2,\cdots,n)$
  - S_i로부터 얻은 수열과 S_j로부터 얻은 수열은 완벽한 상관 특성을 갖는다고 가정



1. 송신기와 다수의 수신기는 소수 p를 정함
2. 수신기 U_i는 개인키 k_i를 이용하여 수열 $s_i \in S_i$를 선택하고 송신기는 집합 $F = \{s_1, s_2, \cdots, s_n\}$을 갖음
3. 송신기는 모든 수신기에게 신호 $\{m_1 \otimes s_1, m_2 \otimes s_2, \cdots, m_{n-1} \otimes s_{n-1}, m_n \otimes s_n\}$를 보냄

- **정리 2**

  임의의 정수 $m = 1,2,\cdots,p-1$에 대해 $S(\boldsymbol{g}(\kappa, m, \tau))$은 p^{p-1} 개의 서로 순환적 동치가 아닌 (*cyclically inequivalent*) 수열을 갖고 있다. 완전히 별개의 (*completely distinct*) 수열집합 F의 개수는 적어도 $\varphi(p-1) \cdot p^{p-1}$개이다.

  - 예를 들어, 시스템이 $p = 31$을 선택했다고 가정하자
  - 최적수열집합 F는 $\varphi(30)31^{30} \approx 2^{158}$개의 후보군을 갖는다. 이는 AES-128의 키집합 개수인 2^{128} 보다 큰 숫자이다.
  - 전수조사공격 측면에서 제안한 시스템이 AES-128을 사용하는 시스템보다 안전하다.

- **참고문헌**

[1] G. Raviparkash, P. Tripathi, and B. Ravi, "*Generation of Low Probability of Intercept Signals*," International Journal of Scientific Engineering and Technology, Vol.2, issue 9, pp. 835-839, Sep. 2013.

[2] C. S. Sin, "*Technologies to counter the GPS jamming*," TTA Journal, vol. 149, pp.92-99, 2013.

[3] K.-H. Park, H.-Y. Song, D. S. Kim, and S. W. Golomb, "*Optimal Families of Perfect Polyphase Sequences from the Array Structure of Fermatquotient Sequences*," IEEE Transactions on Information Theory, vol.62, no.2, pp.1076-1086, February, 2016.