

Inherent Vulnerabilities in Hybrid CDMA & Cryptographic Spread Spectrum for Space Systems

Edd Salkield, Sebastian Köhler, Simon Birnbach, Ivan Martinovic

Systems Security Lab

Security for Space Systems 2025



Direct Sequence Security Multiple Access

Hybrid System

Overvie

Attack

Eavesdroppin Spoofing Jamming

Evaluation

Results

Mext Steps

Conclusion

Fundamentals of Cryptographic Spread Spectrum

Direct Sequence Spreading

Transmitter



Direct Sequence Security Multiple Access

Hybrid Systen

Overvie

Attack

Eavesdroppin Spoofing Jamming

EvaluationThreat Model

Next Step

Conclusion

Fundamentals of Cryptographic Spread Spectrum

Direct Sequence Spreading

Transmitter



Direct Sequence Security Multiple Access

Hybrid Systen

Overview PN Reuse

Attack

Eavesdroppin Spoofing Jamming

Evaluation
Threat Model

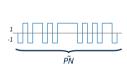
lext Step

Conclusion

Fundamentals of Cryptographic Spread Spectrum

Direct Sequence Spreading

Transmitter





Direct Sequence

Hvbrid

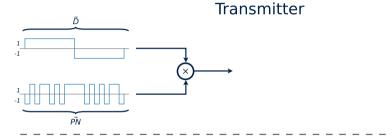
Attack

Evaluation

Conclusion

Fundamentals of Cryptographic Spread Spectrum

Direct Sequence Spreading





Direct Sequence Security Multiple Access

Hybrid Systen

Overviev PN Reusi

Attack

Eavesdroppin Spoofing Jamming

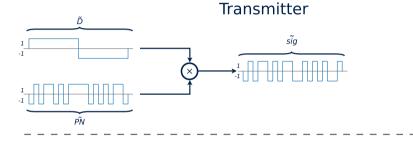
Evaluation Threat Model

Nove Stor

Conclusion

Fundamentals of Cryptographic Spread Spectrum

Direct Sequence Spreading





Direct Sequence Security Multiple Access

Hybrid Systen

> Overviev PN Reus

Attack

Eavesdroppin Spoofing Jamming

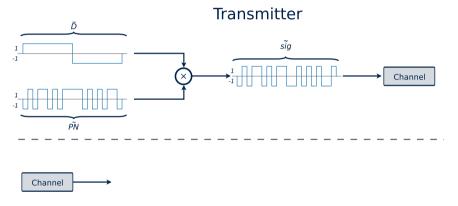
Evaluation
Threat Model

Next Step

Conclusion

Fundamentals of Cryptographic Spread Spectrum

Direct Sequence Spreading





Direct Sequence Security Multiple Access

Hybrid Systen

Overvie

Attack

Eavesdroppin Spoofing Jamming

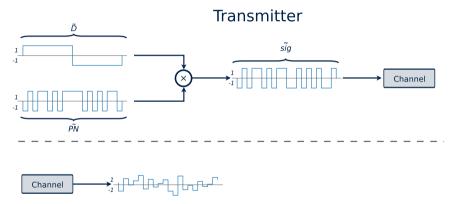
Evaluation Threat Model

lext Step

Conclusion

Fundamentals of Cryptographic Spread Spectrum

Direct Sequence Spreading





Direct Sequence Security Multiple Access

Hybrid Systen

Overvie PN Pour

Attack

Eavesdroppin Spoofing Jamming

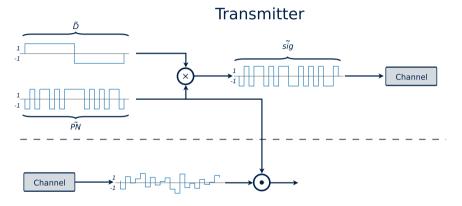
Evaluation Threat Model

Next Step

Conclusion

Fundamentals of Cryptographic Spread Spectrum

Direct Sequence Spreading





Direct Sequence Security Multiple Access

Hybrid Systen

Overvie PN Pour

Attack

Eavesdropping
Spoofing
Jamming

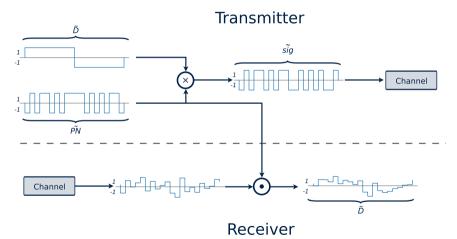
Evaluation
Threat Model

Next Step

Conclusion

Fundamentals of Cryptographic Spread Spectrum

Direct Sequence Spreading





Direct Sequence
Security
Multiple Access

System

Overview

Attack

Eavesdroppin Spoofing Jamming

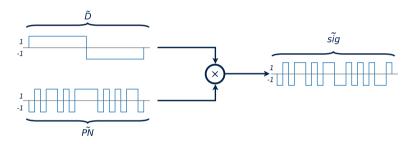
EvaluationThreat Model

Novt Ston

Conclusion

Effect of DSSS

Security Properties: Secrecy/Authenticity





Security

Multiple Access

Hybrid System

Overviev PN Reuse

Attack

Eavesdropping Spoofing Jamming

Evaluation Threat Model

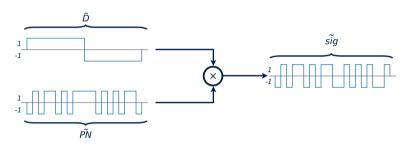
Results

Next Steps

Conclusion

Effect of DSSS

Security Properties: Secrecy/Authenticity



Cryptographic $ilde{PN}$ is equivalent to PHY-layer XOR



Direct Sequence
Security
Multiple Access

Hybrid System

Overview PN Reuse

Attack

Eavesdroppin Spoofing Jamming

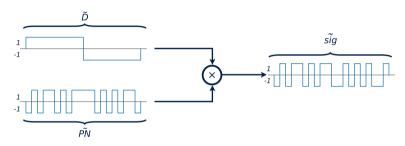
Evaluation Threat Model

Next Step

Conclusion

Effect of DSSS

Security Properties: Secrecy/Authenticity



Cryptographic \tilde{PN} is equivalent to PHY-layer XOR

• **Secrecy** - data is encrypted at PHY-layer



Direct Sequence
Security
Multiple Access

Hybrid Systen

Overview PN Reuse

Attack Eavesdroppi

Eavesdroppin Spoofing Jamming

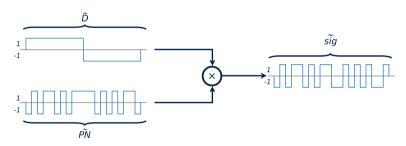
Evaluation
Threat Model

Next Step

Conclusion

Effect of DSSS

Security Properties: Secrecy/Authenticity



Cryptographic \tilde{PN} is equivalent to PHY-layer XOR

- **Secrecy** data is encrypted at PHY-layer
- (Authenticity) as much as provided by XOR with random sequence



Direct Sequence
Security
Multiple Access

Syste

Overvie

Attack

Eavesdropping
Spoofing
Jamming

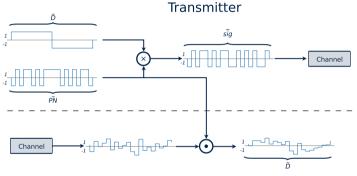
Evaluation Threat Model

Next Step:

Conclusion

Effect of DSSS

Security Properties: Availability



Receiver



Direct Sequence
Security
Multiple Access

Hybrid System

Overview

Attack

Eavesdroppin Spoofing Jamming

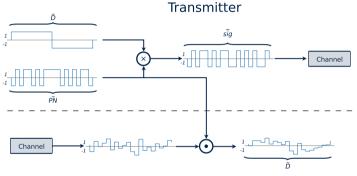
Evaluation
Threat Model
Results

Next Step

Conclusion

Effect of DSSS

Security Properties: Availability



Receiver

Increasing chips per bit improves bit detection



Direct Sequence
Security
Multiple Access

Hybrid Systen

Overview PN Reuse

Attack

Eavesdropping Spoofing Jamming

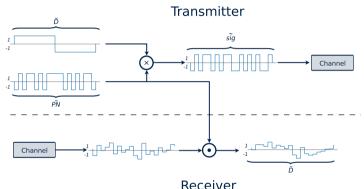
Evaluation
Threat Model
Results

Next Step

Conclusion

Effect of DSSS

Security Properties: Availability



- Increasing chips per bit improves bit detection
- Availability chips per bit can be scaled to provide required jammer tolerance



Direct Sequence
Security
Multiple Access

Syste

Overvie PN Reus

Attack

Eavesdroppin Spoofing Jamming

EvaluationThreat Model

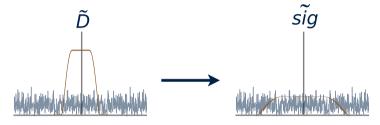
Results

Next Step

Conclusion

Effect of DSSS

Security Properties: Unobservability



Increasing the chip rate increases the bandwidth



Security

Hvbrid

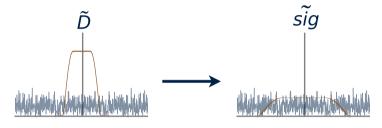
Attack

Evaluation

Conclusion

Effect of DSSS

Security Properties: Unobservability

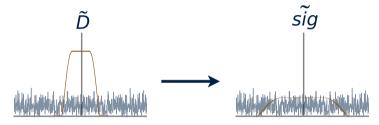


- Increasing the chip rate increases the bandwidth
- Select *chips per bit* to detect signal beneath noise floor



Effect of DSSS

Security Properties: Unobservability



- Increasing the chip rate increases the bandwidth
- Select chips per bit to detect signal beneath noise floor
- **Unobservability** adversaries without knowledge of \tilde{PN} cannot detect presence of signal

Crypto Spread Spectrum

Direct Sequence
Security
Multiple Access

Hybrid Systen

Overviev

Attack Eavesdropp

Evaluation

Next Step

Conclusion



Effect of DSSS

Security Properties

Crypto Spread Spectrum

Security Multiple Aco

Hybrid System

Overview PN Reuse

Attack Eavesdroppii

Eavesdropping Spoofing Jamming

Evaluation
Threat Model

Next Step

Conclusion

- **Secrecy** data is encrypted at PHY-layer
 - **Unobservability** adversaries without knowledge of \tilde{PN} cannot detect presence of signal
- Availability chips per bit can be scaled to provide required jammer tolerance
- Authenticity as much as provided by XOR with random sequence



Security Multiple Ace

Hybrid System

Overview PN Reuse

Attack
Eavesdropping
Spoofing

Evaluation Threat Model

Next Step

Conclusion

Effect of DSSS

Security Properties

- **Secrecy** data is encrypted at PHY-layer
 - **Unobservability** adversaries without knowledge of \tilde{PN} cannot detect presence of signal
- **Availability** chips per bit can be scaled to provide required jammer tolerance
- Authenticity as much as provided by XOR with random sequence

Each depends on secrecy of spreading sequence $ilde{PN}$



Multiple Acc Hybrid

System Overview

Attack
Eavesdropping
Spoofing

Evaluation Threat Model

Next Step

Conclusion

Effect of DSSS

Security Properties

- **Secrecy** data is encrypted at PHY-layer
 - **Unobservability** adversaries without knowledge of \tilde{PN} cannot detect presence of signal
- Availability chips per bit can be scaled to provide required jammer tolerance
- Authenticity as much as provided by XOR with random sequence

Each depends on secrecy of spreading sequence $ilde{PN}$

Therefore \tilde{PN} should be a **cryptographic random sequence**



Direct Sequence
Security
Multiple Access

Hybrid Systen

Overview PN Reuse

Attack

Eavesdropping Spoofing Jamming

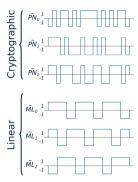
Evaluation Threat Model

Next Step

Conclusion

Effect of DSSS

Multiple Access Properties



Cryptographic sequences have up to 30 dB higher interfering power¹

¹ "Fittipaldi et al. (2011, renewed 2021) Cryptographic Pseudo-Noise Codes and Related Acquisition Techniques for Direct-Sequence Spread Spectrum Transponders"



Direct Sequence
Security
Multiple Access

Hybrid Systen

Overvie

Attack

Eavesdropping
Spoofing
Jamming

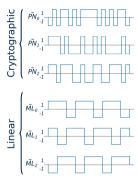
Evaluation
Threat Model

Next Step:

Conclusion

Effect of DSSS

Multiple Access Properties



Cryptographic sequences have up to 30 dB higher interfering power¹

Q: Can security and multiple access be supported simultaneously?

^{1 &}quot;Fittipaldi et al. (2011, renewed 2021) Cryptographic Pseudo-Noise Codes and Related Acquisition Techniques for Direct-Sequence Spread Spectrum Transponders"



Spectrum
Direct Sequence

Multiple Acces

System

Overview PN Reuse

Attack

Eavesdroppin Spoofing

Evaluation
Threat Model

Next Step

Conclusion

Hybrid Cryptographic/CDMA Spread Spectrum

Mechanism Overview

> Cryptographic Pseudo-Noise Codes and Related Acquisition Techniques for Direct-Sequence Spread Spectrum Transponders

Written by	Responsibility	
G. Fittipaldi		
Verified by		
L.Simone		
Approved by		
R. Giangreco	Program Manager	

^aGarello et al. (2025) "AES and Mixed AES/Gold Spreading Sequences for Satellite Uplink Code Division Multiplexing"



Hybrid

System Overview

PN Reus

Attack

Eavesdroppir Spoofing Jamming

Evaluation
Threat Model

Next Step

Conclusion

Hybrid Cryptographic/CDMA Spread Spectrum

Mechanism Overview

| Reference : RPT-RFP_ESA_00019_AASI
| Date : 13/07/2021 |
| Space | Issue : 3 | Page : 1/125 |

Cryptographic Pseudo-Noise Codes and Related Acquisition Techniques for Direct-Sequence Spread Spectrum Transponders

Final Report

Written by	Responsibility	
G. Fittipaldi		
Verified by		
L.Simone		
Approved by		
R. Giangreco	Program Manager	

Developed in 2011, renewed in 2021

^aGarello et al. (2025) "AES and Mixed AES/Gold Spreading Sequences for Satellite Uplink Code Division Multiplexing"



Hybrid System

Overview PN Reuse

Attack

Eavesdroppir Spoofing Jamming

Evaluation
Threat Model

Next Step

Conclusion

Hybrid Cryptographic/CDMA Spread Spectrum

Mechanism Overview

	Reference:	RPT	-RFP-ESA-00013-AA
'halesAlenia	Date :	13/0	7/2021
Space	Issue :	3	Page:1/125

Cryptographic Pseudo-Noise Codes and Related Acquisition Techniques for Direct-Sequence Spread Spectrum Transponders

Written by	Responsibility
G. Fittipaldi	
Verified by	
L.Simone	
Approved by	
R. Giangreco	Program Manager

- Developed in 2011, renewed in 2021
- Provides multiple access properties similar to ETSI standards

^aGarello et al. (2025) "AES and Mixed AES/Gold Spreading Sequences for Satellite Uplink Code Division Multiplexing"



Hybrid System

PN Reus

Attack

Eavesdroppin Spoofing Jamming

Evaluation
Threat Model
Possilts

Next Step

Conclusion

Hybrid Cryptographic/CDMA Spread Spectrum

Mechanism Overview

	Reference:	RPT	-RFP-ESA-00013-AAS
halesAlenía	Date :	13/0	7/2021
Space	Issue :	3	Page:1/125

Cryptographic Pseudo-Noise Codes and Related Acquisition Techniques for Direct-Sequence Spread Spectrum Transponders

Written by	Responsibility	
G. Fittipaldi		
Verified by		
L.Simone		
Approved by		
R. Giangreco	Program Manager	

- Developed in 2011, renewed in 2021
- Provides multiple access properties similar to ETSI standards
- Designed for multiple satellite uplink relays e.g. TDRS

^aGarello et al. (2025) "AES and Mixed AES/Gold Spreading Sequences for Satellite Uplink Code Division Multiplexing"



Hybrid System

Overvie PN Reus

Attack

Eavesdropping Spoofing Jamming

Evaluation
Threat Model

Next Step

Conclusion

Hybrid Cryptographic/CDMA Spread Spectrum

Mechanism Overview

	Reference:	RPT	-RFP-ESA-00013-AASI
'halesAlenia	Date :	13/0	7/2021
Space	Issue :	3	Page: 1/125

Cryptographic Pseudo-Noise Codes and Related Acquisition Techniques for Direct-Sequence Spread Spectrum Transponders

Written by	Responsibility	
G. Fittipaldi		
Verified by		
L.Simone		
Approved by		
R. Giangreco	Program Manager	

- Developed in 2011, renewed in 2021
- Provides multiple access properties similar to ETSI standards
- Designed for multiple satellite uplink relays e.g. TDRS
- No security analysis conducted so far

^aGarello et al. (2025) "AES and Mixed AES/Gold Spreading Sequences for Satellite Uplink Code Division Multiplexing"



Hybrid System

Overvie PN Reus

Attack

Eavesdropping Spoofing Jamming

Evaluation
Threat Model

Next Step

Conclusion

Hybrid Cryptographic/CDMA Spread Spectrum

Mechanism Overview

	Reference:	RPT	-RFP-ESA-00013-AASI
halesAlenia	Date :	13/0	7/2021
Space	Issue :	3	Page: 1/125

Cryptographic Pseudo-Noise Codes and Related Acquisition Techniques for Direct-Sequence Spread Spectrum Transponders

Written by	Responsibility	
G. Fittipaldi		
Verified by		
L.Simone		
Approved by		
R. Giangreco	Program Manager	

- Developed in 2011, renewed in 2021
- Provides multiple access properties similar to ETSI standards
- Designed for multiple satellite uplink relays e.g. TDRS
- No security analysis conducted so far
- Other hybrid systems designed under similar construction^a

^aGarello et al. (2025) "AES and Mixed AES/Gold Spreading Sequences for Satellite Uplink Code Division Multiplexing"



Crypto Spread

Direct Sequer Security

Hybrid System

Overview

Attack

Eavesdroppin Spoofing Jamming

Evaluation
Threat Model

10030103

itext Step

Conclusion

Hybrid Cryptographic/CDMA Spread Spectrum

Mechanism Overview

Satellite Data



Direct Sequen Security

Hybrid System

Overview PN Reuse

Attack

Eavesdropping Spoofing Jamming

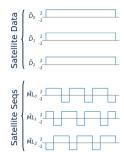
EvaluationThreat Model

Results

Next Step

Conclusion

Hybrid Cryptographic/CDMA Spread Spectrum





Spectrum

Security Multiple Acce

Hybrid System

Overview PN Reuse

Attack

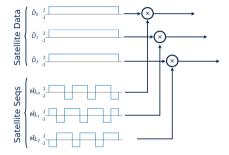
Eavesdroppin Spoofing Jamming

Evaluation Threat Model

Next Ster

Conclusion

Hybrid Cryptographic/CDMA Spread Spectrum





Spectrum

Direct Sequence

Security Multiple Acce

Hybrid System

Overview PN Reuse

Attack

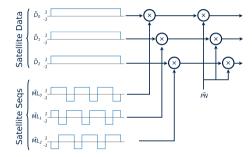
Eavesdroppin Spoofing Jamming

Evaluation Threat Model

Next Step

Conclusion

Hybrid Cryptographic/CDMA Spread Spectrum





Spectrun Direct Sequer

Direct Sequer Security Multiple Acce

Hybrid System

Overview PN Reuse

Attack

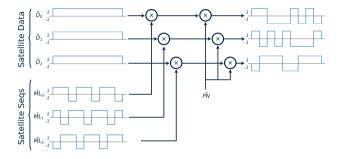
Eavesdropping Spoofing Jamming

Evaluation Threat Model

Next Ste

Conclusion

Hybrid Cryptographic/CDMA Spread Spectrum





Spectrum Direct Sequen

Direct Sequent Security Multiple Acces

Hybrid System

Overview PN Reuse

Attack

Eavesdropping Spoofing Jamming

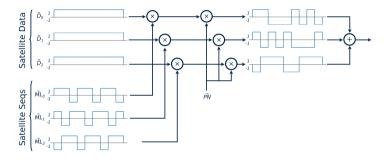
Evaluation Threat Model

Next Ste

Conclusion

Hybrid Cryptographic/CDMA Spread Spectrum

Mechanism Overview





Spectrum Direct Sequen

Security Multiple Acce

Hybrid System

Overview PN Reuse

Attack

Eavesdroppin Spoofing Jamming

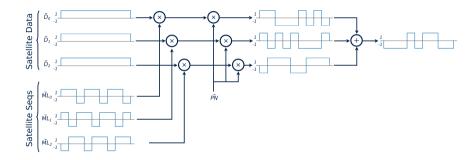
Evaluation Threat Model

Next Step

Conclusion

Hybrid Cryptographic/CDMA Spread Spectrum

Mechanism Overview





Hvbrid

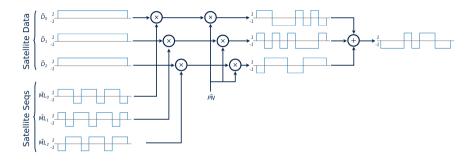
System Overview

Evaluation

Conclusion

Hybrid Cryptographic/CDMA Spread Spectrum

Mechanism Overview



• Spreading sequence cryptographically random since XORed with \widetilde{PN}



Direct Sequent
Security
Multiple Access

Hybrid System Overview

Overvier PN Reus

Attack
Eavesdroppin
Spoofing

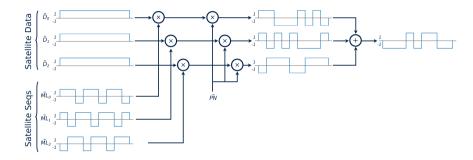
Evaluation
Threat Model

Next Steps

Conclusion

Hybrid Cryptographic/CDMA Spread Spectrum

Mechanism Overview



- ullet Spreading sequence cryptographically random since XORed with $ilde{PN}$
- Receivers undo $ilde{PN}$, reducing to per-satellite linear spreading codes $ilde{ML}$



Crypto Spread Spectrum Direct Sequence

Hybrid System

Overview PN Reuse

Attack Eavesdropp

Eavesdropping Spoofing Jamming

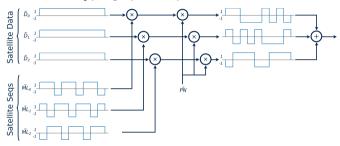
Evaluation Threat Model

Next Step

Conclusion

Key Security Issue

Reuse of Cryptographic Sequence





Hybrid System

PN Reuse

Attack

Eavesdroppin

Spoofing

Jamming

Evaluation
Threat Model
Results

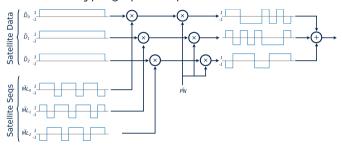
Next Step

Conclusion

Key Security Issue

Reuse of Cryptographic Sequence

NB: Same cryptographic sequence \tilde{PN} reused across all data sequences



Intuition: insufficient entropy entering the system to protect the data



Hybrid System

Overview PN Reuse

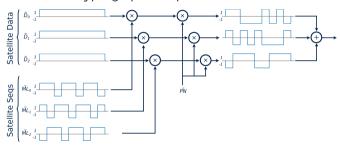
Attack
Eavesdroppin
Spoofing
Jamming

Evaluation
Threat Model
Results

Conclusion

Key Security Issue

Reuse of Cryptographic Sequence



- Intuition: insufficient entropy entering the system to protect the data
- \bullet \widetilde{PN} has effect of randomising sign of aggregate chip, but not magnitude



Hybrid System

PN Reuse

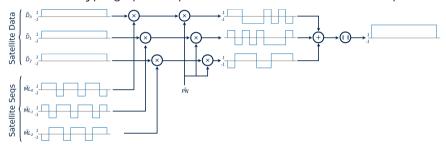
Attack
Eavesdroppin
Spoofing
Jamming

Evaluation
Threat Model
Results

Conclusion

Key Security Issue

Reuse of Cryptographic Sequence



- Intuition: insufficient entropy entering the system to protect the data
- ullet $ilde{PN}$ has effect of randomising $ilde{sign}$ of aggregate chip, but not $ilde{magnitude}$



Hybrid System

PN Reuse

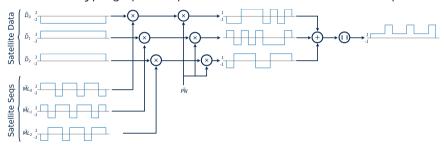
Attack
Eavesdroppin
Spoofing

Evaluation
Threat Model

Conclusion

Key Security Issue

Reuse of Cryptographic Sequence



- Intuition: insufficient entropy entering the system to protect the data
- ullet $ilde{PN}$ has effect of randomising $ilde{sign}$ of aggregate chip, but not $ilde{magnitude}$



Hybrid System

Overview PN Reuse

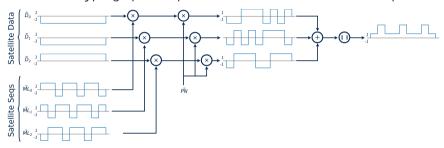
Attack
Eavesdroppin
Spoofing
Jamming

Evaluation
Threat Model
Results

Conclusion

Key Security Issue

Reuse of Cryptographic Sequence



- Intuition: insufficient entropy entering the system to protect the data
- \bullet \widetilde{PN} has effect of randomising sign of aggregate chip, but not magnitude



Hybrid System Overview PN Reuse

Attack

Eavesdroppi

Spoofing
Jamming

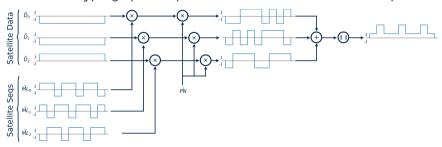
Evaluation

Threat Model Results

Next Steps
Conclusion

Key Security Issue

Reuse of Cryptographic Sequence



- Intuition: insufficient entropy entering the system to protect the data
- \tilde{PN} has effect of randomising sign of aggregate chip, but not magnitude
- Aggregate chip magnitudes repeat many times, leaking information about the data



Attack: Eavesdropping

Unobservability

Possible aggregate chip sequences:

 D_0 D_1 D_2

Hvbrid

Attack

Eavesdropping

Evaluation

Conclusion



Direct Sequence Security

Multiple Acce

Syste

Overvie PN Reus

Attack

Eavesdropping Spoofing Jamming

Evaluation

Results

Next Step

Conclusion

Attack: Eavesdropping

Unobservability

Possible aggregate chip sequences:





Hvbrid

Attack

Eavesdropping

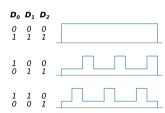
Evaluation

Conclusion

Attack: Eavesdropping

Unobservability

Possible aggregate chip sequences:





Security

Multiple Acces

Hybrid

Overvie

PN Reus

Attack

Eavesdropping
Spoofing
Jamming

Evaluation
Threat Model

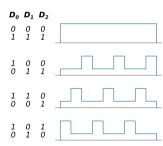
Nove Stor

Conclusion

Attack: Eavesdropping

Unobservability

Possible aggregate chip sequences:





Hvbrid

Attack

Eavesdropping

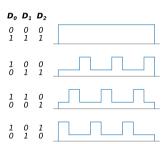
Evaluation

Conclusion

Attack: Eavesdropping

Unobservability

Possible aggregate chip sequences:



Unobservability broken by correlating for known, repeating aggregate sequences



Security
Multiple Access

Hybrid System

Overview PN Reuse

Attack Eavesdropping

Eavesdropping Spoofing Jamming

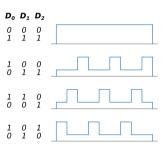
Evaluation
Threat Model
Possilts

Next Steps

Attack: Eavesdropping

Unobservability

Possible aggregate chip sequences:



Unobservability broken by correlating for known, repeating aggregate sequences Q: In general case, how can the original data sequence be determined given a noisy waveform?



SSL Systems Security Lab

Spectrum

Direct Sequence
Security

Hybrid System Overview

Attack

Eavesdropping
Spoofing
Jamming

Evaluation
Threat Model
Results

Next Steps

Conclusion

Attack: Eavesdropping

Adversarial Decoding

Algorithm 1 Eavesdropping Decoder Optimization

 $\overline{\mathsf{EAVESDROP}(\mathbf{b},\mathbf{ML},\mathbf{g}) \to (\mathbf{D}^*,\mathbf{PN}^*)}$

b_1, \dots, b_N ML_1, \dots, ML_n a_1, \dots, a_n

Received aggregate chips L_n Satellite ML sequences
Satellite gains

Variables

 D_1, D_2, \dots, D_n Data chip values PN_1, \dots, PN_N Cryptographic pseudo-noise $e_1^+, e_1^-, \dots, e_N^+, e_N^-$ Error terms to minimize

Key principle: Find data D_i and pseudo-noise PN_i that minimize distance between received and expected chips.

Objective:

Minimize
$$Z = e_1^+ + e_1^- + \ldots + e_N^+ + e_N^-$$

Key Constraints:

$$\begin{aligned} g_1 M L_1[1] D_1 P N_1 + \ldots + g_n M L_n[1] D_n P N_1 + e_1^+ - e_1^- = b_1 \\ g_1 M L_1[N] D_1 P N_N + \ldots + g_n M L_n[N] D_n P N_N + e_N^+ - e_N^- = b_N \end{aligned}$$

$$-1 \le D_1, \dots, D_n, PN_1, \dots, PN_N \le 1$$

 $e_1^+, e_1^-, e_2^+, e_2^- \ge 0$



Spectrum

Hvbrid

Attack

Eavesdropping

Evaluation

Conclusion

Attack: Eavesdropping

Adversarial Decoding

Algorithm 1 Eavesdropping Decoder Optimization

EAVESDROP(b, ML, g) \rightarrow (D*, PN*) Constants

b_1, \ldots, b_N ML_1, \dots, ML_n

Received aggregate chips Satellite ML sequences Satellite gains

q_1, \dots, q_n Variables

D_1, D_2, \dots, D_n Data chip values PN_1, \dots, PN_N Cryptographic pseudo-noise $e_1^+, e_1^-, \dots, e_N^+, e_N^-$ Error terms to minimize

Key principle: Find data Di and pseudo-noise PNi that minimize distance between received and expected chips.

Objective:

Minimize
$$Z = e_1^+ + e_1^- + ... + e_N^+ + e_N^-$$

Key Constraints:

$$\begin{aligned} g_1 M L_1[1] D_1 P N_1 + \ldots + g_n M L_n[1] D_n P N_1 + e_1^+ - e_1^- = b_1 \\ & \dots \\ g_1 M L_1[N] D_1 P N_N + \ldots + g_n M L_n[N] D_n P N_N + e_N^+ - e_N^- = b_N \end{aligned}$$

Bounding Constraints:

$$-1 \le D_1, \dots, D_n, PN_1, \dots, PN_N \le 1$$

 $e_1^+, e_1^-, e_2^+, e_2^- \ge 0$

 Solve optimisation problem by Maximum Likelihood decodina



Spectrum

Hvbrid

Attack

Eavesdropping

Evaluation

Conclusion

Attack: Eavesdropping

Adversarial Decoding

Algorithm 1 Eavesdropping Decoder Optimization

EAVESDROP(b, ML, g) \rightarrow (D*, PN*) Constants

 b_1, \dots, b_N ML_1, \dots, ML_n q_1, \dots, q_n

Received aggregate chips Satellite ML sequences Satellite gains

Variables

 D_1, D_2, \dots, D_n Data chip values PN_1, \dots, PN_N Cryptographic pseudo-noise $e_1^+, e_1^-, \dots, e_N^+, e_N^-$ Error terms to minimize

Key principle: Find data Di and pseudo-noise PNi that minimize distance between received and expected chips.

Objective:

Minimize
$$Z = e_1^+ + e_1^- + ... + e_N^+ + e_N^-$$

Key Constraints:

$$\begin{aligned} g_1 M L_1[1] D_1 P N_1 + \ldots + g_n M L_n[1] D_n P N_1 + e_1^+ - e_1^- = b_1 \\ g_1 M L_1[N] D_1 P N_N + \ldots + g_n M L_n[N] D_n P N_N + e_N^+ - e_N^- = b_N \end{aligned}$$

$$-1 \le D_1, \dots, D_n, PN_1, \dots, PN_N \le 1$$

 $e_1^+, e_1^-, e_2^+, e_2^- \ge 0$

- Solve optimisation problem by Maximum Likelihood decodina
- "What was the most likely transmitted data sequence given the waveform?"



Spectrum

Hvbrid System

Attack

Eavesdropping

Evaluation

Conclusion

Attack: Eavesdropping

Adversarial Decoding

Algorithm 1 Eavesdropping Decoder Optimization

EAVESDROP(b, ML, g) \rightarrow (D*, PN*) Constants

 b_1, \ldots, b_N ML_1, \dots, ML_n q_1, \dots, q_n

Received aggregate chips Satellite ML sequences Satellite gains

Variables

 D_1, D_2, \dots, D_n Data chin values PN_1, \dots, PN_N Cryptographic pseudo-noise $e_1^+, e_1^-, \dots, e_N^+, e_N^-$ Error terms to minimize

Key principle: Find data Di and pseudo-noise PNi that minimize distance between received and expected chips.

Objective:

Minimize
$$Z = e_1^+ + e_1^- + ... + e_N^+ + e_N^-$$

Key Constraints:

$$\begin{aligned} &g_1ML_1[1]D_1PN_1+\ldots+g_nML_n[1]D_nPN_1+e_1^+-e_1^- = \\ &b_1 \\ &\cdots \\ &g_1ML_1[N]D_1PN_N+\ldots+g_nML_n[N]D_nPN_N+e_N^+ - \\ &e_N^- = b_N \end{aligned}$$

$$-1 \le D_1, \dots, D_n, PN_1, \dots, PN_N \le 1$$

 $e_1^+, e_1^-, e_2^+, e_2^- \ge 0$

- Solve optimisation problem by Maximum Likelihood decodina
- "What was the most likely transmitted data sequence given the waveform?"
- Takes into account many repeating chip magnitudes



Spectrum

Hvbrid

Attack

Eavesdropping

Evaluation

Conclusion

Attack: Eavesdropping

Adversarial Decoding

Algorithm 1 Eavesdropping Decoder Optimization

EAVESDROP(b, ML, g) \rightarrow (D*, PN*) Constants

b_1, \ldots, b_N ML_1, \dots, ML_n

Received aggregate chips Satellite ML sequences Satellite gains

q_1, \dots, q_n Variables

 D_1, D_2, \dots, D_n Data chip values PN_1, \dots, PN_N Cryptographic pseudo-noise $e_1^+, e_1^-, \dots, e_N^+, e_N^-$ Error terms to minimize

Key principle: Find data Di and pseudo-noise PNi that minimize distance between received and expected chips.

Objective:

Minimize
$$Z = e_1^+ + e_1^- + \ldots + e_N^+ + e_N^-$$

Key Constraints:

$$\begin{cases} g_1ML_1[1]D_1PN_1+\ldots+g_nML_n[1]D_nPN_1+e_1^+-e_1^- = b_1\\ b_1\\ g_1ML_1[N]D_1PN_N+\ldots+g_nML_n[N]D_nPN_N+e_N^+-\\ e_N^- = b_N \end{cases}$$

$$-1 \le D_1, \dots, D_n, PN_1, \dots, PN_N \le 1$$

 $e_1^+, e_1^-, e_2^+, e_2^- \ge 0$

- Solve optimisation problem by Maximum Likelihood decodina
- "What was the most likely transmitted data sequence given the waveform?"
- Takes into account many repeating chip magnitudes
- Catastrophic outcome: almost always reduces to 2 bits of entropy



SSL
Systems Security Lab
Crypto Spread

Spectrum
Direct Sequence
Security
Multiple Access

Hybrid System Overview PN Reuse

Attack

Eavesdropping Spoofing Jamming

Evaluation
Threat Model
Results

Conclusion

Results Next Ster

Algorithm 1 Eavesdropping Decoder Optimization

EAVESDROP($\mathbf{b}, \mathbf{ML}, \mathbf{g}) \rightarrow (\mathbf{D}^*, \mathbf{PN}^*)$

b_1, \ldots, b_N ML_1, \ldots, ML_n

Received aggregate chips Satellite ML sequences Satellite gains

g_1, \dots, g_n Variables

 D_1, D_2, \dots, D_n Data chip values PN_1, \dots, PN_N Cryptographic pseudo-noise $e_1^+, e_1^-, \dots, e_N^+, e_N^-$ Error terms to minimize

Key principle: Find data D_i and pseudo-noise PN_i that minimize distance between received and expected chips.

Objective:

Minimize
$$Z = e_1^+ + e_1^- + \ldots + e_N^+ + e_N^-$$

Key Constraints:

 $e_N^- = b_N$

$$g_1ML_1[1]D_1PN_1+...+g_nML_n[1]D_nPN_1+e_1^+-e_1^-=b_1$$

...
 $g_1ML_1[N]D_1PN_N+...+g_nML_n[N]D_nPN_N+e_N^+-$

Bounding Constraints:

$$-1 \le D_1, \dots, D_n, PN_1, \dots, PN_N \le 1$$

 $e_1^+, e_1^-, e_2^+, e_2^- \ge 0$

Attack: Eavesdropping

Adversarial Decoding

- Solve optimisation problem by Maximum Likelihood decoding
- "What was the most likely transmitted data sequence given the waveform?"
- Takes into account many repeating chip magnitudes
- Catastrophic outcome: almost always reduces to 2 bits of entropy
- Any satellite's data sequence is sufficient to recover all other satellites' data



Security

Multiple Acces

Hybrid

Overviev

PN Reus

Attack

Eavesdropping

Spoofing

Jamming

Evaluation

Results

Hext Step.

Conclusion

Attack: Spoofing

 \tilde{PN} Spreading Sequence Recovery

To create new messages, the attacker must know \tilde{PN} .



Direct Sequence Security Multiple Access

Hybrid System Overview

Overviev PN Reuse

Attack

Spoofing

Jamming

Evaluation Threat Model

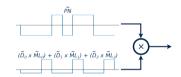
Next Step

Conclusion

Attack: Spoofing

 \tilde{PN} Spreading Sequence Recovery

To create new messages, the attacker must know \tilde{PN} .





Direct Sequence Security Multiple Access

Hybrid System Overview

Attack

Eavesdropping

Spoofing

Jamming

Evaluation
Threat Model

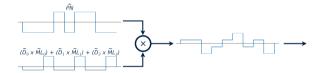
Next Step

Conclusion

Attack: Spoofing

 \tilde{PN} Spreading Sequence Recovery

To create new messages, the attacker must know \tilde{PN} .





Direct Sequence Security Multiple Access

Hybrid Systen Overview

Overview PN Reuse

Attack

Spoofing

Jamming

Evaluation Threat Model

Next Step

Conclusion

Attack: Spoofing

 \tilde{PN} Spreading Sequence Recovery

To create new messages, the attacker must know \tilde{PN} .





Spectrum
Direct Sequence

Security

Multiple Access

Hybrid Systen Overview

Overview PN Reuse

Attack

Spoofing
Jamming

Evaluation

Threat Model

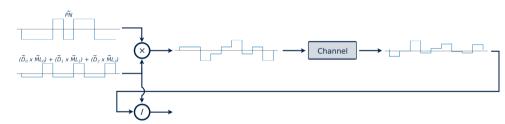
Next Step

Conclusion

Attack: Spoofing

 \tilde{PN} Spreading Sequence Recovery

To create new messages, the attacker must know \tilde{PN} .





Spectrum Direct Sequence

Security Multiple Access

Hybrid Systen Overview

PN Reuse

Attack

Spoofing
Jamming

Evaluation
Threat Model

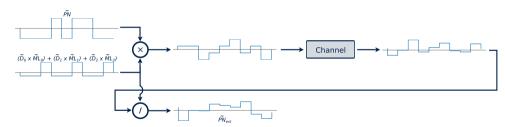
Next Step

Conclusion

Attack: Spoofing

 \tilde{PN} Spreading Sequence Recovery

To create new messages, the attacker must know \tilde{PN} .





Spectrum

Multiple Acce

System

Overview PN Reuse

Attack

Spoofing
Jamming

Evaluation
Threat Model
Possilts

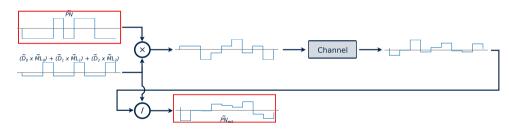
Next Step

Conclusion

Attack: Spoofing

 \tilde{PN} Spreading Sequence Recovery

To create new messages, the attacker must know \tilde{PN} .





Spectrum Direct Sequence

Multiple Acce

Hybrid System Overview

Overview PN Reuse

Attack

Eavesdropping
Spoofing
Jamming

Evaluation
Threat Model
Results

Next Step

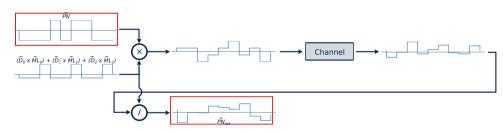
Conclusion

Attack: Spoofing

 \tilde{PN} Spreading Sequence Recovery

To create new messages, the attacker must know \tilde{PN} .

Q: How can \tilde{PN} be recovered?



This recovers a noisy estimate of the spreading sequence $\tilde{PN} = \tilde{PN}_{cot} + noise$

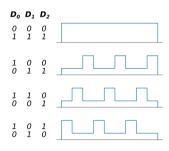


Attack

Evaluation

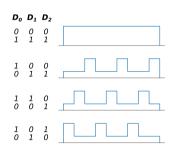
Conclusion

Attack: Jamming





Attack: Jamming



During each bit period, the jammer...

Evaluation

Attack



Systems Security Lab Crypto Spread Do D1

Spectrum Direct Sequence

Security

Multiple Access

Hybrid System

Overview PN Reuse

Attack

Spoofing

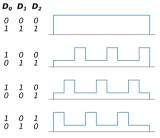
Jamming

Evaluation Threat Model

Next Step

Conclusion

Attack: Jamming



- During each bit period, the jammer...
 - detects the current aggregate bit sequence



Spectrum

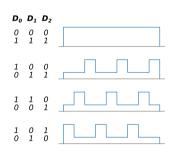
Hvbrid

Attack

Evaluation

Conclusion

Attack: Jamming



- During each bit period, the jammer...
 - detects the current aggregate bit sequence
 - targets the lowest-power sequences



Spectrum Direct Sequen

Security Multiple Acces

Syster

Overview PN Reuse

Attack

Eavesdroppin Spoofing Jamming

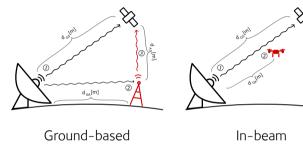
Evaluation Threat Model

Threat N
Results

Next Step

Conclusion

Threat Model





Satellite



Spectrum

Direct Sequence

Security

Multiple Acces **Hybrid**

System Overview

Attack

Eavesdroppin Spoofing Jamming

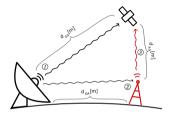
Evaluation Threat Model

Next Step

Conclusion

Threat Model

Scenarios



Ground-based



In-beam



Satellite

- **Secrecy** eavesdropping
- Authenticity spoofing
- Availability jamming



Spectrum
Direct Sequence
Security

Hybrid System Overview

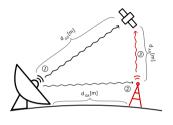
Attack
Eavesdropping
Spoofing
Jamming

Evaluation Threat Model

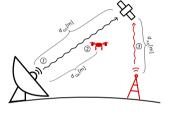
Next Step

Conclusion

Threat Model



Ground-based



In-beam



Satellite

- **Secrecy** eavesdropping
- Authenticity spoofing
- Availability jamming

Source code available:

https://github.com/ssloxford/hybrid-crypto-spreading-code



Spectrum Direct Sequence

Direct Sequence
Security
Multiple Access

Hybrid System

Overview PN Reuse

Attack

Eavesdropping Spoofing Jamming

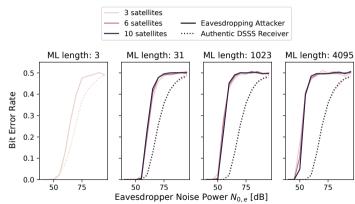
EvaluationThreat Model

Results
Next Ste

Conclusion

Evaluation

Eavesdropping



Decoding without knowledge of the spreading sequence at only $\sim\!10\,\mathrm{dB}$ less power than with knowledge of the sequence.



Spectrum Direct Sequence

Security

Multiple Access

Hybrid System

Overview PN Reuse

Attack
Eavesdropping
Spoofing

Evaluation

Threat Model

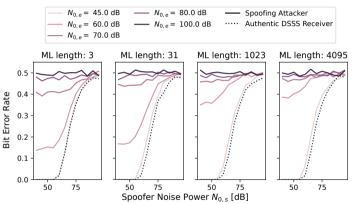
Results

Next Step

Conclusion

Evaluation

Spoofing



Spoofing depends primarily on the noise in the spreading sequence estimate. "Lifting" it from the noise floor through e.g. high gain antennas not required.



Direct Sequence Security

Hvbrid

Syste

Overview PN Reuse

Attack

Eavesdropping
Spoofing
Jamming

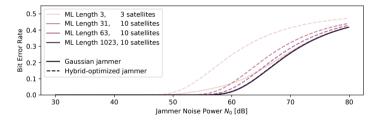
Evaluation

Results

Next Step:

Conclusion

Evaluation Jamming



Jammer advantage is high for low ML lengths, and decreases as the length increases.



Countermeasures

Spectrum

Security
Multiple Acces

Hybrid

Overviev

Attacl

Eavesdroppin Spoofing Jamming

Evaluation

Rosults

Next Steps

Conclusion



Crypto Spread Spectrum Direct Sequence

Security

Multiple Access

Hybrid System

Overvie

PN Reus

Attack

Eavesdroppin Spoofing Jamming

Evaluation Threat Model

Next Steps

Conclusion

Countermeasures

- Non-hybrid spread spectrum
 - $\bullet\,$ Suffers up to $30\,\mathrm{dB}$ performance loss under multiple access
 - Secure hybrid systems for future standardisation must be secure against the presented attacks



Spectrum

Direct Sequence
Security

Multiple Access

Hybrid System Overview PN Reuse

Attack

Eavesdropping

Spoofing

Jamming

Evaluation
Threat Model

Next Steps

Conclusion

Countermeasures

- Non-hybrid spread spectrum
 - $\bullet\,$ Suffers up to $30\,\mathrm{dB}$ performance loss under multiple access
 - Secure hybrid systems for future standardisation must be secure against the presented attacks
- Preventing synchronization data reuse
 - Initialisation parameters are transmitted in the clear, allowing the adversary to record, modify, and replay as discussed
 - Authenticity protection and freshness guarantees required in session establishment



Spectrum
Direct Sequence
Security
Multiple Access

Hybrid System Overview PN Reuse

Attack
Eavesdropping
Spoofing
Jamming

Evaluation
Threat Model
Results

Next Steps

Conclusion

Countermeasures

- Non-hybrid spread spectrum
 - ullet Suffers up to $30\,\mathrm{dB}$ performance loss under multiple access
 - Secure hybrid systems for future standardisation must be secure against the presented attacks
- Preventing synchronization data reuse
 - Initialisation parameters are transmitted in the clear, allowing the adversary to record, modify, and replay as discussed
 - Authenticity protection and freshness guarantees required in session establishment
- Cryptographic scrambling
 - Prevents recovery of the data sequences
 - Does not provide unobservability
 - Does not protect against bit-flipping spoofing attacks



Thank you for your attention

Fdd Salkield Systems Security Lab, University of Oxford https://seclab.cs.ox.ac.uk

edward.salkield@cs.ox.ac.uk

https://edd.salkield.uk

Hvbrid

Attack

Evaluation

Conclusion