Physical Layer Security Enhancement with MIMO Systems: Authentication and Key Establishment

Michael Jensen, Sneha Kasera
Chan Chen, Yan Shi, Yanling Yang
PHY Security and Reliability

Topics Covered

• **Secret-Key Establishment**
  – MIMO-enabled performance bounds
  – Key-establishment algorithms and protocols

• **Authentication**
  – Radio finger-printing measurements
  – Performance impact of MIMO

Other Developments

• **Robust MIMO Scheduling**
  – Parametric-based scheduling for multi-user MIMO networks

• **Network Channel Modeling**
  – Analysis of covariance behavior using novel closed-form analysis

• **Cooperative MIMO Communications**
  – Novel measurements from coherent base stations
Key Question: How can Alice and Bob securely distribute the secret key?
Motivation

Conventional Key Distribution

Key Distribution Center

- E(S; M_{a\leftrightarrow KDC})
- E(S; M_{b\leftrightarrow KDC})

Alice
Bob

Pre-shared Master Key
Session Key
Encryption Function

Vulnerabilities
- Delivery of master keys
- Centralized key control

Diffie-Hellman Exchange

Alice

Generate
\( X_a < p \)

Calculate
\( Y_a = \text{mod}(\alpha^{X_a}, p) \)

Calculate
\( K = \text{mod}(Y_b^{X_a}, p) \)

Bob

Generate
\( X_b < p \)

Calculate
\( Y_b = \text{mod}(\alpha^{X_b}, p) \)

Calculate
\( K = \text{mod}(Y_a^{X_b}, p) \)

Vulnerabilities
- Computational power increases
- Discovery of efficient methods for solving discrete logarithms
Motivation
Secret-Key Establishment

Establish Key by Exploiting Common Randomness

common randomness

Alice

Bob

$X$  $Y$

$I(X;Y)$

Eve

$Z$

Reciprocal channel = common randomness

More antennas = more randomness?

$H_{ba} = H + \Delta H_{ba}$

$H_{ab} = H + \Delta H_{ab}$

$I(H; H_{ae}) = I(H; H_{be}) = 0$
Analysis
Bound on Secret Key Establishment

Performance

Stack samples within one interval into vectors: \[ h_a = h + \Delta h_a \]
\[ h_b = h + \Delta h_b \]

Bound on # bits generated: \[ I_B = I(h_a, h_b) \]
\[ = \log_2 \frac{|R + \sigma_n^2 I|}{|R + \sigma_n^2 I - R(R + \sigma_n^2 I)^{-1} R|} \]

\[ R = E\{h h^H\} \]
Key Establishment Bound
Different Sampling Strategies (SISO)

Fixed Segment Length

- $L_c$
- $K = 2$
- $K = 3$
- $K = 4$

Fixed Sample Interval

- $d$
- $K = 2$
- $K = 3$
- $K = 4$

Graphs showing the relationship between the number of samples and the bound on key length for different segment lengths and sample intervals.

$L_{key} = 128$
Channel Quantization
Dynamic Detection Region

Dramatically improves probability of key agreement

Alice sends subregion bit

Bob modifies detection region
CSI-Based Key Establishment
MIMO and Channel Quantization

MIMO Advantage: Increased # of random variables
MIMO Disadvantage: Correlation of random variables

Channel Matrix Sequence

Construct Space-Time Covariance

Whiten

Quantization

\[
H^{(1)}, H^{(2)}, \ldots, H^{(N)}
\]

\[
h = \begin{bmatrix}
\text{vec}\{H^{(1)}\}^T & \text{vec}\{H^{(2)}\}^T & \cdots & \text{vec}\{H^{(K)}\}^T
\end{bmatrix}^T
\]

\[
R = \mathbb{E}\{hh^H\} = USU^H
\]

\[
h_0 = U^H h
\]
Channel Quantization
Determining Quantization Level

Simulation:
- i.i.d. Gaussian channel
- i.i.d. Gaussian noise
- 128-bit key

\[ h_0 = U^H h \quad \Rightarrow \quad \mathbb{E}\{h_0 h_0^H\} = S \]

Quantization level for each element of \( h_0 \) based on eigenvalue to achieve a specified KER
Channel Quantization
Space-Time Whitening

\[ R_a = E\{h_a h_a^H\} = U_a S_a U_a^H \]
\[ R_b = E\{h_b h_b^H\} = U_b S_b U_b^H \]

Whiten each channel using own eigenvectors
Whiten both channels using \( U_a \)

Using common eigenvectors dramatically improves key agreement performance
Correlated MIMO Channels Performance

KER for Different Algorithms

KER for Different Arrays

KER = 10^{-3}

L_{\text{key}} = 128
Correlated MIMO Channels Performance using Measured Data

\[ d = \frac{L_c}{9} \]

2x2

KER = 10^{-3}

\[ L_{\text{key}} = 128 \]
Channel Quantization
Dynamic Detection Region

More subdivisions, better key agreement
KER Performance
Impact of Increased Subregions

KER vs. SNR

SNR to Achieve KER = $10^{-3}$
vs. # subregions
PHY Security and Reliability

Topics Covered

• **Secret-Key Establishment**
  – MIMO-enabled performance bounds
  – Key-establishment algorithms and protocols

• **Authentication**
  – Radio fingerprinting measurements
  – Performance impact of MIMO

Other Developments

• **Robust MIMO Scheduling**
  – Parametric-based scheduling for multi-user MIMO networks

• **Network Channel Modeling**
  – Analysis of covariance behavior using novel closed-form analysis

• **Cooperative MIMO Communications**
  – Novel measurements from coherent base stations
Radio Fingerprinting
General Concept

Transmitter has Unique “Radio Signature” → Authentication

• How does signature time variation impact authentication?
• What is impact of MIMO (multiple radios) on authentication?
Radio Fingerprinting Measurements

- Measurement of 21 MIMO NICs (three antennas each)
- Recorded 14 different radiometric features for each radio
- Use maximum relevance minimum redundancy (MRMR) to select best subset of features for identification
- Use bagging algorithm to perform classification based on training data
Radio Fingerprinting
Feature Selection

Observations

• MIMO significantly outperforms SISO
• 3 features achieve most of performance (frequency error, sync correlation, IQ offset)
Radio Fingerprinting
Feature Selection

Observations
- Relatively small amount of training yields good performance
- Observing over more time significantly improves worst case performance
PHY Security and Reliability

Topics Covered

• Secret-Key Establishment
  – MIMO-enabled performance bounds
  – Key-establishment algorithms and protocols

• Authentication
  – Radio fingerprinting measurements
  – Performance impact of MIMO

Other Developments

• Robust MIMO Scheduling
  – Parametric-based scheduling for multi-user MIMO networks

• Network Channel Modeling
  – Analysis of covariance behavior using novel closed-form analysis

• Cooperative MIMO Communications
  – Novel measurements from coherent base stations
Papers Published in Peer-Reviewed Journals (5 additional in review)


Papers Published in Peer-Reviewed Conference Proceedings