Secure Identification for Gaussian Channels

Wafa Labidi, Christian Deppe and Holger Boche

Technische Universität München
Lehrstuhl für Theoretische Informationstechnik

ICASSP 2020
Outline

1 Identification: Overview

2 Identification for the Gaussian Wiretap Channel

3 Conclusions
Outline

1 Identification: Overview

2 Identification for the Gaussian Wiretap Channel

3 Conclusions
What is Identification?

Alice

\[ m \rightarrow \text{Enc} \rightarrow x^n \in X^n \rightarrow \text{noisy channel} W^n \rightarrow y^n \in Y^n \rightarrow \text{Dec} \rightarrow m' \text{ transmitted or not?} \]

Bob

Ahlswede/Dueck Picture 1989
What is Identification?

Shannon Picture 1948

• Receiver’s goal: What is the message sent?

• Sender chooses and sends the message $m \in \mathcal{M} = \{1, \ldots, M = 2^{nC}\}$

Ahlswede/Dueck Picture 1989

• Receiver’s goal: Is $m'$ the message sent?

• Sender chooses and sends the identity $m \in \mathcal{N} = \{1, \ldots, N = 2^{2nC}\}$
Randomized Identification (ID)-Code

Randomized ID-code

A randomized \((n, N, \lambda_1, \lambda_2)\) ID-code for a discrete memoryless channel (DMC) \(W\) is a family of pairs \(\{(Q_i, D_i)\mid i = 1, \ldots, N\}\) with \(\lambda_1, \lambda_2 \leq \lambda < \frac{1}{2}\) and \(\forall i \in \{1, \ldots, N\}:\)

- \(Q_i \in \mathcal{P}(X^n), D_i \subseteq Y^n\)
- \(\sum_{x^n \in X^n} Q_i(x^n) W^n(D^c_i|x^n) \leq \lambda_1 \iff \text{channel noise}\)
- \(\sum_{x^n \in X^n} Q_j(x^n) W^n(D_i|x^n) \leq \lambda_2 \iff \text{ID-code}\)
Randomized ID-Code

$y^n = x^n$ 

$\mathcal{D}_i \propto \lambda_2^{(i,j)} \mathcal{D}_j$ 

ID-code for a binary noiseless channel
Randomized ID-Code

$y^n = x^n$

$D_i \propto \lambda_2^{(i,j)}$

$D_j \propto \lambda_2^{(j,k)}$

$D_k \propto \lambda_2^{(j,l)}$

ID-code for a binary noisless channel
Randomized ID-Code

\[ y^n = x^n \]

\[ \propto \lambda_2^{(i,k)} \]

\[ \propto \lambda_2^{(i,j)} \]

\[ \propto \lambda_2^{(j,l)} \]

\[ \propto \lambda_2^{(i,l)} \]

ID-code for a binary noisless channel
Randomized ID-Code

Secure Identification for Gaussian Channels
Theorem

Let $W$ be a finite DMC and $N(n, \lambda)$ the maximal number s.t. an $(n, N, \lambda_1, \lambda_2)$ ID-code for $W(f, P)$ exists with $\lambda_1, \lambda_2 \leq \lambda$ then:

$$C_{ID}(W) = C(W), \quad \forall \lambda \in (0, \frac{1}{2})$$

$C(W)$ is the Shannon transmission capacity of $W$, $C_{ID}(W) \triangleq \lim_{n \to \infty} \frac{1}{n} \log \log N(n, \lambda)$

---

To send a message $i$, we prepare a set of coloring functions $T_i$ known by the sender and the receiver(s)
To send a message $i$, we prepare a set of coloring functions $T_i$ known by the sender and the receiver(s):

$$T_i : \{1, \ldots, M'\} \rightarrow \{1, \ldots, M''\}$$

$$j \mapsto T_i(j)$$

\[\begin{array}{c|c|c|c|c}
1 & \multicolumn{3}{c|}{\cdots} & M' \\
2 & \multicolumn{3}{c|}{\cdots} & M'' \\
\vdots & \multicolumn{3}{c|}{\cdots} & \vdots \\
j & \multicolumn{3}{c|}{\cdots} & \vdots \\
\vdots & \multicolumn{3}{c|}{\cdots} & \vdots \\
M' & \multicolumn{3}{c|}{T_1} & T_1(1) = T_N(1) = 2
\end{array}\]

\[\begin{array}{c|c|c|c|c}
1 & \multicolumn{3}{c|}{\cdots} & M' \\
2 & \multicolumn{3}{c|}{\cdots} & M'' \\
\vdots & \multicolumn{3}{c|}{\cdots} & \vdots \\
j & \multicolumn{3}{c|}{\cdots} & \vdots \\
\vdots & \multicolumn{3}{c|}{\cdots} & \vdots \\
M' & \multicolumn{3}{c|}{T_N} & T_N(1) = T_N(1) = 2
\end{array}\]
Direct Proof: Coding Scheme

1. To send a message $i$, we prepare a set of coloring functions $T_i$ known by the sender and the receiver(s).

2. The sender chooses a coloring $j$ randomly and calculates the color of the message $i$ under coloring $j$ denoted by $T_i(j)$. 

Send $(j, T_i(j))$ over the channel.

The receiver, interested in $i'$, calculates $T_i'(j)$.

If $T_i(j) = T_i'(j)$, then $i = i'$. 

Secure Identification for Gaussian Channels 9
To send a message $i$, we prepare a set of coloring functions $T_i$ known by the sender and the receiver(s).

The sender chooses a coloring $j$ randomly and calculates the color of the message $i$ under coloring $j$ denoted by $T_i(j)$.

Send $(j, T_i(j))$ over the channel.
Direct Proof: Coding Scheme

1. To send a message $i$, we prepare a set of coloring functions $T_i$ known by the sender and the receiver(s).
2. The sender chooses a coloring $j$ randomly and calculates the color of the message $i$ under coloring $j$ denoted by $T_i(j)$.
3. Send $(j, T_i(j))$ over the channel.
4. The receiver, interested in $i'$, calculates $T_{i'}(\hat{j})$. 

Secure Identification for Gaussian Channels
To send a message $i$, we prepare a set of coloring functions $T_i$ known by the sender and the receiver(s)

The sender chooses a coloring $j$ randomly and calculates the color of the message $i$ under coloring $j$ denoted by $T_i(j)$

Send $(j, T_i(j))$ over the channel

The receiver, interested in $i'$, calculates $T_{i'}(j)$

If $T_i(j) = T_{i'}(j)$, then $i = i'$
Direct Proof: Code Construction

\[ \mathcal{C}' = \{ (u'_j, D'_j), j \in \{1, \ldots, M'\} \} \]
\[ (n, M', 2^{-n\gamma}) \]
\[ |\mathcal{C}'| = \lceil 2^n(C - \epsilon) \rceil \]

\[ \mathcal{C}'' = \{ (u''_k, D''_k), k \in \{1, \ldots, M''\} \} \]
\[ (\lceil \sqrt{n} \rceil, M'', 2^{-\sqrt{n}\gamma}) \]
\[ |\mathcal{C}''| = \lceil 2^{\sqrt{n}\epsilon} \rceil \]

\[ \in \mathcal{C} = \{ (Q_i, D_i), i \in \{1, \ldots, N\} \} \]
Outline

1 Identification: Overview

2 Identification for the Gaussian Wiretap Channel

3 Conclusions
Wiretap Channel

Requirements:

- Secrecy (here strong): $I(M; Z^n) \leq \xi_1$, $\xi_1 > 0$
- Reliability: $P_e^{(n)} \triangleq \Pr[\hat{M} \neq M] \leq \xi_2$, $\xi_2 > 0$
Dichotomy Theorem

We denote by $C(W)$ the capacity of the channel $W$ and by $C_{SID}(W, V)$ the identification capacity of the wiretap channel $(W, V)$ then:

$$C_{SID}(W, V) = \begin{cases} C(W) & \text{if } C_S(W, V) > 0 \\ 0 & \text{if } C_S(W, V) = 0 \end{cases}$$

---

Proof: Code Construction

transmission code
\[ C' = \{ (u'_j, D'_j), j \in \{1, \ldots, M'\} \} \]

|C'| = \lceil 2^{n(C - \epsilon)} \rceil

wiretap code
\[ C'' = \{ (u''_k, D''_k), k \in \{1, \ldots, M''\} \} \]

|C''| = \lceil 2^{\sqrt{n} \epsilon} \rceil

\[ u' \in C = \{ (Q_i, D_i), i \in \{1, \ldots, N\} \} \]
Wiretap transmission codes

An \((n, M, \lambda)\) wiretap code for \((W, V, g, g', P)\) is a family of pairs \(\{(Q(\cdot|i), D_i), \ i = 1, \ldots, M\}\) such that for all \(i \in \{1, \ldots, M\}\):

\[
\begin{align*}
\text{• } & Q(\cdot|i) \in \mathcal{P}(X^n), \quad D_i \subset Y^n \\
\text{• } & D_i \cap D_j = \emptyset, \quad \forall i \neq j \\
\text{• } & \int_{x^n \in X^n} Q(x^n|i) W^n(D_i^c|x^n) dx^n x^n \leq \lambda \\
\text{• } & I(U; Z^n) \leq \lambda
\end{align*}
\]
A randomized \((n, N, \lambda_1, \lambda_2)\) wiretap ID-code for \((V, W, g, g', P)\) is a family of pairs \(\{(Q(\cdot|i), D_i), i = 1, \ldots, N\}\) such that for \(\lambda_1, \lambda_2 \leq \lambda < \frac{1}{2}\), \(\forall \mathcal{E} \subset \mathbb{Z}^n, \forall i:\)

\[
\begin{align*}
\bullet & \quad Q(\cdot|i) \in P(X^n), \quad D_i \subset Y^n \\
\bullet & \quad \sum_{l=1}^{n} x_l^2 \leq n \cdot P, \quad \forall x^n \in X^n \\
\bullet & \quad \int_{x^n \in X^n} Q(x^n|i)W^n(D_i^c|x^n)d^n x^n \leq \lambda_1 \\
\bullet & \quad \int_{x^n \in X^n} Q(x^n|j)W^n(D_i|x^n)d^n x^n \leq \lambda_2, \quad \forall i \neq j \\
\bullet & \quad \int_{x^n \in X^n} Q(x^n|j)V^n(\mathcal{E}|x^n) + Q(x^n|i)V^n(\mathcal{E}^c|x^n)d^n x^n \geq 1 - \lambda, \quad \forall i \neq j
\end{align*}
\]
Extension for the Gaussian Case

- **W**: $y_i = x_i + n_i, \quad n_i \sim \mathcal{N}(0, N) \triangleq g, \quad 1 \leq i \leq n$
- **V**: $z_i = x_i + n'_i, \quad n'_i \sim \mathcal{N}(0, N') \triangleq g', \quad 1 \leq i \leq n$
- Average power constraint: $\frac{1}{n} \sum_{i=1}^{n} x_i^2 \leq P$
- $Y = Z = \mathbb{R}$

$\Rightarrow$ We call this channel $(W, V, g, g', P)$
Extension for the Gaussian Case: Dichotomy Theorem

Theorem \( (\text{Secure identification capacity}) \)

Let \( C_{\text{SID}}(g, g', P) \) be the identification capacity of the wiretap channel \( (W, V, g, g', P) \) then:

\[
C_{\text{SID}}(g, g', P) = \begin{cases} 
C(g, P) & \text{if } C_S(g, g', P) > 0 \\
0 & \text{if } C_S(g, g', P) = 0
\end{cases}
\]
Outline

1 Identification: Overview

2 Identification for the Gaussian Wiretap Channel

3 Conclusions
Conclusions and Outlook

• We provided a coding scheme for the Gaussian wiretap channel and calculated the corresponding secure identification capacity. 😊

• Future:
  • Explore identification and secure identification for the single-user MIMO channel
  • Investigate identification over multi-user MIMO channels