Full-duplex vs. Half-duplex secret-key generation

Hendrik Vogt, Aydin Sezgin

WIFS 2015
Rome, Italy
Contents

1 Full-duplex and key generation

2 System model

3 Performance metrics

4 Results
Contents

1 Full-duplex and key generation

2 System model

3 Performance metrics

4 Results
Full-duplex and key generation

Classic secret-key generation

Basic idea: Utilize reciprocal channel states as shared secret

Channel estimation by half-duplex (HD) probing
Full-duplex and key generation

Classic secret-key generation

Basic idea: Utilize reciprocal channel states as shared secret

Channel estimation by **half-duplex (HD)** probing

Alice and Bob “talk” about their estimations by **HD** communication (**key reconciliation**)
Full-duplex and key generation

Classic secret-key generation

Basic idea: Utilize reciprocal channel states as shared secret

1. Channel estimation by **half-duplex (HD) probing**

2. Alice and Bob “talk” about their estimations by **HD communication (key reconciliation)**

3. Reduce leakage to eavesdropper (**privacy amplification**)

```
<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bob</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
```
Full-duplex and key generation

Classic secret-key generation

Basic idea: Utilize reciprocal channel states as shared secret

1. Channel estimation by half-duplex (HD) probing
2. Alice and Bob “talk” about their estimations by HD communication (key reconciliation)
3. Reduce leakage to eavesdropper (privacy amplification)
4. Bit strings are declared as secret key
In-band full-duplex (IBFD)

- IBFD means transmitting/receiving at the **same** time and **frequency** band
- Key technology in 5G
- Self-interference problem is challenging, but manageable (successful prototypes!)
In-band full-duplex (IBFD)

- IBFD means transmitting/receiving at the same time and frequency band
- Key technology in 5G
- Self-interference problem is challenging, but manageable (successful prototypes!)

Key advantage

Simultaneous channel probing is **downgrading** an eavesdropper!
Full-duplex and key generation

Proposed secret-key generation

1. Channel estimation by **full-duplex (FD) probing**

2. Alice and Bob “talk” about their estimations by **FD communication (key reconciliation)**

3. ... 

4. ...
Contents

1 Full-duplex and key generation

2 System model

3 Performance metrics

4 Results
**System model**

**Nodes in scene**

- Single-antenna scenario, multi-antenna Eve emulated by higher correlation
- Channels comply with real-valued flat-fading model
- Alice and Bob can switch between HD and FD mode
System model

Execution flow

Channel coherence block

Probing phase

Reconciliation phase

Probing phase

Obtain channel estimations by probing

Reconciliation phase

Alice transmits message to Bob

Key generation

Based on estimations and reconciliation, Alice and Bob agree on a key
### System model

#### Probing phase (HD mode)

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td></td>
<td>$x = \sqrt{\text{snr}} h_{ba} + n_{a}$</td>
</tr>
<tr>
<td>Bob</td>
<td></td>
<td>$y = \sqrt{\text{snr}} h_{ab} + n_{b}$</td>
</tr>
<tr>
<td>Eve</td>
<td></td>
<td>$z_{1} = \sqrt{\text{snr}<em>{ae}} h</em>{ae} + n_{ae}$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$z_{2} = \sqrt{\text{snr}<em>{be}} h</em>{be} + n_{be}$</td>
</tr>
</tbody>
</table>

- Channels $h_{ij}$ are jointly **Gaussian** distributed with zero mean and unit variance
- Correlation measure $\mathbb{E}[h_{ba} h_{ab}] = \delta \cdot \rho_{ba}$
- Parameter $0 < \delta < 1$ denotes the **penalty** of delayed HD probing
System model

Probing phase (FD mode)

<table>
<thead>
<tr>
<th></th>
<th>Equation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>$x = \sqrt{\text{snr}} h_{ba} + \alpha \sqrt{\text{snr}} n_{la} + n_a$</td>
</tr>
<tr>
<td>Bob</td>
<td>$y = \sqrt{\text{snr}} h_{ab} + \alpha \sqrt{\text{snr}} n_{lb} + n_b$</td>
</tr>
<tr>
<td>Eve</td>
<td>$z = \sqrt{\text{snr}<em>{ae}} h</em>{ae} + \sqrt{\text{snr}<em>{be}} h</em>{be} + n_e$</td>
</tr>
</tbody>
</table>

- Alice and Bob suffer from Gaussian self-interference (SI)
- Parameter $0 < \alpha < 1$ denotes the strength of residual SI
- Eve obtains only a superposition of probing signals
System model

Reconciliation phase

- Alice sends an authenticated, public message to Bob

- This is *point-to-point* communication over a fading channel

- Bob has only *partial* channel state information

**Communication rate** $R_p$

Number of bits per channel use that satisfy **reliability** condition
Contents

1 Full-duplex and key generation

2 System model

3 Performance metrics

4 Results
Performance metrics

Rates

Secret-key rate $R_{sk}$:

Number of bits per channel estimation that satisfy

1. Reliability
2. Uniformity
3. Secrecy

conditions.

- Functional relationship between $R_{sk}$ and communication rate $R_p$:
  Key-communication function
Performance metrics

Key-communication function

\[ R_{sk}(R_p) = \frac{\beta}{2} \log_2 \left( 1 - 2^{-2 \frac{R_p}{\beta}} \left( \|b_x\|^2 - \|e_x\|^2 \right) + \|b_x\|^2 \right) \]

<table>
<thead>
<tr>
<th>( \beta )</th>
<th><strong>Time-sharing</strong> of probing and reconciliation phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>( R_p )</td>
<td>Communication rate during reconciliation phase</td>
</tr>
<tr>
<td>( |b_x|^2 )</td>
<td>Quality of <strong>legitimate users’</strong> estimation</td>
</tr>
<tr>
<td>( |e_x|^2 )</td>
<td>Quality of <strong>Eve’s</strong> estimation</td>
</tr>
</tbody>
</table>
**Performance metrics**

**Key-communication function**

\[ R_{sk}(R_p) = \frac{\beta}{2} \log_2 \frac{1 - 2^{-2} \frac{R_p}{\beta} (\|b_x\|^2 - \|e_x\|^2) + \|b_x\|^2}{1 + \|e_x\|^2} \]

**Property**

\( R_{sk} \) is **positive** if and only if

1. \( R_p > 0 \),
2. \( \|b_x\|^2 > \|e_x\|^2 \)

hold.
Performance metrics

Key-communication function

\[ R_{sk}(R_p) = \frac{\beta}{2} \log_2 \left( 1 - 2^{-2} \frac{R_p}{\beta} (\|b_x\|^2 - \|e_x\|^2) + \|b_x\|^2 \right) \]

- We apply the key-communication function to HD and FD modes
- HD mode - Upper bound
  \[ R_{sk}^{HD}(R_{p}^{HD}) < \bar{R}_{sk}^{HD} \]
- FD mode - Lower bound
  \[ R_{sk}^{FD}(R_{p}^{FD}) > \bar{R}_{sk}^{FD} \]
Contents

1. Full-duplex and key generation
2. System model
3. Performance metrics
4. Results
### Results

#### HD vs. FD performance

![Graph showing HD vs. FD performance](image)

- **Parameters**
  - $\rho_{ae} = \rho_{be} = \rho_e = 0.4$, $\rho_{ba}^2 = 1$, $\delta = 0.97$, $\text{snr}_{ae} = \text{snr}_{be} = \text{snr}$ and $\beta = 0.5$
Results

Probing-reconciliation trade-off

Time-sharing $\beta$ between probing and reconciliation phase can be optimized.

![Graph showing the relationship between $\beta^*$ and $\text{snr}$ (dB).]

- Parameters: $\rho_{ba} = 1$, $\delta = 0.95$, $\rho_{ae} = \rho_{be} = \rho_e = 0.4$, $\text{snr}_{ae} = \text{snr}_{be} = \text{snr}$ and $\alpha = -15$ dB.
Results

Conclusion

- We formulate a system model for channel probing and reconciliation phases for HD and FD modes.
- We derive the key-communication function and provide bounds for HD and FD modes.
- Simulations show FD system often performs better than HD, the impact of SI is insignificant.
- Trade-off between probing and reconciliation phase is different for HD and FD modes.
Thank you! Any questions?