Safeguarding the 5G Era and Beyond with Physical Layer Wireless Security

Nan (Jonas) Yang*, Xiangyun (Sean) Zhou*, and Jemin Lee†

*Research School of Electrical, Energy and Materials Engineering
The Australian National University, Canberra, ACT, Australia

†Information and Communication Engineering
Daegu Gyeongbuk Institute of Science and Technology, Daegu, South Korea

24 May 2019
Outline

• Security in mobile communication networks
  – Evolution of cellular networks
  – Security issues in cellular networks
  – Re-shape security design in 5G and beyond wireless networks

• Theoretical advancement in PHY layer security
  – Fundamentals of PHY layer security
  – Existing secrecy performance metrics
  – New secrecy performance metrics
  – Trust degree-aided secure communication
  – PHY layer key generation

• Cutting-edge PHY layer security solutions
  – Heterogeneous secure communication
  – Full-duplex secure communication
  – Massive MIMO-aided secure communication
  – Secure communication over mmWave channels
  – Machine type secure communication
  – NOMA-based security
  – Security for URLLC
  – Energy-efficient secure communication
  – Unmanned aerial vehicle secure communication
  – Software defined radio-based prototyping

• Future directions, challenges and open issues
  – PHY layer security beyond content secrecy
  – Cross-layer security
  – Challenges imposed by future wireless world
Outline

- Security in mobile communication networks
  - Evolution of cellular networks
  - Security issues in cellular networks
  - Re-shape security design in 5G and beyond wireless networks

- Theoretical advancement in PHY layer security
  - Fundamentals of PHY layer security
  - Existing secrecy performance metrics
  - New secrecy performance metrics
  - Trust degree-aided secure communication
  - PHY layer key generation

- Cutting-edge PHY layer security solutions
  - Heterogeneous secure communication
  - Full-duplex secure communication
  - Massive MIMO-aided secure communication
  - Secure communication over mmWave channels
  - Machine type secure communication
  - NOMA-based security
  - Security for URLLC
  - Energy-efficient secure communication
  - Unmanned aerial vehicle secure communication
  - Software defined radio-based prototyping

- Future directions, challenges and open issues
  - PHY layer security beyond content secrecy
  - Cross-layer security
  - Challenges imposed by future wireless world

©Nan Yang, Xiangyun Zhou, and Jemin Lee
We Are in a Wireless World

• In today’s networked society, we need connections to move ahead.
• To enable such a society, mobile phones may be the most successful consumer product of the age.
• Built on this together with other wireless devices, wireless communications have been instrumental in transforming our contemporary societies in the past decades.
• From the first-generation (1G) of analogue mobile phone systems to the commercial fourth-generation (4G) long-term evolution (LTE) networks deployed widely across the globe, wireless communications have fundamentally alter the ways as to how humans in the modern society access, exchange, and share information with each other.
• With the launching of 5G, we are now at an era of mobile wireless Internet with explosive big data.
Cellular Wireless Evolution

1G
1st Generation wireless network
- Basic voice service
- Analog-based protocols

2G
2nd Generation wireless network
- Designed for voice
- Improved coverage and capacity
- First digital standards (GSM, CDMA)

3G
3rd Generation wireless network
- Designed for voice with some data consideration (multimedia, text, internet)
- First mobile broadband

4G
4th Generation wireless network
- Designed primarily for data
- IP-based protocols (LTE)
- True mobile broadband

The Need for Speed
- 1G: 2.4 kbps
- 2G: 64 kbps
- 3G: 2,000 kbps
- 4G: 100,000 kbps


©Nan Yang, Xiangyun Zhou, and Jemin Lee
Security Issues In Cellular Networks

• The infrastructure for cellular networks is massive, complex with multiple entities coordinating together, such as the IP Internet coordinating with the core network. Therefore, it presents a challenge for the network to provide security at every possible communication path.

• Limitations of cellular networks
  – Open wireless access medium: Wireless channel has no physical barrier separating an attacker.
  – Limited bandwidth: Everyone shares the medium, although wiretap bandwidth is increasing.
  – System complexity: Adding more complexity to systems introduce new security vulnerabilities.
  – Limited power: Wireless devices typically have a limited time battery life.
  – Limited processing capability: The processors are not powerful enough to carry out intensive processing.
  – Relatively unreliable network connection: The wireless medium is an unreliable medium with a high rate of errors, compared to a wired network.
Security Issues In Cellular Networks

• Security Issues
  – Confidentiality: With the increased use of cellular phones in sensitive communication, there is a need for a secure channel in order to transmit information.
  – Integrity: With services such as SMS, chat and file transfer, it is important that the data arrives without any modifications.
  – Authentication: Since the purpose of cellular network is to enable people to communicate from anywhere in the world, the issue of cross region and cross provider authentication becomes an issue.
  – Access control: The cellular device may have files that need to have restricted access to them. The device might access a database where some sort of role based access control is necessary.
  – Operating systems in mobile devices: Cellular phones have evolved from low processing power, ad-hoc supervisors to high power processors and full fledged operating systems. Issues may arise in the OS which might open security holes.
Security Issues In Cellular Networks

• Security Issues
  – Web services: A web service is a component that provides functionality accessible through the web using the standard HTTP protocol. This opens the cellular device to various security issues such as viruses, buffer overflows, denial of service attacks etc.
  – Viruses and malware: With increased functionality provided in cellular systems, problems prevalent in larger systems such as viruses and malware arise. An affected device can also be used to attack the cellular network infrastructure by becoming part of a large scale denial of service attack.
  – Downloaded contents: Spyware might be downloaded causing security issues. Another problem is that of digital rights management.
  – Device security: If a device is lost or stolen, it needs to be protected from unauthorised use so that potential sensitive information such as emails, documents, phone numbers etc. cannot be accessed.
Taking 4G Network as an Example

This is the focus of physical layer security.

Illustration of basic LTE network architecture.


©Nan Yang, Xiangyun Zhou, and Jemin Lee
Taking 4G Network as an Example

• Key security threats/risks in the **Access** segment

  – **Physical attacks**: LTE connection in densely populated areas have given rise to smaller cell sites, installation of eNodeB’s in public locations (such as shopping malls, utility poles), introduction of femtocells and installation of less expensive Home eNodeBs on the LTE edge. eNodeB’s in public location are vulnerable to physical tampering allowing for unauthorised access to the network.

  – **Rogue eNodeB**: Smaller LTE eNodeB’s are not cost prohibitive. Being accessible, attackers attempt to introduce rogue eNodeB’s into the LTE network to impersonate the operator’s node and to intercept voice and data transmission from the UE.

  – **Eavesdropping**: Attackers can take advantage of a known weakness in LTE wherein the user identity transference occurs unencrypted during the initial attach procedure. This allows an eavesdropper to track user cell location and information.

Some physical layer methods need to be used to improve the security of wireless networks.


©Nan Yang, Xiangyun Zhou, and Jemin Lee
What Does 5G and Beyond Look Like?

- Wireless networks in 5G and beyond era are a unifying connectivity fabric for society.

Enhanced mobile broadband

Mission-critical services

Massive Internet of Things

Unifying connectivity platform for future innovation

Convergence of spectrum types/bands, diverse services, and deployments


©Nan Yang, Xiangyun Zhou, and Jemin Lee
Diverse Service and Devices in 5G and Beyond

- Ultra-low energy: 10+ years of battery life
- Ultra-low complexity: 10s of bits per second
- Ultra-high density: 1 million nodes per Km²
- Extreme capacity: 10 Tbps per Km²
- Extreme data rates: Multi-Gbps peak rates; 100+ Mbps user experienced rates

- Deep coverage: To reach challenging locations
- Mission-critical control: Ultra-high reliability <1 out of 100 million packets lost
- Ultra-low latency: As low as 1 millisecond
- Extreme user mobility: Or no mobility at all
- Strong security: e.g. Health / government / financial trusted
- Discovery and optimization:


©Nan Yang, Xiangyun Zhou, and Jemin Lee
5G and Beyond: Touching All Aspects of Life

Precision agriculture → Real-time shipping → Smart logistics → Autonomous driving

Sustainable society → Immersive commerce

Immersive entertainment → Drone delivery → Flexible manufacturing → Collaborative workspace

Qualcomm, “5G: The Fabric for Society”, June 2018
©Nan Yang, Xiangyun Zhou, and Jemin Lee
New technologies brought both challenges and opportunities to safeguard the 5G and beyond era.


©Nan Yang, Xiangyun Zhou, and Jemin Lee
Outline

• Security in mobile communication networks
  – Evolution of cellular networks
  – Security issues in cellular networks
  – Re-shape security design in 5G and beyond wireless networks

• Theoretical advancement in PHY layer security
  – Fundamentals of PHY layer security
  – Existing secrecy performance metrics
  – New secrecy performance metrics
  – Trust degree-aided secure communication
  – PHY layer key generation

• Cutting-edge PHY layer security solutions
  – Heterogeneous secure communication
  – Full-duplex secure communication
  – Massive MIMO-aided secure communication
  – Secure communication over mmWave channels
  – Machine type secure communication
  – NOMA-based security
  – Security for URLLC
  – Energy-efficient secure communication
  – Unmanned aerial vehicle secure communication
  – Software defined radio-based prototyping

• Future directions, challenges and open issues
  – PHY layer security beyond content secrecy
  – Cross-layer security
  – Challenges imposed by future wireless world
Physical Layer Security Fundamentals

- Objectives of physical layer security:
  - **Reliability**: Bob can decode the message error-free (perfect reliability)
    \[
    \mathbb{P}(\hat{M} = M) \to 1
    \]
  - **Secrecy**: Eve obtains no information about the message (perfect secrecy)
    \[
    \mathbb{I}(Z, M) \to 0
    \]
  - The symbol “⟶” has different definitions which lead to different level of secrecy.
More rigorously, we know the following information:

- The confidential message, $M$, is encoded into a sequence of symbols (codeword) denoted as a vector of length $n$, i.e., $X^n$. The received symbol vectors are $Y^n$ and $Z^n$.

- Strong secrecy:
  \[ \lim_{n \to \infty} I(M; Z^n) = 0. \]

- Weak secrecy:
  \[ \lim_{n \to \infty} \frac{1}{n} I(M; Z^n) = 0. \]

- With a slight abuse of terminology, we will refer to both as “perfect secrecy”.
Physical Layer Security Fundamentals

- Reliability and secrecy performance depend on the capacity of Bob and Eve’s channel.
- Intuitive and non-rigorous understanding: capacity means the capability of differentiating different patterns/regions.

<table>
<thead>
<tr>
<th>Capacity = 2 bits</th>
<th>Capacity = 3 bits</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Diagram 2 bits" /></td>
<td><img src="image2.png" alt="Diagram 3 bits" /></td>
</tr>
<tr>
<td>4 different patterns/regions</td>
<td>8 different patterns/regions</td>
</tr>
</tbody>
</table>
Physical Layer Security Fundamentals

- **Secure Encoding (Wiretap code):**
  - Alice has $K$ possible messages to sent. The amount of information carried by one message (# of bits per message): $R_s = \log_2 K$.
  - For each message, Alice generates $N$ different codewords. Hence, the # bits carried by one codeword: $R_b = \log_2 KN$.
  - For example: $K = 2$ and $N = 4$, i.e., $R_s = 1$ bit and $R_b = 3$ bits.
  - Codebook:
    $\begin{bmatrix}
    x_{1,a} & x_{1,b} & x_{1,c} & x_{1,d} \\
    x_{2,a} & x_{2,b} & x_{2,c} & x_{2,d}
    \end{bmatrix}$
  - where each $x$ is a codeword, i.e., a sequence of symbols.
  - When Alice wants to transmit one message, she randomly transmits one of the $N$ codewords that belong to this message.
  - That is, $R_b$ bits are transmitted to carry $R_s$ bits of information.
  - The rate redundancy, $R_e = R_b - R_s = \log_2 N$, represents the randomness added into the code to confuse Eve.
Physical Layer Security Fundamentals

- Encoding rate parameters: $R_s = 1$ bit, $R_b = 3$ bits, $R_e = 2$ bits.
  - If Bob’s channel capacity $> R_b$, it can easily differentiate 8 patterns/regions, hence perfect reliability is achieved.
  - If Eve’s channel capacity $\leq R_e$, it can at most differentiate 4 patterns/regions, hence perfect secrecy is achieved.
More rigorously, one needs to construct a coding scheme (e.g., based on random binning) to show:

- If Bob’s channel capacity > $R_b$, then $\mathbb{P}(\hat{M} = M) \to 1$
- If Eve’s channel capacity ≤ $R_e$, then $\mathbb{I}(Z, M) \to 0$
- Thus, if the channel state information (CSI) of both links is known to the legitimate users, it is possible to construct a coding scheme with carefully chosen rate parameters ($R_b$ and $R_e$) to achieve both perfect reliability and perfect secrecy.
Existing Physical Layer Security Metrics

- Performance metric for physical layer security was first developed by in 1970s, when research was focused on the wired AWGN channel.
- **Secrecy capacity** over AWGN channel: The maximum achievable rate satisfying perfect reliability and perfect secrecy:
  \[ C_s = [C_b - C_e]^+ \]
  or in terms of SNR:
  \[ C_s = [\log_2(1 + \gamma_b) - \log_2(1 + \gamma_e)]^+ \]
- To achieve the secrecy capacity, the CSI of both links should be known to legitimate users in order to construct a coding scheme with appropriate rate parameters.
- For fading channels, the secrecy metric depends on the time-variation of the fading channel:
  - Fast (ergodic) fading or slow (quasi-static) fading
Existing Physical Layer Security Metrics

- For **fast** fading channel, the **ergodic secrecy capacity** is maximum achievable rate satisfying perfect reliability and perfect secrecy [Gopala_TIT_08].
  - When the CSI of both links are known to the legitimate users:
    \[
    \bar{C}_s^F = \int_0^\infty \int_0^\infty (\log_2(1 + \gamma_b) - \log_2(1 + \gamma_e)) f_{\gamma_b}(\gamma_b) f_{\gamma_e}(\gamma_e) d\gamma_b d\gamma_e
    \]
  - When only the CSI of Alice-Bob link is known:
    \[
    \bar{C}_s^M = \int_0^\infty \int_0^\infty [\log_2(1 + \gamma_b) - \log_2(1 + \gamma_e)]^+ f_{\gamma_b}(\gamma_b) f_{\gamma_e}(\gamma_e) d\gamma_b d\gamma_e
    \]

- Similarity: Variable-rate transmission (according to instantaneous CSI) is used in both cases. This is in contrast to non-secrecy transmission where a constant rate is used.
- Difference: With CSI of both links, transmission is suspended when Bob’s channel is worse than Eve’s channel.

Existing Physical Layer Security Metrics

- Numerical example of ergodic secrecy capacity [He_IET_17]:

![Graph showing ergodic secrecy capacity vs. average power constraint](image)

Existing Physical Layer Security Metrics

- For slow fading channel, the fading gain stays constant over the transmission of a codeword, hence outage-based metrics are used.
  - Secrecy Outage (Definition I): \( C_b - C_e < R_s \)
  - With a given secret message rate of \( R_s \), outage means it is not possible to achieve both perfect reliability and perfect secrecy at that point in time.
  - Secrecy Outage (Definition II): \( C_e > R_b - R_s \) | message transmission
  - With a given wiretap encoding scheme with \( R_b \) and \( R_s \) as the rate parameters, outage means the transmission at that point in time fails to achieve perfect secrecy.

- [Example] Consider on-off transmission where transmission is suspended when \( C_b < R_s \). Whenever transmission is suspended, there is secrecy outage in Definition I but not secrecy outage in Definition II.

- See [Zhou_CL_11] for detailed discussion on the difference between two definitions.

Existing Physical Layer Security Metrics

- Numerical example of secrecy outage probability [He_IET_17]:

\[ p_{out}^{D1} = \mathbb{P}(C_s < R_s) = \mathbb{P}(C_b - C_e < R_s) \]

\[ p_{out}^{D2} = \mathbb{P}(C_e > R_b - R_s \mid \text{message transmission}) \]

Transmission adopts adaptive rate chosen as \( R_b = C_b \).

Transmission is suspended when \( C_b < R_s \).
Role of Channel State Information

- The CSI assumptions play a very important role:

- For AWGN channel, the secrecy capacity $C_s = [C_b - C_e]^+$ is achievable only under the full CSI assumption, i.e., the legitimate users know the CSI of both Bob and Eve’s channels.

- For fast fading channel, the ergodic secrecy capacity has different expressions under different CSI assumptions.

- Different CSI enables different levels of rate adaptation and the possibility of on-off transmission. This significantly affects the performance.

- More generally speaking, the location and the number of antennas used by the eavesdropper is also part of the eavesdropper CSI.
  - For example, [He_TWC_15] provided a framework to study secrecy capacity with uncertainty in the exact location and the number of antennas at the eavesdropper.

Existing Physical Layer Security Metrics

- All previously discussed secrecy metrics are based on **perfect secrecy**, which is mutual-information based metrics.

- **Shortcomings:**
  - No insights into the amount of information leakage to the eavesdropper when perfect secrecy is not achieved.
  - These mutual-information based metrics cannot be easily measured and understood in practice, e.g., they are not directly related to decoding error probability of the eavesdropper.
  - These mutual-information based metrics are also not directly related to metrics used by the cryptography community.

- The concepts of both information leakage and decoding error probability are not in the regime of **perfect secrecy**, but in the regime of **partial secrecy**.
Physical Layer Security Fundamentals

- **Equivocation (at Eve):**
  - It quantifies the level at which Eve is confused.
  - It is defined as the conditional entropy $H(M | Z^n)$.
  - $H(M | Z^n) = H(M)$ means Eve is totally confused, i.e., perfect secrecy.
  - $H(M | Z^n) = 0$ means there is no confused at all at Eve, i.e., no secrecy at all, the message is perfectly obtained by Eve.

- **Fractional Equivocation:** $\Delta = \frac{H(M | Z^n)}{H(M)}$. 

\[ M \rightarrow X \quad Y \rightarrow \hat{M} \]

\[ Z \]
Physical Layer Security Fundamentals

• Fractional Equivocation

\[ \Delta = \frac{H(M \mid Z^n)}{H(M)} \]

• It gives an asymptotic lower bound on the decoding error probability at Eve:

\[ \lim_{K \to \infty} P_e \geq \Delta - \lim_{K \to \infty} \frac{1}{\log_2(K)} = \Delta. \]

• where \( K \) is the number of possible messages Alice can transmit.
Physical Layer Security Fundamentals

• In fading channels, the fractional equivocation is a random quantity.
• For a given set of fading channel realisations, the maximum achievable fractional equivocation is given by

\[ \Delta = \begin{cases} 
1, & \text{if } C_e \leq C_b - R_s \\
(C_b - C_e)/R_s, & \text{if } C_b - R_s < C_e < C_b \\
0, & \text{if } C_b \leq C_e,
\end{cases} \]

• Averaging over the distributions of the fading channels, the average fractional equivocation gives an asymptotic lower bound on the overall decoding error probability at Eve: 

\[ \bar{\Delta} = \mathbb{E}\{\Delta\} \]

• The average information leakage rate (# bits per symbol Eve can possibly obtain):

\[ R_L = \mathbb{E} \left\{ \frac{I(M;Z^n)}{n} \right\} = \mathbb{E} \left\{ (1 - \Delta)R_s \right\} \]

©Nan Yang, Xiangyun Zhou, and Jemin Lee
New Physical Layer Security Metrics

- Let’s take an example from [He-TWC’16].
- Fixed-rate transmission, i.e., $R_b$ and $R_s$ are fixed.
- Transmission occurs when $R_b < C_b$.
- For the fixed-rate transmission scheme, the fractional equivocation is given by

\[
\Delta = \begin{cases} 
1 & \text{if } C_e \leq R_b - R_s, \\
(R_b - C_e)/R_s & \text{if } R_b - R_s < C_e < R_b, \\
0 & \text{if } R_b \leq C_e.
\end{cases}
\]

- The fractional equivocation is a random variable in fading channels due to the variation in $C_e$.
- Let’s consider a Rayleigh fading scenario.

New Physical Layer Security Metrics

- **Secrecy Metric 1:** Eavesdropper decoding error probability.
  - An asymptotic lower bound on the eavesdropper decoding error probability is given by the average fractional equivocation:

  \[
  \bar{\Delta} = E\{\Delta\} \\
  = \int_0^{2^{R_b-R_s-1}} f_{\gamma_e}(\gamma_e) d\gamma_e + \int_{2^{R_b-R_s-1}}^{2^{R_b-1}} \left( \frac{R_b - \log_2(1+\gamma_e)}{R_s} \right) f_{\gamma_e}(\gamma_e) d\gamma_e \\
  = 1 - \frac{1}{R_s \ln 2} \exp\left(\frac{1}{\bar{\gamma}_e}\right) \left( \text{Ei} \left( -\frac{2R_b}{\bar{\gamma}_e} \right) - \text{Ei} \left( -\frac{2R_b-R_s}{\bar{\gamma}_e} \right) \right)
  \]

- **Secrecy Metric 2:** Average information leakage rate.

  \[
  R_L = R_s \cdot (1 - \bar{\Delta}) \\
  = \frac{1}{\ln 2} \exp\left(\frac{1}{\bar{\gamma}_e}\right) \left( \text{Ei} \left( -\frac{2R_b}{\bar{\gamma}_e} \right) - \text{Ei} \left( -\frac{2R_b-R_s}{\bar{\gamma}_e} \right) \right)
  \]
New Physical Layer Security Metrics

- Secrecy Metric 1: Eavesdropper decoding error probability.

Asymptotic lower bound on the decoding error probability at Eve versus confidential information rate. Results are shown for networks with different average received SNRs at Eve, $\gamma_e = 1, 2$. The other parameter is $R_b = 4$. 

©Nan Yang, Xiangyun Zhou, and Jemin Lee
New Physical Layer Security Metrics

- Secrecy Metric 2: Average information leakage rate.
New Physical Layer Security Metrics

- All the above results are based on the theoretically best possible codes with infinite blocklength.
- To move ahead, we need to extend the results to practical code with finite blocklength.
  - [Pfister_ICC_17] studied equivocation for finite blocklength codes.
  - [Harrison_ES_18] studied decoding error probability for practical codes, e.g., what’s the probability that the BER at Eve after her decoding is very close to 0.5 for a BCH code.
- Overall, this new direction of research:
  - Partial secrecy: Look at the information leakage and decoding error probability
  - Look at practical codes with a finite blocklength, which can be tested with practical implementations.

---

Existing Physical Layer Security Metrics

- Recall the previously mentioned shortcomings of perfect secrecy metrics:
  - No insights into the amount of information leakage to the eavesdropper when perfect secrecy is not achieved.
  - These mutual-information based metrics cannot be easily measured and understood in practice, e.g., they are not directly related to decoding error probability of the eavesdropper.
  - These mutual-information based metrics are also not directly related to metrics used by the cryptography community.

- Partial secrecy based metrics discussed in the previous few slides overcome the first two shortcomings. What about the third one?
New Physical Layer Security Metrics

• Recall the existing definitions of perfect secrecy:
  – Weak secrecy: \( \lim_{n \to \infty} \frac{1}{n} I(M; Z^n) = 0. \)
  – Strong secrecy: \( \lim_{n \to \infty} I(M; Z^n) = 0. \)

• Assumption used: the random message \( M \) follows a uniform distribution over \( \{0, 1\}^m \)

• **Semantic-security based metric** [Bellare_CRYPTO_12]:
  \[
  \lim_{n \to \infty} \max_{P_M} I(M; Z^n) = 0.
  \]

• Key feature: instead of ensuring secrecy for the uniform distributed random message, it ensures secrecy for any arbitrary message distribution.

• Importance: it is proven to be equivalent to the semantic secrecy concept used in the cryptography community: for every message distribution the eavesdropper cannot infer any more about any function of the message \( f(M) \) than a random guess.

Trust Degree-aided Secure Communication

- Challenges on Secure Communication with Untrustworthy Nodes
  - For example, when a transmitter and a receiver do not have reliable direct channel, a cooperative user (i.e., a relay) can help by forwarding the date of the transmitter.
  - However, we often do not know whether the cooperative user is trustworthy or not.
    - Even when all users belong to the same networks (e.g., military or banking networks), they may have different levels of data access
    - They can be Potential Eavesdroppers (PEs); willing to help but curious about other user’s confidential information

©Nan Yang, Xiangyun Zhou, and Jemin Lee
Trust Degree-aided Secure Communication

- **How to communicate securely with the untrustworthy relay?**
  - We can communicate assuming the *worst case*, i.e.,
    - Transmit user treats a relay as an eavesdropper if it is untrustworthy.
    - However, it can be inefficient as the untrustworthy relay can be a friend, not foe.
  - By combining the concepts of physical networks with social networks, the transmit user may more efficiently send confidential message using the untrustworthy relay
    - If transmit user has information for the *trust degree of the relay*, it can use it to design the transmission for better communication secrecy.

©Nan Yang, Xiangyun Zhou, and Jemin Lee
Trust Degree-aided Secure Communication

• The establishment of trust relationship is a complex progressive process, which depends on interaction history, trust recommendation, trust management, and so on.
  – For example, in social domain, users frequently communicate with their acquaintances such as friends and family.

• Trust degree
  – The trust degree has been defined as a belief level that one node can put on another node for a certain action, according to previous direct or indirect information, obtained from observations of behavior [Li_CM_08].

Trust Degree-aided Secure Communication

- The establishment of trust relationship is a complex progressive process, which depends on interaction history, trust recommendation, trust management, and so on.
  - For example, in social domain, users frequently communicate with their acquaintances such as friends and family.
- Trust degree
  - The trust degree has been defined as a belief level that one node can put on another node for a certain action, according to previous direct or indirect information, obtained from observations of behavior [Li_CM_08].
- Trust degree in communication secrecy can be used as estimates on
  - Whether the user will eavesdrop the confidential date of source.
  - Whether the user denies my request such as relaying or computation.

Trust Degree-aided Secure Communication

- Take an example of **trust degree in communication secrecy** in [Ryu_TWC_16]

![Diagram showing Trust Degree-aided Secure Communication]

- Transmit user (TU) transmits intended message to receive user (RU) via physical wireless channels \((g_0, g_e, g_r)\)
- Potential eavesdropper may eavesdrop intended message
- Tie \(\alpha\) (trust information) of trust link denotes the degree of trust of connected users
  - Degree of trust \(\rightarrow\) Probability not to eavesdropping intended message
  - Trust information between TU and RU: \(\alpha_0=1\)
  - Trust information between TU and PE: \(0 \leq \alpha_e \leq 1\)

Trust Degree-aided Secure Communication

- In this case, the transmit user can make a choice on its transmission strategies.

**Direct transmission**

- In the case that PE does not relay the message of TU even if she is not an eavesdropper
- TU transmits directly to RU
  - the intended message with the power $P_I$
  - the known Jamming message at RU (not PE) with the power $P_J$

**Cooperative transmission**

- In the case that PE relays the message of TU to RU if PE is not an eavesdropper
- TU can select between
  - Direct transmission and
  - Full-duplex decode-and-forward (DF) user relaying via PE
Trust Degree-aided Secure Communication

• Direct Transmission: Achievable Rates
  – With the assumption that RU can perfectly cancel jamming signal from the received signal, the achievable rates at RU and PE can be given by
  
  At RU: \[ R_0 (P_C) = \log \left( 1 + \frac{P_C g_0}{\sigma^2_N} \right), \]
  
  At PE: \[ R_1 (P_C, P_J) = \log \left( 1 + \frac{P_C g_1}{\sigma^2_N + P_J g_1} \right), \]

  \( P_C \): Transmit power at TU \( P_C \): Jamming power at TU
  \( g_0, g_1 \): Channel gain

• Direct Transmission: Expected Secrecy Rate
  – If PE is not an eavesdropper, the expected rate is maximized by conventional Gaussian codeword (not the wiretap code).
  – Hence, TU can transmit its data using either Gaussian or wiretap codewords.
  
  \[ \bar{R}_{se,d} (P_C, P_J) \]
  
  \[ = \begin{cases} 
  R_G (P_C) = \alpha R_0 (P_C), & \text{if } C = C_G \quad \text{Gaussian codeword case} \\
  R_W (P_C, P_J) = [R_0 (P_C) - R_1 (P_C, P_J)]_+, & \text{if } C = C_W \quad \text{Wiretap codeword case}
  \end{cases} \]
Trust Degree-aided Secure Communication

• Cooperative Transmission: Achievable Rates
  
  In the relaying transmission, the RU can receive the message from both TU and PE. For the case that PE is not an eavesdropper, the achievable rate is

  \[ R_{0,u}(P_C) = \min [R_1(P_C), R_{ur}(P_C)] \]

  where \( R_{ur}(P_C) \) is the achievable rate at RU, given by

  \[ R_{ur}(P_C) = \log \left( 1 + \frac{P_C g_0}{\sigma^2_N} + \frac{P_1 g_{10}}{\sigma^2_N} \right) \]

• Cooperative Transmission: Expected Secrecy Rate
  
  Similar to the direct transmission case, the expected secrecy rate is given by

  \[ \overline{R}_{sc,u}(P_C) = \begin{cases} R_{G,u}(P_C) = \alpha_1 R_{0,u}(P_C), & \text{if } \mathcal{C} = \mathcal{C}_G \\ \text{Gaussian codeword case} \\
  R_{W,u}(P_C) = [R_{0,u}(P_C) - R_1(P_C)], & \text{if } \mathcal{C} = \mathcal{C}_W \\ \text{Wiretap codeword case} \end{cases} \]
Trust Degree-aided Secure Communication

- Some insights obtained from [Ryu_TWC_16]
  - In direct transmission case (from Theorem 1)
    - When the trust degree is sufficiently high, i.e., $\alpha_1 \geq \bar{\alpha}_d$, allocation all power to the confidential message (no jamming transmission) can achieve better expected secrecy rate.
  - In cooperative transmission case (from Theorem 3)
    - When the trust degree is sufficiently high, i.e., $\alpha_1 \geq \bar{\alpha}_c$, the optimal transmission strategy is the cooperative transmission with full transmission power at the TU.
    - In other words, if PE is sufficiently reliable user for TU, TU can transmit its confidential message without jamming by cooperative transmission via the PE.

\[
\bar{\alpha}_d = \frac{\log \left( \frac{(\rho T g_0 g_1 + g_0 + g_1)^2}{4 g_0 g_1 (1 + \rho T g_0)} \right)}{\log (1 + \rho T g_0)}
\]

\[
\bar{\alpha}_c = \frac{\log \left( \frac{(\rho T g_0 g_1 + g_0 + g_1)^2}{4 g_0 g_1 (1 + \rho T g_1)} \right)}{\log (1 + \rho T g_1)}
\]  

\[
\frac{\log \left( \frac{(\rho T g_0 g_1 + g_0 + g_1)^2}{4 g_0 g_1 (1 + \rho T g_1)} \right)}{\log (1 + \rho T g_0 + \rho_1 g_1)}
, \text{ if } g_{10} > \frac{P_T}{P_1} (g_1 - g_0)
\]

\[
\frac{\log \left( \frac{(\rho T g_0 g_1 + g_0 + g_1)^2}{4 g_0 g_1 (1 + \rho T g_1)} \right)}{\log (1 + \rho T g_0 + \rho_1 g_1)}
, \text{ otherwise}
\]
Trust Degree-aided Secure Communication

- Numerical examples of expected secrecy rate
  - Cooperative transmission much improves expected secrecy rate when trust degree of PE is high.
  - Performance gap between the cooperative and direct transmission becomes larger for higher trust degree.
Trust Degree-aided Secure Communication

• Some more examples:
  – In [Ryu_CL_16], the transmission rate and beamformer design against an opportunistic attack, which eavesdrops or generates jamming signal with certain probabilities.
  – In [Zha_TWC_17], the user cooperation system with multiple antennas is considered, and the power allocation and precoder design for various antenna configurations including SISO, MISO, and MIMO are presented.
  – In [Wan_TCOM_18], a social ties based hybrid cooperative beamforming and jamming scheme are considered under a stochastic geometry framework, where the friendly nodes are categorized into relays and jammers according to their locations and social trust degrees with the source node.

Physical Layer Key Generation

- Principle

Wireless Channel

Principles:
- Channel Reciprocity
- Spatial Decorrelation
- Temporal Variation

Physical Layer Key Generation

• Evaluation metrics
  – Key Bit Randomness (KBR):
    • The key sequence must look pretty random according to certain statistical tests.
  – Key Generation Rate (KGR)
    \[ KGR = \frac{N}{T} \]
  – Key Disagreement Rate (KDR)
    \[ KDR = \frac{\sum_{i=1}^{N} |K^A(i) - K^B(i)|}{N} \]
  – From the information-theoretic viewpoint: Secrecy key capacity.
Physical Layer Key Generation

- Relation between KDP, KGP, and KBR
  - Generating a bit from many consecutive measurements
    - Low Key Disagreement Prob. but Low Key Generation Rate
  - Increasing channel sampling rate
    - High Key Generation Rate but Low Key Bit Randomness (due to correlated measurements)
  - Extracting key at different channel coherent time intervals
    - High Key Bit Randomness but Low Key Generation Rate in RSS-based scheme
    - No constraint on KBR in phase-based scheme (since both random initial phase and channel phase contribute to the randomness of generated key)

Key generation scheme should be developed considering the required values of KDP, KGR, and KBR
Physical Layer Key Generation

- **Procedure**
  1. **Channel Probing**
     - Measuring channel using public pilot
  2. **Quantization**
     - Analog to digital (binary) conversion
  3. **Information Reconciliation**
     - Error correction
  4. **Privacy Amplification**
     - Removing information leakage
Physical Layer Key Generation

• Key Generation Sources
  – Received Signal Strength (RSS)-based Generation
    • Exploiting power of received signal
    • Low key generation rate
    • E.g., [Azi_CCS_07, Mat_Mobicom_08, Liu_TMC_14, Tha_TIFS_19]
  – Channel Phase-based Generation
    • Exploiting phase reciprocity of channel
    • High resolution phase estimation, resulting in high key bit generation, but expensive
    • E.g., [Wan_Infocom_11, Wan_JSAC_12]

Physical Layer Key Generation

- Example of RSS Quantization [Jan_Mobicom_09]
  - The values between lower and upper threshold are dropped.
  - The value greater than the upper threshold is encoded as 1.
  - The value less than the lower threshold is encoded as 0.

Quantizer output: 1010011

## Physical Layer Key Generation

<table>
<thead>
<tr>
<th>Technique</th>
<th>Modulation</th>
<th>Parameter</th>
<th>Features</th>
<th>Testbed</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE 802.11</td>
<td>MIMO OFDM</td>
<td>RSS, CSI</td>
<td>MIMO OFDM enables CSI measurements both in frequency and spatial domain</td>
<td>RSS: all NICs; CSI: Intel 5300 NIC, and customized hardware platforms, such as USRP and WARP</td>
</tr>
<tr>
<td></td>
<td>OFDM</td>
<td>RSS, CSI</td>
<td>OFDM enables fine-grained CSI measurements</td>
<td></td>
</tr>
<tr>
<td></td>
<td>OFDM, DSSS</td>
<td>RSS, CSI</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DSSS</td>
<td>RSS</td>
<td>RSS available</td>
<td></td>
</tr>
<tr>
<td>IEEE 802.15.4</td>
<td>DSSS</td>
<td>RSS</td>
<td>Widely used in WSN; sensor motes are battery-powered and with low computational capacity; usually low mobility</td>
<td>MicaZ and TelosB</td>
</tr>
<tr>
<td>Bluetooth</td>
<td>FHSS</td>
<td>RSS</td>
<td>FHSS allows sampling RSS in different frequencies.</td>
<td>Smartphones</td>
</tr>
<tr>
<td>UWB</td>
<td>Pulse</td>
<td>CIR</td>
<td>Low power, large bandwidth (&gt; 500 MHz)</td>
<td>Constructed by oscilloscope, waveform generator, etc</td>
</tr>
<tr>
<td>LTE</td>
<td>MIMO OFDM</td>
<td>RSS, CSI</td>
<td>Only applied in slow fading channel for key generation; Ability to adjust parameters, such as power allocation; no practical implementation reported yet</td>
<td>Smartphones</td>
</tr>
</tbody>
</table>
Physical Layer Key Generation

- **Secret Key Generation with Untrustworthy Relay (UR)**
  - URs know public network information and communication protocols.
  - URs play the man-in-the-middle role who have better version of the relayed signal than the intended receiver.

- **Fundamental Questions from Those Challenges**
  - How does the UR affect communication secrecy?
  - Can we use the relayed information to generate secret key?
  - How do we define the trust level of URs, and further how to use the trust information to enhance the communication confidentiality?
Physical Layer Key Generation

- Exemplary Protocol [Tha_TWC_16]
  - Main design principle: make the untrustworthy relay speaks (transmits) more but listens (receives) less
    - Three phase transmissions
    - Channel estimation (using MMSE scheme)

Untrustworthy Relay

- Key generation at Alice and Bob using the estimated channel measurement
  - Theoretical analysis of secret key rate
    - Key generation rate at Alice and Bob and leaked key rate to UR

Physical Layer Group Key Generation

• Physical Layer Group Key Generation
  – In many scenarios, the common-key generation for a group of legitimate users is necessary to share confidential information only between people in a certain group, e.g., polices, soldiers.

• Extending the physical-layer key generation scheme for several users is practically challenging.
  – The channel information used for key generation is characterized only between two users in terms of channel reciprocity and randomness.
    • For group key generation, these two users need to forward the information to other users in a group, which leads to a risk of leaking information to eavesdroppers.
  – As more users exist, there are more channels among them.
    • Advantage: Longer group key can be generated.
    • Disadvantage: A scheme requires a longer channel coherence time as it needs to probe all those channel information while the channels stay the same.
Physical Layer Group Key Generation

- Some works on group key generation
  - In [Liu_TMC_14], the star and chain network topologies are considered for single-antenna nodes.
  - In [Tha_TIFS_19], the mesh network topology is considered for multi-antenna users of a group.


©Nan Yang, Xiangyun Zhou, and Jemin Lee
Physical Layer Group Key Generation

- Exemplary Secret Group Key Generation Protocol for Mesh Topology [Tha_TIFS_19]
  - Transmission: **Sounding phase**
    - We select the channels used for the key generation considering the channel coherence time.
    - Each (selected) antenna of all nodes transmit pilot signals.

**Sounding phase example for multiple-antenna nodes**

**Sounding phase example for single antenna nodes**
Physical Layer Group Key Generation

- Transmission: **Broadcast phase**
  - Each node broadcasts the information of the channels it estimated in the sounding phase so that other legitimate nodes can estimate the channels that they did not estimate.

<table>
<thead>
<tr>
<th>Already have</th>
<th>Broadcast</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice: $h_1, h_4, h_5$</td>
<td>$x_A = a_1h_1 + a_4h_4 + a_5h_5$</td>
</tr>
<tr>
<td>Bob: $h_1, h_2, h_6$</td>
<td>$x_B = b_1h_1 + b_2h_2 + b_6h_6$</td>
</tr>
<tr>
<td>Carol: $h_2, h_3, h_5$</td>
<td>$x_C = c_2h_2 + c_3h_3 + c_5h_5$</td>
</tr>
<tr>
<td>Dave: $h_3, h_4, h_6$</td>
<td>$x_D = d_3h_3 + d_4h_4 + d_6h_6$</td>
</tr>
<tr>
<td>Eve: $g_1, g_2, g_3, g_4$</td>
<td>Receive 4 signals but need to estimate 6 variables</td>
</tr>
</tbody>
</table>

- **Estimation**: Linked channels and Forwarded channels’ estimations
- **Quantization/Encoding/Concatenation**
Physical Layer Group Key Generation

- Numerical Results
  - Key rate of 7.2 bits/channel use.

<Key disagreement probability for 3 group members>

<Key disagreement probability according to the number of group members>
Outline

• Security in mobile communication networks
  – Evolution of cellular networks
  – Security issues in cellular networks
  – Re-shape security design in 5G and beyond wireless networks

• Theoretical advancement in PHY layer security
  – Fundamentals of PHY layer security
  – Existing secrecy performance metrics
  – New secrecy performance metrics
  – Trust degree-aided secure communication
  – PHY layer key generation

• Cutting-edge PHY layer security solutions
  – Heterogeneous secure communication
  – Full-duplex secure communication
  – Massive MIMO-aided secure communication
  – Secure communication over mmWave channels
  – Machine type secure communication
  – NOMA-based security
  – Security for URLLC
  – Energy-efficient secure communication
  – Unmanned aerial vehicle secure communication
  – Software defined radio-based prototyping

• Future directions, challenges and open issues
  – PHY layer security beyond content secrecy
  – Cross-layer security
  – Challenges imposed by future wireless world

©Nan Yang, Xiangyun Zhou, and Jemin Lee
Deployment Scenarios for 5G and Beyond

- 5G systems are expected to offer ultra-high-quality wireless service through utilising new frequency bands, leveraging various radio access technologies, and deploying massive machine type devices.
The HetNet is a promising network densification architecture in the 5G and beyond era.
Heterogeneous Secure Communication

• In the HetNet, nodes with different transmit powers, coverage areas, and radio access technologies are deployed to build a multi-tier hierarchical architecture.

• Small cells, e.g., pico cells and femto cells, are deployed under macro cell umbrellas to augment indoor coverage in highly populated buildings, and multi-tenant dwelling units, enterprises, and outdoor coverage in dense urban, suburban, or rural areas.

• Conventional physical layer security technologies for multi-antenna systems, multi-user transmission, and relay-aided communication can be borrowed. But this is not enough.

• Some unique features associated with the HetNet, such as spatial modelling, interference mitigation, mobile association, and device connection, need to be addressed.
Heterogeneous Secure Communication

- **Recent Contributions**
  - In [Wang_TCOM_2016], a $K$-tier HetNet was considered.
  - As shown in the figure, a UE connects to the BS providing the highest truncated average received signal power (ARSP) instead of the nearest BS, where an access threshold $\tau$ was adopted in the mobile association.
  - Those UEs outside the serving regions of BSs cannot be served. A BS remains idle if it has no UE to serve.
  - The UEs coexist with Eves, both of which follow independent PPP distributions.
  - Each BS employs the artificial-noise-aided transmission strategy to deliberately confuse Eves while guaranteeing reliable links to UEs.


©Nan Yang, Xiangyun Zhou, and Jemin Lee
Heterogeneous Secure Communication

Secrecy probability in a 2-tier HetNet vs. transmit power in Tier 1.

Secrecy probability in Tier 2 reaches one when $P_1$ is large enough.

Secrecy probability in Tier 1 first decreases and then slowly rises to a constant value.

Secrecy probabilities of both tiers increase as $\tau$ decreases.

Heterogeneous Secure Communication

Secrecy throughput in a 2-tier HetNet vs. power allocation in Tier 2.


©Nan Yang, Xiangyun Zhou, and Jemin Lee
Heterogeneous Secure Communication

• The secrecy performance in the HetNet is indeed affected by various parameters in the network, such as:
  – The location or distribution density of users and/or eavesdroppers;
  – The number of transmit antennas at the base station or access point in each tier;
  – The transmit power at the base station or access point in each tier;
  – The choice of mobile association strategy;
  – The choice of resource allocation (e.g., power allocation) strategy;
  – The choice of secure transmission strategy.

• Therefore, the careful design based on the aforementioned parameters is needed for securing the wireless transmission in the HetNet.
Heterogeneous Secure Communication

- Future Challenges in This Area
  - Interference management
    - The interference may become intolerable if we only address the security purpose in the HetNet, no matter we consider the multi-tier or the cognitive radio architecture.
    - How to avoid/manage the interference to other cells (same tier or different tier) or the primary network is an important issue to solve.
  - Cooperative or collaborative transmission
    - If the cooperation from relay nodes and/or collaboration from other BSs is allowed, how to optimise such cooperative/collaborative transmission is an interesting topic to explore.
  - Secrecy-reliability trade-off
    - Security vs. reliability, which one is of priority? How to design parameters to ensure that the secrecy and reliability performance is at the acceptable level?
  - Promising approaches may include beamformer design, power and spectrum allocation, interference alignment, and convex/non-convex optimisation.
Full-Duplex Secure Communication

- Full-duplex communication — simultaneous transmission and reception on the same frequency channel — is an emerging and transformative communication technology that can substantially improve spectrum efficiency.
Full-Duplex Secure Communication

• Benefits of an FD transceiver in wiretap channels include:
  – Bob can transmit artificial noise to create interference.
  – More interference Eve will have when she moves closer to Bob.

• Additional advantages relative to having a cooperative jammer include:
  – No synchronisation between different devices is required.
  – No trustworthiness issues exist.
Full-Duplex Secure Communication

- Recent Contributions
  - In [Yan_TIFS_2018], an FD wiretap channel is considered, where Rayleigh fading channels, including the self-interference channel, are assumed;
  - Bob is equipped with multiple FD antennas, i.e., all $N_B$ antennas are used for reception and transmission simultaneously;
  - Pilot and data symbols with an average power constraint over a fading block.


Bob transmits secret pilots for channel estimation.
Full-Duplex Secure Communication

The maximum connection probability increases as $\epsilon$ increases, which shows the trade-off between the effective throughput and the secrecy constraint.

The proposed scheme outperforms the non-secret scheme, since the proposed scheme prevents Eve from obtaining the CSI of the jamming channel through the use of secret pilots.

Comparison of maximum connection probability.


©Nan Yang, Xiangyun Zhou, and Jemin Lee
Full-Duplex Secure Communication

Comparison of the optimal transmit power at Alice.

More transmit power is allocated to data transmission as the secrecy constraint is relaxed.

More transmit power is allocated to data transmission at Alice as $N_E$ decreases.

Full-Duplex Secure Communication

• Future Challenges in This Area
  – How do we design the transmitted signals, including those for both channel estimation and data transmission, for practical FD wiretap channels?
  – How do we design an effective scheme to perform self-interference cancellation and secure transmission simultaneously and achieve the best secrecy performance?
  – How do we perform the joint design if multiple FD devices exist in the system and collaborate? Among these multiple FD devices, what would we do if some of them are not trustable?
  – How do we design and analyse the system if the eavesdropper is an FD device such that attacking/jamming signals can be sent from the eavesdropper?
Massive MIMO-aided Secure Communication

Massive MIMO enabled by a large number of antennas at the BSs is an energy-efficient way to simultaneously serve a large number of users and to boost the system capacity.

The benefits of the massive MIMO technique are realised by using very large antenna arrays (typically hundreds).

Massive MIMO systems are emerging as a new research field and have attracted significant interest from both scientists and industrialists.
Massive MIMO-aided Secure Communication

- By exploiting the large arrays gain, massive MIMO systems provide high power and spectrum efficiencies via low-complexity transmission designs.
- Random impairments such as small-scale fading and noise can be averaged out when a large number of antennas are deployed at the BS.
- When the number of antennas grows sufficiently large, the interference and hardware impairments vanish, leaving only pilot contamination as the performance limit.
- Given the fact that massive MIMO will serve as an essential enabling technology for the wireless network in the 5G and beyond era, the design of physical layer security needs to be carefully performed to fully realise the tremendous potential of massive MIMO systems.
- This design opens a new and promising research avenue, extending current multi-antenna security studies to a new area.
Massive MIMO-aided Secure Communication

• Recent Contributions
  – In [Zhu_TWC_2016], an $M$-cell massive MIMO network was considered.
  – Each cell includes one $N_T$-antenna BS, $K \leq N_T$ single-antenna users, and potentially an $N_E$-antenna passive eavesdropper.
  – Each BS generates artificial noise signals to mask its information-carrying signal and to prevent eavesdropping.
  – The following precoders were investigated:
    • Selfish/collaborative zero-forcing (ZF) precoder
    • Selfish/collaborative regularised channel inversion (RCI) precoder
    • Random null-space AN precoder
    • Selfish/collaborative null-space AN precoders

Selfish precoders require only the CSI of the users in the local cell, thus causing inter-cell interference and inter-cell AN leakage.

Collaborative precoders require the CSI between local BS and users in all cells, reducing inter-cell interference and AN leakage.

Massive MIMO-aided Secure Communication

Ergodic secrecy rate for a lightly loaded network with $K = 10$ and $M = 2$.

Massive MIMO-aided Secure Communication

For the dense network, the collaborative precoder designs are not able to suppress inter-cell interference and AN leakage to other cells sufficiently well to outperform the selfish precoder designs.

Ergodic secrecy rate for a dense network with $K = 20$ and $M = 7$.

Massive MIMO-aided Secure Communication

- Some interesting insights provided by [Zhu_TWC_2016] are:
  - Collaborative precoders outperform selfish designs only in the lightly loaded network where a sufficient number of degrees of freedom for suppressing inter-cell interference and sufficient resources for training are available.
  - Collaborative null-space AN precoding is preferable over selfish null-space AN precoding in the lightly loaded network as it causes less AN leakage to the information-carrying signal. Differently, in a more heavily loaded network, collaborative null-space AN precoding does not have sufficient degrees of freedom for effectively degrading the eavesdropper channel and thus, the selfish null-space AN precoding is preferable.
  - For a large number of eavesdropper antennas, where only small positive secrecy rates are achievable, the matched filter precoding is always preferable compared to selfish or collaborative ZF precoding.

Massive MIMO-aided Secure Communication

• Future Challenges in This Area
  – The estimation of the precise CSI is always a problem in massive MIMO since the CSI acquisition process is a high complex procedure with the growth of the number of antennas.
    • Imperfect CSI caused by pilot contamination;
    • Imperfect reciprocity calibration in time division duplex (TDD) mode.
  – Antenna correlation is a practical challenge underlying the deployment of massive MIMO systems. A significant amount of correlation may exist between large antenna arrays, due to either the limited aperture of the antenna array or a lack of scattering.
    • Very little detailed work has specifically been carried out to analyse the effect of antenna correlation on the secrecy performance of massive MIMO systems.
  – The application scenarios where all devices are equipped with massive antennas or all devices are distributed within an area but interconnected via backhaul are still open research topics.
    • The secrecy capacity in this scenario is a critical metric for using massive MIMO in physical layer security.
Secure Communication over mmWave Channels

MmWave communication, operating in the frequency range of 30–300 GHz, is recognised as a promising solution for 5G+.
Secure Communication over mmWave Channels

- MmWave systems provide high bandwidths, e.g., as high as GHz. The secrecy outage probability would be remarkably reduced if the transmitter sets a lower transmit secrecy rate. Also, high secrecy throughput can be obtained with large mmWave bandwidths.

- MmWave signals in the higher frequencies experience an increase in free-space path loss by several orders of magnitude. The valid assumption surrounding the ability of eavesdroppers, especially those remotely located, needs to be identified.

- In mmWave systems, highly directional communication with narrow beams is employed for suppressing the interference from neighbours. Thus, the SNRs at the eavesdroppers may be super low such that the eavesdroppers cannot recover information signals from the overheard messages.
Secure Communication over mmWave Channels

- **Recent Contributions**
  - In [Ju_TCOM_2017], an MISO wiretap mmWave channel was addressed.
  - Different from traditional wireless channels, scattering and multipaths in the mmWave band are sparse, which means that correlated fading exists.
  - Three schemes were investigated:
    - **Maximum ratio transmitting (MRT) beamforming**
      - Transmit signals in all directions of destination’s resolvable paths, which contain some paths to eavesdropper.
    - **Partial MRT (PMRT) beamforming**
      - Transmit signals only in partial directions of the destination’s resolvable paths excluding the directions of common paths.
    - **Artificial noise (AN) beamforming.**

Secure Communication over mmWave Channels

Secrecy throughput comparison versus transmit power.

PMRT is the best choice when the transmit power is medium and high.

MRT beamforming presents a comparable performance to AN beamforming when the transmit power is low.

Secrecy throughput increases with the transmit power.

Secure Communication over mmWave Channels

Secrecy throughput comparison versus the number of common paths.

Secrecy throughput is higher when $L_C$ decreases.

Secrecy throughput is higher when $r_D$ decreases, i.e., the destination is closer to the transmitter.

AN beamforming is the best scheme when $L_C$ is large. When $L_C$ is small, the PMRT beamforming is the best scheme.


©Nan Yang, Xiangyun Zhou, and Jemin Lee
Secure Communication over mmWave Channels

• Future Challenges in This Area
  – How do we use the propagation characteristics at high frequencies, especially for indoor transmission, into the effective design of physical layer security in mmWave systems, such as multi-path delay spread, small-scale mmWave fading, and the uncertainty in signal penetration and propagation loss?
  – How do we design new secure transmission schemes based on specific transmission strategy at mmWave frequencies, such as hybrid beamforming with full- or sub-connected architecture?
  – Considering the 5G cellular networks with the joint use of microwave and mmWave, how do we analyse the trade-off between security and coverage and how do we design the transmission to achieve this trade-off?
  – How will we design secure mechanisms over THz communications systems?
Machine type communication (MTC) can exchange and share data without any requirement on human interventions.

• The MTC carries a lot of unique features:
  – a massive number of devices;
  – small and infrequent data transmissions;
  – distinct service scenarios;
  – fewer opportunities for recharging devices.

• These features bring in unprecedented challenges for MTC, especially in security.
Machine Type Secure Communication

- As a key cornerstone of MTC, **D2D communication** has been acknowledged as a competitive technology for 5G cellular networks.

- D2D communications enable **direct communications between users** in proximity, without traversing base stations or core networks. Thus, **spectrum efficiency** and **energy efficiency** can be significantly **improved**.

- Due to spectrum sharing within the cellular networks, D2D communications could generate a large **interference** to cellular users, resulting in performance degradation.

- Although the interferences from D2D communications are harmful, it actually can be exploited to enhance transmission security of cellular networks, since the **D2D interference** as a cooperative **jammer** to the illegitimate eavesdropper.
Machine Type Secure Communication

- Recent Contributions
  - In [Ma_TCOM_2015], a large-scale D2D-enabled cellular network was considered.
    - Transmit power and access control of the D2D link were jointly optimised to maximise the achievable data rate of D2D communications, subject to a secrecy outage probability constraint for cellular users.
    - It shows that the interference from D2D communications can enhance physical layer security and at the same time create extra transmission opportunities for D2D users.
  - In [Chu_IET_2015], a MISO downlink with multiple eavesdroppers and multiple D2D links was considered.
    - Robust beamforming at a multi-antenna transmitter was designed to minimise transmit power and to maximise secrecy rate, subject to a D2D transmission rate constraint.
    - It shows that D2D communications can potentially improve the secrecy performance.

Machine Type Secure Communication

• Future Challenges in This Area
  – Simply speaking, the trade-off between performance (e.g., secrecy throughput, secrecy outage probability, latency, etc.) versus complexity and required overhead (e.g., feedback or control signalling) needs to be examined.
  – Physical layer security needs to be re-designed based on the change of standard assumptions in MTC, including:
    • Large packets \(\Rightarrow\) small packets;
    • High data rate \(\Rightarrow\) low data rate;
    • Downlink focused communication \(\Rightarrow\) uplink focused communication.
  – Physical layer security design needs to address new promising techniques and requirements in MTC, including:
    • Non-orthogonal medium access;
    • Grant-free access control;
    • Low energy consumption and low complexity.
NOMA-Based Security

- Non-orthogonal multiple access (NOMA) has received significant attention for 5G and beyond wireless systems due to its unique properties such as high spectral efficiency, low latency, improved coverage, massive connectivity, and fairness.

- **Power-domain (PD) NOMA**: Different users’ signals are directly superimposed by assigning channel quality-based power allocation to them, while sharing the same frequency-time resources.

- **Code-domain (CD) NOMA**: Non-orthogonal codes with lower cross correlation or sparse sequences are used at users while the same frequency-time resources are shared.
NOMA-Based Security

- Let us take PD NOMA as an example.

- Security designs against external eavesdroppers
- Security designs against internal eavesdroppers
- Security designs against both internal and external eavesdroppers
NOMA-Based Security

• Recent Contributions
  – In [Zhang_CL_2016], secure transmission was designed for a NOMA system which consists of one transmitter, multiple users, and one eavesdropper, and with perfect CSI of users and no CSI of the eavesdropper. Perfect successive interference cancellation (SIC) is performed at each user.
    • The optimal power allocation policy was determined to maximise the secrecy sum rate under each user’s QoS constraint.
  – In [Liu_TWC_2017], the same CSI assumption was adopted while an eavesdropper exclusion zone in which no eavesdropper exists was established. The secrecy performance of the NOMA network was thoroughly analysed.
    • Security performance of NOMA can be improved by invoking the protected zone and by generating artificial noise at the base station.

NOMA-Based Security

• Recent Contributions

  – In [Ding_TCOM_2017], a NOMA network with both **multicasting** and **unicasting** transmissions was considered.
    • The use of the NOMA assisted multicast-unicast scheme yields a significant improvement in spectral efficiency compared with OMA schemes which realise multicasting and uncasting services separately.
  – In [He_JSAC_2017], the optimal designs of decoding order, transmission rates, and power allocated among **multiple users** were investigated.
    • The problem of minimising the transmit power subject to the secrecy outage and quality of service constraints, and the problem of maximising the minimum confidential information rate among users subject to the secrecy outage and transmit power constraints were solved.
    • The advantage of NOMA over OMA was shown.

NOMA-Based Security

- Future Challenges in This Area
  - The physical layer security model for untrusted users (including untrusted near user and untrusted far user) needs to be carefully established. Based on such model(s), novel physical layer security techniques need to be proposed to provide security for NOMA.
  - Many security techniques in NOMA assumed that there is only a single eavesdropper that has a limited set of observations. However, if there are more than one eavesdropper (at different locations) that can collaborate with each other, then this may lead to zero secrecy capacity.
  - Physical layer security design needs to address the practical factors in NOMA, e.g., imperfect channel estimation, various SIC strategies at the eavesdropper, and SIC error propagation.
  - To meet the diverse requirements of NOMA users and for joint design of throughput, secrecy, delay, reliability and the trade-offs among them, the cross-layer security design which involves physical layer design needs to be considered.
Security for URLLC

- Ultra-reliable and low-latency communication (URLLC) is a key requirement in the 5G and beyond era.

- URLLC is envisioned to enable the wireless exchange of data packets with ultra-high reliability (error probability on the order of $10^{-7}$) and ultra-low latency (end-to-end delay on the order of 1 ms).

- The former creates confidence that wireless communications can be used even in life-threatening circumstances, while the latter ensures real-time functionality in time-critical interactive communications.

- Security issues are very important in most application scenarios of URLLC. For example, one key requirement arising from the nature of the tactile Internet is security and privacy. The leakage of critical and confidential information in URLLC applications of may lead to attacks that are difficult to defend against.
If a malicious vehicle obtains a legitimate vehicle’s random number sequence (used for authentication or critical vehicle control), the malicious vehicle can successfully inject misleading information (e.g., dangerous control information) into the network, potentially causing fatal accidents.
Security for URLLC

The maximal secret communication rate is lower bounded by

\[
R(N, \epsilon, \delta) = \log_2(1 + \gamma_A) - \log_2(1 + \gamma_E)
- \sqrt{1 - (1 + \gamma_A)^{-2}} \frac{Q^{-1}(\epsilon)}{N \ln 2}
- \sqrt{1 - (1 + \gamma_E)^{-2}} \frac{Q^{-1}(\delta)}{N \ln 2}
\]

\(\epsilon\): Decoding error probability
\(\delta\): Secrecy constraint on information leakage

Security for URLLC

• Future Challenges in This Area

  – Coherent Communications versus Non-Coherent Communications
    • In URLLC, there may not be enough channel uses to perform channel estimation and feedback during one block. This leads to URLLC without CSI, i.e., non-coherent communications.
    • This limits Eve’s opportunity to obtain its own CSI. Thus, we need to clarify the conditions under which non-coherent communications outperform coherent communications and how much performance gain can be achieved.

  – Channel Inversion Power Control based on Channel Reciprocity
    • In some applications (e.g., emergence alert systems), only uplink or downlink communication requires URLLC. Channel inversion power control (CIPC) based on channel reciprocity can overcome CSI issues. Secrecy performance analysis and optimisation of CIPC are challenging.

  – Location-Based Beamforming with and without Artificial Noise
    • Location-based beamforming can improve reliability and security in some URLLC scenarios where line-of-sight (LOS) components exist in channels. The impact of location information accuracy and the LOS component weight on the use of artificial noise needs to be explored.
Energy-Efficient Secure Communication

An example of future energy efficient wireless communications networks.

FreeNet Page of the Advanced Networking Laboratory at New Jersey Institute of Technology.

©Nan Yang, Xiangyun Zhou, and Jemin Lee
Energy-Efficient Secure Communication

- Energy-efficient communications is the keystone underpinning the concept of green communications. In conventional physical layer security studies, **power allocation** is a widely-adopted method to optimise the use of energy.

- In future research, the consideration of physical layer security with promising energy-efficient methods, such as energy harvesting and wireless power transfer, would bring new opportunities for realising energy-efficient secure communication in the 5G and beyond era.

- Simultaneous wireless information and power transfer (SWIPT), where a source transmits information signals and power signals simultaneously to one or multiple receivers, receives considerable interests from academia and industry.

- Wireless power transfer can **prolong** the **lifetime** of a wireless network. Moreover, both information and power are transferred concurrently over the same carrier, which **extends** the function of traditional wireless systems.
Energy-Efficient Secure Communication

- Potential Risks within Secure Wireless Power Transfer:
  - When both the power receiver and the information receiver exist in the system, a security risk arises if the power receiver is malicious and able to successfully decode the information.
  - There may be an external eavesdropper, who pretends to be a legitimate information or power receiver and decode the information.
Energy-Efficient Secure Communication

- **Recent Contributions**
  - Using *multi-antenna techniques* exhibits a strong capability to enhance security, since it can support efficient power transfer and secure information transmission by making use of *spatial degrees of freedom*, e.g., [Shi_TWC_2015].
  - The *joint design of beamforming and artificial noise* can significantly improve the secrecy performance in some scenarios, e.g., [Tian_SPL_2015].
  - Introducing an *extra helper*, such as a cooperative relay or jammer, would introduce jamming interference and assist the source to supply wireless power, e.g., [Zhang_TCOM_2015].
  - When *massive MIMO* is deployed, the power transfer efficiency is improved significantly since the information leakage decreases sharply due to the use of high-resolution spatial beamformer, e.g., [Chen_TVT_2016].

Energy-Efficient Secure Communication

- Future Challenges in This Area
  - CSI Acquisition
    - The unavailability of the eavesdropper’s CSI, due to its passiveness;
    - The unavailability of the power receiver’s CSI, due to the lack of baseband circuit;
    - The imperfectness of the information receiver’s CSI.
  - Design Objective
    - Energy saving and wireless security are not aligned with each other.
    - Secrecy energy efficiency, i.e., secrecy rate / energy consumption, may be a proper quantity to leverage a trade-off between energy saving and security guarantee.
    - However, the maximisation of the secrecy energy efficiency is a non-trivial task, since the problem is always non-convex.
  - Adaptive Environment Sensing
    - It is imperative to enhance the capability of environment sensing, i.e., sensing the information and behaviours of the eavesdroppers, to improve the secrecy performance.
Unmanned Aerial Vehicle Secure Comm.

• By 2035, the number of UAV operations will surpass that of manned aircraft operations

• Many applications
  – Proposals from Facebook and Google to boost connectivity from the sky.
  – Communication, drone delivery, aerial surveillance, disaster management, live streaming, etc.

• Despite the research efforts devoted to physical layer security, the security issue of UAV wireless communication has so far drawn little attention.

Facebook Project ‘Aquila’

Google Project ‘LOON’
Unmanned Aerial Vehicle Secure Comm.

• UAV Communication Characteristics - Three types of UAV comm. channels
  – Ground to Ground (G2G) channel
    • Terrestrial communication
    • Generally in Non-Line-of-Sight (NLoS) environment, i.e., Rayleigh fading
  – Air to Air (A2A) channel [God_GCW_15,Kha_18]
    • Drone-to-drone channel
    • Generally in Line-of-Sight (LoS) environment, i.e., Rician fading
  – Air to Ground (A2G)/Ground to Air (G2A) channel
    • Can be either LoS or NLoS environment
      – Rayleigh fading for NLoS environment
      – Rician fading for LoS environment


Unlike terrestrial communications, the elevation angles affect the communication performance of not only the legitimate user but also eavesdropper.

- **Elevation angle**
  \[
  \theta_i = \arctan \left( \frac{d_i^{(V)}}{d_i^{(H)}} \right)
  \]
  - \(d_i^{(V)}\): vertical distance
  - \(d_i^{(H)}\): horizontal distance
- **LoS probability for G2A/A2G Channels** [AIH_WCL_14]
  \[
  p_L(\theta_i) = \frac{1}{1 + a_1 \exp \left\{ -b_1 (\theta_i - a_1) \right\}}
  \]
  - \(a_1\) and \(b_1\) are the environment dependent parameters (e.g., urban, suburban, dense urban).
  - When the elevation angle increases, the LoS probability increases.

Unmanned Aerial Vehicle Secure Comm.

- Recent Contributions
  - **UAV as a relay** in the presence of ground eavesdropper [Wan_WCL_17]
    - With the assumption that the instantaneous channel state information (CSI) of the eavesdropping link is known at the source, the secrecy rate is analyzed.
    - All nodes are equipped with a single antenna and the LoS link is used to characterize the ground-to-air channel.
  - **UAV as a receiver** in the presence of a full-duplex active eavesdropper on the ground [Liu_TWC_19]
    - Ground-to-air channel model with node-height-dependent LoS probability.
    - Eavesdropper can transmit directional jamming signals towards the UAV.
    - Source transmits information signals together with artificial noise (AN) to confuse the eavesdropper.
    - Determine the optimal power allocation factor between information signals and AN signals at the source as well as the operating height of UAV.


©Nan Yang, Xiangyun Zhou, and Jemin Lee
Unmanned Aerial Vehicle Secure Comm.

- **Recent Contributions**
  - **UAV as a friendly jammer** of unknown eavesdropper location [Zho-TVT_18]
    - An air-to-ground friendly jammer assisting secure communications between a legitimate transmitter-receiver pair for unknown eavesdropper location.
    - Impact of the UAV jamming power and its three-dimensional spatial deployment on the outage probability of the legitimate receiver and the intercept probability of the eavesdropper is examined.
  - **UAV with high mobility as a transmitter/receiver** in the presence of eavesdropper on the ground [Zha_TWC_19]
    - Both the downlink and uplink UAV communications with a ground node.
    - Ground-to-air channel model with node-height-dependent probability of having LoS link.
    - Jointly optimizing the UAV’s trajectory and the transmit power of the legitimate transmitter over a given flight period of the UAV to maximize the average secrecy rates of the UAV-to-ground and ground-to-UAV transmissions, respectively.


Unmanned Aerial Vehicle Secure Comm.

- **Brief Review on [Liu_TWC_19]**
  - **Legitimate system**
    - An $N_s$-antenna source + A single-antenna UAV
    - Spatially randomly distributed obstacles between source and UAV.
  - **Adversary model**
    - A full-duplex active eavesdropper (i.e., eavesdropping (receiving) data and transmitting jamming signal both at the same time)
    - $N_e$ transmitting antennas, $N_j$ jamming antennas, and $N_e + N_j = N_t$
  - **Artificial noise transmission at the source**
    - Source transmits artificial noise (AN) signals, in addition to information signals to confuse the eavesdropper.

Unmanned Aerial Vehicle Secure Comm.

- **Numerical Results**
  - Unique the artificial noise power portion at source that minimises the hybrid outage probability, which increase with the source antenna number.
  - Unique the UAV height that minimises the hybrid outage probability, which increases with the source transmission power.
Unmanned Aerial Vehicle Secure Comm.

• Numerical Results
  
  – Purely malicious jamming from the eavesdropper is no longer the optimal strategy for the eavesdropper.

©Nan Yang, Xiangyun Zhou, and Jemin Lee
Unmanned Aerial Vehicle Secure Comm.

- **Future Challenges in This Area**
  - Different to mobile nodes in terrestrial networks, UAV has higher mobility and 3-D location with stricter power constraint, which gives various new challenges.
  - **Communication secrecy against multiple eavesdropping UAVs**
    - Generally, the UAV-to-UAV (i.e., A2A) channel or the UAV-to-ground node (i.e., A2G) channel has larger channel gain as the LoS link is formed with high probability, which can increase the probability of being eavesdropped by the malicious UAVs.
    - Especially, in the scenario that multiple UAVs can be potential eavesdopppers, more efficient security techniques are required.
  - **Energy efficient physical layer security techniques for UAVs**
    - Energy efficiency is the most critical design parameter in UAV-related techniques as UAVs are battery-powered device. Hence, traditional techniques consuming more power such as friendly jamming or artificial noise-based schemes can not be suitable for UAVs.
    - The techniques which get help from ground devices (e.g., ground jammer) or exploit the mobility of UAVs to get closer to some targets are required.
Prototyping via Software Defined Radio

- The use of Universal Software Radio Peripheral (USRP) is a rapid and easy-to-use way for prototyping wireless systems. This connection between an USRP and a PC includes four series:
  - **Bus (B) Series** – Connected to a host computer via a USB
  - **Network (N) Series** – Connected to a host computer via an Ethernet
  - **High Performance (X) Series** – Connection can be Ethernet or a x4 PCI-Express connection
  - **Embedded (E) Series** – Stand-alone (without a host computer).

©Nan Yang, Xiangyun Zhou, and Jemin Lee
Prototyping via Software Defined Radio

- The use of Wireless Open Access Research Platform (WARP) is another option for prototyping wireless systems.
- Strictly speaking, this is not an SDR-based prototyping. But it has been widely used by many researchers.

http://warpproject.org/trac

©Nan Yang, Xiangyun Zhou, and Jemin Lee
Prototyping via Software Defined Radio

- WARPLab Reference Design
  - Fast physical layer algorithm prototype
  - WARP hardware + MATLAB (physical layer algorithm programming)
  - Wireless transmission (real time/real channel) + signal processing (offline)
Prototyping via Software Defined Radio

• Some Results on Physical Layer Group Key Generation
  – Group key generation scheme in [Tha_TIFS_19]
  – Setup
    • NI 8135 Controller
    • NI 1082 PXI Chassis
    • USRP RIO 2952
    • Labview Communication Design Suite
  – Implementation Issue
    • Rapid toggling in between TX & RX modes
      – FPGA based muxing automatic transmit / receive (ATR) registers
      – Toggling Tx Enable & Rx Enable bits


©Nan Yang, Xiangyun Zhou, and Jemin Lee
Prototyping via Software Defined Radio

- Some Results on Friendly Jamming
  - Performance Evaluation
    - Quality of image received at the receiver
    - Quality of image at eavesdropper
  - Structure Similarity Index [Zho_TIP_04]
    - Assesses the visual impact of luminance, contrast and structure
  - Experiment Setup
    - Grid of 6 m x 10 m
    - Transmitter at [3, 6.5]
    - Receiver at [3, 10]
    - Friendly Jammer at [3, 3]

Prototyping via Software Defined Radio

- Measurement at Legitimate Receiver

(a) Original image
(b) $C_1$ SSIM = 0.9476
(c) $C_2$ SSIM = 0.5695
(d) $C_3$ SSIM = 0.1406

- Receiver have a imperceptible image under C1 and C2 cases of jamming power

### TABLE I

<table>
<thead>
<tr>
<th>No.</th>
<th>$P_T$ (dB)</th>
<th>$P_J$ (dB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>C2</td>
<td>10</td>
<td>5</td>
</tr>
<tr>
<td>C3</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>C4</td>
<td>10</td>
<td>15</td>
</tr>
</tbody>
</table>
Prototyping via Software Defined Radio

- Secure Region Measurement
  - By changing the location of eavesdropper, we measure the area that the eavesdropper does not get good quality of the image.
  - That means by placing the friendly jammer, we can guarantee of the communication secrecy for the potential eavesdroppers in the secure region.
Outline

• Security in mobile communication networks
  – Evolution of cellular networks
  – Security issues in cellular networks
  – Re-shape security design in 5G and beyond wireless networks

• Theoretical advancement in PHY layer security
  – Fundamentals of PHY layer security
  – Existing secrecy performance metrics
  – New secrecy performance metrics
  – Trust degree-aided secure communication
  – PHY layer key generation

• Cutting-edge PHY layer security solutions
  – Heterogeneous secure communication
  – Full-duplex secure communication
  – Massive MIMO-aided secure communication
  – Secure communication over mmWave channels
  – Machine type secure communication
  – NOMA-based security
  – Security for URLLC
  – Energy-efficient secure communication
  – Unmanned aerial vehicle secure communication
  – Software defined radio-based prototyping

• Future directions, challenges and open issues
  – PHY layer security beyond content secrecy
  – Cross-layer security
  – Challenges imposed by future wireless world
Physical Layer Security Beyond Content Secrecy

• In this part, we will focus on the following three topics:
  – Covert Communication – Protect the Existence of Communication
  – Physical Layer Authentication
  – Physical Layer Forensics and Identification
Background in Covert Communications

• What is covert wireless communication?

• Three users:
  o Transmitter: Alice
  o Receiver: Bob
  o Warden: Willie

• Two aspects of the problem:
  o Communications from Alice to Bob
  o Detection of Alice’s transmission at Willie

• Why are covert wireless communications important?
  – Preserve the privacy/secrecy of a transmitter (e.g., its existence, its activity, its location information);
  – The content of communication can be better protected if the existence of communication is undetectable (in most cases).
Background in Covert Communications

- Covert wireless communications was addressed by spread spectrum (SS) techniques (Frequency Hopping SS, Direct Sequence SS, etc.).
  - The achieved security has never been proven theoretically – hence we do not know how often SS techniques fail to hide wireless transmissions and how to optimally design for covert communications.

- Recent research in covert wireless communications aims to establish the theoretical foundation, which answers questions like:
  - What is the maximum achievable communication rate at which Willie is not able to detect with high probability?

- Difference from current physical layer security studies:
  - Current PHY security aims to protect the content of communication from being understood by illegitimate users.
  - Covert communication aims to protect the existence of communication from being detected by unwanted users.
Background in Covert Communications

- Bob’s communication performance depends on:
  - Alice’s transmit power
  - Alice-Bob channel
  - Bob’s knowledge about the channel
  - Coding scheme (e.g., length of codeword)
  - ...

- Willie’s detection performance depends on:
  - Alice’s transmit power
  - Alice-Willie channel
  - Willie’s knowledge about the channel
  - Coding scheme (e.g., length of codeword)
  - ...

©Nan Yang, Xiangyun Zhou, and Jemin Lee
Ways to Covert Communications

• To achieve some level of covertness
  – Control the packet length to limit the amount of observations at Willie
  – Make use of the variation in ambient noise/interference
  – Make use of the time-varying nature of the fading channel
  – Intentionally create time-varying interference
...

• Let’s look into two examples:
  – Covert Communication with finite blocklength [Yan_TIFS_17]
  – Covert Communication with noise uncertainty [He_CL_17]

Infinite Blocklength vs Finite Blocklength

- **Blocklength means**
  - The number of channel used to transmit one message, or equivalently
  - The length of the codeword

- **Covert communication with infinite blocklength (i.e., Prior Research)**
  - No positive rate is achievable if Willie has perfect knowledge of the channel statistics.
  - Alice can transmit at most $O(\sqrt{n})$ bits in $n$ channel uses covertly to Bob as $n \to \infty$.

- **Why finite (and possibly short) blocklength makes a difference?**
  - It means a finite number of observations at Willie, which leads to uncertainty.
  - In fact (as we will see), a positive covert rate is achievable with finite blocklength (if we allow some small error probability at Bob).
Covert Communication: Finite Blocklength

- **Main assumptions:**
  - AWGN channels for both Bob and Willie
  - Gaussian signalling at Alice
  - Finite blocklength, i.e., $n \leq N$

- **Questions to address:**
  - What is the optimal $n$ for covert communications?
  - What is Alice’s maximum allowable transmit power, hence the maximum rate?
Covert Communication: Finite Blocklength

- Signal Model, Achievable Rate and Throughput
  - Received signal for each channel use at Bob:
    \[ y_b[i] = x[i] + r_b[i]. \]
  - where \( i = 1, 2, ..., n. \)
  - For a given decoding error probability \( \delta \), the channel coding rate (i.e., data rate) of the channel from Alice to Bob is given by this well-known approximation
    \[ R \approx \log_2(1 + \gamma_b) - \sqrt{\frac{\gamma_b(\gamma_b + 2)}{n(\gamma_b + 1)^2}} \frac{Q^{-1}(\delta)}{\ln(2)} + \frac{3\log_2(n)}{2n}, \]
  - where \( \gamma_b = P/\sigma_b^2 \) is the signal-to-noise ratio (SNR) at Bob.
  - The effective throughput from Alice to Bob within \( n \) channel uses is given by
    \[ \eta = nR(1 - \delta). \]
Covert Communication: Finite Blocklength

- Willie’s Detection: Binary Hypothesis Testing
  - Two Hypotheses:
    \[
    \begin{align*}
    \mathcal{H}_0 &: y_w[i] = r_w[i] \\
    \mathcal{H}_1 &: y_w[i] = x[i] + r_w[i]
    \end{align*}
    \]
  - Likelihood ratio test that minimizes the total error:
    \[
    \frac{P_1}{P_0} \triangleq \frac{\prod_{i=1}^{n} f(y_w[i] | \mathcal{H}_1)}{\prod_{i=1}^{n} f(y_w[i] | \mathcal{H}_0)} \overset{D_1}{\underset{D_0}{\geq}} 1.
    \]
  - Effectively, radiometer is the optimal detector, which is given by
    \[
    T \triangleq \frac{1}{n} \sum_{i=1}^{n} |y_w[i]|^2 \overset{D_1}{\underset{D_0}{\geq}} \Gamma = \frac{(P + \sigma_w^2)\sigma_w^2}{P} \ln \left( \frac{P + \sigma_w^2}{\sigma_w^2} \right)
    \]
    - i.e., compare the average received power with a predetermined threshold
Covert Communication: Finite Blocklength

- **Willie’s Detection Performance:**
  - False alarm probability and miss detection probability:
    \[
    P_F = \Pr(T > \Gamma | \mathcal{H}_0) = 1 - \frac{\gamma \left(n, \frac{n\Gamma}{\sigma_w^2}\right)}{\Gamma(n)},
    \]
    \[
    P_M = \Pr(T < \Gamma | \mathcal{H}_1) = \frac{\gamma \left(n, \frac{n\Gamma}{P + \sigma_w^2}\right)}{\Gamma(n)}.
    \]
  - The sum error probability (for equal a priori probability) is given by \(P_F + P_M\).
  - To simplify the analysis, we use a lower bound on the total error probability:
    \[
    P_F + P_M \geq 1 - \sqrt{\frac{1}{2} \mathcal{D}(P_0 \| P_1)},
    \]
  - where \(\mathcal{D}(P_0 \| P_1)\) is the Kullback-Leibler (KL) divergence from \(P_0\) to \(P_1\), expressed as
    \[
    \mathcal{D}(P_0 \| P_1) = n \left[ \ln \left( \frac{P + \sigma_w^2}{\sigma_w^2} \right) - \frac{P}{P + \sigma_w^2} \right]
    \]
Covert Communication: Finite Blocklength

• Covert constraint:
  – A direct covert constraint: \( \xi = P_F + P_M \geq 1 - \epsilon \)
  – With the aid of the lower bound on the total error probability, a more strict covert constraint is given by
    \[
    \mathcal{D}(\mathbb{P}_0||\mathbb{P}_1) \leq 2\epsilon^2
    \]

• Optimisation problem at Alice:
  \[
  \max_{n,P} \eta, \quad \text{s.t. } \mathcal{D}(\mathbb{P}_0||\mathbb{P}_1) \leq 2\epsilon^2, \quad n \leq N.
  \]

• Solution:
  – The transmit power \( P \) reduces as \( n \) increases to maintain the covert constraint.
  – The optimal \( n \) is its maximum value: \( N \).
Covert Communication: Finite Blocklength

- The throughput (total number of bits) increases with blocklength, but the data rate (number of bits per channel use) decreases with blocklength.
Previously We Have Said ...

- Covert communication with infinite blocklength (i.e., Prior Research)
  - No positive rate is achievable if Willie has perfect knowledge of the channel statistics.
  - The main reason is that Willie has (i) an infinite number of observations; (ii) no uncertainty in the statistics of its received signal.
- Introducing uncertainty in Willie’s noise power
  - In wireless networks, Willie’s noise consists of its own receiver noise and ambient interference. The latter may be time-varying.
  - Hence, Willie probably has uncertainty in its noise power.
  - As we will see, a positive covert rate is achievable in this case.
Covert Communication: Noise Uncertainty

• Main assumptions:
  – AWGN channels for both Bob and Willie
  – Gaussian signalling at Alice
  – Willie does not know its exact noise power.

• Questions to address:
  – What is the maximum covert rate?
  – How does the maximum covert rate change with the noise uncertainty?
Covert Communication: Noise Uncertainty

- Two Hypotheses:
  - $H_0$: Alice is not transmitting to Bob
  - $H_1$: Alice is transmitting to Bob

- The received signal at Willie:
  $$H_0 : y_w[n] = v_w[n]$$
  $$H_1 : y_w[n] = \sqrt{P_t/r_\alpha} x[n] + v_w[n]$$
  - where the noise follows a Gaussian distribution with variance $\sigma_w^2$

- Noise Uncertainty at Willie: Willie doesn’t know the exact value of $\sigma_w^2$.
- For simplicity, we do not consider noise uncertainty at Bob.
Covert Communication: Noise Uncertainty

• In [He_CL_17], we have adopted two noise uncertainty models, one bounded and one unbounded. We use the unbounded model as an example:

Unbounded uncertainty model: We have $\sigma_{w,dB}^2 \in [-\infty, +\infty]$. We assume that the difference between the exact noise power and the nominal noise power in the dB domain follows a normal distribution, i.e., $\Delta = \sigma_{w,dB}^2 - \sigma_{n,dB}^2 \sim \mathcal{N}(0, \sigma_{\Delta,dB}^2)$. Denoting $k = \ln(10)/10$, the log-normal distribution of $\sigma_{w}^2$ is given by

$$f_{\sigma_{w}^2}(x) = \begin{cases} \frac{1}{x\sqrt{2\pi k^2\sigma_{\Delta,dB}^2}} \exp\left(-\frac{(\ln(x)-k\sigma_{n,dB}^2)^2}{2k^2\sigma_{\Delta,dB}^2}\right), & \text{if } x > 0 \\ 0, & \text{otherwise.} \end{cases}$$

• In other words, Willie knows that its noise power in dB follows a Gaussian distribution with a known mean and variance.
The received signal at Willie:

\[ H_0 : y_w[n] = v_w[n] \]

\[ H_1 : y_w[n] = \sqrt{P_t/r_{w_0}^\alpha} x[n] + v_w[n] \]

Similar to previous studies, Willie’s detection is to compare the average received power with a given threshold:

\[
T(y_w) = \frac{1}{N} \sum_{n=1}^{N} |y_w[n]|^2 \begin{cases} \mathcal{D}_1 & > \gamma \\ \mathcal{D}_0 & \leq \gamma \end{cases}
\]

The total detection error probability, \( \xi = P_{FA} + P_{MD} \), at Willie for a given threshold (known) and noise power (unknown) can be computed and denoted by \( \xi(\sigma_w^2, \gamma) \).
Covert Communication: Noise Uncertainty

- The average total detection error probability (averaged over the distribution of Willie’s noise power) is given by

\[
\bar{\xi} = \min_{\gamma} \int_{0}^{\infty} \xi(\sigma_w^2, \gamma) f_{\sigma_w^2}(\sigma_w^2) d\sigma_w^2
\]

- The minimisation means that Willie uses the best detection threshold to minimise the averaged total error probability.

- The covert requirement from Alice & Bob’s viewpoint is given by (as \(N \to \infty\)):

\[
\bar{\xi} \geq 1 - \epsilon
\]

- Hence, the maximum covert rate is given by solving the following problem:

\[
\max_{P_t} \quad R = \frac{1}{2} \log_2 \left(1 + \frac{P_t}{r_b^\alpha \sigma_b^2}\right)
\]

s.t. \(\bar{\xi} \geq 1 - \epsilon\).
Covert Communication: Noise Uncertainty

- Achievable rate under different covertness requirements, for the log-normal model of the noise power with the mean value of -100dBm.
Covert Communications with Intentionally Generated Interference

- **Left**: Full-duplex Receiver scenario [Shahzad_TWC_18]
  - The full-duplex receiver sends time-varying interference with self-interference cancellation capability.

- **Right**: Backscatter communication scenario [Shahzad_ICC_19]
  - The (full-duplex) reader sends time-varying Gaussian-modulated signal for the tag to perform backscatter communication.

Physical Layer Authentication

• Authentication is the process of verifying the identity of a user:
  – verifying you are who you say you are.
  – knowing you are talking to the right person.

• Authentication makes use of attributes unique to a single user.

• At the physical layer, unique attributes include [Wang-CM’16]:
  – Channel characteristics (fading channel gain, received signal strength indicator, round-trip time, etc.)
  – Analog front-end characteristics (IQ imbalance, carrier frequency offset, DAC convertor and power amplifier features, etc.)

• These channel and device characteristics are typically estimated and compensated at the receiver side for data reception. Hence, authentication based on these known features do not incur significant overhead.

Physical Layer Forensics and Identification

- Forensic evidence should be tracked in the wireless network in order to:
  - identify and locate the security attacks
  - identify and locate unauthorised communications

- Forensics of jamming attack is an example [Liu-ICASSP_15]. Forensics evidences include
  - Received signal strength and angle of arrival

- In the case of unauthorised communication, signal processing techniques can be used to identify [Eldemerdash-CST_16]:
  - Carrier frequency and spectrum usage
  - Modulation scheme
  - Coding scheme
  - Number of transmit antennas


• The physical layer security community:
  – Very few of us knows cryptography and system-level security.
  – Some of us even still claim that physical layer security can replace cryptography in many scenarios.
  – Our most-used information-theoretic secrecy metrics are difficult to be measured in practice and has no direct connection to cryptographic secrecy metrics.

• The cryptography community:
  – Very few of them knows communication theory and signal processing
  – Almost all current security solutions are using cryptography. Why bother considering a completely new approach for security?

• Probably the only solution is for PHY security people to approach cryptography people and convince them that we can work together.

• But how?
Cross-Layer Security: Road Ahead

• Secret key generation from wireless channel:
  – This is already a starting point and directly connects to cryptography;
  – However, the main issue is that the key generation rate is often too small for stationary and low-mobility devices.

• Talk in the same language of cryptography people:
  – Understand cryptography;
  – Use physical layer techniques to enhance the performance of certain cryptographic method;
  – The performance metric should be the one used in cryptography.
  – In this regard, we see two very different directions of research: semantic security (very strong security requirement) and partial-secrecy based security (not so strong security requirement). We will talk about the latter one a bit further.
Cross-Layer Security: Example

- The block diagram of a cross-layer secure communication system [Harrison_Dis_12]

  ![Block Diagram]

- Physical layer techniques (making use of smart channel coding, modulation and signal processing) can ensure that the ciphertext received at Bob is almost free of error and the ciphertext received at Eve contains a certain amount of error.

- [Harrison_Dis_12] studied the performance of a certain cryptographic method giving erroneous ciphertext at Eve.

Cross-Layer Security: Example

- [Harrison_Dis_12] took a stream cipher (using a keystream generator based on linear-feedback shift register) as an example. Some well-known correlation attack is tested.

- The figure shows the expected bound on the number of trials required to find the secret key. The parameter \((1-p_1)\) is the correlation value of the keystream generator and \(p_2\) is the error probability in the ciphertext at Eve.

- Increasing the bit error probability at Eve causes orders of magnitude increase in the required time to obtain the key.
Challenges Imposed by Future Wireless World
Challenges Imposed by Future Wireless World

- In 5G and beyond business environment, security is a necessary enabler for continuity of the business.
  - Users already realise that security and privacy are important, and they could be aware of the security/privacy service provided to them.
  - The extent and strength of the security mechanisms provided correlate with the perceived security level, at least in the long run.

- In the 5G and beyond context, users may already have some perception of provided security level based on experience with earlier generations.
  - Security and privacy features that exist in earlier generations are also present in 5G and beyond, although the actual technical security mechanisms may be different.

- It is not sufficient just to provide the same security features as in the legacy systems because there may be new security requirements and challenges.
  - 5G and beyond systems are service-oriented. This implies a special emphasis on security and privacy requirements that stem from the angle of services.
Challenges Imposed by Future Wireless World

• Security Challenges Ahead
  – New Business Models
    • In traditional mobile communications networks, users may communicate by text messages, voice calls, and video calls, or surf Internet or access app services using smart phones.
    • 5G era is no longer confined to individual customers, i.e., not simply about having a faster mobile network or richer functions in smart phones.
    • 5G and beyond networks will serve vertical industries, from which a diversity of new services will stem.
  – IT-Driven Network Architecture
    • New IT technologies, such as virtualisation and Software Defined Network (SDN)/Network Functions Virtualisation (NFV), are seen as a way to make 5G and beyond networks more nimble and efficient, yet less costly.
    • Security cannot be built for 5G and beyond services unless the network infrastructure is robust. In 5G, virtual network elements (NEs) are on cloud-based infrastructure. Thus, it is the right time to take 5G infrastructure security into consideration.
Challenges Imposed by Future Wireless World

- **Security Challenges Ahead**
  
  - **Heterogeneous Access**
    
    - Heterogeneous is one of the network features of next-generation access networks, coming not only from the use of different access technologies (WiFi and LTE), but from multi-network environment. So, security designers need to build security architecture suitable for different access technologies.
    
    - IoT devices may access networks directly, or via a gateway, or in the D2D or relay fashion. Comparing to mobile handset, security management of IoT device in 5G and beyond networks may be efficient and lightweight to establish trust relationships between devices and networks.
  
  - **Privacy Protection**
    
    - Vertical industries, including health care, smart home, and smart transport, will resort to 5G and beyond networks. As open network platforms, 5G and beyond networks raise serious concerns on privacy leakage.
    
    - Mobile networks carries data and signalling that contains many personal privacy information (for instance, identity, position, and private content). To offer differentiated quality of service, networks may need to sense the type of service a user is using, which may involve user privacy.
Challenges Imposed by Future Wireless World

- Future security design provides security protection for everything-connected world.
- Special attention needs to be paid to
  - End-to-end security for vertical industries with differentiated security protection, flexibility, and privacy protection.
  - Secure infrastructure with diversified system level protection of IT-aware infrastructure, identity management, and data protection.

- 4G: Networks authenticate users for network access. User-service authentication is not covered by networks.
- 5G: Networks cooperate with service providers to carry out an even secure and more efficient identity management.
Conclusion

Security is a necessary requirement in wireless communications networks

Physical layer security – fundamentals and existing contributions

Physical layer security – new promising techniques

Security in future wireless networks, i.e., 5G and beyond era.

©Nan Yang, Xiangyun Zhou, and Jemin Lee