

Random Graphs and Wireless Communication Networks

Part 7: Incorporating Secrecy and Trust into Network Analysis

September 6, 2016

Justin P. Coon

with Geojie Chen, Carl Dettmann, Marco Di Renzo and Orestis Georgiou



Outline

- Overview of Security in Wireless Networks
- Countering Security Threats in Wireless Networks
- Fundamentals of Physical Layer Security
- Physical Layer Security in Random Networks
- Trusted Networks

Overview of Security in Wireless Networks

- Secrecy is a key issue in wireless communication networks
 - 5G Communications, i.e., D2D, M2M
 - Near Field Communications, i.e., Apple Pay
 - Military Networks, i.e., Drone Self-Organized Networks
 - Medical Communications



Overview of Security in Wireless Networks

Layered communications architecture

Application	Secure Shell (SSH)
Transport	Transport Layer Security (TLS/SSL)
Network	Internet Protocol Security (IPSec)
Link	Wired Equivalent Privacy (WEP)
Physical	Information theoretic security

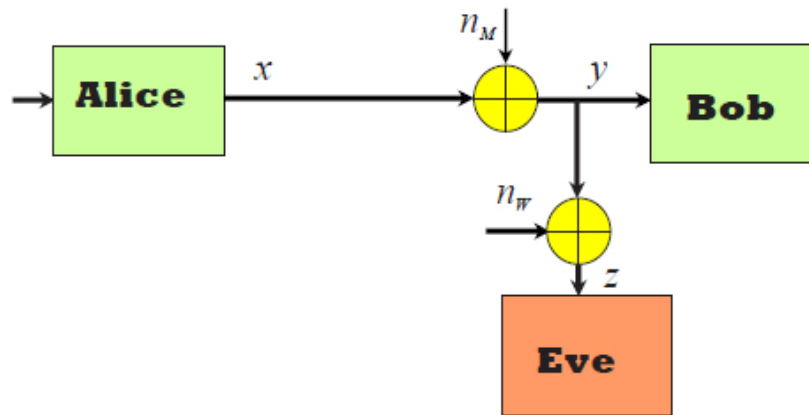
Countering Security Threats in Wireless Networks

- Cryptography
 - ✓ Assumes limited computational power at the eavesdropper
 - ✓ Vulnerable to large-scale implementation of quantum computers
 - ✓ At higher layers of the protocol stack
- Spread spectrum, e.g., frequency hopping & CDMA
 - ✓ Assumes limited knowledge at the eavesdropper
 - ✓ Vulnerable to rogue or captured node events
 - ✓ At the physical layer
- Information theoretic security
 - ✓ No assumptions of limited computational power or knowledge at eavesdropper
 - ✓ Absolutely secure
 - ✓ At the physical layer
 - ✓ Uses signal processing, communications and coding schemes

Fundamentals of PHY Security

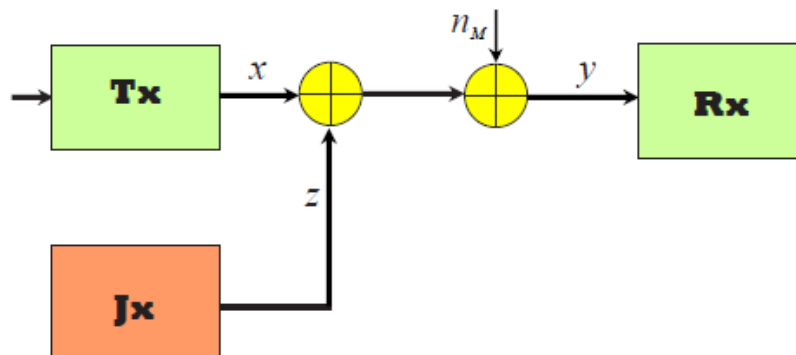
Breaches in wireless (physical layer) network security

✓ Eavesdropping



The purpose of an eavesdropper is to listen to the transmission, and try to detect the secret messages encoded therein.

✓ Jamming



The purpose of a jammer is solely to disrupt the process of communication by increasing the legitimate receiver's probability of decoding error.

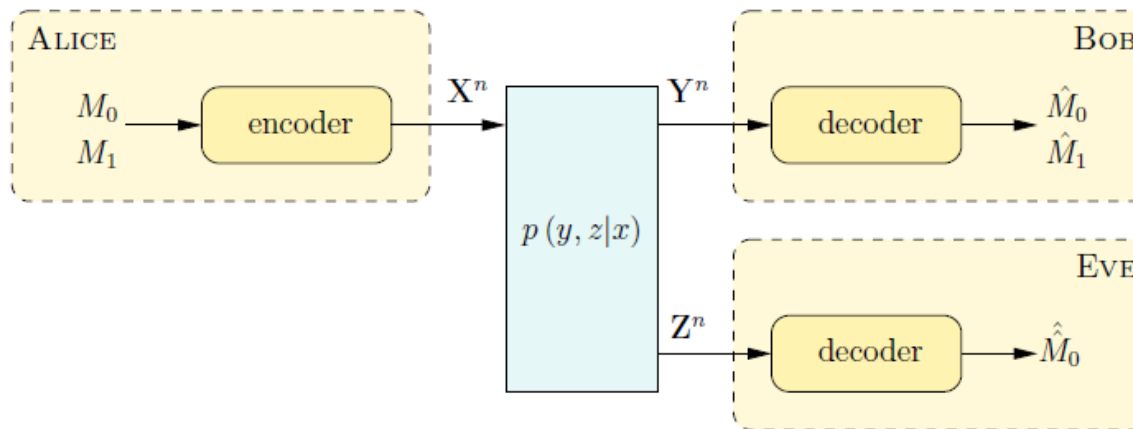
Fundamentals of PHY Security

- **Cipher**

Security: $H(K) > H(S)$

[Shannon, 1949]

- **Wire-tap Channel**



Reliability: $P_r(\hat{M}_n \neq M_n) \rightarrow 0$

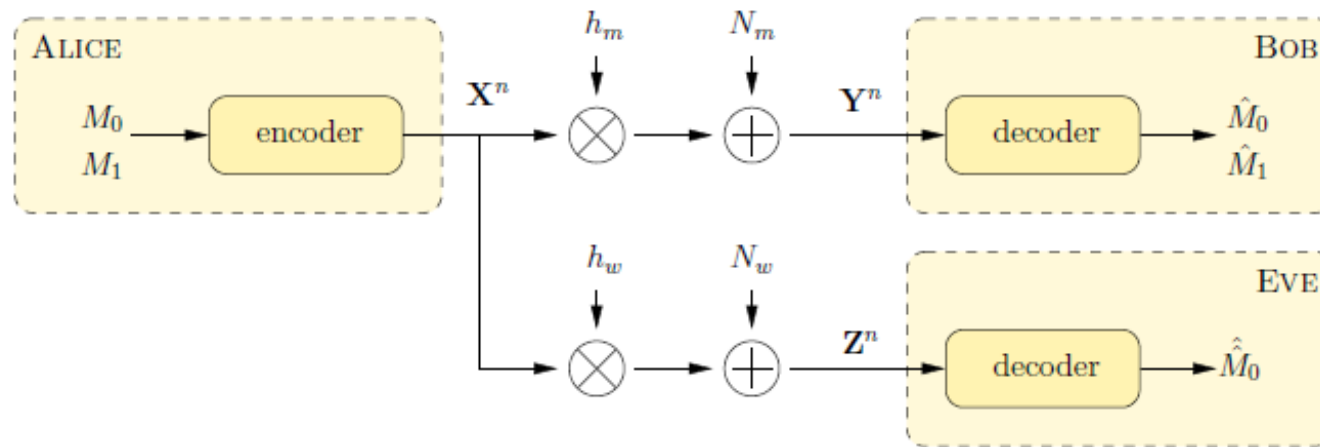
Security: $\bar{I}(M_n; Z^n) \rightarrow 0$

The wire-tap channel must be **degraded**.

[Wyner, 1975; Csiszar & Korner, 1978]

Fundamentals of PHY Security

- Fading Wire-tap Channel



Secrecy capacity:

$$C_s = [C_b - C_e]^+$$

Secrecy outage probability:

$$P_{so} = Pr(C_s < \epsilon)$$

Secrecy connectivity probability:

$$P_{sc} = Pr(C_s > 0)$$

Fundamentals of PHY Security

Secrecy Enhancement for PHY Security

- ✓ Preprocessing
 - Coding
 - Secrecy Key Generation

- ✓ Signal Processing
 - MIMO/massive MIMO & beamforming
 - Transmit antenna selection
 - Full duplex communication/artificial noise

- ✓ Cooperation Communications
 - Relay & artificial noise

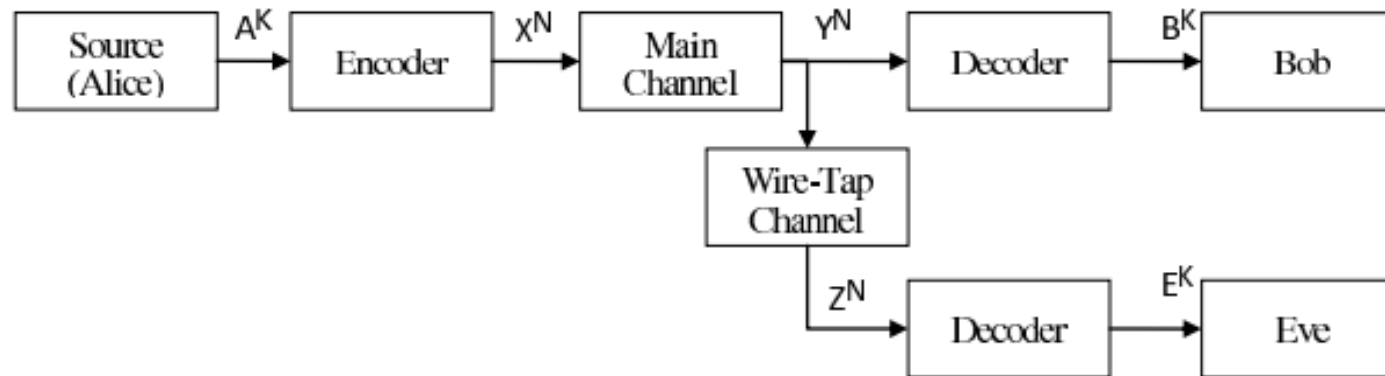
- ✓ Game Theoretic Methods

Secrecy Enhancement

Preprocessing

Coding

- To fully exploit the randomness of the channel for security, we need secrecy-capacity-achieving channel codes



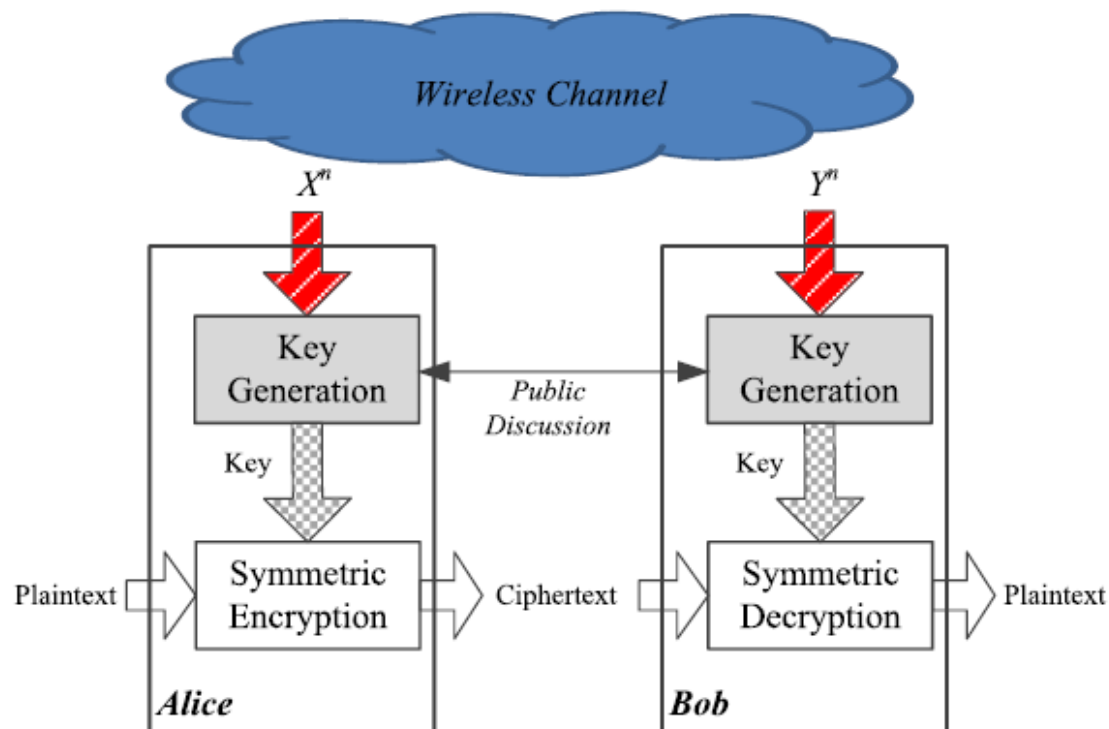
- The coding problem for Alice in the wire tap channel involves adding redundancy for enabling Bob to correct errors (across the main channel) and adding randomness to keep Eve in the dark (across the wire-tap channel), which is different from coding in traditional communications.
- Polar codes, LDPC will be used potentially in 5G standard

Secrecy Enhancement

Preprocessing

Secure key generation

- The ability to exchange keys between users is vital in any wireless based security system. So a key generation technique that exploits the randomness of the wireless channel is a promising alternative to existing key distribution techniques, e.g., public key cryptography.



[Zhang, 2016]

Secrecy Enhancement

Signal Processing

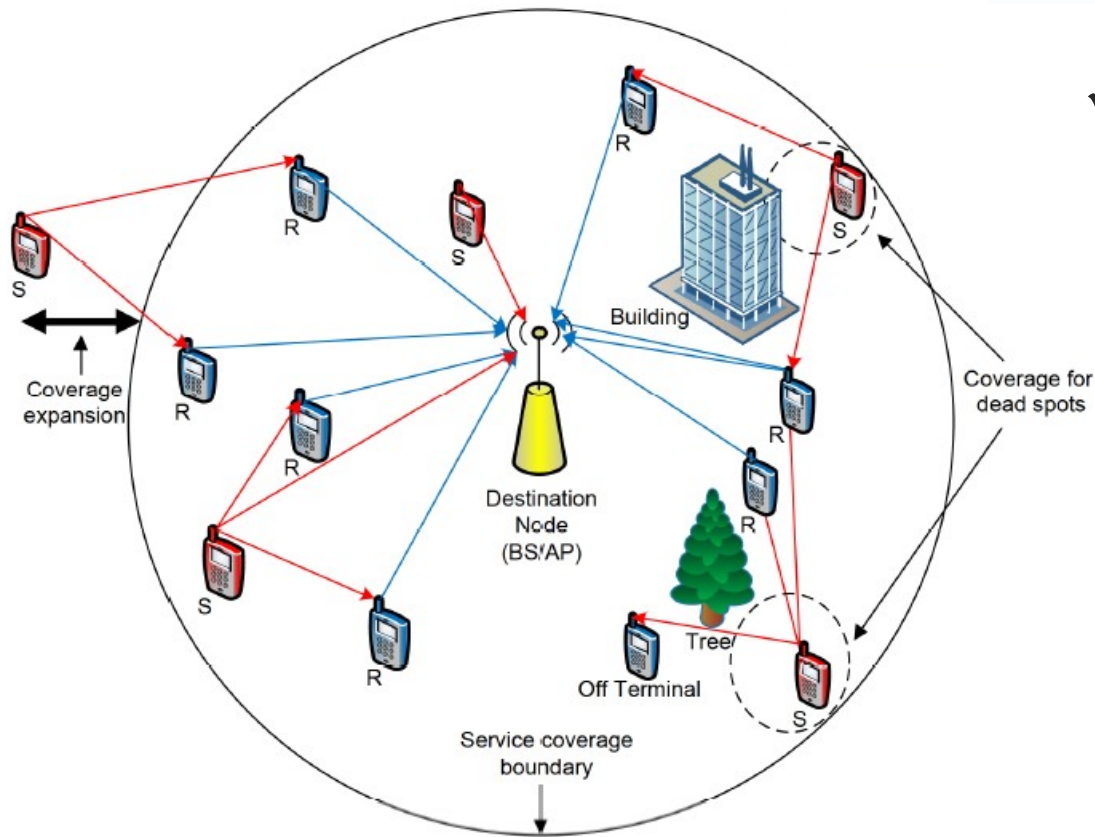
- ✓ Beamforming
 - Generate a useful signal with a pencil beam aligned with the legitimate user (LU)
 - Generate an artificial noise signal in the null space of the LU

- ✓ Antenna selection
 - Secrecy performance can be enhanced by exploiting the diversity gain of the intended link.
 - Reduces the implementation complexity of MIMO/massive MIMO
 - Channel state information between the transmitter and eavesdroppers could be perfectly known or partially known.

- ✓ Full duplex transmission
 - Thanks to self-interference (SI) cancellation techniques, the power of residual SI can be close to the noise level.
 - An artificial noise/jamming signal will affect passive eavesdroppers.

Secrecy Enhancement

Cooperative Communications



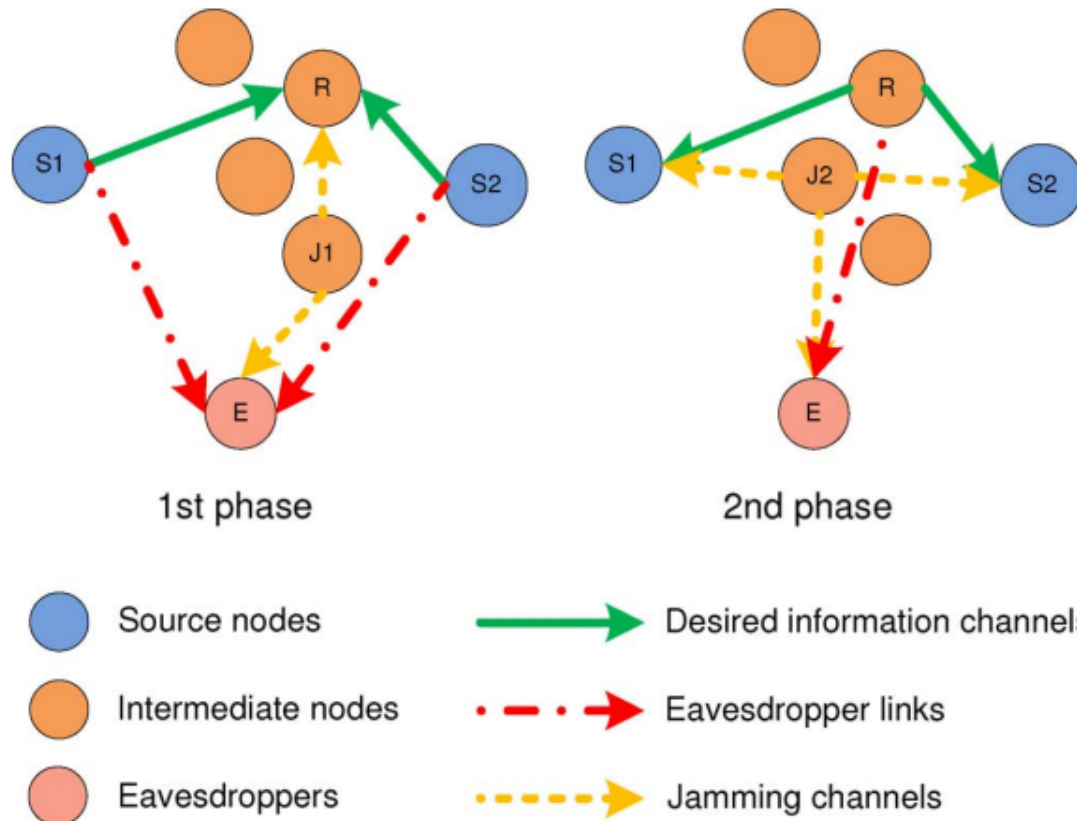
✓ What is the advantage of cooperative communication?

- Relays are used to assist transmission between source and destination
- Performance gains
- Enlarge the coverage

Secrecy Enhancement

Cooperative Communications

- ✓ Relay-assisted & jamming (artificial noise)



[Chen, 2012]

Secrecy Enhancement

Cooperative Communications

- ✓ Relay-assisted & jamming (artificial noise)
 - Friendly jammer selection
 - Buffer-added relay selection
 - Dual antenna selection with full duplex scheme

- ✓ Key issues for secrecy enhancement
 - Need to know the CSI between the transmitter and the eavesdropper(s)
 - Need to know the location(s) of eavesdropper(s)
 - Mostly, only a few nodes have been considered in the literature

Summary: A significant amount of work has been done to study information theoretic security in three-node and small networks.

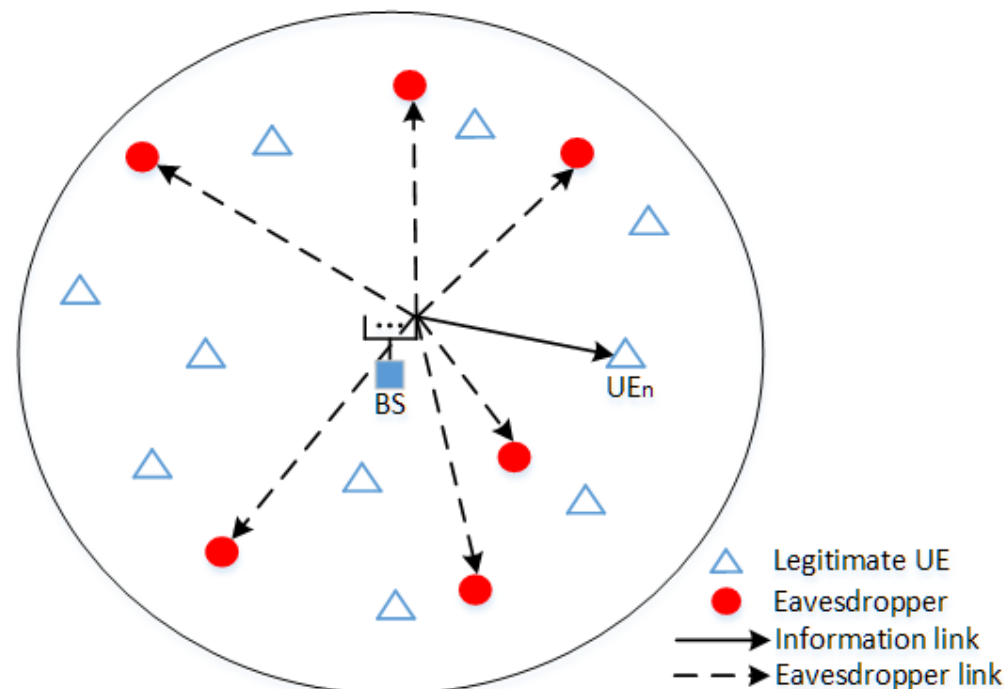
We, as a community, are now in a position to develop models, theory and methods to describe and optimize security in large-scale networks.

But what kinds of questions would we like to ask?

- Do information theoretic security techniques scale?
- How can we design and optimize network features?
- How robust are PHY secrecy solutions to eavesdropper scaling?
- How does spatial randomness affect secrecy?

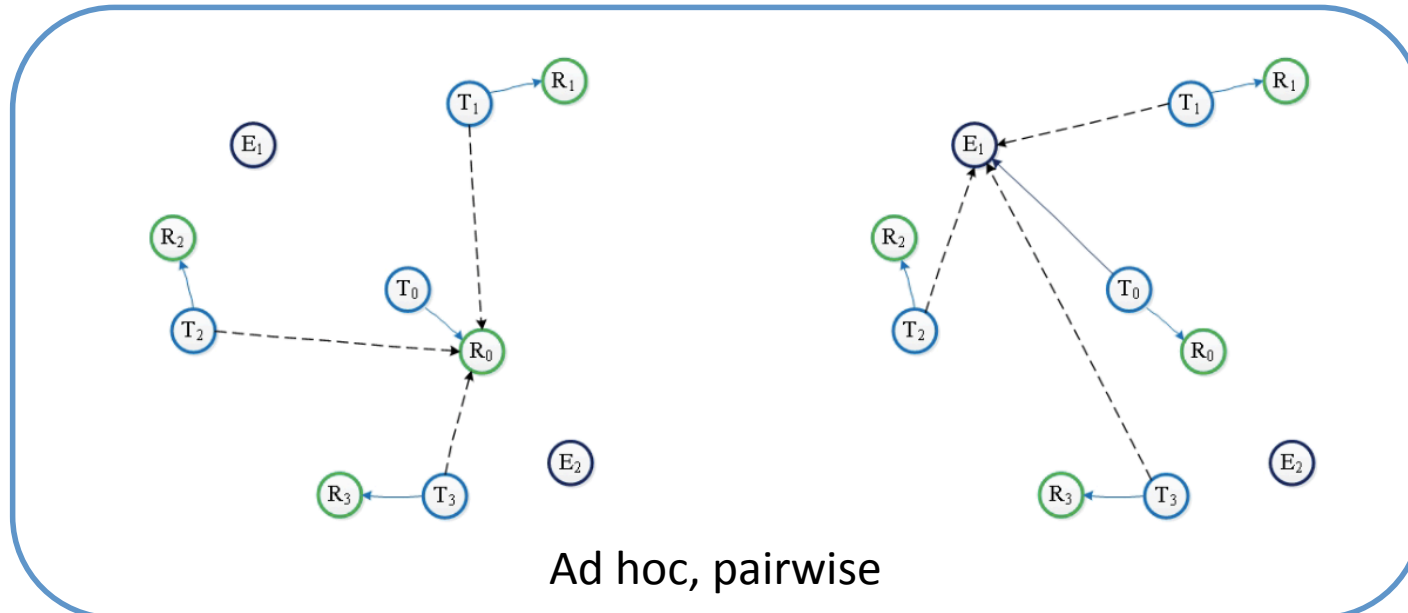
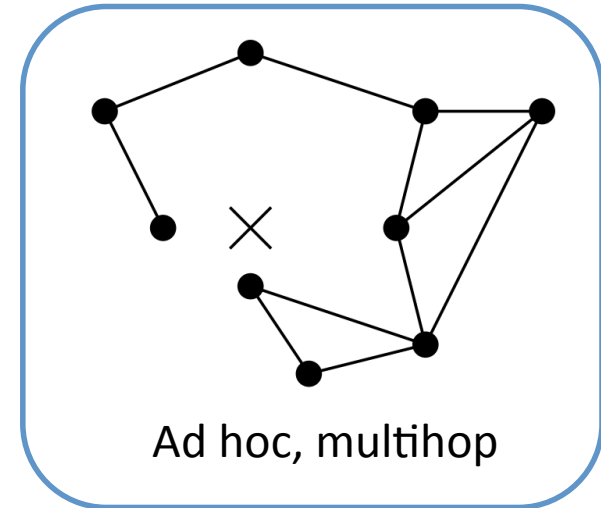
How can we model secrecy in large networks?

- **Point processes and random graph formalisms**
 - ✓ Large number of nodes can be analysed accurately
 - ✓ Average performance can be analysed; locations and CSI for eavesdroppers are random



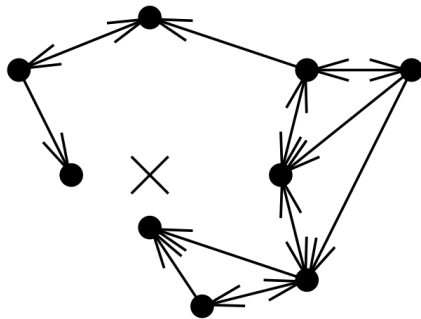
Main Network Models for Secrecy

- Several different network models have been studied
 - Ad hoc, multihop
 - Ad hoc, pairwise
 - Broadcast, cellular

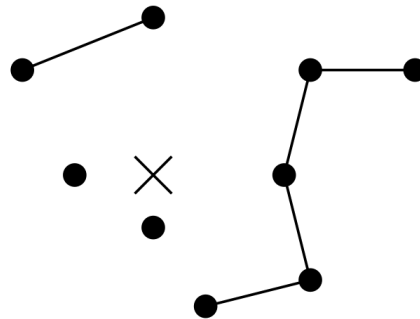


First Secrecy Network Models: Ad Hoc, Multihop

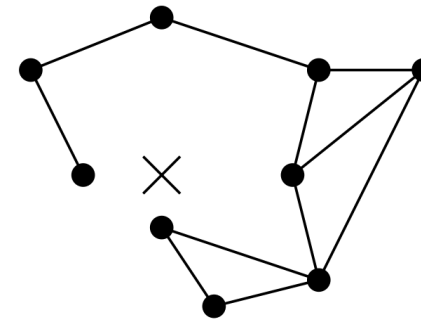
- The first forays into network secrecy took a simplistic view
 - Secrecy graph [Haenggi, 2008], [Goel, 2010]
 - Few eavesdroppers, focused on hard disk connection



(a) Directed SG \vec{G}



(b) Basic SG G



(c) Enhanced SG G'

- Directed SG: contains all directional information
- Basic SG: bidirectional secrecy
- Enhanced SG: secrecy can exist in logical OR fashion

Intrinsically Secure Graphs

- Pinto et al brought information theoretic secrecy into the network domain through the notion of the “intrinsically secure graph (iS-graph)”.

- ✓ The secrecy capacity (rate) of the Gaussian wire-tap channel is

$$\mathcal{R}_s = \left[\log_2 \left(1 + \frac{P_\ell \cdot |h_\ell|^2}{\sigma_\ell^2} \right) - \log_2 \left(1 + \frac{P_\ell \cdot |h_e|^2}{\sigma_e^2} \right) \right]^+$$

- ✓ Definition: Let $\Pi_\ell = \{x_i\}_{i=1}^\infty \subset \mathbb{R}^d$ denote the set of legitimate nodes and $\Pi_e = \{e_i\}_{i=1}^\infty \subset \mathbb{R}^d$ denote the set of eavesdroppers. The iS-graph is the directed graph $G = \{\Pi_\ell, \mathcal{E}\}$ with vertex set Π_ℓ and edge set

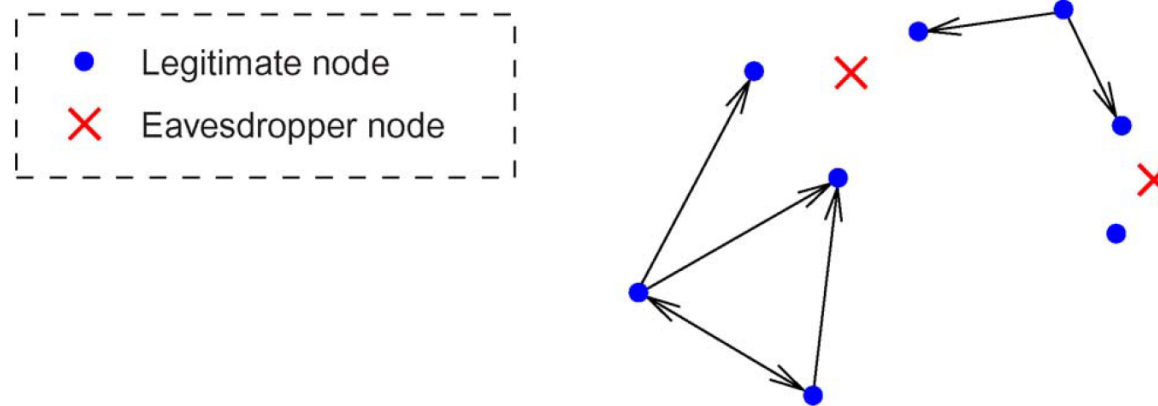
$$\mathcal{E} = \left\{ \overrightarrow{x_i x_j} : \mathcal{R}_s(x_i, x_j) > \varrho \right\}$$

where ϱ is a threshold representing the prescribed infimum secrecy rate for each communication link.

[Pinto, 2012]

Intrinsically Secure Graphs

- ✓ The iS-graph in two dimensional space



- ✓ The Poisson iS-graph is an iS-graph where $\Pi_\ell, \Pi_e \subset \mathbb{R}^d$ are mutually independent, homogeneous Poisson point processes with densities λ_ℓ and λ_e , respectively.
- ✓ **In-isolation:** A typical node $x_i \in \Pi_\ell \cap \mathcal{R}$ cannot receive from any node $x_j \in \Pi_\ell \cap \mathcal{R}$ ($x_j \neq x_i$) with positive secrecy rate
- ✓ **Out-isolation:** A typical node $x_i \in \Pi_\ell \cap \mathcal{R}$ cannot transmit to any node $x_j \in \Pi_\ell \cap \mathcal{R}$ ($x_j \neq x_i$) with positive secrecy rate

[Pinto, 2012]

Intrinsically Secure Graphs

- **Full Out and In Connectivity in the Poisson iS-Graph**

- ✓ **Full out connectivity:** A legitimate node $x_i \in \Pi_\ell \cap \mathcal{R}$ is fully out-connected with respect to a region \mathcal{R} if in the iS-graph there exists a directed path from x_i to every node $x_j \in \Pi_\ell \cap \mathcal{R}$ for $x_j \neq x_i$.

$$p_{\text{out-con}} \leq \mathbb{P}\{\text{no in-isolated nodes in } \mathcal{R}\}$$

- ✓ **Full in connectivity:** A legitimate node $x_i \in \Pi_\ell \cap \mathcal{R}$ is fully in-connected with respect to a region \mathcal{R} if in the iS-graph there exists a directed path to x_i from every node $x_j \in \Pi_\ell \cap \mathcal{R}$ for $x_j \neq x_i$.

$$p_{\text{in-con}} \leq \mathbb{P}\{\text{no out-isolated nodes in } \mathcal{R}\}$$

Intrinsically Secure Graphs: Recent Results

- **What is full secrecy connectivity?**
 - ✓ All nodes can communicate to each other, possibly through multiple hops, with a positive secrecy rate.
- **Why is full secrecy connectivity important?**
 - ✓ Full connectivity is a desirable feature for some scenarios, i.e., military networks and disaster relief.
 - ✓ It is a key condition that ensures certain high priority nodes in the network always remain connected.
- **Three types of full secrecy connectivity**
 - ✓ Full bidirectional secrecy connectivity
 - ✓ Full strong secrecy connectivity
 - ✓ Full weak secrecy connectivity

Intrinsically Secure Graphs: Recent Results

- **Three types of full secrecy connectivity**

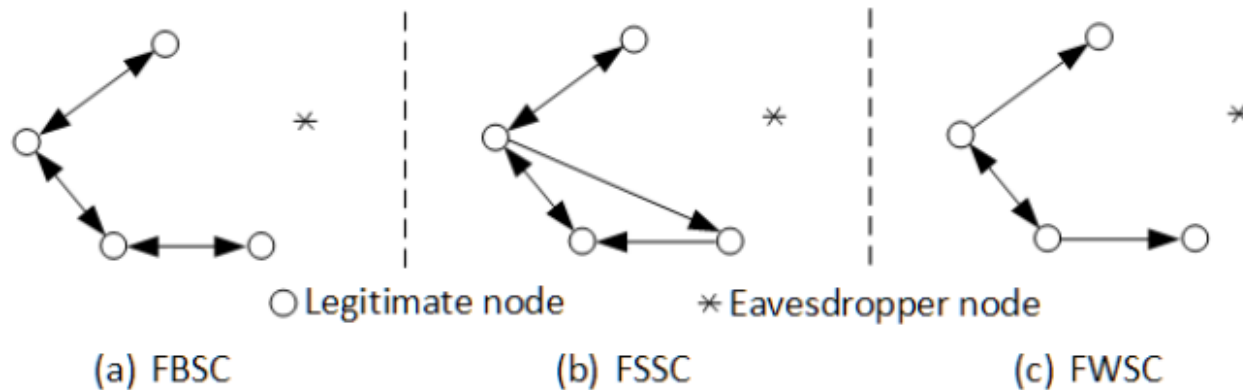


Fig. 1 Examples for the three types of full secrecy connectivity.

- ✓ **Full bidirectional secrecy connectivity (FBSC):** All nodes can communicate with each other through bi-directional links with a positive secrecy rate, possibly through multiple hops. (like Haenggi's "basic SG" model)
- ✓ **Full strong secrecy connectivity (FSSC):** All nodes can communicate with each other through directional links with a positive secrecy rate, possibly through multiple hops.
- ✓ **Full weak secrecy connectivity (FWSC):** All nodes can communicate with each other through either forward directional links or reverse directional links with a positive secrecy rate, possibly through multiple hops.

Refinement
of Haenggi's
enhanced SG

Intrinsically Secure Graphs: Recent Results

- **Full bidirectional secrecy connectivity:**

- ✓ Bidirectional secrecy connectivity

$$\begin{aligned}
 \mathcal{SC}_{ij} &= Pr(C_{ij} > z)Pr(C_{ji} > z) = \left(1 - Pr \left(\frac{|h_{ij}|^2}{\max_{e \in M} (|h_{ie}|^2)} < z \right) \right) \left(1 - Pr \left(\frac{|h_{ji}|^2}{\max_{e \in M} (|h_{je}|^2)} < z \right) \right) \\
 &= \sum_{l=1, k=1}^M \left(\frac{(-1)^{l-1}}{l!} \underbrace{\sum_{n_1} \sum_{n_2} \cdots \sum_{n_l} \frac{\lambda_{ij}}{\sum_{t=1}^l \lambda_{ie_{n_t}} z + \lambda_{ij}}}_{n_1 \neq n_2 \neq \cdots \neq n_l} \right) \left(\frac{(-1)^{k-1}}{k!} \underbrace{\sum_{n_1} \sum_{n_2} \cdots \sum_{n_k} \frac{\lambda_{ji}}{\sum_{t=1}^k \lambda_{je_{n_t}} z + \lambda_{ji}}}_{n_1 \neq n_2 \neq \cdots \neq n_k} \right)
 \end{aligned}$$

- ✓ At high node densities, the probability of full connectivity is simply the complement of the probability of an isolated node [4]. Therefore, we can obtain an upper bound for the overall probability of full bidirectional secrecy connectivity as:

$$P_{fbsc} \leq P_{fbsc}^{(u)} = 1 - \sum_{i=1}^N \prod_{j \neq i} (1 - \mathcal{SC}_{ij}).$$

Intrinsically Secure Graphs: Recent Results

- **Full strong secrecy connectivity:**

- ✓ The out-isolated and in-isolated probability for legitimate user x_i can be defined as:

$$P_{oi} = Pr \left(\frac{\max_{j \in N} (|h_{ij}|^2)}{\max_{e \in M} (|h_{ie}|^2)} < z \right) \quad \text{and} \quad P_{ii} = Pr \left(\max_{j \in N} \left(\frac{(|h_{ij}|^2)}{\max_{e \in M} (|h_{je}|^2)} \right) < z \right)$$

- ✓ The lower bound for full strong secrecy connectivity is the probability that every node is out-connected **and** in-connected,

$$P_{fssc} \geq P_{fssc}^{(l)} = \prod_{i \in M} ((1 - P_{oi})(1 - P_{ii}))$$

- **Full weak secrecy connectivity:**

- ✓ The lower bound for full weak secrecy connectivity is the probability that every node is out-connected **or** in-connected,

$$P_{fwsc} \geq P_{fwsc}^{(l)} = \prod_{i \in M} (1 - P_{oi}P_{ii})$$

Network Secrecy Enhancement

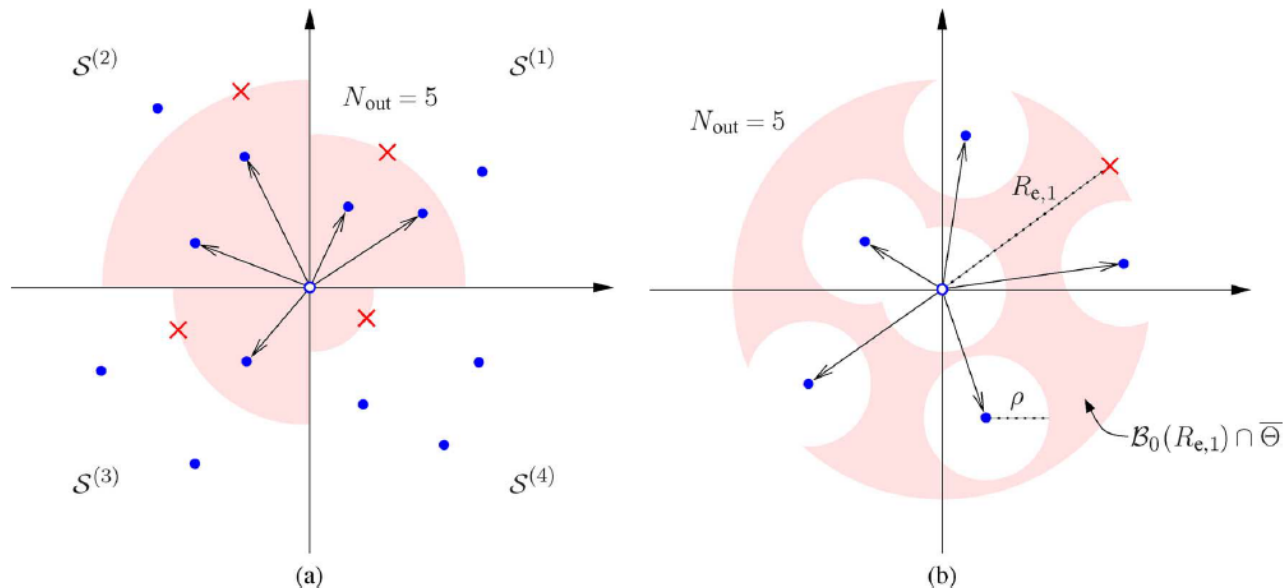
- **Secrecy Enhancement Techniques**

- ✓ Sectorized Transmission

- Each legitimate node transmits independently in multiple sectors of the plane (e.g., using directional antennas)

- ✓ Eavesdropper Neutralization

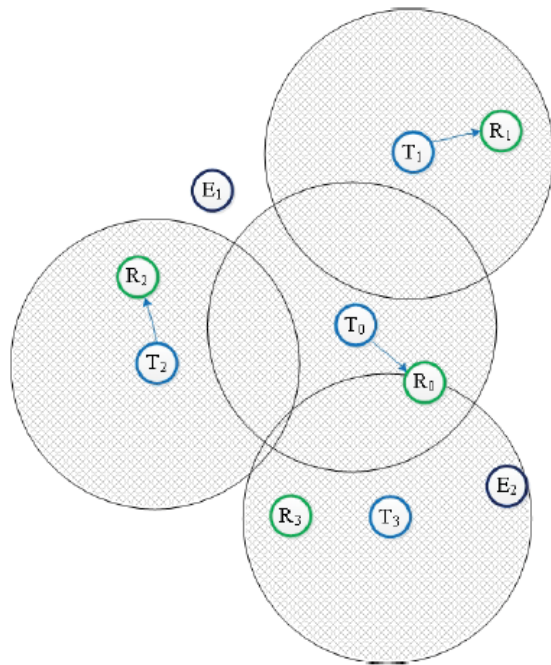
- Each legitimate node guarantees the absence of eavesdroppers in a surrounding region (e.g., by deactivating such eavesdroppers)



[PINTO, 2012]

Network Secrecy Enhancement

- ✓ Secrecy Guard Zone and Artificial Noise
 - Since unsecure transmission is mainly due to the presence of an eavesdropper close to the transmitter, the use of a secrecy guard zone for networks in which the legitimate transmitters are able to detect the existence of eavesdroppers in their vicinities has been considered

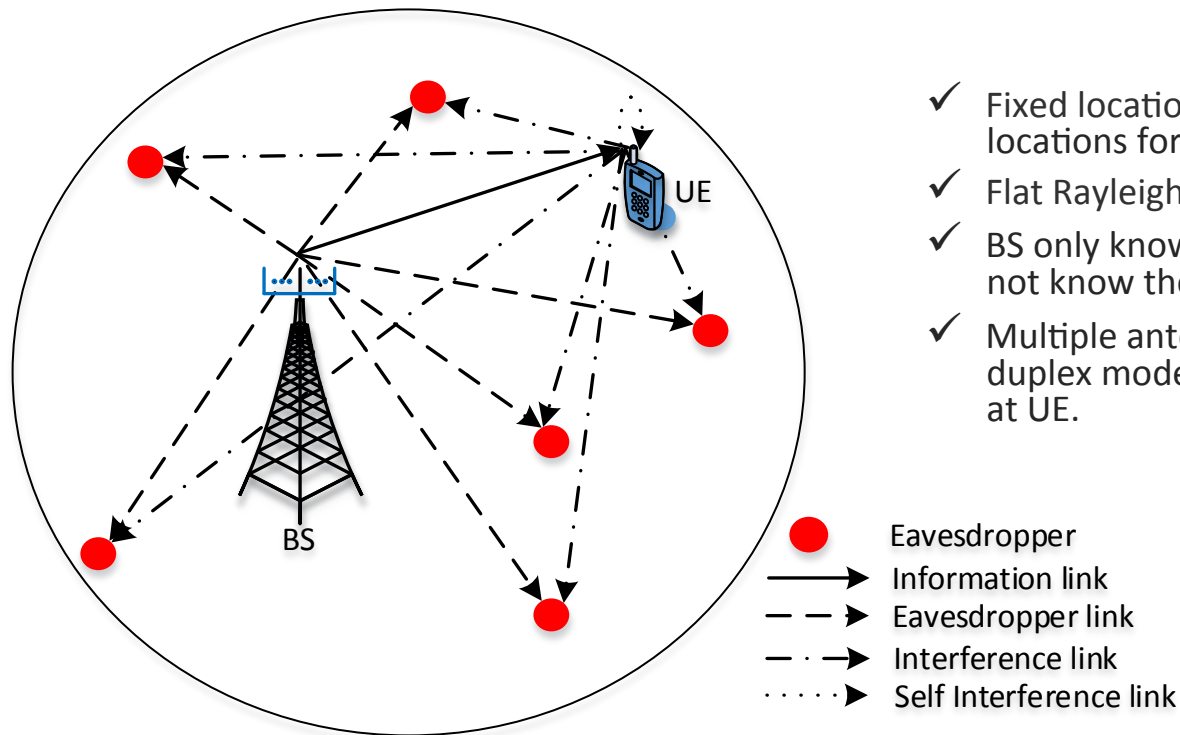


Snapshot of a part of a network with a secrecy guard zone around each transmitter. Transmitters T₀, T₁, and T₂ do not find any eavesdroppers inside their individual guard zone, and hence can transmit confidential messages to their intended receivers. However, transmitter T₃ detects an eavesdropper, E₂, inside its guard zone. If a non-cooperative protocol is used, T₃ remains silent. If a cooperative protocol is used, T₃ transmits artificial noise.

[Zhou, 2011]

Network Security Enhancement: Worked Example 1

- ✓ Transmit Antenna Selection (TAS) & Full Duplex (FD) UE

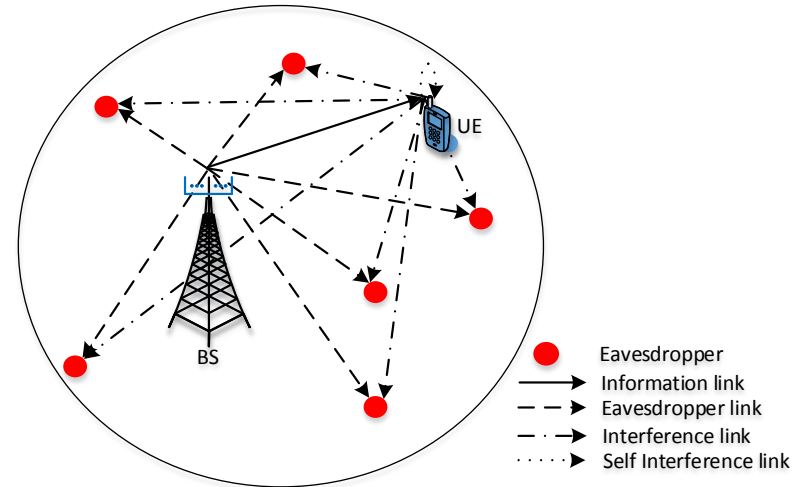


- ✓ Fixed location for BS and UE, random locations for eavesdroppers in a disc.
- ✓ Flat Rayleigh fading channel.
- ✓ BS only knows the CSI of the UE, does not know the CSI for eavesdroppers.
- ✓ Multiple antennas at BS with half duplex mode and full duplex antenna at UE.

Fig: The system model for fixed BS and UE with randomly located eavesdroppers.

We will analyze the secrecy outage probability for this model...

Secrecy Outage Analysis: TAS with HD/FD UE



- Secrecy Outage Definition

✓ After TAS, the end-to-end SNR at the UE and the worst ED can be written as:

$$\gamma_{BU} = \frac{P_B \max_{k \in \{1 \dots K\}} \left(\frac{|h_{B_k U}|^2}{d_{BU}^\alpha} \right)}{\varpi P_U |g_{UU}|^2 + \sigma_n^2} \quad \gamma_{BE_*} = \mathcal{F} \left(\frac{\frac{P_B |h_{B_* E_e}|^2}{d_{BE_e}^\alpha}}{\varpi \frac{P_U |h_{UE_e}|^2}{d_{UE_e}^\alpha} + \sigma_n^2} \right)$$

where $\varpi = 0$ for HD UE, $\varpi = 1$ for FD UE, and

$$\mathcal{F}(\cdot) = \max_{e \in \Phi}(\cdot) \text{ for independent EDs and } \mathcal{F}(\cdot) = \sum_{e \in \Phi}(\cdot) \text{ for colluding EDs}$$

✓ Probability of secrecy outage is well approximated by

$$P_{so} = \mathbb{P}([C_{BU} - C_{BE_*}]^+ < \epsilon) \simeq \mathbb{P} \left(\frac{\gamma_{BU}}{\gamma_{BE_*}} < \beta \right)$$

Outage: HD UE, No Collusion

Proposition 1: The downlink secrecy outage probability for an HD UE is given by

$$P_{so}^{(H)} = 1 - \sum_{k=0}^K (-1)^{k+1} C_K^k \frac{\sqrt{pq}}{2^{\frac{p+2q-3}{2}} \pi^{\frac{p+2q}{2} - 1}} \times G_{0,p+2q}^{p+2q,0} \left(\frac{a_k^{2q} b^p}{p^p 4^q q^{2q}} \mid 0, \frac{1}{p}, \dots, \frac{p-1}{p}, \frac{1}{2q}, \frac{2}{2q}, \dots, 1 \right)$$

where $G_{s,t}^{m,n} \left(z \mid \begin{matrix} u_1, \dots, u_s \\ v_1, \dots, v_t \end{matrix} \right)$ is the Meijer G function, $C_K^k = K!/((K-k)!k!)$ is the binomial coefficient, $a_k = kd_{BU}^\alpha$, $b = \pi\rho_E\Gamma(1+2/\alpha)\beta^{2/\alpha}$, $p, q \in \mathbb{Z}^+$ so that $\alpha = p/q$ is a positive rational number, and $\Gamma(x) = \int_0^\infty t^{x-1} e^{-t} dt$ is the standard gamma function.

Outage: HD UE, No Collusion (Proof)

Calculate PDF of
BS-UE SNR
(all channels are i.i.d.)

$$F_{\gamma_{BU}}(x) = \left(1 - e^{-x d_{BU}^\alpha}\right)^K = \sum_{k=0}^K C_K^k (-1)^k e^{-k x d_{BU}^\alpha},$$

$$f_{\gamma_{BU}}(x) = \sum_{k=0}^K C_K^k (-1)^{k+1} k d_{BU}^\alpha e^{-k x d_{BU}^\alpha},$$

Calculate CDF of
BS-ED SNR (worst case)

- Condition on ED distances and invoke independence
- Probability generating functional for PPPs
- Integrate (incomplete gamma function)
- Large R asymptotics for upper incomplete gamma function

$$F_{\gamma_{BE^*}}(y) = \mathbb{P} \left(\max_{e \in \Phi} \left(\frac{|h_{B^*E_e}|^2}{d_{BE_e}^\alpha} \right) < y \right)$$

$$\stackrel{(a)}{=} E_\Phi \left[\prod_{e \in \Phi} \mathbb{P} (|h_{B^*E_e}|^2 < y d_{BE_e}^\alpha \mid \Phi) \right]$$

$$= E_\Phi \left[\prod_{e \in \Phi} \left(1 - e^{-y d_{BE_e}^\alpha} \right) \right]$$

$$\stackrel{(b)}{=} \exp \left(-\rho_E \int_0^{2\pi} \int_0^R r \left(e^{-y r^\alpha} \right) dr d\theta \right)$$

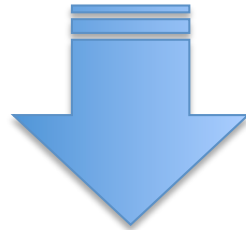
$$\stackrel{(c)}{=} \exp \left(-\frac{2\pi\rho_E}{\alpha y^{\frac{2}{\alpha}}} \left(\Gamma \left(\frac{2}{\alpha} \right) - \Gamma \left(\frac{2}{\alpha}, y R^\alpha \right) \right) \right)$$

$$\stackrel{(d)}{\simeq} \exp \left(-\frac{2\pi\rho_E}{\alpha y^{\frac{2}{\alpha}}} \Gamma \left(\frac{2}{\alpha} \right) \right) \left(1 + O(R^{2-\alpha} e^{-y R^\alpha}) \right)$$

Outage: HD UE, No Collusion (Proof)

Rearrange outage expression and substitute

$$P_{so} = \mathbb{P}([C_{BU} - C_{BE_*}]^+ < \epsilon) \simeq \mathbb{P}\left(\frac{\gamma_{BU}}{\gamma_{BE_*}} < \beta\right)$$



$$\begin{aligned} P_{so}^{(H)} &= 1 - \int_0^\infty f_{\gamma_{BU}}(x) F_{\gamma_{BE_*}}\left(\frac{x}{\beta}\right) dx \\ &= 1 - \sum_{k=0}^K C_K^k (-1)^{k+1} k d_{BU}^\alpha \int_0^\infty e^{-kx d_{BU}^\alpha} e^{-\frac{2\pi\rho_E}{\alpha\left(\frac{x}{\beta}\right)^{2/\alpha}} \Gamma\left(\frac{2}{\alpha}\right)} dx \end{aligned}$$

Outage: HD UE, No Collusion (Proof)

To evaluate...

$$\int_0^{\infty} e^{-kx d_{BU}^{\alpha}} e^{-\frac{2\pi\rho_E}{\alpha} \left(\frac{x}{\beta}\right)^{2/\alpha} \Gamma\left(\frac{2}{\alpha}\right)} dx$$

we will need the Mellin convolution property...

$$\int_0^{\infty} K(x/y)f(y)dy/y \longleftrightarrow K(s)F(s)$$

Consider the integral...

$$I = \int_0^{\infty} e^{-ax} e^{-\frac{b}{x^c}} dx = \int_0^{\infty} u e^{-au} e^{-\left(\frac{b^{1/c}}{x}\right)^c} \frac{du}{u}$$

with $a = kd_{BU}^{\alpha}$, $b = \frac{2\pi\rho_E}{\alpha} \Gamma\left(\frac{2q}{p}\right) \beta^{2q/p}$ and $c = 2q/p$

Outage: HD UE, No Collusion (Proof)

The Mellin transform of the integral is...

$$\mathcal{M}[I; s] = \frac{p}{2qa^{s+1}} \Gamma\left(\frac{ps}{2q}\right) \Gamma(1+s)$$

and the inverse is...

$$\begin{aligned} I &= \frac{p}{2\pi ia} \int_{u-i\infty}^{u+i\infty} \Gamma(ps) \Gamma\left(2q\left(s + \frac{1}{2q}\right)\right) (a^{2q}b^p)^{-s} ds \\ &\stackrel{(a)}{=} \frac{\sqrt{pq}}{a2^{\frac{p+2q-3}{2}} \pi^{\frac{p+2q}{2}-1}} \frac{1}{2\pi i} \\ &\times \int_{u-i\infty}^{u+i\infty} \left(\frac{a^{2q}b^p}{p^p 4^q q^{2q}}\right)^{-s} \prod_{n=0}^{p-1} \Gamma\left(s + \frac{n}{p}\right) \prod_{n=0}^{2q-1} \Gamma\left(s + \frac{1+n}{2q}\right) ds \\ &= \frac{\sqrt{pq}}{a2^{\frac{p+2q-3}{2}} \pi^{\frac{p+2q}{2}-1}} \\ &\times G_{0,p+2q}^{p+2q,0} \left(\frac{a^{2q}b^p}{p^p 4^q q^{2q}} \mid 0, \frac{1}{p}, \dots, \frac{p-1}{p}, \frac{1}{2q}, \frac{2}{2q}, \dots, 1 \right), \end{aligned}$$

$$\prod_{k=0}^{m-1} \Gamma\left(z + \frac{k}{m}\right) = (2\pi)^{\frac{m-1}{2}} m^{\frac{1}{2}-mz} \Gamma(mz)$$

Outage Scaling: HD UE, No Collusion

Scaling for large numbers of antennas...

Lemma 2: The downlink secrecy outage probability for an HD UE located in the presence of independently acting EDs is lower bounded by

$$P_{so}^{(H)} > \frac{\pi \rho_E d_{BU}^2 \beta^{2/\alpha} \Gamma(1 + 2/\alpha)}{e (\ln K)^{2/\alpha}} \left(1 + O\left(\frac{1}{(\ln K)^{2/\alpha}}\right) \right)$$

as $K \rightarrow \infty$.

Outage Scaling: FD UE, No Collusion

Proposition 3: The downlink secrecy outage probability for an FD UE located in the presence of independently acting EDs is upper bounded by

$$P_{so}^{(F)} \leq 1 - e^{-\rho_E \pi R^2} \sum_{k=1}^K (-1)^{k+1} k C_K^k \int_0^\infty \frac{\frac{P_U}{d_{BU}^\alpha} (1 + \lambda_{UU}) + kx \lambda_{UU}}{(\frac{P_U}{d_{BU}^\alpha} + kx \lambda_{UU})^2} \exp\left(\rho_E R^2 \Psi\left(\frac{x}{\beta}; \alpha, \frac{d_{BU}}{R}\right) - \frac{k d_{BU}^\alpha}{P_U} x\right) dx$$

where

$$\Psi(y; \alpha, \delta) = \int_0^{2\pi} \int_0^1 \frac{yz^{\alpha+1}}{yz^\alpha + (z^2 + \delta^2 - 2z\delta \cos \theta)^{\alpha/2}} dz d\theta$$

and $\lambda_{UU} = \mathbb{E}[|g_{UU}|^2]$ is the average gain of the self-interference channel at the FD UE.

Outage Scaling: FD UE, No Collusion

- Proposition 3 does not admit a closed form
- Occasionally, we might get lucky with closed-form calculations for certain system parameters
 - In practice, try path loss exponents of 2 and 4
 - Consider “pathological” or limiting cases
 - Expand about given points, e.g., UE position is at the cell edge
- For a path loss exponent of 2, the double integral reduces to

$$\Psi(y; 2, \delta) = \frac{\pi y}{(y+1)^3} \left((y+1)(\psi(y, \delta) - \delta^2) + \delta^2(y-1) \ln \left(\frac{2\delta^2 y}{\delta^2(y-1) + (y+1)(\psi(y, \delta) + y + 1)} \right) \right)$$

where

$$\psi(y, \delta) = \sqrt{\delta^4 + 2\delta^2(y-1) + (y+1)^2}.$$

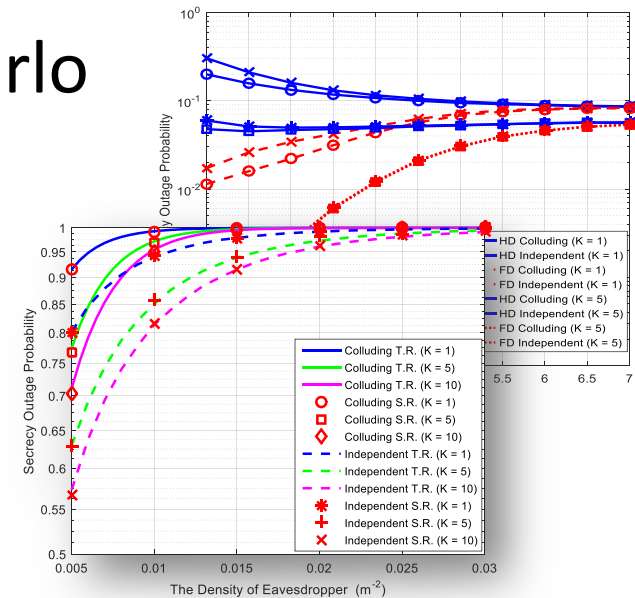
Secrecy Outage Analysis: Theory vs Simulation

- We can easily construct Monte Carlo simulations

- Fix the BS and the UE and generate random positions of eavesdroppers
- Generate random fading variates
- Test each link (roll the dice)
- Log the results
- MATLAB is particularly useful and efficient

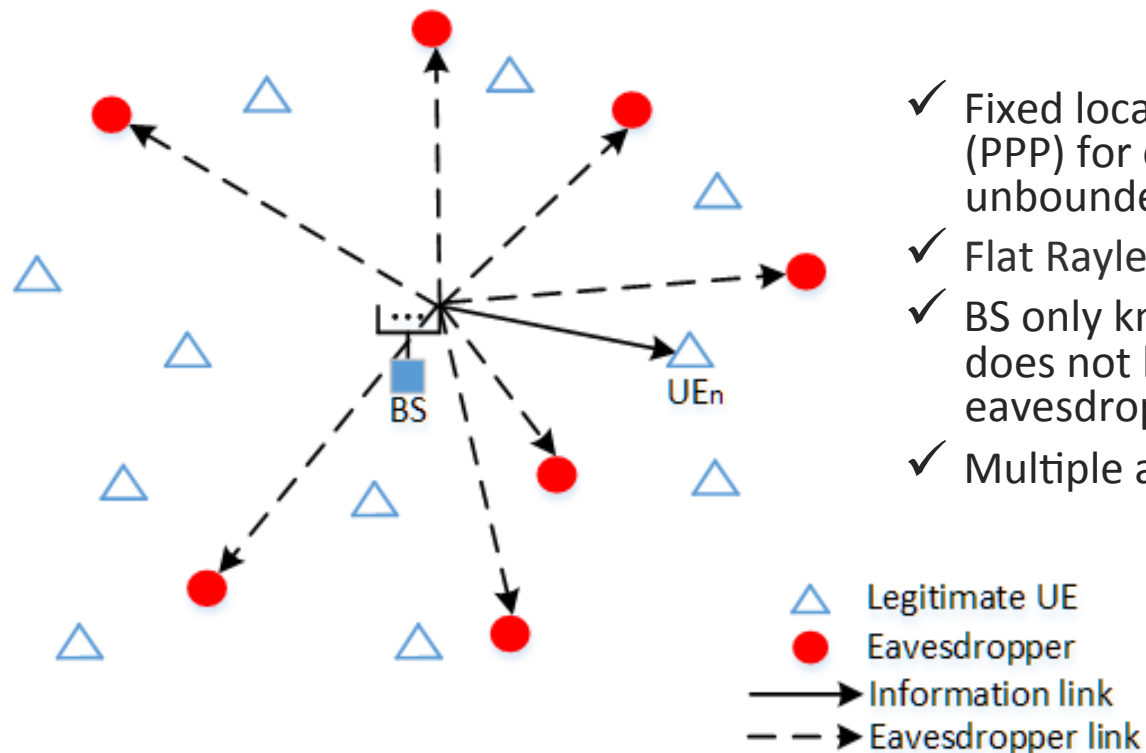
- Results are printed in your notes

- Notice that theory is a good predictor of simulation/reality
- System is more difficult to simulate since eavesdropper behaviour is unknown



Network Secrecy Enhancement: Worked Example 2

- ✓ Transmit Antenna Selection (TAS) & UE Ordering



- ✓ Fixed location for BS, random location (PPP) for eavesdroppers and UEs in an unbounded two dimensional space.
- ✓ Flat Rayleigh fading channel.
- ✓ BS only knows the CSI of the UEs, does not know the CSI for eavesdroppers.
- ✓ Multiple antennas at the BS with TAS.

Fig. 8 The system model for a spatially random wireless network.

Secrecy Outage Analysis: TAS with UE Ordering

- **Two Ordering Policies**

- ✓ Policy I: Based on distance

- Order the UE by using the distance (d_{BU}) between the UE and the BS
- If CSI cannot be estimated accurately, we can use this approach.

- ✓ Policy II: Based on distance and fading

- Order the UE by using the combination of distance and fading ($\frac{|h_{B_*U}|^2}{d_{BU}^\alpha}$) between the UE and the BS, where

$$B_* = \arg \max_{i \in (1 \dots K)} (|h_{B_i U_n}|^2)$$

- If the CSI can be estimated accurately, we can (hopefully) obtain an improved secrecy performance relative to the distance-based policy noted above.

Secrecy Outage Analysis: TAS with UE Ordering

- **Two Ordering Policies**

- ✓ Policy I: Based on distance

- Order the UE by using the distance (d_{BU}) between the UE and the BS
- If CSI cannot be estimated accurately, we can use this approach.

- ✓ Policy II: Based on distance and fading

- Order the UE by using the combination of distance and fading ($\frac{|h_{B_*U}|^2}{d_{BU}^\alpha}$) between the UE and the BS, where

$$B_* = \arg \max_{i \in (1 \dots K)} (|h_{B_i U_n}|^2)$$

- If the CSI can be estimated accurately, we can (hopefully) obtain an improved secrecy performance relative to the distance-based policy noted above.

An Aside: The Mapping Theorem

Mapping Theorem

Let Φ be a PPP on \mathbb{R}^d with intensity function λ . Furthermore, let $f: \mathbb{R}^d \rightarrow \mathbb{R}^s$ be a measurable mapping such that f does not shrink a compact set to a point. Define the measure

$$\mu(B) = \Lambda(f^{-1}(B)) = \int_{f^{-1}(B)} \lambda(x) dx < \infty$$

for all compact sets B . Then

$$f(\Phi) = \bigcup_{x \in \Phi} f(x)$$

is a PPP with intensity measure μ .

Mapping Theorem: Examples

Linear mapping

Suppose Φ is a PPP on \mathbb{R}^d with intensity function λ , and let A denote a non-singular linear mapping from \mathbb{R}^d to \mathbb{R}^d , i.e., A is a $d \times d$ real non-singular matrix. Then $A(\Phi) = \{Ax: x \in \Phi\}$ is a PPP with intensity $\lambda \det(A^{-1})$.

Distance mapping

What is the intensity function of $\Phi' = \{\|x_i\|\}$, (i.e., we map from x_i to $\|x_i\|$)? For the mapping $f(x) = \|x\|$, we have that $f^{-1}(B) = b(o, r)$ for the set $B = [0, r)$. Hence,

$$\mu([0, r)) = \Lambda(b(o, r)) = \int_{b(o, r)} \lambda \, dx = \lambda \pi r^2$$

and thus the new intensity function is the derivative

$$\lambda'(x) = 2\lambda\pi x, \quad x \geq 0.$$

Secrecy Outage Analysis: Policy II

- ✓ First, we let $x_n = \frac{d_{BU_n}^\alpha}{\max_{i \in (1 \dots K)} (|h_{B_i U_n}|^2)}$ and define the intensity of the set $\Psi = \{x_n, n \in \mathbb{N}\}$ as ρ_Ψ . The intensity function of Ψ can be written as

$$\rho_\Psi(\psi) = \sum_{l=0}^{K-1} C_K^l (-1)^l \frac{2\pi\rho_U K \psi^{\frac{2}{\alpha}-1} \Gamma(\frac{2}{\alpha} + 1)}{\alpha(l+1)^{\frac{2}{\alpha}+1}}$$

- ✓ The PDF of x_n under the Rayleigh fading can be obtained as:

$$f_{x_n}(x) = \frac{2(A_u \psi^{\frac{2}{\alpha}})^n e^{-A_u \psi^{\frac{2}{\alpha}}}}{\alpha \psi \Gamma(n)},$$

where $A_u = \sum_{l=0}^{K-1} C_K^l (-1)^l \frac{\pi\rho_U K \Gamma(\frac{2}{\alpha}+1)}{(l+1)^{\frac{2}{\alpha}+1}}$ and the CDF of the reciprocal of x_n is

$$F_{\frac{1}{x_n}}(x) = 1 - \int_0^x \frac{2(A_u \psi^{\frac{2}{\alpha}})^n e^{-A_u \psi^{\frac{2}{\alpha}}}}{\alpha \psi \Gamma(n)} d\psi = \frac{\Gamma(n, A_u x^{\frac{2}{\alpha}})}{\Gamma(n)}$$

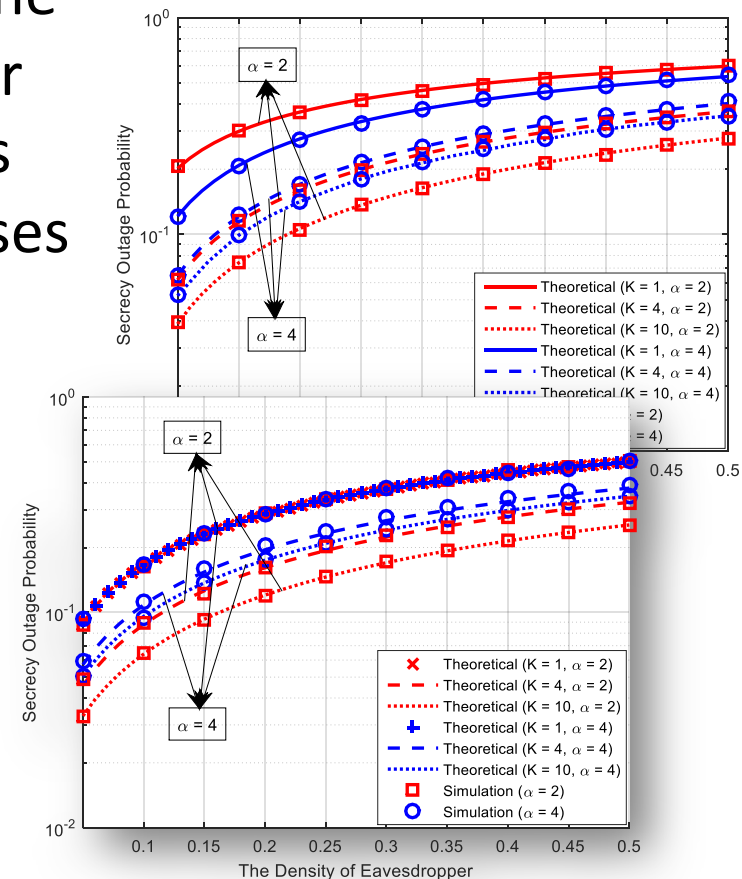
- ✓ Finally, the secrecy outage probability for the n th UE can be derived as

$$\begin{aligned} P_{so}^{(II)}(\beta) &= \mathbb{P}\left(\frac{\gamma_{BU}}{\gamma_{BE_*}} < \beta\right) \\ &= 1 - \int_0^\infty F_{\frac{1}{x_n}}(\beta y) f_{\gamma_{BE_*}}(y) dy \\ &= 1 - \left(\frac{A_u \beta^{-\frac{2}{\alpha}}}{A_u \beta^{-\frac{2}{\alpha}} + A_e}\right)^n \end{aligned}$$

Displacement
and mapping
theorems

Secrecy Outage Analysis: Theory vs Simulation

- Again, results are printed in your notes
 - For wireless enthusiasts, note the relative behaviour of outage for different path loss exponents as the number of antennas increases
- Being able to predict system performance in wireless networks is very important, particularly as the complexity of the network grows (system-level simulation becomes problematic)

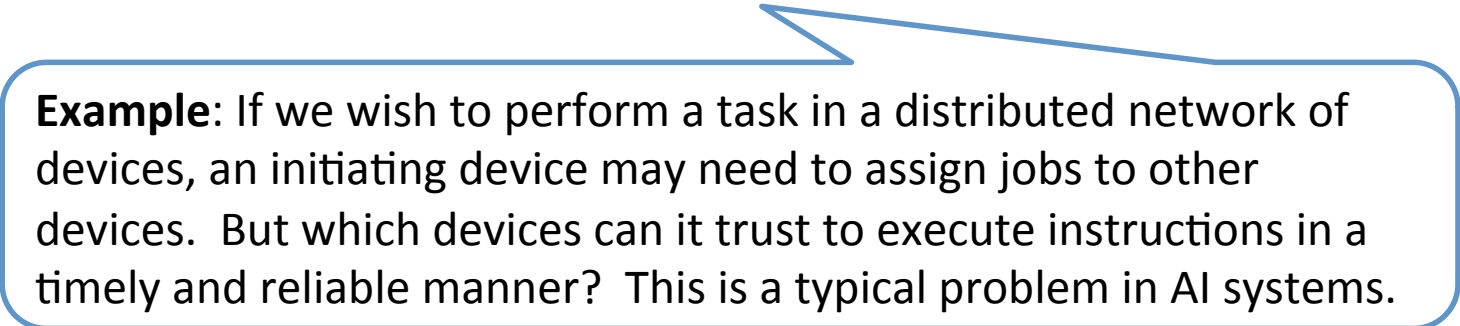


Literature (Other Results)

- Ad hoc networks with pairwise transmissions, transmission capacity [**Zhou, 2011**]
- Beamforming and artificial noise in a Poisson field of eavesdroppers [**Ghogho, 2011**]
- Broadcast channels, linear beamforming to ensure secrecy [**Geraci, 2014**]
- Colluding, noncolluding (independently acting) eavesdroppers [**Zheng, 2014**]
- Artificial noise enhanced transmission with optimal power allocation [**Zheng, 2015**]
- Antenna selection, full-duplex artificial noise [**Chen, 2016**]
- Antenna selection, user ordering [**Chen, 2016**]
- Secrecy in mm-wave networks [**Wang, 2016**]

From Secrecy to Trust

- Focus has been on intrinsic security through information theoretic secrecy so far
- Some applications require trust, not secrecy
 - Low security ad hoc networks
 - Multi-agent distributed systems

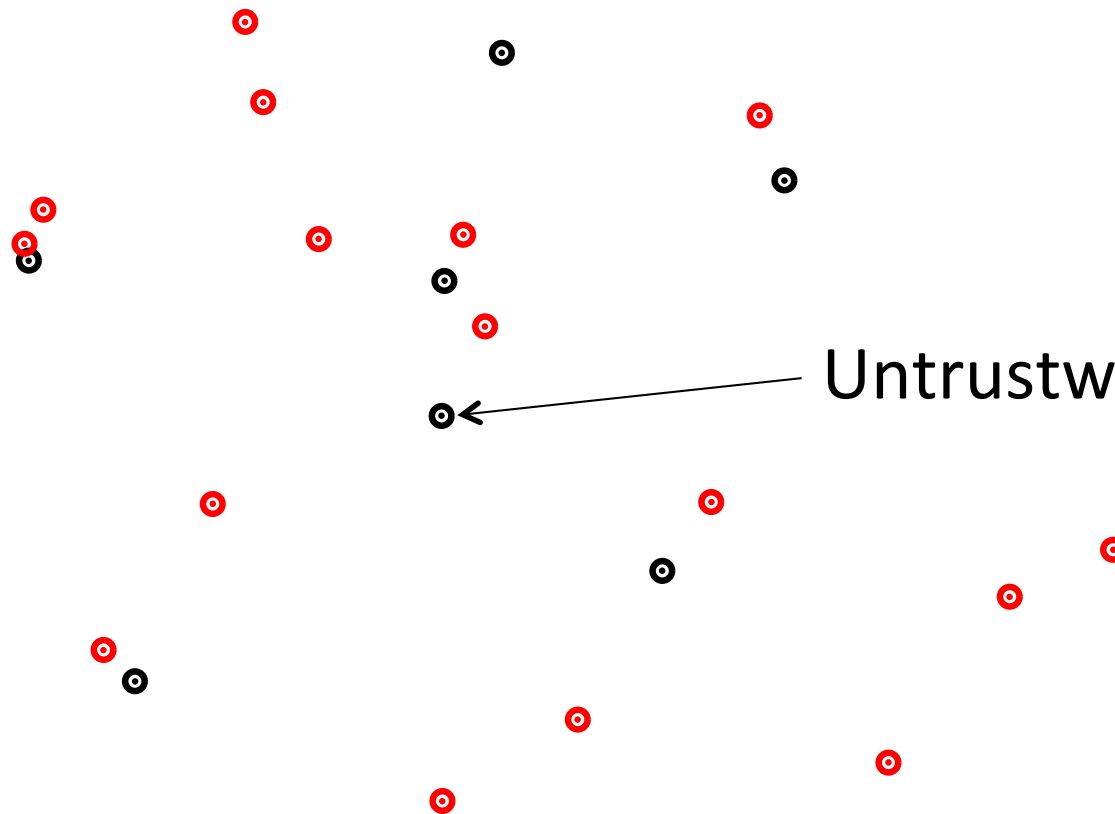


Example: If we wish to perform a task in a distributed network of devices, an initiating device may need to assign jobs to other devices. But which devices can it trust to execute instructions in a timely and reliable manner? This is a typical problem in AI systems.

We need a way to model trust in large-scale networks

Trusted Networks

Trustworthy set: A



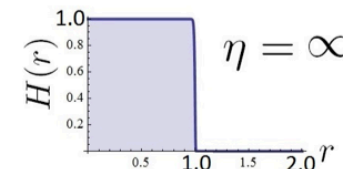
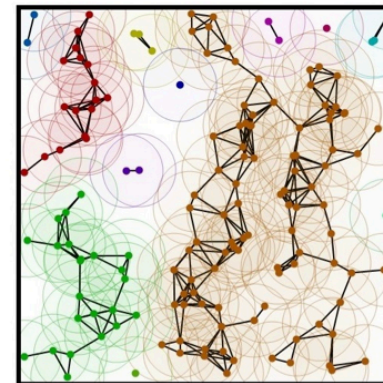
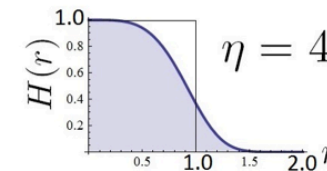
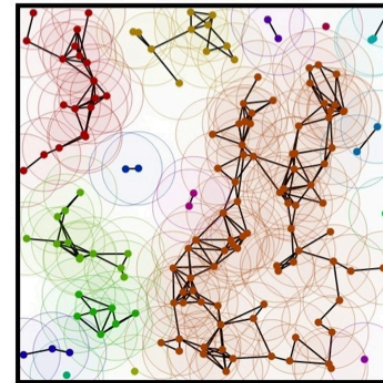
Untrustworthy set: B



Network Model

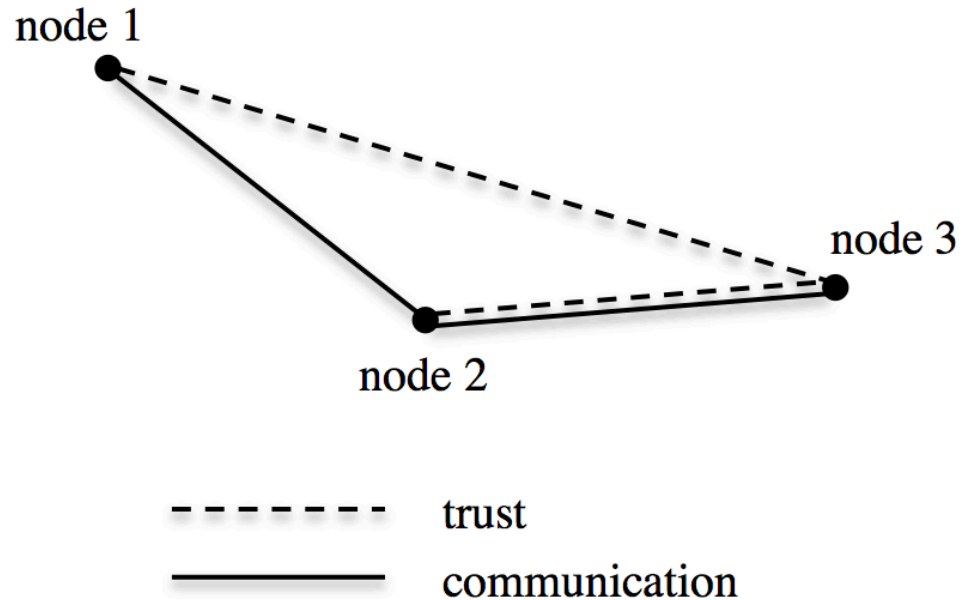
- Random geometric graph
- Pairwise connection: probabilistic vs. unit disk (Gilbert model)
- Boundaries accounted for

Focus: probability that a trusted network can be formed



Trust Model

- Trust is uncertain – probability of trust
- Pairwise trust can only be established if two nodes can communicate directly
- Proximity or experience based



Example: Beta Reputation System

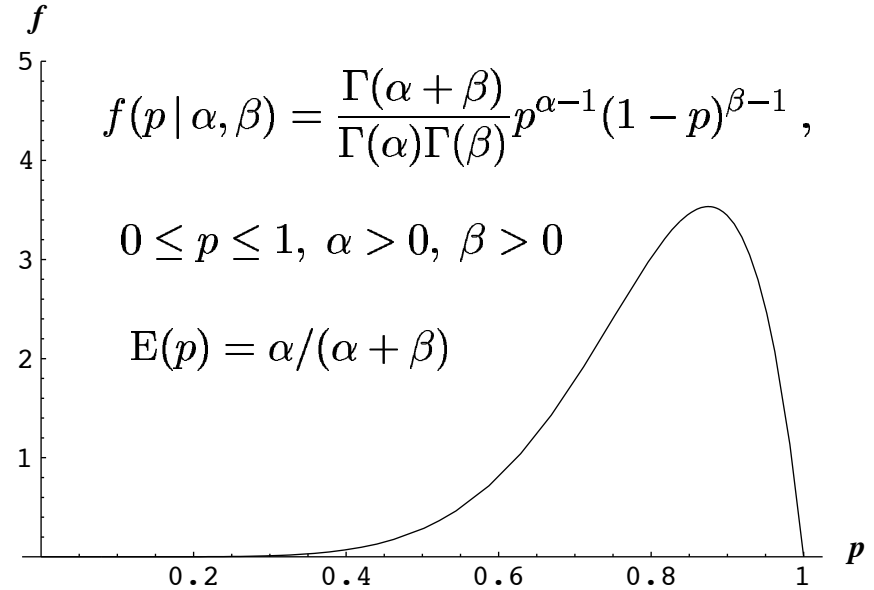
The Beta Reputation System

Audun Jøsang

Distributed Systems Technology Centre *
Queensland University of Technology, GPO Box 2434, Brisbane Qld 4001, Australia
tel:+61-7-3864 1051, fax:+61-7-3864 1282
email: ajosang@dstc.edu.au

Roslan Ismail

Information Security Research Centre
Queensland University of Technology, GPO Box 2434, Brisbane Qld 4001, Australia
tel:+61-7-3864 2575, fax:+61-7-3221 2384
email: r.ismail@student.qut.edu.au



Definition 1 (Reputation Function) Let r_T^X and s_T^X respectively represent the (collective) amount of positive and negative feedback about target entity T provided by an agent (or collection of agents) denoted by X , then the function $\varphi(p | r_T^X, s_T^X)$ defined by:

$$\varphi(p | r_T^X, s_T^X) = \frac{\Gamma(r_T^X + s_T^X + 2)}{\Gamma(r_T^X + 1)\Gamma(s_T^X + 1)} p^{r_T^X} (1-p)^{s_T^X}, \quad \text{where } 0 \leq p \leq 1, 0 \leq r_T^X, 0 \leq s_T^X. \quad (4)$$

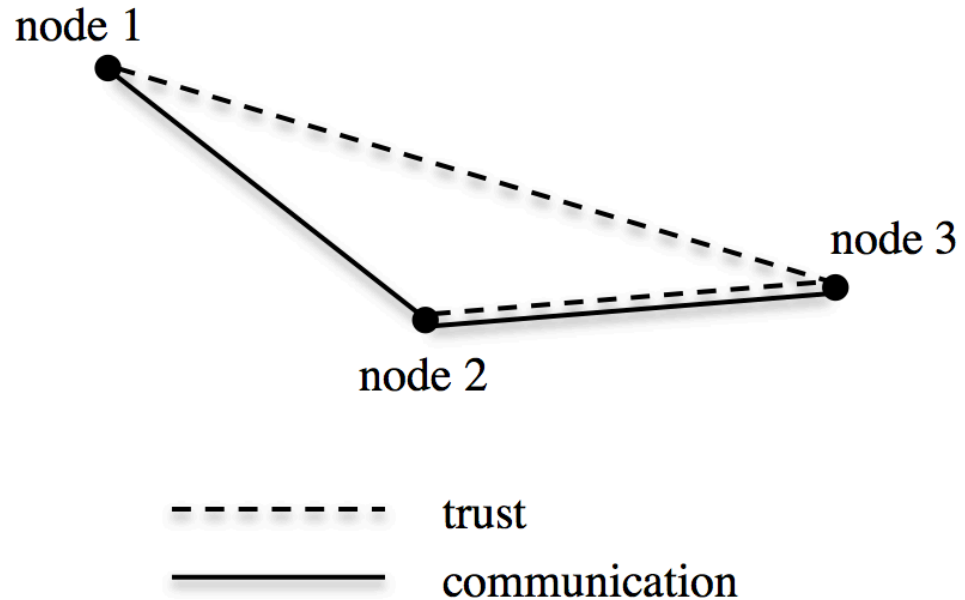
is called T 's reputation function by X . The tuple (r_T^X, s_T^X) will be called T 's reputation parameters by X . For simplicity and compactness of notation we will sometimes write φ_T^X instead of $\varphi(p | r_T^X, s_T^X)$.

By using Eq.(2) the probability expectation value of the reputation function can be expressed as:

$$E(\varphi(p | r_T^X, s_T^X)) = (r_T^X + 1) / (r_T^X + s_T^X + 2). \quad (5)$$

Trust Model

- Trust is uncertain – probability of trust
- Pairwise trust can only be established if two nodes can communicate directly
- Proximity or experience based

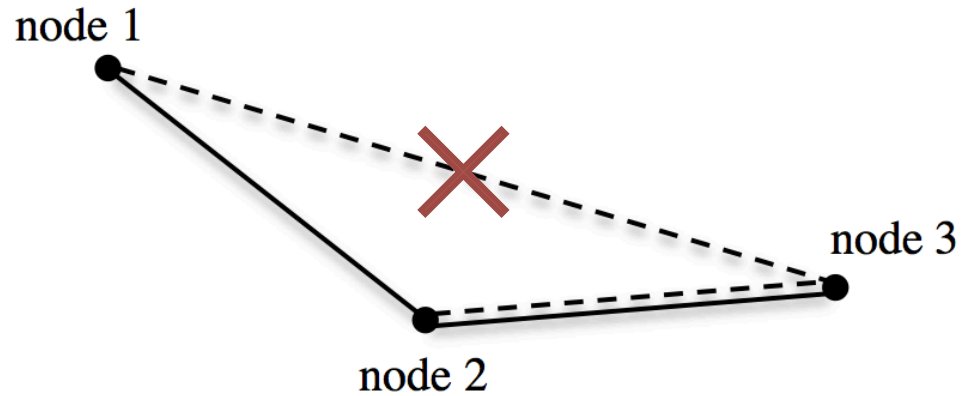


Trust Model

Assumption: Trust cannot be established without communication

$\{i \sim j\} \rightarrow \text{Trust}$

$\{i \leftrightarrow j\} \rightarrow \text{Communication}$



----- trust
 _____ communication

$$\mathbb{P}(i \sim j) = \mathbb{P}(i \sim j | i \leftrightarrow j) \mathbb{P}(i \leftrightarrow j) + \mathbb{P}(i \sim j | i \not\leftrightarrow j) \mathbb{P}(i \not\leftrightarrow j) = T_{ij} H_{ij} = \tau_{ij}$$

trust \nearrow
 \nwarrow communication

Proximity Based Trust

- Trust protocols in D2D networks could be proximity based
- Leading order in density of A
 - Implies A is connected; don't care about B
 - Simplifies to a study of the bridging probability
- Numbers of nodes in A and B are large
- Cluster expansion...

$$P_{t,\mathcal{A}}(\mathbf{a}_1, \dots, \mathbf{a}_{N_A}) = 1 - \sum_{g \in \mathcal{G}_{N_A-1}^A} \pi_g - \sum_{g \in \mathcal{G}_{N_A-2}^A} \pi_g - \dots$$

$$\pi_g = \prod_{(i,j) \in g} \tau_{ij} \prod_{(i,j) \notin g} (1 - \tau_{ij})$$

Proximity Based Trust

Probability that a trusted network is established in the presence of untrustworthy nodes (set B)...

$$P_t = \left\langle \left\langle P_{t,\mathcal{A}}(\mathbf{a}_1, \dots, \mathbf{a}_{N_A}) \prod_{j=1}^{N_B} \prod_{i=1}^{N_A} (1 - \tau(|\mathbf{a}_i - \mathbf{b}_j|)) \right\rangle_{\mathcal{A}} \right\rangle_{\mathcal{B}}$$

Bridging probability

If trustworthy set A is dense...

$$P_t \approx \left\langle \prod_{j=1}^{N_B} \left\langle \prod_{i=1}^{N_A} (1 - \tau_{ij}) \right\rangle_{\mathcal{A}} \right\rangle_{\mathcal{B}}$$

$$- \left\langle \left\langle \left(\sum_{p=1}^{N_A} \prod_{i \neq p} (1 - \tau_{ip}) \right) \left(\prod_{j=1}^{N_B} \prod_{i=1}^{N_A} (1 - \tau_{ij}) \right) \right\rangle_{\mathcal{A}} \right\rangle_{\mathcal{B}}$$

Proximity Based Trust

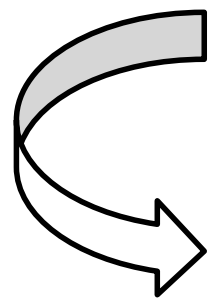
Leading order probability of trusted connectivity

$$\begin{aligned}
 P_t^{(1)} &= \left\langle \prod_{j=1}^{N_B} \left\langle \prod_{i=1}^{N_A} (1 - \tau_{ij}) \right\rangle_{\mathcal{A}} \right\rangle_{\mathcal{B}} \\
 &= \left\langle \prod_{j=1}^{N_B} \left(1 - \frac{\rho_A}{N_A} \int_{\mathcal{V}} \tau(|\mathbf{a} - \mathbf{b}_j|) d\mathbf{a} \right)^{N_A} \right\rangle_{\mathcal{B}} \\
 &= \left(\frac{1}{V} \int_{\mathcal{V}} e^{-\rho_A \int_{\mathcal{V}} \tau(|\mathbf{a} - \mathbf{b}|) d\mathbf{a}} (1 + O(1/N_A)) d\mathbf{b} \right)^{N_B}
 \end{aligned}$$

density of set A
no. nodes in set A

Proximity Based Trust

A well designed trust protocol will ensure that


$$\tau_{ij} \ll 1, \quad i \in \mathcal{A} \text{ and } j \in \mathcal{B}$$
$$T(r_{ij}) \ll \frac{1}{\rho_A H(r_{ij})}, \quad r_{ij} \geq 0$$

- Links trust protocol to density of network A and physical communication
- Valid irrespective of size of set B

Proximity Based Trust

If the trust bridging probability is small, we can approximate (to first order)...

$$P_t^{(1)} \approx \left(1 - \frac{\rho_A \rho_B M[\tau]}{N_B} \right)^{N_B} \approx e^{-\rho_A \rho_B M[\tau]}$$

$$M[\tau] = \int_{\mathcal{V}^2} \tau(|\mathbf{a} - \mathbf{b}|) \, d\mathbf{a} \, d\mathbf{b}$$

Exponential approximation valid for large $|B|$, small(ish) density of set B , and small bridging probability

Proximity Based Trust

The power of pair distance...

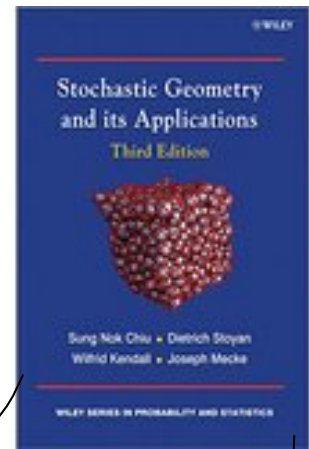
Transform integrals using pair distance to obtain

$$M[\tau] = \frac{2\pi^{d/2}}{\Gamma(d/2)} \int_0^D r^{d-1} \gamma_{\mathcal{V}}(r) \tau(r) dr$$

If τ is small for $r \gg 0$ (and the bounding region is convex), we have

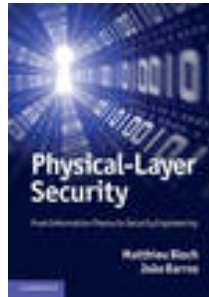
$$M[\tau] = \frac{\pi^{d/2} T(0) V}{\Gamma(\frac{d}{2} + 1)} r_0^d + O(r_0^{d+1})$$

Links the dimension of the network d , the volume of the confining geometry V , and the trust protocol

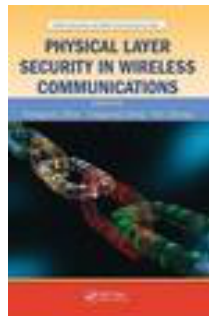


Chiu et al

Books



Bloch, Matthieu, and Joao Barros. *Physical-layer security: from information theory to security engineering*. Cambridge University Press, 2011.



Zhou, Xiangyun, Lingyang Song, and Yan Zhang, eds. *Physical Layer Security in Wireless Communications*. Crc Press, 2013.



Zou, Yulong, and Jia Zhu. *Physical-Layer Security for Cooperative Relay Networks*. Springer, 2016.

References

- [1] A. D. Wyner, “The wire-tap channel,” *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Jan. 1975.
- [2] I. Csiszar and J. Korner, “Broadcast channels with confidential messages,” *IEEE Trans. Inform. Theory*, pp. 339-348, May 1978.
- [3] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjørungnes, “On the throughput cost of physical layer security in decentralized wireless networks,” *IEEE Trans. Wireless Commun.*, vol. 10, pp. 2764–2775, Aug. 2011.
- [4] P. C. Pinto, J. Barros, and M. Z. Win, “Secure communication in stochastic wireless networks-part I: Connectivity,” *IEEE Trans. Inf. Forensics and Security*, vol. 7, pp. 125–138, Feb. 2012.
- [5] P. C. Pinto, J. Barros, and M. Z. Win, “Secure communication in stochastic wireless networks-part II: Maximum rate and collusion,” *IEEE Trans. Inf. Forensics and Security*, vol. 7, pp. 139–147, Feb 2012.
- [6] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, “Joint relay and jammer selection for secure two-way relay networks,” *IEEE Trans. Inf. Forens. Security*, vol. 7, no. 1, pp. 310-320, Feb. 2012
- [7] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, “Principles of physical layer security in multiuser wireless networks: A survey,” *IEEE Commun. Surveys Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.
- [8] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, “Physical layer network security in the full-duplex relay system,” *IEEE Trans. Inform. Forensics and Security*, vol. 10, no. 3, pp. 574–583, Apr. 2015.
- [9] N. Yang, L. Wang, G. Geraci, M. ElKashlan, J. Yuan, and M. D. Renzo, “Safeguarding 5G wireless communication networks using physical layer security,” *IEEE Commun. Magazine*, vol. 53, pp. 20–27, April 2015.
- [10] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, “Key Generation From Wireless Channels: A Review,” *IEEE Access*, vol. 4, pp. 614-626, Mar. 2016

References

- [11] J. P. Coon, “Modelling trust in random wireless networks,” in *Wireless Communication Systems (ISWCS)*, 2014. 11th International Symposium on, Aug. 26-29, 2014, pp. 976-981, invited paper.
- [12] M. Haenggi, “The secrecy graph and some of its properties,” in *Proc. IEEE Int. Symp. Inf. Theory*, July 2008, pp. 539–543.
- [13] S. Goel, V. Aggarwal, A. Yener, and A. R. Calderbank, “Modeling location uncertainty for eavesdroppers: a secrecy graph approach,” in *Proc. IEEE Int. Symp. Inf. Theory*, June 2010.
- [14] P. C. Pinto and M. Z. Win, “Continuum percolation in the intrinsically secure communications graph,” in *Proc. IEEE Int. Symp. Inf. Theory and its Applications*, Oct. 2010.
- [15] G. Geraci, S. Singh, J. G. Andrews, J. Yuan, and I. B. Collings, “Secrecy rates in broadcast channels with confidential messages and external eavesdroppers,” *IEEE Trans. on Wireless Commun.*, vol. 13, pp. 2931–2943, May 2014.
- [16] T. X. Zheng, H. M. Wang, and Q. Yin, “On transmission secrecy outage of a multi-antenna system with randomly located eavesdroppers,” *IEEE Commun. Lett.*, vol. 18, pp. 1299–1302, Aug. 2014.
- [17] T. X. Zheng, H. M. Wang, J. Yuan, D. Towsley, and M. H. Lee, “Multi- antenna transmission with artificial noise against randomly distributed eaves- droppers,” *IEEE Trans. on Commun.*, vol. 63, pp. 4347–4362, Nov. 2015.
- [18] M. Ghogho and A. Swami, “Physical-layer secrecy of MIMO communi- cations in the presence of a poisson random field of eavesdroppers,” in *Communications Workshops (ICC), 2011 IEEE International Conference on*, pp. 1–5, June 2011.
- [19] C. Wang and H. M. Wang, “Physical Layer Security in Millimeter Wave Cellular Networks,” in *IEEE Transactions on Wireless Communications*, vol. 15, no. 8, pp. 5569-5585, Aug. 2016.