

Wireless Security: An Information Theoretic View

Şennur Ulukuş

Department of ECE

University of Maryland

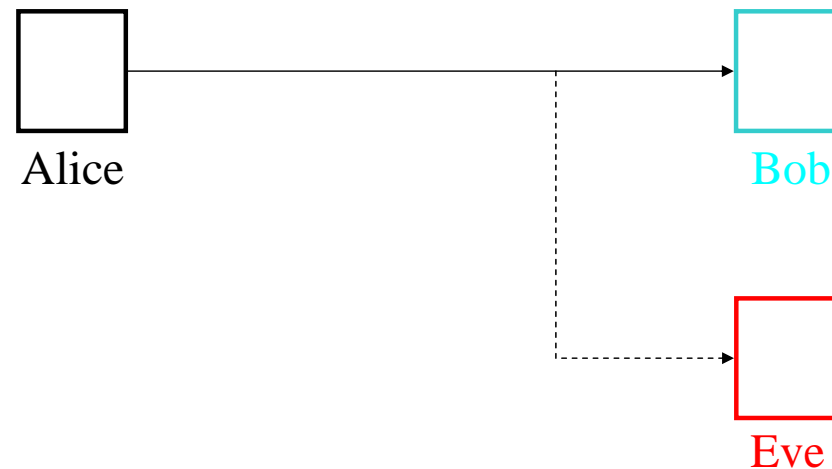
ulukus@umd.edu

Security in Wireless Systems

- Inherent openness in wireless communications channel: **eavesdropping** and **jamming**
- Countering security threats at different protocol layers:
 - **Cryptography**
 - * at higher layers of the protocol stack
 - * based on limited computational power at Eve
 - **Techniques like frequency hopping, CDMA**
 - * at the physical layer
 - * based on limited knowledge at Eve
 - **Information theoretic security**
 - * at the physical layer
 - * no assumption on Eve's computational power
 - * no assumption on Eve's available information
 - * **provable** secrecy and **ultimate** secrecy limits
- Combining all: multi-dimensional **cross-layer** security

Secrecy in Wire-tap Channel

- Wyner, 1975: wire-tap channel
- Eve gets a worse (degraded) version of Bob's signal: wire-tapping



- Secrecy measured by equivocation rate at Eve, i.e.,

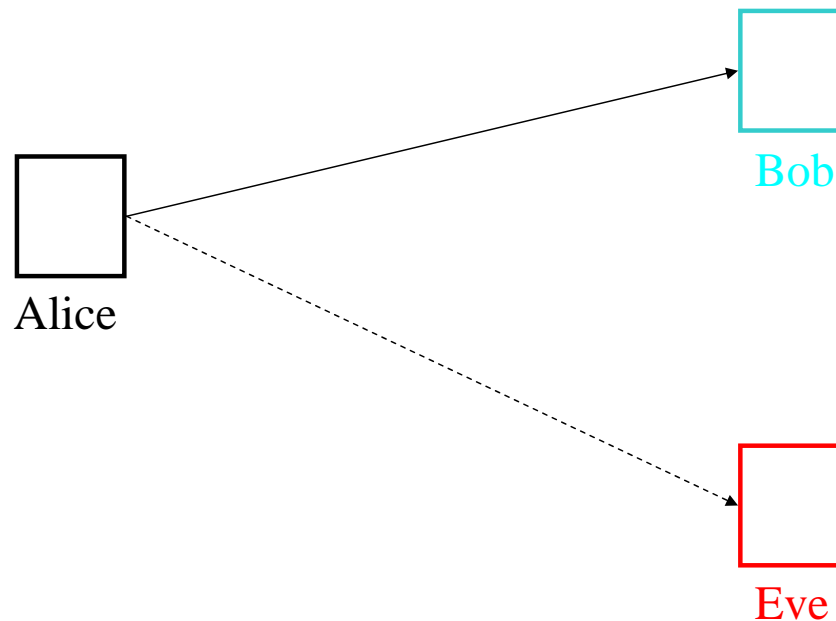
$$H(W|Z^n) = H(W)$$

- The **perfect** secrecy capacity

$$C_s = \max_{X \rightarrow Y \rightarrow Z} I(X;Y) - I(X;Z)$$

Secrecy in Broadcast Channel

- Csiszar and Korner, 1978: broadcast channel (applicable to wireless)
- Eve's signal is not necessarily a degraded version of Bob's signal

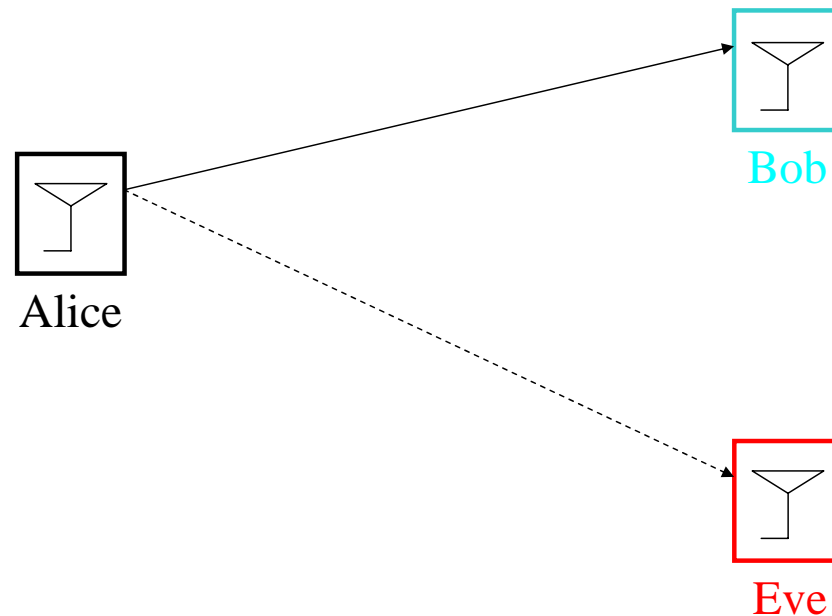


- Pre-processing of information might be necessary to confuse Eve
- The **perfect** secrecy capacity

$$C_s = \max_{U \rightarrow X \rightarrow YZ} I(U; Y) - I(U; Z)$$

Secrecy in Gaussian Channel

- Leung-Yang-Cheong and Hellman, 1978: Gaussian wire-tap channel
- Eve's signal is Bob's signal plus Gaussian noise



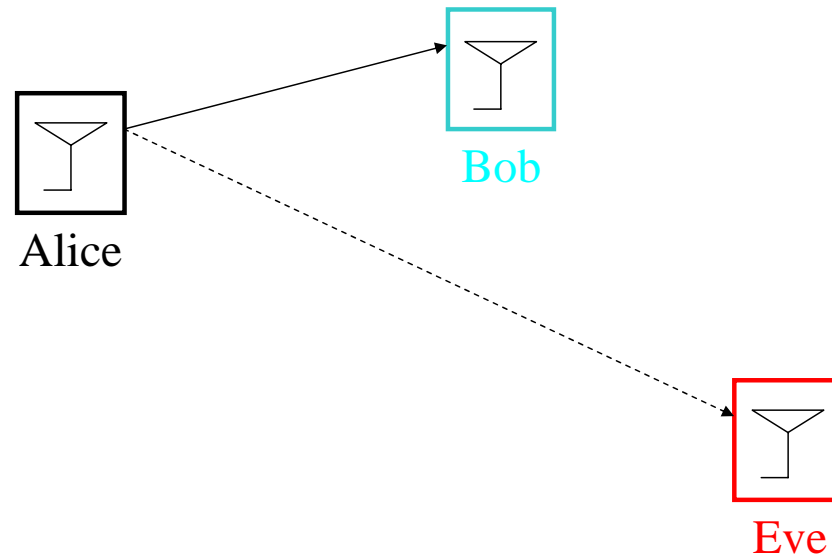
- No pre-processing of information is necessary and Gaussian signalling is optimal
- The **perfect** secrecy capacity

$$C_s = \max_{X \rightarrow Y \rightarrow Z} I(X; Y) - I(X; Z) = C_B - C_E$$

Caveat in the SISO Case

- In general, the secrecy capacity is $(C_B - C_E)^+$.
- That is, if Eve's channel is worse than Bob's, then positive secrecy capacity, i.e.,

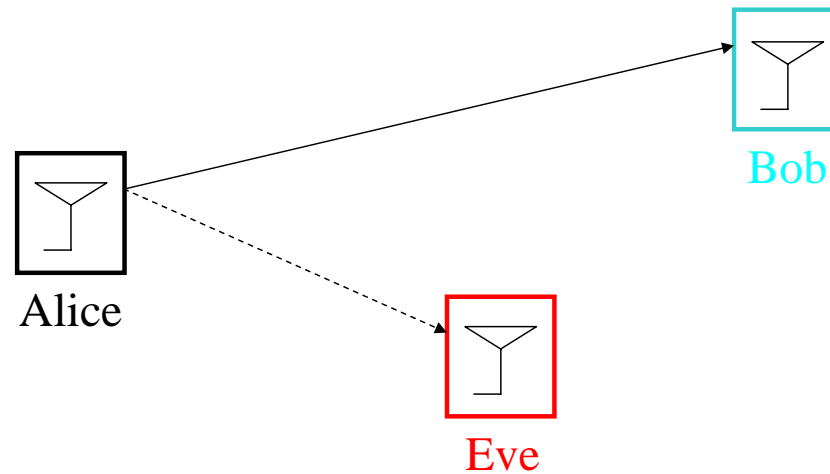
$$C_s = C_B - C_E$$



Caveat in the SISO Case

- In general, the secrecy capacity is $(C_B - C_E)^+$.
- That is, if Eve's channel is better than Bob's, then zero secrecy capacity, i.e.,

$$C_s = 0$$



Outlook at the End of 1970s

- Information theoretic secrecy is extremely powerful:
 - no limitation on Eve's computational power
 - no limitation on Eve's available information
 - yet, we are able to provide secrecy to the legitimate user
 - **provable** secrecy and **ultimate** secrecy limits
- We seem to be at the mercy of the nature:
 - if Bob's channel is stronger, positive perfect secrecy rate
 - if Eve's channel is stronger, no secrecy
- Wireless channel provides many options:
 - time, space, multi-user diversity
 - cooperation

Jump to 2000s

- Two NSF grants:
 - **Multi-user Wireless Security**, PIs: S. Ulukus, A. Yener, 2005-2008, [ITR-Cybertrust/CCR](#).
 - **Secure Capacity of Wireless Networks**, PIs: S. Ulukus, A. Yener, 2007-2010, [Cybertrust](#).
- First papers on information-theoretic security after late 1970s:
 - S. Shafiee and S. Ulukus, **CISS Conference, March 2005**,
Correlated jamming in multiple access channels.
 - E. Tekin, S. Serbetli and A. Yener, **Asilomar Conference, November 2005**,
On secure signalling for the Gaussian multiple access channel.
 - J. Barros and M. Rodrigues, **ISIT Conference, July 2006**,
Secrecy capacity of wireless channels.
 - Y. Liang and H. V. Poor, **ISIT Conference, July 2006**,
Generalized multiple access channels with confidential messages.
- First new ideas:
 - Multi-user secrecy measures
 - Cooperative jamming
 - Exploiting time diversity (fading) for security

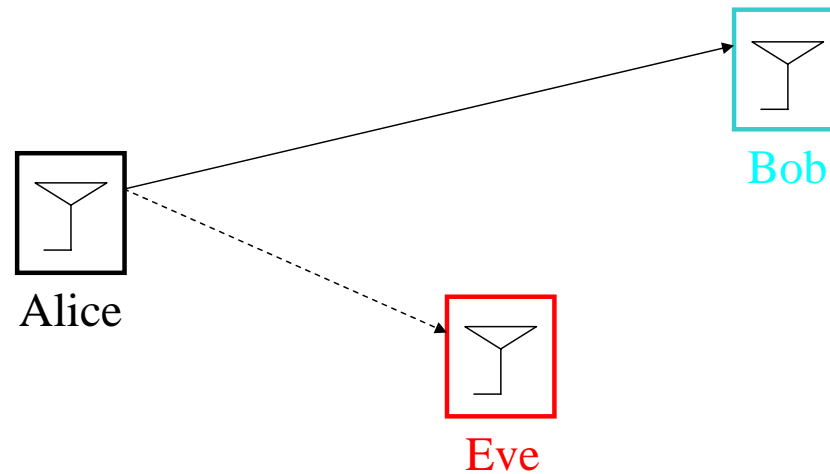
Recent Literature on Information Theoretic Secrecy

- **Multiple access channel:** Tekin-Yener 2007, Liang-Poor 2008, Ekrem-Ulukus 2008
- **Broadcast channel:** Liu-Poor 2007, Liu-Maric-Spasojevic-Yates 2008, Khisti-Tchamkerten-Wornell 2008, Ekrem-Ulukus 2008
- **Interference channel:** Liang-Somekh-Baruch-Poor-Shamai-Verdu 2007
Liu-Maric-Spasojevic-Yates 2008
- **Relay channel:** Lai-El Gamal 2006, Oohama 2007, He-Yener 2007, Yuksel-Erkip 2007
- **Fading:** Barros-Rodrigues 2006, Gopala-Lai-El Gamal 2006, Li-Yates-Trappe 2007, Khisti-Tchamkerten-Wornell 2008, Liang-Poor-Shamai 2008,
- **Multiple antennas:** Khisti-Wornell 2007, Shafiee-Ulukus 2007, Shafiee-Liu-Ulukus 2007, Oggier-Hassibi 2007, Liu-Poor 2007, Liu-Shamai 2008
- **Cooperation versus secrecy:** He-Yener 2007, Ekrem-Ulukus 2008

Recall: Caveat in the SISO Case

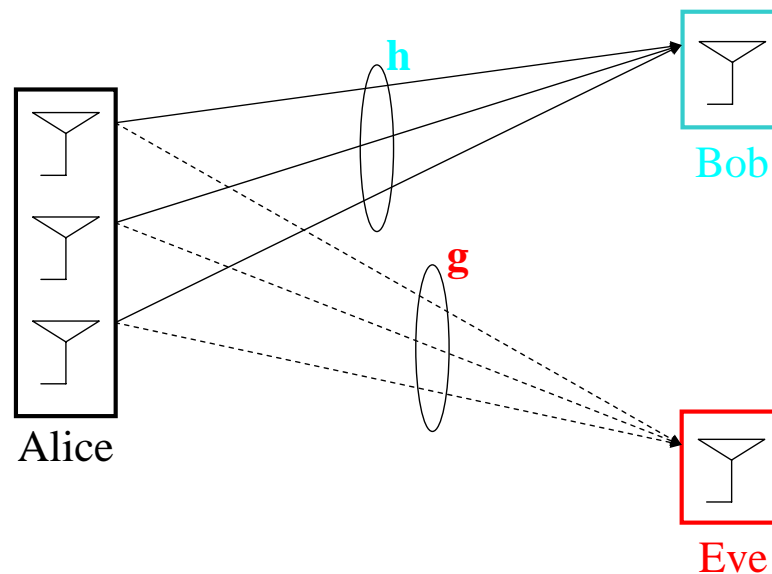
- In general, the secrecy capacity is $(C_B - C_E)^+$.
- That is, if Eve's channel is better than Bob's, then zero secrecy capacity, i.e.,

$$C_s = 0$$



Secrecy in MISO/MIMO Channel

- MISO: Shafiee-Ulukus, Li-Trappe-Yates, Khisti-Wornell-Wiesel-Eldar (all in 2007)
- MIMO: Shafiee-Liu-Ulukus, Khisti-Wornell, Oggier-Hassibi, Liu-Shamai (2007 and 2008)
- Because of multiple antennas, Eve's channel is not degraded

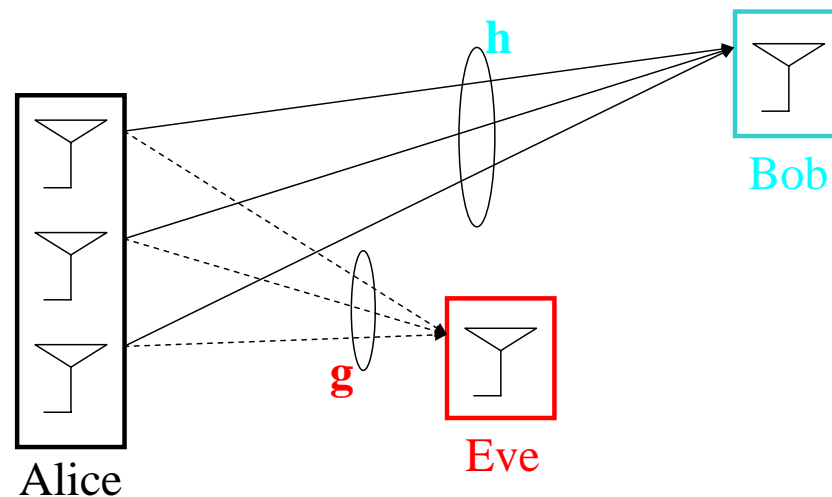


- **We proved:** no pre-processing of information is necessary and Gaussian signalling is optimal
- The **perfect** secrecy capacity

$$C_s = \max_{U \rightarrow X \rightarrow YZ} I(U; Y) - I(U; Z) = \max_{X \rightarrow YZ} I(X; Y) - I(X; Z)$$

Implications of MISO/MIMO for Secrecy

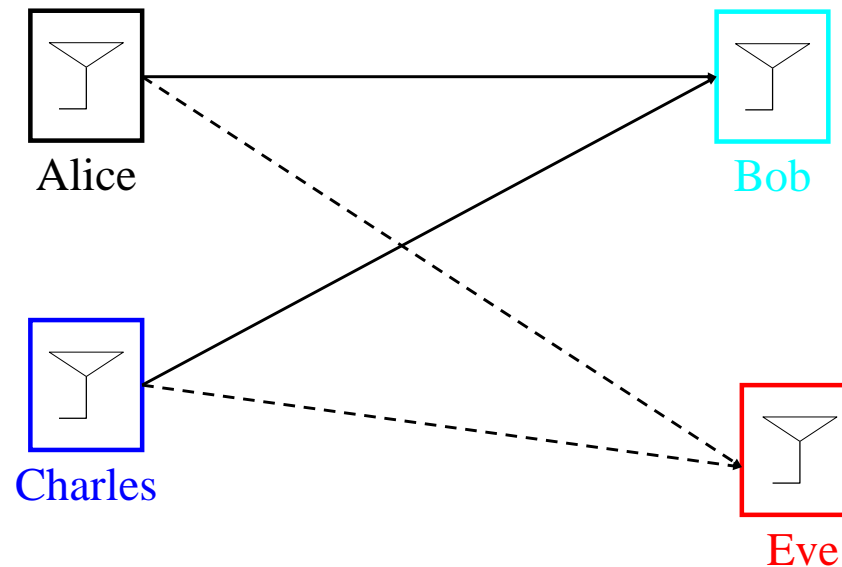
- Multiple dimensions (MISO/MIMO) improve secrecy.
- Even when Eve is closer than Bob, **we can beamform away from Eve's direction.**



- Even when we do not know where Eve is,
 - we can transmit noise in the null space of Bob's direction [Negi-Goel, 2005]
- Information theoretic **provable** secrecy, using **signal processing** techniques, **in the PHY layer.**

Secrecy in the Multiple Access Channel

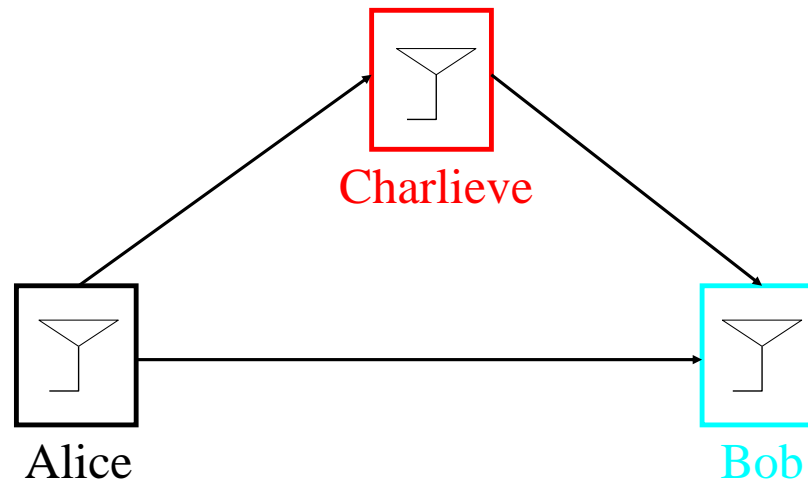
- Multi-user secrecy measures [Tekin-Yener 2006]:
 - Interactions between the secrets of Alice and Charles
- Cooperative jamming [Tekin-Yener 2006]:
 - If Charles is close to Eve, he can jam Eve, to improve the secrecy of Alice



- Secrecy capacity region is still open with recent progress in [Ekrem-Ulukus 2008]

Interactions of Cooperation and Secrecy

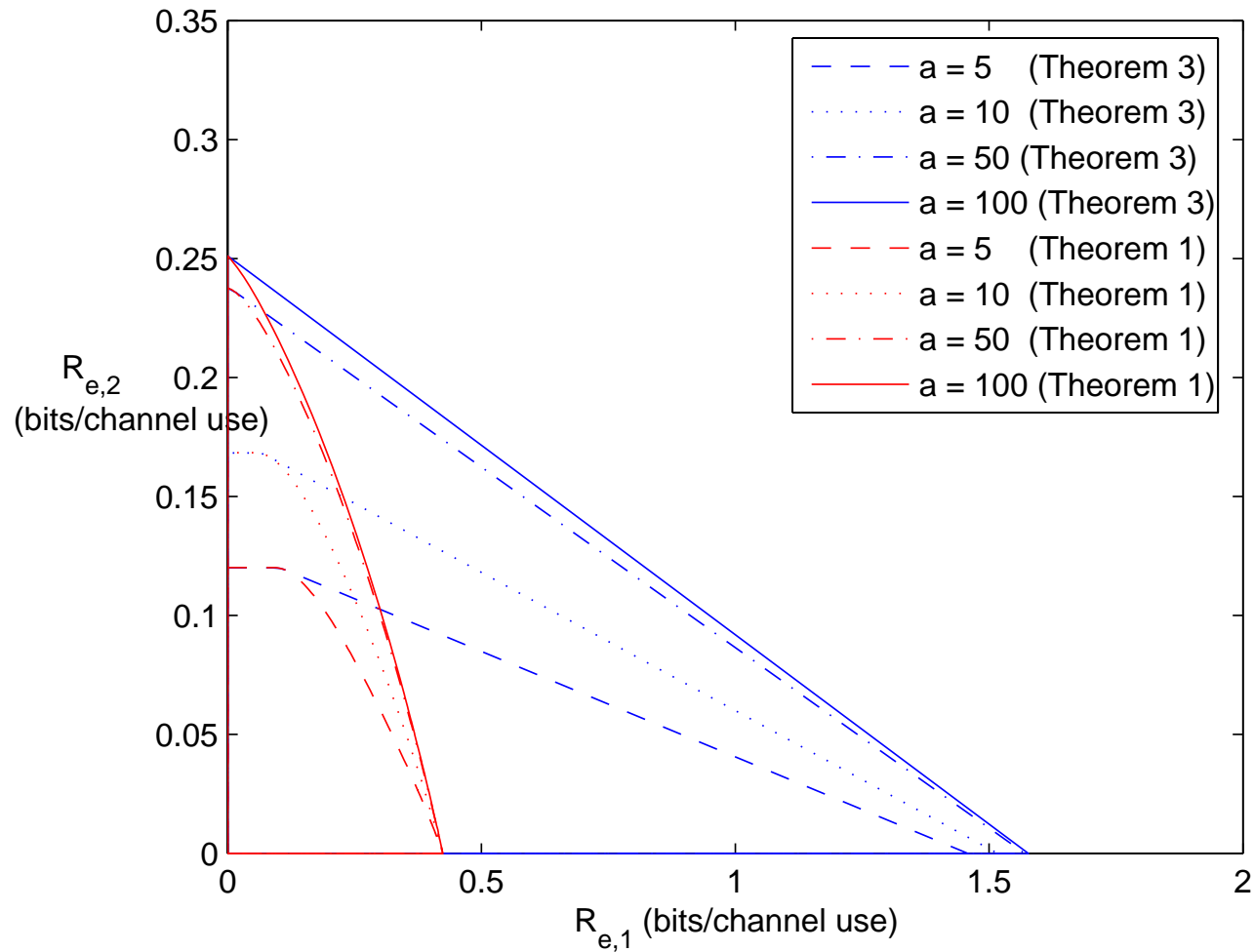
- How do **cooperation** and **secrecy** interact?
 - Is there a **trade-off** or a **parallelism**?
- Depends on the cooperation mechanism:
 - If decode-and-forward based: cooperation decreases secrecy
 - If compress-and-forward based: cooperation can increase secrecy



- Relay channel [He-Yener 2007], cooperative broadcast [Ekrem-Ulukus 2008], cooperative multiple access [Ekrem-Ulukus 2008].

Example: Gaussian Channels, $N_1 < N_2$, Theorems 1 and 3

Dependent V_1, V_2 (DPC for user 1)



Conclusions

- Information theoretic secrecy is extremely powerful:
 - no limitation on adversary's computational power or available information.
- The achievable secrecy is **quantifiable, provable** and **ultimate**.
- It is in the lower layers (PHY and perhaps MAC).
- Combining with other kinds of security measures: **multi-dimensional, cross-layer** security.
- In some applications, e.g., sensor and RFID networks, physical layer security is a necessity.
- Many open problems, a vital and active research area, with potential for high impact.