Physical Layer Security

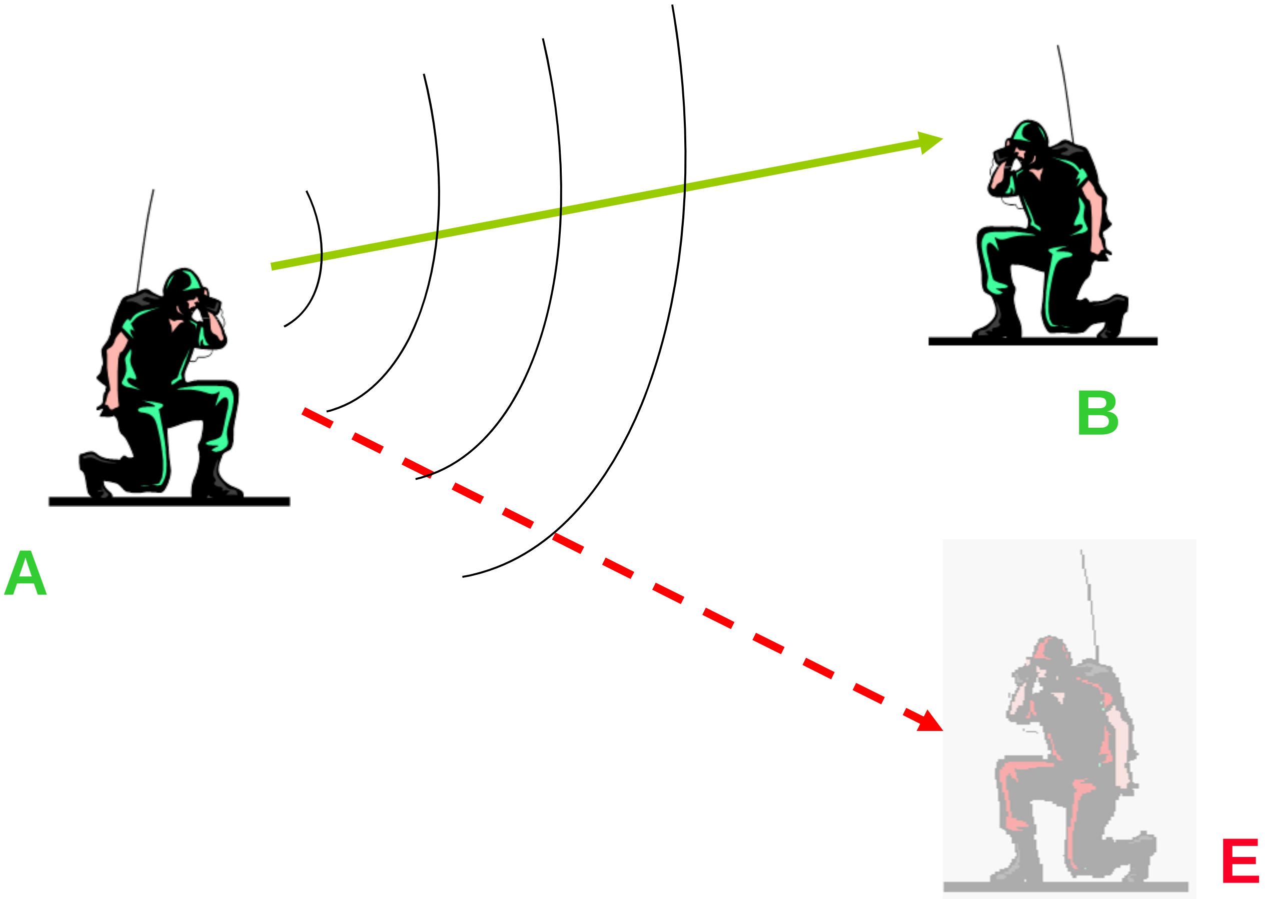
Şennur Ulukuş
ECE / ISR
University of Maryland

FOR UMD USE ONLY

Security in Wireless Systems

Inherent openness in the wireless communications channel:

eavesdropping and **jamming** attacks

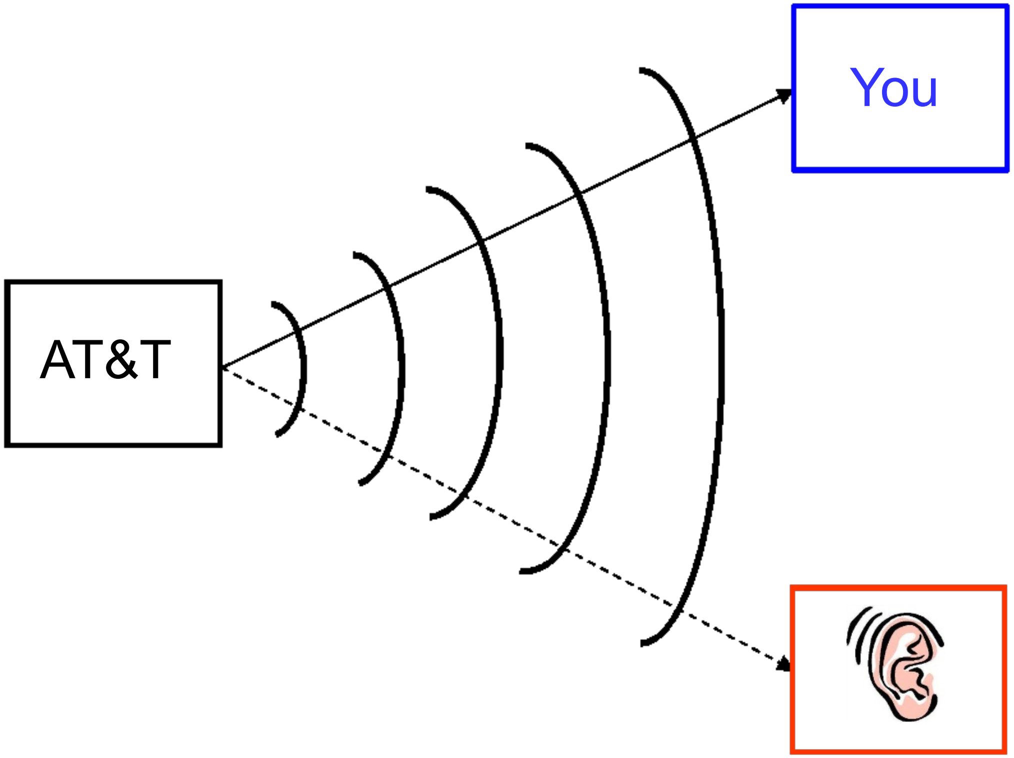


FOR UMD USE ONLY

Security in Wireless Systems

Inherent openness in the wireless communications channel:

eavesdropping and **jamming** attacks

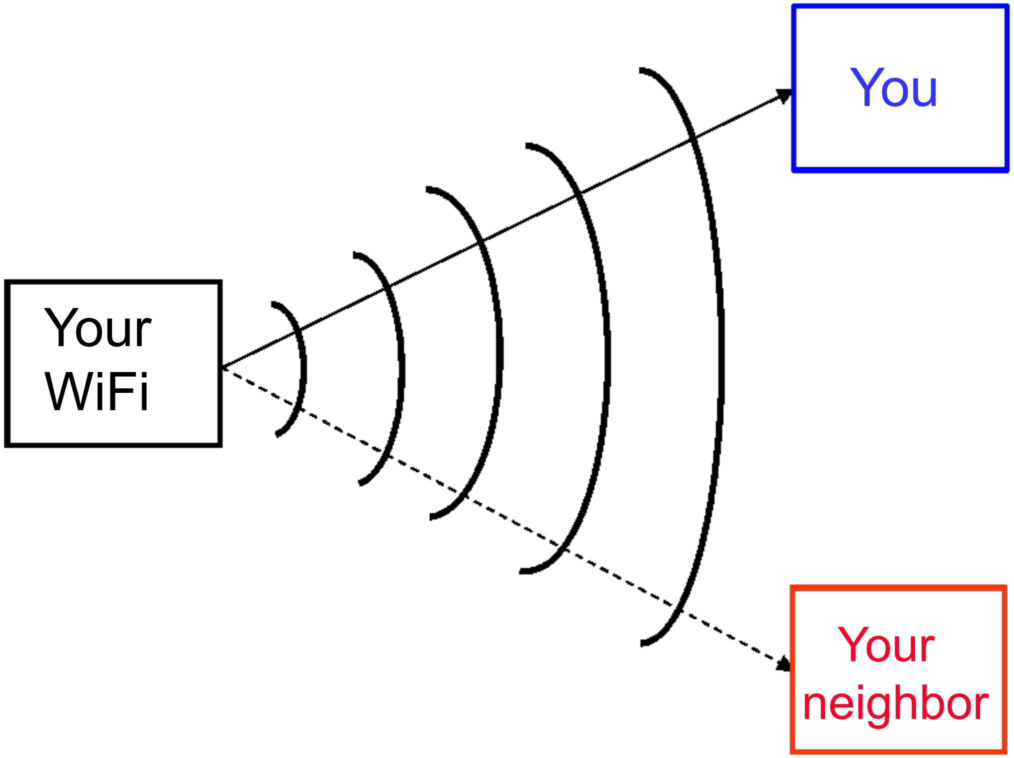


FOR UMD USE ONLY

Security in Wireless Systems

Inherent openness in the wireless communications channel:

eavesdropping and **jamming** attacks

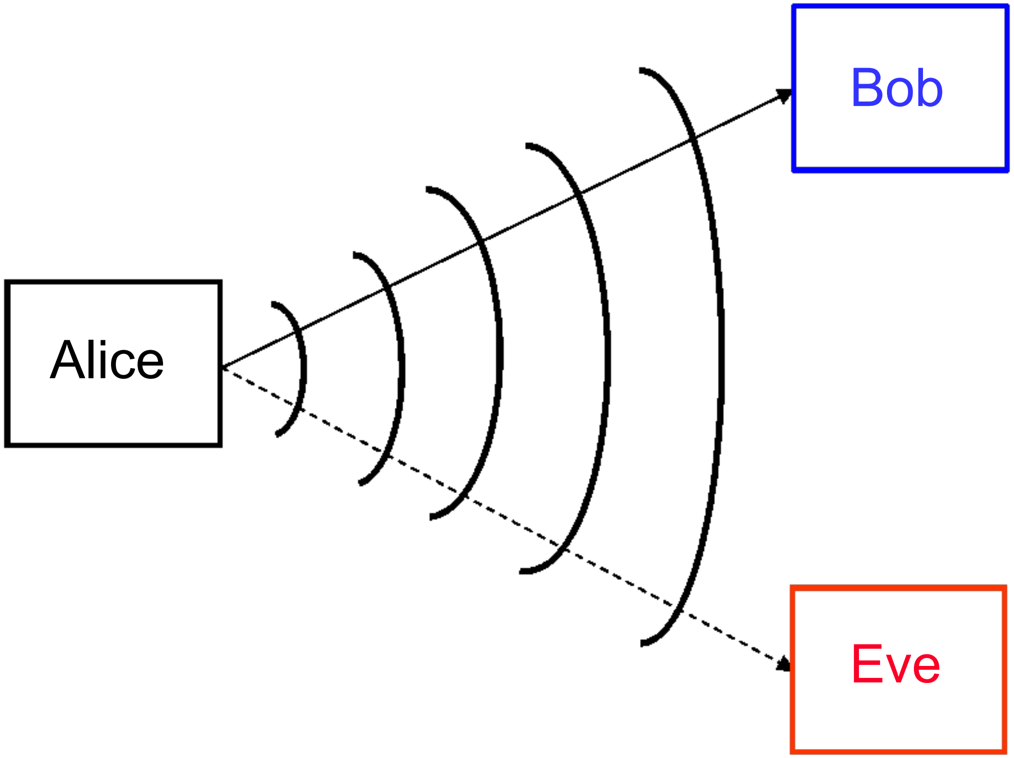


FOR UMD USE ONLY

Security in Wireless Systems

Inherent openness in the wireless communications channel:

eavesdropping and **jamming** attacks

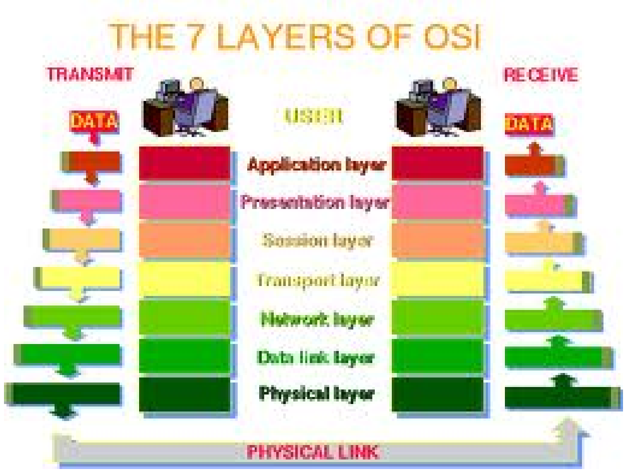


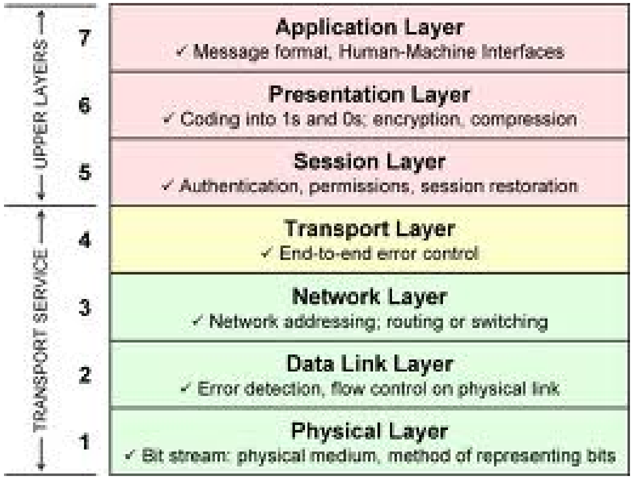
FOR UMD USE ONLY

What is the Physical Layer?

The **lowest layer** of the 7-layer OSI protocol stack.

The level at which **bits** are transmitted/received.





UPPER LAYERS	7	**Application Layer** ✓ Message format, Human-Machine Interfaces
	6	**Presentation Layer** ✓ Coding into 1s and 0s; encryption, compression
	5	**Session Layer** ✓ Authentication, permissions, session restoration
TRANSPORT SERVICE	4	**Transport Layer** ✓ End-to-end error control
	3	**Network Layer** ✓ Network addressing; routing or switching
	2	**Data Link Layer** ✓ Error detection, flow control on physical link
	1	**Physical Layer** ✓ Bit stream: physical medium, method of representing bits

Countering Security Threats: Current State-of-the-Art

Cryptography:

- at higher layers of the protocol stack
- based on **limited computational power** at the adversary

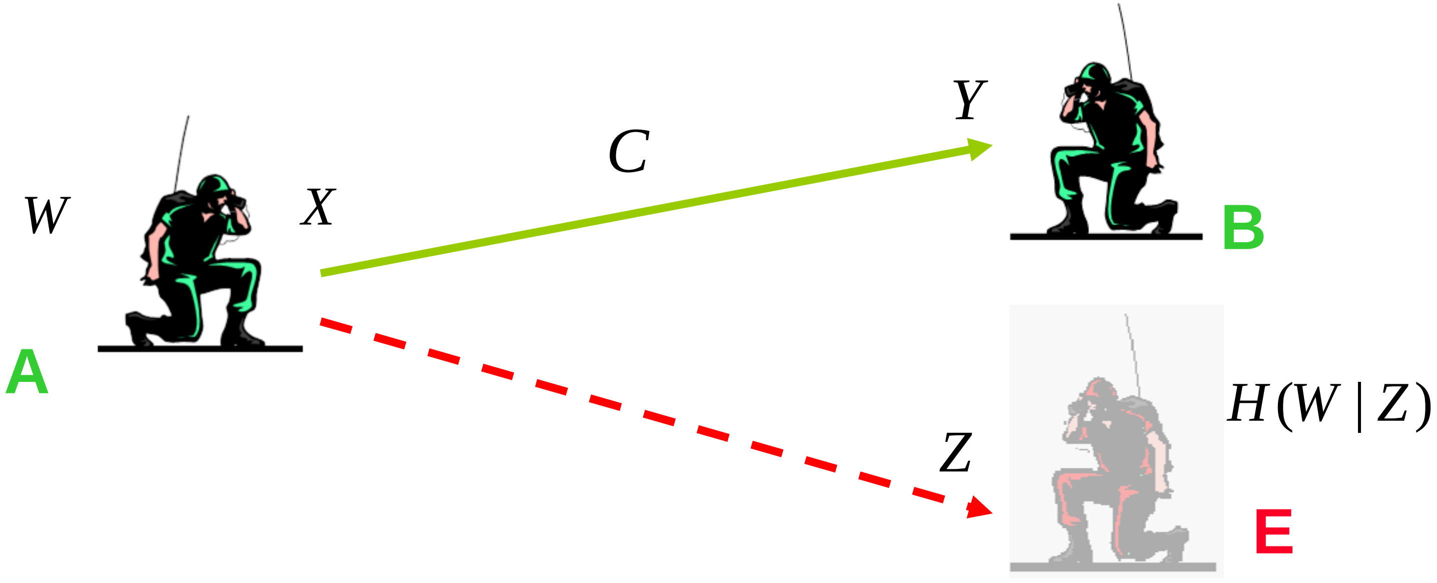
Spread spectrum, e.g., frequency hopping and CDMA:

- at the physical layer
- based on **limited knowledge** at the adversary

Physical layer security:

- at the physical layer
- no assumption on adversary’s computational power
- no assumption on adversary’s available information
- **provable** and **quantifiable** (in bits/sec/hertz)
- **implementable** using signal proc, comm and coding techniques

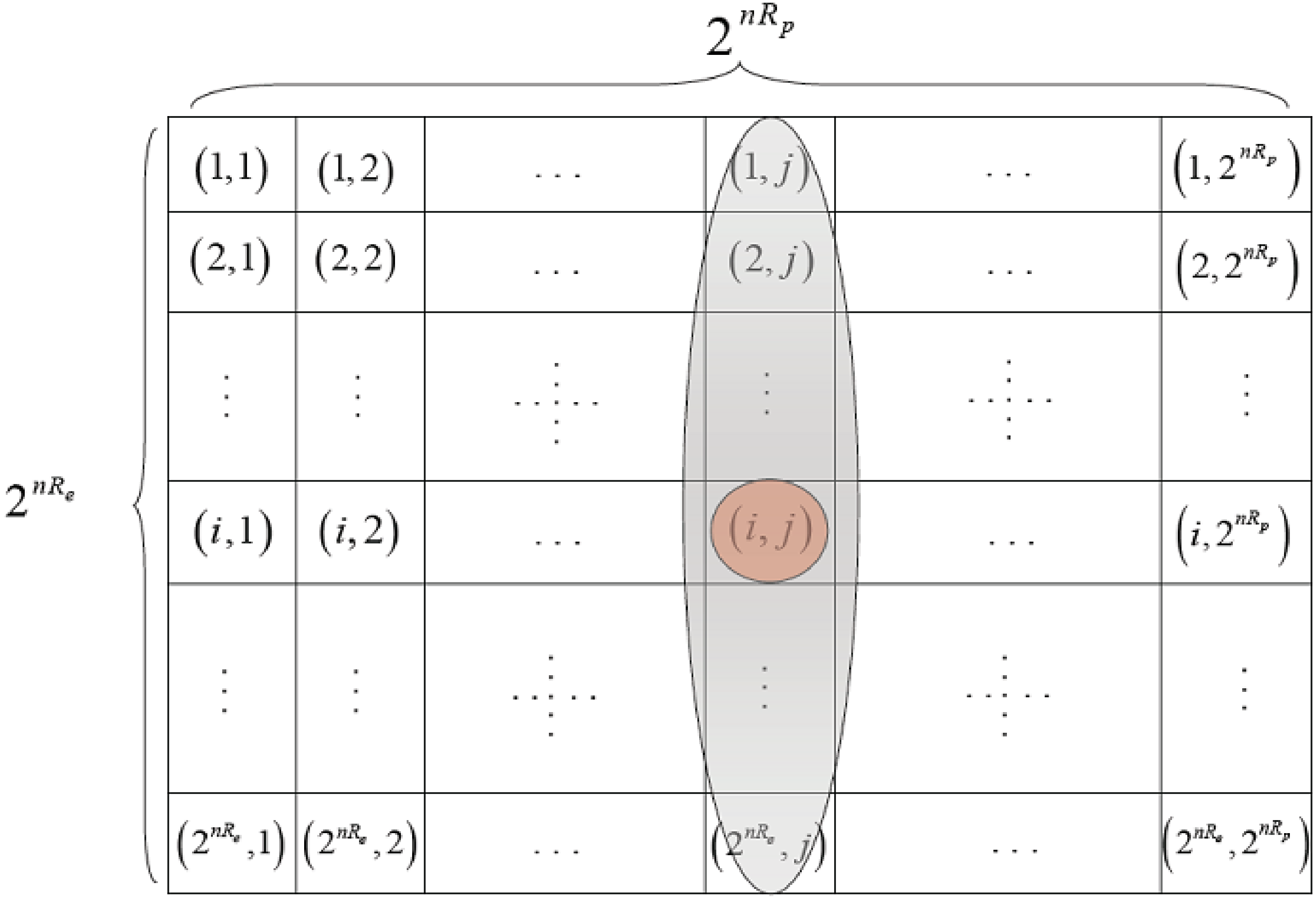
Wireless Wiretap Channel



- Perfect secrecy: $H(W|Z) = H(W)$
- Perfect secrecy capacity: $C = \max\ I(X;Y) - I(X;Z)$
- For certain channels (but not always): $C = C_B - C_E$

FOR UMD USE ONLY

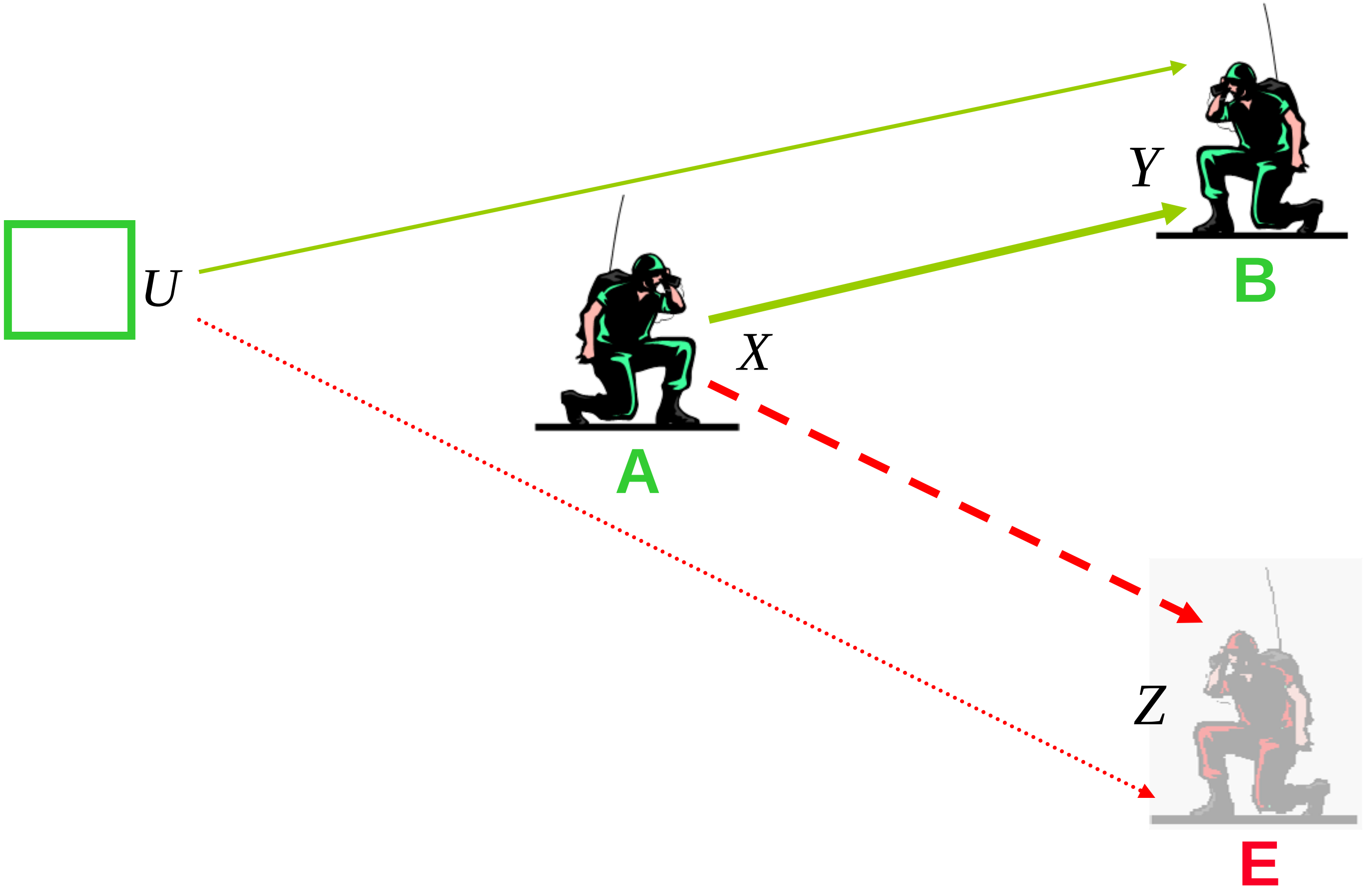
Main Tools: Stochastic Encoding



$(1,1)$	$(1,2)$	$\cdots$	$(1,j)$	$\cdots$	$(1,2^{nR_p})$
$(2,1)$	$(2,2)$	$\cdots$	$(2,j)$	$\cdots$	$(2,2^{nR_p})$
$\vdots$	$\vdots$	$\cdots\vdots\cdots$	$\vdots$	$\cdots\vdots\cdots$	$\vdots$
$(i,1)$	$(i,2)$	$\cdots$	(i,j)	$\cdots$	$(i,2^{nR_p})$
$\vdots$	$\vdots$	$\cdots\vdots\cdots$	$\vdots$	$\cdots\vdots\cdots$	$\vdots$
$(2^{nR_e},1)$	$(2^{nR_e},2)$	$\cdots$	$(2^{nR_e},j)$	$\cdots$	$(2^{nR_e},2^{nR_p})$

$$R_e = I(X;Y) - I(X;Z), \quad R_p = I(X;Z)$$

Main Tools: Channel Pre-fixing

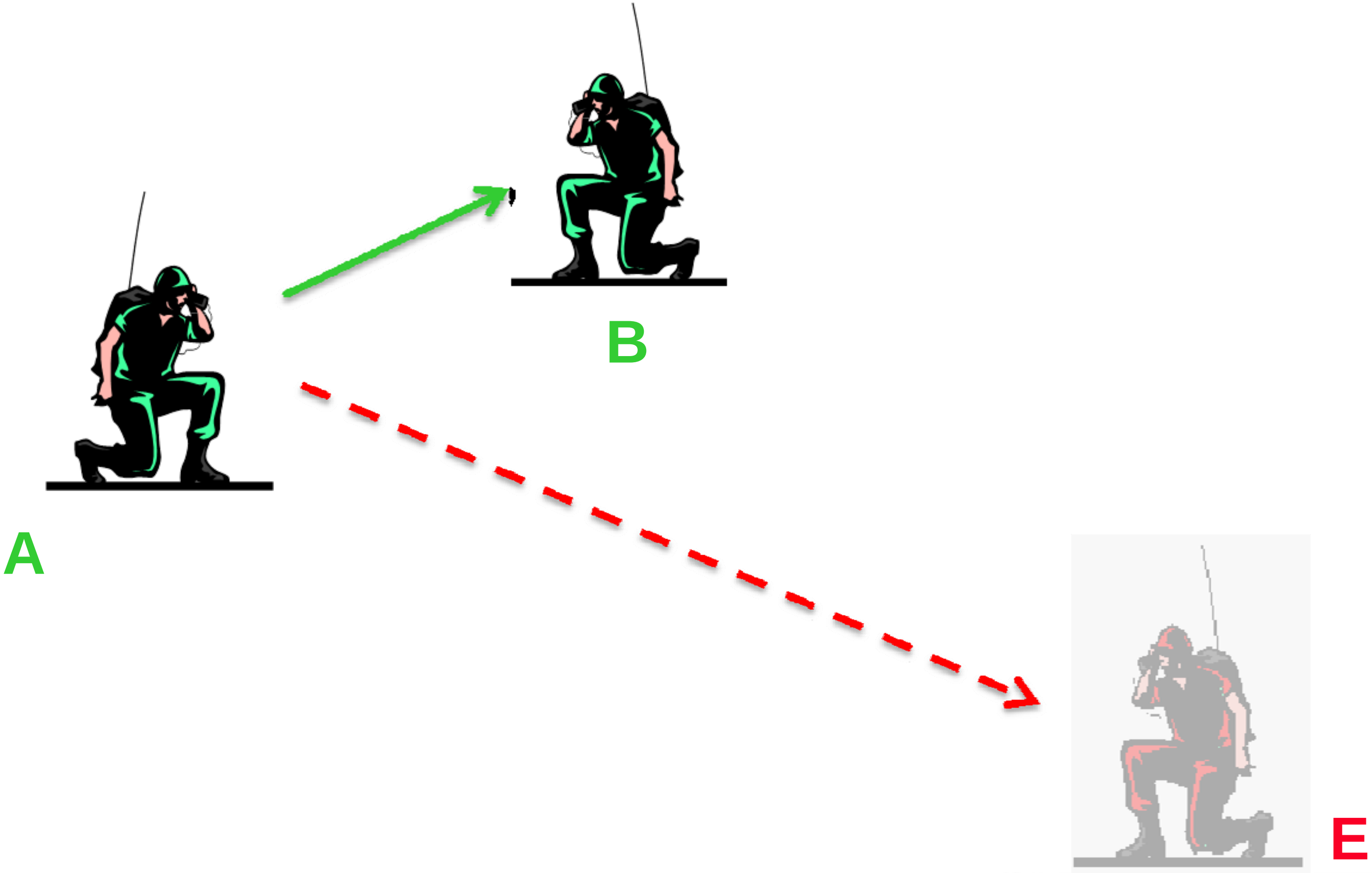


- Perfect secrecy capacity: $C = \max \; I(U;Y) - I(U;Z)$

FOR UMD USE ONLY

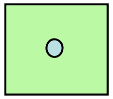
Simple Illustrative Example: Stochastic Encoding

Bob has a better (less noisy) channel than Eve.

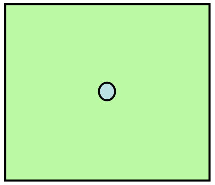


FOR UMD USE ONLY

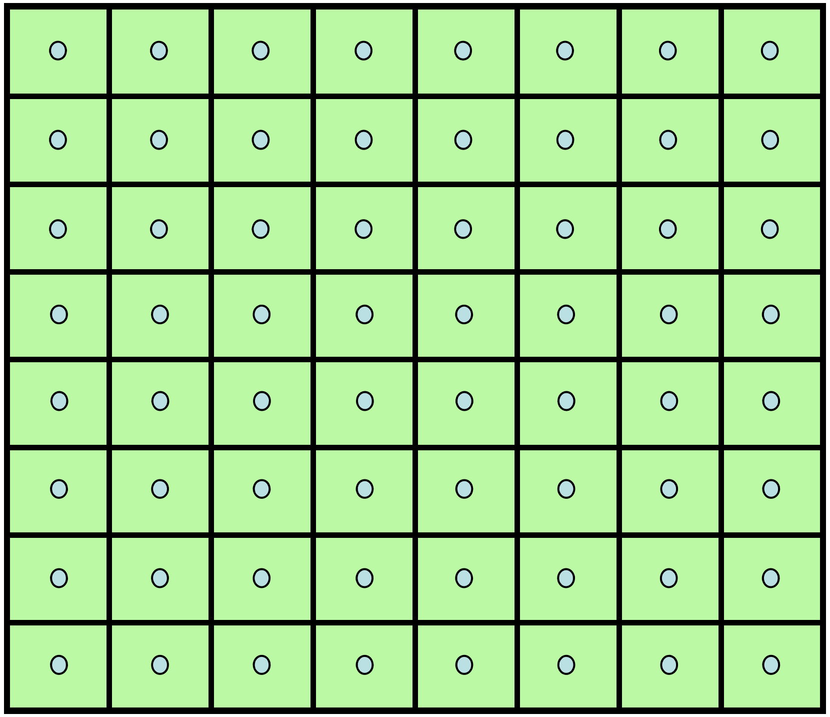
Bob’s noise



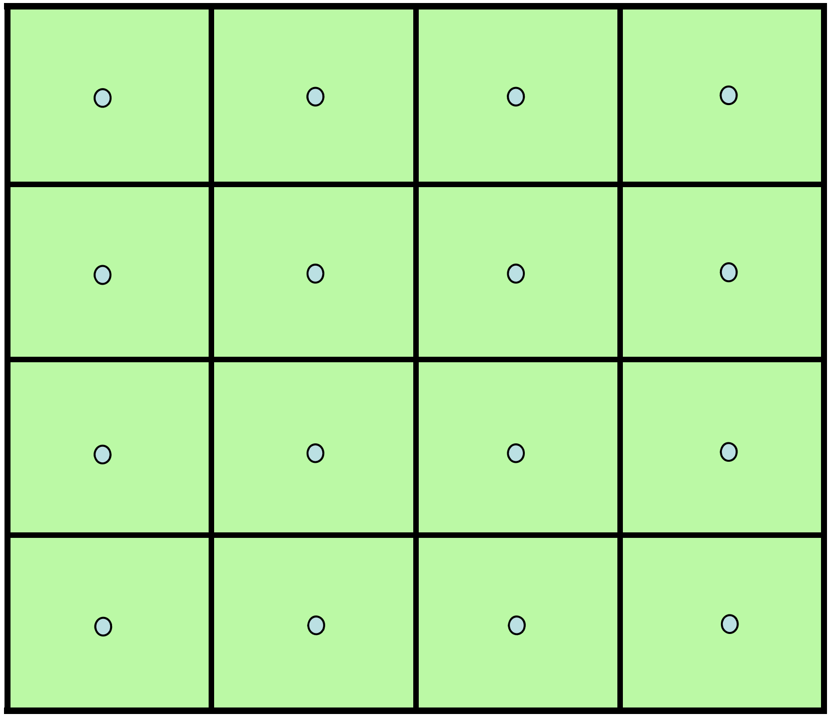
Eve’s noise



Bob’s constellation



Eve’s constellation

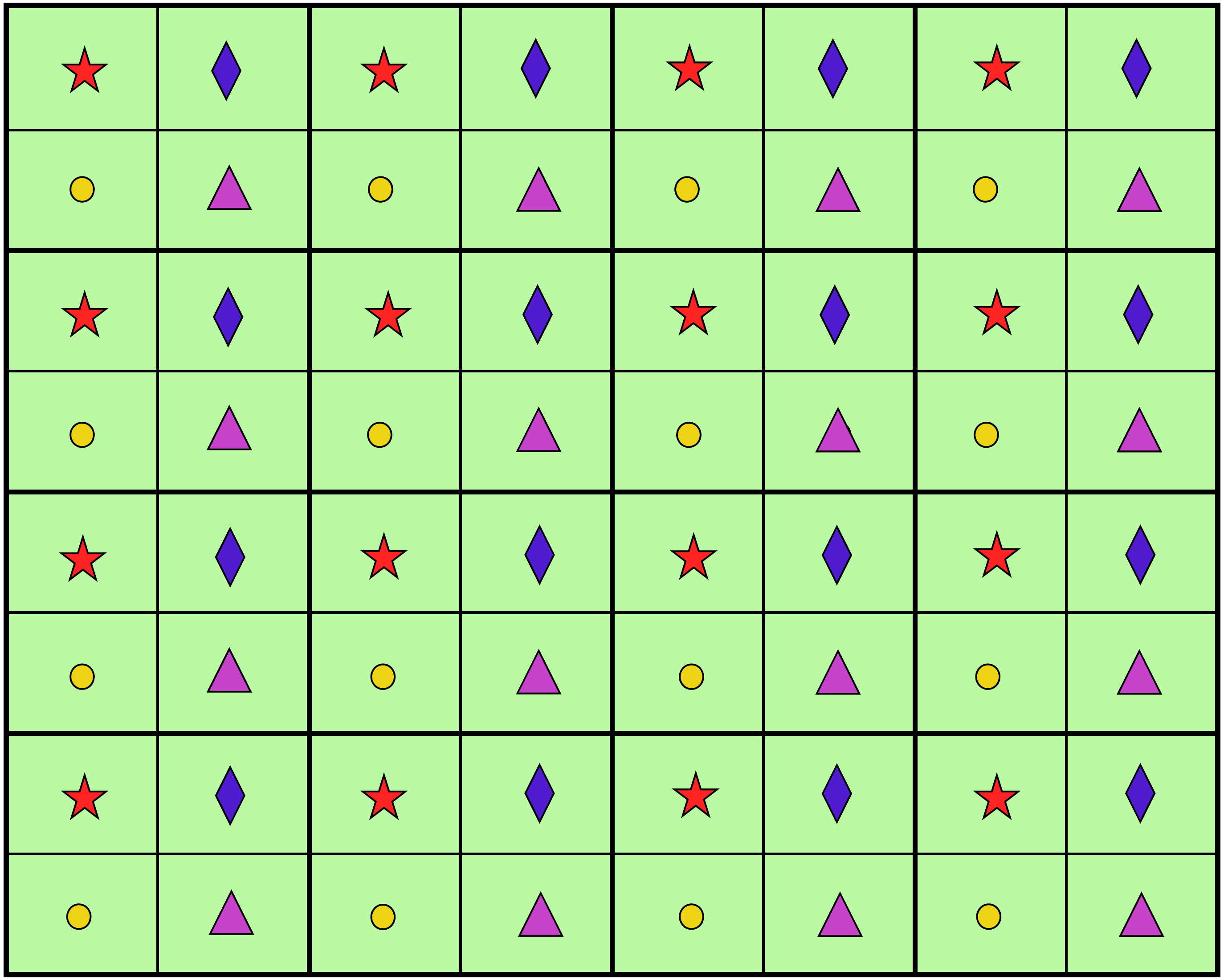


$$C_B = \log_2 64 = 6 \text{ b/s}$$

$$C_E = \log_2 16 = 4 \text{ b/s}$$

$$C_s = C_B - C_E = 2 \text{ b/s}$$

Divide Bob’s constellation into 4 subsets.



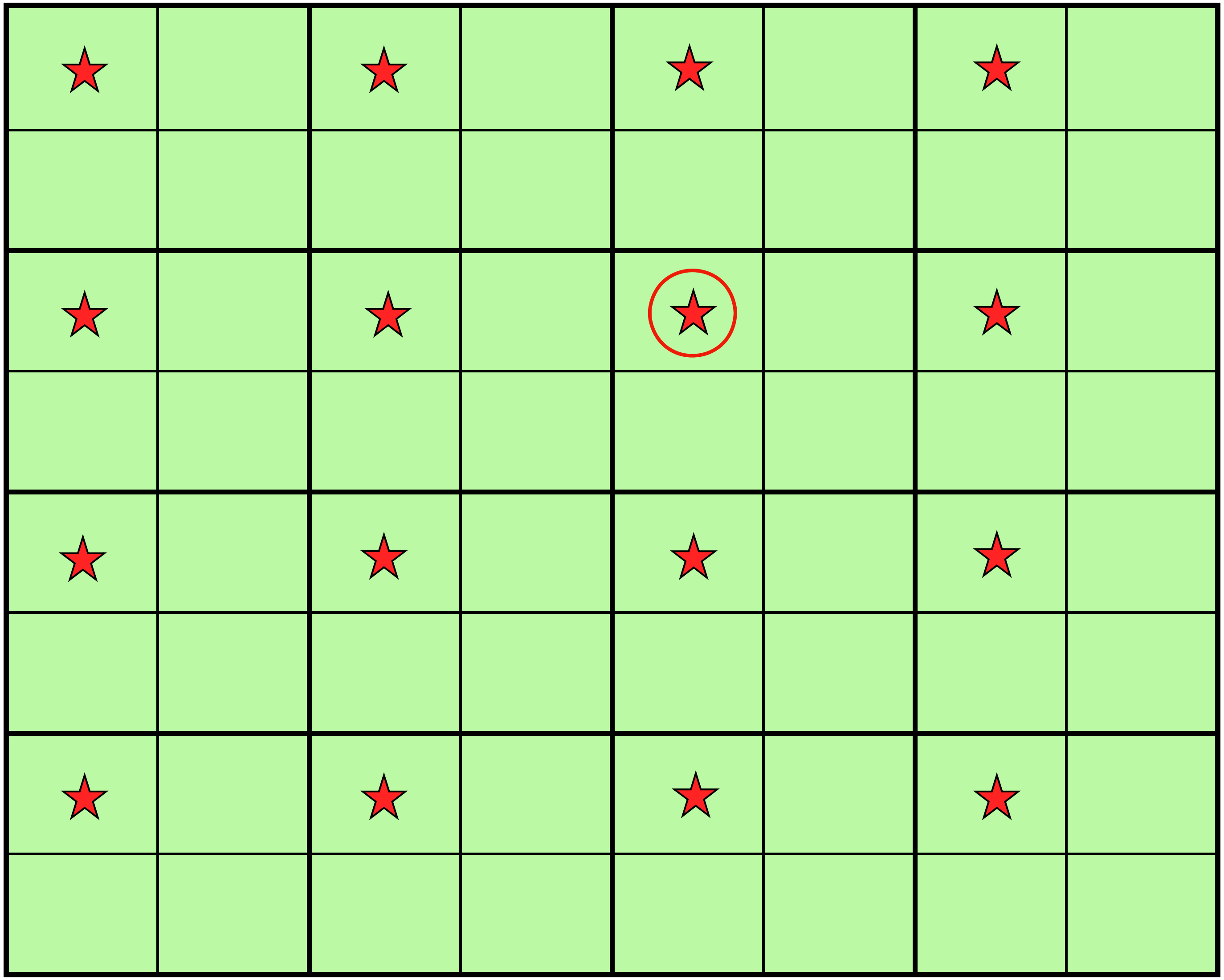
● Message 1

▲ Message 2

◆ Message 3

★ Message 4

All red stars denote the same message. Pick one randomly.



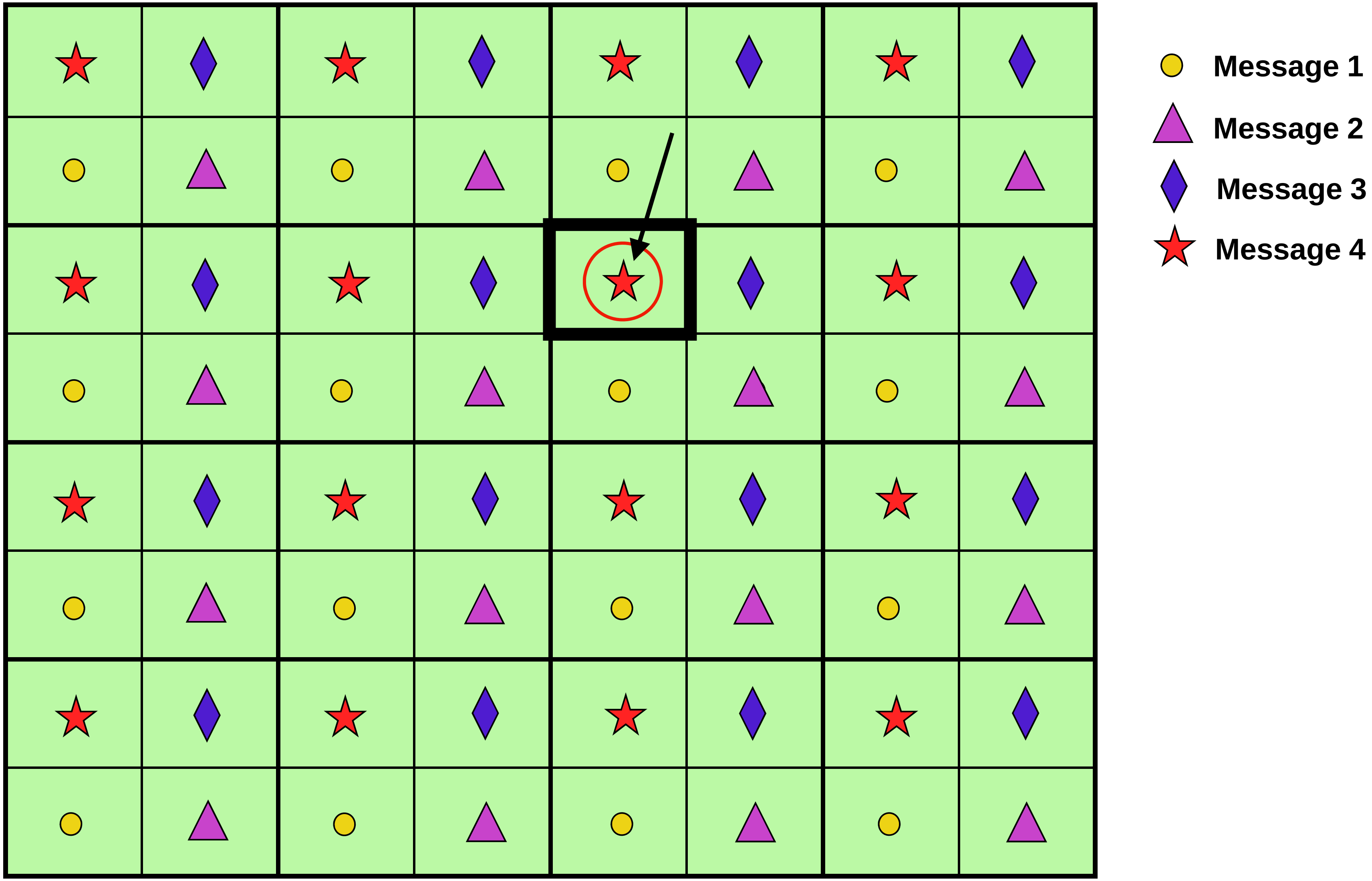
● Message 1

▲ Message 2

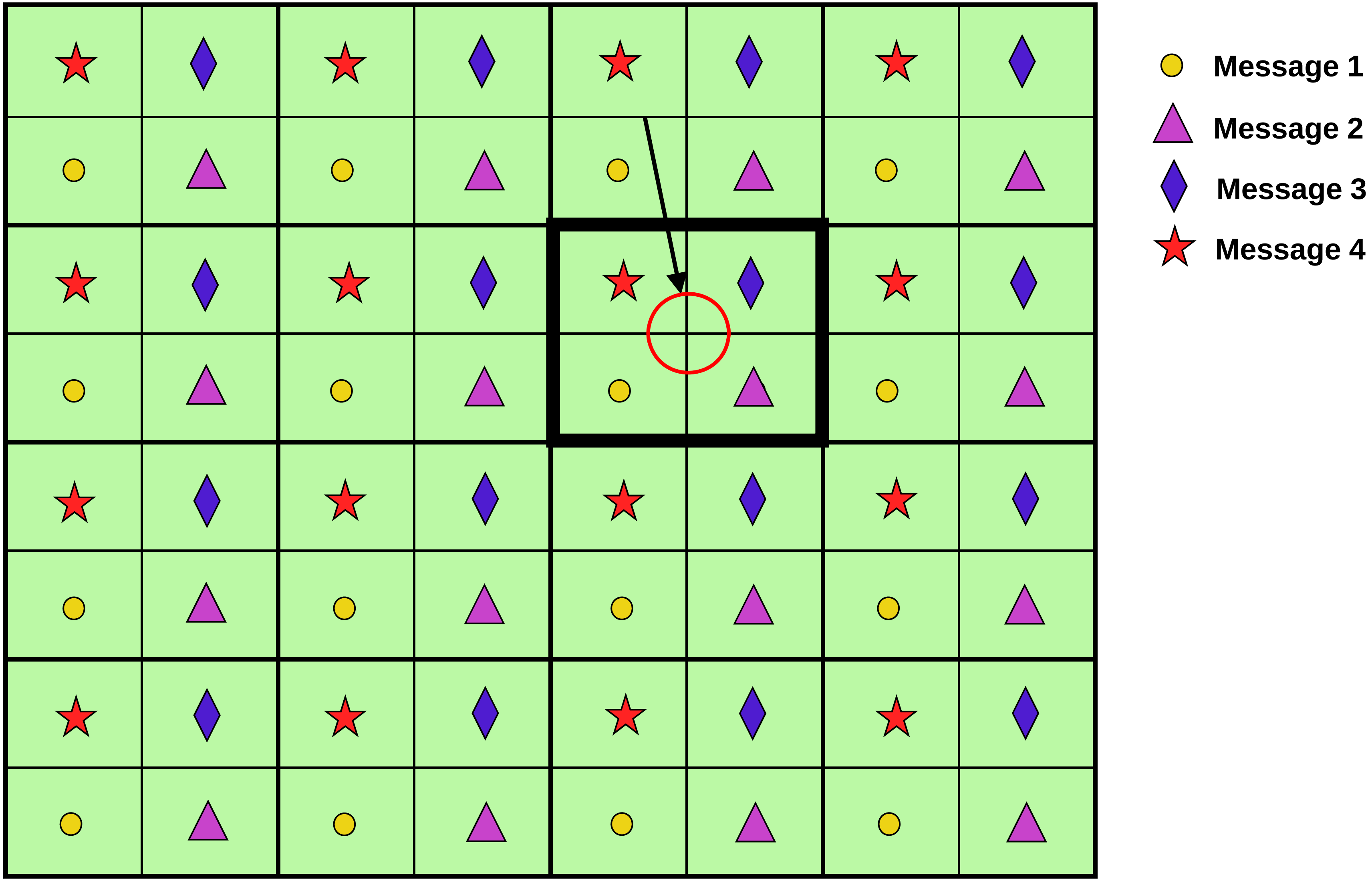
◆ Message 3

★ Message 4

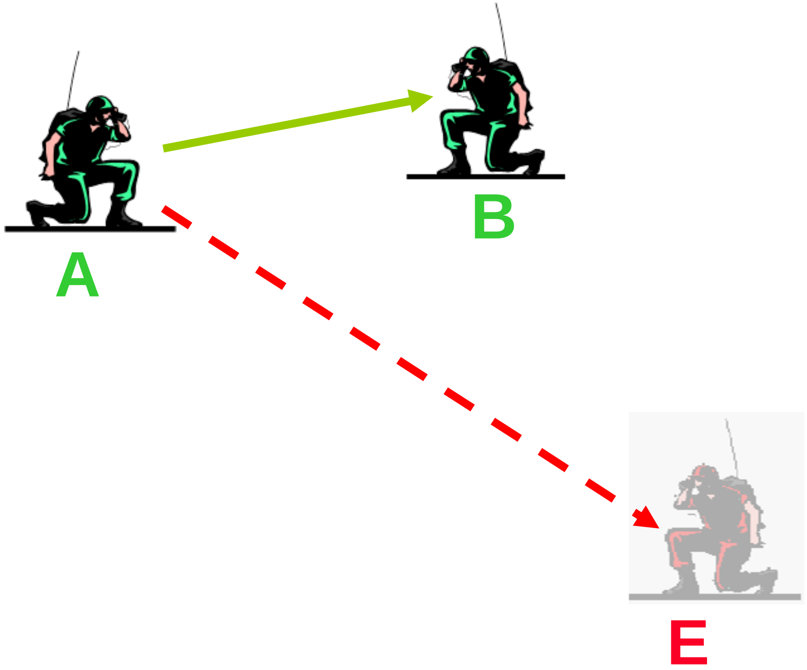
Bob can decode the message reliably.



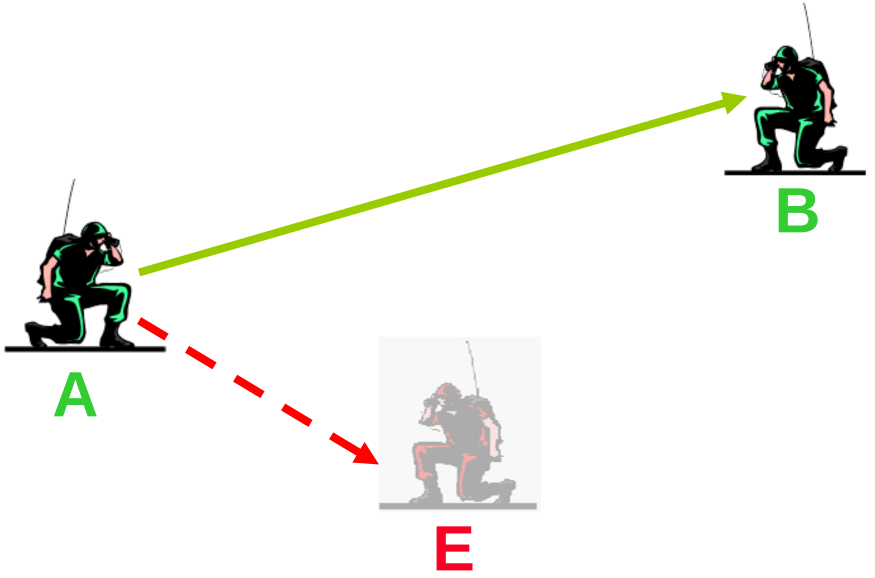
For Eve, all 4 messages are equally-likely.



Caveat: Need Channel Advantage



positive secure capacity



zero secure capacity

Two Recurring Themes:

1) Creating advantage for the good guys:

- □ computational advantage (crypto)
- □ knowledge advantage (spread spectrum)
- □ channel advantage (physical layer security)

2) Exhausting the capabilities of the bad guys:

- □ exhausting computational power (crypto)
- □ exhausting searching power (spread spectrum)
- □ exhausting decoding capability (physical layer security)

Obvious Applications with Natural Channel Advantage:

1) Near Field Communications

2) Medical Communications

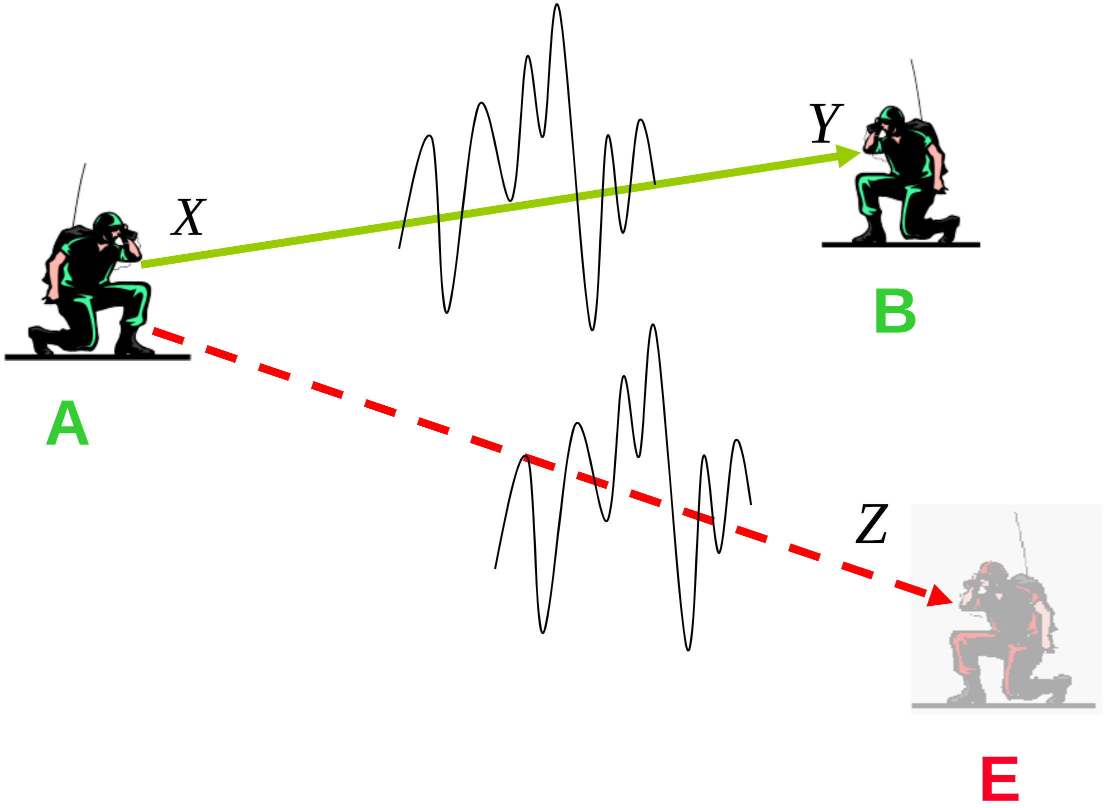
3) Military/Civilian Green Zones

Former Republican Palace, Bagdad, Iraq

Creating Channel Advantage

Exploiting channel variations (fading)

Opportunistic transmissions

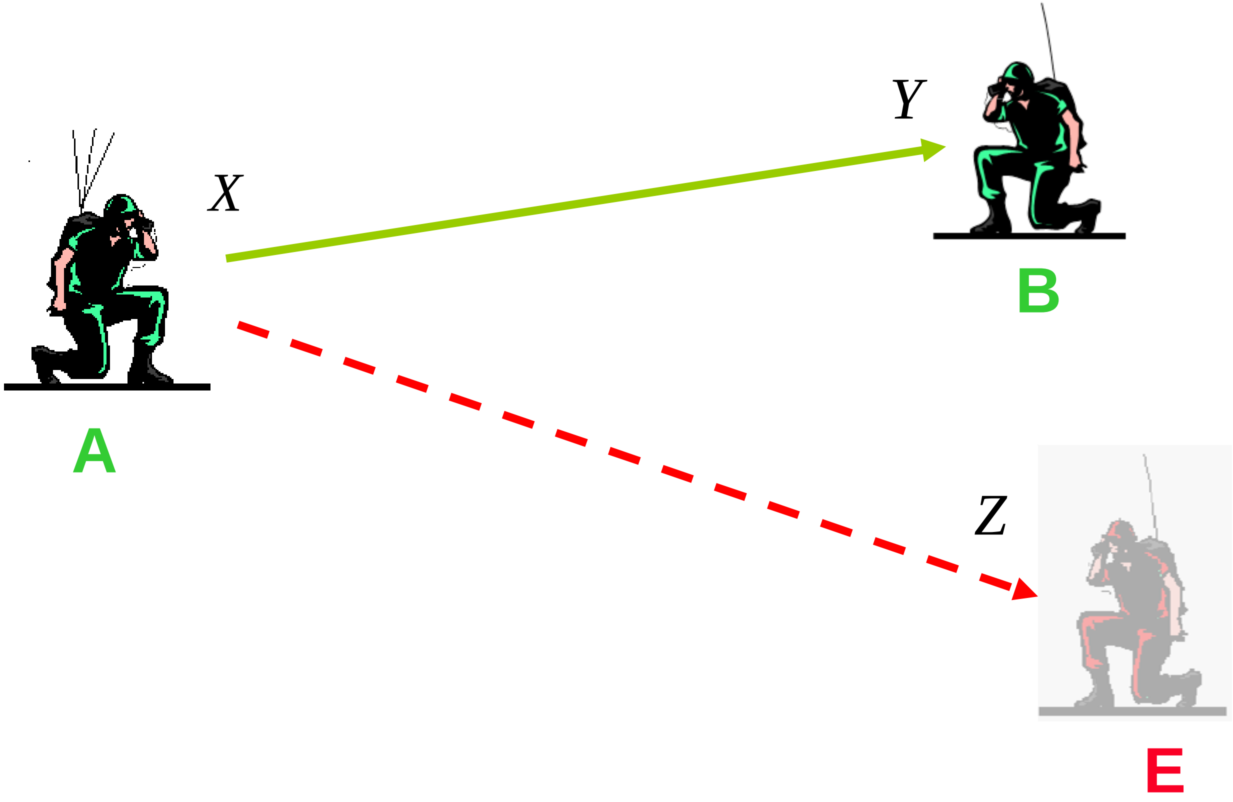


FOR UMD USE ONLY

Creating Channel Advantage

Use of multiple antennas

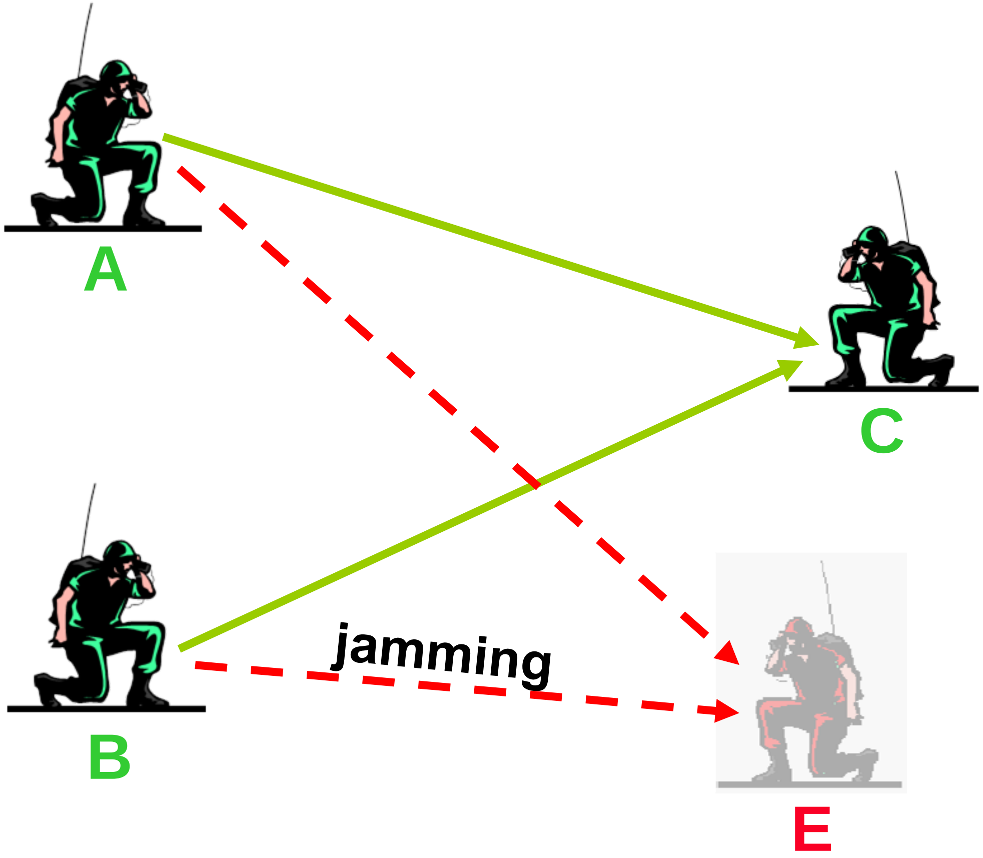
Spatial diversity



FOR UMD USE ONLY

Cooperation for Security

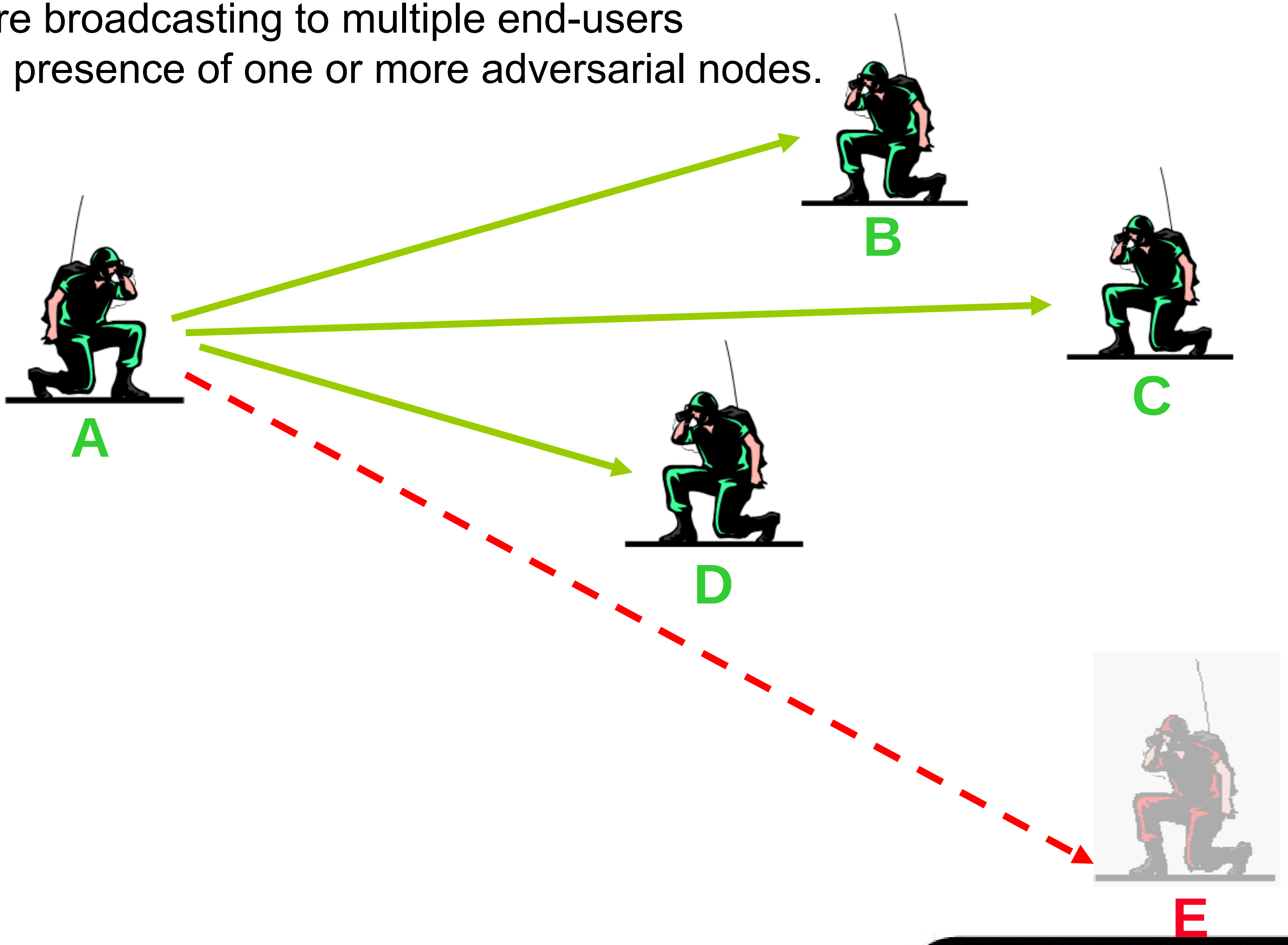
Cooperation using (or without using) overheard signals.



FOR UMD USE ONLY

Secure Broadcasting

Secure broadcasting to multiple end-users
in the presence of one or more adversarial nodes.

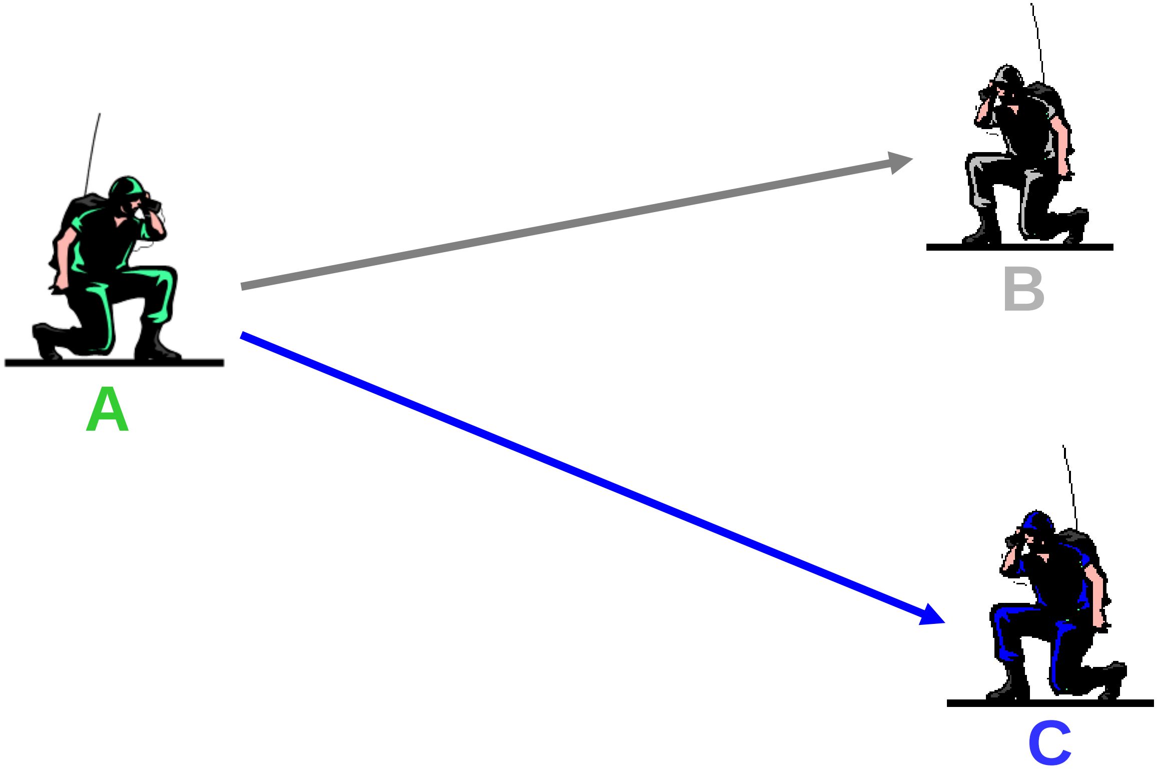


FOR UMD USE ONLY

Varying Security Clearance Levels

Both B and C are friendly nodes, but they have different security clearances.

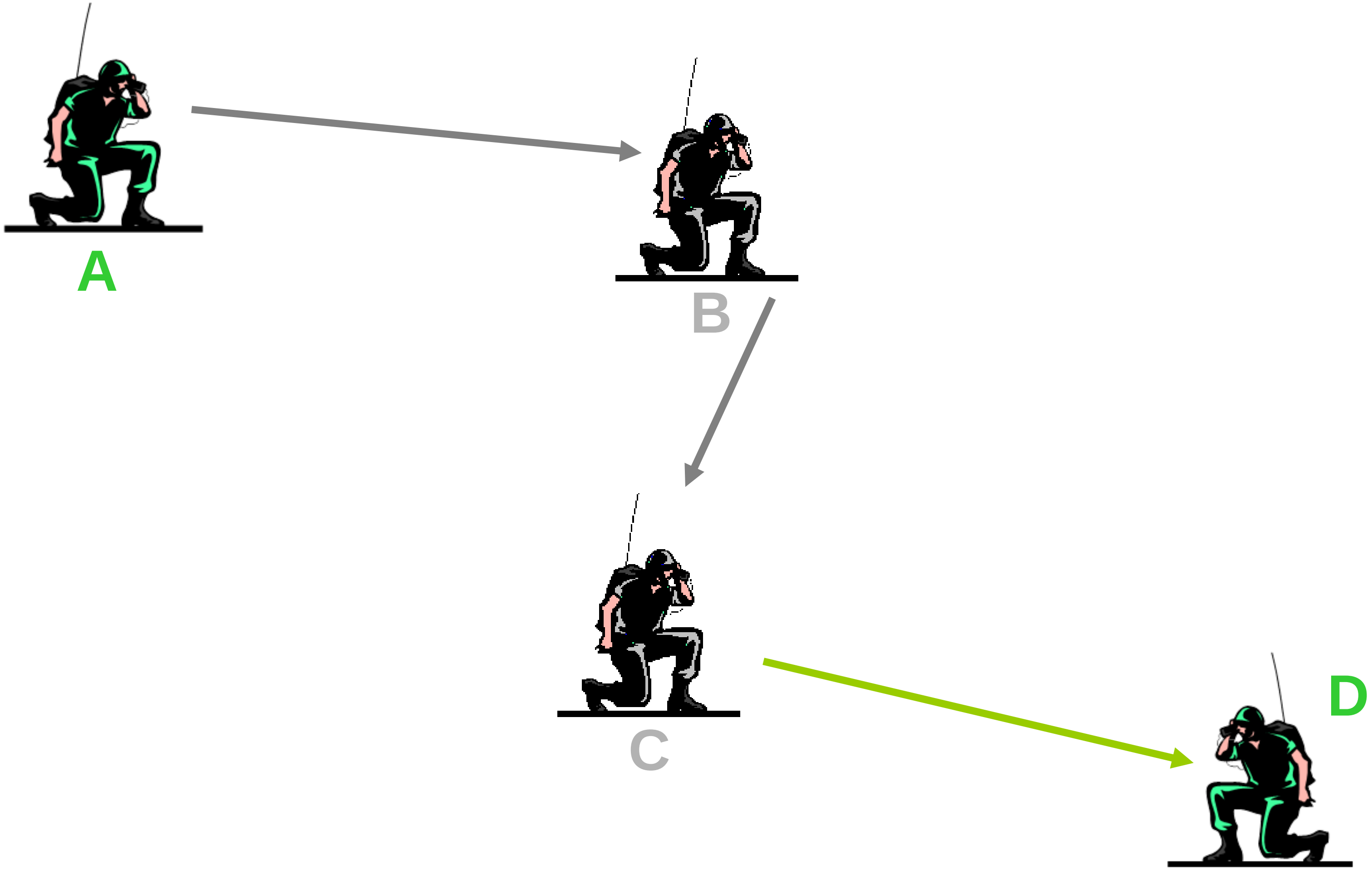
We can send secure information to B (un-decodable by C), and visa versa.



FOR UMD USE ONLY

Untrusted (but Friendly) Relays

Nodes B and C relay information without being able to decode its content.



FOR UMD USE ONLY

Conclusions

Physical-layer security is powerful:

- ❑ no limitation on adversary’s computation power or available information
- ❑ **provable, quantifiable** (bits/sec/hertz) and **implementable**

Many open problems:

- ❑ explicit code constructions
- ❑ implementing in the existing infrastructure
- ❑ better modeling adversary – e.g., active adversaries
- ❑ robust modeling of adversary – e.g., no CSI
- ❑ combining with cryptography
- ❑ …

Contact me with questions/comments/ideas:

Sennur Ulukus **ulukus@umd.edu** **http://www.ece.umd.edu/~ulukus**

FOR UMD USE ONLY