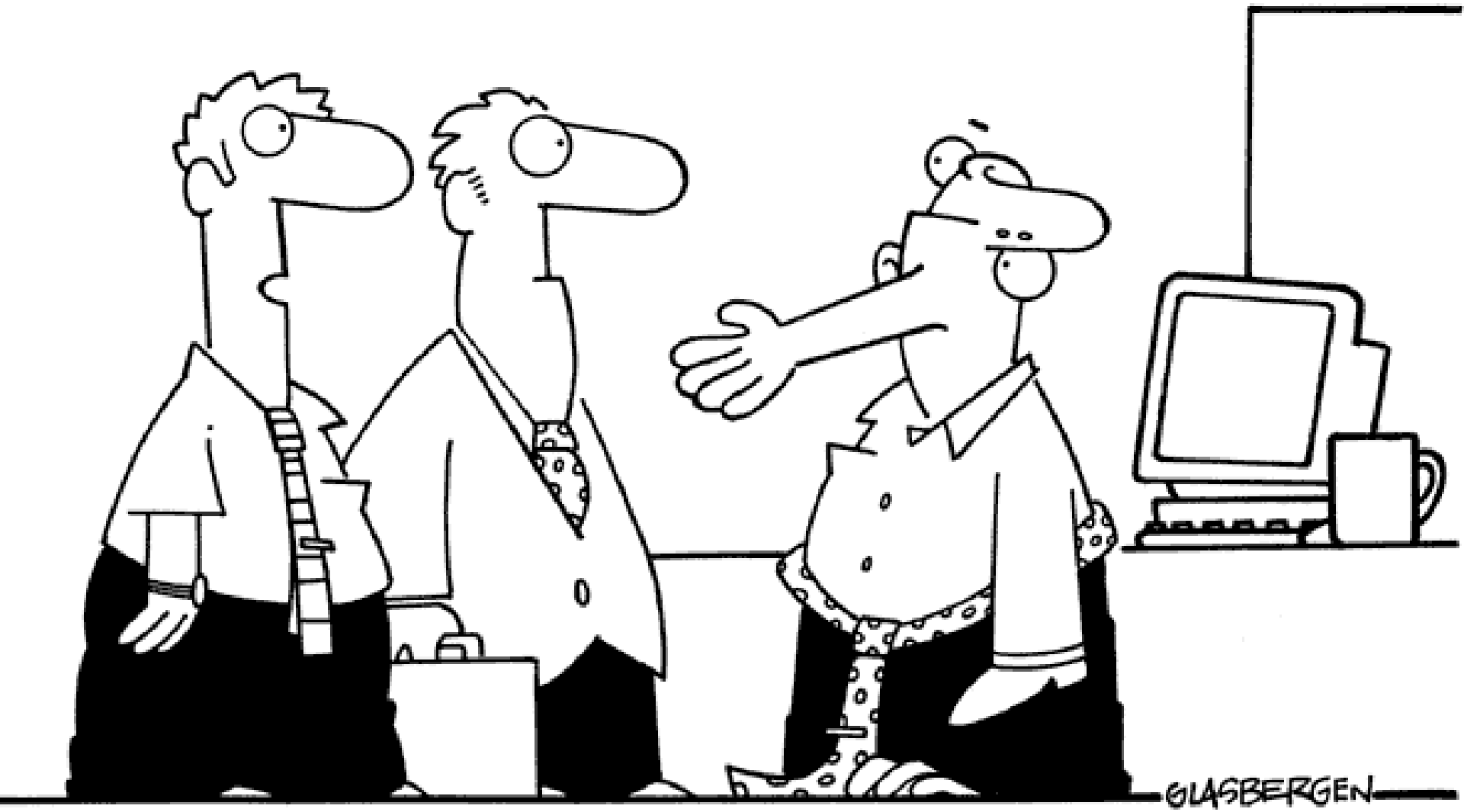
Secrecy level of communication under Uncoordinated Frequency Hopping (UFH)

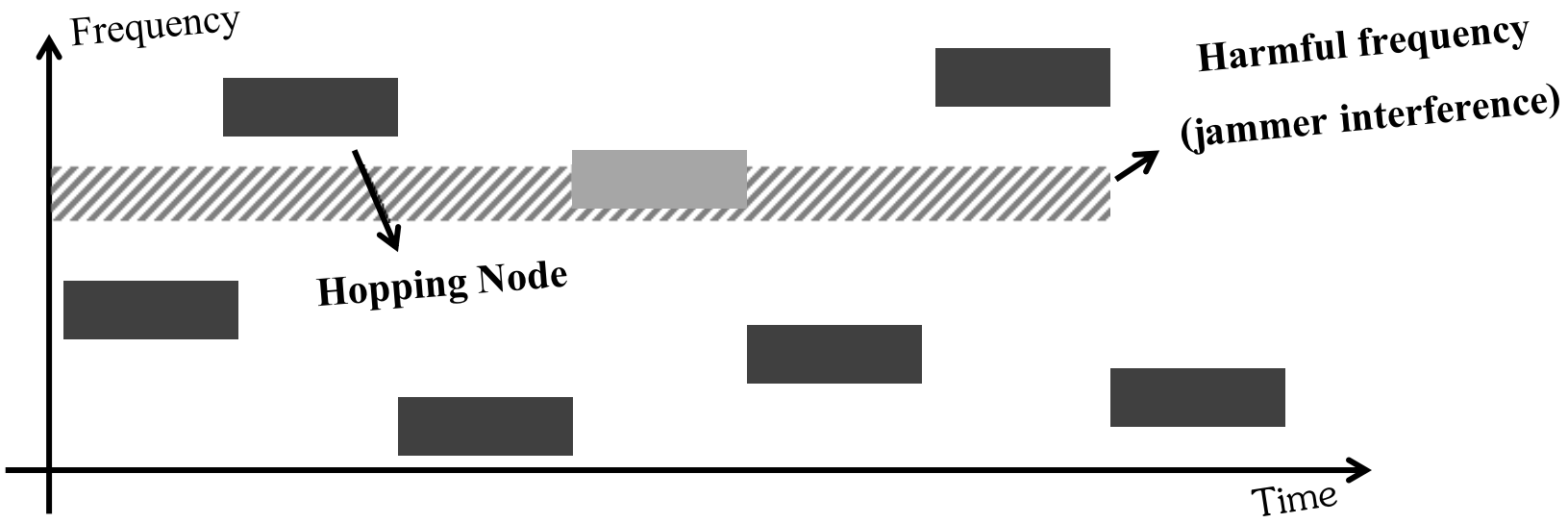
Authors: João André Sá & João Vilela

CISUC/DEI – Universidade de Coimbra

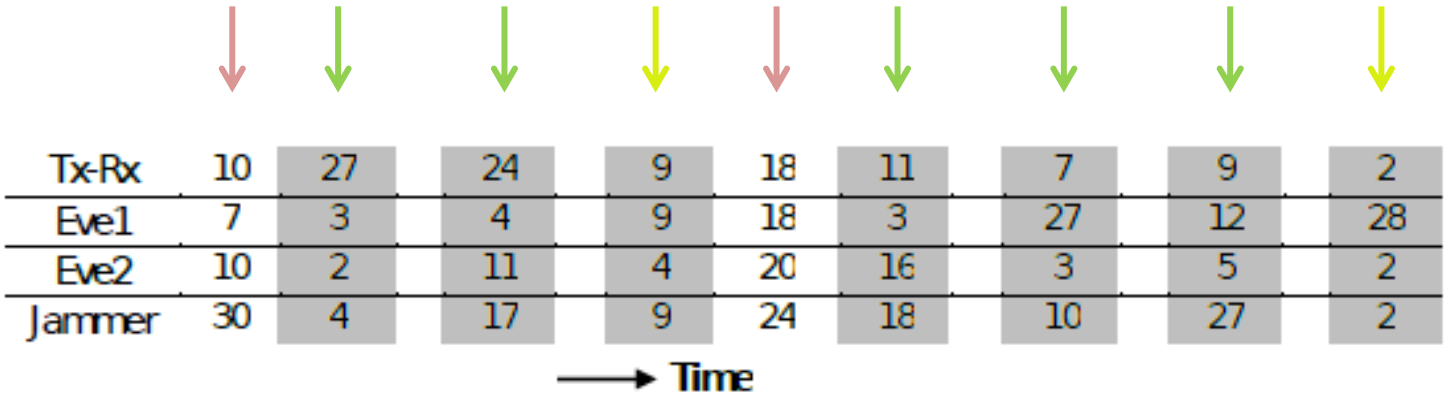


"That's our CIO. He's encrypted for security purposes."

Uncoordinated Frequency Hopping (UFH)



From: M. Strasser, C. Popper, S. Capkun, and M. Cagalj, *"Jamming-resistant key establishment using uncoordinated frequency hopping,"* in IEEE Symposium on Security and Privacy, 2008, pp. 64–78.



Won't the jammers interfere with Tx-Rx communication?

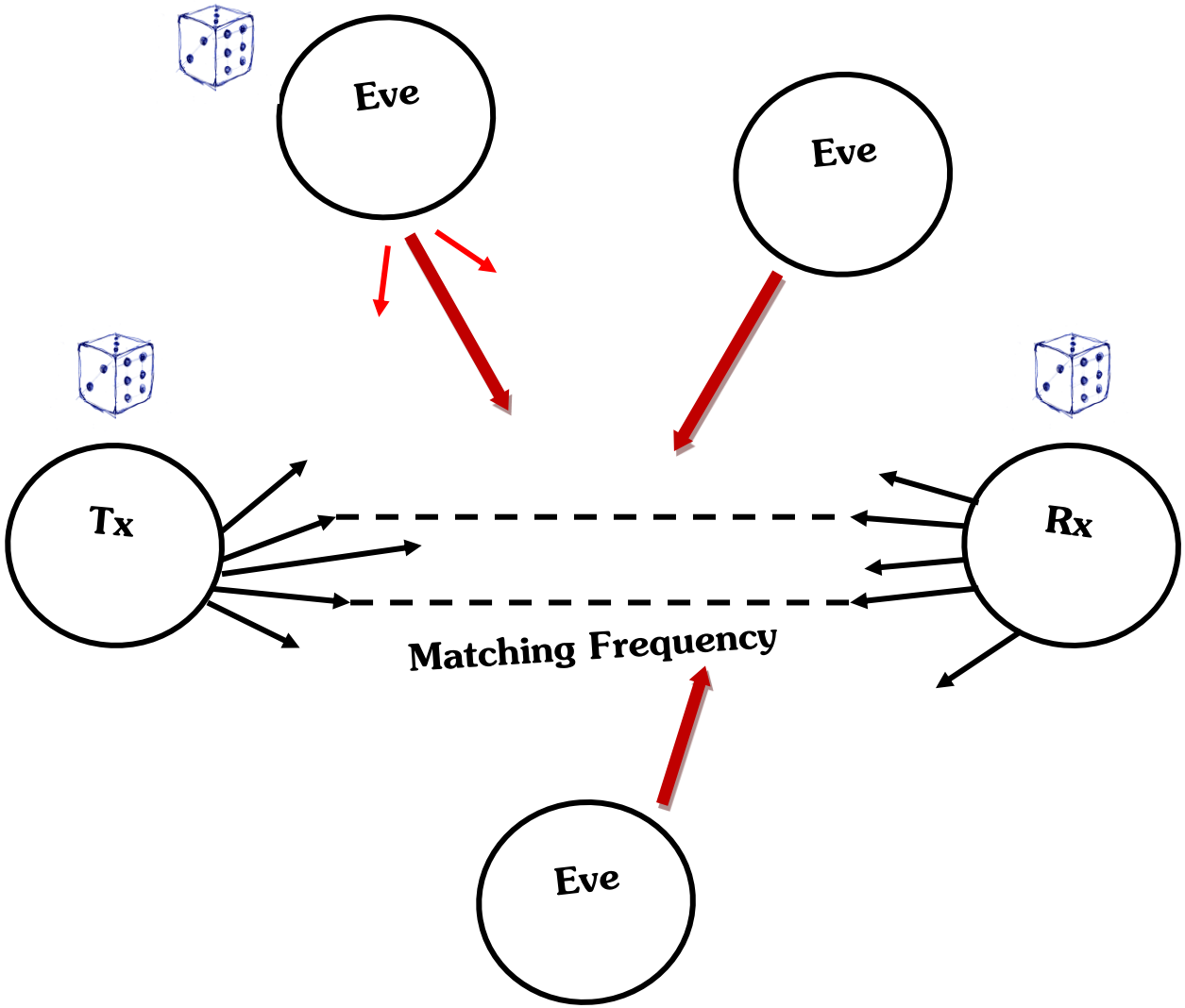
System Setup

- 2 Nodes (identical)
- Rx and Tx
- UFH Communication paradigm
- K eavesdroppers
- J Defensive Jammers

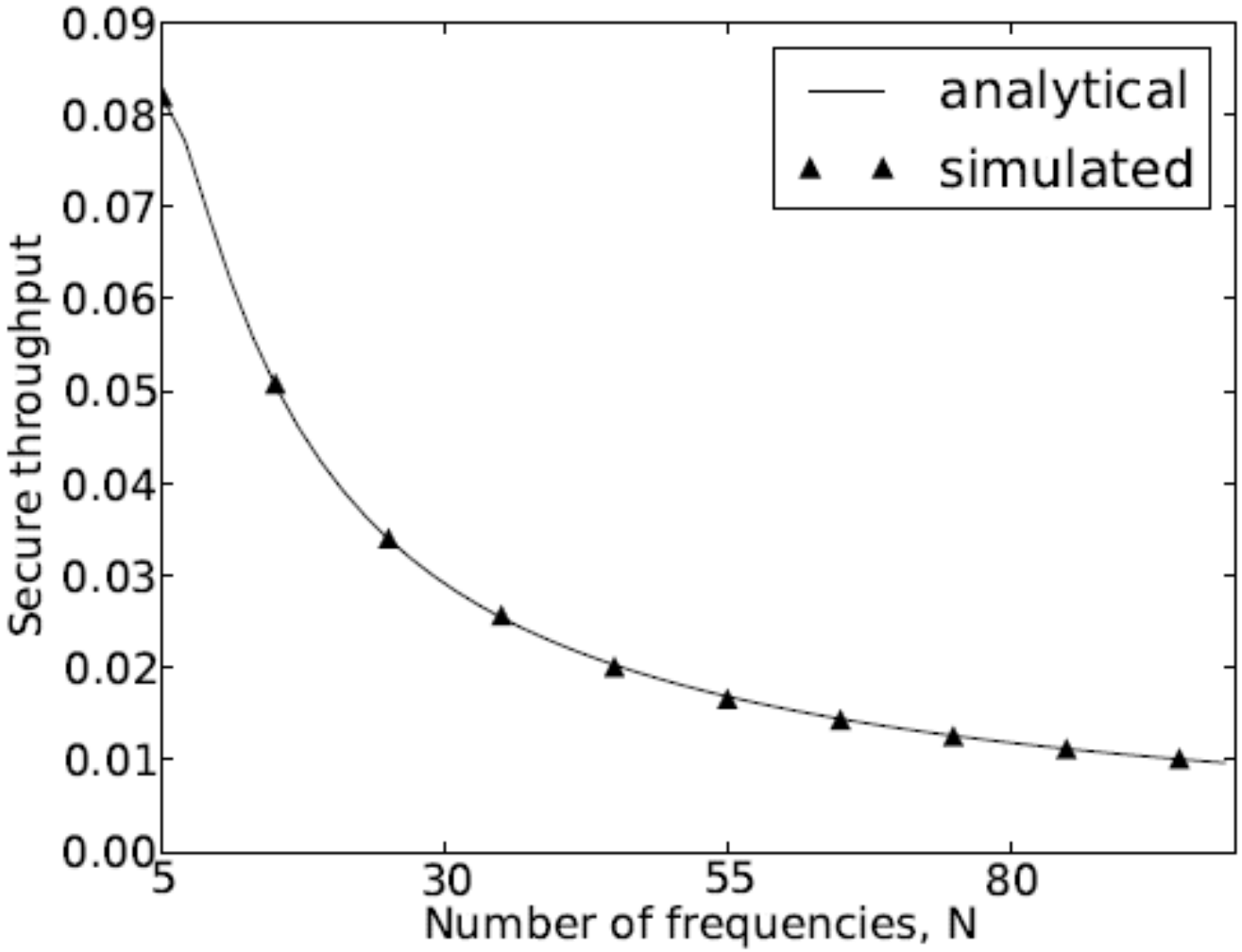
$$\mathcal{T}_s \triangleq \mathbb{P}\left\{ \mathrm{Tx} \rightarrow \mathrm{Rx} \ \wedge \bigwedge_{e_i \in \Pi_e} \mathrm{Tx} \nrightarrow e_i \right\}.$$

Secure Throughput

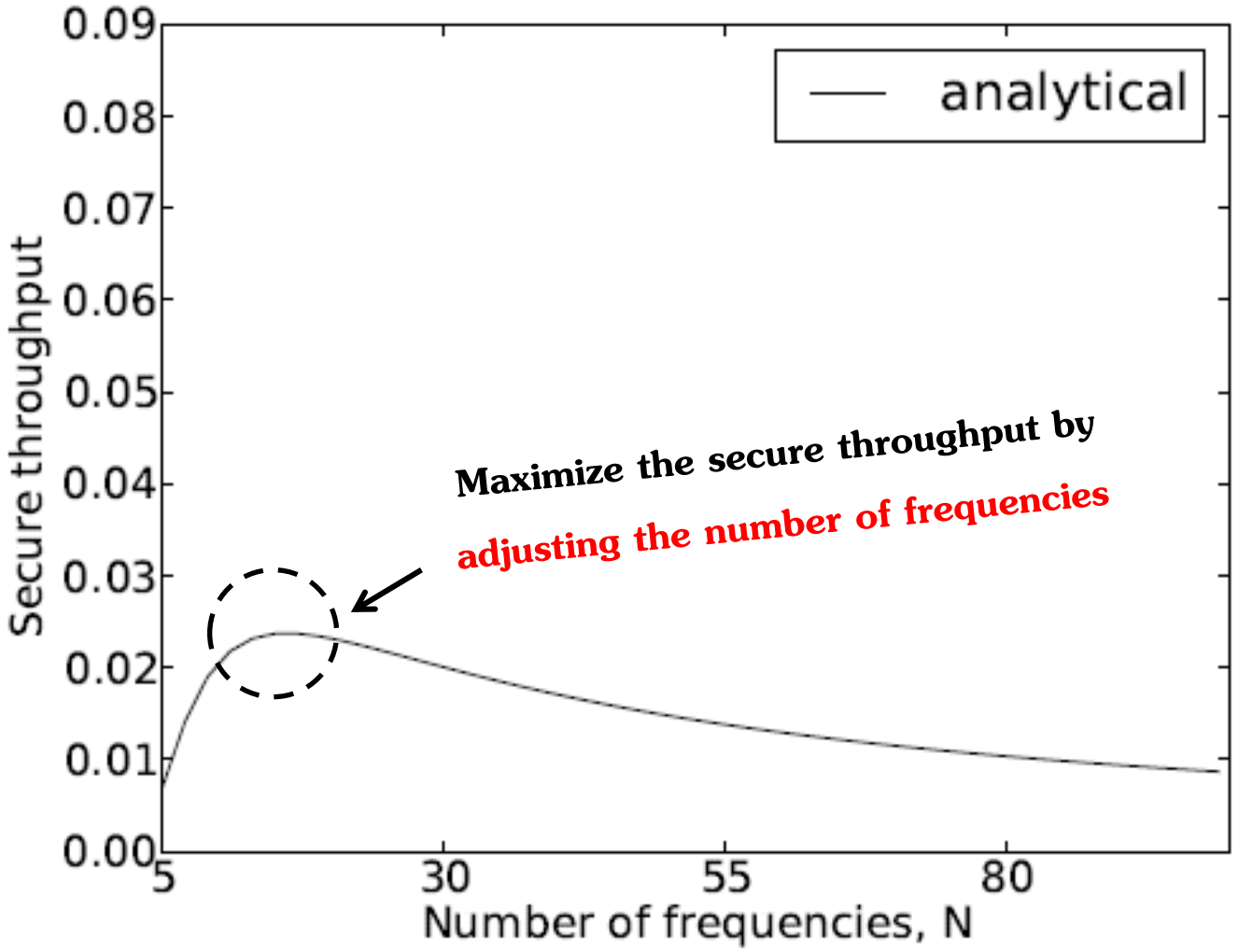
Cenario I



Secure Throughput for K=4 Eavesdroppers



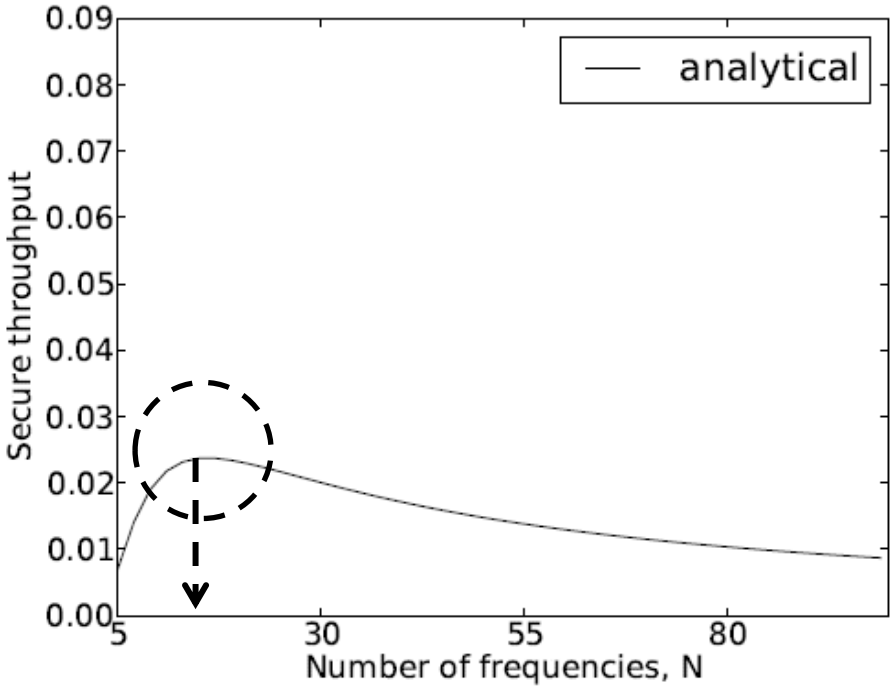
Secure Throughput For K=15 Eavesdroppers



Maximize Secure Throughput

$$\mathcal{T}_s = \frac{N \times (N-1)^K}{N^{K+2}}$$

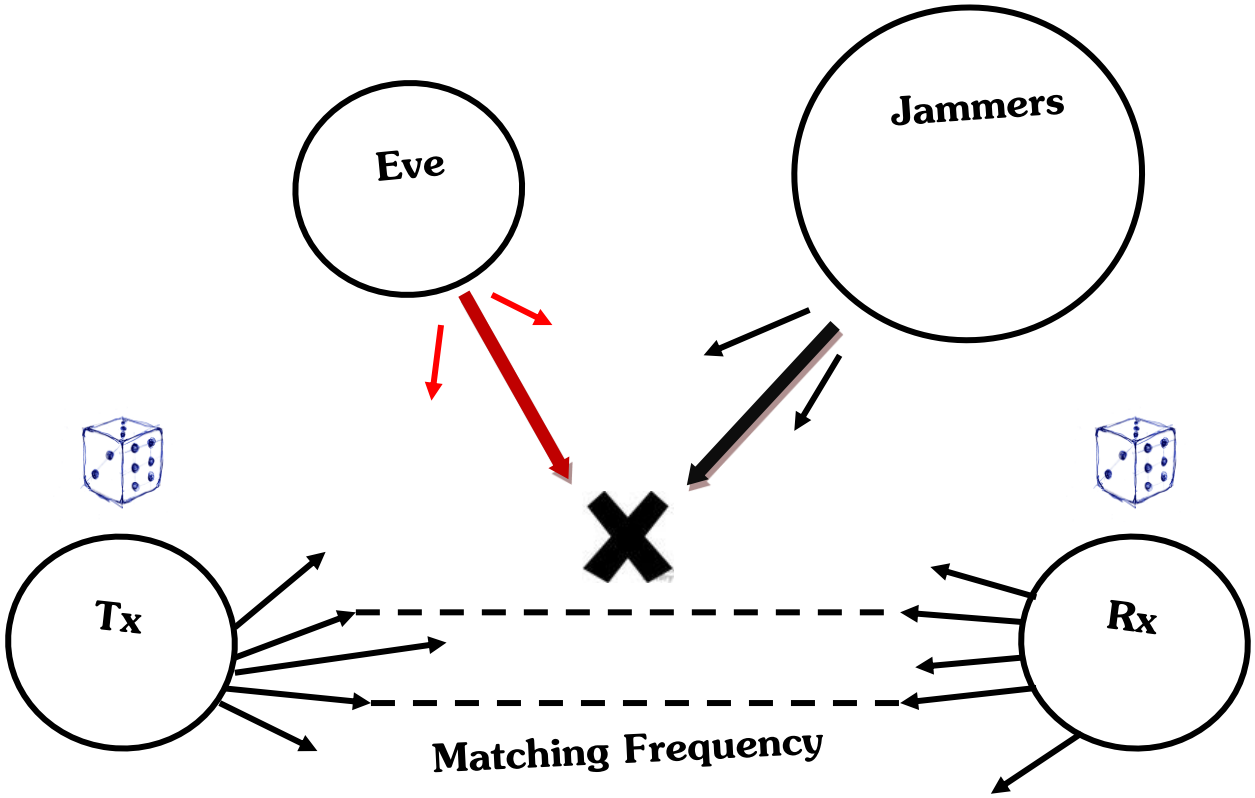
Maximize the secure throughput by blocking K (eves) and adjusting N (frequencies)



MAXIMUM

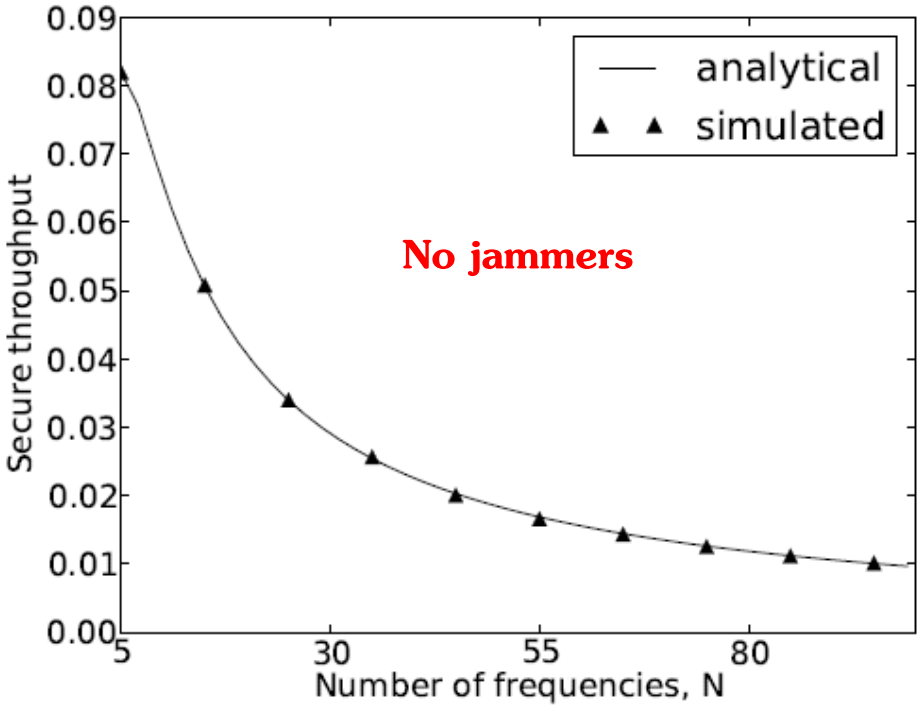
N=K+1

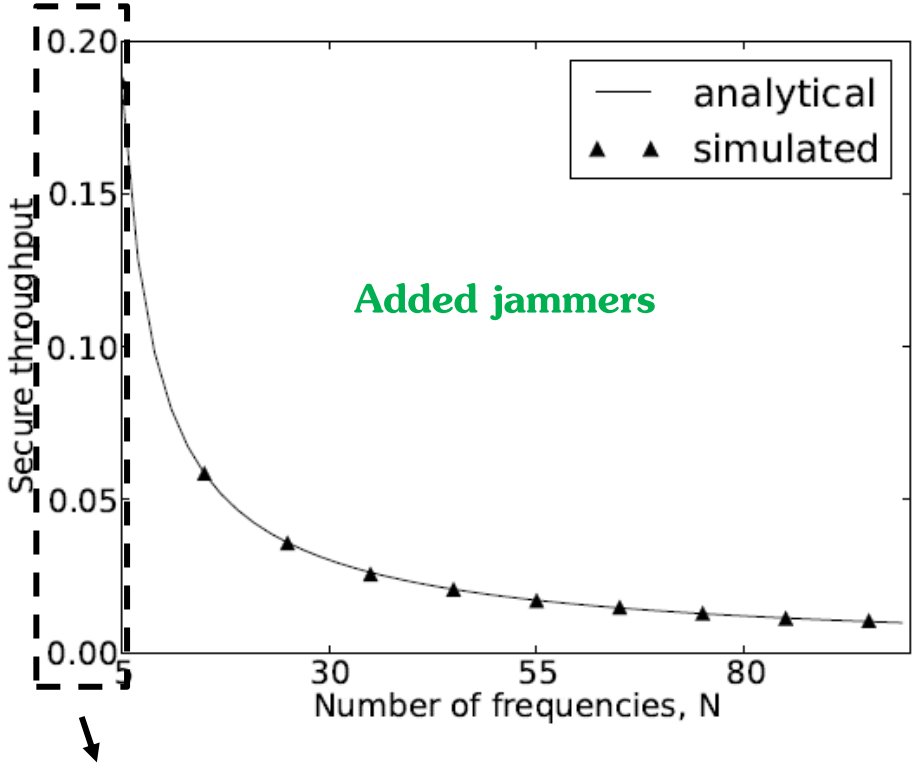
Cenario II



Comparing Secure Throughput

K=4 Eavesdroppers and J=5 jammers

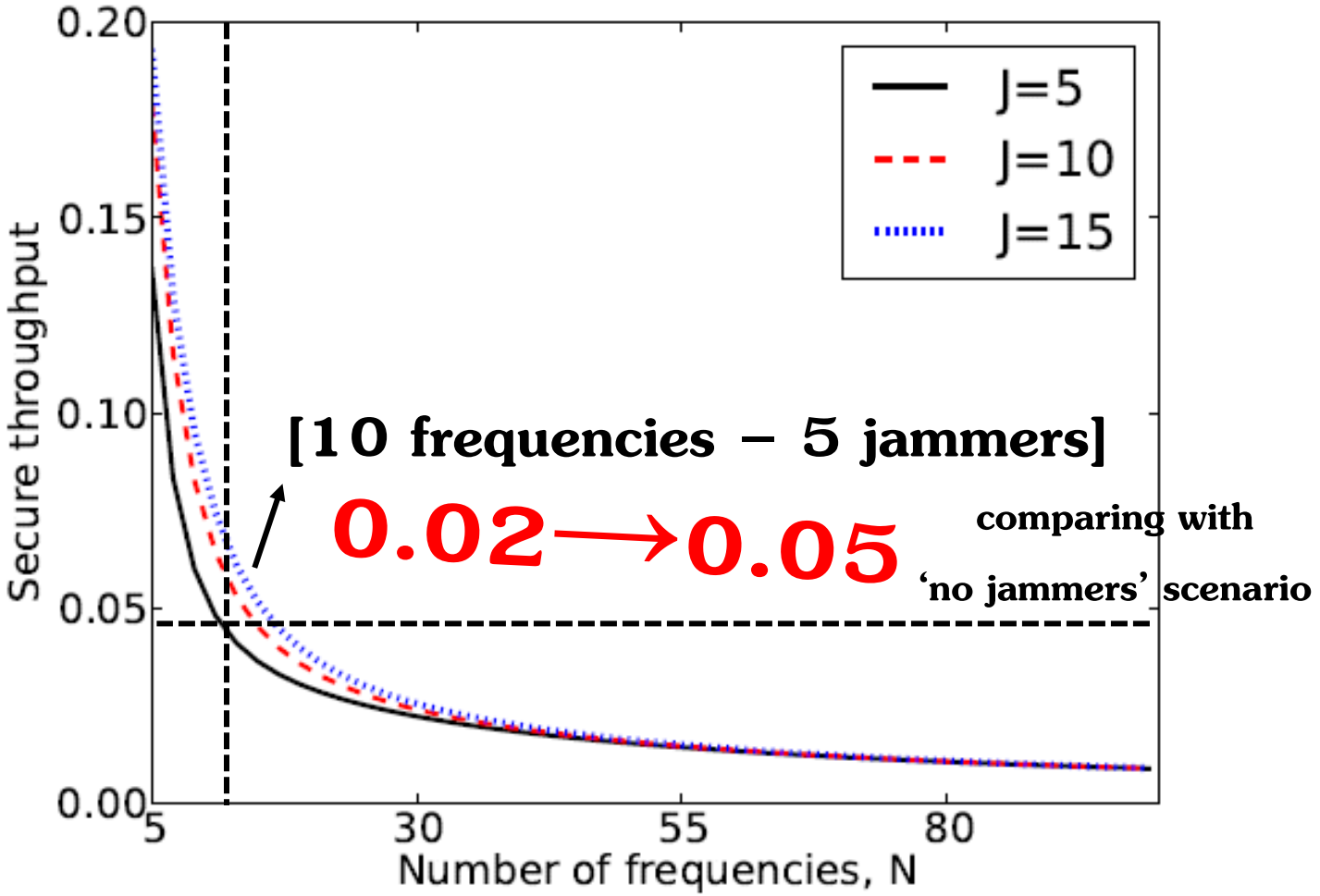




Adding jammers **dramatically increases** the secure throughput (for lower sets of frequencies)

Secure Throughput for

K=15 Eavesdroppers and J=5,10,15 Jammers



Conclusion

Increase in the secure throughput which allows a more efficient and realiable UFH mechanism.

Defensive Jammers

Maximized throughput

Adjusting the number of frequencies can help improve performance in scenarios were there are no defensive agents (N=K+1).

Performance

Small secure throughput values does not necessarily mean bad performance → higher protection for key exchange.

Future Work

- Degradation factor
- Different hoping rates
- Test bed implemantation