Intelligent Transportation Systems: A case of Jamming Attacks

Axel Krings

Ahmed Serageldin & Hani Alturkostani

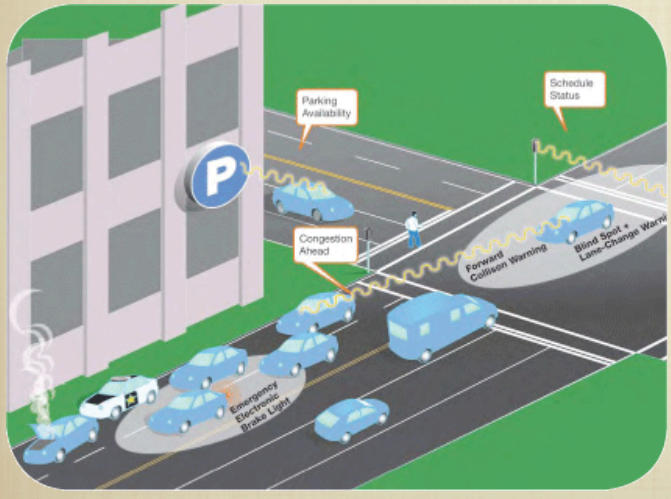
This research was supported by grant DTFH61-10-P- 00123 from the Federal Highway Administration - US DoT

On the Reliability of DSRC Safety Applications: A Case of Jamming

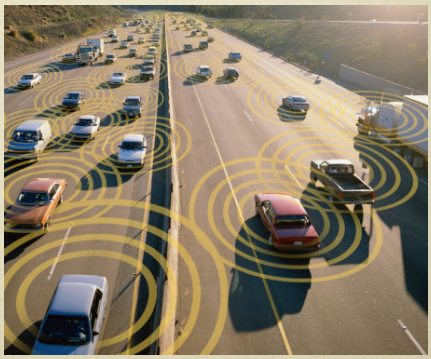
Ahmed Serageldin, Hani Alturkostani and Axel Krings
Department of Computer Science
University of Idaho
Moscow, ID 83843-1010
Email: Sera1405@vandals.uidaho.edu, altu2655@vandals.uidaho.edu, krings@uidaho.edu

ITS and Cyberspace

- IntelliDrive & Connected Vehicles



Toll rate displayed on variable message sign

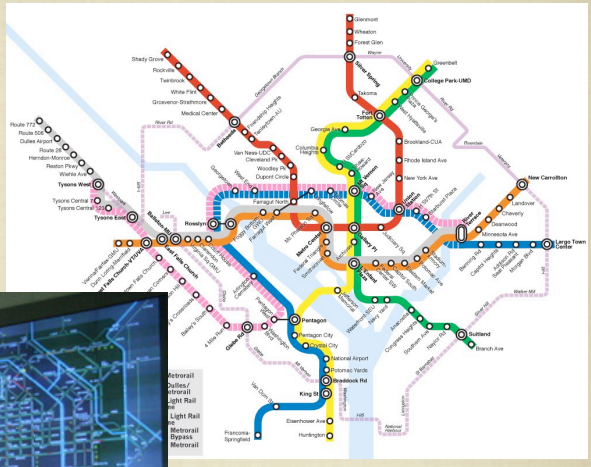


ITS and Cyberspace

- Aging Population

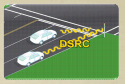
ITS and Cyberspace

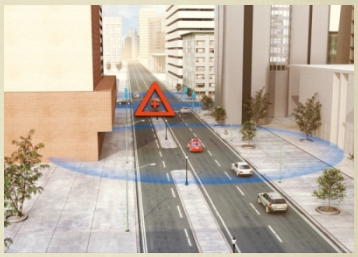
- Traffic Management



Potentials

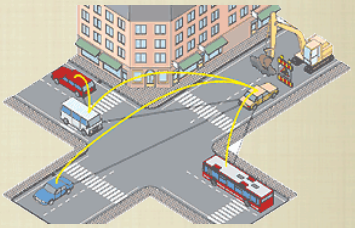
- Include communication from vehicles to the infrastructure
  - approaching emergency vehicles
  - medical conditions
  - oncoming hazards
  - traffic statistics
  - in-vehicle signing
  - etc.

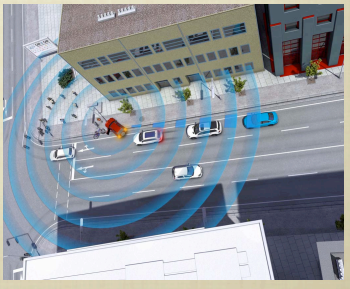




Potentials cont.

- Include communication from infrastructure to vehicles
  - notifications about surface conditions
  - communicate hazard to vehicles in vicinity
  - notifications about safety threats
  - communicating route changes
  - location service
  - vehicle safety inspection
  - etc.





What do they all have in common?

- Safety concerns
- Reliability concerns
- Availability concerns

What do they all have in common?

- They operate in an unbounded system environment affected by problems related to
  - computer and network security
  - system fault-tolerance
  - survivability

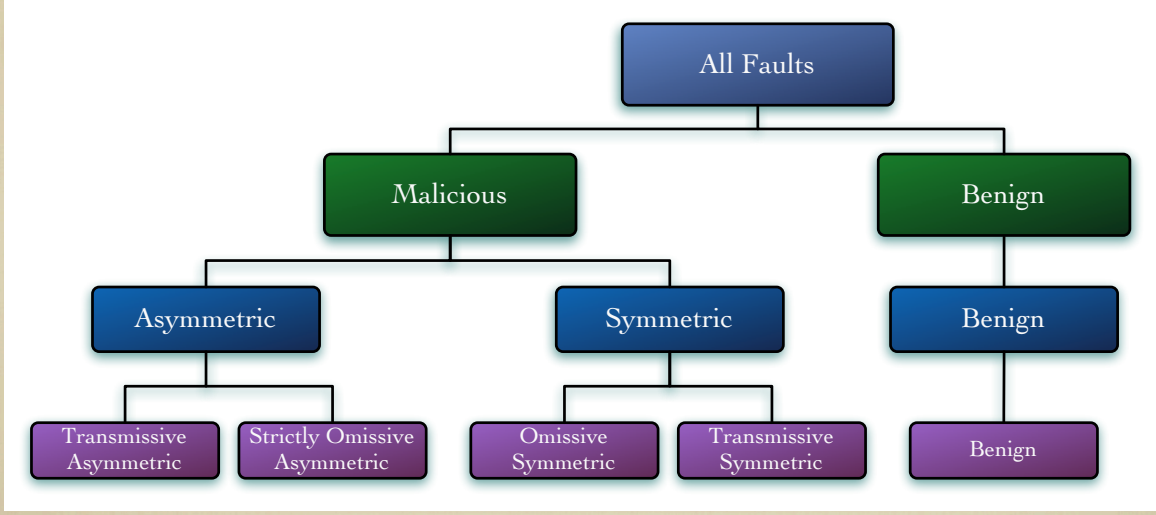
What do they all have in common?

- Public support would be vastly damaged by
  - system failure ...leading to safety violations
  - cyber attacks ...leading ...
  - malicious act ...leading ...

What assumptions should one place on a system?

- Anything is possible!
  - and it <u>will</u> happen!
- Faults will occur sooner or later
- Malicious act will occur sooner or later
- It is hard or impossible to predict the behavior/time of an attack

Fault Models:
The world in which we live/operate



Terminology

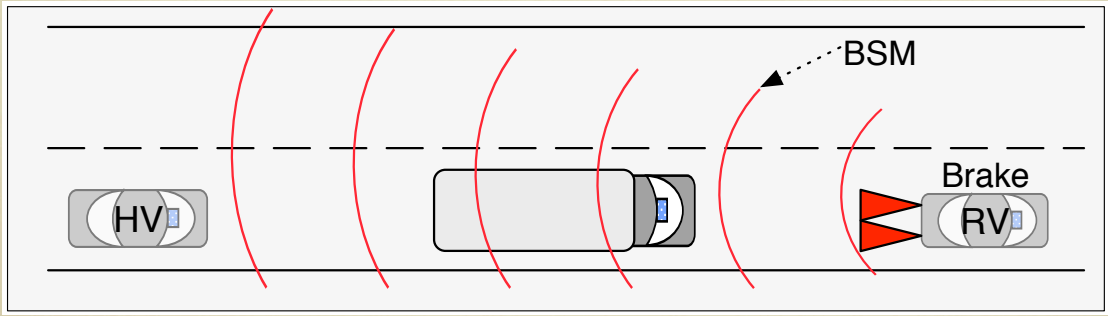
- Intelligent Transportation Systems (ITS)
- Vehicular ad hoc Networks (VANET)
- Dedicated Short Range Communication (DSRC)
- Media Access Control (MAC)

DSRC Channel Allocation

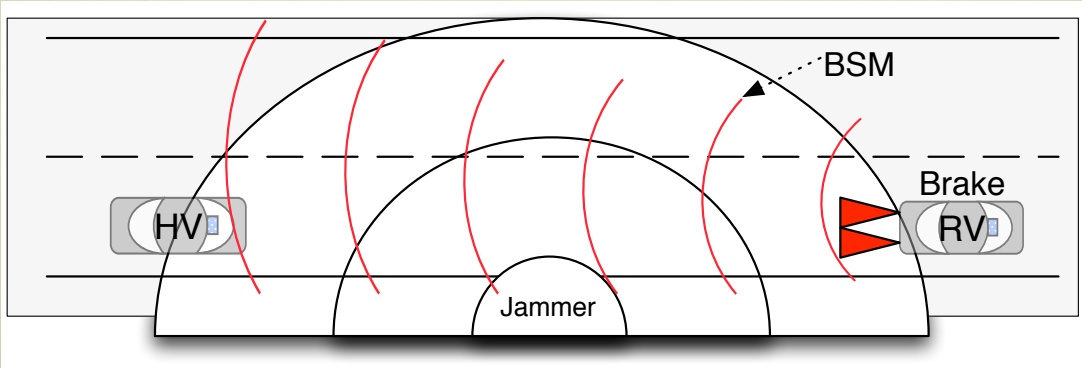
Channel Number		Channel Use	Bitrate (Mbps)		Bandwidth (MHz)		Frequency Range (GHz)
CH170		Reserved	-		5		5.850 - 5.855
CH172		SCH	3-27		10		5.855 - 5.865
CH174	CH175	SCH	3-27	6-54	10	20	5.865 - 5.875
CH176		SCH	3-27		10		5.875 - 5.885
CH178		CCH	3-27		10		5.885 - 5.895
CH180	CH181	SCH	3-27	6-54	10	20	5.895 - 5.905
CH182		SCH	3-27		10		5.905 - 5.915
CH184		SCH	3-27		10		5.915 - 5.925

Forward Collision Warning

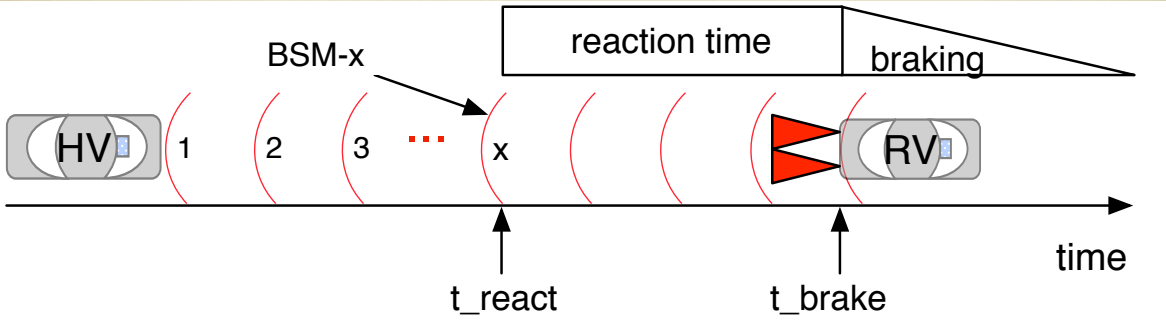
- Basic Safety Message
  - 100ms broadcast interval
  - 300m range
  - contains many parameters about the vehicle
  - is THE message for safety applications!



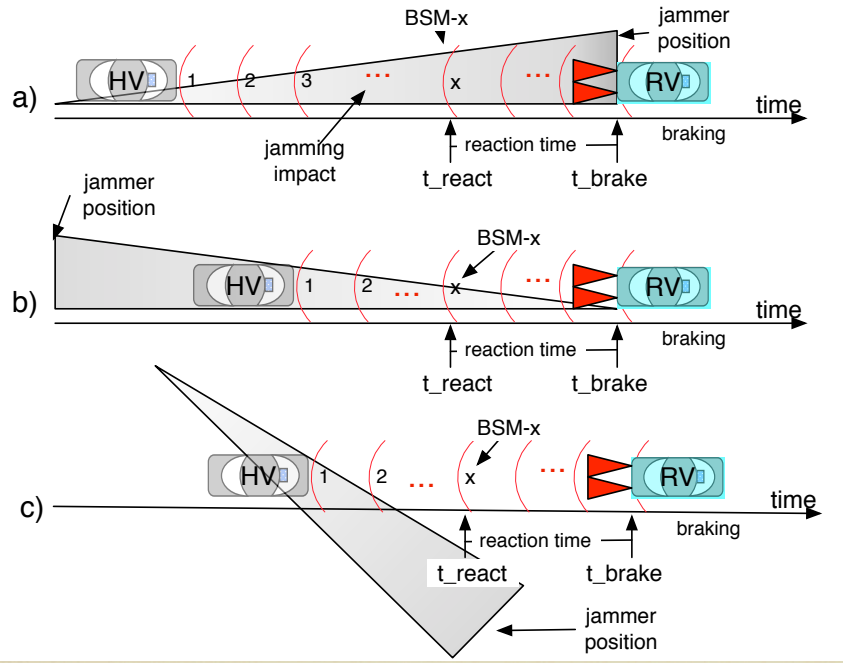
Forward Collision Warning with Jamming



Timing & Distances



Jammer Positions



Jamming

- The Issue of Power and Detection
  - Constant Jammer
  - Random Jammer
  - Deceptive Jammer
  - Reactive Jammer
  - Intelligent Jammer

Constant Jammer

This type of jammer emits a constant radio signal interfering with legitimate communication, violating the underlying MAC protocol. This is considered the worst case of jammer by many researchers as it indiscriminately affect the signal of ongoing communication. However, it is the least energy efficient and is relatively easy to detect and locate.

Random Jammer

Here the attacker jams for t_j and sleeps for t_s seconds. The jam and sleep periods may be unpredictable, e.g., t_j and t_s can be samples of two random variables T_j and T_s, respectively, following different distributions [10]. Random jammers consume less energy than constant jammers, but can be harder to detect.

Intelligent Jammer

This type of jammer, sometimes called a "Protocol Aware Jammer", can target specific message types or selected messages, and can be used in sophisticated attack scenarios. It is extremely difficult to detect and very energy efficient.

Application Reliability

How does one get the application reliability ?

Or should we look at Unreliability?

Application Reliability

Since the application fails only if no BSM message is received before t_{react}, we use the unreliability $Q(t) = 1 - R(t)$, i.e., the probability of all x messages being lost, which is

$$Q(t) = \prod_{1}^{x} Q_i(t_i) \tag{1}$$

where Q_i is the probability that BSM message i was not received, i.e., the packet error probability of BSM$_i$, and t_i is the time BSM$_i$ should be received.

Jamming-to-Noise Ratio

$$\frac{J}{R} = \frac{P_j G_{jr} G_{rj} R_{tr}^2 L_r B_r}{P_t G_{tr} G_{rt} R_{jr}^2 L_j B_j} \quad (2)$$

Subscript j refers to the jammer, r to the receiver and t to the transmitter
Transmission power of node x is denoted by P_x,
Antenna gain from node x to y is G_{xy}
Distance between nodes x and y is R_{xy}
Communication link's signal loss is L_r
Jamming signal loss is L_j
Nodes x bandwidth is B_x

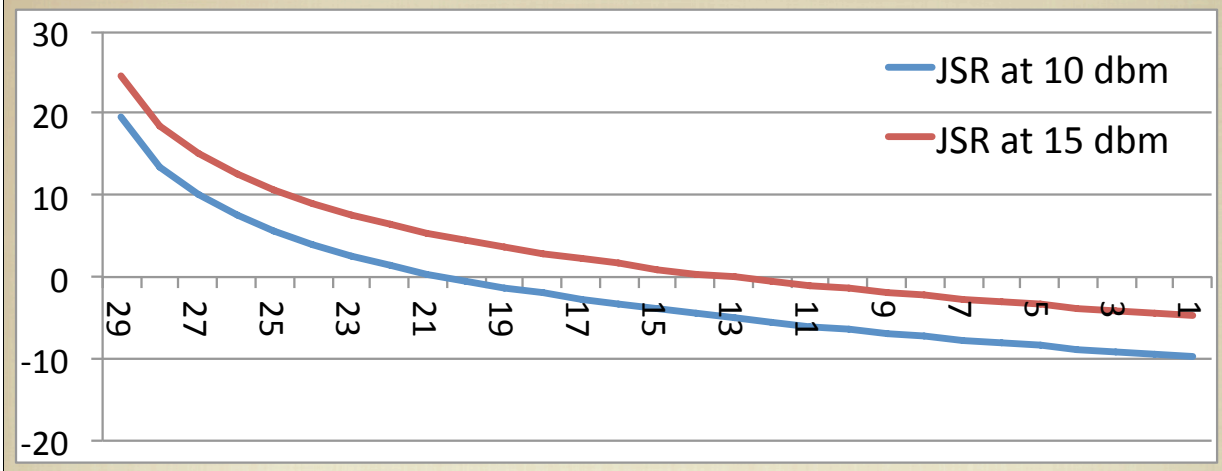


Fig. 5. Jamming-to-signal ratio in dB related to messages BSM_i

6Mbps CS172 uses QPSK

$$P_b = \frac{1}{2} erfc\left(\sqrt{\frac{E_b}{N_0}}\right)$$

This is related to the SNR by

$$\frac{E_b}{N_0} = SNR\frac{B}{R}$$

Packet Error Probability

The packet error probability P_p is now derived as

$$P_p = 1 - (1 - P_b)^N \tag{7}$$

where N is the number of bits of the BSM message. We use $N = 1500$ bits as an approximation for the message length. The packet error rate P_p is the unreliability Q_i used in Equation 1.

FCW Application Unreliability

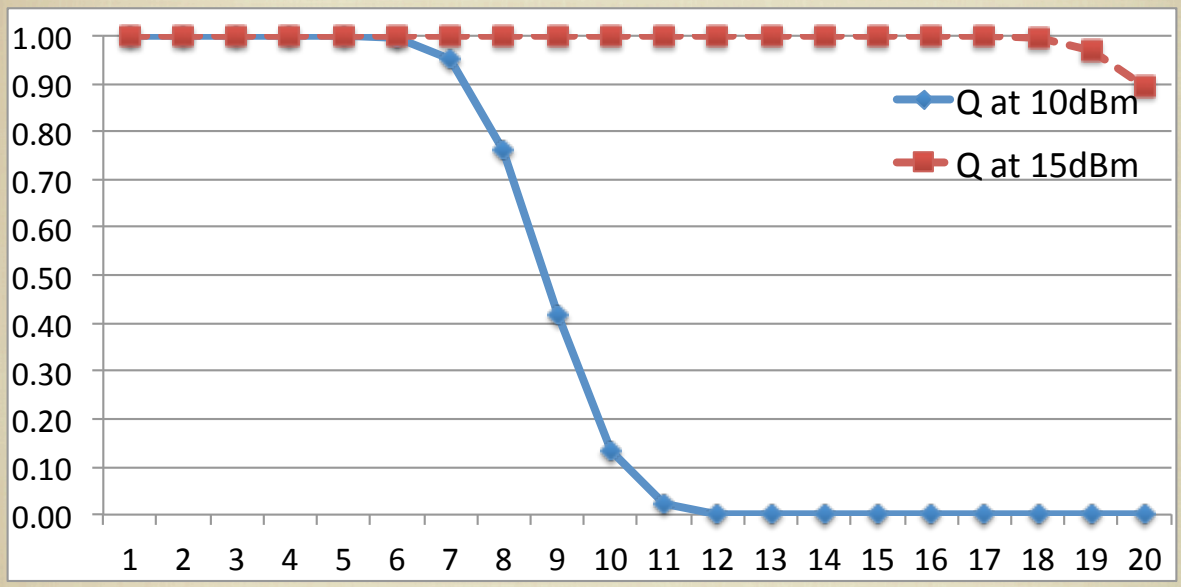


Fig. 6. $Q(t)$ under constant jamming over number of BSM messages sent

Random Jammer

How does one get the application reliability in this case?

Recall: Random Jammer

Here the attacker jams for t_j and sleeps for t_s seconds. The jam and sleep periods may be unpredictable, e.g., t_j and t_s can be samples of two random variables T_j and T_s, respectively, following different distributions [10]. Random jammers consume less energy than constant jammers, but can be harder to detect.

Impact of Random Jammer

If a BSM message is sent during any sleep time before the reaction time t_{react}, the application reliability is at least as high as the probability of receiving that unjammed BSM message. Thus, the application unreliability as it is affected by random jamming is

$$Q_{rand}(t) = \prod_{1}^{x}(1 - P_s)Q_i(t_i) \tag{8}$$

where $Q_i(t_i)$ is the unreliability of BSM reception at t_i during jamming.

Probability of Sleeping

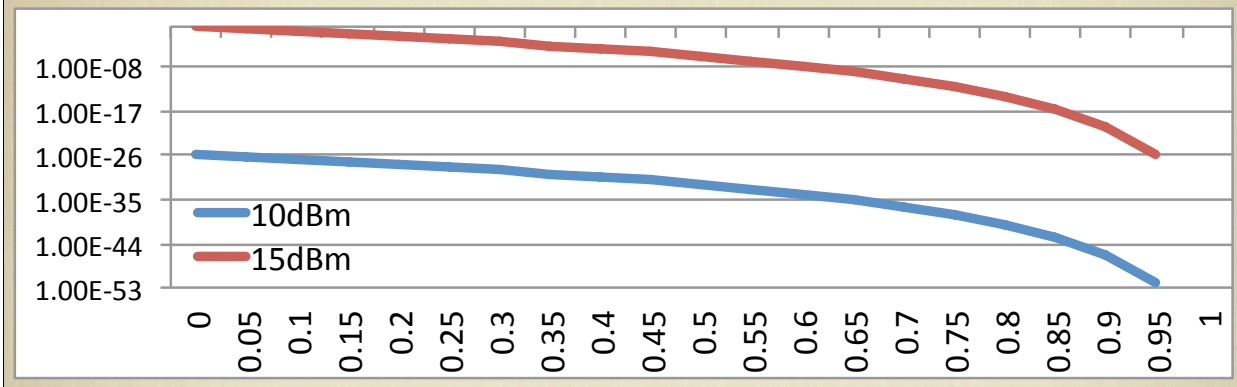


Fig. 7. Impact of sleeping probability on Q(t)

Redundancy

- Dissimilarity
  - using A la Carte Message (ACM)
  - using Probe Vehicle Data (PVD)
- Redundancy
  - BSM is limited to CH172
  - Use two separate radio devices
  - Control Channel CH178 (with ACM)
  - High power CH184 (with PVD)

Redundant Systems

How does on derive the reliability of a redundant system?

What are the assumptions one can make?

Impact of Redundancy

Considering only benign faults, a system consisting of N redundant subsystems S_i, $i = 1, .., N$, fails only if all N subsystems fail.

$$Q_N(t) = \prod_{1}^{N} Q_i(t) \tag{9}$$

Application Unreliability

$$Q_{dual}(t) = Q_{172}(t)Q_{178}(t)$$

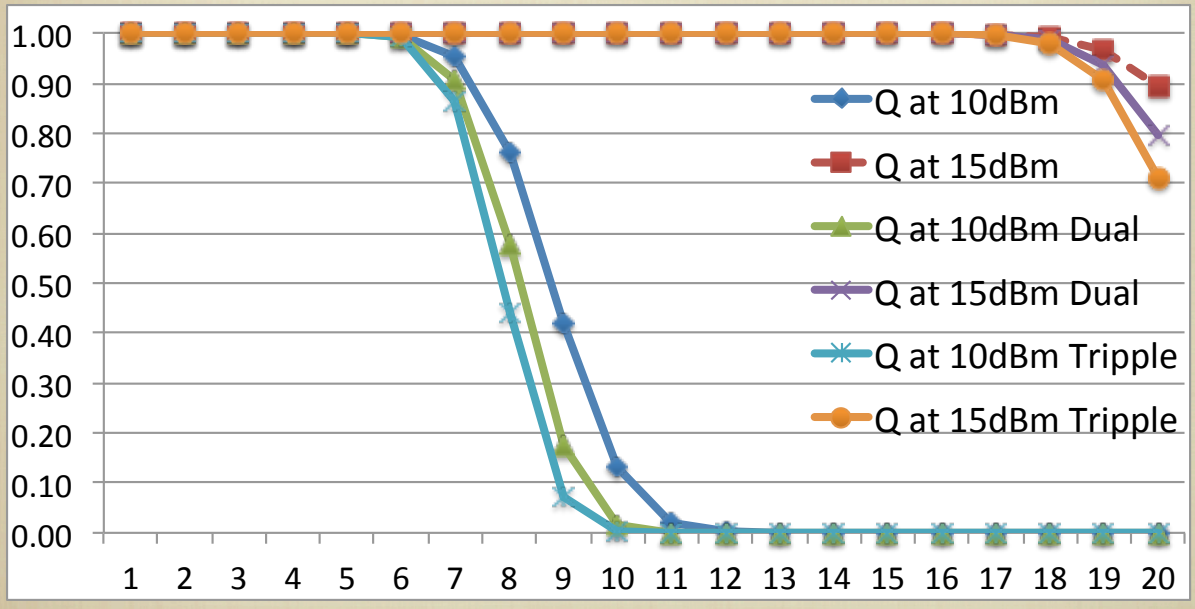
$$Q_{triple}(t) = Q_{172}(t)Q_{178}(t)Q_{184}(t)$$

if we assume that both channels have the same reliabilities

$$Q_{dual}(t) = Q(t)^2$$

$$Q_{triple}(t) = Q(t)^3$$

Impact of redundancy on Q(t)



Conclusion Quiz

- What was the main result w.r.t.
  - Constant Jammer
  - Reactive Jammer
  - Intelligent Jammer
  - Dissimilarity
  - Redundancy....?

Questions