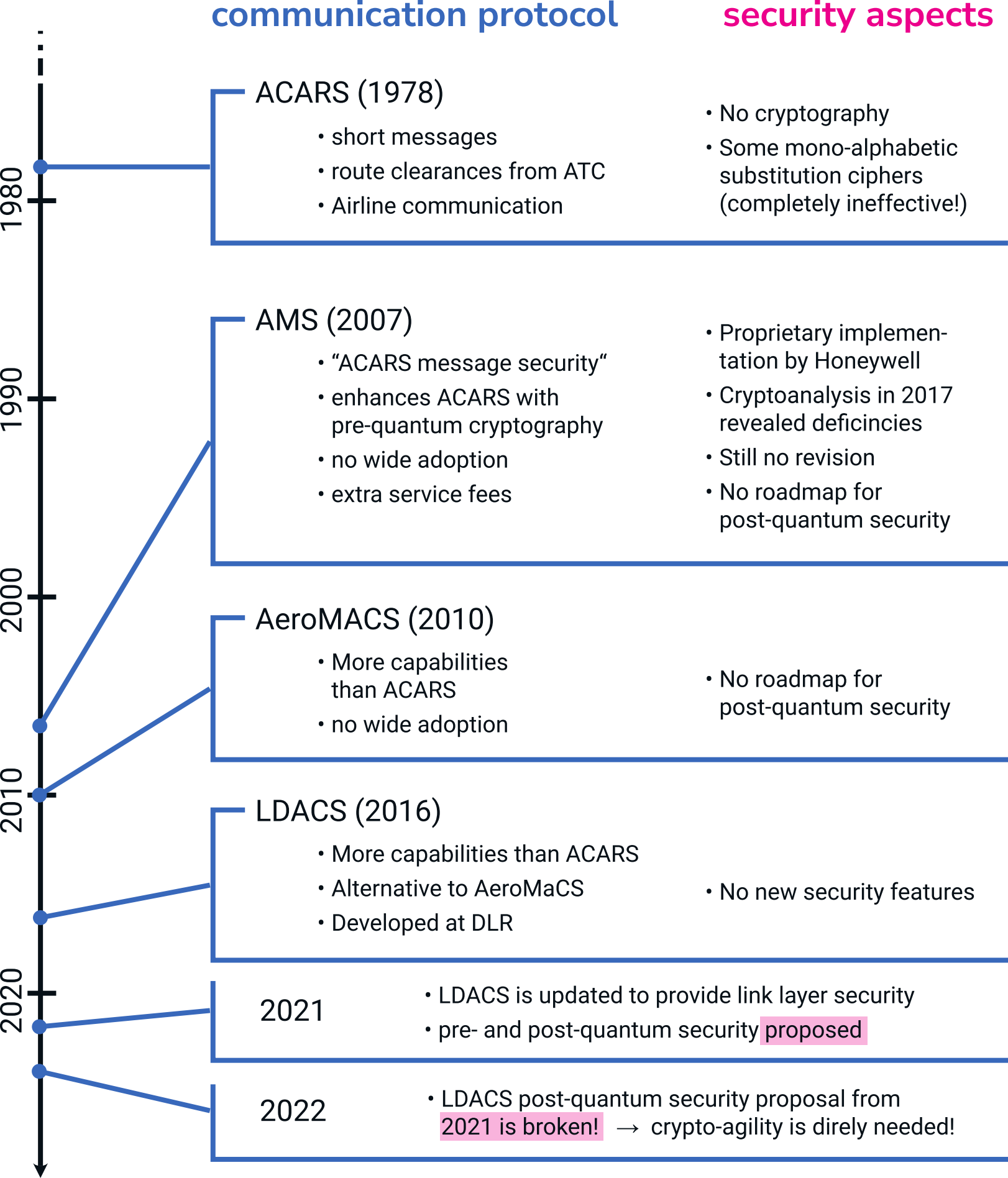
communication protocol
security aspects
1980
1990
2000
2010
2020
ACARS (1978)
• short messages
• route clearances from ATC
• Airline communication
• No cryptography
• Some mono-alphabetic substitution ciphers (completely ineffective!)
AMS (2007)
• "ACARS message security"
• enhances ACARS with pre-quantum cryptography
• no wide adoption
• extra service fees
• Proprietary implementation by Honeywell
• Cryptoanalysis in 2017 revealed deficincies
• Still no revision
• No roadmap for post-quantum security
AeroMACS (2010)
• More capabilities than ACARS
• no wide adoption
• No roadmap for post-quantum security
LDACS (2016)
• More capabilities than ACARS
• Alternative to AeroMaCS
• Developed at DLR
• No new security features
2021
• LDACS is updated to provide link layer security
• pre- and post-quantum security proposed
2022
• LDACS post-quantum security proposal from 2021 is broken! → crypto-agility is direly needed!