Architecting Wireless for Safety Critical Machine to Machine Communication

Michael Green argues that wireless communication in an increasingly crowded radio spectrum is inherently and increasingly hazardous for command & control operations. Machine to machine (m2m) / Internet of Things (IoT) communication between embedded devices is particularly at risk. As such 'critical' m2m messages sent over wireless should never be relied upon to be 'safely' received. All is not lost, in addition to best practice risk mitigation, new technologies are being applied to wireless that will ensure messages that get delivered can be more trusted, thus enabling safer sensing, command & control of assets at distance.

'Critical' messages over wireless ... what are they?

Referencing the work of Nancy Leveson & Dr John Thomas at MIT [1] on system safety, a 'critical message' within a system would be one that has potential to cause a significant 'loss' scenario, such as an "undesired or unplanned event that results in human injury or death, property damage, environmental pollution, mission loss, etc". To be safe, a 'critical message' must arrive from a trusted sender in time to be acted upon by the recipient.

'Critical' messages over wireless ... examples:

Definitely 'critical':

- Wireless remote control of individual aircraft, drones, vessels, vehicles, machinery and infrastructure
- Wireless control of assets in formation such as a platoon of trucks, a fleet of boats or a formation of drones such as a swarm
- Commands sent to assets operating autonomously, such as updated orders, status feedback or for firmware updates
- Sensing an alarm condition that will result in loss, such as a gas or radiation leak, intruder, fire alarm or a water level sensor
- Messages to/from medical devices where lives are dependent on those devices operating as intended

NB: for real time (millisecond) control, wired communication is typically used, but there are cases where wire is not an option. Where wireless is used, allowance should be made for latency, loss of connection, lost packets and retries.

"Unforeseen developments, unpredictable communication, changes in behaviours: The Arlington Report on the communication on 11 September 2001, the report on the hearings of the City of London after the events referred to as the 'London Bombings' in 2007, the lessons from the 2016 terrorist attacks in Brussels. Communication while working from home or quarantining, remote alerting in the coronavirus era – all these examples underscore the fact that mobile phones alone cannot be the only solution for communication in extreme situations." [2]

What it might also be (depending on the context):

- A message to a satellite commanding it to de-orbit
- A distress message from a car that has crashed or failed, perhaps in a remote region without mobile/cell coverage
- A message to an autonomous marine vessel or drone transferring control to a new operator
- Messages to and from infrastructure, such as controlling the state of traffic lights
- A heartbeat message raised by a fire sensor or a water level sensor to indicate it is working ok

What it is not (typically):

- Music radio broadcasts
- Satellite TV broadcasts
- Voice calls & texts made over the telecoms network (most of the time)
- A 'heartbeat' message from a sensor device indicating it's working normally
- A sequence of messages from one or more sensors reporting the average moisture level in a field

As you can see, a 'critical' message depends on the context, the level of loss and the tolerance of stakeholders to risk.

Understanding Rising Spectrum Congestion & Interference

The Electromagnetic Spectrum is a limited capacity resource which, as a society, we entrust national and international regulators to divide up. To achieve this, regulators divide the radio frequency and microwave spectrum into bands based on its characteristics and a learned assessment of its suitability for specific applications. With this done, they 'license' these 'bands' in whole or part to organisations for their use. As a catch all, some frequency bands are defined as 'unlicensed', which can be used by anyone within an authority's geographical jurisdiction … provided, they adhere to the 'rules' of that band; if not, enforcement is by prosecution under national & international laws based on regulators jurisdiction.

The best-known frequency band is Wi-Fi. In the UK this band spans 2.412 to 2.484 GHz. The Wi-Fi band is further split into 13 channels, each 20MHz wide in most world regions. Exceptions being 11 in the USA and 14 in Japan, hence the region question during set up.

A caveat being that the regulator, for the purpose of giving fair access, requires the radiated power (Effective Isotropic Radiated Power - EIRP) must be no more than 20dBm / 100mW.

This is important, because radio communication is akin to people in a room chatting. The regulator says, no one must raise their voice, if they do, they'll be fined.

Now consider that everyone is compliant, but many speak different languages (radio protocols) and some even try to save energy (low power protocols) by whispering. You can easily imagine that distance between people becomes critical to everyone's ability to communicate.

As the room gets busier, everyone stays compliant but some start to use novel ways to get themselves heard (encodings). There are lots of tricks used. Perhaps clicking to get attention, or emphasising certain words.

So, the regulator, has introduced the concept of a 'duty cycle' in some rooms (typically unlicensed frequency allocations like the Industrial Scientific & Medical – ISM bands). In this scenario everyone who talks for 1 second (say) must wait 99 seconds before talking again.

All works as well as it can, conversations get harder and shorter as the room noise increases. People start to repeat messages and some start to guess things they haven't heard (error correction).

While 'critical' conversations were possible when the room was empty … would people think the same as it gets busier and busier? What if a Rock Band (solar storm?) or a big crowd (9/11 situation) or a very angry person / adversary (who doesn't obey rules) arrives?

Now communication steadily or suddenly becomes impossible, including that which is critical.

Symbols

Hopefully the noisy room scenario is in mind. Now imagine the lights are turned off and everyone is given a buzzer. They now 'talk' using Morse code! The long buzz & short buzz are referred to as 'Symbols'. Sequences of symbols define letters and sets of letters, words.

With the richness of human speech removed, it's easy to realise that if everyone presses their buzzer equally loudly (amplitude) and at the same pace (frequency), chaos will ensue. To communicate, everyone needs to be either a) very close to the party they are talking with or b) listening out for differences in the buzzer sounds. Different 'symbols'.

Some people, being ingenious, decide to change the speed at which they send their Morse code, while others listen to the buzzer starting, or ending its sound. Still others get their buzzers to get louder slowly versus immediately. These are known as modulations.

Add encryption to messages, so others can't tell what you are saying. Get clever, changing the order of buzzer beeps (bit flipping) … you get the picture!

This is the situation with wireless in the wild. It's hard to talk, harder to hear someone's messages but, somehow, it works most of the time. If messages are encrypted, they can be hard to crack, but with the right skills, determination and tools [2], it is sometimes possible!

Wireless – inherently hazardous? … why?

Despite all the ingenuity and endeavours of people working in the wireless communications field to make it so incredibly reliable and useful, there will always remain a possibility that a wireless connection will fail and/or the message being carried will not arrive in a timely manner, arrive corrupted and need to be resent.

Even in an environment where everyone is compliant with regulations, wireless communication remains vulnerable to spectrum interference or non-compliant operator [3].

We should also not ignore the risk that communications are intercepted, decrypted and/or subverted by an adversary [3].

Wireless for 'critical' sensing, command and control - the risks:

While the exploits referenced earlier, are historic, Safety Risks persist from several vectors:

The spectrum

To quote: "Unlike wired networks, wireless communication channels are unstable, scarce, and prone to interference." [4]

1. the unstable nature of wireless spectrum, puts the reliability of wireless communication largely beyond the sender's / receiver's control
2. architectural choices come into play, such as whether the wireless device is normally connected or disconnected, if the protocol is adaptive, message repeated etc.

Probability

3. will the message arrive? … it depends on the state of the spectrum
4. will it be in a consistent state, unaltered from the original? … hopefully, but not guaranteed in all cases (watch the Packet in Packet exploit [5])
5. will it be in time to be actioned as intended? … if it does get received, then maybe

Trust

6. can the sender's identity be confirmed as true and trusted?
7. is the sender trusted?
8. is there assurance that the privacy of the message is uncompromised?

In terms of things that can be improved in wireless communications, recent work on wireless blockchain indicates that improving message Trust and utility, has significant potential.

In summary, best practice for 'critical' sensing, command & control over wireless, requires

an alternative communication path [6] to be on standby, ready to step-in on failure / interference, however small. Meantime we can embrace emerging opportunities to ensure messages that are received over the radio spectrum are secure and can be fully trusted.

To some extent this requires us to go back several millennia, to the time when each message carried its own seal. A seal that could be verified as being unbroken by the recipient and who's origin could be trusted.

Architecting wireless for safety 'critical' m2m messages …

From an architectural perspective, in this digital world, there are essentially two options. Both these options are implemented at the seventh ISO stack 'application layer':

Architecture #1 – **centralised verification** - using Certificate Authority (CA) technologies

Architecturally, in today's digital world, this requires implementing a system where each message packet is encrypted AND signed BEFORE delivery. On receipt, the recipient device contacts the signing CA to confirm the message is unaltered (consistent) and its origin can be verified.

In effect, this equates to using an X.509 certificate to sign each and every radio packet, with the associated communications to create, sign and verify plus maintain stores for large numbers of public and private keys.

This architecture may work for normally connected wireless communications, but is almost certainly unfeasible at all but small scale.

Architecture #2 – **distributed verification** - using (decentralised) blockchain technologies

Blockchain is an emergent technology that has many flavours [7]. It provides four benefits at once:

- message privacy – as does encryption
- immutability – ensuring the message received is consistent with the one sent
- auditability – enabling messages to be traced back to their origin, and
- smart contracts potential (the ability to send code that is trusted to a remote device for execution, in contrast to predicting actions and saving code on the device until needed).

However, there are other implementations, some of which are engineered to use minimal resources that have been tried on wireless communication testbeds. Blockchain systems may be centrally managed or distributed, with various strategies for deciding who can update the chain and how transactions in the chain are linked. In brief, blockchain is a ledger. It differs surprisingly little from the historic vision of a trusted scribe writing on parchment with indelible ink. The differences with regard to blockchain are:

- There can now be more than one trusted scribe
- Trust is assessed by a quorum using an agreed process, such as proof of stake (PoS) or proof of work (PoW)
- Parchment has gone digital and can thus reside in more than one place at (almost) the same time

In terms of implementation, this depends on the type of blockchain being applied, many are resource hungry and unsuitable for a resource constrained environment like wireless.

Another consideration is whether the wireless network operates in a normally connected or normally disconnected manner. There are initiatives to apply blockchain to normally connected wireless networks like Wi-Fi and 5G, however the task of applying blockchain to a normally disconnected wireless network poses all of the resource challenges PLUS the need to minimise transactions over spectrum, ideally to just the one.

Conclusion

Wireless communication should never be considered to be 100% safe, despite it being ever more reliable with the development and application of new standards, such as the 5G New Radio (NR) for air interface [8].

Given that wireless communication is now amazingly useful despite operating over an inherently hazardous spectrum, there is an opportunity to evolve the utility of messages transmitted to ensure they remain trusted and secure in the dawn of the quantum computing era [9].

References

[1] John Thomas, "Introduction to STPA", Engineering Systems Lab MIT, 2020 http://psas.scripts.mit.edu/home/wp-content/uploads/2020/07/JThomas-STPA-Introduction.pdf

[2] Matt Knight of Bastille Networks, "Decoding LoRa PHY (33c3)", 2016 https://youtu.be/NoquBA7IMNc

[3] Bart Hendrickx, "Russia gears up for electronic warfare in space" The Space Review, Oct 2020, https://www.thespacereview.com/article/4056/1

[4] D. Yu, W. Li, H. Xu and L. Zhang, "Low Reliable and Low Latency Communications for Mission Critical Distributed Industrial Internet of Things," in IEEE Communications Letters, vol. 25, no. 1, pp. 313-317, Jan. 2021, doi: 10.1109/LCOMM.2020.3021367

[5] Travis Goodspeed and Sergey Bratus and Ryan Speers and Ricky Melgares, "Packet in Packets: Orson Welles' In-Band Signalling Attacks for Modern Radios", In Proceedings of the 5th USENIX conference on Offensive Technologies, 2011, https://www.usenix.org/legacy/events/woot11/tech/final_files/Goodspeed.pdf

[6] Quote from Press Release Critical Messaging Association Sept 2020 https://critmsg.org/wp-content/uploads/2020/04/202009-Press-Release-New-Home-for-CMA.pdf

[7] Liehuang Zhu, Keke Gai, Meng Li, "Blockchain Technology in Internet of Things", 2019, DOI 10.1007/978-3-030-21766-2

[8] Sacha Kavanagh, "What is 5G New Radio", March 2020, 5G.co.uk https://5g.co.uk/guides/what-is-5g-new-radio/

[9] National Cyber Security Centre, "Preparing for Quantum-Safe Cryptography", Gov.uk, Nov 2020 https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography

Michael Green, Founder & Director, eComergy Wireless.Works Ltd., Weightless.Space Ltd

Michael has a degree in Mechanical Aeronautical & Production Engineering. He started programming 50 years ago with ICL, and has implemented both large and small systems including IT security for banks and multinationals. In the last decade Michael has focused on the challenges of Low Power Wide Area (LPWA) wireless networks for IoT device deployments beyond the range of mobile / cell networks, hence the interest in low frequency (sub-1GHz) on aerial and satellite platforms for critical sensing, command & control that are both highly robust and able to scale.