Technology
Innovation
Institute

Secure Comms Shield: A Zero-Trust Network Solution for Distributed Communications

Secure Systems
Research Center

tii.ae

Innovation for a better world

Contents

Scaling autonomous systems

It is easy to get caught up in autonomous systems as a single self-driving car or individual drone. However, the real promise of autonomous systems comes when autonomous capabilities are simultaneously scaled to improve the control of individual things, the orchestration of a collection of things, and the understanding of things at scale.

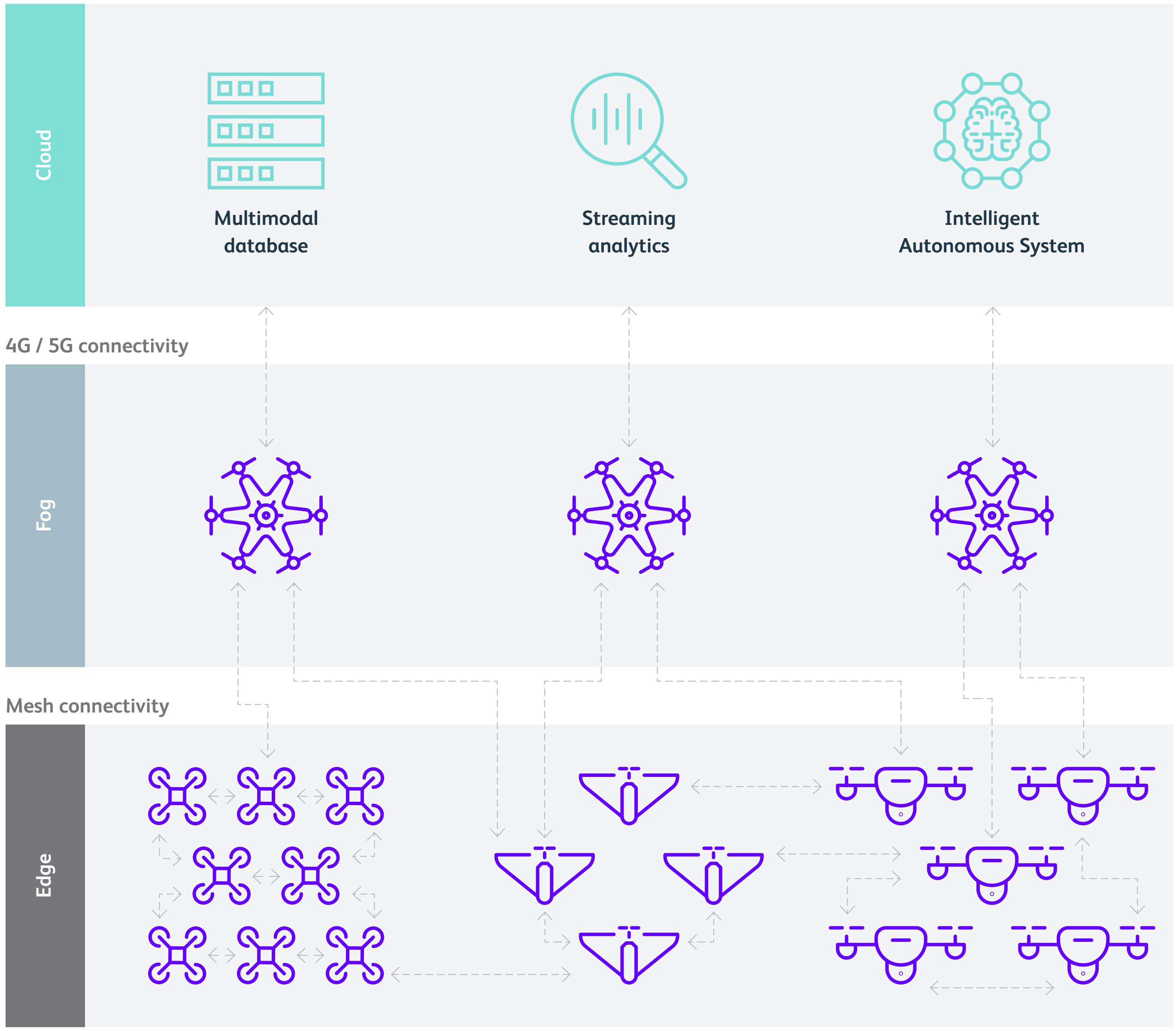
The individual-level can be considered as the evolution from cruise control to automated braking and fully self-driving cars. The orchestration-level entails the evolution from synchronized traffic lights to dynamically adjusted traffic lights to advanced mapping services that route cars around traffic jams. Autonomous understanding systems include traffic monitoring cameras to crowdsourcing dashcam video into dynamically updated digital twins for improving overall traffic.

These same three factors of control, orchestration, and understanding play out across various use cases. A warehouse robot might reduce the need for staff. An autonomous warehouse management system could optimize the scheduling and staging of items in the warehouse. In contrast, an autonomous understanding system could help reengineer the warehouse design to further increase performance in the same space.

This combination of autonomous control, autonomous orchestration, and autonomous understanding is already showing some promise in the UAE. For example, one pilot project has created an autonomous port truck system that automates the process of shifting shipping containers from boats to trucks.

Gartner refers to the simultaneous evolution of control, orchestration, and understanding in IT systems as hyperautomation. In this case, enterprises use individual robotic process automation (RPA) software robots (called bots) to automate a collection of human tasks. Orchestration engines help organize the flow of work across multiple bots. Then, process and task mining bots analyze enterprise applications or even watch over the shoulders of individuals to find further opportunities for improvement.

Researchers are just starting to explore how similar practices may be extended to include autonomous vehicles. That is one of the reasons ATRC's ASPIRE chose to focus on autonomous swarm coordination as part of its next grand challenge project. ASPIRE is tasked with hosting grand challenge competitions loosely organized like the US DARPA's challenge that spearheaded research on autonomous vehicles. The upcoming challenge tasks researchers with finding the best way to orchestrate a swarm for drones to search for and retrieve objects hidden on ships that are too heavy for any individual drone.



The need for secure communications

Communication networks transfer an increasing amount of data due to billions of users and devices, creating several challenges for threat detection. Moreover, Denial of Service (DoS) attacks already reached more than 1.35 terabits per second and the longest in 2016 lasted 197 hours. This number increased yearly. In November 2021 Microsoft's Azure DDoS protection platform mitigated a massive 3.47 terabits per second attack with a packet rate of 340 million packets per second (pps) for a customer in Asia.[1] And in 2022 google detected more than 100,000 requests per second, an increase of more than 80% of the previous "record".[2] Current security systems such as Security Information and Event Management (SIEM) systems are designed to gather and analyze data in a single point, yet are not effective, since 85% of network intrusions are detected weeks after they had happened, with an average detection time of 206 days.[3]

Particularly in mission-critical environments, such networks should conduct communications even under the most extreme circumstances, with guaranteed capacity, performance, and quality. Mission-critical networks have high requirements on availability, coverage, capacity, security, and quality of service (QoS). This means that these networks always need to be available and operate independently of a network provider in a distributed environment.[4] Thus, a mission-critical network should provide secure and resilient communications, using heterogeneous devices and protocols, from resource-constrained devices to a fleet of Unmanned aerial vehicles (UAV) using public or private infrastructures. As an example, a wide area swarm is deployed for long- term surveillance, such as protecting a nature reserve or border. The swarm uses a mesh network protocol to communicate, and attackers attempt to jam the network to temporarily halt communication between the swarm and the control center. As a result, a distributed optimization reconfiguration scheme is designed to allow the swarm to reconfigure itself to re-establish contact. This scenario could also help improve strategies for slowing the propagation of malicious code or data among vehicles in the swarm.[5]

Moreover, resilience, security, and dependability are highly-desirable properties of future wireless embedded systems. While networks can rarely expect to incorporate all these properties, they should, at the same time, always sustain a high communication performance. For example, this allows the real-time exchange of high-resolution audio/video, the transmission of sensor data and position information at high data rates, the detection of events on a large scale, as well as the creation of performant and highly-mobile mesh networks (e.g., multi-drone networks, and ad-hoc networks for emergency response).

[1] Epic DDoS Fail: Azure Cloud Fends Off 'Largest Attack Ever Reported in History, David Ramel, 01/31/2022, https://virtualizationreview.com/articles/2022/01/31/azure-ddos.aspx

[2] Google blocks largest HTTPS DDoS attack 'reported to date', Ionut Ilascu, 18/08/2022 https://www.bleepingcomputer.com/news/security/google-blocks-largest-https-ddos-attack-reported-to-date/

[3] Lobato, A. G. P., Andreoni Lopez, M., Cardenas, A. A., Duarte, O. C. M., & Pujolle, G. (2022). A fast and accurate threat detection and prevention architecture using stream processing. Concurrency and Computation: Practice and Experience, 34(3), e6561.

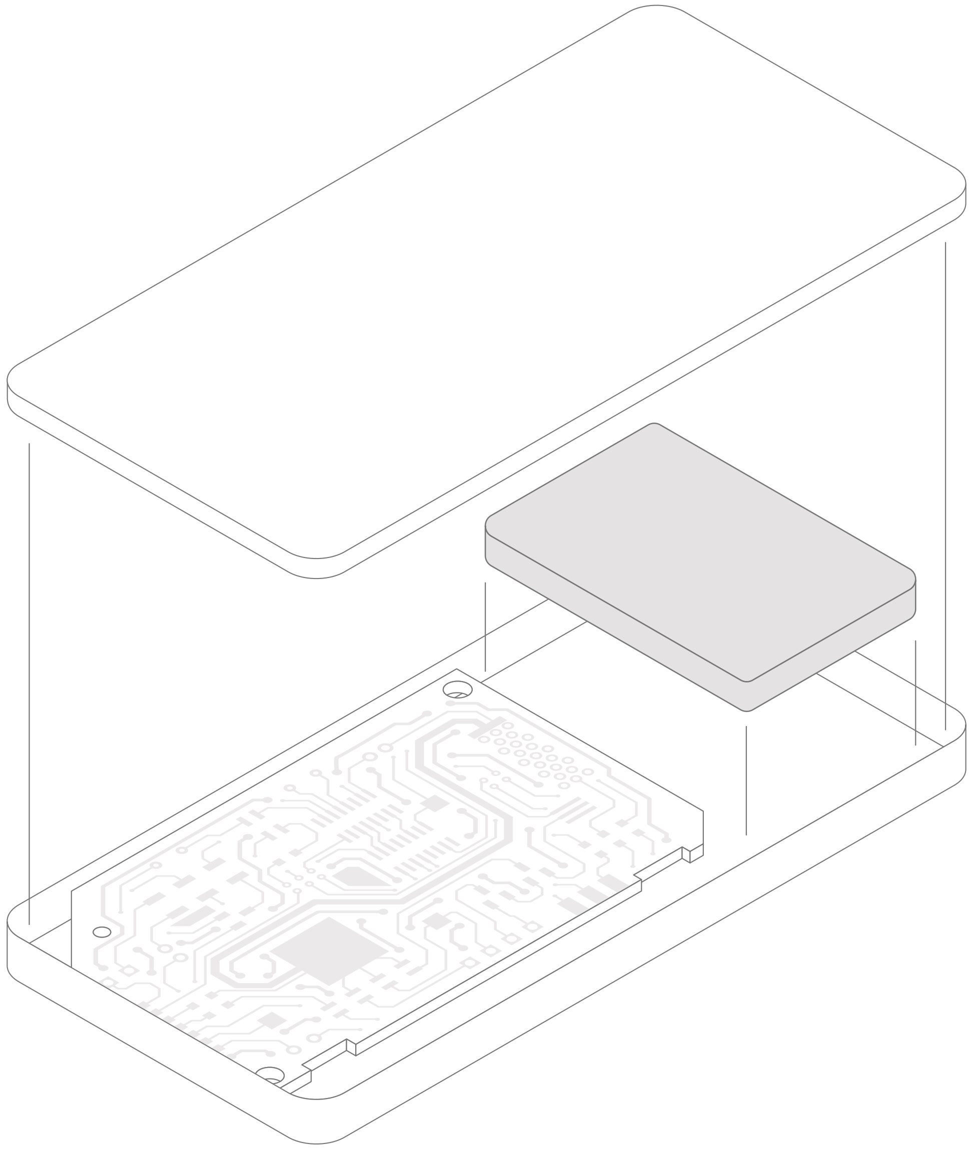
[4] Ericsson White Paper GFMC-18:000199, Ensuring critical communication with a secure national symbiotic network. 01/12/2021, https://www.ericsson.com/en/reports-and-papers/white-papers/ensuring-critical-communication-with-a-secure-national-symbiotic-network

[5] obtained from TII A Zero Trust approach to autonomous systems of systems security white paper

The SSRC Comms Shield: secure and resilient communications

At SSRC we have developed the first Secure Comms Shield Enabled Network Router device - supported as a handheld unit for first responders, or as an integrated communications module for autonomous UAV networks.The device provides a core network, a security management layer, and Connectivity management. The core network is provided by a Secure Mesh Network working with a Dynamic Gateway allocation, so the devices can establish a secure connection between them and communicate with the "outside world" through a most efficient gateway that is maintained dynamically. The security management layer is composed of the Mesh Shield with all its security features such as, mutual, and continuous authentication, phy-layer security, anomaly detection, and a secure network decision engine. This layer allows for establishing secure communication providing Confidentiality, integrity, and availability of the data, as well as the privacy of the network members. The connectivity management layer supports several Radio on-boarding for Gateway (LTE, 5G, others). In addition, this layer supports several device-to-device connectivity radios such as Wi-Fi / BT on board, as well as Zigbee / LoRa via interfaces.

The following figure shows a diagram of the device in its lite form factor. The computer module of the device is a RPi CM4 SOM. The comm module runs a Secure OS with a native container to provide isolation. In addition, key pairs are stored in a Soft-HSM. On the communication, the device uses the Wi-Fi: QCA9880, QCA9590 (Doodle Labs) as well as the onboard Broadcom card. For Bluetooth, we are using a Nordic nRF52840 chip. The device is composed of circuit board antennas and has USB, mPCIe, and uHDMI interfaces. The performance of the Comms Shield qualifies for operations up to 55 deg C Ambient Temperature, within a 1-hop range of up to 7 km, static mesh setup, reaching up to 1.6 Mb/s under a UDP connection, using 2.4 GHz with 5 MHz bandwidth. The Mesh Shield can be used as a first companion comms device for a Phone paired wirelessly with it through an Access Point. Thus, it is possible to use a phone to create secure communication with another phone or Comms Shield device. Moreover, the device can be integrated with an ethernet port to communicate with the mission computer on a drone system. Hence, the drone can establish a secure connection with a drone/ fleet of drones or even with a phone.



Applying a Zero-Trust approach to mesh communications

Wireless mesh networks are infrastructure-less communication systems allowing multiple nodes to communicate with each other. While such networks can greatly extend the range of communication, and be deployed in an ad-hoc fashion, like all wireless communications they are vulnerable to various attacks and misuse activities (such as eavesdropping and jamming) due to the broadcast nature of their transmissions. Moreover, guaranteeing security in the ever-evolving future communication networks is challenging owing to mobility, cooperativeness, heterogeneity, and the lack of central infrastructure.

Traditional key-based cryptographic approaches implemented at the upper layers may become inefficient in future communication networks. Moreover, weaknesses inherent within mesh protocols and standards have introduced new attack surfaces and present novel security challenges. We have therefore outlined the main vulnerabilities and threats across the entire mesh communication stack, from the physical to the application layer.

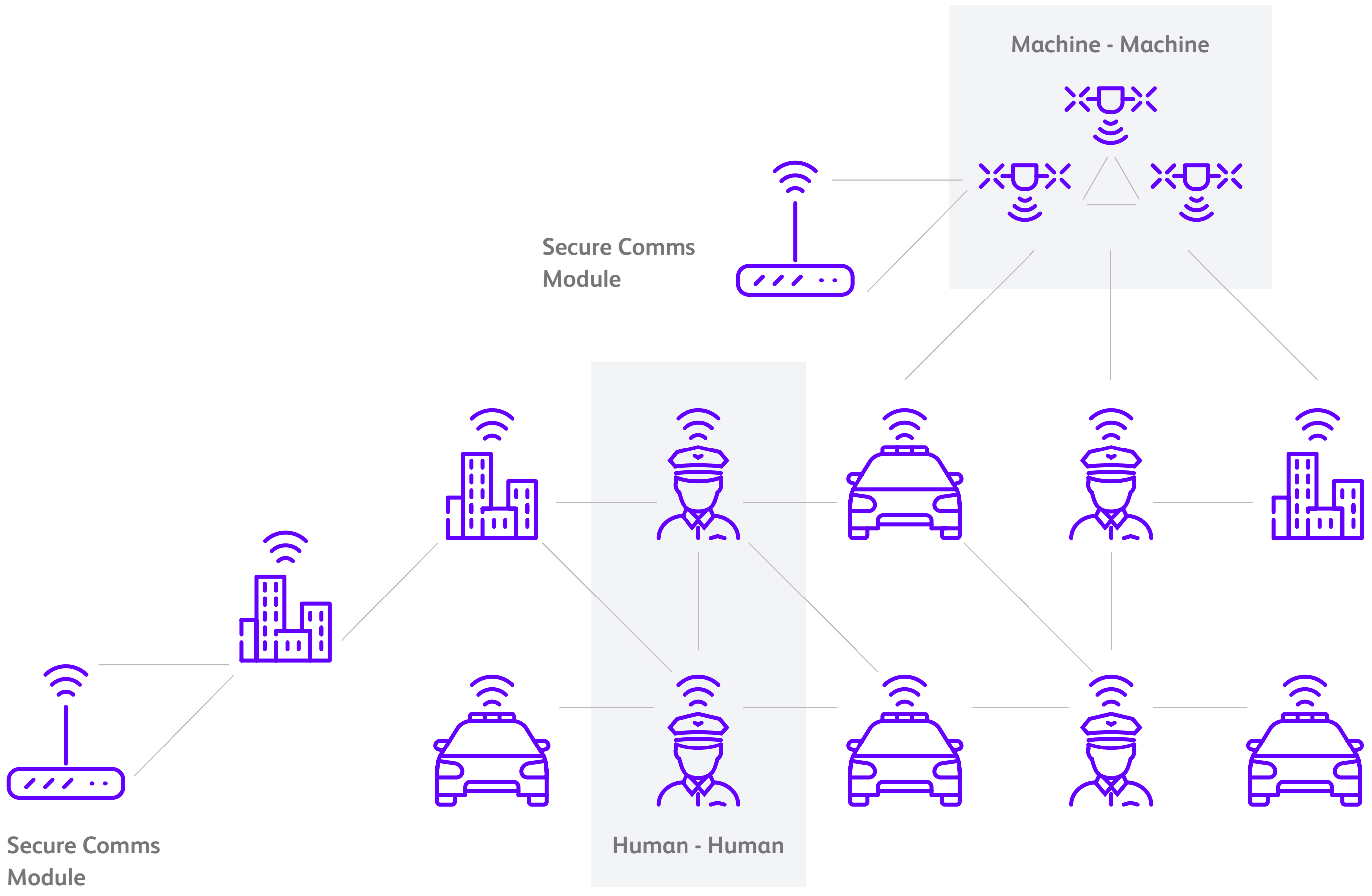
Layer	Threat/Vulnerability	Exploit
Physical	Passive Eavesdropping	Broadcast Nature of Wireless Channels
	RF Jamming	Wireless contention
Link	Spoofing	Intentional Collision
	Frame Modification	MAC Spoofing
Network	Routing Forwarding	Selfish Attacks
	Data Forwarding	Collusion Attacks
Transport	Packet Corruption	Denial of Service (DoS)
	Protocol Weakness	Session Hijacking
Application	Open Protocols	Injection

In this sense, it is necessary to design systems within the Zero Trust and Zero Touch architecture. In a zero-trust Architecture, the protection system is supposed not to trust anything and keep verifying every entity before granting them access, or the hassles of passwords are expected to be eliminated, which is likely the mainstream of network security systems to stop data breaches.

As shown in figure 1, at the Secure System Research Centre (SSRC), mesh networks are applied in two main use cases: i) Machine-to-Machine communication, to communicate with autonomous devices, e.g.: a swarm of drones; and ii) Human-to-Human communication, to communicate with people within secure networks, allowing mobility and supporting global as well as point-to-point exchanges between humans and machines, within a continuously resilient and trusted link. Therefore, at SSRC we are developing a secure solution based on mesh communication. The Mesh Shield, a secure & resilient Mesh Comm system that provides protection against a variety of attacks (De-auth, MitM, Penetration, Routing, flooding, exfiltration, etc.). The Mesh Shield has been designed with the zero-trust concept in mind. Thus, the network layer is untrusted, and everything needs to be end-to-end encrypted from the moment it enters the infrastructure to its interaction between various nodes, as well as data that leaves the infrastructure.

We have developed different security features to improve the entire security of our mesh communication. Hence, Mutual Authentication, Continuous Authentication, Traffic anomaly detection, and a Network system decision engine are the security features to create a zero-trust architecture for a secure Mesh Shield to protect distributed communications. In addition, the Mesh Shield has the capability to run a multi-radio environment and different communication protocols to be resilient to Jamming attacks.

All the mentioned features are executed in our flagship device, our Secure Comms Module. This device is capable of establishing secure and resilient communications between different devices, running in a mesh topology in a fully distributed manner. Our entire secure system allows ad-hoc setup, coverage based on deployment, and non-permanent communications, enabling higher security and availability of communications with the flexibility of deploying a network anywhere. The Mesh Shield communicator can be used by first responders such as police, firefighters deploying a mix of voice, data, and video communications in conjunction with autonomous drones. Also, it can be used on military and defense applications, adding more sensors used on the battlefield. And finally, adding value to current logistics solutions using autonomic and resilient UAV systems for applications like surveillance.



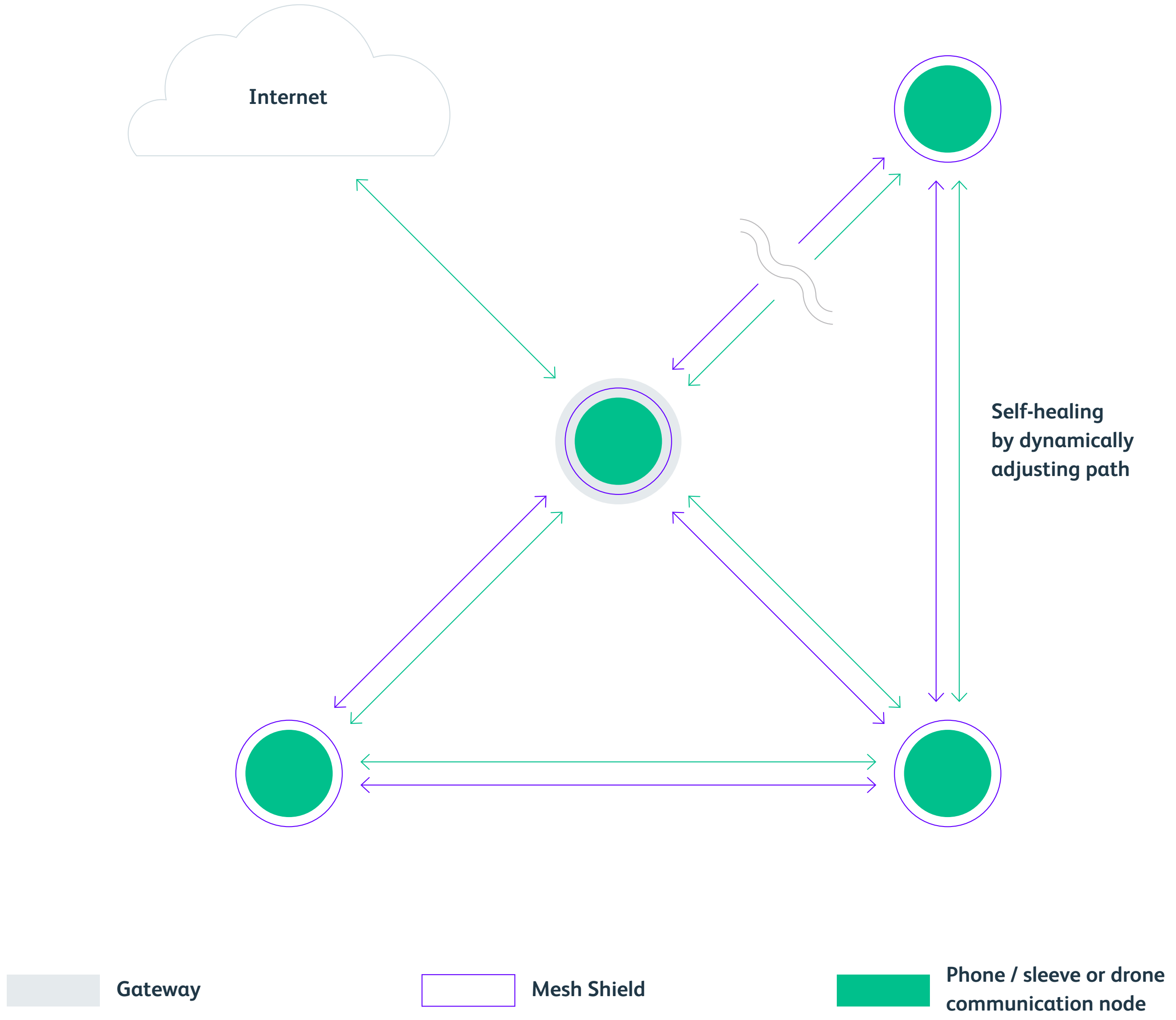
Securing distributed communications

1 Secure Protocols

Many mesh protocols are designed with no security or assume security issues are handled on the above layers. This assumption, and the absence of a global view, make the protocol layers vulnerable to several threats. The two most popular mesh proactive routing protocols, The Better Approach to Mobile Ad-hoc Networking (B.A.T.M.A.N.) and Optimized Link State Routing Protocol (OLSR) also present security vulnerabilities. Therefore, a simple Denial of Service (DoS) attack would seem relatively straightforward to consume bandwidth or take down the network. In DoS attacks, the perpetrator seeks to make a network resource unavailable to its intended users by disrupting the services of a host connected to a network. As an example, in the B.A.T.M.A.N. protocol, each node periodically generates a single originator message (OGM). This message determines the link qualities to the direct neighbors and spreads this link quality information through the whole mesh broadcasted on all hard interfaces. A simple Denial of Service can be executed by sending bogus OGMs. This attack could cause the size of routing tables to explode or disrupt the routing within the mesh. Another attack is to force traffic to route through a hostile node, enabling man-in-the-middle exploits. Similarly, for OLSR, an incorrect hello message is also called the Id spoofing attack. In such a type of attack, the attacker node uses the id of the other node and shows itself as the other node. Thus, we need to use secure methods to protect these protocols.

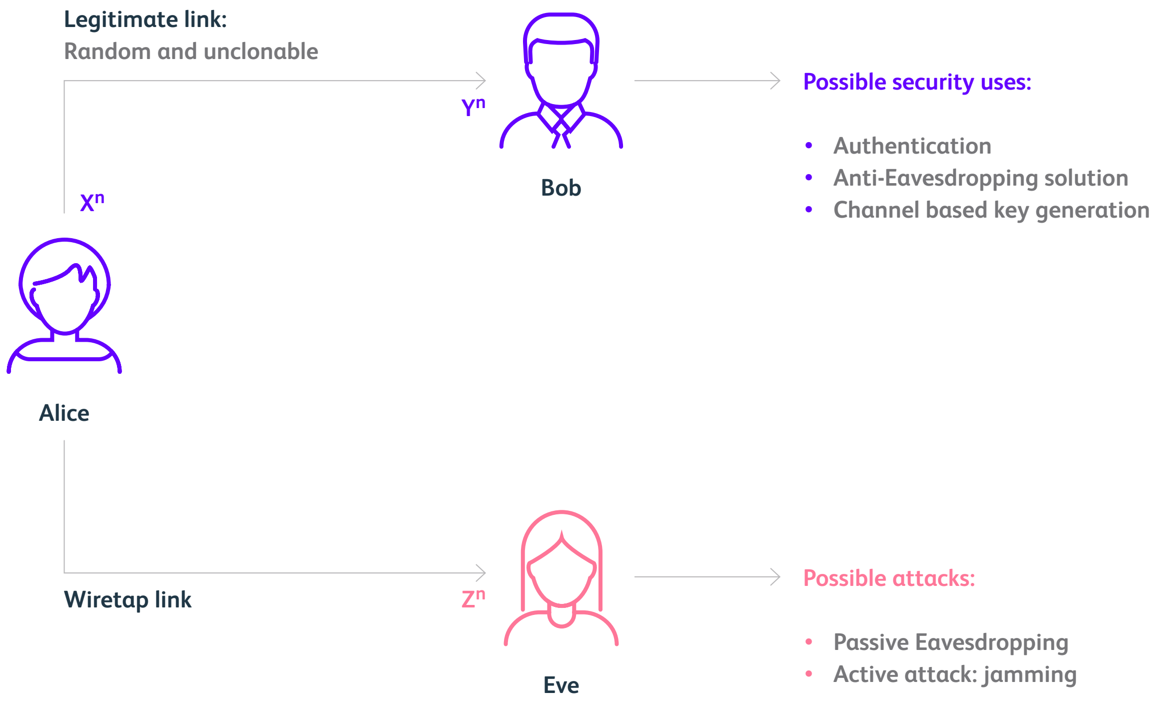
At SSRC, we are aiming to create secure protocols to avoid some of these protocol vulnerabilities. For example, secure B.A.T.M.A.N. routing makes the nodes that are a part of a restricted network only accept routing updates from other nodes that are appropriately authenticated. By only accepting OGMs from authenticated nodes, the network traffic is only routed to or via trusted nodes.

Figure 2 shows the Mesh Shield working along with the phone sleeve or drone communication node via a secure protocol, that allows the system to self-healing in case of failure or threat by dynamically adjusting the routing path.


Internet
Self-healing by dynamically adjusting path
Gateway
Mesh Shield
Phone / sleeve or drone communication node

2 Physical layer assisted security

Recently, there has been an increased interest in tapping the wireless channel's random and unique features for developing security solutions. Referred to as physical layer security (PHY-security), these exploit the inherent characteristics of the physical channel, such as multipath fading, interferences, propagation delay, etc., to realize key-less secure transmissions through various coding and signal design and processing techniques. For instance, consider the system shown in the below figure. Herein, the Alice-to-Bob link is completely uncorrelated from an Alice-to-Eve link in a rich scattering environment and provided they are half-wavelength apart. Specifically, the principle is to somehow degrade the quality of the malicious user link i.e., the Alice-to-Eave link, compared to the legitimate user(s) i.e., Alice-to-Bob, and then transmit at a rate that only the legitimate user (Bob) can decode. If the wiretap channel is a degraded version of the main channel, secure transmission can be achieved in an information-theoretic sense. These solutions have lower complexity, require less network overhead, and have low end-to-end latency compared to the existing key-based solutions. Also, PHY-security does not need a trusted authority and tamper-proof devices and can offer adaptive security solutions. All these benefits come with the notion to achieve perfect secrecy. Furthermore, these solutions operate independently of the existing key-based security solutions and complement the existing security infrastructure. PHY-security can be used to derive secret keys and mitigate attacks like spoofing, Sybil attacks, eavesdropping, and jamming.



Possible security uses:

- Authentication
- Anti-Eavesdropping solution
- Channel based key generation

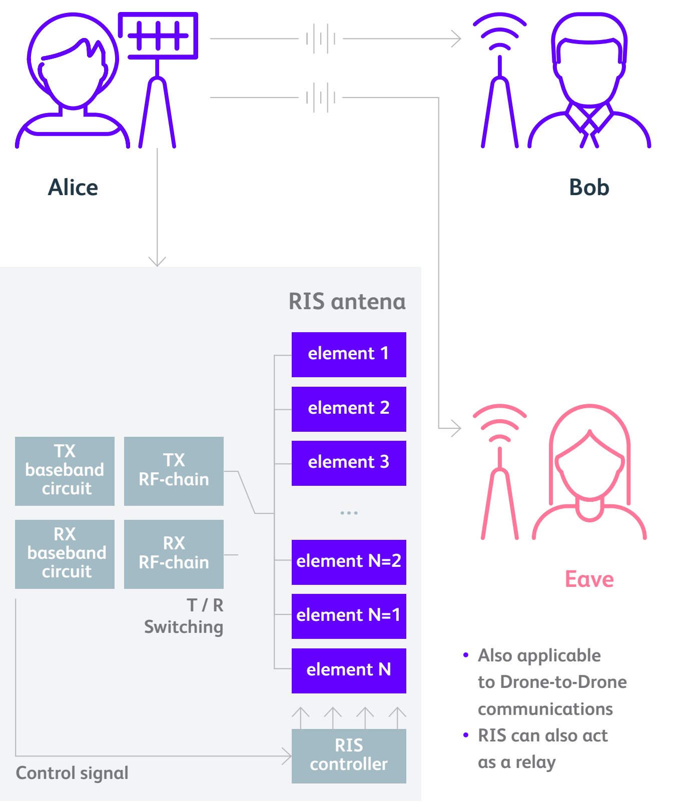
Possible attacks:

- Passive Eavesdropping
- Active attack: jamming

At SSRC, we are considering PHY-security to develop schemes for mutual and continuous authentication, anti-eavesdropping, and jamming-resistant solutions. The authentication schemes will exploit the unique channel-based features such as received signal strength, channel state information, and radio-frequency frontend imperfections like clock offset values to identify nodes uniquely. Moreover, we are also working to couple physical unclonable functions with the unique PHY-channel characteristics to generate a secret key framework. Such a framework requires no third-party intervention and has no storage obligations. We are also working to exploit the diversity in the space, time, and frequency domains to design a secure precoding scheme resistant to jamming and eavesdropping attacks and it can improve communication reliability.

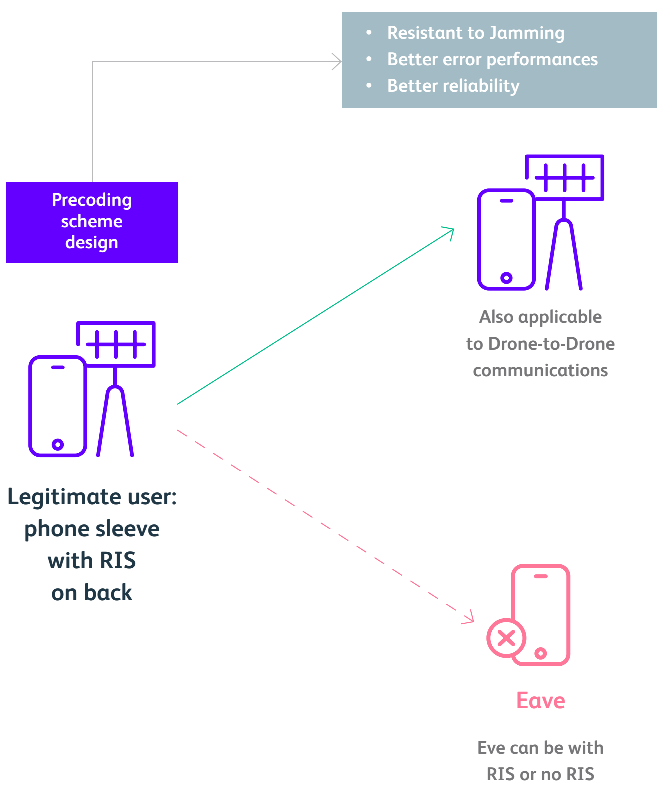
The random channel behavior is beneficial for developing infrastructure-less PHY-security solutions. However, this uncontrollable nature of wireless channels is also the ultimate barrier to achieving high capacity and ultra-reliable communications. The existing solutions, such as massive multiple-input-multiple-output (MIMO), adaptive modulation can only adapt and provide no control over the channels. Moreover, some scenarios exist, such as rural environments and the availability of direct line-of-sight links (e.g., aerial-to terrestrial links) where the channel does not offer much randomness. There is a requirement for somehow controlling the wireless channel behavior. Recently, Reconfigurable Intelligent Surfaces (RISs) have emerged as a potential solution to overcome these limitations and achieve high rate, ultra-reliable, and secure wireless communications. RIS, an artificial planar surface, consists of tuneable low-cost passive reflecting elements. They can alter the propagation of waves impinging on it by adjusting the reflection amplitude, phase shift, and departure angle and perform passive beamforming. Thus, RISs can turn the random wireless environment into a programmable and partially deterministic space. RISs can offer better capacity, energy savings (passive elements), security, and efficient spectrum utilization (full-duplex operation without self-interference concerns) at a lower hardware complexity. Owing to the benefits RIS offers, the RISs-aided wireless communication paradigm can support many states of art use-cases of the sixth generation (6G) beyond communication networks.

At SSRC, we look to exploit the RIS technology to design secure transmissions by designing secure beamforming and secure non-linear precoding solutions. Also, we hope the technology will benefit our existing PHY-security solutions by enabling us to tailor the wireless channels as per our needs. Some use-cases we look to exploit can be seen in the below figures.



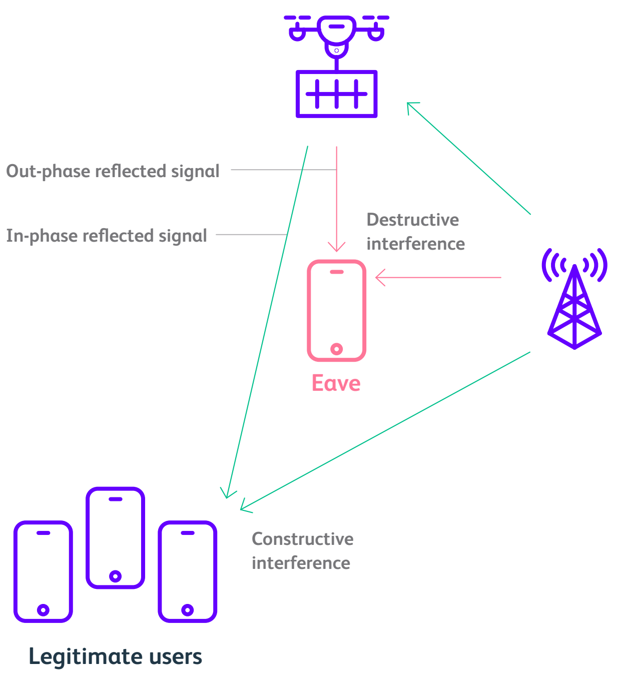
RIS-assisted Secret Key Generation

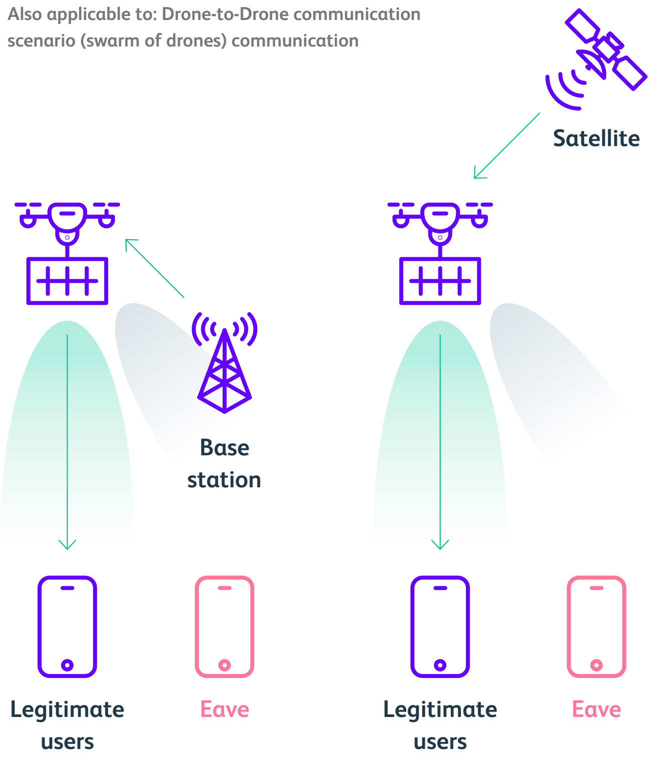
- The RIS surface-based features can be used for key generation
- RIS can mitigate low random channel behavior
- Also applicable to phone-use case


Resistant to Jamming
Better error performances
Better reliability
Precoding scheme design
Legitimate user: phone sleeve with RIS on back
Also applicable to Drone-to-Drone communications
Eave
Eve can be with RIS or no RIS

RIS-assisted Secure Precoding scheme

- RIS-features can be used to designed a signal scrambling scheme
- Malicious user can not decode unless facilitated with full precoding design
- Can ensure perfect secrecy


Out-phase reflected signal
In-phase reflected signal
Destructive interference
Eave
Constructive interference
Legitimate users


Also applicable to: Drone-to-Drone communication scenario (swarm of drones) communication

Friendly jamming via UAV-enabled RIS

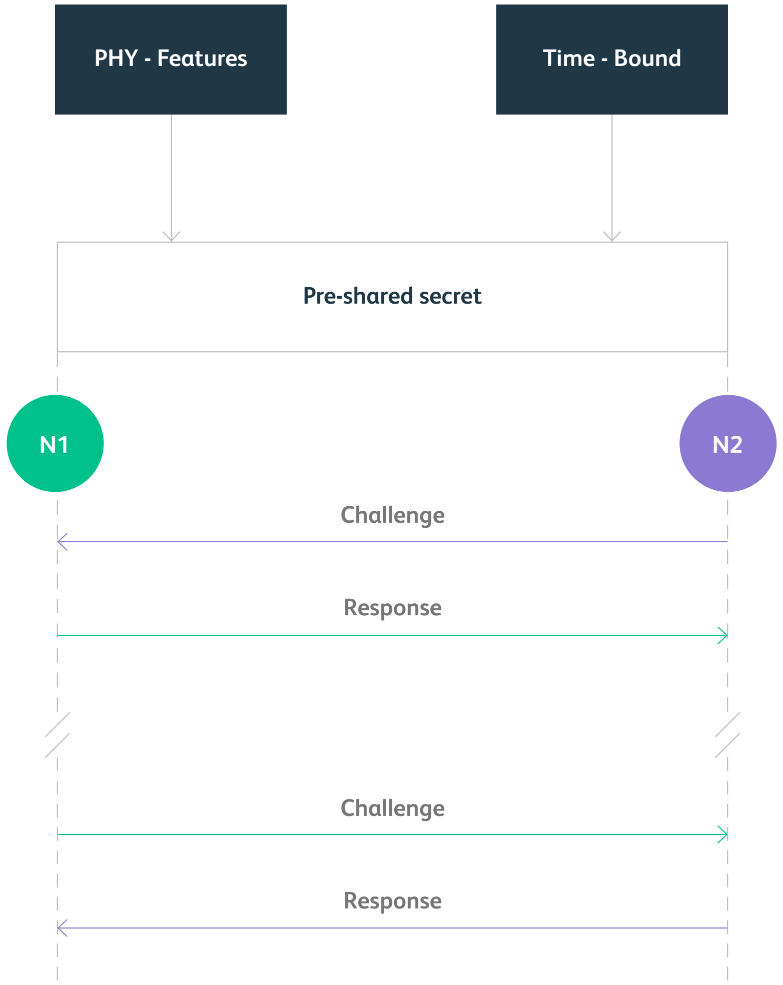
- No additional power for inducing jamming
- Better received signal power at legitimate users which also improves security
- Full-duplex communication with no throughput loss

Secure beamforming via UAV-enabled RIS

- A Focused Beam towards a dedicated target via signal Processing
- Better signal power at legitimate user thus improving security
- Poor received power fails the eave to decode anything

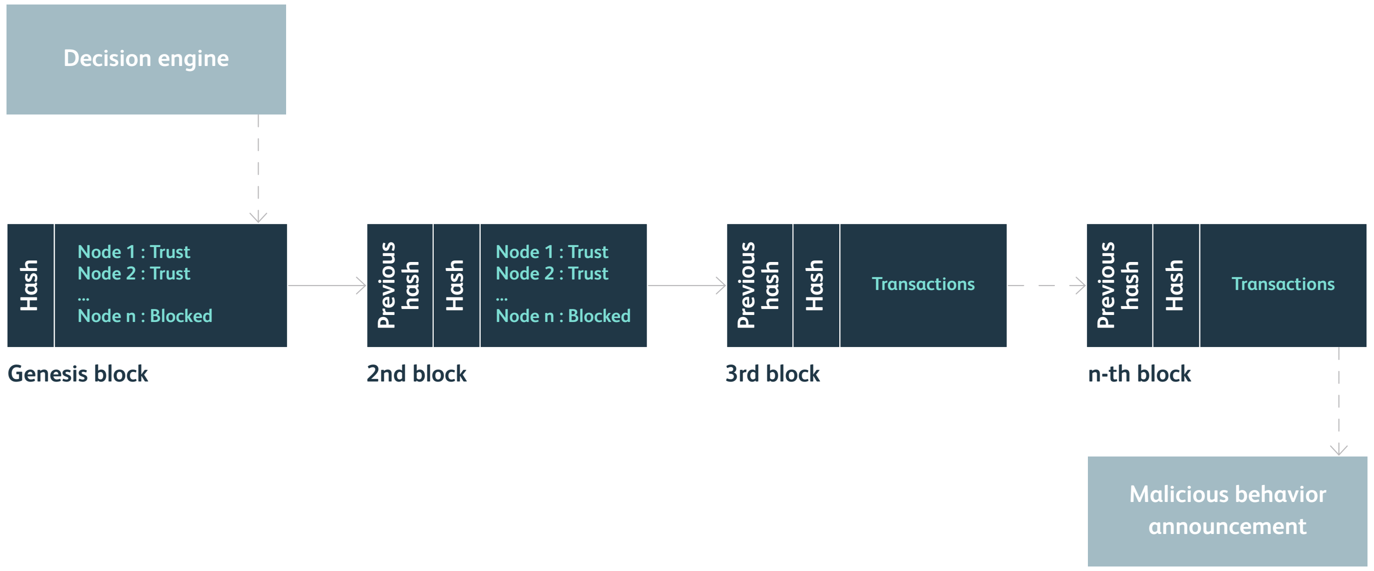
3 Continuous and distributed authentication

During a mission, it is possible that no external network connection exists. Thus, certificate provisioning must avoid communicating with Certificate Authority (CA) during the mission. Initially, the certificate can be provisioned during the manufacturing process and key pairs can be stored in Hardware Secure Module (HSM) tamper-resistant approach. In this module, the private key is securely stored and never leaves. If the certificates are provisioned by the manufacturer, it is assumed a delegated trust route, where all the web is trusted until the producer root. Authentication must be performed on both sides, with the certificates obtained in the provisioning step, each node should authenticate with its immediate neighbor mutually. Once the node is authenticated, it will be able to join the secure mesh. Nevertheless, since the SSRC Mesh Shield follows a zero-trust concept, in which we assume anyone on the internal network could be a bad actor. Thus, any node in the network should be able to launch a continuous authentication process within any other node, to verify its behavior. This step is executed after a node joins the network. Continuous authentication is performed with the node's neighbors, and it obtains multiple inputs to perform the authentication. We consider valid inputs as PHY layer parameters, time-bound tokens, or even ephemeral keys. In the end, a decision engine generates a trust value for each neighbor.



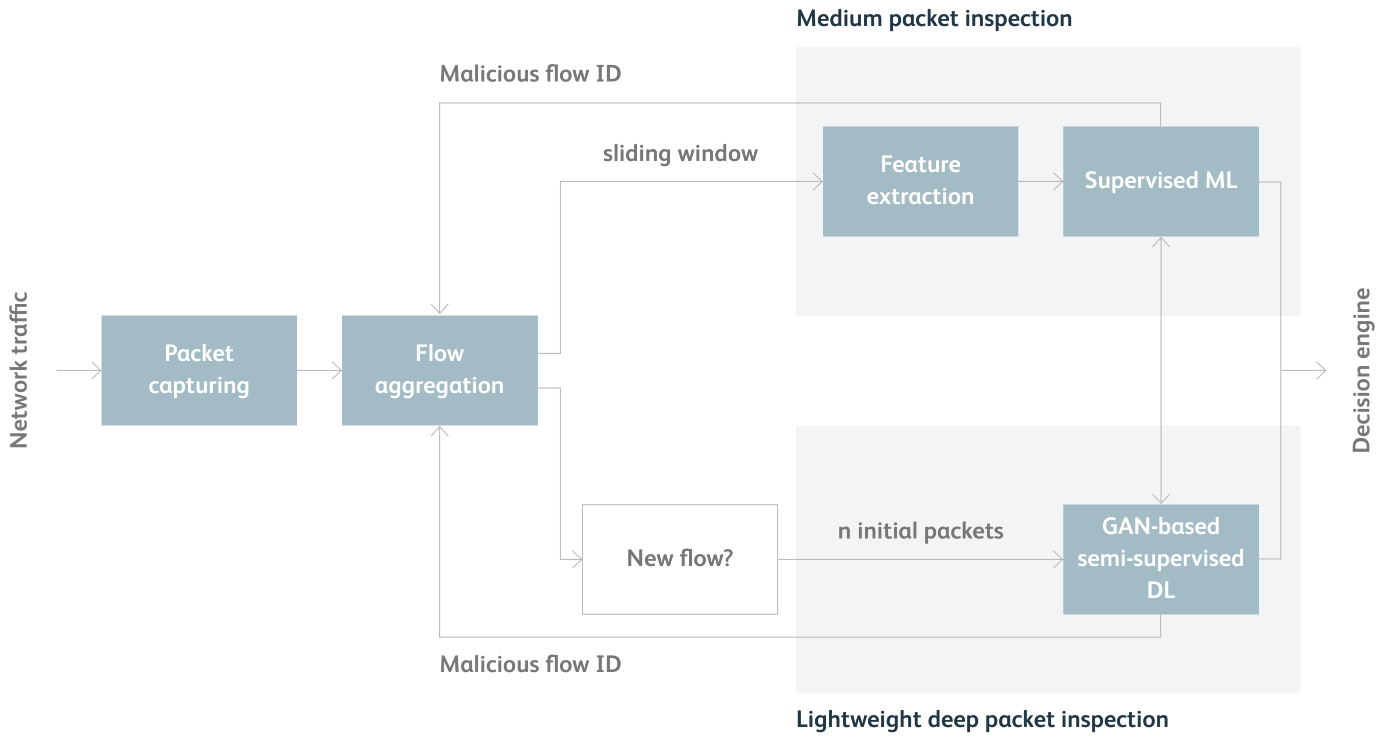
4 Distributed Ledger Technology and Blockchain

Over the last decade, Blockchain, and the Distributed Ledger Technology (DLT) underpinning it has emerged as a revolutionary data management framework to establish consensus and agreements in a trust-less and distributed environment. Blockchain offers an immutable, transparent, secure, and auditable ledger, to verify the integrity and traceability of information/assets during their life cycle. In addition, it eliminates the need for a central authority. Rather, it is managed by distributed peers, each having a copy of the ledger. In a blockchain, the users that execute and confirm transactions are called miners. Before digitally signing and appending the transaction into the blockchain network, these miners verify the transactions by following a mining mechanism. Since blockchain is a distributed public ledger, it holds immutable data in a secure and encrypted way. It also ensures that the transactions cannot be altered, thus preventing data and execution tampering. In the SSRC Mesh Shield, the blockchain is used to register all the security steps like mutual and continuous authentication, quarantine, and other security measures to protect the mesh network. This way the integrity of data is maintained by all peers, and it is hard to tamper with the data since the intruder would have to change all the blocks in the blockchain.



5 Network traffic anomaly detection

Anomaly-based network anomaly detection relies on building a profile of the normal traffic. These systems attempt to estimate the normal behavior of the network and generate anomaly alarms whenever a divergence between a given observation and the known normality distribution exceeds a predefined threshold. Anomaly-based systems do not require a recurrent update of databases to detect novel attack variants. Deep Learning (DL) emerged as a game-changer to help automatically build network profiles using feature learning. It can effectively learn structured and complex non-linear traffic feature representations directly from the raw bytes of a large volume of normal data. Based on a well-represented traffic profile, it is expected that the capabilities of the system to isolate anomalies from the normal traffic to be increased, while decreasing the false alarms. However, the naive adoption of DL may imply misleading design choices, and the introduction of several challenges, such as speeding up the detection speed, and reaction time. In addition to a careful definition of the model's architecture, training artifices could be exploited for improving the method's effectiveness, without degrading the efficiency due to the increased number of parameters and model size. We have developed a network Intrusion Detection System (IDS) composed of two major modules: a supervised machine learning approach that performs medium packet inspection on a sliding window basis, and a semi-supervised DL-based approach for early anomaly detection that performs deep packet inspection and builds a profile of the normal traffic based on the raw network flow's bytes by leveraging Convolutional Neural Networks (CNNs) and Generative Adversarial Networks (GANs).



Supervised Medium Packet Inspection

The supervised medium packet inspection module employs state-of-the-art supervised ML algorithms to detect malicious network traffic flows given packets captured on a sliding window. Feature engineering plays an important step here, therefore, more than one hundred relevant network traffic features were proposed. These features are extracted in real-time from the packet's headers in the sliding window, allowing real-time detection with high accuracy of well-known attacks and malware.

Adversarially Regularized Convolutional Autoencoder for Unsupervised Network Anomaly Detection (ARCADE).

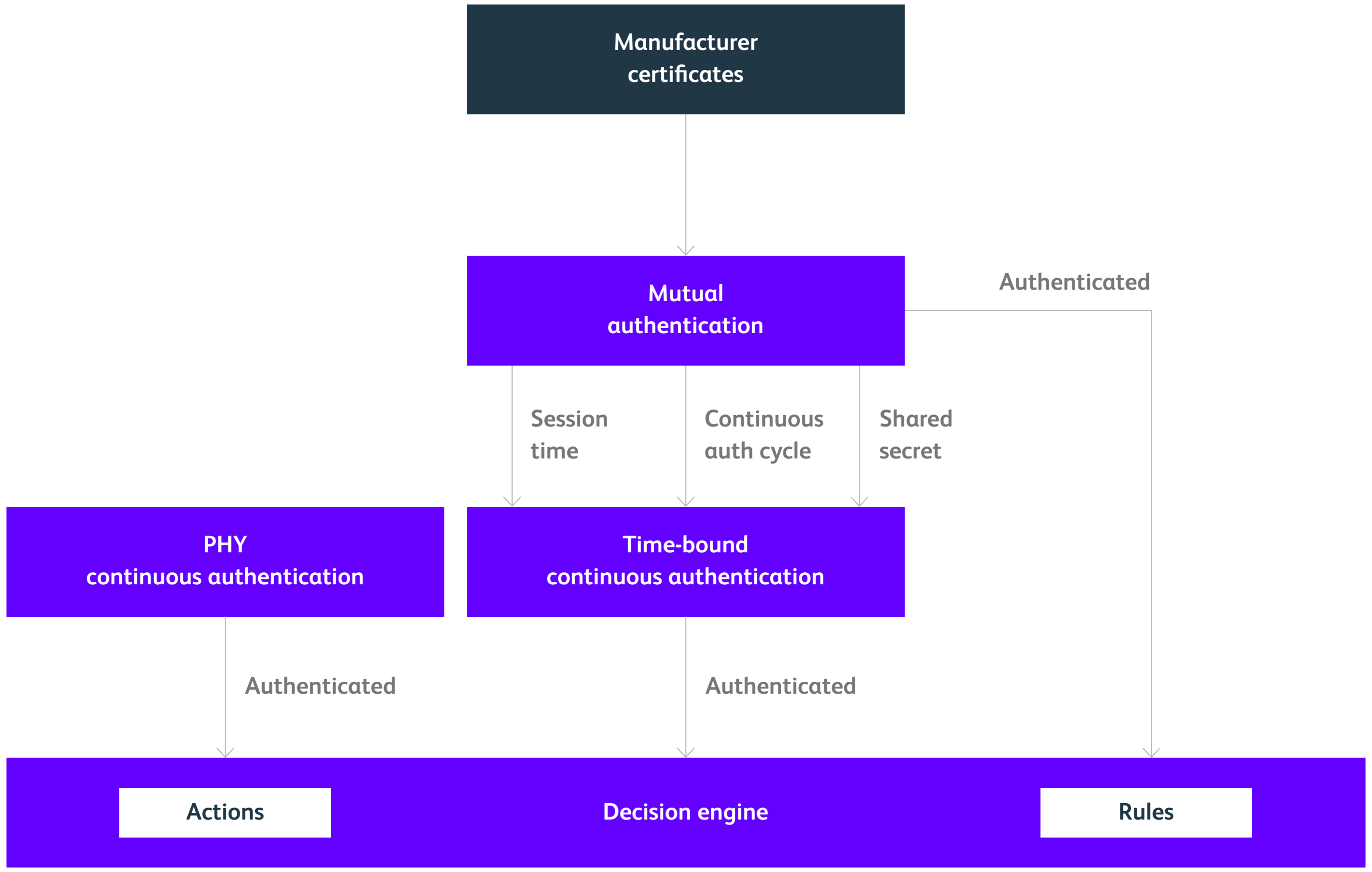
ARCADE exploits the property of 1D CNNs and GANs to automatically build the normal traffic profile based on a subset of raw bytes of a few initial packets of network flows.[6] It can detect network flow anomalies (zero-day) given a small sample of its initial packets, allowing it to prevent network attacks before they could cause any more damage. A lightweight convolutional Auto Encoder (AE) model is employed to suit online detection in resource-constrained environments. The model is trained following a novel adversarial training strategy that decreases the AE capabilities to reconstruct network flows that are out of the normal distribution, improving its anomaly detection capabilities. The proposed approach is far more effective than existing state-of-the-art deep learning approaches for network anomaly detection and significantly reduces detection time.

[6] Lunardi, Willian T., Andreoni Lopez Martin , and Giacalone Jean-Pierre. "ARCADE: Adversarially Regularized Convolutional Autoencoder for Network Anomaly Detection." arXiv preprint arXiv:2205.01432 (2022).

6 Network Expert Security System Decision

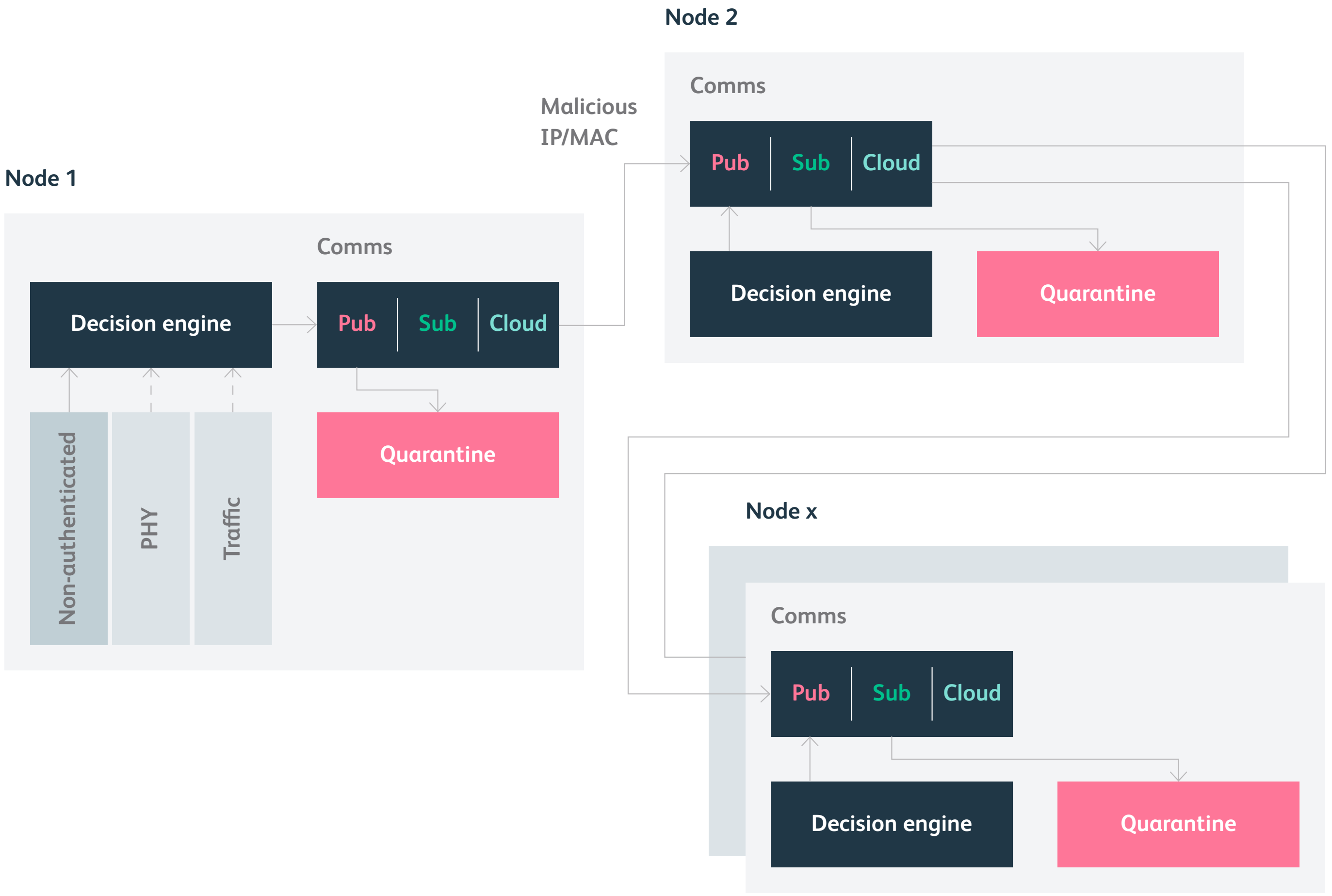
Along TII Mesh Network Security Architecture (a.k.a. Mesh Shield) roadmap several security functions are being aggregated to form the final “Security Shield”. These functions cover Authentication, Trust, Resilience, and Privacy layers of security. Based on these, several different types of errors will be reported and various security decision strategies will be deployed accordingly along with the roadmap which poses the question of scalability and adaptability of our Security Analysis and Report approach.

Based on those error reports exposed through what can be called a Dashboard, Expertise-based decisions have proven to give efficient results in making decisions. Supervisor-based architectures have been extensively deployed in similar decision domains where Expert Knowledge plays an important role like Safety and Security. The results provided by such a system are meant to maintain Mesh Network operations integrity and trigger Minimal Risk operations in case a critical case is found. Moreover, there is no need to infer results from large sets of data. As the decision impacts system safety (and security), we need the result to be fully explainable. Knowledge and rules can easily deal with uncertainty in the data and knowledge and Rules can be gradually updated to improve the quality of the decision, like for an Expert. As a natural follow-up, TII Mesh Shield Network Expert Security System (NESS) Decision is going to infer security outcomes based on the rules



7 Malicious Announcement and Quarantine

After an anomalous behavior is detected locally, by any of the security features mentioned above, the other nodes in the network need to be informed. For this reason, the node sends a message with a decision. Communication is the core of this module. For this purpose, we used a broadcast announcement approach. For the implementation, encrypted UDP sockets, with messages signed by each node are used to communicate the message. The information can contain IP and MAC addresses, and fingerprints of certificates among other information from the malicious node. This information is then broadcasted to all nodes in the network. The information is received and treated by the Quarantine module to maintain the node under observation for a period. This module runs on every node and will block the malicious IP address for the compromised node. Once a node receives more than one message, it will proceed with a voting system to block the node. The voting system prevents collusion attacks, where two or more nodes intentionally try to remove a node in the network sending fake information. Thus, the voting system consists in having n/2 (n being the number of nodes in the network) vote positives or negatives in a reduced time window.



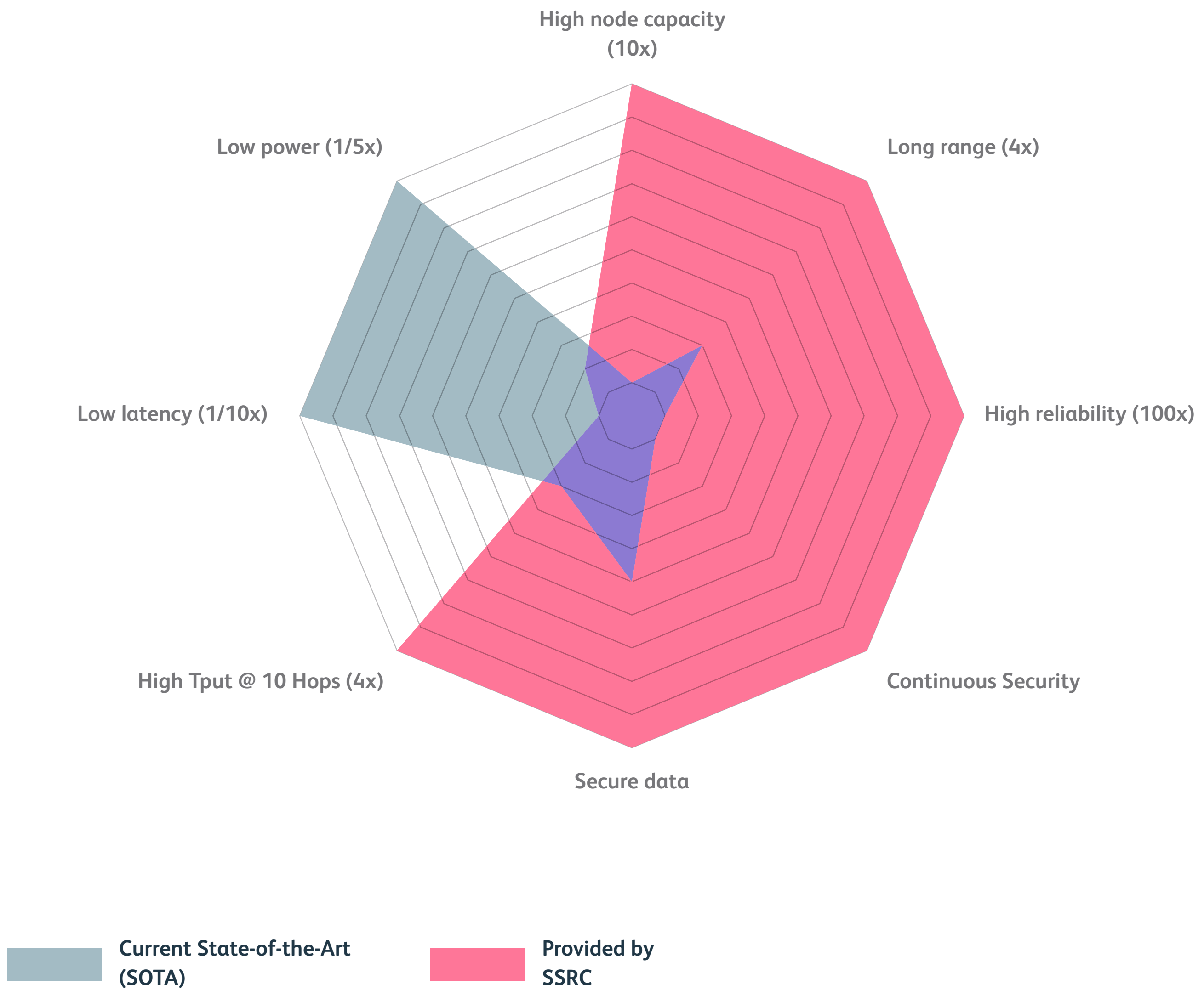
Ensuring end-to-end communications resilience

1 Testbeds and Benchmarking

Traditionally, benchmarking suites aid system designers and industry practitioners to identify the best combination of communication technology, network stack, and protocol parameters for a given application scenario. Unfortunately, when it comes to evaluating the performance of wireless mesh networks, there is a severe lack of benchmarks. On the one hand, this is due to the fact that existing benchmarks such as EEMBC's IoTMark-BLE, Cisco's TPCx-IoT, and RIoTBench focus on different performance criteria; namely, on the energy-efficiency of edge devices, on the data aggregation or storage capabilities of IoT gateways, and on distributed stream processing systems hosted on cloud data-centers, respectively. On the other hand, the many public testbeds available to test and evaluate wireless (mesh) solutions hardly offer features to systematically and automatically quantify performance in an objective way. As a result, the divergence across experimental setups is often extreme, at a point where it is hard to draw the line between a fair and unfair comparison.

At SSRC our goal is to create the first comprehensive wireless mesh benchmark facility that can evaluate the performance of communication protocols in a fully-automated way, end-to-end, across multiple sites. This will help us attain rigorous benchmarking, and provide a platform for robust penetration testing of our wireless protocols and mesh security solutions.

Towards this goal, we work with our university partners to enable experimentation across Wi-Fi mesh networks (e.g., using IEEE 802.11s or B.A.T.M.A.N. Advanced) and to study the resilience of existing mesh solutions to injected faults and attacks. This will give us the means to quantitatively assess and analyze the performance of mesh networking protocols (in terms of resilience, security, reliability, throughput, end-to-end latency, and energy efficiency), to model their behavior, as well as to expose their weaknesses(e.g., to malicious entities introduced in the mesh). This will ultimately enable the creation of resilient and high-throughput mesh networking solutions that can sustain a dependable performance and mitigate security threats.



2 Synchronous Flooding

Humans, as well as wireless devices, typically communicate with each other politely, meaning that basic principles of conversational manners and wireless design favored strategies that prevent multiple speakers/transmitters from talking over each other. People's tendency to listen before talking and not interrupting others did inspire wireless MAC designs such as carrier sense multiple access with collision avoidance (CSMA/CA) when more intrusive approaches like ALOHA had proven to achieve less effective communication throughput. Time Division Multiple Access (TDMA), the other dominant communication paradigm, emulates turn-taking in human conversation.

Concurrent Transmission (CT)-based communication is, however, a more disruptive approach and is beyond the polite conversational conventions mentioned above.[7] CT encourages multiple wireless devices to transmit data exactly at the same time.

Finding analogies of CT in a normal human situation is not difficult though. Think about listening, understanding, and potentially remembering an unheard song sung by multiple people at the same time in a crowded room. The ability to successfully decode data transmitted by multiple concurrent transmitters was pioneered by Glossy, a decade ago, for low-power wireless networks. In Glossy, all the transmitters send the same data just like the same song is sung by all the room's attendees. Now, imagine listening to an argument between a group of people who are talking over each other, trying to get their different points of view across. Yet, the loudest voice and often its contents can be understood even in this seemingly chaotic situation. Low-power wireless radios, not very different from human listeners, can understand the loudest of many signals due to the capture effect of radios.
This phenomenon enabled new flexible designs that permit multiple concurrent transmitters to send different data packets simultaneously. Based on these techniques, powerful flooding protocols can be developed, allowing devices to disseminate information quickly and reliably across an entire mesh network.

Concurrent transmissions rely on two RF properties, non-destructive interference, and the capture effect.

Non-Destructive Interference:
Usually, when two nodes transit at the same time, they will cause destructive interference resulting in a collision at the receiver - meaning both transmissions fail. However, if nodes are well-synchronized (to within half a chip period - i.e., 0.5µs in IEEE 802.15.4) then the transmission can be reliably demodulated in FSK (frequency) modulated systems. Importantly, this technique of non-destructive interference is used to allow multiple nodes to send the same data simultaneously, providing the transmission with sender diversity that can be modeled in a similar fashion to multipath.

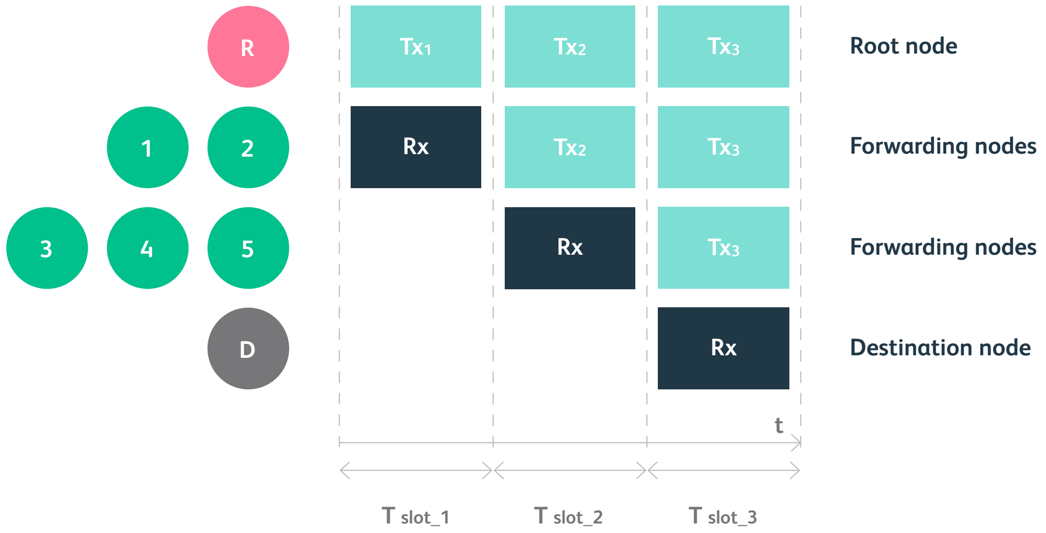
Capture Effect:
The second RF property utilized within CT is the capture effect. This is again a property of FSK modulated systems where if one transmission is received with higher power than the other (~3dB in IEEE 802.15.4) that transmission will be reliably received.

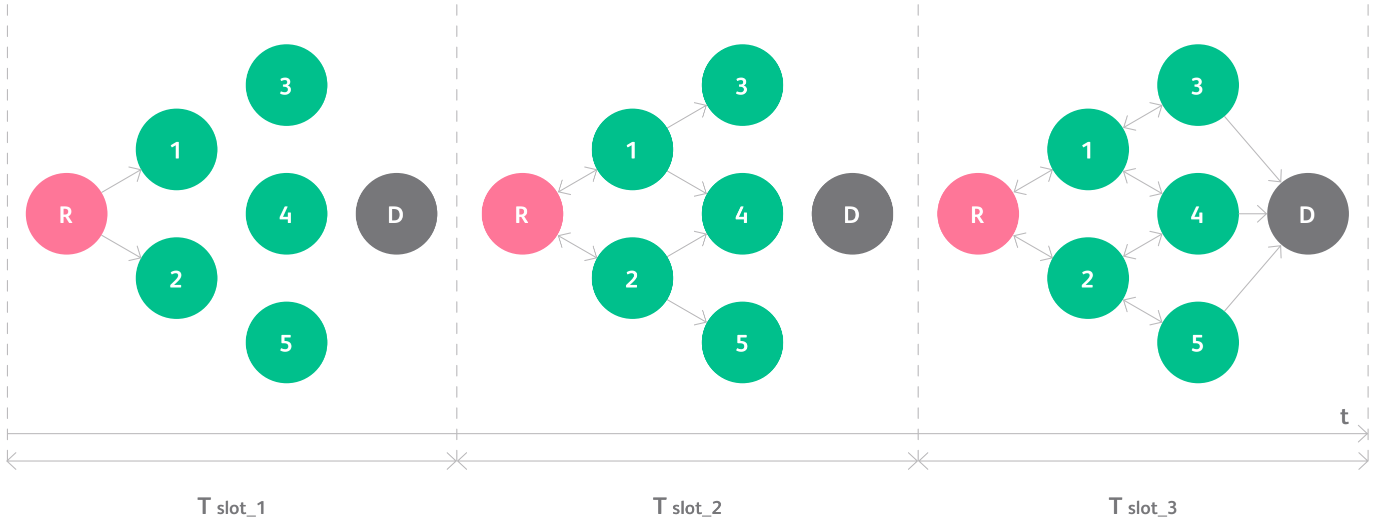
Based on these two properties, it is possible to realize and implement efficient flooding protocols that outperform SOTA narrowband mesh routing protocols.

SSRC will use this technique to provide resilient broadcast channels for robust and reliable communication in the face of RF interference and malicious jammers.[8] Such channels can ensure essential communications are maintained across the network, for example allowing nodes to collaborate to detect, avoid, and even localize an attacker.

[7] M. Baddeley, CA. Boano, A. Escobar-Molero, Y. Liu, X. Ma, U. Raza, M. Schuβ, and A. Stanoev, The Impact of the Physical Layer on the Performance of Concurrent Transmissions. In Proceedings of the 28th IEEE International Conference on Network Protocols (ICNP). Virtual event. October 2020

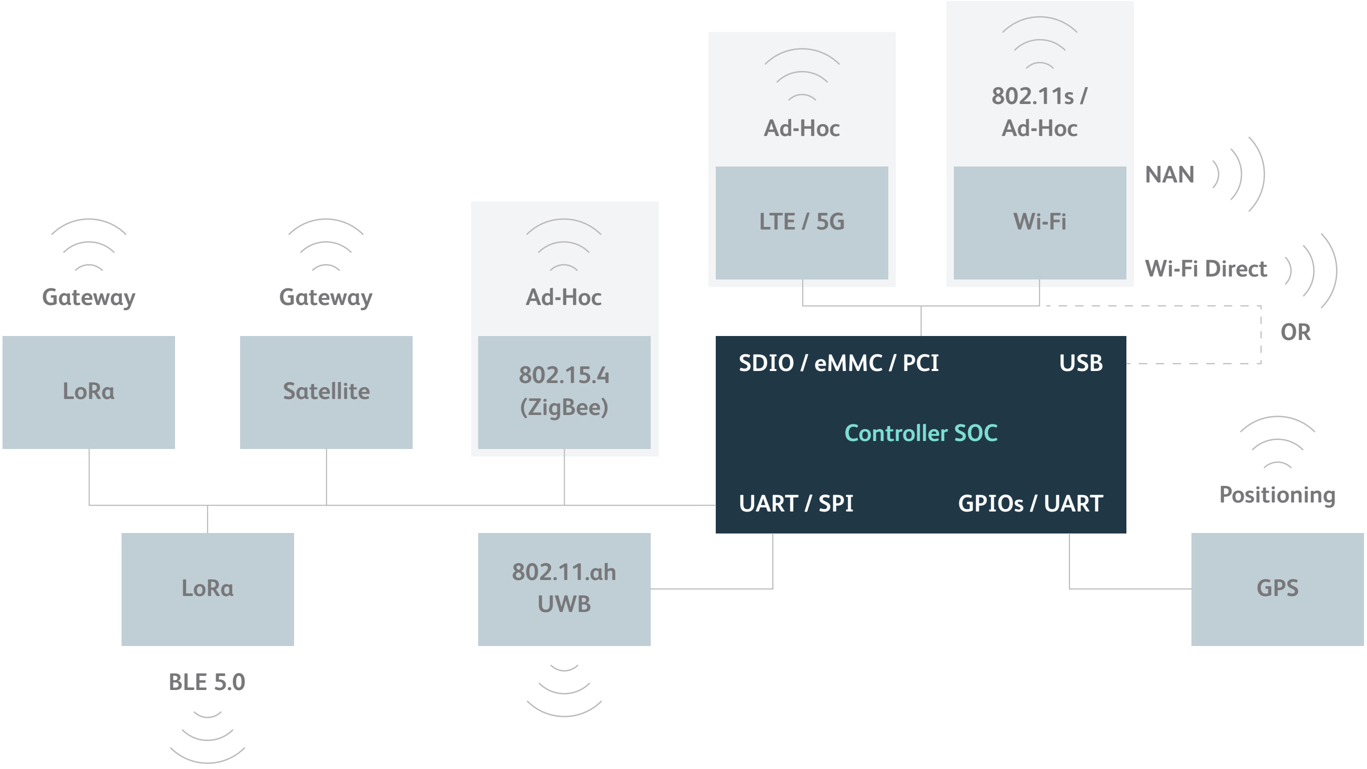
[8] M. Baddeley, Y. Gyl, M. Schuss, X. Ma, and CA. Boano, OSF: An Open-Source Framework for Synchronous Flooding over Multiple Physical Layers. In Proceedings of the 19th International Conference on Embedded Wireless Systems and Networks (EWSN). Linz, Austria. October 2022.


R
1
2
3
4
5
D
Tx1
Tx2
Tx3
Rx
Tx2
Tx3
Rx
Tx3
Rx
t
T slot_1
T slot_2
T slot_3
Root node
Forwarding nodes
Forwarding nodes
Destination node

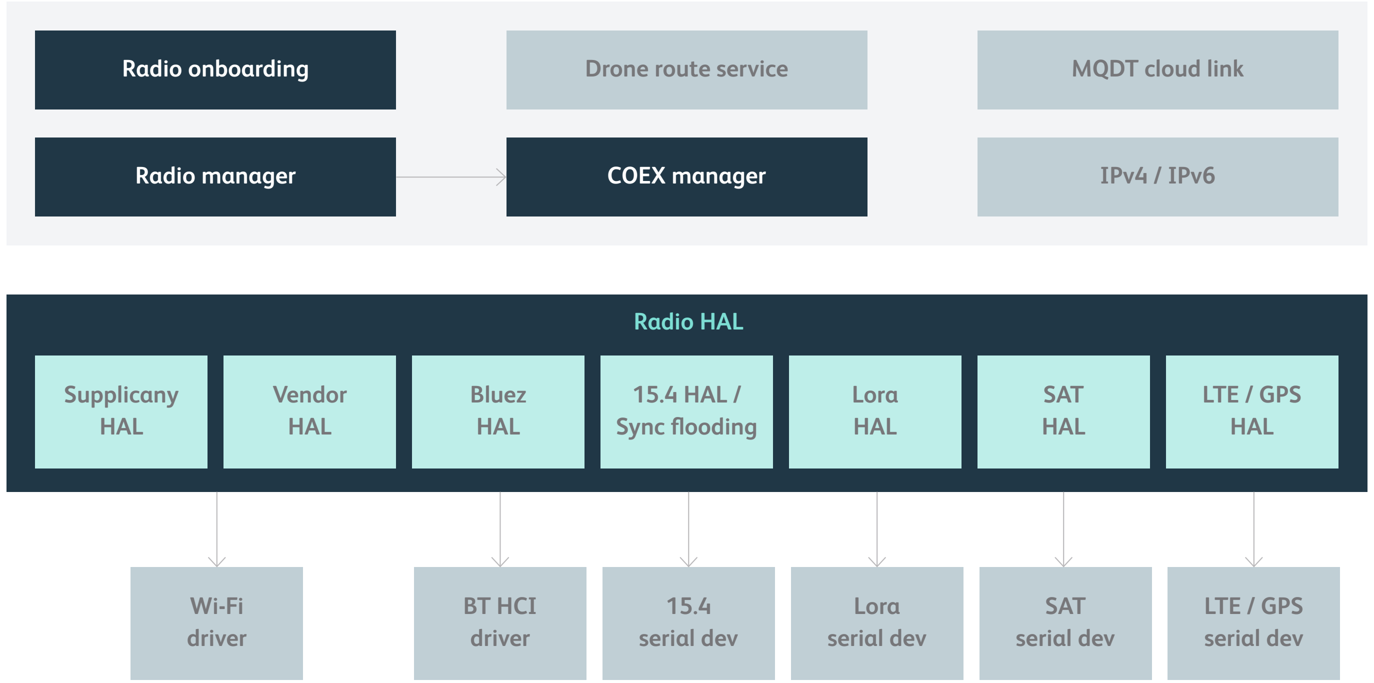

R
1
2
3
4
5
D
t
T slot_1
T slot_2
T slot_3

3 Multi-Radio Communications

Multi-radio wireless mesh network architecture improves the network capacity by exploiting multiple radio channels in different bands concurrently. It is resilient to narrowband interference and jamming scenarios by using software-based channel hopping and provides improved QoS. Channel assignment and routing are underlying challenges in multi-radio architectures as they are the key factors for determining the traffic distribution over radio links and associated channels.

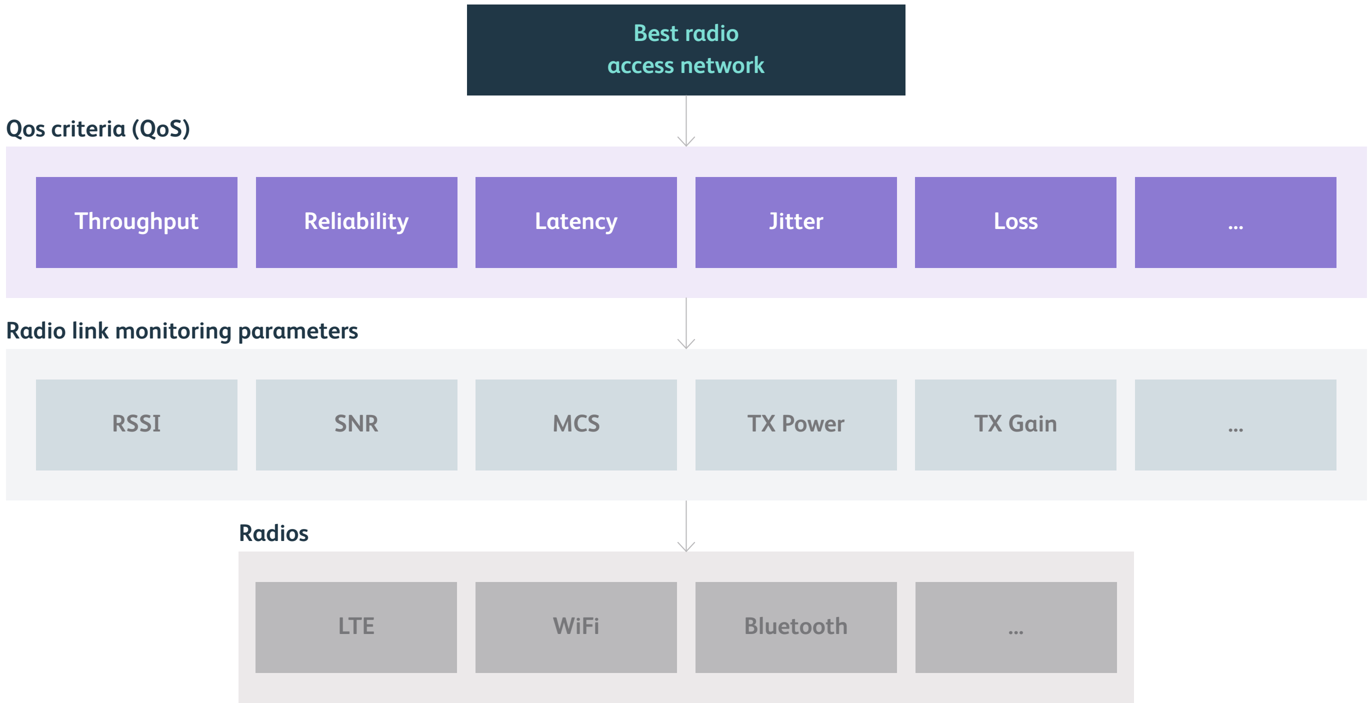


At SSRC we are developing a software-defined multi-radio framework comprising radio management HAL, radio resource management, link monitoring, spectrum sensing, and adaptive QoS routing with coexistence awareness. It is a potential solution that can enable efficient utilization of wireless link spectrum through improvised channel assignments and routing. Moreover, it is susceptible to interference with improved QoS for different static and mobile use cases. A high-level representation of the Multi-Radio Resilient (MRR) software framework is given below.



Multi-Radio Resilient Software Architecture

As seen in the architecture above, the multi-radio resilient framework will perform radio on-boarding, link management, radio-coexistence, and spectrum management in a modular and abstract manner for a defined use case. Radio HAL provides the layer of abstraction between the radio manager and the actual radio devices. The core entity of this framework is the radio manager (RM) which is responsible for radio enumeration, radio state definition, radio resource management, and communication with the other components such as the radio coexistence manager. Among these functional units of RM, radio resource management (RRM) is by itself a major component. RRM is in charge of monitoring the link quality of the radios and selecting the best radio for transmission based on the QoS requirements of the application. As different user applications require different QoS, the importance of the network attributes such as RSSI, SNR, etc., will vary accordingly. A scheme will be implemented in order to assign weights to these network attributes based on the QoS criteria. The radio access network that meets the QoS criteria will be chosen as the best radio access network.



Best radio access network

Qos criteria (QoS)

Throughput | Reliability | Latency | Jitter | Loss | ...

Radio link monitoring parameters

RSSI | SNR | MCS | TX Power | TX Gain | ...

Radios

LTE | WiFi | Bluetooth | ...

4 Jamming Protection

The broadcast nature of wireless communications makes it difficult to shield transmitted signals from benign external interference or the presence of an attacker's intent on by malicious jamming. Adversarial users are commonly modeled as either passive eavesdropper that tries to intercept a transmitted signal and extracts information without being detected or active jammer that tries to degrade the signal quality at the intended receiver and prevent the recipient from receiving the required transmitted information. These security threats have become a big concern due to the increasing reliance on wireless services. A modern swarm of Unnamed Assisted Vehicles (UAVs), for example, mostly use off-the-shelf infrastructure-less wireless communication, such as 802.11s in mesh mode, and can be very significantly affected by these kinds of threats.

Furthermore, with the advances in Software Defined Radios (SDR) technologies, it has become easy to launch a jamming attack on wireless networks, making it simple for an attacker to program off-the-shelf devices. These devices are both powerful, flexible, and capable of tuning to a huge portion of the radio frequency (RF). Moreover, there are many different types of jamming attack strategies that significantly deteriorate the performance of a victim's wireless communication system – often without the victim's knowledge. Therefore, this makes it imperative to study RF jamming mitigation strategies and implement them to mitigate their effects. At SSRC we have undertaken an approach whereby we have initially developed our own jamming toolset, to attack our own networks and expose weaknesses. This allows us to inherently understand the key challenges faced by standard techniques and apply state-of-the-art approaches such as AI and Machine Learning to not only detect an attack taking place but mitigate and avoid the attack altogether.

5 Next steps: lab testing and in-field testing

SSRC is developing a testing lab for experimentation, evaluation, and investigation of all the previously mentioned secure features. The laboratory will be composed of a big anechoic chamber, designed to stop reflections of either sound or electromagnetic waves, where experiments about jamming and malicious attack can be performed.

The laboratory will utilize the latest technology and automation software to analyze and enhance all distributed communications. In addition, the lab setting environment will allow SSRC to execute penetration testing on the Secure Comms Module, removing vulnerabilities and ensuring high resilient communications.

Finally, SSRC is preparing a mobile laboratory to perform experiments in-field. This will help to ensure analysis and execution in a real environment.

Technology Innovation Institute LLC
P.O. Box 9639
Abu Dhabi, UAE

tii.ae