Network Design

In a network comprising 100 workstations, 200 sensors, a variable number of IoT devices, as well as 8 distinct servers, all connected via different media, fulfilling different functions, the structure may become complex. The devices in the network are found at five physically separated locations – the operational control room (HQ), the laboratory, a data centre (DC), data collection sites (the ponds) and a remote cloud of IoT devices. Due to costs, the buildings (HQ, lab and data centre) will be connected wirelessly via Wireless Access Points but will internally make use of wired networks.

Physical Layout of System

The network can be viewed as one wide area network of four distinct subnets – three of which are further decomposed into subnets. Each subnet represents either a building or system of IP devices in the network. The network requirements for each are as follows (shown schematically in Figure 1):

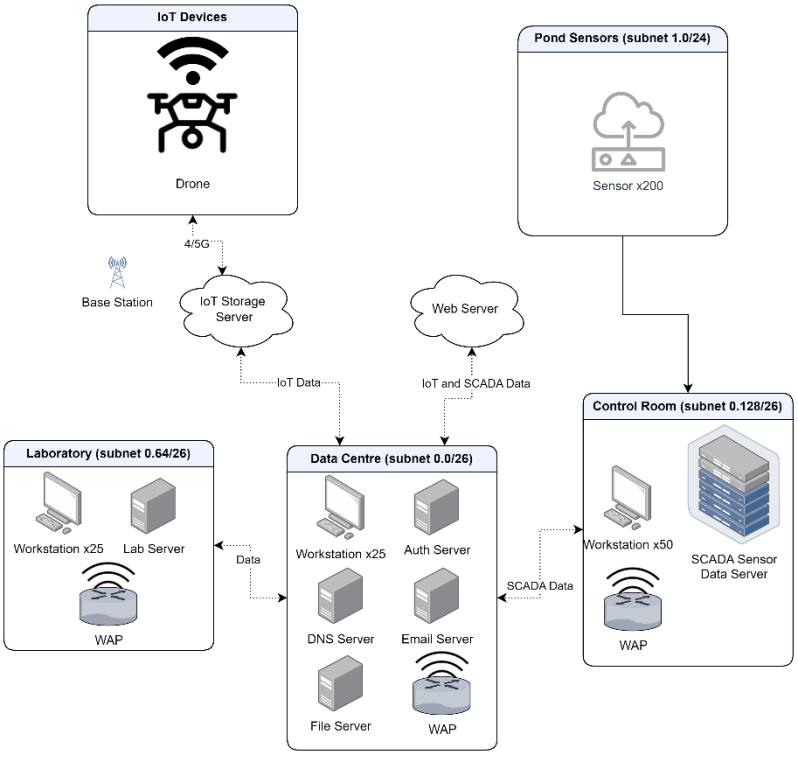

Figure 1 – Physical Layout of the Network

HQ contains 50 workstations and 1 data server that receives and stores data from the SCADA pond sensors, which, in turn, comprises 200 devices. The SCADA architecture can integrate with the TCP/IP stack effectively at the data link layer, transport layer, and application layer [1]. Due to the proximity of the SCADA devices to HQ, as well as the safety-critical role that HQ plays, the SCADA system will be wired using Ethernet cabling for simple compatibility with the HQ's wired IP network. The laboratory building is like HQ in that it comprises only workstations (25, instead of 50) and a single server used to store lab applications and processed data. The DC has the most complexity – it contains 25 workstations, 1 authorisation server, 1 DNS server, 1 Email server, and 1 file server. This building is accessed by the other two departments *via* wireless connection, and directly accesses the Web and IoT storage servers to manage data

presentation and data acquisition, respectively. The drones are IoT devices that will have a subscriber identity module (SIM) to allow them to connect to pre-existing 4G networks, since they are highly mobile devices. Each of the buildings (HQ, DC and the lab) will have wireless access points (WAPs) that provide a connection outside of each building.

The overall design of the wireless network is based on 802.11s architecture – a peer-to-peer extension of the 802.11 architecture that doesn't rely on access to base stations that are not managed by the company. The wide area network created here comprises both wireless (802.11s) and wired networks (Ethernet and SCADA).

IP Address Design of System

In order to logically separate each of the departments, the WAN is split into four subnets, representing department buildings and the SCADA network. Figure 2 illustrates this but for clarity, the subnets are described.

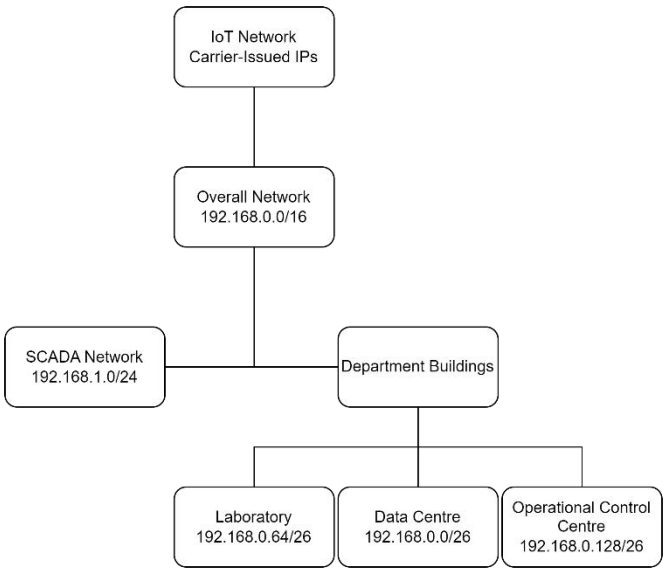

Figure 2 – Network logical design overview

The overall network assumes the class C private network IP address range (CIDR representation 192.168.0.0/16) due to the relatively small number of IP devices required (16 bits allows for 65,536 devices – far greater than the 308 IP devices in the system).

The department buildings divide the 192.168.0.0/24 subnet between them equally, resulting in 192.168.0.0/26, 192.168.0.64/26 and 192.168.0.128/26 subnets, each providing 254 addresses to the devices in their LANs. The devices within each department are also further divided into subnets. The laboratory and HQ have subnets for the workstations, as well as servers. The address ranges for both are slightly larger than required to provide room for growth if needed. The address range for servers in each subnet is 192.168.0.x+2/30 and that for workstations is 192.168.0.x+6/27 (Figure 3).

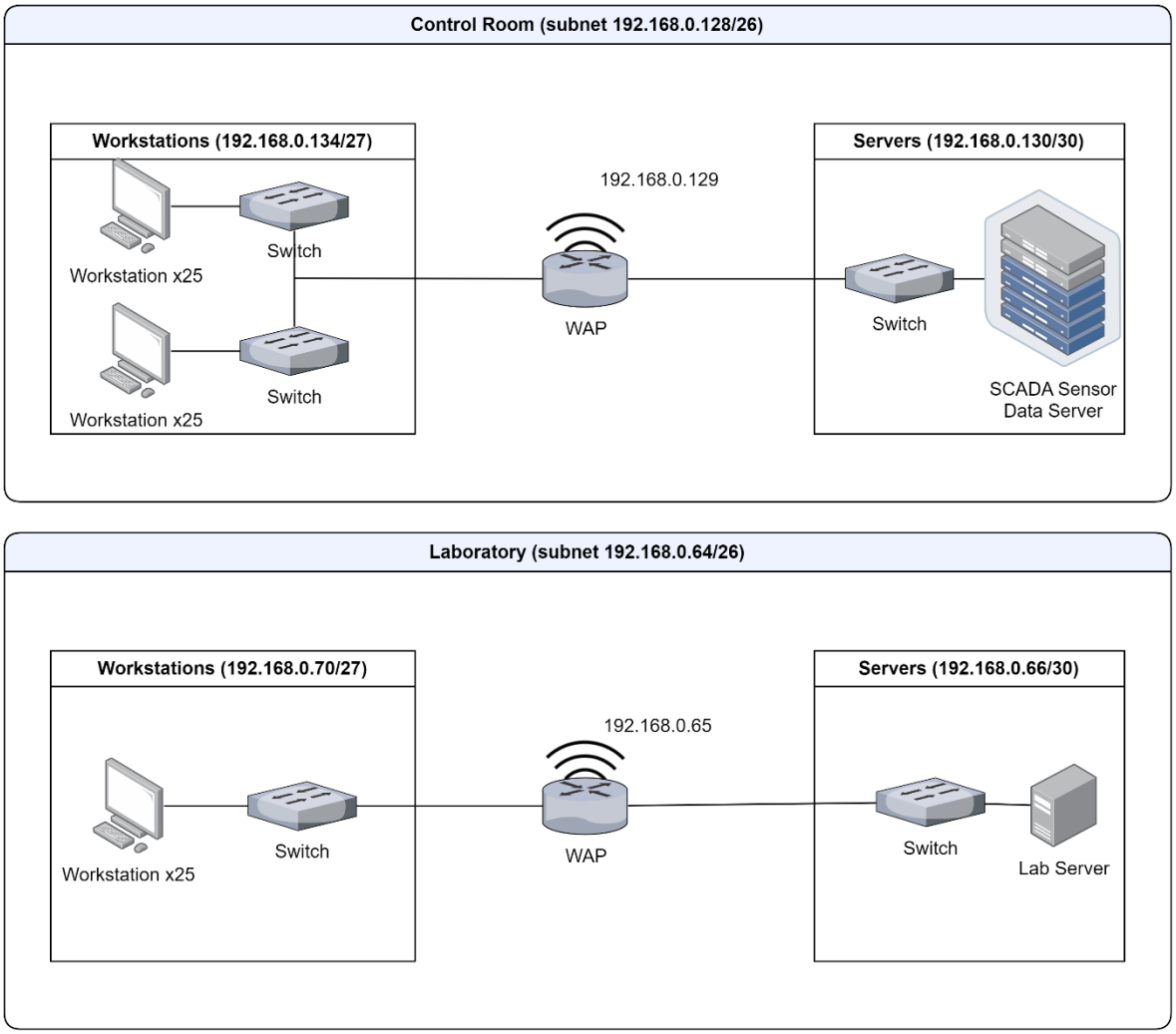

Figure 3 – IP Address Structure of Lab and HQ subnets

SCADA (Supervisory Control and Data Acquisition) is an industrial system architecture that creates a wired network of devices. To integrate with the IP network *via* the HQ, the DNP3 protocol suite can be encapsulated within TCP/IP in lieu of an application layer. As such, each device in the SCADA network must be assigned an IP address in the 192.168.1.0/24 range [2], which is enough to accommodate the 200 sensors, plus any master devices. The master device acts as an interface between the SCADA architecture and the 802.3 Ethernet architecture in HQ where the WAP acts as a portal between 802.11s and 802.3.

The IoT network can be logically associated with this system using a carrier-issued Access Point Name (APN). In doing so, the carrier creates a dedicated network for the IoT devices that can be used in conjunction with the cloud server. Each drone is also issued an IP address in this way.

Protocols and Network Components

The wireless access points are the most interesting component of the system for a few reasons. They should make use of the 802.11s Mesh Networking architecture to create a decentralised peer-to-peer network of. The 802.11s architecture is ideal for this scenario because it creates a lightweight ad hoc network with fewer hardware requirements outside of the WAPs. Each WAP acts as a Mesh Access Point (MAP) in this case. Since we are using the 802.11s structure, the

default routing protocol is Hybrid Wireless Mesh Protocol (HWMP, eq.1) – a MAC layer decentralised routing protocol that is derived from RM-AODV distance vector algorithm [3], [4].

$$c = \left[O + \frac{B_t}{r}\right]\frac{1}{1-e_f} \text{(eq.1)}$$

Where c is the cost for the node. This algorithm directly considers the physical and MAC layer overheads to reflect the condition of the wireless link. The *ad hoc* mesh topology of the wireless portion of this network minimises power consumption by reducing "waking time" of each node [5] whilst maintaining its ability to connect.

The MAP in the Data Centre may be used as an Internet access point. This is necessary to access the IoT Device server and Web server that are hosted on a cloud network. Web server usage will rely on file transfer over HTTP (Hypertext transfer protocol) *via* Web browsers on the 25 workstations in the DC. In fact, the DC is the central hub of data transfer between the three buildings as it has Web server access, email server hosting and file storage. The application layer protocols associated with these are HTTP, Simple Mail Transfer Protocol and either POP3 or IMAP to access emails, and File Transfer Protocol to manage transfer of files between departments' servers. Each of these would be used over TCP due to the guaranteed delivery of content required by each, as well as the fact that it is isn't time-sensitive or safety-critical.

Because the DC's WAP requires use of the Internet, it must have a public IP address, allocated by IANA. As such, this router will contain a NAT table to map private-facing IP addresses to the outer Internet. A probable NAT traversal mechanism used here would be TCP hole punching [6] or STUN [7]. The router in the DC will also play the role of DHCP server, using DHCP to dynamically assign IP addresses to devices in the entire WAN, allowing for seamless connection and disconnection of devices. For example, company-trusted laptops may be added to subnets with available address space if they connect to a switch via Cat5 cable.

In this network, the three WAP devices will be routers. This will isolate broadcast domains and collision domains between buildings, which would otherwise have drastic effects on data transfer. The layer 3 switching device also allows for IP-based routing, as well as layer 2 MAC routing (using HWMP). The layer 3 routing algorithm does not necessitate a DV algorithm, as the router can act as a centralised controller in a small software-defined network (SDN). A link-state algorithm like OSPF would suffice here.

The switch in each of the workstation subnets must be a high-speed 48-port switch, that will service 25 workstations each. These will be directly connected to the department's WAP. In the server's subnets, there will also be a smaller switch to allow for extra servers in future. Switches are used at the outermost regions of the network to divide large collision domains (not a function of hubs) into smaller domains, while still allowing for the broadcasting of data within a switched subnet.

IT Director Concerns

Signal Strength Mitigation

Wireless networks are known to have issues with signal attenuation, particularly in weather-prone areas [8]. Being reliant on other 802.11 architectures, 802.11s suffers attenuation across the entire 2.4GHz to 6GHz range. This occurs because radio waves emitted by devices are light, and light gets absorbed by physical matter. In principle, the more matter along the path that a radio wave will follow, the more absorption and signal attenuation. In conjunction with this,

radio waves are also affected by two phenomena known as multipath and specular propagation. Specular propagation refers to the deterministic path that light may follow from transmitter to receiver, which may be contributed to by reflections from smooth or reflective surfaces (like open bodies of water). Multipath propagation refers to components of a received signal that are not deterministic. These propagated signals are the result of light being scattered by rough or curved surfaces such as buildings or organic matter like trees [9]. This dense multipath component (DMC) causes distortion in the received signal as the same signal will arrive at different rates or with different intensities (Figure 4). Another problem is posed by signal

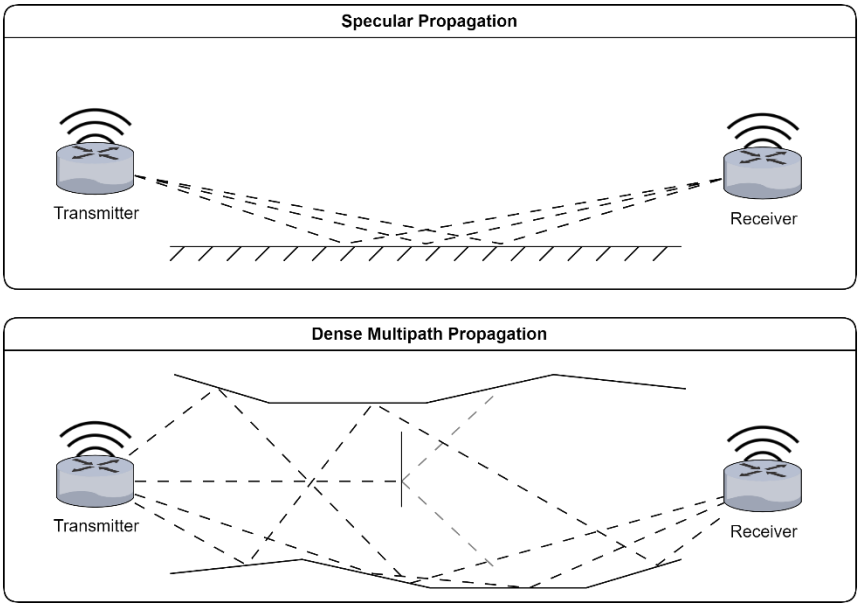

Figure 4 – Specular vs. DMC propagation. DMC propagation results in multiple paths with different time of flight, as well as attenuation by scattering materials such as leaves.

interference. Since 802.11 signals are radio waves in the 2.4 – 6GHz range, there will be other devices transmitting in this range too. IoT devices use this frequency band, as do the nationwide 4G and 5G networks. Signal interference can make it difficult to differentiate signals transmitted by one device from that of another [10].

So, combining the efforts of rainfall, interference and DMC, the wireless signal between nodes becomes erratic and potentially weak. The IT director wants to know how to overcome this using more devices and methods. First, let's address the devices we could use to mitigate the weakened signal.

802.11s is a mesh network standard that employs devices as mesh nodes. A mesh point (MP) is often a router device that, if it isn't acting as a MAP, will only relay transmitted data along its journey. As a level 3 device, it will perform data integrity checks at the MAC (cyclic redundancy check) and IP layers (checksum) before repeating the signal. Reducing the distance between MPs reduces signal noise by attenuation, interference and DMC. Another benefit of this is that more MPs results in higher redundancy and more potential routes for traffic to take depending on traffic conditions, which reduces the load placed on each MP. The downside to more MPs, however, is that each hop adds a delay proportional to the cost at each node (eq. 1). This means a balance must be struck between more nodes to reduce signal fading and fewer nodes to combat signal delay.

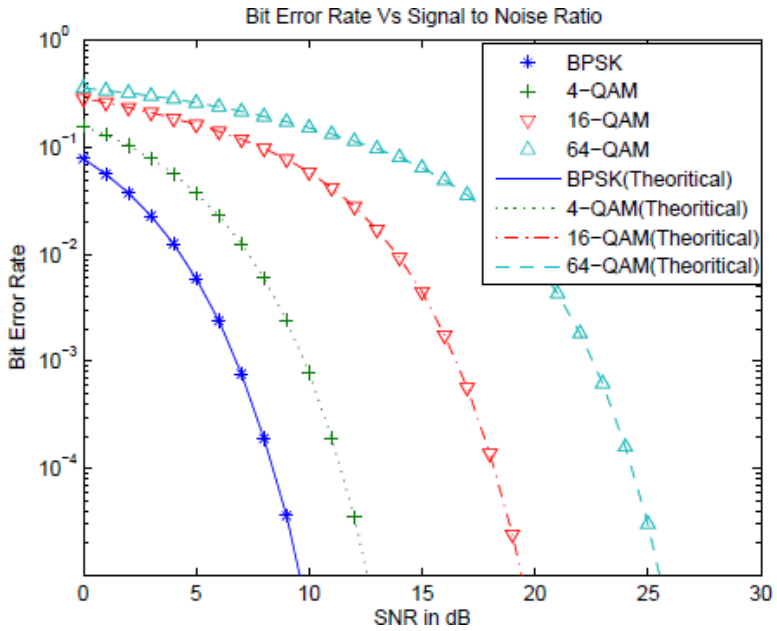

Figure 5 – from [12], graph illustrates relationship between transmission rate, Signal-to-Noise Ratio, and Bit Error Rate. The modulation techniques BPSK, 4-QAM, 16-QAM and 64-QAM have transmission rates of 6, 12, 24 and 48Mbps, respectively

Signal to noise ratio (SNR) has a direct relationship with transmission rate (selected by physical layer modulation) and bit error rate (BER) in received signal. Figure 5 illustrates that a higher SNR leads to lower BERs, and higher transmission rates lead to higher BERs [11]. Thus, a solution to reducing the *effects* of signal fading lies in Automated Modulation Recognition (AMR) – algorithms that select the most appropriate modulation based on current conditions. A machine learning approach to this can result in >96% accuracy of appropriate modulation [12], [13]. Choosing the right modulation technique will allow for consistent BERs regardless of weather conditions.

IoT Growth

A variable number of IoT devices in the network will inevitably come with further network requirements. With the current design of the network, all Internet access is passed through a single gateway in the DC. In fact, a significant proportion of network traffic passes through this gateway. If there are only a few IoT devices uploading to the IoT cloud server, a single WAP might be able to handle the traffic. In times of growth, it may necessitate that the other departments contain their own Internet gateways to reduce the load on the default gateway.

As mentioned previously, adding 802.11s MPs to the network introduces redundancy, offering multiple routes for data to be passed along – in the event of an MP's failure, other MPs can offer an alternative route from source to destination [14]. This improves resilience of the network, particularly in adverse weather conditions or maintenance periods.

Quality of Service (QoS) can be implemented in several ways to decrease the load placed on routers, and to deliver prioritisation based on needs. The 802.11s standard, based on 802.11e, uses EDCA to assign a class-based arbitration number to frames [15]. The priority classes can be found in Table 1a. Other class of service protocols exist [16], [17], but EDCA is a distance-based prioritisation technique, meaning that it balances the priority classes with the distance that the packet has had to travel over [15]. Prioritising data that has travelled less distance (i.e.

that which comes from the DC, rather than HQ or lab) will improve the throughput of IoT data from the cloud.

On the Ethernet side of the network, 802.1Q implements VLANs over Ethernet. Applications running on workstations in each department will assign a priority code point (PCP) to the frame being passed down. The 802.1Q MAC inserts a VLAN tag into the regular 802.3 frame. There are eight priority classes laid out by 802.1p (Table 1b). If workstations are separated into VLANs, or applications apply different PCPs based on traffic type, priority can be given to processes that require higher throughput. Since the network uses both EDCA and potentially VLANs, there are two dimensions (three if you include distance) on which to prioritise data flow.

Priority Level	Name	Code
1	Background	AC_BK
2	Best Effort	AC_BE
3	Video	AC_VI
4	Voice	AC_VO

Table 1a – 802.11e PCP values. They can be roughly mapped to those found in 802.1p

Priority	Name
1	Background
2	Spare
0	Best Effort
3	Excellent Effort
4	Controlled Load
5	Video
6	Voice
7	Network Control

Table 1b – 802.1p PCP values. 0 is the default Best Effort

As a final recommendation, 802.11s mesh networks can be built on 802.11ax (Wi-Fi 6), which boasts more, and greater, modulation rates (up to 1024-QAM), as well as multi-user MIMO to allow for more simultaneous communication between MAPs. Due to the modular nature of 802.11, it is simple to upgrade these network devices as new technologies arrive (Wi-Fi 7, 8 etc.).

CISO Officer Concerns

IoT Devices

The CISO is concerned about the IoT devices connected to 4G. The primary issue is with security – how do we ensure that nobody is intercepting IoT data, joining the network of IoT drones, or reading any captured data? The simplest course of action is to use secure protocols. IoT devices will be uploading data to the cloud server using HTTP over TLS (HTTPS). TLS is a transport layer protocol operating above TCP that offers encryption and secure transmission using both asymmetric and symmetric encryption, as well as a 4-way handshake. The two types of encryptions ensure that any interception of data for any given session is secure, and the 4-way handshake ensures distribution of certificates and encryption keys before the connection is continued.

One way to ensure the IoT network remains closed to unauthorised individuals over 4G is to leverage the carrier-issued APN. The APN is managed by a trusted carrier that uses challenge-handshake authentication protocols such as RADIUS to (re)-authenticate devices throughout the course of their connection to the APN network. RADIUS is an application-layer authentication, authorisation and accounting protocol that will be run on the authentication server held in the data centre [18], [19]. This will also be a protocol running throughout the 802.3 network to regulate login credentials of lab, HQ and DC workstations. The APN network and its devices can be managed by the network manager using Enterprise Mobility Management, as well as the carrier itself. Because the APN is managed by the 4G carrier and the network

manager, credentials are only provisioned through these entities. Use of secure protocols like HTTPS over the APN ensure that the APN remains private.

SCADA Breach Implications

SCADA systems, just like any other network, are prone to security attacks leading to informational and physical issues. A SCADA system can be attacked laterally *via* a compromised network or using malware to intercept (man-in-the-middle) or disrupt communications (with DoS). In the event of a DoS attack, it would become difficult for the HQ to operate sluices and gates, with potentially dangerous implications for the water supply in York. Malicious attacks may also result in loss of control over pumps and gates, leading to untreated wastewater flowing into local rivers in unexceptional conditions. Naturally, this would lead to environmental damage as human and chemical waste are deposited in the ecosystem; furthermore, the Ouse is prone to flooding – if untreated water flows through during floods, it may become unsafe for humans in the area. If this were to happen, this would also likely be a breach of the permit YEWAT has to discharge water and it could be revoked.

If the SCADA system is breached directly and the connection to the rest of the network isn't secured, it's possible that the attacker could obtain information about the network and individuals working on it. This would be a breach of the Computer Misuse Act 1990 [20], and YEWAT could be held liable for breach of GDPR, costing them up to €20 million [21].

Overall, the transition from SCADA-based sensor technology to IP-based wireless sensors could prove beneficial. SCADA systems suffer from obsolescence and are considered legacy systems [22]. This makes them increasingly difficult and expensive to maintain and keep secure, leaving them and the network they are connected to more vulnerable. The 4G-connected IoT devices are considerably more secure because the connection is managed by a trusted carrier, and the technology is generally more maintainable. There are security issues with both, but there is more ongoing research in cellular network security than in SCADA security.

The transition between SCADA and IoT sensors could be a vulnerability – more workload placed on the network management staff results in poorer performance and more errors [23]. Taking example from the recent Linux vulnerability [24], [25], a tired worker is a vulnerable worker. A malicious expert might offer their help to the overworked network manager and plant malware and entry points in the network that would allow the friendly attacker access to the network. The more human interaction with a network in transition, the more issues it could cause.

References

[1] B. Galloway and G. P. Hancke, 'Introduction to Industrial Control Networks', *IEEE Commun. Surv. Tutor.*, vol. 15, no. 2, pp. 860–880, 2013, doi: 10.1109/SURV.2012.071812.00124.

[2] 'IEEE Standard for Electric Power Systems Communications – Distributed Network Protocol (DNP3)', *IEEE Std 1815-2010*, pp. 1–775, Jul. 2010, doi: 10.1109/IEEESTD.2010.5518537.

[3] A. Sgora, D. D. Vergados, and P. Chatzimisios, 'IEEE 802.11s Wireless Mesh Networks: Challenges and Perspectives', in *Mobile Lightweight Wireless Systems*, F. Granelli, C. Skianis, P. Chatzimisios, Y. Xiao, and S. Redana, Eds., Berlin, Heidelberg: Springer, 2009, pp. 263–271. doi: 10.1007/978-3-642-03819-8_25.

[4] C. E. Perkins and E. M. Royer, 'Ad-hoc On-Demand Distance Vector Routing', in *Proceedings of the Second IEEE Workshop on Mobile Computer Systems and Applications*, in WMCSA '99. USA: IEEE Computer Society, Feb. 1999, p. 90.

[5] X. Wang and A. O. Lim, 'IEEE 802.11s wireless mesh networks: Framework and challenges', *Ad Hoc Netw.*, vol. 6, no. 6, pp. 970–984, Aug. 2008, doi: 10.1016/j.adhoc.2007.09.003.

[6] B. Ford, D. Kegel, and P. Srisuresh, 'State of Peer-to-Peer (P2P) Communication across Network Address Translators (NATs)', Internet Engineering Task Force, Request for Comments RFC 5128, Mar. 2008. doi: 10.17487/RFC5128.

[7] J. Rosenberg, C. Huitema, R. Mahy, and J. Weinberger, 'STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)', Internet Engineering Task Force, Request for Comments RFC 3489, Mar. 2003. doi: 10.17487/RFC3489.

[8] E. Alozie *et al.*, 'A Review on Rain Signal Attenuation Modeling, Analysis and Validation Techniques: Advances, Challenges and Future Direction', *Sustainability*, vol. 14, no. 18, Art. no. 18, Jan. 2022, doi: 10.3390/su141811744.

[9] S. Jiang, W. Wang, Y. Miao, W. Fan, and A. F. Molisch, 'A Survey of Dense Multipath and Its Impact on Wireless Systems', *IEEE Open J. Antennas Propag.*, vol. 3, pp. 435–460, 2022, doi: 10.1109/OJAP.2022.3168400.

[10] P. Cardieri, 'Modeling Interference in Wireless Ad Hoc Networks', *IEEE Commun. Surv. Tutor.*, vol. 12, no. 4, pp. 551–572, 2010, doi: 10.1109/SURV.2010.032710.00096.

[11] R. A. Shafik, Md. S. Rahman, and A. R. Islam, 'On the Extended Relationships Among EVM, BER and SNR as Performance Metrics', in *2006 International Conference on Electrical and Computer Engineering*, Dec. 2006, pp. 408–411. doi: 10.1109/ICECE.2006.355657.

[12] A. K. Nandi and E. E. Azzouz, 'Algorithms for automatic modulation recognition of communication signals', *IEEE Trans. Commun.*, vol. 46, no. 4, pp. 431–436, Apr. 1998, doi: 10.1109/26.664294.

[13] B. Jdid, K. Hassan, I. Dayoub, W. H. Lim, and M. Mokayef, 'Machine Learning Based Automatic Modulation Recognition for Wireless Communications: A Comprehensive Survey', *IEEE Access*, vol. 9, pp. 57851–57873, 2021, doi: 10.1109/ACCESS.2021.3071801.

[14] R. Vaishampayan, J. J. Garcia-Luna-Aceves, and K. Obraczka, 'An adaptive redundancy protocol for mesh based multicasting', *Comput. Commun.*, vol. 30, no. 5, pp. 1015–1028, Mar. 2007, doi: 10.1016/j.comcom.2006.08.031.

[15] N. Shafiul, K. Chowdhury, Md. S. Hussain, A. Sultana, and F. Ahmed, 'Distance Dependent Service Differentiation of the IEEE 802.11e EDCA on Single Access Point Based WLAN Systems', *J. Bangladesh Electron. Soc.*, vol. 11, Jun. 2011.

[16] I. Onwuegbuzie, S. Razak, I. Isnin, T. Darwish, and A. Al-dhaqm, 'Optimized backoff scheme for prioritized data in wireless sensor networks: A class of service approach', *PLOS ONE*, vol. 15, p. e0237154, Aug. 2020, doi: 10.1371/journal.pone.0237154.

[17] A. Alawadhi, Mohd. H. Omar, A. Almogahed, N. Nordin, S. A. Alqahtani, and A. M. Alamri, 'DNBP-CCA: A Novel Approach to Enhancing Heterogeneous Data Traffic and Reliable Data Transmission for Body Area Network', *Comput. Mater. Contin.*, vol. 79, no. 2, pp. 2851–2878, 2024, doi: 10.32604/cmc.2024.050154.

[18] A. Rubens, C. Rigney, S. Willens, and W. A. Simpson, 'Remote Authentication Dial In User Service (RADIUS)', Internet Engineering Task Force, Request for Comments RFC 2865, Jun. 2000. doi: 10.17487/RFC2865.
[19] C. Rigney, 'RADIUS Accounting', Internet Engineering Task Force, Request for Comments RFC 2866, Jun. 2000. doi: 10.17487/RFC2866.
[20] E. Participation, 'Computer Misuse Act 1990'. Accessed: Jun. 24, 2024. [Online]. Available: https://www.legislation.gov.uk/ukpga/1990/18/contents
[21] 'General Data Protection Regulation (GDPR) – Legal Text', General Data Protection Regulation (GDPR). Accessed: Jun. 24, 2024. [Online]. Available: https://gdpr-info.eu/
[22] S. Brad, M. Murar, G. Vlad, E. Brad, and M. Popanton, 'Lifecycle Design of Disruptive SCADA Systems for Waste-Water Treatment Installations', *Sustainability*, vol. 13, no. 9, Art. no. 9, Jan. 2021, doi: 10.3390/su13094950.
[23] J. Fan and A. P. Smith, 'The Impact of Workload and Fatigue on Performance', in *Human Mental Workload: Models and Applications*, L. Longo and M. C. Leva, Eds., Cham: Springer International Publishing, 2017, pp. 90–105. doi: 10.1007/978-3-319-61061-0_6.
[24] M. Lins, R. Mayrhofer, M. Roland, D. Hofer, and M. Schwaighofer, 'On the critical path to implant backdoors and the effectiveness of potential mitigation techniques: Early learnings from XZ'. arXiv, Apr. 13, 2024. doi: 10.48550/arXiv.2404.08987.
[25] 'This backdoor almost infected Linux everywhere: The XZ Utils close call', ZDNET. Accessed: Jun. 24, 2024. [Online]. Available: https://www.zdnet.com/article/this-backdoor-almost-infected-linux-everywhere-the-xz-utils-close-call/