network

MDPI

Article

Unmanned Agricultural Tractors in Private Mobile Networks

Marjo Heikkilä [1,*,†], Jani Suomalainen [2,*,†], Ossi Saukko [1,†], Tero Kippola [1,†], Kalle Lähetkangas [3], Pekka Koskela [2], Juha Kalliovaara [4], Hannu Haapala [5], Juho Pirttiniemi [5], Anastasia Yastrebova [2] and Harri Posti [3]

1 Centria University of Applied Sciences, 84100 Ylivieska, Finland; ossi.saukko@centria.fi (O.S.); tero.kippola@centria.fi (T.K.)
2 VTT Technical Research Centre of Finland, 02044 Espoo, Finland; pekka.koskela@vtt.fi (P.K.); anastasia.yastrebova@vtt.fi (A.Y.)
3 Centre for Wireless Communications, University of Oulu, 90570 Oulu, Finland; kalle.lahetkangas@oulu.fi (K.L.); harri.posti@oulu.fi (H.P.)
4 Turku University of Applied Sciences, 20520 Turku, Finland; juha.kalliovaara@turkuamk.fi
5 JAMK University of Applied Sciences, 43130 Saarijärvi, Finland; hannu.haapala@jamk.fi (H.H.); juho.pirttiniemi@jamk.fi (J.P.)
* Correspondence: marjo.heikkila@centria.fi (M.H.); jani.suomalainen@vtt.fi (J.S.)
† These authors contributed equally to this work.

Abstract: The need for high-quality communications networks is urgent in data-based farming. A particular challenge is how to achieve reliable, cost-efficient, secure, and broadband last-mile data transfer to enable agricultural machine control. The trialed ad hoc private communications networks built and interconnected with different alternative wireless technologies, including 4G, 5G, satellite and tactical networks, provide interesting practical solutions for connectivity. A remotely controlled tractor is exemplified as a use case of machine control in the demonstrated private communication network. This paper describes the results of a comparative technology analysis and a field trial in a realistic environment. The study includes the practical implementation of video monitoring and the optimization of the control channel for remote-controlled unmanned agricultural tractors. The findings from this study verify and consolidate the requirements for network technologies and for cybersecurity enablers. They highlight insights into the suitability of different wireless technologies for smart farming and tractor scenarios and identify potential paths for future research.

Keywords: smart farming; remote control; unmanned tractor; 5G; private network; field trial; controller area network; ISOBUS; tactical network; cybersecurity

Citation: Heikkilä, M.; Suomalainen, J.; Saukko, O.; Kippola, T.; Lähetkangas, K.; Koskela, P.; Kalliovaara, J.; Haapala, H.; Pirttiniemi, J.; Yastrebova, A.; et al. Unmanned Agricultural Tractors in Private Mobile Networks. *Network* **2022**, 2, 1–20. https://doi.org/10.3390/network2010001

Academic Editor: Youn-Hee Han

Received: 29 November 2021
Accepted: 27 December 2021
Published: 30 December 2021

1. Introduction

Connectivity technologies are an essential part of modern agriculture called smart farming (SF), which utilizes various digital technologies to improve the efficiency of farming operations. SF utilizes the newest technologies to make farming sustainable simultaneously in environmental, social, and economic aspects. These developments are catalyzed by drivers such as the United Nations' Sustainable Development Goals (SDGs) and the EU's Green Deal. Sustainable farming aims to be achieved with precision farming (PF) technologies that provide customized and right-timed treatment for each individual location inside the fields. Recently, intensive acquisition of site-specific and market-related data has been introduced for farm management information systems (FMISs). In an FMIS, the use of real-time data and decision support software increases farmers' situational awareness and adds intelligent features to the decision-making process of farms. To be realized, SF demands communication solutions that are reliable and operational in rural and remote areas.

The current trend in SF technologies is increased automation and remote control of robots, tractors, and tractor implements. Major agricultural tractors and equipment

manufacturers aim to achieve fully autonomous systems. One of the steps toward fully autonomous operation is the development and assessment of remotely controlled tractors. This development increases the need for data and hence communication between machines [1]. One special case of increased automation, the principle of which was initially developed more than a century ago, is a master–slave tractor system in which the farmer controls one or several slave tractors from a master one [2]. The slave tractor can operate mainly independently, but the farmer takes control whenever needed. The first implementations were mechanical, but radio waves soon replaced them. Nowadays, the solutions, if applied, are fully digital. A remotely controlled tractor, regardless of whether it is controlled from the farm office or the cabin of another tractor, relies on reliable, high-quality communications and extended coverage of the network. Farms are usually located in rural and sparsely populated areas, where the data connection often limits or prevents farmers from utilizing solutions that demand high amounts of data [3]. Consequently, the main idea of the experiment reported here was to establish an ad hoc private network or a private network bubble to enable remote operations of a tractor performing a fertilization task in a field.

Autonomous and remote-controlled tractors have gained high interest from researchers in increasing productivity [4–8]. Approaches such as cloud-based dynamics control have been studied to improve the maneuverability, mobility, and handling performance of unmanned ground vehicles [9]. The remote control study defined in this paper focuses on supporting commonly used systems in agriculture, such as ISO 11783 [10], commonly known as ISOBUS. ISOBUS is a widely used communication standard for providing an open, interconnected system for on-board electronics. It allows connections between tractors and implements without dependence on the brand. ISOBUS is based on SAE J1939 protocol [11], including controller area network (CAN), which enables electronic control units (ECUs) for communicating through CAN buses; thus, together, they can create a uniform system. Autonomous control algorithms have been studied for agricultural tractors using ISOBUS standard-based communication [12]. Our study aims to enable remote control of the tractor interconnecting the in-vehicle CAN of the tractor and the CAN bus of the remote control system. CAN traffic relaying over IP networks has been identified as a potential solution for monitoring and remote controlling vehicles [13–16]. Cannelloni [17] is a software that allows controller area networks to be connected over a local area network but does not support secure data transmission over the internet or a mobile network. This paper describes the study of a solution based on Cannelloni, Socat [18], and secure shell (SSH) to securely transfer control messages over networks. We propose a solution that adapts to the limited resources in networks by enabling the transfer of only selected CAN frames.

Emerging communication technologies—5G, sensor networks, satellite systems, and tactical networks as wireless backbones—provide new opportunities for SF [19–21]. 5G provides a reliable, low-latency, high-capacity channel for vehicle communications, control, and surveillance [22]. Wi-Fi, satellite, and long range wide area network (LoRaWAN)-based sensor networks support monitoring, surveillance, and situational awareness in the farm environment. As SF and autonomous tractor scenarios involve external stakeholders and connectivity with different sensors and assets, cybersecurity is an essential requirement [23,24]. Cybersecurity architecture can build on wireless security [25], application layer security solutions for SF [26], the internet of things (IoT) [27], and vehicles [28]. However, there is a need to identify requirements for a combined SF cybersecurity architecture that addresses threats and challenges stemming from farm vehicles, IoT sensor networks, cooperative business models, scarce cybersecurity resources in SFs, and private network technologies. More trials and comparative research are also needed to verify the feasibility of different wireless networks and network interconnection solutions for SF applications.

This study is part of the PRIORITY project that develops and trials communication and digitalization technologies for business- and mission-critical end users. One of our agricultural scenarios—grass cultivation in a dairy farm—consists of four uses cases: (1)

the sensor systems in the animal shelter and fields, (2) drones and satellite remote sensing (Airbus Verde [29]) for data collection, (3) artificial intelligence for recognizing fertilizer spreading and foreign objects, and 4) unmanned tractors in which communication plays a significant role. Based on the scenario, a field trial with a private mobile network was built on an educational farm. This farm consisted of several different locations. Hence, the private network consisted of several private network bubbles [30], and elements that can form independent ad hoc private networks. These were used for tests in different environments to guarantee network performance in every location.

The study contributes to the scientific community by verifying the feasibility of different private networking and internetworking technologies for emerging smart farm and unmanned tractor applications. We collected and consolidated the requirements for telecommunications networks and cybersecurity. Practical experiences enabled us to define qualitative and quantitative demands related to functionality, performance, interoperability, and cybersecurity, as well as to identify technology gaps for future research. We also explored approaches to customize and optimize applications and networks based on needs in SF.

The remainder of this article is organized as follows. In Section 2, we describe the requirements for networks and security solutions. Section 3 describes the technology enablers—private networks, remote control software, and security components—that were trialed. The section also highlights the main results and insights gained during the development and trial. Section 4 describes our contributions in light of related research. In Section 5, we discuss the conclusions and recommend potential directions for future research.

2. Requirements from Autonomy and Remote Control in Smart Farms

Unmanned tractors with different capabilities and different ways to operate impose various technical requirements on the underlying information technology and communication infrastructure. Similarly, smart farm environments set their own restrictions and demands. This section explores these requirements, particularly from the perspective of network quality in Section 2.1 and cybersecurity in Section 2.2.

The autonomous and remotely controlled operations of farm machinery are actually the end points of a spectrum of operation modes. The International Society of Automotive Engineers (SAE) has defined the autonomy levels of vehicles ranging from no driving automation (Level 0) to full driving automation (Level 5) [31], as listed below:

- Level 0—No Driving Automation
- Level 1—Driver Assistance
- Level 2—Partial Driving Automation (“hands off”)
- Level 3—Conditional Driving Automation (“eyes off”)
- Level 4—High Driving Automation (“mind off”)
- Level 5—Full Driving Automation

A range of assisting technologies enables intermediate modes, where some of the functions are explicitly controlled by an operator, while others can be independently decided by the machinery. Such assisting technologies include global navigation satellite system positioning, video cameras, and proximity sensors. The tendency is from remote control to fully autonomous operation, as this will lessen the operator workload and hence improve efficiency. However, legislation and regulations set the boundaries for the operation. Currently, legislation in several countries, such as Finland, does not permit unmanned vehicles to operate outside closed environments. Before fully unmanned autonomous or remotely controlled tractors may become more common, the development of legislation is needed [32] to clarify liabilities.

2.1. Requirements for Communications Networks

The communication needs of remote control depend on the autonomy level of the vehicle, where no driving automation will be most demanding for remote control, and full driving automation may not need any remote control support.

A remote control system with control services, including cameras, sensors, and control devices, may involve many other services, such as weather forecasts, engine remote maintenance, cultivation plans, navigation, collision avoidance, and logistic information services. However, the most demanding service in terms of wireless communication is remote control in which the tractor is operated by a person from a remote area based on data from tractor cameras and sensors. For the scenario of remote control of the tractor, the communication medium must meet the requirements of latency and bandwidth for video and control data transfer.

Control data include steering-related information as well as feedback information. The status information from different tractor subsystems is also included in the transmission, such as temperature and battery levels. In the current trial, the tractor control was based on the CAN bus [33]. The CAN protocol specification allows bit rates of up to 1 Mbps. Our implementation optimized CAN communication by filtering CAN frames so that the tunneled network traffic utilized a 85-kbps bitrate from the tractor and a 53-kbps bitrate to the tractor. These bitrates were from measurements that may involve small amounts of other data traffic. The trialed tractor had five cameras: the forward-facing camera required a minimum of 2 Mbps constant bit rate, while the forward side-cameras, which did not need as good a video quality, could use 1 Mbps. In total, the five cameras required an uplink bitrate of 8 Mbps. A forward-moving tractor requires a minimum view of three cameras.

Concerning human remote control based on video camera views, humans will need 100 ms to recognize or become aware of stimuli, and a minimum 180 ms to see an object and make movements such as pressing a key [34]. Thus, the end-to-end latency of the system can have 180 ms in human intervention remote control. The end-to-end system latency consists of information processing delays, such as video processing and packet transmission delays, where video processing will have a dominant role [30].

When vehicle-to-everything (V2X) remote control involves autonomous services without human interaction, different latencies [35] and quality requirements apply. 5GAA Automotive Association [36] specified that the maximum latency tolerable for gaining awareness of pedestrians in danger is 100 ms, of which the recommended latency for communication is 20 ms when the assumed vehicle speed is 50 km/h. This indicates that the vehicle will move an additional 28 cm due to a network delay. 3GPP has also specified V2X requirements for cellular networks, as listed in Table 1, which vary between 5 ms and 100 ms (video stream to a remote cabin and CAN messages to the tractor). The trialed scenario did not involve use cases with close cooperation with other vehicles, such as platooning interactions, but it supported pedestrian safety, and 10 ms was the minimum latency caused by a network for one directional packet. If we assume a tractor with a velocity of 15 km/h and a safety limit due to a network delay of 28 cm, the allowed latency is 67.2 ms (33.6 ms in one direction). However, when tractors are equipped with sensors that can autonomously prevent collisions or when tractors are not used in road traffic, but in private fields without external pedestrians, these requirements may be more relaxed.

Table 1. Network quality of service requirements for different unmanned vehicle-related services from 3GPP [37,38] and 5GAA [36]. Packet delay requirements are additional delays due to a network for one directional transmission.

Services	Packet Delay Budget	Packet Error Rate
V2X messages, remote driving [37]	5 ms	10^{-5}
Information sharing for automated driving between vehicles or vehicle and road side unit [38]	100 ms	10^{-4}
Platooning informative exchange [38]	20 ms	10^{-1}–10^{-4}
Sensor sharing [38]	50–100 ms	10^{-2}
Video sharing [38]	10–50 ms	10^{-4}
Cooperative collision avoidance [38]	10 ms	10^{-4}
Notification of dangerous situations [36]	10 ms	10^{-3}
Remote control of a tractor (15 km/h)	34 ms	10^{-3}

2.2. Requirements for Cyber and Network Security

Security in smart farming and unmanned tractor scenarios is motivated by different cyber threats such as discontinued business due to ransomware, network unavailability due to botnet signaling, and human, animal, and food safety due to integrity violated machinery and vehicles or tampered situational awareness. Security challenges in the farm context vary. First, the heterogeneous device landscape indicates that security management and delivering security updates to devices are more challenging. Different devices are also dependent on each other. Business models are becoming more complex from a networking point of view. For instance, specialized service providers, such as tractor entrepreneurs, may need to connect to information sources on the farm. External input, such as satellite images or weather forecasts, may come from various sources. Moreover, maintenance and repair services are often outsourced and external users or devices may need to be granted access to assets, such as tractor systems, for a temporary period of time. Further, security cultures in farms are more varied. Farm personnel often have limited experience, skills, and resources for security configurations, making security error-prone. Finally, physical protection is often limited. The farm network can span large geographical areas without human guarding or monitoring.

The cyber and network security architecture for private network bubbles must be able to address these challenges and support known applications and devices. At the same time, the architecture must be flexible to address emerging applications and security threats, and support restrictions in smart farms (e.g., demand of being easy to use and suitable for harsh conditions). Central objectives as well as functional and qualitative requirements for the security architecture are highlighted in Table 2.

Table 2. Objectives for cyber and network security architecture.

Security Objectives	Requirements and Potential Solutions
Communications security	Access technology specific confidentiality, authenticity, integrity, and replay protection solutions. 3GPP security and Wi-Fi security cover essentially wireless channels. The 3GPP specifications [39] extend protection to backhaul and support application layer communication.
End-to-end security	Application layer solutions, including SSH, TLS, and SRTP, secure critical communications when infrastructure cannot be completely trusted. In private networks where edge computing is used, for example, for accelerating computation or interoperability, end-to-end security may not be feasible. These cases demand that security breakpoints in the edge are trusted.
Network and subsystem authorizations	Practical access control requires easy solutions to distribute credentials, that authorize access to networked assets—services and data stored in the network. Fine-grained service specific access control mitigates potential insider and malware attacks. Firewalls, which enforce authorizations, are needed in network borders and in many hosts within the network. Network credentials, such as eSIM, can be delivered, for example, through QR codes. Application credentials, for example, through delegated authorization, such as OAuth2.
Resilience	Solutions to assure availability under denial of service attacks or in congestion situations. Reactive security, access control, and traffic prioritization solutions as well as sufficient and redundant capacity, such as satellite links, should be applied when possible.
Secure cooperation	Secure networked business models require trusted external partners. Access to partners' external assets must be secure and integrity verified. Externals access to assets and functions in smart farm should be restricted by time and capabilities to minimize insider threats.
Security posture of subsystems	Technical and procedural approaches to manage and verify that different devices in farm and tractors are secure, for example, are enforcing security policies and are running trusted up-to-date software. The network is monitored to detect security policy and integrity violations indicating security breaches or malware.

3. Field Trialed System

This section describes the components and subsystems that were integrated into the field trial that was held in Saarijärvi, Finland, in June 2021. Different technologies and assets in the smart farm were interconnected with several alternative wireless private networks. The network architecture and technology configurations are described in Section 3.1. A smart unmanned tractor prototype, Valtra N175D Direct Model [40], from AGCO, was remotely controlled through the network. Section 3.2 describes our implementation and optimization to enable remote control. We also tested tractor's autonomous driving capabilities, which were in level 2 ("hands off"). A large number of sensors exist on smart farms. These sensors provide situational information that may be applied, for example, when planning tractors' operations and when operating tractors. Access to sensitive information, tractor subsystems, and other farm assets is restricted to identified, authorized, and trusted users and devices. Section 3.3 describes cyber and network security building blocks.

3.1. Local Private Network

This section describes the architecture of the local private network used in the smart farming trial for remote areas. Figure 1 shows the trial network topology at a high level.

The topology enables remote control of a tractor via multiple local access points and via the internet. It also offers a connection to and inside a smart barn for remote surveillance. More specifically, the optical and thermal cameras and air quality sensors allowed us to

monitor the welfare of the animals and the quality of their surroundings inside the cow shed. Soil sensors provided environmental information about the field.

The trial topology is a hybrid combination of multiple ad hoc network bubbles. Figure 2 shows the setup of the trialed ad hoc private network. Here, the Bittium Tactical Wireless IP Network (TAC WIN MESH) [41] offers the backbone network for three local 4G access points and one local 5G access point. The backbone network is built with three tactical nodes, for example, tactical routers with radio heads. These routers can automatically reroute any given data from the source to the destination via alternative routes, if the primary route fails. One tactical router has a wired connection to the internet. The internet connection is then shared with the office and with the end users of the access points.

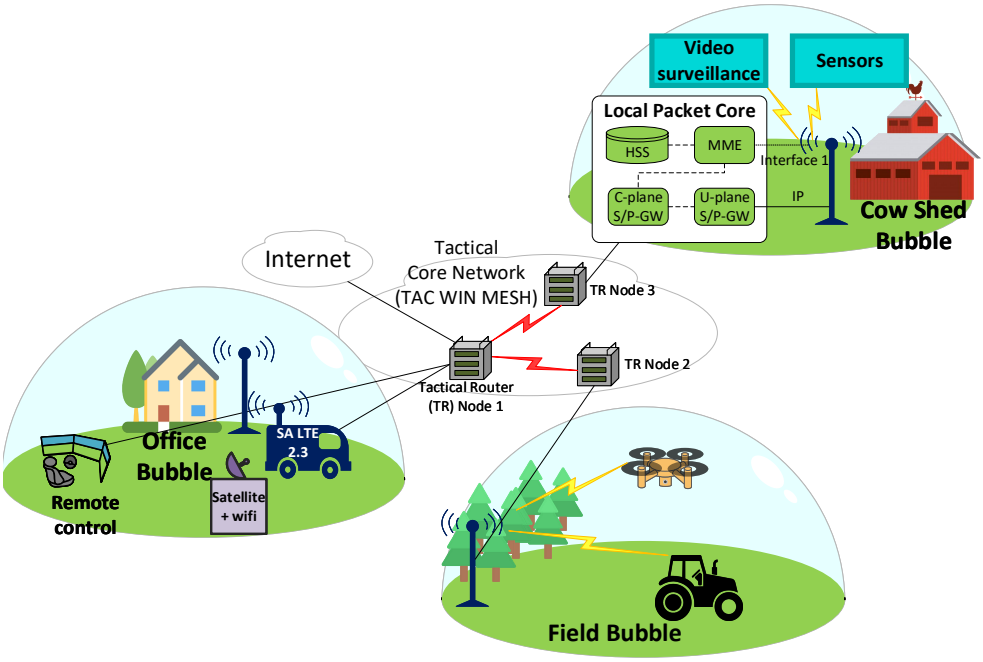

Figure 1. Topology of the private network bubble system with three interconnected bubbles.

Figure 2. Setup phase of ad hoc private network bubble.

Every tactical router has a wired connection to either a 4G or a 5G access point, or both. Next to the office, there is a 5G stand-alone access point for wireless users. It uses a stand-alone 5G core for authentication. The office bubble has a stand-alone 4G access

point in a van. This 4G access point uses an EPC in the van to authenticate the end users. The van EPC is also used for a 4G access point next to the field that needs to be fertilized with the tractor. There is a separate stand-alone 4G access point outside the smart barn. This access point uses its own 4G EPC for authentication. With this kind of setup, bubbles can also be used independently.

In addition to the setup shown in Figure 1, air sensors are connected to the internet via LoRaWAN [42,43] and soil sensors in the fields are connected with LoRaWAN and with ISM bands and 3G [44]. This technology provides a long range and a good battery life. Moreover, the tractor can use a commercial 4G network with a higher priority subscriber identity module (SIM), denoted as QC128.

A satellite connection is also available as a backup communication system [45]. The geostationary (GEO) satellite provides sufficient throughput but cannot support remote control of the tractor due to its large latency. Nevertheless, GEO satellites can be efficiently used to share situational awareness data for farms. Although commercial mobile network infrastructure is widespread, there are still gaps in rural and sparsely populated areas. Another aspect is that it might be impossible to deploy terrestrial infrastructure. Satellite systems can provide a fast deployment solution. Once the antenna is deployed, and line-of-sight to the satellite is in place, transmission is possible. See Table 3 for more specific information about the trial access points.

Table 3. Comparing technologies for tactical bubbles.

	Technology Capabilities in Trialed Private Networks		
Characteristics	**StandAlone LTE/Cow Shed Bubble**	**StandAlone LTE van + Field Bubbles**	**Satellite & Wi-Fi**
Coverage avg	1000 m	500–1500 m	Global
Capacity uplink avg/max	2 Mbps/8 Mbps	N/A/10	9.8 Mbps
Capacity downlink avg/max	7 Mbps/108 Mbps	N/A/50	34.0 Mbps
Latency (RTT median)	50–70 ms	30–85 ms	700 ms (geostationary)
Security	3GPP [46]	3GPP [46]	WPA [47]
Frequency	2350 MHz	2310 MHz	26.5–40 GHz
Band	40	40	K_a
Bandwidth	20 MHz	20 MHz	N/A
Transmit power	5 W	1 W	N/A
Ant. height	5 m	10–21 m	0.75 m
Rx antenna gain	Omni 2 dBi	Omni 2 dBi	N/A

3.2. Remote Controlled Tractor

In the field test, a tractor was remotely controlled over mobile networks. The objective was to drive the tractor remotely to the field using a fertilizer work machine. After that, the work machine was able to automatically fertilize the field together with the tractor. Remote control was then used to monitor and guide the tractor. To do this, the remote control cabin had a steering wheel, pedals, and other controls needed for operating the tractor (Figure 3). Three screens were attached to display video feeds from the tractor.

Figure 3. Elements of the remote-controlled tractor: the remote control cabin on the left, the remote-controlled tractor on the middle, and the computer for CAN tunneling over mobile networks on the right.

Figure 4 shows an overview of the network and devices for remotely controlling the tractor. All network traffic went over a virtual private network (VPN) connection, and from the device's perspective, they were all in the same local area network. A router [48] from Goodmill Systems connected the tractor to the tactical network using various mobile networks. By default, the router uses all these connections simultaneously and switches between them to provide the best possible service. For the trial, the router was configured to use the networks one at a time for testing purposes.

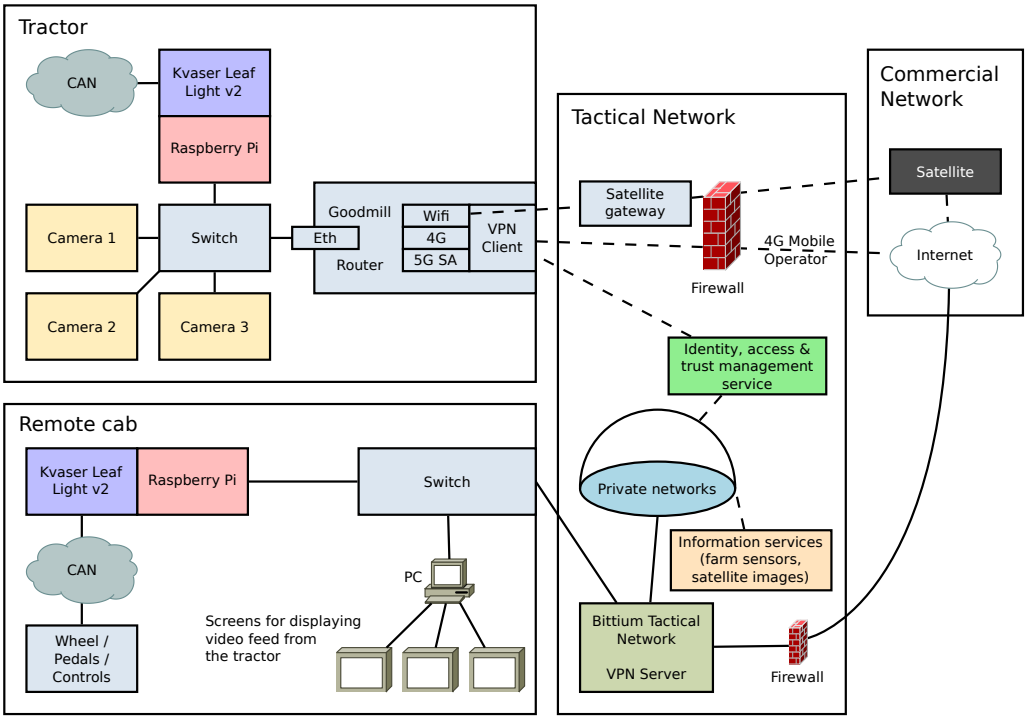

Figure 4. Simplified overview of the network from a remote controlling perspective.

3.2.1. Remote Controlling Tunnel between the Tractor and the Remote Control Cabin

The target for the remote control was to verify the remote controllability of the tractor through different trial networks. This was done by transmitting CAN messages over the network. While exploring the possible technologies, SocketCAN [49] was found. SocketCAN allows for controlling and programming the CAN interface as a standard network interface. SocketCAN userspace utilities and tools make it possible to set up and test the CAN network with ease. Furthermore, the Cannelloni tool allows the transfer of CAN data over an Ethernet tunnel.

Cannelloni supports tunneling over user datagram protocol (UDP) or stream control transmission protocol (SCTP). The UDP is faster but unreliable, while the optional SCTP provides reliable transport. At this point in the research, there was a perception that all the messages should go through. Therefore, SCTP was chosen.

Initial testing was conducted using virtual CAN interfaces from SocketCAN. Functionality was then tested using real hardware. For this, Kvaser Leaf Light v2 was chosen, which has a SocketCAN driver available directly on the Linux kernel. Kvaser adapters were verified to work using a test CAN network. The test CAN network was a cable made using a single termination resistor between the high and low CAN lines. After CAN tunneling was possible in a local area network, the next goal was to conduct traffic securely over the public network. The SSH port forwarding was chosen to transfer the CAN traffic over the network and encrypt it. However, SSH port forwarding does not work with SCTP. Therefore, one more step was required to convert SCTP to the transmission control protocol (TCP). Protocol conversion was done using the Socat utility. Figure 5 shows the components and protocols used to tunnel CAN traffic over networks.

Both the tractor and remote control cabin have Raspberry Pi 4 computers connected to the local CAN using a Kvaser USB adapter. The Raspberry Pi on the tractor side works as a client to establish a connection to the server Rasberry Pi computer on the remote cab. The idea is that the remote control cabin server has a known address on the internet, while the tractor can be behind the mobile operator's network address translation (NAT) and or firewall. The software on the tractor side will consistently attempt to establish a connection to the server until the connection is made. If the connection to the server is lost, the client continues to try to make a new connection.

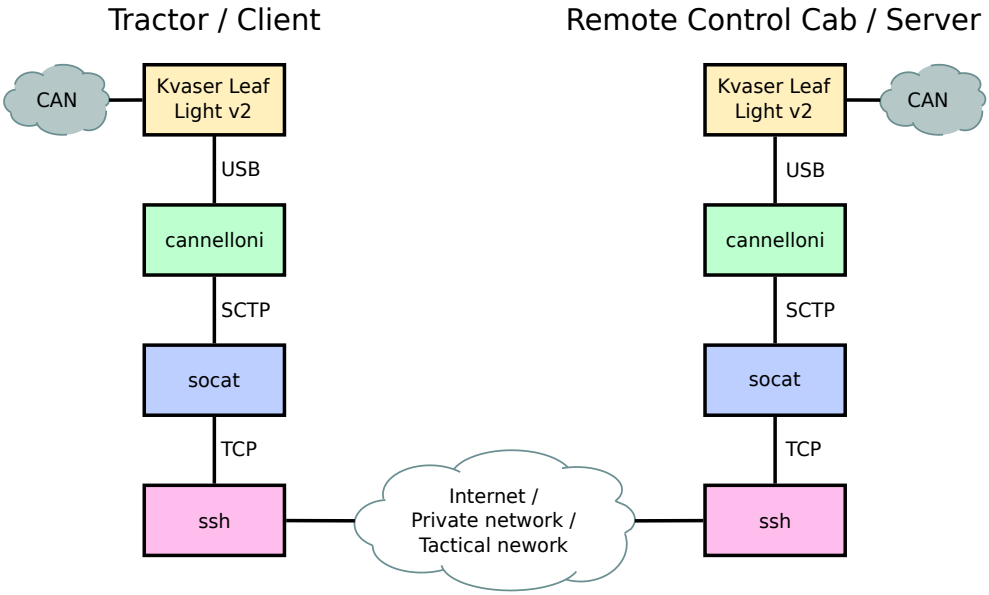

Figure 5. Components and protocols for controlling traffic. The computer on the tractor works as a client and establishes a connection to the server. The server computer runs on the remote control cabin.

Devices on the tractor generate a lot of CAN traffic, most of which are not relevant for remote control. The same is also true for the remote control cabin. Therefore, message filtering was added for both ends to pass through only the required messages. Filtering was implemented by modifying the Cannelloni software to accept filtering rules for outgoing and incoming traffic. During the field trial, it was sufficient to filter outbound traffic at both ends.

3.2.2. Filtering, Frame Aggregation, and Overhead Measurements

In the Cannelloni program, we can specify how long to wait for new CAN messages before forwarding them through the tunnel. A longer time allows sending several CAN frames in one Ethernet frame, which improves throughput but causes latency. For time-critical messages, it is possible to provide their CAN IDs and customized timeout values. During the field trial, a very short timeout of 5 ms was used to minimize latency. A short timeout causes a lot of network overhead, but this was not an issue because filtering also reduces the number of CAN frames to be sent to the minimum.

Filtering rules can be assigned to the SocketCAN interface. The filtering rule includes a mask and filter ID. A received CAN frame is passed if:

$$\text{Received ID \& Mask} == \text{Filter ID \& Mask},$$

where & is a bitwise AND operator, and == is equal comparison.

The Cannelloni program was modified to allow for filtering rules from files. A rule file defines masks and filters IDs. These rules can be applied to both incoming and outgoing CAN frames. Outgoing frames from the local CAN network are filtered using SocketCAN,

located directly in the Linux kernel. A similar implementation was added to the Cannelloni for incoming frames over a network, which checked CAN frames after they were decoded.

The Cannelloni performs CAN frame aggregation by adding a 5 bytes header containing the protocol version, frame type, sequence number, and number of CAN frames included. This data is then encapsulated in the SCTP message, which adds around 32 extra bytes, depending on how much chunk padding is needed. Next, the SCTP message is converted to TCP using Socat. Conversion removes chunk padding and replaces the SCTP header with the TCP header, which is 4 bytes longer. Finally, data are encrypted and sent using SSH, which also increases packet size. In the worst case, for sending one 13-byte CAN frame, 171 extra bytes are needed, which indicates 93% overhead.

Table 4 shows the amount of network overhead based on how many CAN frames are sent together. The CAN data column is the number of bytes for actual CAN traffic. SCTP and TCP indicate packet size after the aggregation and conversion steps. SCTP and TCP values are without Internet Protocol version 4 (IPv4) and Ethernet II headers. The total bytes column contain all the bytes sent over the SSH, including the ACK message. The extra bytes and overhead columns show how many extra bytes are needed and how much of the transmitted bytes are needed to tunnel the payload over the networks.

Table 4. Network traffic efficiency, depending on how many CAN frames are transmitted at once.

CAN Messages	CAN Data	SCTP	TCP	Total	Extra bytes	Overhead
1	13	48	50	184	171	93%
2	26	60	63	200	174	87%
4	52	88	89	224	172	77%
8	104	140	141	280	176	63%
16	208	244	245	384	176	46%
32	416	452	453	592	176	30%
64	832	868	869	1008	176	17%
96	1248	1284	1285	1424	176	12%
100	1300	1336	1337	1472	172	12%

A customized CAN message was used to control a tractor. The information required to drive a tractor was packed into a single message. The electronic control unit (ECU) was programmed to control the tractor based on the message as long as messages arrived within at least 100 ms of each other. If the interval between messages is longer than 100 ms, the ECU starts to stop the tractor for safety reasons. The interval target introduces a requirement for even network communication and how long Cannelloni can wait for frame aggregation. When the interval requirement is not met, steering and driving are jerky because the ECU occasionally tries to stop the tractor.

3.2.3. Remote View from the Tractor

For the remote control of a tractor, it is essential to see where the tractor is going. Therefore, various cameras (listed in Table 5) were tested during the trial to provide views from the tractor. For safety reasons, a human driver was also in the tractor cockpit, ready to take manual control if needed.

The shortest latency was obtained using the H.264 codec. Other codecs available from the cameras were H.265 and MJPEG. The Hikvision camera with the Chrome browser extension provided the best results on the screen-to-screen, with a delay of about 100 ms. For the other cameras, the delay was about 250 ms. Multiple cameras were tested simultaneously by opening their views on separate screens, but the best results were obtained using a single-camera setup. When several video transmissions were used, the video would lag and freeze from time to time.

The cameras were connected using two different router setups. With the Goodmill router, the camera traffic was forwarded through a cloud server, and with the Teltonika

router, the traffic was directly forwarded using port forwarding. Dynamic DNS (DDNS) was also used to allow a connection to the cameras with dynamically changing IP addresses.

Table 5. Devices used to provide remote views from the tractor.

Device	Name
Camera	AXIS P3935-LR
Camera	Hikvision DS-2CD2326G2-ISU/SL
Camera	Dahua IPC-HDW4231EM-ASE
Camera	Dahua IPC-B1B20P (×2)
Switch	Tenda TEF1105P PoE-switch
Router	Teltonika RUT955
Router	Goodmill w24h-S
PC	HP ProDesk 600 G3 DM Mini PC Core i5-7500T 2.7 GHz 8/256 SSD (SATA) Win 10 Pro
PC	Lenovo C24-25

3.2.4. Network Quality Measurements

This section describes how we conducted a performance analysis of the available networks. Network quality must be measured to verify reliable remote control. In this trial, adequate remote control required at least two high-definition videos. Furthermore, these videos require a total throughput of 5 Mbps in the uplink direction. An uplink throughput of 5 Mbps was then obtained with the 2.3 GHz time division duplex van mounted base station when the reference signal received power (RSRP) was over −98 dBm. Figure 6 shows the RSRP measurements of the base station. From this figure, it is possible to roughly estimate the remote driving range of this base station configuration. Note that the uplink-downlink frame configuration had two subframes for uplink and six for downlink due to the obtained frequency license.

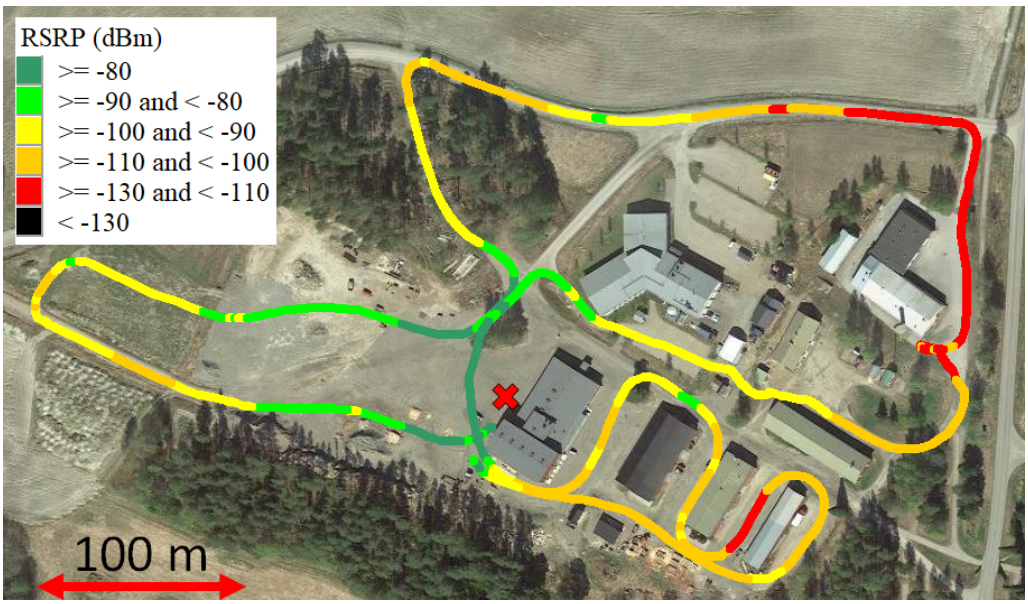

Figure 6. Standalone private LTE 2.3 base station RSRP measurement. The red X marks the van-mounted base station with a transmit antenna height of 10 m.

The round-trip time (RTT) of the same base station is shown in Figure 7. Note that the one-way delay is approximately half of the RTT. Thus, the control messages reaches the tractor faster. Whenever a network is good enough for videos, the control messages are fast enough with the local network. We also measured commercial network round-trip times. The RTT was approximately 30–40 ms faster with a local base station than with a commercial network. The delays were sufficient for the use case.

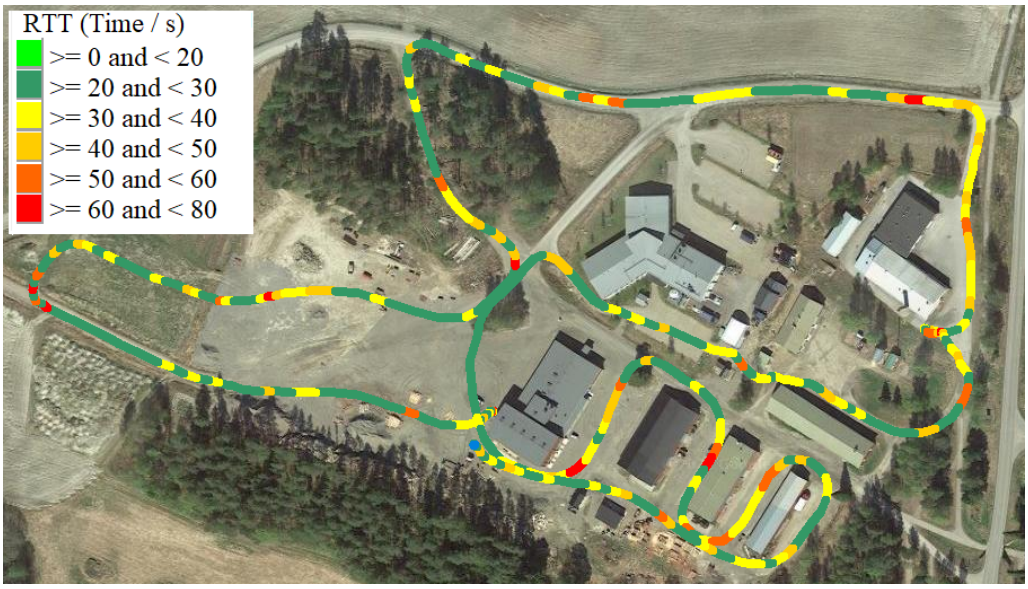

Figure 7. Standalone private LTE 2.3 base station RTT measurement to router 1.

3.3. Cyber and Network Security

This section describes the applied security solutions that fulfil the objectives for security architecture, which are presented in Table 2.

The baseline security—confidentiality and authenticity—of communications is based on standard security architectures [39,47] for access and backhaul networks. Radio access is secured with appropriate security protocols for 3GPP or Wi-Fi networks. Key distribution is based on physical SIM in the case of 4G and 5G networks and on passwords, which can be shared with QR codes, for example, in the case of Wi-Fi in the satellite bubble. Further, different application-layer security protocols were utilized to provide additional security, such as SSH for CAN and TLS for sensor communication and web-based information services.

Communication between different private networks, which were inter-connected with a tactical core network, was secured with frequency hopping and adaptive modulation [41] and connections that spanned over the internet were secured with IPsec based VPN. The internet and other external services were behind firewalls, which were hosted within the tactical core network or outsourced for commercial service provider.

Custom security needs in smart farming and remote-controlled tractor scenarios include fine-grained access control mechanisms to segregate users and devices, thus protecting assets and minimizing the threat of malware. Custom security needs in remote-controlled tractor scenarios emphasize the trustworthiness, reliability, and integrity of the safety-critical components as well as the availability of low latency communication needed for navigation.

3.3.1. Access Control and Security Posture Management for the IoT

We trialed a solution for identity, access and trustworthiness management. The proposed access control service authenticates and verifies IoT devices that request access to services within the network. The widely used OAuth 2.0 identity and access management framework [50] authorizes new users and devices for the information and application services in the farm. In addition to authenticating IoT devices, the solution verifies that devices with trusted execution environments are running the expected, trusted software. To support networked business models in SF, authorizations can be temporary.

During the trial we verified the feasibility of our extensions to the OAuth 2.0 framework. The extension, which we specified in [51], allows IoT devices to prove their software integrity using device attestation as part of OAuth's delegated authorization protocol. The approach is able to detect and locate compromised devices and malware as well as verify the trustworthiness of devices requesting access to services. The solution and

performance measurements [51] demonstrated the feasibility of the approach. The latency (during the security handshake phase) depends on the processing capabilities of the IoT platform. Total latency of handshake—made when a device first accesses a service and that contains authentication and attestation phases—was around 11.1 s for the ARM TrustZone-based NuvotonM2351 class micro-controller. The attestation procedure is a relatively rare operation and will not impair the feasibility of sensor applications.

3.3.2. Resilience through a Satellite Link

The network can recover from detected threats and failures in different ways, for example, by replacing compromised components with trusted ones. We also studied recovery with alternative connections, particularly using alternative private networks, commercial networks and a satellite link.

A satellite link provides a backup backhaul channel that may be utilized when commercial backbaul is unavailable. Our satellite solution included a GEO satellite, a connection that was arranged by Dawson Ka-Sat SC-Zero 70K nomadic terminal from Viasat. This satellite terminal is capable of providing broadband connectivity. Transmission was performed using the Ka-band. The satellite terminal was then connected to the Goodmill router. The router is a multi-channel solution that allows us to monitor the networks and change the wireless transmission technology based on the QoS or other rules employed at the router. It is also possible to direct specific traffic flows to certain tunnels and set the desired backhaul for them. This approach can add an extra layer of protection for security-critical endpoints (such as a UE) by directing sensitive traffic through the most trustworthy route. Thus, when security incidents are detected in the commercial network, based on the specific traffic rules the Goodmill router can switch connectivity to use the secured satellite backup link.

Apart from the backup satellite link, the utilization of satellite systems can be beneficial in terms of traffic balancing. The terrestrial network could be used to stream the video and the satellite network could be used to broadcast situational awareness data.

4. Related Works

This section reviews and compares related research with our contributions. In particular, we will survey and analyze efforts related to vehicle remote control as well as to 5G networks and cybersecurity architectures for smart farms.

The CAN bus protocol allows communication between the electronic control units inside the vehicle and is widely researched as an embedded system to get tactical and status information from the vehicle and its surroundings. The protocol has been applied for data collection and monitoring, such as temperature acquisition for mining equipment [52] and status monitoring for off-road studies [53]. There are also research studies concentrating on steering system based headlight control using CAN [54], and utilizing the CAN protocol to obtain data from the driver for further analysis [55]. However, many of the reviewed works related to the CAN protocol concentrate on modeling and simulations and not actual integrated solutions. One of the few implementation works [56] describes a combination of real-time kinematic positioning and global navigation satellite system and the CAN bus protocol for control algorithms of the tractor. The work was concentrated on the accuracy of the automated tractor movement rather than network performance. Hu et al. [57] focused on remote steering of the wheel of the tractor using the CAN bus and CANtest software. Their results showed sufficient response speed and accuracy, satisfying the requirements of an agricultural automatic navigation system.

Our study proposes implementing remote control of the tractor by relaying the in-vehicle CAN messages of the tractor between the CAN of the remote connection system through the mobile network over the IP. Ditze et al. [13] studied relaying ISOBUS messages and implemented over IP over CAN by implementing an IP address into a CAN identifier. Lindgren et al. [14] proposed a similar approach to a modular lightweight IP stack for embedded platforms. A wireless solution with an IEEE 802.11b WLAN was proposed by

Bayilmis et al. [15]. Similar to our approach, Johanson et al. [16] developed a CAN-over-IP tunneling protocol for diagnostic and monitoring purposes. Our approach utilize Cannelloni [17] gateway software to relay the selected CAN messages of two systems over an IP tunnel. The solution was implemented in the real tractor and tested in a mobile network environment.

Several reviews [19–21] have identified the opportunities that mobile communication technologies, particularly 5G, promise for agriculture and SF scenarios. 5G has been proposed as a reliable, low-latency, high-capacity channel that can enable new applications, such as automated machines, real-time monitoring, virtual consultation, predictive maintenance, data analytics, and cloud repositories. Consequently, 5G will facilitate the transformation of farms to become more secure, reliable, environmentally friendly, and energy-efficient. For instance, 5G can provide communication channels for controlling and monitoring different aerial and ground vehicles [22], including unmanned tractors [58] and bulldozers [59]. Other wireless technologies—Wi-Fi, satellite, and LoRaWAN networks—have been considered alternative channels to gather, for example, sensor data, situational awareness, and tractor localization information [60]. To enable interoperability between different systems in SFs, both application [61,62] and network layer solutions have been proposed. We focused on the connectivity between wireless networks and studied wireless backbones. These reliable mesh-based tactical network architectures have previously been used in both enterprise [63] and military [64] domains. Existing field trials and pilots have addressed, for examle, IoT and mobile technologies for SF [65], LoRaWan for IoT [66], as well as 5G for V2X communications [67]. We extend these verification efforts by trialing a unique combination of mobile, tactical, sensor, and satellite network technologies.

Existing cybersecurity research [23,24,26,68–70] has identified threats, challenges, and requirements that must be addressed when deploying wireless networks for SF scenarios. Central challenges include external threats and insider issues due to a lack of security awareness, information technology expertise, and resources. Cybersecurity research has also covered vehicular communications [28,71–73], including tractors [74] and other unmanned work vehicles [75], and has reviewed [76,77] threats, risks, and solutions for 5G-based IoT [76] and critical communications [77]. Our proposal for the security architecture objectives is built on these studies. We combine different viewpoints and propose an approach that highlights SF specific security threats and characteristics. Our approach addresses the risks of farm vehicles but also acknowledges that modern farms and agricultural tractors do not operate in isolation but require large amounts of connected users and assets, including sensors and external services, which must be protected and trustworthy. Remote attestation solutions have been proposed to verify the trustworthiness of IoT-sensors [78] and components in vehicles [79]. Our delegated device attestation proposal [51], which was part of our SF security architecture, specified how integrity verification could be integrated into an identity and access management framework OAuth2. The framework is commonly used on the web, for example, by Google, Microsoft, Amazon, and Apple. Previous research [80,81] demonstrated the integration of OAuth2 and remote attestation. Our novel contribution demonstrated how the approach works with IoT devices and the device identifier composition engine protocol [82]. Consequently, we demonstrated a practical approach to managing the security and trust of different kinds of devices and components within SFs.

5. Conclusions and Future Research

We expect the remote control of machinery to assume a role in future smart farming. As technological advances in various fields are increasing the range of functions that machinery can perform autonomously, we are experiencing analogous developments in road traffic.

The PRIORITY project has concentrated on researching and testing the capability for remote control using a local private mobile network as the communication medium. We have successfully demonstrated the viability of the remote operation of a tractor in a

realistic environment. Future research is needed to support the transition toward more autonomy and thus improved efficiency and productivity. Appropriate regulatory and legislative changes must also be addressed within the boundaries of maintaining a high level of security and safety. The emergence of such changes will likely differ between different countries and regions. In fact, the application of new technologies may actually promote better safety by removing human error.

The development of the trialed system enabled us to learn the need to customize applications and optimize protocols for private networks, where the available resources can be limited. In particular, we demonstrated the optimization of control channel signaling. In the future, emerging network and application technologies and architectures may provide new opportunities. More research is needed to find innovations to (a) adapt applications to restrictions caused by the network or (b) customize the network to support applications. For instance, tractor remote control traffic was implemented using the SSH protocol. The SSH tunnel is convenient, but because SCTP was used with Cannelloni, it introduced the need to perform a protocol conversion using the Socat program. In the future, there is room to replace SSH with end-to-end secure connections that offer better efficiency by eliminating the processing coming from conversion and more security by removing the need for the trusted conversion component. Furthermore, Cannelloni could use UDP instead of SCTP, allowing the dropping of some packets as congestion control. Dropping packets is preferable to inserting old messages into the CAN bus after retransmission is achieved.

Approaches to adapting the quality parameters of low-latency video streams to support different 5G use cases were evaluated in our prior work [83,84] within the project. Video adaptation solutions provide a promising approach for optimizing the video channels used by unmanned tractors. Future research is needed to develop and verify adaptation approaches for unmanned tractor scenarios.

The security approach for coupling identity and access management and our new protocol [51] for attesting the trustworthiness of IoT devices were now demonstrated with farm sensors. Future research is needed to explore whether our combined identity management and delegated attestation architecture would be feasible for unmanned tractors.

The trialed GEO satellites are able to provide large coverage and good throughput capabilities, but the main disadvantage of this solution is large latency, which limits the applicability of the GEO satellites mostly to monitoring use cases. Future work and trials are needed to explore the opportunities provided by low-earth orbiting (LEO) satellites. LEO satellites allow for dramatically decreased transmission latency due to their shorter distance from Earth (e.g., from 500–1400 km compared to 35,786 km for GEO). LEO satellite connectivity possibilities have been trialed, resulting in throughput of 195 Mbps and round-trip latency levels of 70 ms [85]. This connectivity performance would be sufficient not only for monitoring use cases but potentially also for the remote control of an unmanned tractor.

Author Contributions: Conceptualization, M.H., J.S., T.K., K.L., P.K., A.Y. and H.P.; methodology, M.H., J.S., K.L., T.K. and H.P.; software, O.S. and T.K.; validation, O.S., T.K., K.L. and P.K.; writing—original draft preparation, M.H., J.S., K.L., O.S., T.K., P.K., H.H., J.P. and A.Y.; writing—review and editing, M.H., J.S., K.L., O.S., T.K., J.K., A.Y. and H.P. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by Business Finland and the consortium partners of the PRIORITY project. This work was also supported in part by the Academy of Finland 6Genesis Flagship (grant no. 318927).

Acknowledgments: The authors would like to thank: Markus Lassheikki from The Central Union of Agricultural Producers and Forest Owners (MTK) for help in organizing the trial; Kimmo Ahola, Mikko Vehkaperä and Stephan Mehnert for helping with the satellite gateway; Antti Heikkinen for setting up the video services; Jukka Julku and Markku Kylänpää for implementing security approach for IoT; Risto Toivakka and Pekka Päivikkö for co-operation on the development of tractor remote control; Marika Hautala for photos; Mika Pahkasalo, Markus Liuska and Pentti Eteläaho for

supporting and developing the trial; AGCO, Airbus, Bittium, and Goodmill for providing equipment and solutions for trial.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

3GPP	Third Generation Partnership Project
CAN	Controller Area Network
DNS	Domain Name System
DDNS	Dynamic DNS
ECU	Electronic Control Unit
GEO	Geostationary
IP	Internet Protocol
IPsec	Internet Protocol Security
IoT	Internet of Things
LEO	Low Earth Orbit
LoRaWAN	Long Range Wide Area Network
MDPI	Multidisciplinary Digital Publishing Institute
NAT	Network address translation
OAuth	Open Authorization
QoS	Quality of Service
QR code	Quick Response code
RSRP	Reference Signal Received Power
RTT	Round Trip Time
SAE	Society of Automotive Engineers
SCTP	Stream Control Transmission Protocol
SF	Smart Farming
SIM	Subscriber Identity Module
SRTP	Secure Real-time Transport Protocol
SSH	Secure Shell
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
UE	User Equipment
V2X	Vehicle-to-Everything
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity
WPA	Wi-Fi Protected Access

References

1. Thomasson, J.; Baillie, C.; Antille, D.; Lobsey, C.; McCarthy, C.; Agricultural, A.S.; Engineers, B. *Autonomous Technologies in Agricultural Equipment: A Review of the State of the Art*; ASABE Distinguished Lecture Series: Tractor Design; American Society of Agricultural and Biological Engineers: St. Joseph, MI, USA, 2019; pp. 1–17.
2. Zhang, X.; Geimer, M.; Noack, P.; Grandl, L. A semi-autonomous tractor in an intelligent master—Slave vehicle system. *Intell. Serv. Robot.* **2010**, *3*, 263–269. [CrossRef]
3. Mehrabi, Z.; McDowell, M.; Ricciardi, V.; Levers, C.; Martinez, J.; Mehrabi, N.; Wittman, H.; Ramankutty, N.; Jarvis, A. The global divide in data-driven farming. *Nat. Sustain.* **2021**, *4*, 154–160. [CrossRef]
4. Relf-Eckstein, J.; Ballantyne, A.T.; Phillips, P.W. Farming Reimagined: A case study of autonomous farm equipment and creating an innovation opportunity space for broadacre smart farming. *Wagening. J. Life Sci.* **2019**, *90–91*, 100307. [CrossRef]
5. Ünal, I.; Topakci, M. Design of a Remote-Controlled and GPS-Guided Autonomous Robot for Precision Farming. *Int. J. Adv. Robot. Syst.* **2015**, *12*, 1. [CrossRef]
6. Gonzalez-De-Santos, P.; Fernández, R.; Sepúlveda, D.; Navas, E.; Armada, M. Unmanned ground vehicles for smart farms. *Agron.-Clim. Chang. Food Secur.* **2020**, *6*, 73.
7. Bonadies, S.; Lefcourt, A.; Gadsden, S.A. A survey of unmanned ground vehicles with applications to agricultural and environmental sensing. In *Autonomous Air and Ground Sensing Systems for Agricultural Optimization and Phenotyping*; International Society for Optics and Photonics: Washington, DC, USA, 2016; Volume 9866.

8. Roldán, J.J.; del Cerro, J.; Garzón-Ramos, D.; Garcia-Aunon, P.; Garzón, M.; de León, J.; Barrientos, A. Robots in agriculture: State of art and practical experiences. *Serv. Robot.* **2018**, 67–90. [CrossRef]
9. Ni, J.; Hu, J.; Xiang, C. A review for design and dynamics control of unmanned ground vehicle. *Proc. Inst. Mech. Eng. Part D J. Automob. Eng.* **2021**, *235*, 1084–1100. [CrossRef]
10. International Organization for Standardization. *Tractors and Machinery for Agriculture and Forestry—Serial Control and Communications Data Network—Part 1: General Standard for Mobile Data Communication*; ISO 11783-1:2017 (E); International Organization for Standardization: Geneva, Switzerland, 2017.
11. *Standard SAE J1939-1*; On-Highway Equipment Control and Communication Network. SAE International: Warrendale, PA, USA, 2021.
12. Wang, H.; Noguchi, N. Autonomous maneuvers of a robotic tractor for farming. In Proceedings of the 2016 IEEE/SICE International Symposium on System Integration (SII), Sapporo, Japan, 13–15 December 2016; pp. 592–597. [CrossRef]
13. Ditze, M.; Bernhardi-Grisson, R.; Kämper, G.; Altenbernd, P. Porting the Internet Protocol to the Controller Area Network. In Proceedings of the 2nd International Workshop on Real-Time LANs in the Internet Age (RTLIA 2003), Porto, Portugal, 2–4 July 2003.
14. Lindgren, P.; Aittamaa, S.; Eriksson, J. IP over CAN, Transparent Vehicular to Infrastructure Access. In Proceedings of the 2008 5th IEEE Consumer Communications and Networking Conference, Las Vegas, NV, USA, 10–12 January 2008; pp. 758–759. [CrossRef]
15. Bayilmis, C.; Erturk, I.; Ceken, C. Extending CAN segments with IEEE 802.11 WLAN. In Proceedings of the The 3rd ACS/IEEE International Conference on Computer Systems and Applications, Cairo, Egypt, 6 January 2005. [CrossRef]
16. Johanson, M.; Karlsson, L.; Risch, T. Relaying Controller Area Network Frames over Wireless Internetworks for Automotive Testing Applications. In Proceedings of the 2009 Fourth International Conference on Systems and Networks Communications, Porto, Portugal, 20–25 September 2009; pp. 1–5. [CrossRef]
17. Reinhardt, D.; Güntner, M.; Kucera, M.; Waas, T.; Kühnhauser, W. Mapping CAN-to-ethernet Communication Channels within Virtualized Embedded Environments. In Proceedings of the 10th IEEE International Symposium on Industrial Embedded Systems (SIES), Siegen, Germany, 8–10 June 2015. [CrossRef]
18. Socat—Multipurpose Relay. Available online: http://www.dest-unreach.org/socat/ (accesssed on 24 November 2021).
19. Tang, Y.; Dananjayan, S.; Hou, C.; Guo, Q.; Luo, S.; He, Y. A survey on the 5G network and its impact on agriculture: Challenges and opportunities. *Comput. Electron. Agric.* **2021**, *180*, 105895. [CrossRef]
20. Wang, F. *Technology Related to Agricultural Transformation and Development based on 5G Technology*; Journal of Physics: Conference Series; IOP Publishing: Bristol, UK, 2020; Volume 1574, p. 012015.
21. Friha, O.; Ferrag, M.A.; Shu, L.; Maglaras, L.A.; Wang, X. Internet of Things for the Future of Smart Agriculture: A Comprehensive Survey of Emerging Technologies. *IEEE CAA J. Autom. Sin.* **2021**, *8*, 718–752. [CrossRef]
22. Storck, C.R.; Duarte-Figueiredo, F. A survey of 5G technology evolution, standards, and infrastructure associated with vehicle-to-everything communications by internet of vehicles. *IEEE Access* **2020**, *8*, 117593–117614. [CrossRef]
23. Chi, H.; Welch, S.; Vasserman, E.; Kalaimannan, E. A framework of cybersecurity approaches in precision agriculture. In Proceedings of the ICMLG2017 5th International Conference on Management Leadership and Governance, St. Petersburg, Russia, 16–17 March 2017; Acad. Conf. Publ. Int.: Reading, UK, 2017; pp. 90–95.
24. Barreto, L.; Amaral, A. Smart farming: Cyber security challenges. In Proceedings of the 2018 International Conference on Intelligent Systems (IS), Funchal, Portugal, 25–27 September 2018; pp. 870–876.
25. Ahmad, I.; Shahabuddin, S.; Kumar, T.; Okwuibe, J.; Gurtov, A.; Ylianttila, M. Security for 5G and beyond. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 3682–3722. [CrossRef]
26. Sontowski, S.; Gupta, M.; Chukkapalli, S.S.L.; Abdelsalam, M.; Mittal, S.; Joshi, A.; Sandhu, R. Cyber attacks on smart farming infrastructure. In Proceedings of the 2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC), Atlanta, GA, USA, 1–3 December 2020; pp. 135–143.
27. Tange, K.; De Donno, M.; Fafoutis, X.; Dragoni, N. A systematic survey of industrial Internet of Things security: Requirements and fog computing opportunities. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 2489–2520. [CrossRef]
28. Lu, R.; Zhang, L.; Ni, J.; Fang, Y. 5G vehicle-to-everything services: Gearing up for security and privacy. *Proc. IEEE* **2019**, *108*, 373–389. [CrossRef]
29. Airbus. Verde-Crop Imagery & Analytics for Precision Agriculture. Available online: https://oneatlas.airbus.com/service/verde (accessed on 28 November 2021).
30. Heikkilä, M.; Koskela, P.; Suomalainen, J.; Lähetkangas, K.; Kippola, T.; Eteläaho, P.; Erkkilä, J.; Pouttu, A. Field Trial with Tactical Bubbles for Mission Critical Communications. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4385. [CrossRef]
31. *Standard J3016-202104*; Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles. SAE International: Warrendale, PA, USA, 2021.
32. Basu, S.; Omotubora, A.; Beeson, M.; Fox, C. Legal framework for small autonomous agricultural robots. *Ai Soc.* **2020**, *35*, 113–134. [CrossRef]
33. International Organization for Standardization; ISO 11898-1:2015. *Road Vehicles—Controller Area Network (CAN)—Part 1: Data Link Layer and Physical Signalling*; International Organization for Standardization: Geneva, Switzerland, 2015.
34. Vickers, J.N. *Perception, Cognition, and Decision Training: The Quiet Eye in Action*; Human Kinetics: Champaign, IL, USA, 2007.

35. Lee, K.; Kim, J.; Park, Y.; Wang, H.; Hong, D. Latency of cellular-based V2X: Perspectives on TTI-proportional latency and TTI-independent latency. *IEEE Access* **2017**, *5*, 15800–15809. [CrossRef]
36. 5GAA Automotive Association. *C-V2X Use Cases and Service Level Requirements*; Technical Report; Version 3; 5GAA: München, Germany, 2020; Volume I.
37. 3GPP. *Architecture Enhancements for 5G System (5GS) to Support Vehicle-to-Everything (V2X) Services*; Technical Specification TS23.287, Release 16; 3GPP: Valbonne, France, 2021.
38. 3GPP. *System Architecture for the 5G System (5GS)*; Technical Specification 23.287, Release 17; 3GPP: Valbonne, France, 2021.
39. 3GPP. *Security Architecture and Procedures for 5G System*; Technical Specification, TS 33.501, Release 15; 3GPP: Valbonne, France, 2018.
40. Valtra. Valtra N Series Tractors 135–201 HP. Available online: https://www.valtra.co.uk/products/nseries.html (accesssed on 22 November 2021).
41. Bittium. Tactical Wireless IP Network. Available online: https://www.bittium.com/tactical-communications/bittium-tactical-wireless-ip-network (accesssed on 30 October 2021).
42. Digita. LoRaWAN Technology. Available online: https://www.digita.fi/en/services/iot/lorawan-technology/#/ (accesssed on 24 November 2021).
43. LoRa Alliance. LoRaWAN 1.1 Specification. 2017. Available online: https://lora-alliance.org/resource_hub/lorawan-specification-v1-1/ (accessed on 30 October 2021).
44. Wireless Soil Moisture Sensor for Agriculture. Available online: https://soilscout.com/applications/agriculture (accessed on 30 October 2021).
45. Vehkaperä, M.; Hoppari, M.; Suomalainen, J.; Roivainen, J.; Rantala, S.J. Testbed for Local-Area Private Network with Satellite-Terrestrial Backhauling. In Proceedings of the International Conference on Electrical, Communication, and Computer Engineering (ICECCE), Kuala Lumpur, Malaysia, 12–13 June 2021; pp. 1–6.
46. 3GPP; 3GPP System Architecture Evolution (SAE). *Security Architecture*; Technical Specification TS 33.401, Release 16; 3GPP: Valbonne, France, 2020.
47. Wi-Fi Alliance. Wi-Fi Protected Access—WPA 3, Specification, Version 3.0. 2020. Available online: https://www.wi-fi.org/download.php?file=/sites/default/files/private/WPA3_Specification_v3.0.pdf (accesssed on 28 November 2021).
48. Goodmill Systems. Goodmill Systems w24h-S Managed Multichannel Router. Data Sheet. Available online: https://goodmillsystems.com/application/files/2615/8860/4850/Goodmill_w24h-S_Datasheet.pdf (accesssed on 28 November 2021).
49. SocketCAN—Controller Area Network. Available online: https://www.kernel.org/doc/html/latest/networking/can.html (accesssed on 24 November 2021).
50. Hardt, D. *The OAuth 2.0 Authorization Framework*; RFC 6749; IETF: Fremont, CA, USA, 2012.
51. Julku, J.; Suomalainen, J.; Markku, K. Delegated Device Attestation for IoT. In Proceedings of the 8th International Conference on Internet of Things: Systems, Management and Security (IoTSMS), Gandia, Spain, 6–9 December 2021.
52. Wu, Z.; Shen, X.; Gao, M.; Zeng, Y. Design of Distributed Remote Data Monitoring System Based on CAN Bus. In Proceedings of the 2018 Eighth International Conference on Instrumentation & Measurement, Computer, Communication and Control (IMCCC), Harbin, China, 19–21 July 2018; pp. 1403–1406.
53. Rohrer, R.A.; Pitla, S.K.; Luck, J.D. Tractor CAN bus interface tools and application development for real-time data analysis. *Comput. Electron. Agric.* **2019**, *163*, 104847. [CrossRef]
54. Dhivya, M.; Devi, K.G.; Suguna, S.K. Design and Implementation of Steering Based Headlight Control System Using CAN Bus. In *International Conference on Computer Networks and Inventive Communication Technologies*; Springer: Berlin, Germany, 2019; pp. 373–383.
55. Fugiglando, U.; Massaro, E.; Santi, P.; Milardo, S.; Abida, K.; Stahlmann, R.; Netter, F.; Ratti, C. Driving behavior analysis through CAN bus data in an uncontrolled environment. *IEEE Trans. Intell. Transp. Syst.* **2018**, *20*, 737–748. [CrossRef]
56. Wang, H.; Niu, W.; Fu, W.; Ren, Y.; Hu, S.; Meng, Z. A Low-cost Tractor Navigation System with Changing Speed Adaptability. In Proceedings of the 2021 33rd Chinese Control and Decision Conference (CCDC), Kunming, China, 22–24 May 2021; pp. 96–102.
57. Hu, S.; Fu, W.; Li, Y.; Cong, Y.; Shang, Y.; Meng, Z. Research on Automatic Steering Control System of Full Hydraulic Steering Tractor. In *International Conference on Computer and Computing Technologies in Agriculture*; Springer: Berlin, Germany, 2017; pp. 517–528.
58. Isihibashi, R.; Tsubaki, T.; Okada, S.; Yamamoto, H.; Kuwahara, T.; Kavamura, K.; Wakao, K.; Moriyama, T.; Ospina, R.; Okamoto, H.; et al. Experiment of Integrated Technologies in Robotics, Network, and Computing for Smart Agriculture. *IEICE Trans. Commun.* **2021**. [CrossRef]
59. You, K.; Ding, L.; Zhou, C.; Dou, Q.; Wang, X.; Hu, B. 5G-based earthwork monitoring system for an unmanned bulldozer. *Autom. Constr.* **2021**, *131*, 103891. [CrossRef]
60. Drenjanac, D.; Tomic, S.; Agüera, J.; Perez-Ruiz, M. Wi-fi and satellite-based location techniques for intelligent agricultural machinery controlled by a human operator. *Sensors* **2014**, *14*, 19767–19784. [CrossRef]
61. Chukkapalli, S.S.L.; Mittal, S.; Gupta, M.; Abdelsalam, M.; Joshi, A.; Sandhu, R.; Joshi, K. Ontologies and artificial intelligence systems for the cooperative smart farming ecosystem. *IEEE Access* **2020**, *8*, 164045–164064. [CrossRef]
62. Cathey, G.; Benson, J.; Gupta, M.; Sandhu, R. Edge Centric Secure Data Sharing with Digital Twins in Smart Ecosystems. *arXiv* **2021**, arXiv:2110.04691.

63. Raniwala, A.; Chiueh, T.c. Evaluation of a wireless enterprise backbone network architecture. In Proceedings of the 12th Annual IEEE Symposium on High Performance Interconnects, Stanford, CA, USA, 27 August 2004; pp. 98–104.
64. Pawgasame, W.; Wipusitwarakun, K. Tactical wireless networks: A survey for issues and challenges. In Proceedings of the 2015 Asian Conference on Defence Technology (ACDT), Hua Hin, Thailand, 23–25 April 2015; pp. 97–102.
65. Brewster, C.; Roussaki, I.; Kalatzis, N.; Doolin, K.; Ellis, K. IoT in agriculture: Designing a Europe-wide large-scale pilot. *IEEE Commun. Mag.* **2017**, *55*, 26–33. [CrossRef]
66. Miles, B.; Bourennane, E.B.; Boucherkha, S.; Chikhi, S. A study of LoRaWAN protocol performance for IoT applications in smart agriculture. *Comput. Commun.* **2020**, *164*, 148–157. [CrossRef]
67. Serizawa, K.; Mikami, M.; Moto, K.; Yoshino, H. Field trial activities on 5G NR V2V direct communication towards application to truck platooning. In Proceedings of the 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall), Honolulu, HI, USA, 22–25 September 2019; pp. 1–5.
68. Nikander, J.; Manninen, O.; Laajalahti, M. Requirements for cybersecurity in agricultural communication networks. *Comput. Electron. Agric.* **2020**, *179*, 105776. [CrossRef]
69. Gupta, M.; Abdelsalam, M.; Khorsandroo, S.; Mittal, S. Security and privacy in smart farming: Challenges and opportunities. *IEEE Access* **2020**, *8*, 34564–34584. [CrossRef]
70. Adkisson, M.; Kimmel, J.C.; Gupta, M.; Abdelsalam, M. Autoencoder-based Anomaly Detection in Smart Farming Ecosystem. *arXiv* **2021**, arXiv:2111.00099.
71. Sharma, V.; You, I.; Guizani, N. Security of 5G-V2X: Technologies, Standardization, and Research Directions. *IEEE Netw.* **2020**, *34*, 306–314. [CrossRef]
72. Hussain, R.; Hussain, F.; Zeadally, S. Integration of VANET and 5G Security: A review of design and implementation issues. *Future Gener. Comput. Syst.* **2019**, *101*, 843–864. [CrossRef]
73. Gupta, M.; Sandhu, R. Authorization framework for secure cloud assisted connected cars and vehicular internet of things. In Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies, Indianapolis, IN, USA, 13–15 June 2018; pp. 193–204.
74. Stachowski, S.; Bielawski, R.; Weimerskirch, A. *Cybersecurity Research Considerations for Heavy Vehicles*; Report DOT HS 812 636; Technical Report; U.S. Department of Transportation: Washington, DC, USA, 2019.
75. Bilbao-Arechabala, S.; Jorge-Hernandez, F. Security Architecture for Swarms of Autonomous Vehicles in Smart Farming. *Appl. Sci.* **2021**, *11*, 4341.
76. Rahimi, H.; Zibaeenejad, A.; Rajabzadeh, P.; Safavi, A.A. On the security of the 5G-IoT architecture. In Proceedings of the International Conference on Smart Cities and Internet of Things, Mashhad, Iran, 26–27 September 2018; pp. 1–8.
77. Suomalainen, J.; Julku, J.; Vehkaperä, M.; Posti, H. Securing Public Safety Communications on Commercial and Tactical 5G Networks: A Survey and Future Research Directions. *IEEE Open J. Commun. Soc.* **2021**, *2*, 1590–1615. [CrossRef]
78. Gong, B.; Zhang, Y.; Wang, Y. A remote attestation mechanism for the sensing layer nodes of the Internet of Things. *Future Gener. Comput. Syst.* **2018**, *78*, 867–886. [CrossRef]
79. Khodari, M.; Rawat, A.; Asplund, M.; Gurtov, A. Decentralized firmware attestation for in-vehicle networks. In Proceedings of the 5th on Cyber-Physical System Security Workshop, Auckland, New Zealand, 8 July 2019; pp. 47–56.
80. Ali, T.; Nauman, M.; Amin, M.; Alam, M. Scalable, Privacy-Preserving Remote Attestation in and through Federated Identity Management Frameworks. In Proceedings of the 2010 International Conference on Information Science and Applications, Seoul, Korea, 21–23 April 2010; pp. 1–8. [CrossRef]
81. Leicher, A.; Schmidt, A.U.; Shah, Y.; Cha, I. Trusted Computing enhanced OpenID. In Proceedings of the 2010 International Conference for Internet Technology and Secured Transactions, London, UK, 8–11 November 2010; pp. 1–8.
82. Trusted Computing Group. *Implicit Identity Based Device Attestation*; Reference Version 1.0, Revision 0.93; Trusted Computing Group: Beaverton, OR, USA, 2018.
83. Uitto, M.; Heikkinen, A. Exploiting and Evaluating Live 360° Low Latency Video Streaming Using CMAF. In Proceedings of the 2020 European Conference on Networks and Communications (EuCNC), Dubrovnik, Croatia, 15–18 June 2020; pp. 276–280.
84. Uitto, M.; Heikkinen, A. Evaluation of Live Video Streaming Performance for Low Latency Use Cases in 5G. In Proceedings of the 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Porto, Portugal, 8–11 June 2021; pp. 431–436.
85. Erillisverkot. OneWeb and Erillisverkot Demonstrated Low Earth Orbit Satellite Connectivity to Finnish Government Agencies at Westcott Venture Park. Available online: https://www.erillisverkot.fi/en/oneweb-and-erillisverkot-demonstrated-low-earth-orbit-satellite-connectivity-to-finnish-government-agencies-at-westcott-venture-park/ (accesssed on 24 November 2021).