telecom

MDPI

Article

A Survey on the Implementation and Management of Secure Virtual Private Networks (VPNs) and Virtual LANs (VLANs) in Static and Mobile Scenarios

Antonio Francesco Gentile [1], Peppino Fazio [2,*] and Giuseppe Miceli [3]

[1] Istituto di Calcolo e Reti ad Alte Prestazioni del Consiglio Nazionale delle Ricerche (ICAR-CNR), Via Bucci 41c, 87036 Rende, CS, Italy; antoniofrancesco.gentile@icar.cnr.it
[2] Department of Molecular Sciences and Nanosystems (DSMN), Ca' Foscari University of Venice, Via Torino 155, Mestre, 30172 Venezia, VE, Italy
[3] IT Department, Agenzia della Regione Calabria per le Erogazioni in Agricoltura (ARCEA), Località Germaneto, 88100 Catanzaro, CZ, Italy; giuseppe.miceli@arcea.it
* Correspondence: peppino.fazio@unive.it

Abstract: Nowadays, the demand for connection between the remote offices of a company, or between research locations, and constantly increasing work mobility (partly due to the current pandemic emergency) have grown hand in hand with the quality and speed of broadband connections. The logical consequence of this scenario is the increasingly widespread use of Virtual Private Network (VPN) connections. They allow one to securely connect the two ends of a connection via a dedicated network, typically using the Internet and reducing the costs of Content Delivery Network (CDN) lines (dedicated connections). At the same time, Virtual Local Area Networks (VLANs) are able to decrease the impact of some scalability issues of large networks. Given the background above, this paper is focused on overviewing and surveying the main progresses related to VPNs and VLANs in wireless networks, by collecting the most important contributions in this area and describing how they can be implemented. We state that security issues in VLANs can be effectively mitigated through the combination of good network-management practices, effective network design and the application of advanced security products. However, obviously, the implementation of VPNs and VLANs poses specific issues regarding information and network security; thus some good solutions are also surveyed.

Keywords: QoS; VPN; mobile VPN; security; MANETs

Citation: Gentile, A.F.; Fazio, P.; Miceli, G. A Survey on the Implementation and Management of Secure Virtual Private Networks (VPNs) and Virtual LANs (VLANs) in Static and Mobile Scenarios. *Telecom* **2021**, 2, 430–445. https://doi.org/10.3390/telecom2040025

Academic Editors: Alexandros-Apostolos A. Boulogeorgos and Alessandro Pozzebon

Received: 3 July 2021
Accepted: 28 October 2021
Published: 5 November 2021

1. Introduction

In the last decade, security solutions and features in WPAN, WLAN, WMAN and distributed wireless systems have become increasingly mandatory [1,2]. The number of Virtual Private Network (VPN) implementations has rapidly grown due to the enormous appeal of using "public" infrastructure to implement a secure link between the different locations of a company (e.g., a university) or between a "road warrior" and its seat [3], also involving cellular architectures. There are several advantages to implementing a VPN, such as the following:

(a) Cost effectiveness (cost of infrastructure is lower, and the appropriate choice of the implementation phase allows one to choose the best solution at the lowest sustainable cost);
(b) Simplicity (the technology is very mature and does not require esoteric skills);
(c) Safety (the technology is based on open standards and is mostly universally safe).

Therefore, with little effort, it is possible to achieve a good compromise between ease of access and reasonable safety.

The VPN concept is quite simple: it is based on the paradigm of "hub and spoke", with a central location from which a huge set of connections departs to remote locations.

By using appropriate rules, it is possible to decide whether each remote site exclusively accesses the central node or whether traffic between the suburbs should be enabled.

The solutions for implementing these kinds of accesses are very wide and different, ranging from a simple server equipped with open-source software to expensive redundant appliances in High Availability (HA). The precise choice depends on the costs, the grade of integration with existing infrastructure, the required bandwidth, the workload and/or the criticism of the link (to mention just a few factors that affect the choice of VPN system). Moreover, recently, the energy consumption of the adopted security solutions has become an aspect to consider [4].

In fact, with the general operation of a VPN, all traffic between the two endpoints of the VPN is encapsulated into pre-established tunnels that can be on different levels of the ISO/OSI model (IPSEC or IKEv2 IPSEC at layer three, PPTP at layer five, L2TP at layer two and OpenVPN or Virtual Tunnel Daemon at layer four) [5–14].

This paper is focused on giving a deep overview of the possible implementations of VPNs and Virtual Local Area Networks (VLANs) and their recent progresses in wireless and mobile scenarios. In particular, our main aim is to give a detailed review of the efficient implementation of VPN for a mobile scenario. In fact, conventional VPN solutions (as referenced above) are dedicated to static networks (with no mobile nodes). It is known that in a mobile scenario, connections are not as reliable as in the wired case: mobility effects, obviously, reflect on VPN performance, resulting in low-speed connections, packet loss and low throughput.

With the rapid proliferation of mobile devices and high speeds (e.g., with the fifth generation (5G)), users are more oriented to use not just their home devices but also their mobile devices (such as smart phones and tablets), considering opportunistic communication and services [15,16]. Cloud Computing (CC) has reached a high grade of development, and nowadays, users connect with their mobile devices to the cloud in order to access their cloud services.

In the above scenario, it is clear that establishing a reliable session is essential, and VPNs are the first "tool" that can be used to guarantee security and robustness. Unfortunately, VPNs work well only with stable network connections. If connection losses or service degradations occur, VPN connections will surely break, and users will not be satisfied with the results, which can involve data loss and continuous session breaks.

Therefore, the main aim of this work is to review and survey the main VPN solutions for static (stationary nodes) and dynamic (mobile nodes) networks from a practical point of view. A valid alternative to VPNs is VLAN technology. This allows networks to be grouped logically rather than by physical location, and it enables the segmentation of a network into virtual networks or virtual groups (a feature that is supported by most network switches).

The main contributions of this paper can be summarized as follows:

(a) An extensive literature review is given, providing the reader with insight into the key contributions in the area of VPN and VLAN implementations in static and dynamic networks;
(b) Several details about the protocols and signaling used in VPN/VLAN systems are given, providing the reader with detailed information about security management in the considered scenario;
(c) Mobility issues are addressed, and some solutions (such as available software tools) are described in detail and suggested for some mobile environments;
(d) Some command lines are also described, providing the reader with instructions on how to address some VPN security issues.

The remainder of the paper is structured as follows: Section 2 addresses VPNs in static and dynamic networks, while Section 3 illustrates the main features of VLANs. Section 4 illustrates the best solution for mobility management in VPNs and VLANs, while Section 5 describes some real security implementations. Section 6 concludes the paper.

2. Virtual Private Networks in Static and Dynamic Networks

This section reviews the main contributions in terms of applications and protocols for static and dynamic networks.

2.1. Classical VPN Solutions for Static Networks

There are several protocols for implementing secure VPNs (implementing only VPN does not provide any encryption or confidentiality to the traffic passing through it):

(a) Layer 2 Tunneling Protocol (L2TP)/IPsec [7] is a built-in solution for all modern operating systems and VPN-capable devices. L2TP protocol uses UDP port 1701 and IPsec ports 500 and 4500 for NAT purposes. It requires an advanced configuration (port forwarding) when using a firewall (this is in contrast to SSL, which can use the TCP port 443 to make it indistinguishable from normal HTTPS traffic). On the other hand, IPsec encryption is considered very safe, using an algorithm such as AES, and it is considered a "de facto" standard, although data is encapsulated twice and therefore it is slightly slower than an SSL;

(b) OpenVPN is a very recent open-source technology that uses the Open Secure Sockets Layer (OpenSSL) [9] and SSLv3/TLSv1 [10] library protocols (TLS stands for Transport Layer Security), provided by the OpenVPN company (6200 Stoneridge Mall Road, Pleasanton, CA 94588, USA). It is able to provide a strong and reliable VPN solution. It is highly configurable, it can be set to run on any port, including TCP 443; its default transport protocol is UDP, with port 1194. Using port TCP 443 makes its traffic undistinguishable from the HTTPS traffic, and therefore, it is extremely difficult to block. Another advantage of OpenVPN is that the OpenSSL library provides several encryption algorithms (such as AES, Blowfish, 3DES, CAST-128, etc.) [11]. The speed of execution of an OpenVPN connection depends on the used coding level, but it is generally faster than IPsec;

(c) Secure Socket Tunneling Protocol (SSTP) [12] was introduced by Microsoft (Redmond, WA, USA) in Windows Vista SP1 and, although it is now available for any Linux (a California Public Benefit Corporation) platform, it is still largely a single Windows platform. SSTP uses SSL v3, and it works like OpenVPN (it has also the ability to use TCP port 443 to avoid problems with NAT firewall). It is integrated into Windows and it might be considered easier to use and more stable;

(d) Point-to-Point Tunneling Protocol (PPTP) [13] is a Microsoft product for the creation of VPN-based dial-up networks; for a long while it has been the standard protocol for private corporate networks. It is a VPN protocol based on different authentication methods, able to ensure security, e.g., Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP) v2. By changing MS-CHAP-v2 with Protected Extensible Authentication Protocol (PEAP) the security level of PPTP increases, although it is recommended to use L2TP/IPsec [8] or Secure Socket Tunneling Protocol (SSTP) [12]. PPTP offers an integrated client for almost all platforms, including smartphones. Its implementation requires a very low computational overhead and it is very easy to set up, enabling fast data management;

(e) Internet Key Exchange version 2 (IKEv2) is an IPSec-based [14] tunneling protocol developed by Microsoft and Cisco (San Jose, CA, USA), installed by default in Windows 7 and above. It is not a real VPN protocol at all, but a control protocol for IPSec key exchange, supported by Blackberry (Waterloo, ON, Canada) devices. It can be independently developed and implemented as open source in Linux, BSD and other proprietary OSes. IKEv2 provides the automatic re-establishing of a VPN connection when users temporarily loses their Internet connections; in addition it supports Mobility and Multi-homing protocols [17]. This feature is great for mobile phone users who, for example, connect their smart phones to a WiFi network, but then switch to mobile data connection, based on the best signal or WiFi availability. IKEv2 is faster than PPTP, SSTP and L2TP, as it does not involve the overhead associated with Point-to-Point protocols (PPP). It is very stable and secure (supporting AES 128,

AES 192, AES 256 and 3DES ciphers) and easy to setup on the client side, although not yet supported on many platforms.

2.2. Possible Solutions When Dealing with Mobility in VPNs

There have been several contributions in the literature for dealing with mobility in VPNs. When the tunneling should be maintained during mobile sessions, the VPN client should be able to frequently provide adequate session information. In order to avoid this continuous data exchange between clients and servers, caching mechanisms have been proposed [18], trying to hide disconnections/reconnections of VPN tunnels at the application layer (so, transparently to the users). In fact, the authors of [19] provided a method to modify the OpenVPN in order to overcome the issue of frequent client disconnections. Their idea is based on caching the packets which have not been acknowledged, avoiding data loss, service degradations and TCP retransmission-related operations (such as slow start, etc.) which degrade the overall throughput.

Another kind of proposal which has been introduced to overcome mobility effects in VPNs is the connection splitting, which has been implemented by several vendors, mainly Columbitech which has recently merged with Sectra Communications (Kirjatyöntekijänkatu 14, 00170 Helsinki, Finland) [20,21]. The proposed software solution, called Mobile VPN, provides mobile users with reliable and secure access to data and applications. The solution supports a two-factor authentication with up to 256-bit AES encryption. The core of the idea consists of splitting the connection into three subconnections: (a) a TCP/UDP connection between the application and VPN clients (installed on the mobile device), (b) a UDP connection between the VPN client and VPN server, and (c) a TCP/UDP connection between the VPN and application servers.

In this way, the application on the mobile device is directly connected to the application server, while it is only connected to the VPN client (as illustrated in Figure 1). The VPN session between mobile client and server is setup by the Wireless Transport Layer Security (WTLS) [22].

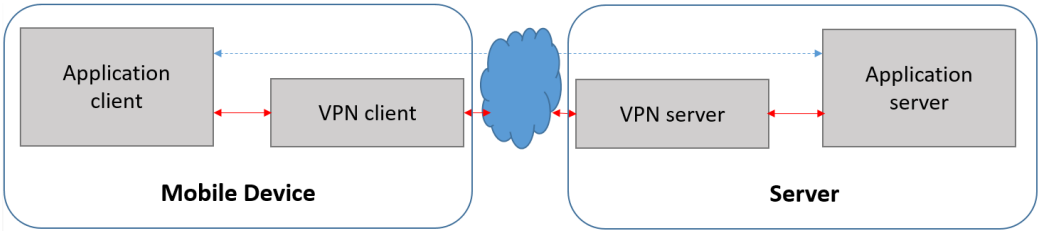

Figure 1. An example of VPN splitting technique: split connection (solid lines) and transparent connection (dotted line).

The authors of [23] proposed a new approach for providing mobile OpenVPN sessions to users moving between WiFi cells: the main idea consists of the autoreconfiguration of the OpenVPN tunnel "immediately" after mobile user handover events. This is obtained by informing the VPN server about the new VPN tunnel context after the mobile user receives the new address. In contrast to caching approaches, packet loss is not avoided, but simply minimized; the number of lost packets is directly proportional to the time taken by mobile users to complete the handover operation.

In [24], an extension of the Secure SHell (SSH) is proposed, in order to give to the applications the possibility to continue their sessions after a brief and temporary physical disconnection from the network. The core of the idea is the possibility to resume a previously established connection, although new TCP connections need to be created after reconnection. To do so, a buffer stores the data of the previous socket, then it is copied and retransmitted after the new one has been created. In this kind of approach, a non-negligible amount of overhead is introduced when the new session keys have to be renegotiated.

The work in [25] describes and enhances the effort given by the IETF Network Mobility working group [26]. The authors propose their Secure Network Mobility (SeNEMO) scheme

as an extension of the Mobile VPN of [24], introducing the Session Initiation Protocol (SIP) and implementing a new system dedicated to real-time applications over VPN. The performance of the proposed idea is validated by several analytical models and simulations.

3. The Virtual LAN Segmentation in Static and Dynamic Networks

As earlier mentioned, with VPN a "tunnel" between two communicating devices, supporting secure communication and secure Internet browsing, can be created. In such a configuration, the original packet (including data and their headers, which may contain information such as the addresses of the source and destination, the type of information provided, the length and the packet sequence number) is encrypted. Then, it is encapsulated in another packet containing only the IP addresses of the two communicating devices (i.e., routers). This configuration protects the traffic and its contents from unauthorized access and allows access to the VPN only to devices with the correct "key". Network devices between the client and the server will not be able to access or view data. The main difference between HTTPS (SSL/TLS) and VPN is that HTTPS encrypts only the actual data of a packet, while with VPN the entire packet can be encrypted and encapsulated to create a protected "tunnel". So, VPN provides a secure method for connecting to a private network through an unsecured public network such as the Internet.

A valid alternative to VPN is Virtual LAN (VLAN) technology. It allows networks to be grouped logically rather than by physical location, and it enables the segmentation of a network into virtual networks or virtual groups (a feature that is supported by most network switches). Only users in a specific group are able to exchange data or access certain resources on the network. The primary protocol used when configuring VLANs is IEEE 802.1Q, which tags each frame or packet with extra bytes to indicate the virtual network to which the packet belongs.

In Figure 2, VLANs are set to different switches. First, each of the two different LANs are segmented into VLAN 20 and VLAN 30.

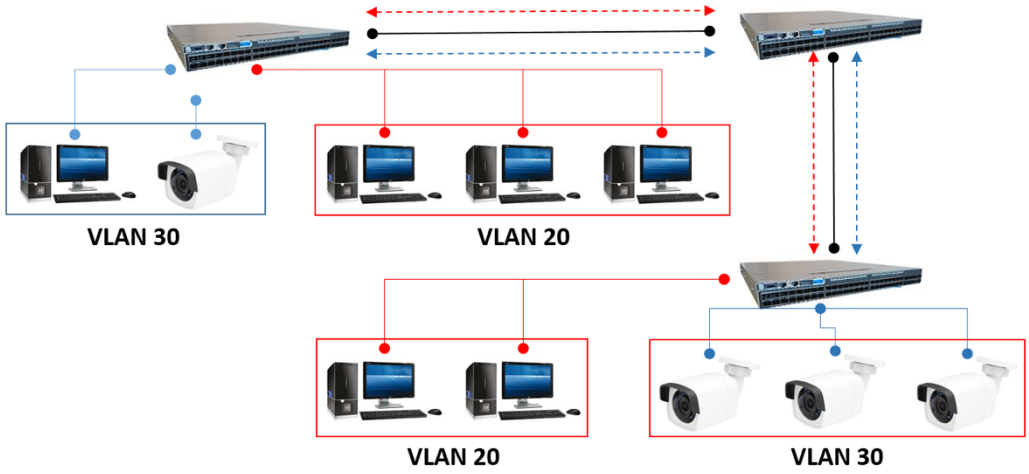

Figure 2. An example of VLAN segmentation.

The links between the switches carry data from different VLANs. Only members of the same VLAN can exchange data, either within the same network and on different networks (the example shows the separation of a video network from a corporate network). VLANs can be configured in different ways, and depending on the type, different technology is applied. In practice, we can find two types of applications: port-based VLANs and tagged VLANs.

(1) Port-based VLAN (or Trunked VLAN): inside a switch, each network participant is directed to a port. Ports are also used to connect the switches together. If two VLANs should be obtained from a single physical network, the related ports are assigned to the desired virtual network. The configuration through different switches is also

possible when the port-based VLAN installation is implemented on small networks and is carried out within a single switch. Thus, for example, ports one to three on the first switch and port one on the second switch can be connected together to a single VLAN. To do this, the two switches must be connected to each other with two cables, providing a connection for each VLAN. Network administrators set up and assign ports to their respective VLANs. In this case, the VLAN is defined as static. If VLANs need to be configured differently, the ports need to be redistributed when configuring the switch. Furthermore, each port (and therefore, each device connected to it) belongs only to a single VLAN. This type of connection is called "trunking", and switches have one or more ports designed for this purpose. It is independent from the PHY layer; it does not matter whether copper or fiber optic cables or a wireless connection are used;

(2) Frame-based VLAN (or Tagged VLAN): in this case, the assignment to the VLAN is more dynamic, in the sense that it is guaranteed by a tag in the packet frame, which replaces the permanent setting in the switch. The tag contains the information that indicates which VLAN the frame belongs to. Each switch recognizes in which segment the communication takes place, and on the basis of this, forwards the message. Each VLAN has its own number. Tagged VLANs can also be implemented directly on network cards (Linux, for example, supports the standard by default). The frame structure follows the IEEE 802.1Q standard [27], which is the most used (other solutions also exist, as the Cisco Inter-Switch Link Protocol (ISL) [28], able to encapsulate the full data frame to enable multiple VLANs).

The advantage of a tagged VLAN compared to a port-assigned VLAN, is the connection between different switches. For port-based VLANs, at least two cables must be placed between the switches, as each Virtual LAN needs its own connection. On the other hand, for trunking in tagged VLANs, only one cable is required, as data is distributed through the information of the frame. The switch recognizes the exact VLAN and forwards it to the destination switch, where the tag is dropped and the frame is forwarded to the correct destination node. Mainly, there are two protocols for managing VLANs:

(1) Tagged VLANs protocol: IEEE802.1Q is the standard reference for VLANs [29], in particular for the tagged ones. It is a Layer-2 encapsulation protocol, which allows for logical separation of different traffic flows, as if they follow distinct physical paths. The IEEE802.1Q does not encapsulate the original frame, but adds 4 bytes to the header (Figure 3). The first 2 bytes regard the TPID protocol identifier tag (it is set to 0×8100, which indicates that the frame is in IEEE 802.1Q format). The next 2 bytes regard the Tag for Control Information TCI (also called VLAN Tag). The TCI is divided as follows: 3 bits for the Priority Code Point (PCP), used to indicate a priority level for the frame, 1 bit for the Drop Eligible Indicator (DEI), indicating the ability to skip the frame in case of congestion, 12 bits for the VLAN ID (VID), indicating the ID of the VLANs (up to 4096, but only 4094 are really available, because the IDs 0 and 4095 are reserved). The rest of the Ethernet frame remains as the original. Obviously, since the header is changed (hence the frame is changed), the 802.1Q encapsulation mechanism requires the recalculation of the FCS field in the Ethernet trailer.

(2) Trunked VLANs protocol: The VLAN Trunking Protocol (VTP) [30,31] is a Cisco proprietary Layer-2 protocol, which allows management of VLAN information, making it available to all switches on the network. The protocol requires the existence of a VTP server: when a VLAN is created or modified, the information is distributed to all the switches of the VTP domain, starting from the server, using the VTP announcements. The VTP advertising operation consists of invitation update messages on the management VLAN (default VLAN1). This is the reason why all trunk connections between switches must be configured to allow traffic to VLAN1. To find out which is the most recent configuration, the VTP information is presented with a revision number, the VTP Configuration Revision Number (CRN), increased by one with each modification of the VLANs. There are, basically, three types of message:

(a) Summary announcements: the switches send them every 5 min or as soon as there is a change in the VLAN database; these messages contain the VTP domain name and the VTP CRN. If a VLAN is added, deleted, or modified, the server increments the revision number and sends a summary update. If a switch receives an update containing a different VTP domain name than its own, the VTP information is simply ignored. If the name matches, then the revision number is checked—if this is higher than the one in possession, an advertisement request is sent;

(b) Advertising requests: VTP clients use these messages to request information about VLANs. The update requests immediately after a switch reboot, a change of the VTP domain name, or new revision numbers;

(c) Sub-advertisements: as soon as a server, following changes on the VLANs, increases the revision number and sends an update summary, it follows up some "subset" messages containing information on the individual VLANs. If there are multiple VLANs, multiple subset messages are created;

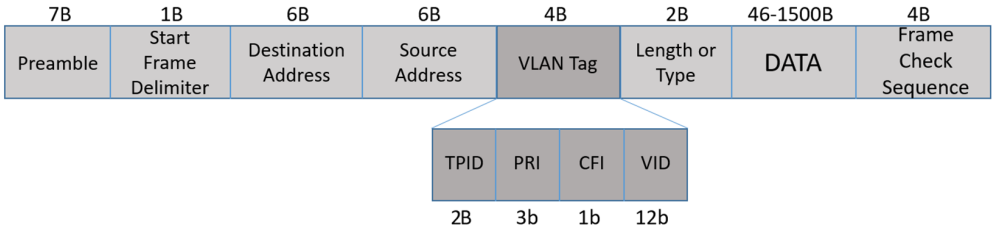

Figure 3. The encapsulated Ethernet frame format for IEEE802.1Q.

In addition, a VTP switch may have three possible roles:

(a) Server: this is the default mode in which VLANs can be created, removed and modified, as well as the ability to set the VTP version. Server switches are then synchronized with the other switches of the VTP domain through the trunk connections, every 5 min or immediately on the basis of a new event.

(b) Client: this is the mode allowing all changes to the VLAN database to be received. The switch can forward received updates, but cannot make changes to the VTP database information. However, if the information forwarded has a higher "Revision Number" than the one present on the clients and servers, it will be modified locally, i.e., the local VLAN database will be updated.

(c) Transparent: in this mode the switch does not participate in any VTP domain; however, it carries out the forwarding of VTP information to trunk ports, thus avoiding interruptions in the exchange of information between client and server.

Both VLAN and VPN are good solutions to manage the access to the network on the basis of the administrative desires. VLANs are more suitable when an organization wants to fragment the existing LAN into smaller chunks, in order to reach a better control. Regarding protection and security, instead, VPN is the better choice. Table 1 shows a brief comparison between the main features of VPNs and VLAN.

Table 1. A comparison between VLANs and VPNs.

VLANs	VPNs
Purely a level two construct	They operate from level one to level three
Used to group multiple computers that are not usually located within the same geographic areas in the same broadcast domain.	Create a smaller subnet on a larger existing network than the VLAN.
They can separate computers in a larger local network into smaller networks for each office or department	Used for secure data transmission between two separate entities (point-to-point case)

Table 1. *Cont.*

VLANs	VPNs
They can shield the data so that it does not behave as if it is on the same network even if it is on the same switch.	Create a virtual tunnel for secure data transmission over the Internet.
They allow the grouping of devices scattered across multiple physical locations into a single transmission domain.	Provide encryption and anonymization.
They can be intended as a subcategory of VPNs.	They increase the overall efficiency of a network distributed over multiple geographic locations
Optimal for splitting a network into logical parts for better management, but they do not provide any security features.	Operates in an unsecured online environment by definition.
Reduce the need for routers and the expense of managing them.	Enable users to reliably send and receive sensitive data by providing an encrypted connection over the Internet.
They remove latency in the network and improve its efficiency, facilitate its management and scalability, and save HW network resources.	They allow connection partners to securely facilitate the transmission of sensitive data.
They use the layer-two frame tag for encapsulation and can scale up to 4000 VLANs.	Mitigate access attempts by malicious hackers by exploiting any confidential information.
	Help workers do their work remotely in their organizations.
	Connection partners leverage this technology to access regionally restricted websites and maintain encryption during browsing activities for maximum protection from any type of cyber damage.

4. Practical Mobility Management in Modern Scenarios

With the huge proliferation of mobile devices, and therefore, different kind of mobility (pedestrian, vehicular, autonomous, flying, etc.), modern networks must accommodate the effects of movement, strictly reflected to the physical layer of the involved devices (Doppler shifts, fading, path loss, shadowing, reflection, refraction, etc.). Standard solutions, such as VLANs and VPNs, which originally have been designed for static networks, are not inherently ready for mobility management, so several solutions have been proposed. In this section, we will overview the main existing solutions which give the opportunity to manage mobility, while maintaining the advantages of the previous solutions.

4.1. Dealing with Mobility via VPN Applications

WireGuard [32–35] is a free software (registered trademarks of Jason A. Donenfeld) recently established in the IT market for creating VPNs, allowing efficient management to regulate access to certain network resources and isolating user's data flow from the outside world. It is also defined as the "the Next Generation Kernel Network Tunnel" software [36], and it belongs to the Noise Protocol Framework [37]. It is a free tool under the GPLv2 license, written in the "C" and "Go" languages and works with Windows, macOS, BSD, iOS and Android. It offers optimizations for mobile devices and IoT systems. Given its excellent features, it has been integrated directly into the Linux kernel, making it virtually available on all connected devices around the world, which is also possible because it is relatively light and has very low hardware requirements. WireGuard is based on so-called Cryptokey Routing, where the IP addresses of the tunnel are assigned in a one-to-one mode to the peer's public key for decryption of incoming packets, which are delivered only if they come from the address corresponding to the key. WireGuard does not negotiate the cryptographic bases of the handshake individually, but only a subset of them. If one of the cryptographic bases is no longer secure, a new version of the protocol is published to protect the data flow. One of the strengths of WireGuard is its codebase, consisting of about 4000 lines of code compared to those of OpenVPN or IPsec which are, respectively, 10,000 and 600,000, and is therefore intrinsically more secure because it is easily maintainable

and with a minimal attack surface. The codebase guarantees greater security and higher performance. By providing higher transmission speed and lower latency than historic protocols, if no data is passing through the tunnel, WireGuard is "at rest", thus reducing the amount of used energy. It provides very useful features for use in the mobile and IOT world, thanks to roaming support from the Wi-Fi network to the mobile phone network and vice versa. In fact, in [33], the protocol underlying WireGuard is deeply analyzed and tested by the CryptoVerif proof assistant. The authors conducted a large, deep analysis of WireGuard signaling messages (such as the transport data messages), proofing and confirming the goodness of the VPN in terms of secrecy, authentication, session uniqueness, replay attacks, etc. The authors of [34], instead, demonstrated how data security can be guaranteed by WireGuard in a real VPN, involving a laboratory and several African universities. The authors coupled WireGuard and Apache Guacamole, testing the strength of the considered VPN in terms of secrecy robustness. In [35], the WireGuard VPN is considered in the context of 5G network slicing, for the success of its security performance. The importance of [35] consists of the practical demonstration of the Wireguard strength, performed by the implementation of a real, secure network, tunneling protocol in a real 5G network, providing virtualized network functions. The market penetration of OpenVPN and Wireguard is demonstrated by their integration into some new static and mobile devices, such as UAVs and RaspberryPi (37 Hills Rd, Cambridge CB2 1NF, UK) (from versions two onwards), as well as in the most advanced IoT sensor systems, even if it is always possible to use firmware such as OpenWRT [38,39] as an MQTT [40–42] broker on the endpoints to convey traffic safely.

Figure 4 illustrates a typical use case of a VPN (which can be integrated by WireGuard) over a connection between an LTE-connected (or 5G-connected) Unmanned Aerial Vehicle (UAVs) and the related Ground Control Station (GCS), which could be also connected via LTE or 5G.

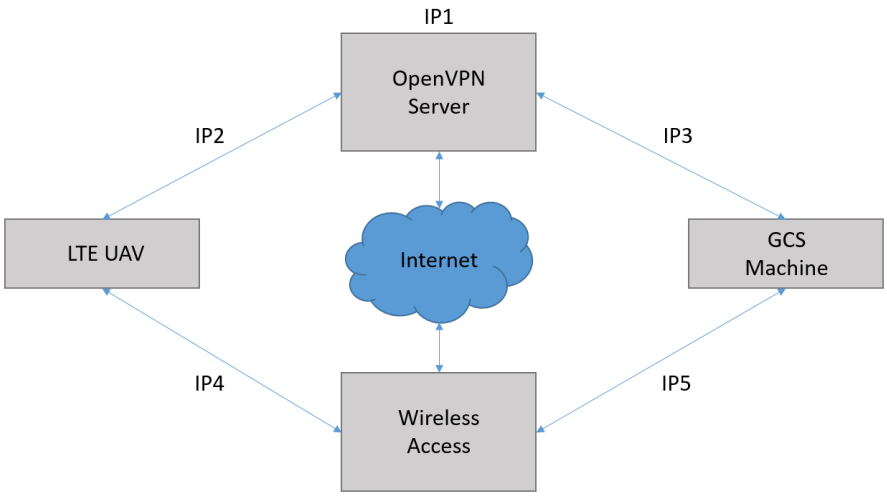

Figure 4. An example of VPN management for a Long Term Evolution (LTE) Unmanned Aerial Vehicle (UAV) and a Ground Control Station (GCS) device.

Both UAV and GCS have their IP addresses on the basis of their service provider (we assume that the UAV is not directly connected to the GCS, because their IP addresses are not visible to each other). The right management can be obtained by a VPN (Figure 4): we assume that the server has a static address IP1 address, while the UAV has obtained its IP4 address from the LTE Wireless Network, as well as the GCS with IP5. The OpenVPN server runs on the IP1 device, while the OpenVPN clients run on the IP4 (UAV) and IP5 (GCS) devices, so they can receive VPN addresses as illustrated, i.e., IP2 for the UAV and IP3 for the GCS. The IP2 and IP3 addresses belong to the same VPN network, so the UAV can directly communicate with the GCS.

Additionally, in [43], a secure interconnection of UAVs with GCSs via VPN is presented (Figure 5). The authors demonstrated the feasibility of using a 4G connection to link the drone directly to a data server (green and short dotted line), where the "interesting" data (audio, video, telemetry, etc.) can be stored for further processing. The second VPN connection (red long dotted line) is realized between drone and GCS, in order to perform First Person View (FPV) operations at Line of Sight (LOS) or Beyond Visual LOS (BVLOS) conditions. The proposed VPN-based idea is able to provide a long-range and high-capacity connection (they based the experiments on video and audio streaming [44]), by creating the VPN tunnel to the public Internet and towards the GCS. The proposed architecture underlines the need to overcoming security issues in UAVs scenarios [45].

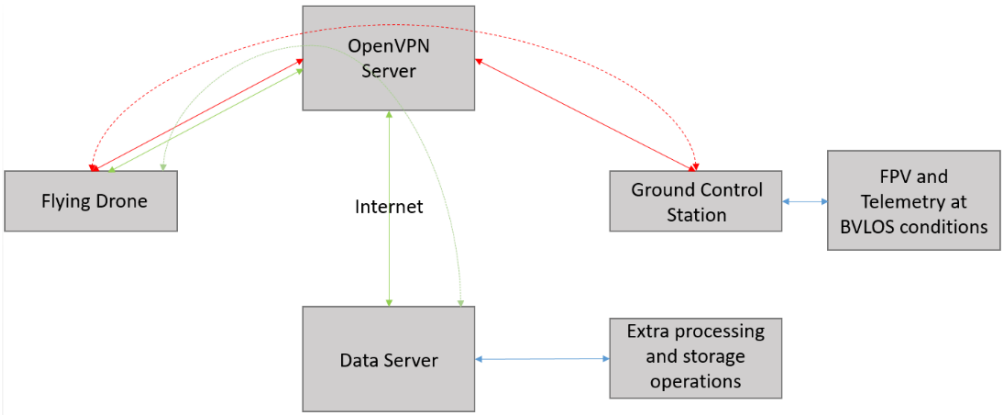

Figure 5. A logical representation of the VPN architecture considered in [37].

4.2. Possible Issues and Solutions When Dealing with Mobility in VLANs

One of the main issues when dealing with VLAN in mobile environments is the management of the IP addresses. In general, DHCP servers are responsible for IP address assignments, but the huge increase in available mobile devices induces great challenges related to DHCP performance. One countermeasure is represented by reconfiguring the IP lease times and the address pools dynamically, adapting them to the WiFi user behavior [46]. In the first case, the lease times are set on the basis of the historical time pattern to reclaim IP addresses, while in the second case the IP addresses are migrated across VLANs on the basis of the spatial–temporal mobility correlation.

Regarding the address pools, for a higher number of clients, DHCP messages (generally broadcast messages) will consume more bandwidth. The main solution is to split the overall network into a subset of VLANs, without implementing a DHCP server for each VLAN. It is possible to exploit the advantages of using a DHCP relay agent [47] for each VLAN, able to change the properties of the DHCP packet broadcasted by the client in its broadcast domain and forward it to DHCP server (Figure 6). In this way, most of the traffic is cut from the network, increasing the overall throughput.

Regarding the IP lease time, there are three main states for leasing an address:

(a) Initializing: the IP address is acquired after a set of message exchanges (discover message from client C to broadcast B, offer message from server S to C, unicast request message from C to S and the acknowledgement from S to C);
(b) Renewing: in this state, a message is sent by the client (if it is still present in the network) to the server, asking for the extension (in time) of the lease; it is a periodical message (the period is equal to the half of the lease time);
(c) Releasing: this state occurs if the client sends a clear release message to the server (because it wants to leave the network) or if the periodical renew message has not been sent.

After these considerations, it is clear that the lease time should be set adequately: if it is too high, the address pool could exhaust soon, while if it is too low, DHCP servers could

be overloaded. So, one of the best solutions is to evaluate users behavior in terms of DHCP requests, and then adapt the lease time to the network as needed in terms of online time pattern to reclaim IP in time.

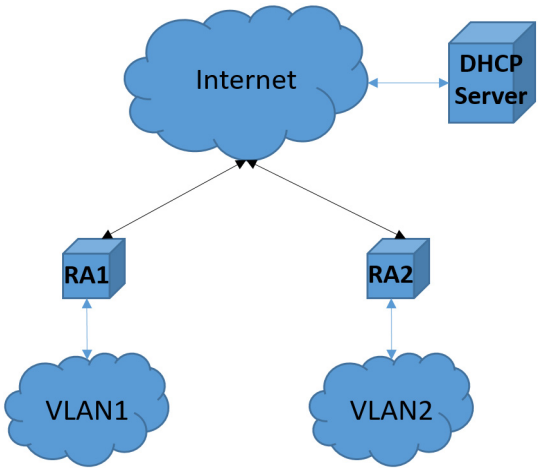

Figure 6. The typical structure of a VLAN segmented network and the presence of DHCP Relay Agents (RAs) [40].

5. Real Security Implementations for VPNs and VLANs

This section is dedicated to the illustration of the security issues and countermeasures related to VPNs and VLANs. Some examples of real scripts are given, in order to learn how to configure devices properly.

5.1. Security Issues and Countermeasures in VLANs

In this section, we focus on the security of VLAN and how to apply it in a corporate environment. As a reference, we use Cisco switches, but many concepts can be applied for other vendors. The first level of security, and often the most overlooked, is the physical security of the equipment: tampering is always unwanted, so it is good to protect the access to the virtual terminal (VTY), by configuring proper credentials and a timeout:

```
S# configure terminal
S(config)# username admin privilege 15 secret P4$$w0rd_!
S(config)# line console 0
S(config-line)# login local
S(config-line)# password P4$$w0rd_!
S(config-line)# exec-timeout 60 0
```

In addition, by applying the same configuration also the VTY (telnet/ssh) and creating an access list to limit access only to certain hosts or subnets it is possible avoid brute-force attacks:

```
S(config)# line vty 0 15
S(config-line)# password P4$$w0rd_!
S(config-line)# login local
S(config-line)# exec-timeout 60 0
S(config-line)# transport preferred ssh
S(config-line)# access-class 115 in
S(config)# access-list 115 remark Inbound Limitations
S(config)# access-list 115 permit ip host 1.2.3.4 any
S(config)# access-list 115 permit ip 192.168.100.0 0.0.0.255 any
```

The general rule, in addition, is to avoid the use of VLAN 1 (the default VLAN) data traffic, and VLAN pruning. The default VLAN is present in all network devices, as well as being untagged, because it is used for the exchange of information through protocols,

such as Cisco Discovery Protocol (CDP) and VTP. Another good technique that a network administrator must consider is the pruning, allowing only strictly necessary VLANs on each link, so considering a switch S:

```
S(config)# interface fastethernet0/24
S(config-if)# switchport trunk allowed vlan remove 1,2,3,4,5
S(config-if)# switchport access vlan 24
```

It is also suggested to disable 'risky' protocols from all ports if they are not needed. Certain information-exchange protocols, such as CDP and UniDirectional Link Detection (UDLD) for example, can create security holes:

```
S(config)# interface fastethernet0/24
S(config-if)# no cdp enable
S(config-if)# no udld port
```

Pay particular attention to the configuration of VTP—if it appears to be misconfigured, it can become a dangerous security hole. If we consider a Core switch (C) and an Edge Switch (E), the following lines should be considered:

```
C(config)# vtp domain VTPdomain
C(config)# vtp password P4$$w0rd_! secret
C(config)# vtp mode server
C(config)# vtp version 2
C(config)# vtp pruning


E(config)# vtp domain VTPdomain
E(config)# vtp password P4$$w0rd_! secret
E(config)# vtp mode client
E(config)# vtp version 2
E(config)# vtp pruning
```

Another key feature for VLAN security is the restriction of inter-VLAN routing via access lists. Routing between VLAN should be allowed, but to ensure a higher level of security, the routing can be limited adequately [48]. For example, with the following scripts, VLAN24 can be allowed to access the Internet and only the DNS server of the VLAN:

```
C(config)# access-list 100 remark Allow DNS
C(config)# access-list 100 permit udp 192.168.240.0 0.0.0.255 host 192.168.240.1 eq 53
C(config)# access-list 100 deny ip 192.168.240.0 0.0.0.255 192.168.240.0 0.0.0.255 log
C(config)# access-list 100 permit ip 192.168.240.0 0.0.0.255 any
C(config)# interface vlan 24
C(config-if)# ip access-group 100 in
```

Some examples of real VPN implementations can be found in [49–51].

5.2. Security Issues and Countermeasures in VPNs

Nowadays, all network devices provide VPN functionalities. First of all, a basic VPN protection consists of the firewall, which should be always present in a network. Most recent security solutions suggest the integration of firewalls with complicated Intrusion Detection Systems (IDSs) [52] or Intrusion Prevention Systems (IPSs) [23,53], in order to improve VPN security performance. We will give a short introduction to IDSs, then their integration with VPNs will be illustrated.

5.2.1. IDSs, IPSs and Intrusion Detection and Prevention Systems (IDPSs)

IDS refers to a software component or to a hardware device with an embedded dedicated software, adapted to analyze the traffic in transit to or from the specific network

in which it is installed. The purpose of having an IDS in a network (usually a LAN) is to monitor the traffic in order to detect any suspicious activity and/or malicious activity towards any host (whether client or server) in the network. Such systems are often able to generate alerts and log files based on their activities or analysis—they will have access to relational databases, while saving information about the particular network traffic that is 'interesting' from the point of view of the network administrator.

An IPS consists, instead, of a software or hardware component disposed within a network, intended to prevent attempts to attack the network. The most common preventive actions taken by an IPS are: packet or session dropping, reset of the session and adding to a black-list the host that moved the attack.

IDS and IPS are complementary technologies in the field of network security and able to work in synergy. Both are activated (alert or prevention) based on the matching between certain rules provided by the network and transiting packets. For these reasons, IDS and IPS are implemented together, obtaining a hybrid system called Intrusion Detection and Prevention System (IDPSs).

There are four different types of IDPS technologies:

(a) Network-Based IDPSs (NB-IDPSs): these monitor traffic, with particular regard to the application and network layers. Typically they are installed on the edge of the network topology (before firewalls and gateways) or on the extreme limits of the DeMilitarized Zones (DMZs);
(b) Wireless IDPSs: these are dedicated to monitoring only wireless traffic, with particular attention paid to the networking protocols;
(c) Network Behavior Analysis IDPSs (NBA-IDPSs): these examine packets to identify threats that generate suspicious traffic uncommon for a network, such as attempted Distributed Denial of Service (DDoS). They are also often used to monitor internal traffic on the same network, or to give access to external third parties;
(d) Host-Based IDPSs (HB-IDPSs): these are dedicated to monitoring everything that happens within the single host to which they belong: they are typically a server, reachable from outside the network, or a client of public access. They monitor data ranging from processes running on the machine, the file access, system logs, etc.

The general context of using IDPSs is business: the processing of sensitive data by companies requires them to use appropriate and effective data protection systems in their internal networks, in order to prevent violations of corporate security policies. Most IDPS use different detection technologies, potentially in combination, to provide a better degree of accuracy. There are three main technologies:

(a) Signature-based: a comparison of the signatures managed by the network and the transiting packets is carried out. This technology is very effective in identifying known threats that have static attack patterns, but they are almost useless against unknown threats;
(b) Statistical anomaly-based detection: this technology is based on maintaining a vision of the statistical data related to normal network flows, and providing warning situations when the given parameters deviate from their standard values. Obviously the initial statistics about "normal activity" require a preliminary study of the network in order to determine which are the normal values;
(c) Stateful protocol analysis: in this case, network flows are analyzed, comparing them with specific profiles (e.g., a user having accesses to an FTP server, without having obtained the authentication privileges yet). This type of analysis is very sophisticated but, at the same time, it is very difficult and complex because profiles need to be created for each protocol, covering all possible use cases, with a high computational cost.

5.2.2. Integration of IDSs and IPSs with VPNs

There are several works in the literature tackling the issue of strengthening the security level in VPNs with IDSs and IPSs. For example, in [52] the authors considered the DoS attack based on the TCP SYN field, which is able to start TCP connections on HTTP servers

in a very short time and periodically, using fake IP addresses. Firewalls, of course, are able to block the attack, but they become the victims. It is necessary therefore to create an IDS with a timely detection, consequently fixing the problem. After attack detection, the attack can be successfully blocked by creating a dedicated Access Control List (ACL), able to block the attack. The automatic blocking of DoS and similar attacks is feasible by integrating the VPN with an IPS. In [23], the authors face the issue of implementing an IPS in wireless networks (generally the solution is a Wireless IPS—WIPS): their idea is called WTLS-Based VPN (WBVPN), by which a single path is built between wireless device and their destination, exploiting the session-resuming feature of WTLS. In this way, the IPS can analyze the traffic and prevent unauthorized operations. The authors also considered a real case, showing the good performance of the proposed scheme. The article in [53] focuses on the additional efforts which could be made to overcome security issues in a network via VPN, proposing a new framework. It argues about the maximization of the synchronization of the security services, while reducing the overhead traffic.

6. Conclusions

In this paper we provide a deep knowledge of the main practical countermeasures for preventing and combating security issues in static and dynamic networks. In particular, VPNs and VLANs have been considered, giving particular emphasis to the ways that mobility and security can be ensured. We decided to summarize the main contributions in these areas of interest given the huge demand for connections between remote locations while moving by feet or in a vehicle. We emphasize the capability of a VPN to securely connect the two endpoints through a dedicated and secure tunnel, while VLANs are able to decrease the impact of some scalability issues of large networks. The most recent solutions are illustrated, providing the reader with the possibility of understanding how to behave in one's own corporate network. Of course, the implementation of VPNs and VLANs poses specific issues about security, so some good solutions are also considered and described. Security issues in VLANs can be effectively mitigated through the combination of good network-management practices, effective network design, and the application of advanced security products. For VPNs, there is the availability of strong authentication support, strong encryption algorithms, support for antivirus software and IDS/IPS services, strong default security for administration and maintenance ports, digital certificate support, support for recording and auditing, and the ability to assign addresses to clients on a private network while ensuring that all addresses are kept private.

Author Contributions: Conceptualization, A.F.G. and P.F.; formal analysis, A.F.G. and G.M., investigation, A.F.G.; writing—original draft preparation, P.F.; writing—review and editing, P.F. and G.M.; visualization, A.F.G.; supervision, P.F. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data sharing not applicable.

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

References

1. De Rango, F.; Lentini, D.C.; Marano, S. Static and dynamic 4-way handshake solutions to avoid denial of service attack in Wi-Fi protected access and IEEE 802.11i. *EURASIP J. Wirel. Commun. Netw.* **2006**, *2006*, 047453. [CrossRef]
2. De Rango, F.; Marano, S. Trust-based SAODV protocol with intrusion detection and incentive cooperation in MANET. In Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly, Leipzig, Germany, 21–24 June 2009; pp. 1443–1448.
3. Jahan, S.; Rahman, M.S.; Saha, S. Application specific tunneling protocol selection for Virtual Private Networks. In Proceedings of the International Conference on Networking Systems and Security (NSysS), Dhaka, Bangladesh, 5–8 January 2017.

4. Lupia, A.; de Rango, F. Evaluation of the Energy Consumption Introduced by a Trust Management Scheme on Mobile Ad-hoc Networks. *J. Netw.* **2015**, *10*, 240–251. [CrossRef]
5. De la Cruz, J.E.C.; Goyzueta, C.A.R.; Cahuana, C.D. Open VProxy: Low Cost Squid Proxy Based Teleworking Environment with OpenVPN Encrypted Tunnels to Provide Confidentiality, Integrity and Availability. In Proceedings of the IEEE Engineering International Research Conference (EIRCON), Lima, Peru, 21–23 October 2020.
6. Duddu, S.; Sai, A.R.; Sowjanya, L.S.; Rao, G.R.; Siddabattula, K.S. Secure Socket Layer Stripping Attack Using Address Resolution Protocol Spoofing. In Proceedings of the 4th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 13–15 May 2020.
7. Floissac, N.; L'Hyver, Y. From AES-128 to AES-192 and AES-256, How to Adapt Differential Fault Analysis Attacks on Key Expansion. In Proceedings of the Workshop on Fault Diagnosis and Tolerance in Cryptography, Milan, Italy, 17 September 2011.
8. Luo, J.; Ji, Q. Password Acquisition and Traffic Decryption Based on L2TP/IPSec. In Proceedings of the IEEE 20th International Conference on Communication Technology (ICCT), Nanning, China, 28–31 October 2020.
9. Gui-hong, L.; Hua, Z.; Gui-zhi, L. Building a Secure Web Server Based on OpenSSL and Apache. In Proceedings of the International Conference on E-Business and E-Government, Guangzhou, China, 7–9 May 2010.
10. Rhee, M.Y. Transport Layer Security: SSLv3 and TLSv1. In *Wiley Wireless Mobile Internet Security*; Book Chapter; Wiley: New York, NY, USA, 2013.
11. Semwal, P.; Sharma, M.K. Comparative study of different cryptographic algorithms for data security in cloud computing. In Proceedings of the 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA), Dehradun, India, 15–16 September 2017.
12. Kim, Y.-J.; Kolesnikov, V.; Kim, H.; Thottan, M. SSTP: A scalable and secure transport protocol for smart grid data collection. In Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm), Brussels, Belgium, 17–20 October 2011.
13. Jones, J.; Wimmer, H.; Haddad, R.J. PPTP VPN: An Analysis of the Effects of a DDoS Attack. In Proceedings of the IEEE SoutheastCon, Huntsville, AL, USA, 11–14 April 2019.
14. Kent, S.; Seo, K.; Network Working Group. Request for Comments: 4301. 2005. Available online: https://www.rfc-editor.org/rfc/pdfrfc/rfc4301.txt.pdf (accessed on 18 May 2021).
15. Socievole, A.; Caputo, A.; de Rango, F.; Fazio, P. Routing in mobile opportunistic social networks with selfish nodes. *Wirel. Commun. Mob. Comput.* **2019**, *2019*, 6359806. [CrossRef]
16. Socievole, A.; de Rango, F.; Caputo, A. Wireless contacts, Facebook friendships and interests: Analysis of a multi-layer social network in an academic environment. In Proceedings of the 2014 IFIP Wireless Days (WD), Rio de Janeiro, Brazil, 12–14 November 2014; pp. 1–7.
17. Karbasioun, M.M.; Berenjkub, M.; Taji, B. Securing mobile IP communications using MOBIKE protocol. In Proceedings of the IEEE International Conference on Telecommunications, St. Petersburg, Russia, 16–19 June 2008.
18. Goff, T.; Moronski, J.; Phatak, D.S.; Gupta, V. Freeze-TCP: A true end-to-end TCP enhancement mechanism for mobile environments. In Proceedings of the IEEE INFOCOM Annual Joint Conference of the IEEE Computer and Communications Societies, Tel Aviv, Israel, 26–30 March 2000; Volume 3, pp. 1537–1545.
19. Alshalan, A.; Pisharody, S.; Huang, D. MobiVPN: A Mobile VPN Providing Persistency to Applications. In Proceedings of the International Conference on Computing, Networking and Communications, Wireless Networks, Kauai, HI, USA, 15–18 February 2016.
20. A VPN for a New Era, Sectra Communications. Available online: https://communications.sectra.com/product/secure-mobile-vpn-up-to-restricted/ (accessed on 13 May 2021).
21. Columbitech App for Iphone. Available online: https://apps.apple.com/it/app/columbitech-mobile-vpn/id1046769589 (accessed on 14 April 2021).
22. Dong, L.; Kang, X.; Song, J. A WTLS-based virtual private network for wireless intrusion prevention. In Proceedings of the International Conference on Computer Application and System Modeling (ICCASM), Taiyuan, China, 22–24 October 2010; Volume 3.
23. Zúquete, A.; Frade, C. Fast vpn mobility across wi-fi hotspots. In Proceedings of the IEEE Security and Communication Networks (IWSCN), 2nd International Workshop on, Karlstad, Sweden, 26–28 May 2010; pp. 1–7.
24. Schonwalder, J.; Chulkov, G.; Asgarov, E.; Cretu, M. Session resumption for the secure shell protocol. In Proceedings of the IFIP/IEEE International Symposium on Integrated Network Management, Long Island, NY, USA, 1–5 June 2009; pp. 157–163.
25. Chen, T.-C.; Chen, J.C.; Liu, Z.H. Secure Network Mobility (SeNEMO) for Real-Time Applications. In Proceedings of the IEEE Transactions on Mobile Computing, Abu Dhabi, United Arab Emirates, 10 October 2011; Volume 10, pp. 1113–1130.
26. Ernst, T.; Tj, K. Network Mobility Working Group, IETF. Available online: https://datatracker.ietf.org/wg/nemo/about/ (accessed on 18 May 2021).
27. Xinzhan, L.; Chuanqing, C. Discuss on VLAN Stacking in Packet Network. In Proceedings of the International Symposium on Intelligent Ubiquitous Computing and Education, Chengdu, China, 15–16 May 2009.
28. CISCO ISL Protocol for LAN Switching. Available online: https://www.cisco.com/c/en/us/support/docs/lan-switching/8021q/8758-43.html (accessed on 18 May 2021).

29. IEEE 802.1Q-2018—IEEE Standard for Local and Metropolitan Area Networks—Bridges and Bridged Networks. Available online: https://standards.ieee.org/standard/802_1Q-2018.html (accessed on 25 May 2021).
30. Verma, R.O.; Shriramwar, S.S. Effective VTP Model for Enterprise VLAN Security. In Proceedings of the International Conference on Communication Systems and Network Technologies, Gwalior, India, 6–8 April 2013.
31. Understanding VLAN Trunking Protocol, Cisco. Available online: https://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/10558-21.html?dtid=osscdc000283 (accessed on 19 May 2021).
32. WireGuard. Available online: https://www.wireguard.com/ (accessed on 22 May 2021).
33. Lipp, B.; Blanchet, B.; Bhargavan, K. A Mechanised Cryptographic Proof of the WireGuard Virtual Private Network Protocol. In Proceedings of the IEEE European Symposium on Security and Privacy (EuroS&P), Stockholm, Sweden, 17–19 June 2019.
34. Kossingou, G.M.S.; Dégboé, B.M.; Ouya, S.; Mendy, G. Mutualisation of ICT laboratory resources between West and Central African universities in post-crisis situations: The case of Senegal and the Central African Republic. In Proceedings of the Sixth International Conference on e-Learning (econf), Sakheer, Bahrain, 6–7 December 2020.
35. Haga, S.; Esmaeily, A.; Kralevska, K.; Gligoroski, D. 5G Network Slice Isolation with WireGuard and Open Source MANO: A VPNaaS Proof-of-Concept. In Proceedings of the IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Leganes, Spain, 9–12 November 2020.
36. Donenfeld, J.A. WireGuard: Next Generation Kernel Network Tunnel. *NDSS*. 2017. Available online: https://www.wireguard.com/papers/wireguard.pdf (accessed on 26 May 2021).
37. Trevor Perrin, Noise Protocol Framework. Available online: http://www.noiseprotocol.org/ (accessed on 27 May 2021).
38. Palazzi, C.E.; Brunati, M.; Roccetti, M. An OpenWRT solution for future wireless homes. In Proceedings of the IEEE International Conference on Multimedia and Expo, Singapore, 19–23 July 2010.
39. OpenWrt, a Writable Filesystem with Package Management. Available online: https://openwrt.org/ (accessed on 24 May 2021).
40. Silva, C.R.M.; Silva, F.A.C.M. An IoT Gateway for Modbus and MQTT Integration. In Proceedings of the SBMO/IEEE MTT-S International Microwave and Optoelectronics Conference (IMOC), Aveiro, Portugal, 10–14 November 2019.
41. Message Queue Telemetry Transport (MQTT), the standard for IoT messaging. Available online: https://mqtt.org (accessed on 30 April 2021).
42. de Rango, F.; Potrino, G.; Tropea, M.; Fazio, P. Energy-aware dynamic Internet of Things security system based on Elliptic Curve Cryptography and Message Queue Telemetry Transport protocol for mitigating Replay attacks. *Pervasive Mob. Comput.* **2020**, *61*, 101105. [CrossRef]
43. Guirado, R.; Padró, J.C.; Zoroa, A.; Olivert, J.; Bukva, A.; Cavestany, P. StratoTrans: Unmanned Aerial System (UAS) 4G Communication Framework Applied on the Monitoring of Road Traffic and Linear Infrastructure. *Drones* **2021**, *5*, 10. [CrossRef]
44. de Rango, F.; Tropea, M.; Fazio, P.; Marano, S. Overview on VoIP: Subjective and objective measurement methods. *Int. J. Comput. Sci. Netw. Secur.* **2006**, *6*, 140–153.
45. Álvares, P.; Silva, L.; Magaia, N. Blockchain-Based Solutions for UAV-Assisted Connected Vehicle Networks in Smart Cities: A Review, Open Issues, and Future Perspectives. *Telecom* **2021**, *2*, 108–140. [CrossRef]
46. Miao, C.; Wang, J.; Ji, T.; Wang, H.; Xu, C.; Li, F.; Ren, F. BDAC: A Behavior-aware Dynamic Adaptive Configuration on DHCP in Wireless LANs. In Proceedings of the IEEE 27th International Conference on Network Protocols (ICNP), Chicago, IL, USA, 7–10 October 2019.
47. Patrick, M. *DHCP Relay Agent Information Option*; 2001. Available online: https://www.rfc-editor.org/info/rfc3046 (accessed on 26 May 2021).
48. Malatesta, L. Articoli e Configurazioni. Available online: https://www.malatesta.biz/ (accessed on 26 May 2021).
49. Progetto Cogito. Available online: https://www.icar.cnr.it/progetti/cogito-sistema-dinamico-e-cognitivo-per-consentire-agli-edifici-di-apprendere-ed-adattarsi/ (accessed on 20 May 2021).
50. Distretto Domus Cosenza. Available online: https://www.gruppotim.it/it/archivio-stampa/mercato/2016/TIM-Distretto-Domus-Cosenza-14Dicembre2016.html (accessed on 19 May 2021).
51. Progetto Res Novae. Available online: https://www.cueim.org/progetti/res-novae-reti-edifici-strade-nuovi-obiettivi-virtuosi-per-lambiente-e-lenergia-smart-city/ (accessed on 23 May 2021).
52. Fosić, I.; Žagar, D. VPN network protection by IDS system implementation. In Proceedings of the 34th International Conven-tion MIPRO, Opatija, Croatia, 23–27 May 2011.
53. Dong, L.; Yu, S.; Xia, T.; Liao, R. WBIPS: A Lightweight WTLS-Based Intrusion Prevention Scheme. In Proceedings of the International Conference on Wireless Communications, Networking and Mobile Computing, Shanghai, China, 21–25 September 2007.