Comparison of VPN Protocols at Network Layer Focusing on Wire Guard Protocol

https://doi.org/10.3991/ijim.v14i18.16507

Adnan Mohsin Abdulazeez (✉)
Duhok Polytechnic University, Kurdistan Region, Iraq
adnan.mohsin@dpu.edu.krd

Baraa Wasfi Salim
Nawroz University, Duhok, Iraq

Diyar Qader Zeebaree
Duhok Polytechnic University, Duhok, Iraq

Dana Doghramachi
Erbil Polytechnic University, Erbil, Iraq

Abstract—The key point of this paper is to assess and look over the top of the line network layer-based VPN (Virtual Private Network) protocols because data link layer is hardly ever found to be in use in organizations, the reason is because of its exceedingly high charge. VPN is commonly used in business situations to provide secure communication channels over public infrastructure such as the Internet. VPNs provide secure encrypted communication between remote networks worldwide by using Internet Protocol (IP) tunnels and a shared medium like the Internet. The paper follows and sets standards for different types of protocols and techniques. The VPN architectural feature is made to deliver a dependable and safe network that is not in line with regular networks that provide a higher trust and a higher secure channel between user and organization. The current study took place to summaries the usage of existing VPNs protocol and to show the strength of every VPN, through different studies that have been made by other researchers as well as an extra focus on the state of art protocol, Wire guard. It is also worthy of mentioning that the wire guard compared with other protocols such as IPsec and GRE. The studies show the Wire Guard being a better choice in terms of other well-known procedures to inaugurate a secure and trusted VPN.

Keywords—VPN, IPsec, GRE, Wire Guard, Protocol, Security, Tunnel, IKpsk2, VPN Performance

1 Introduction

Nowadays, Internet communication becomes a major part of infrastructure. Based on the Internet most of the applications of infrastructure systems can be operated [1, 2].

A VPN is known as a better system for collective services delivered by open network structures. VPN offers affordable, competent use of bandwidth, scalable and flexible functionality, safe and remote connections. VPN offers a virtual secure line amongst two network sites that network traffic passing from end to end. VPN network is altered by many aspects such as the operating system, hardware devices being used, interoperability, and algorithm being applied [3–5].

VPNs are at the present time is turning into a universal technique used for distant use of access. Companies have a higher chance of actually branching out to many types of locations and have offices spread out in multiple countries [6, 7]. VPNs safely send the info (file sharing, video conferencing, etc.). By the Internet, portals to not only close by users but also users that are pretty far from any office branches and business associates into an extended corporate network [8, 9].

The second important advantage of VPNs is the ability to change from whatever scalability needed, which aids in saving time in making a new link between the headquarter and new branch buildings by using Internet Service look Providers (ISPs) infrastructure. This process helps make it simpler when adding and modifying the number of connected users so that companies can add important capacity without needing to add infrastructure [10].

Network layer VPNs are made by using Layer 3 tunneling and/or encryption methods. For example, it is the use of the IPsec tunneling and encryption protocol that is of need to create VPNs. Another example is the GRE and Wire Guard procedures [11, 12].

This paper has a key aspect that is around a network layer VPNs. Network layers give a very well comforting place to do encryption [13, 14]. The network layer is reduced just about the right amount in the stack to offer smooth connectivity to all applications that are active on top of it and is on its highest to allow a decent granularity for the traffic that should be part of the VPN according to the extensive IP Addressing architecture in place [11].

This paper is set up in the following order: Section 2 grants comprehensive investigation linked to the matter of this paper, Section 3 presents VPN Types Based on OSI Layer Three and discusses different VPN tunnels and analyses of the performance in each VPN tunnel. Section 4 presents The VPN Tunneling Solutions and emerge the weaknesses and strengths of the (Wire Guard, IP Sec, and GRE) VPN tunnels. Finally, the conclusions and discussion are presented in section5.

2 Literature Review and Problem Statement

The reason for a VPN is to offer an organization the same power as remote contracted lines at a much cheaper cost by means of the joint infrastructure. In this section, a review of VPN protocols is presented. As mentioned above, a lot of work is aimed to find out the best rule for VPN due to the fact that it of great importance in terms of performance. VPN is a pretty used up and not new method that is still a widely used technology. Recent top studies give the image to be non-existent. However, the ones are still informative [3]. Some researches talk about security methods of a VPN [13], while many others focus on the amazingly accurate performance of VPNs [15–17]. However,

no academic research doesn't really seems to compare IP Sec [8, 10] to a more highly state VPNs procedure such as Wire Guard [18, 19] and GRE [20]. One reason the VPN came to existence was for the purpose of giving organizations ability received by closed and not public leased lines at affordable rates by taking advantage of the shared infrastructure, Network abilities and how it is compared to its VPN protocols on both wired and the wireless networks are shown in [21]. In [18, 22–25] authors, which also shows a great overview of the Next Generation Kernel Network Tunnel (Wire Guard) they presented the format verification of the protocol and his architecture in addition to the attribute, strength, weakness and a future challenging promising. The comparative between protocol (SSL) in the data link layer (layer2) and IP Sec protocol in the network layer (layer 3) described in [26]. Problems that may occur in IP Sec policy specification are hard to analyze for three different reasons. First, Encapsulation in IP Sec makes it hard to show specific errors. Second, undesired errors can occur do to overlapping. Third, there is an unclear bond between objective and specific policies. To figure out the solution to the problems, we firstly started a security policy in two levels: requirement level security policy and implementation level security policy. Requirement level policies shows security objective and are implementation independent [27].

3 The Aim of the Paper

The main target of this work is to present the review on the VPN tunnel and to compare the three protocols in the network layer (IPsec, GRE, and Wire guard) mentioned above regarding their features and underlying technologies so as to identify their strengths and weaknesses. A broad purpose of our study is to show which one between the three protocols is the best depending on some of the remarks(characteristics) mentioned in our paper and based on some previous reviewers' papers.

This is of great importance for the researchers in this field to effortlessly find and compare the above points to select the appropriate protocol for each purpose.

To achieve this aim, the following objectives are accomplished:

- The first goal is to do a study of the three protocols. Depending on the newest latest papers
- Performance evaluation of the three VPN protocols depending on standard metrics
- Highlighting the main advantage and disadvantages of each protocol.

4 Types of a Virtual Private Network (VPN)

VPN gives users the opportunity to be in contact with a closed network while using the Internet in a safe way as well as securely. VPN produces converted data and information into codes that prevent interrelation, which is known as a VPN tunnel, and every Internet traffic and communication is taken into the safe tunnel [13, 28]. VPN is practically made of two different kinds:

- Remote Access VPN: Remote Access VPN allows the one using it to have the opportunity to latch to a closed network and open every service and resource available from a distance [29]. The attachment amongst the user and the closed network happens within the Internet, and the connection is safe and closed. Remote Access VPN is beneficial for those who use it at home as well as for business [30].
- Site to Site VPN: A Site-to-Site VPN is also known as Router-to-Router VPN and is typically taken in by massive companies. Companies or organizations, with more than one offices in many kinds of areas, put Site-to-site VPN in use to make an attachment from one office location to the network at additional office location [4, 31, 32].
- Intranet-based VPN: This is known when many offices of the similar company are attached using Site-to-Site VPN type, this is known as Intranet-based VPN [4];
- Extranet based VPN: They are companies that use Site-to-site VPN type to have a company attached to the office of an additional company, it this is known as Extranet based VPN [4].
- VPN Architecture (Framework): A VPN is said to function by routing your device's Internet connection by the VPN's private server of your choosing instead of your Internet service provider (ISP) the result will be your data being transmitted into the Internet. This process actually comes from the VPN instead of the computer [27]. The VPN plays a significant role as a negotiator in some kind of way. So keep in mind, to the Internet, the result will be the stealth of your IP address – the series of figures your ISP gives your device – and defending your identity [33, 34,35]. Furthermore, if your data is somehow interrupted, it will be illegible until it ends up in its final destination. A VPN creates a secure "tunnel" from your device to the Internet and makes your vital data hidden through something that is known as encryption[27, 36] see Fig. 1.

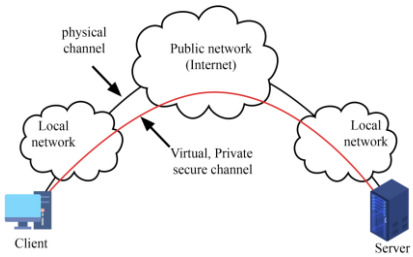

Fig. 1. VPN Architecture.

Types of devices of VPN are of three different kinds, Hardware usually a VPN type of router, Firewall that is much safer, Software ideal for two endpoints not in a similar organization.

4. 1. VPN protocols types based on OSI layer three

VPN depends on tunneling methods for conducting data. The tunneling protocols work at the same OSI network layer. The most popular protocols that linked with VPN

tunnels are Internet protocol security (IP Sec) [36, 37], GRE tunneling and Wire guard tunneling protocol [29]. These VPN tunnels provide security, authentication, Confidentiality, Integrity, and encryption mechanisms [3, 38,40].

Internet protocol security (IP Sec): IP Sec provides validation of those who need to put it into use, coded parts of data, and data reliability in the moment of conduction of data stuck in the middle of the one that sends and the one that receives. It expenditures three main protocols one being Authentication Header (AH), the other Encapsulated Security Payload (ESP), and lastly, Internet Key Exchange (IKE) [41, 42]. They are put into use during launching connection and the transmission of data in a safe way [31, 41]. IP Sec can be worked in two encryption functions:

- Transport mode
- Tunnel mode.

Fig. 2 shows the architecture and design of IPsec VPN tunnel.

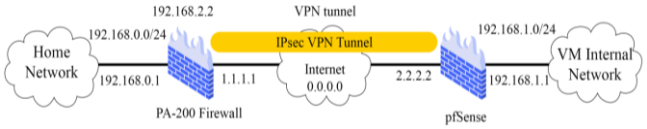

Fig. 2. IP Sec VPN Tunnel

Transport mode encrypts only the data part (Payload) of packets. Tunnel mode is much safer, which codes two things which are the header as well as the payload [13, 43], for a better understanding the below Table 1 has more details that explain the performance of IP Sec VPN tunnels.

IP Sec protocol suite: IKE, AH and ESP: IPsec states procedures that are safe for obtaining a secure IP communication on a point to point basis, counting: the security protocols AH and ESP, the algorithms for validation and encryption, and significant altercation mechanisms. AH and ESP does not necessarily handle the key exchange; the reason for that is because they think that the two nodes have already made a Security Association (SA). A SA is a "contract" amongst the two IPsec endpoints used to create the protection mechanisms and the keys to be in use through the next data transfer. For this reason, IP Sec standard stipulates both the Pre-Shared Key (PSK) mechanism and Internet Key Exchange (IKE) protocol. Conversely, the final use is asymmetric cryptography that is presumed to be substantial weight for minor sensor nodes [3, 17].

Both AH and ESP procedures help connectionless reliability, anti-replay security, and data origin validation. AH validates the entire IP packet, with the exemption of the IP header variable fields, which, being altered by intermediate nodes, cannot be validated. Unlike AH, ESP backs up confidentiality as well. ESP is used to encrypt the payload of an IP packet, but on the other hand, to AH it does not protect the IP header [46]. The Fig. 3 shows the IP Sec Architecture.

The AH and ESP conventions deliver two types of working modes: transport mode and tunnel mode. Conferring to the initial one, IP header and payload are encrypted, which was mentioned before. In tunnel mode, a new IP header is set up in front of the original IP packet, and security functions are applied to the encapsulated IP packet [16].

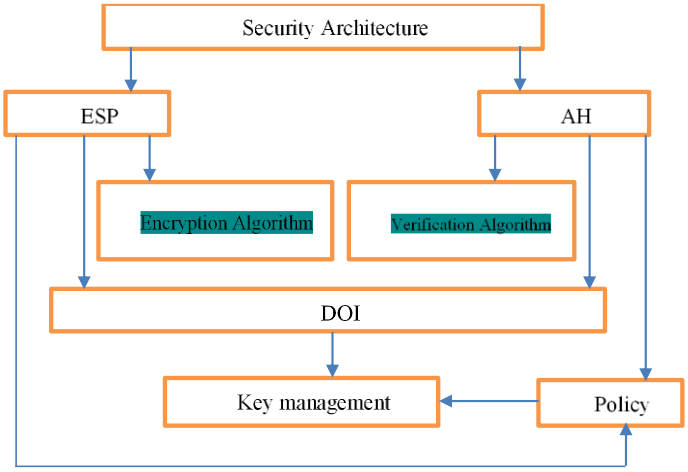

Fig. 3. IP Sec Architecture.

Table 1. The Performance of IP Sec VPN Tunnels

VPN Protocol	Authors	Remark								
		Design	***Confidentiality***	***Cost***	***Encryption***	***Integrity***	***Speed***	***Authentication***	***Security***	***Port***
IP Sec	[15]	–	The ESP protocol provides data confidentiality	–	Security Association which focuses on encryption.	AH protocol provides data integrity.	–	The ESP protocol provides authentication	–	–
	[42]	–	Encapsulating Security Payload provides a confidentiality	–	Encryption: DES, 3DES, AES	Authentication Header	–	Authentication: MD5, SHA–1	Security protocol: AH, ESP, ESP + AH	–
	[16]	–	AH, ESP backs up secrecy	–	ESP is made to encrypt the payload of an IP packet	AH and ESP procedures give connectionless reliability	–	Procedures of AH and ESP for validation	Made for the safety of IP communication on an endwise basis	–
	[41]	–	confidentiality of data	–	provides encryption of info	Gives data integrity	–	provides validation	uses symmetric encryption algorithms for	–

									providing security of data.	
	[26]	designed to provide a mix of security services	IP Sec provides the Data Confidentiality		IP security feature that provides encryption of IP packets	(ESP) seeks to provide integrity		IP security feature that provides robust authentication of IP packets	IPSec provides network security services	its use to TCP and UDP.
	[43]	More complex	confidentiality of data cannot be maintained	high cost	Strong and consistent	used for connectionless integrity	Greater processing speed is required.	authenticate the sender of data	more secure; this makes it an international standard.	Open UDP 500 and 4500
	[21]	–	ESP protocol offers confidentiality.	–	The tunnel mode encrypts both the payload and the header.	AH protocol offers integrity	–	AH protocol provides data origin authentication	Have Tunnel mode which is the more secure	–
	[39]	–	ESP is the second core security protocol which provides confidentiality	–	ESP also provides all encryption services.	The IP Authentication Header (AH) is used to provide Connectionless integrity	–	authentication is provided by Transport mode	–	–
	[13]	–	–	–	encryption of data	data integrity	–	provides authentication of users	–	–
	[20]	–	–	–	–	AH protocol, data integrity is maintained	–	AH protocol, origin authentication is maintained	A more secure and reliable VPN tunneling protocol	–
	[3]	complex tunneling	–	–	High level of encryption for sensitive information.	–	Fast, flexibly scalable and reliable	Best authentication policy for users.	High-security level implement in the network layer	–
	[31]	–	IP Encapsulating Security Payload (ESP) which	–	–	IP authentication header	–	IP authentication header	Complete build-in security mechanisms	–

			provides data confidentiality			(AH) protocol which is used to provide data integrity		(AH) protocol which is used to provide data origin authentication		
	[17]	–	supports network-level peer data confidentiality	–	VPN encryption 256 bit	supports network-level peer data integrity	Require more CPU processing to encapsulate data twice.	supports network-level peer data origin authentication	The highest encryption checks data and encapsulates the data twice.	UPD port 500
	[10]	–	IPsec tunneling technology enhancing confidentiality	–	encrypting the original packets after wrapping IP packets	–	–	–	IPsec tunneling has a big important role in enhancing VPNs' security.	–

Control the quality and characteristics of each protocol; it was taken from a set of approved researchers.

Generic Routing Encapsulation (GRE): The GRE was typically made as an enclosing procedure enfolding an advanced level of practice. Chiefly this tunnel is put into use by conveying IP packets or non-IP packets from end to end of community IP networks. This tunnel correspondingly is put into action for the encapsulation of any OSI layer three procedures. The first data packets are merely enclosed inside GRE header that shields from numerous Internet outbreaks [11, 27, 47]. The following Fig. 4 shows the GRE encapsulation packet format.

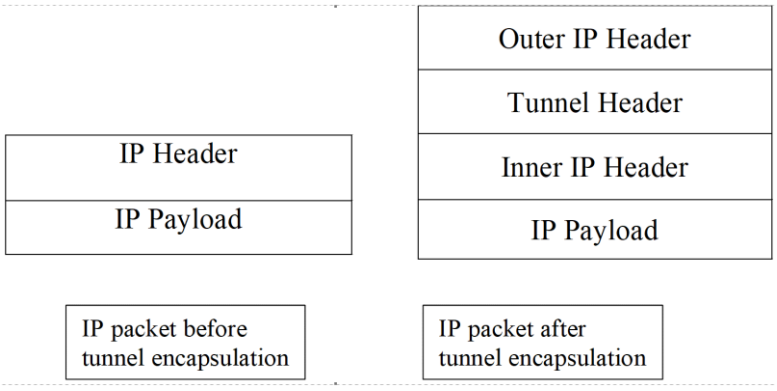

Fig. 4. GRE Packet Format

GRE generates an end to end remote connection that generates a trustworthy and safe communication path. Then again, the communication way is not safe like IP Sec due to the fact that GRE does not offer heavy-duty security structures like encryption, validity, and sequencing. It is very plain but also a prevailing tunneling technique [20, 26]. See Fig. 5 shows the general architecture of GRE.

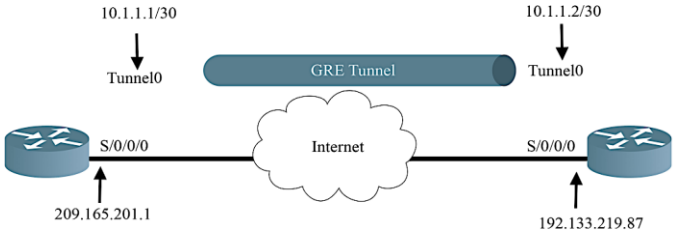

Fig. 5. GRE VPN Tunnel

The GRE tunnel can be taken to implement a quick, dependable, and more laid-back communication within the open network. In the transmitter part of the tunnel, the data packet is acknowledged by the GREs final stage in the routers, and then the packet is later enclosed with the GRE header plus the target location of the tunnel. In the receiver area of the tunnel, receiving an encapsulated packet with receiver end routers decapsulate that packet and, lastly, is brought to the wanted target [20, 33, 48]. For more detail, Table 2 describes the performance of GRE VPN tunnels.

Table 2. The performance of GRE VPN tunnels

VPN Protocol	**Authors**	**Remark**								
		Design	***Confidentiality***	***Cost***	***Encryption***	***Integrity***	***Speed***	***Authentication***	***Security***	***Port***
GRE	[41]		–	–	PPTP uses Generic Routing Encapsulation (GRE) for compressing	–	–	–	–	–
	[20]	GRE is very simple but powerful tunneling technique.	–	–	GRE does not deliver high secure features like encryption,	–	The GRE tunnel fast for performance	GRE doesn't provide high safety of validation	The communication path is not secure like IPSec	–

	[42]	–	–	–	Weak encrypting	–	–	Doesn't provide any Authentication	It secures communication over an untreated network.	–
	[9]	–	–	–	–	–	–	–	(IPsec) in conjunction with GRE tunnel it is possible to secure the data travelling through it	–
	[45]	Simple	The lack of the confidentiality	–	–	The lack of the integrity		GRE deploys an authentication weak mechanism	same limitations as the IP protocol in terms of security	–
	[11]	–	–	–	–	–	–	–	–	UDP port 1701
	[29]	–	–	Low cost	–	–	–	Authentication	Secure	–

Table 2 describes the general performance of the GRE protocol depending on some properties like which port is used, cost of it, in addition to other characteristics described above in Table 2.

Wire Guard: Wire Guard is a first-hand open-source VPN procedure that targets to offer a quicker, easier, and more secure online practice for Internet users. The procedure is appealed to suggest a better performance than OpenVPN, and to be commonly more valuable and better designed than IP Sec [18, 46].

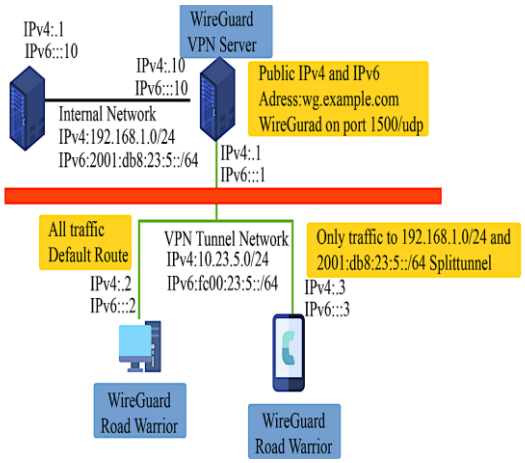

Fig. 6. Wire guard VPN Tunnel.

Wire Guard was created by Jason Donenfeld, the man who opened Edge Security. In spite of how "young" the Wire Guard procedure is (it formally arose in 2018, but was in growth earlier to that date), it has been rapidly acknowledged by online users and even coped to clasp the courtesy of main Linux developer Linus Torvalds who called it a "work of art" [18, 22,50] see Fig. 6 above that describe the Wire Guard.

The Wire Guard Virtual Private Network Protocol: The Wire Guard VPN licenses two parties to make a safe portal by establishing a Diffie-Hellman based key altercation procedure. It functions on layer 3 and has procedures on UDP as a transport layer. Wire Guard hires a new "crypto key routing" method to construct ways to endpoints, and give new ID hiding and DDoS resistance structures, that is later established on a cookie reply system. The handshake is part of the long-term and an ephemeral elliptic curve key [19, 47].

Sanctuary can be reinforced by another way, which is a pre-shared symmetric key. If the handshake does not work like it should of, then the procedure needs to be done again, as UDP does not allow the finding of package loss. After the handshake, the procedure in succession over the secure Wire Guard channel, for example, TCP, can execute all its internal package loss detection techniques. Wire Guard alone cannot notice package forfeiture but only services a sliding window method to reorganize packages [48]. A new handshake is implemented every two minutes or after a number of sent packages redefined in the description, to avoid the possibility of collision attacks on the stream cipher [18, 23, 51].

The Noise Protocol Framework (IKpsk2): Wire Guard has obtained a procedure taken from the Noise Protocol Framework as the main framework for its exchange protocol. The Noise Protocol Framework regulates many kinds of cryptographic two-party key change protocols based on Diffie-Hellman key exchange [50]; skeptical of the exchange that was taken upon. It is stated as a brief language to explain protocols, due to symbols for instance 'e' which means ephemeral, 's' has the meaning of the static long-term key, PSK stands for pre shared key, and a double letter mixture of 'e' and 's' represent Diffie-Hellman work amongst the two combinations: ee, es, se, ss, where the

letter that is prior to the others indicate the participating key from the initiator, and the other letter stands for the participating key for the responder [19, 52, 53].

One rule indicates, IKpsk2 can be separated into the two kinds IK and psk2. Both letters IK mean that the initiator directly sends its static key to the responder in the first protocol message (I for immediately), and the initiator, of course, understands the responder's static key prior (K for known) [54, 55]. The number 2 in the last part of psk2 means the pre-shared key is in use at the final part of the second protocol message. The parameters (s, rs) define the value that is needed to implement an execution protocol. In this situation, it is both static keys, s for one of the initiators, and rs the remote static key, from the responder [19, 23].

Protocol Messages and Key Derivation: The beginner is the party that initiates a procedure by transferring the primary procedure message to an additional party, which is known as the responder. These roles do not technically relate to the classic roles of client and server in a VPN situation, where the client is the customer and the server is an instrument of a VPN supplier. While the client normally is the procedure's start of a handshake, the roles could differ the moment there is a longer VPN "session." The Wire Guard protocol [24, 25, 56,57] is made up of 3 protocol messages that are a must so that joint validation amongst initiator and responder is certain. That is why it is well-thought-out as a 1.5-RTT key exchange protocol. The third message, which is directed from initiator to responder, is a transport data message and can be made of real data [56-58,60,61]. The legitimate encryption in this third message licenses the responder to substantiate the initiator. After these three messages, transport data messages can be swapped in any direction amongst the parties [25, 48, 59].

Table 3 below shows the evaluations depend on many factors which been tested by other researchers.

Table 3. The Performance of Wire guard VPN Tunnels

VPN Protocol	**Authors**	**Remark**								
		Design	***Confidentiality***	***Cost***	***Encryption***	***Integrity***	***Speed***	***Authentication***	***Security***	***Port***
Wireguard	[18]	Made for Linux fewer than 4,000 lines of code,	Connect AEAD keys to the initial key-exchange	Computationally low	ChaCha20Poly1305 authenticated-encryption for encapsulation IKEv2 and DTLS's cookie contrivances include encryption	–	high-speed in a wide diversity of devices	based on NoiseIK	Strong by using the state-of-the-art cryptography	Udp

					and validation					
	[19]	based on the Noise framework	AEAD keys that are used for security		AEAD encryption scheme	associations long-standing and ephemeral Diffie-Hellman values	–	1-RTT handshake is not safe in isolation	the best among VPN based protocol	Udp
	[25]	Originated from the Noise Protocol Framework. By putting into use of the CryptoVerif proof assistant.	message is under safety Additionally, the traffic keys for this tunnel is secure.	Unclosed Virtual Private Network (VPN)	cookie encryption has an extended AEAD structure by putting the following in use: XChaCha20Poly1305,	–	Fast compare to other protocol	mutual authentication	The use of Noise classic key exchange security for IKpsk2IKpsk2 show strong resistance vs DoS attack	Udp port 500

From Table 1-3, Table 4 will Summarize the remark of all protocols against each other.

Table 4. Summarized the performance of IPSec, GRE and Wire Guard VPN tunnels.

VPN Protocols	**IP Sec [3, 10, 13, 15–17, 20, 21, 26, 31, 39, 41–43]**	**GRE [9, 11, 20, 29, 41, 42, 62]**	**Wire guard [18, 19, 25]**
Design	Complex	Simple	focuses on simplicity and usability
Confidentiality	Yes, ESP protocol offers confidentiality	No	Yes
Cost	High cost	Low cost	Low cost
Encryption	Yes encryption: transport mode and tunnel mode used	weak encrypting	Yes, ChaCha20 for symmetric encryption
Integrity	Yes, AH and ESP protocol offers integrity	Yes	Yes
Speed	Greater processing speed is required	Fast	high-speed in a wide diversity of devices
Authentication	Yes, AH and ESP protocol offers authentication	Doesn't provide any authentication	Yes, Poly1305 for Authentication
Security	Good	Less secure than IP Sec	More Secure than IP-Sec
Port	UDP port 500 and TCP	GRE protocol 45	Uses the UDP transmission protocol port 51820

Table 4 shows the final result of the characteristics and properties of the Wire Guard IPsec and GRE protocols' that have been got it from Table 1 to Table 3.

5 The VPN Tunneling Solutions

The necessary core base of safety and its purposes are the encryption and validation of the data traffic, security procedures of consultations amongst communication associates [45], well-defined security assets, and reliable transmission routes of VPN should not be altered with external third parties. The most security assaults of the VPN are man-in-the-middle assaults, DoS assaults, and VPN takeovers [63, 64,65]. The security extortions and exposures occur because it is failing to provide the authentication of valid users, provide weak authentication with the client-side association of the compromised system, deficiency of synchronization between two connecting systems of different retailers, contamination of client-side with virus and malware, etc. [67]. The mentioned weaknesses are reasons that should be controlled to attain the main security goals of the VPN technique [66, 20, 69,70]. In Tables 5–7, the advantage and disadvantages of VPN tunnels such as IP Sec, GRE, and Wire guard are described.

Table 5. Advantages and Disadvantages of IPSec

VPN Protocols	References & Authors	Advantages	References & Authors	Disadvantages
IP Sec	[16, 21, 26]	A great level of implementation in the network layer.	[20]	Issues with compatibility because of diverse standards
	[13, 29]	Screens incoming and outgoing traffic.	[15, 26, 36]	Encryption, decryption, and complex tunneling process
	[26, 31]	Easy maintenance.	[13, 15]	The security algorithm is at risk, usage by IP Sec are split
	–	–	[36]	Greater processing speed is required

Table 6. Advantages and Disadvantages of GRE.

VPN Protocols	References & Authors	Advantages	References & Authors	Disadvantages
GRE	[9, 20]	GRE is an effortless but powerful tunneling technique.	[20, 34]	Due to the fact that GRE-tunnel doesn't have a description, it makes it dangerous to important information sent over by the network.
	[28]	It compresses different types of procedure, like packets inside the IP tunnel.	[35, 36]	It gives virtual connections and static-IP addresses by not even hiding information or data via a network.
	[35, 39]	It is made to configure a separate tunnel for each link.	[39]	The lack of confidentiality.

Table 7. Advantages and Disadvantages of Wire guard.

VPN Protocols	References & Authors	Advantages	References & Authors	Disadvantages
Wire Guard	[18]	Wire Guard uses high-end cryptography to give a much safer online connection.	[24, 25]	Security problems with Wire Guard occur because the way it is automated would make VPN providers log user data.
	[18, 25]	The Wire Guard VPN procedure shows a less heavy code base than OpenVPN and IP Sec, which helps by making it easier to check when finding vulnerabilities.	[18, 24]	Currently, Wire Guard is only effective on UDP). That means it can possibly be blocked by a network admin. Wire Guard is better with Linux distributions.
	[18, 19]	The Wire Guard procedure shows performance enhancements that can decrease battery use and give better roaming maintenance on mobile devices.	[18, 22]	Wire Guard is newer which means not many tests were done
	[19]	A decrease in the amount of code, much safer, better performance, and it is easy to use.	–	–
	[18]	Wire Guard is created to offer high speeds, and recent benchmarks demonstrate that it is quicker than IP Sec and OpenVPN.	–	–

Table 5–7 shows the advantage and disadvantages of the three VPN protocols at the network layer (Wire guard, GRE, IPsec).

6 Discussion of Experimental Results

What was provided in this paper, a review of the most recent and relevant selective researches done on VPN protocols such as IPsec, GRE, Wire guard. It also elaborates on the objective, problems, advantages, and disadvantages in order to select appropriate protocol. To successfully handle the given situation, the decisions made are quite crucial. However, this paper states that there are plenty of open roads to different chances for additional enhancement, as discussed below. On the whole, we perceive that many academics put vast and very effective trials in IPsec, and a major part of organizations have put it into good use due to its security. However, a comparison results on a Wire guard protocol and GRE approaches have also proved to show good prediction as well as performance, with only some limitations of GRE. Thus, the development or advancement of Wire guard tactics that can be considered to be leading a bright future in VPN at network layer 3, according to recent studies. The comparison of Wire guard VPN protocol with two well-known and state of the art protocol IPsec, GRE, the study illustrates the terms, remarks, strength, and reliability of each protocol. As shown in Table 1-5, the study concludes that Wire guard is the simplest protocol in terms of design when compared with IPsec and GRE, but it still works well on Linux. The Wireguard, according to all the research, indicates that it is low cost in comparison with IPsec,

which was and still is one of the most common protocols in a VPN. On the other hand, GRE is also low cost; however, not as secure nor confidential than the other VPN protocols; as a result, it is not preferred to be used by organizations. The tables above show strength point in the encryption scheme, and the integrity was studied in three protocols; both Wire guard and IPsec offer completeness and dedicated usage of protocols that ensure data integrity opposite to GRE, which does not provide good integrity protocol. The speed analysis display again the Wire guard has a reusable high speed in a wide diversity of device; likewise, some researchers suggest the speed of the protocol to the number of lines of code that do not exceed more than 4000 lines, which facilitates the installation process and its speed compared to IP Sec, which has a number of code lines that are close to 70,000 lines.

Furthermore, in term of authentication, the IP Sec shows a stronger authentication than GRE, and Wire guard due to the using AH and ESP, while Wire guard uses handshake.

Finally, the Wire guard and IPsec were competitive in terms of all remarks, but overall, the Wire guard is better than others protocol, but it has its weakness; unfortunately, it is very new and has not been tested thoroughly.

7 Conclusion

Because of that, VPN offers an organization by the same power as remote contracted lines at a much cheaper cost by means of the joint infrastructure, so VPN protocol depended widely. This paper provided a detailed explanation of three main VPN protocols at the network layer in terms of Design, Confidentiality, Cost, Encryption, Integrity, Speed, Authentication, Security, and Port. These metrics are taken from a set of approved researchers. So, dependent metrics are controlling the quality and characteristics of each protocol. Performance of IP Sec, GRE, and Wire guard VPN tunnels have been focused.

It can be concluded that IP Sec provides good encryption, authentication, and security. On the other side, this protocol has Issued compatibility, encryption, decryption, and complex tunneling process, risk-security, and needs more processing speed. While, GRE VPN provides simple-design, low-cost, good-integrity, and fast-speed. However, the GRE protocol suffers from dangerous to important information sent over by the network, giving virtual connections and static-IP addresses without hiding information or data via network and confidentiality lack. Finally, the Wire guard VPN tunnel provides simple and usable design, acceptable confidentiality, low-cost, encryption-support, well-integrity, and high-speed. In addition, it suffers from security problems by making VPN providers log user data, and it is only effective on UDP, which means it can possibly be blocked by a network admin, it is a newer protocol, which means not many tests were done.

8 References

[1] F. A. Salman, "Implementation of IPsec-VPN tunneling using GNS3," Indonesian Journal of Electrical Engineering and Computer Science, Journal vol. 7, no. 3, pp. 855-865, 2017. https://doi.org/10.11591/ijeecs.v7.i3.pp855-860

[2] R. Bibraj, Chug, S., Nath, S. A. N. K. A. R., & Singh, S. L, "Technical study of remote access VPN and its advantages over site to site VPN to analyze the possibility of hybrid setups at radar stations with evolving mobile communication technology," MAUSAM, vol. 69, no. 1, pp. 97-102, 2018.

[3] K. Rao, Rao, N., Sitharam, M., Vardhan, K. A., & Routhu, P. K., "A Study on Performance Analysis of IPSec VPN and MPLS VPN," International Journal of Futuristic Science and Technology, vol. 1, no. 3, pp. 184-190, 2013.

[4] J. a. G. Hopkins, M., " OpenVPN 2.4 Evaluation Summary and Report," 2019.

[5] M. T. Khan, DeBlasio, J., Voelker, G.M., Snoeren, A.C., Kanich, C., & Vallina-Rodriguez, N., "An Empirical Analysis of the Commercial VPN Ecosystem," IMC, 2018. https://doi.org/10.1145/3278532.3278570

[6] I. Coonjah, Catherine, P. C., & Soyjaudah, K. M. S., "Performance evaluation and analysis of layer 3 tunneling between OpenSSH and OpenVPN in a wide area network environment," In 2015 International Conference on Computing, Communication and Security (ICCCS), pp. 1-4, 2015. https://doi.org/10.1109/cccs.2015.7374130

[7] B. A. Ahmed, Saleem, Y., & Waseem, S., "An Implementation of Multiprotocol Label Switching Virtual Private Networks and Internet Protocol Security using Graphical Network Simulator 3 as an Educational Tool," Science International, vol. 27, no. 3, 2015.

[8] Zeebaree, D. Q., Haron, H., & Abdulazeez, A. M. (2018, October). Gene selection and classification of microarray data using convolutional neural network. In 2018 International Conference on Advanced Science and Engineering (ICOASE) (pp. 145-150). IEEE. https://doi.org/10.1109/icoase.2018.8548836

[9] R.Zebari, A.M. Abdulazeez, D. Zeebaree, D. Zebari, J. Saeed," A Comprehensive Review of Dimensionality Reduction Techniques for Feature Selection and Feature Extraction, 2020, Journal of Applied Science and Technology Trends, volume 1,issue 2, PP 56-70. https://doi.org/10.38094/jastt1224

[10] L. Ibrahim, "Virtual Private Network (VPN) Management and IPSec Tunneling Technology," Middle East, vol. 1, 2017.

[11] P. Venkateswari, & Purusothaman, D. T., "Comparative Study of Protocols Used for Establishing VPN," International Journal of Engineering Science and Technology, vol. 3, no. 160-165, 2009.

[12] N. H. Tran, C.-V. Phung, B. Q. Nguyen, and L. Bahri, "An Effective Privacy-Preserving Data Coding in Peer-To-Peer Network," arXiv preprint arXiv:1806.05430, 2018. https://doi.org/10.5121/ijcnc.2018.10305

[13] A. K. Singh, Samaddar, S. G., & Misra, A. K., "Enhancing VPN security through security policy management," In 2012 1st International Conference on Recent Advances in Information Technology (RAIT), pp. 137-142, 2012. https://doi.org/10.1109/rait.2012.6194494

[14] M. Aljumaily, L. Xiao, and D. Xu, "Enhancing Availability for Distributed Replicated Services Considering Network Edge Availability," International Journal of Computer Networks & Communications (IJCNC) Vol, vol. 11, 2019. https://doi.org/10.5121/ijcnc.2019.11101

[15] S. Padhiar, & Verma, P., "A Survey on Performance Evaluation of VPN," International Journal of Engineering Development and Research, vol. 3, no. 4, pp. 516-519, 2015.

[16] A. De Rubertis, Mainetti, L., Mighali, V., Patrono, L., Sergi, I., Stefanizzi, M. L., & Pascali, S., "Performance evaluation of end-to-end security protocols in an internet of things," In 2013 21st International Conference on Software, Telecommunications and Computer Networks-(SoftCOM 2013), pp. 1-6, 2013. https://doi.org/10.1109/softcom.2013.6671893

[17] A. J. Patel, & Gandhi, A., "A survey on performance evaluation of VPN," International Journal of Advance Engineering and Research Development, vol. 4, no. 3, pp. 516-520, 2017.
[18] J. A. Donenfeld, "Wire Guard: Next Generation Kernel Network Tunnel," In NDSS, 2017. https://doi.org/10.14722/ndss.2017.23160
[19] B. Dowling, & Paterson, K. G., "A cryptographic analysis of the Wire Guard protocol," In International Conference on Applied Cryptography and Network Security pp. 3-21, 2018. https://doi.org/10.1007/978-3-319-93387-0_1
[20] S. Jahan, Rahman, M. S., & Saha, S., "Application specific tunneling protocol selection for Virtual Private Networks," In 2017 International Conference on Networking, Systems and Security (NSysS), pp. 39-44, 2017. https://doi.org/10.1109/nsyss.2017.7885799
[21] S. Narayan, Williams, C. J., Hart, D. K., & Qualtrough, M. W., "Network performance comparison of VPN protocols on wired and wireless networks," International Conference on Computer Communication and Informatics (ICCCI), 2015. https://doi.org/10.1109/iccci.2015.7218077
[22] J. A. Donenfeld, & Milner, K., "Formal verification of the wire guard protocol," 2017.
[23] B. Lipp, "Master thesis, A Mechanized Computational Analysis of the Wire Guard Virtual Private Network Protocol", Department of Informatics Karlsruhe, Institute of Theoretical Informatics (ITI), Competence Center for Applied Security Technology (KASTEL), Institute of Technology, and prepared at Prosecco Research Team INRIA Paris, 2018.
[24] P. Wu., "Master's Thesis: Analysis of the Wire Guard protocol," Department of Mathematics and Computer Science, Eindhoven University of Technology 2019.
[25] B. Lipp, Blanchet, B., & Bhargavan, K., "A mechanised cryptographic proof of the WireGuard virtual private network protocol," In 2019 IEEE European Symposium on Security and Privacy (EuroS&P), pp. 231-246, June 2019. https://doi.org/10.1109/eurosp.2019.00026
[26] Y. Raiwani, "IPSec Protocol in VPN," International Journal of Engineering Research & Technology (IJERT), vol. 3, no. 1, January 2014.
[27] D. B. I. R. K. Karuna Jyothi "Study on Virtual Private Network (VPN), VPN's Protocols and Security," International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 3, no. 5, pp. 2456-3307, 2018.
[28] A. e. E. Bahnasse, Najib, "Study and evaluation of the high availability of a Dynamic Multipoint Virtual Private Network," Revue MéDiterranéEnne Des TéLéCommunications, vol. 5, no. 2, 2015.
[29] A. Amankatiyar, Aditya soni, Hemantjain, JayeshSurana, "Research on Tunneling Techniques in Virtual Private Networks," IJEDR, vol. 5, no. 2, pp. 2321-9939, 2017.
[30] D. S. a. K. G. R. Kajal, "Virutal Private Network," International Journal of Advanced Research in Computer Science & Sofware Engineering, vol. 2, no. 10, pp. 428-432, 2012.
[31] F. e. Z. Yang, Lizhen, "IPSec-VPN Availability Research and Simulation," International Conference on Computational Science and Engineering (ICCSE), pp. 290-295, 2015.
[32] C. M. Nawej, & Du, S., "Virtual Private Network's Impact on Network Performance," In 2018 International Conference on Intelligent and Innovative Computing Applications, pp. 1-6, December 2018. https://doi.org/10.1109/iconic.2018.8601281
[33] E. R. K. G. Umar Bashir Sofi, "Comparative Analysis of MPLS Layer 3vpn and MPLS Layer 2 VPN," International Journal of Computer Science Trends and Technology (IJCST), vol. 3, no. 3, 2015.
[34] The New Cloudflare VPN: What It Is and Is Not. Available: https://openvpn.net/what-is-cloudflare-vpn/
[35] G. A. Tizazu, Kim, K. H., & Berhe, A. B., "Dynamic routing influence on secure enterprise network based on DMVPN," In 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN), pp. 756-759, July 2017. https://doi.org/10.1109/icufn.2017.7993894

[36] Zeebaree, D. Q., Haron, H., Abdulazeez, A. M., & Zebari, D. A. (2019, April). Machine learning and Region Growing for Breast Cancer Segmentation. In 2019 International Conference on Advanced Science and Engineering (ICOASE) (pp. 88-93). https://doi.org/10.1109/icoase.2019.8723832
[37] Trainable Model Based on New Uniform LBP Feature to Identify the Risk of the Breast Cancer. In 2019 International Conference on Advanced Science and Engineering (ICOASE) (pp. 106-111). IEEE. https://doi.org/10.1109/icoase.2019.8723827
[38] Zeebaree, D. Q., Abdulazeez, A. M., Hassan, O. M. S., Zebari, D. A., & Saeed, J. N. (2020). Hiding Image by Using Contourlet Transform, vol,83, May - June 2020, PP. 16979 - 16990.
[39] H. Alshamrani, "Internet Protocol Security (IPSec) Mechanisms," International Journal of Scientific & Engineering Research, vol. 5, no. 5, pp. 2229-5518 2014.
[40] J. Scarpati. (2014). IPsec vs SSL VPNs Understanding the Basics. Available: http://searchnetworking.techtarget.com/feature/IPsec-vs-SSLVPNs-Understanding-the-basics
[41] F. Al-Salti, N. Alzeidi, K. Day, B. Arafeh, and A. Touzene, "Grid-based priority routing protocol for uwsns," International Journal of Computer Networks and Communications, vol. 9, no. 6, pp. 1-20, 2017. https://doi.org/10.5121/ijcnc.2017.9601
[42] R. Y. Tripti Sharma, "Security in Virtual private network," IJIACS, vol. 4, 2015.
[43] Y. Nir, & Langley, A., "ChaCha20 and Poly1305 for IETF Protocols," 2015. https://doi.org/10.17487/rfc7539
[44] J. Gokulakrishnan, & Bai, V. T., "A Survey Report on VPN Security & ITS Technologies," Indian Journal of Computer Science and Engineering (IJCSE), vol. 5, no. 4, pp. 3-5, 2014.
[45] A. A. Paul, & Zhang, C., "Tunnel comparison between Generic Routing Encapsulation (GRE) and IP Security (IP Sec)," In School of Information Science, Computer and Electrical Engineering 2012.
[46] A. Shrivastava, & Rizvi, M., "Analysis and Comparison of major mechanisms implementing Virtual Private Networks," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), vol. 3, no. 7, pp. 2374-2381, 2014.
[47] T. Tamanna, & Fatema, T., "MPLS VPN over mGRE design and implementation for a service provider's network using GNS3 simulator," In 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), pp. 2339-2342, March 2017. https://doi.org/10.1109/wispnet.2017.8300178
[48] A. e. E. K. BAHNASSE, Najib, "Security of Dynamic and Multipoint Virtual Private Network," International Journal of Computer Science and Information Security, vol. 14, no. 7, p. 100, 2016.
[49] J. A. Donenfeld. (2019). Wire Guard Linux kernel source. Available: https://git.zx2c4.com/Wire Guard
[50] J. Salter. (2018). Wire Guard VPN review: A new type of VPN offers serious advantages. Available:https://www.reddit.com/r/selfhosted/comments/9apvy5/wireguard_vpn_review_a_new_type_of_vpn_offers/. https://doi.org/10.1016/s1353-4858(00)03014-2
[51] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3," 2018.
[52] K. Bhargavan, Blanchet, B., & Kobeissi, N., "Verified models and reference implementations for the TLS 1.3 standard candidate," In 2017 IEEE Symposium on Security and Privacy (SP), pp. 483-502, May 2017. https://doi.org/10.1109/sp.2017.26
[53] T. Perrin. (2018). The Noise protocol framework. Available: https://noiseprotocol.org/noise.html
[54] G. Girol, "Formalizing and verifying the security protocols from the Noise framework ", ETH Zurich 2019.
[55] P. Wu, "Analysis of the Wire Guard protocol," Department of Mathematics and Computer Science, Dindhoven University of Technology, 2019.
[56] N. Kobeissi, Nicolas, G., & Bhargavan, K., "Noise Explorer: Fully automated modeling and verification for arbitrary Noise protocols," IEEE European Symposium on Security and Privacy (EuroS&P), pp. 356-370, 2019. https://doi.org/10.1109/eurosp.2019.00034

[57] J. Appelbaum, Martindale, C., & Wu, P., "Tiny Wire Guard Tweak," In International Conference on Cryptology in Africa, vol. 11627, pp. 3-20, 2019.
[58] M. Bellare, & Namprempre, C., "Authenticated encryption: Relations among notions and analysis of the generic composition paradigm," In International Conference on the Theory and Application of Cryptology and Information Security, pp. 531-545, December 2000. https://doi.org/10.1007/3-540-44448-3_41
[59] B. Beurdouche, Bhargavan, K., Delignat-Lavaud, A., Fournet, C., Kohlweiss, M., Pironti, A., & Zinzindohoue, J. K., "A messy state of the union: Taming the composite state machines of TLS," In 2015 IEEE Symposium on Security and Privacy, pp. 535-552, May 2015. https://doi.org/10.1109/sp.2015.39
[60] H Sadeeq, A M. Abdulazeez," Hardware implementation of firefly optimization algorithm using FPGAs", 2018, international Conference on Advanced Science and Engineering (ICOASE), IEEE., pp 30-35. https://doi.org/10.1109/icoase.2018.8548822
[61] M.R. Mahmood, A.M.Abdulazeez," Different Model for Hand Gesture Recognition with a Novel Line Feature Extraction", 2019, International Conference on Advanced Science and Engineering (ICOASE), IEEE,pp, 52-57. https://doi.org/10.1109/icoase.2019.8723731
[62] J. K. Zinzindohoué, Bhargavan, K., Protzenko, J., & Beurdouche, B., "HACL*: A verified modern cryptographic library," In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp. 1789-1806, October 2017. https://doi.org/10.1145/3133956.3134043
[63] N. Kobeissi, Bhargavan, K., & Blanchet, B., "Automated verification for secure messaging protocols and their implementations: A symbolic and computational approach," In 2017 IEEE European Symposium on Security and Privacy (EuroS&P) pp. 435-450, April 2017. https://doi.org/10.1109/eurosp.2017.38
[64] R. Schwarz. (January 2019). Adds Emerging Wire Guard VPN Protocol to its Deep Packet Inspection (DPI) Software Library, R&S® PACE 2. Available: https://www.businesswire.com/news/home/20190123005355/en/Rohde-Schwarz-Adds-Emerging-WireGuard-VPN-Protocol.
[65] K. B. a. G. Leurent, "On the practical (in-)security of 64-bit block ciphers: Collision attacks on HTTP over TLS and OpenVPN," In ACM CCS, vol. 3, no. 4, pp. 456–467, 2016. https://doi.org/10.1145/2976749.2978423
[66] T. Malinowski, & Chudzikiewicz, J., "On Improving Communication System Performance in Some Virtual Private Networks," In International Conference on Computer Networks, pp. 64-73, June 2018. https://doi.org/10.1007/978-3-319-92459-5_6
[67] A. Luykx, Mennink, B., & Neves, S., "Security analysis of BLAKE2's modes of operation," IACR Transactions on Symmetric Cryptology, pp. 158-176 2016.
[68] Alsaleem, N. Y. A., Kashmoola, M. A., & Moskalets, M. (2018). Analysis of the efficiency of spacetime access in the mobile communication systems based on an antenna array. Eastern-European Journal of Enterprise Technologies, 6(9–96), 38–47. https://doi.org/10.15587/1729-4061.2018.150921
[69] Kashmoola, M. A., Alsaleem, M. Y. anad, Alsaleem, N. Y. A., & Moskalets, M. (2019). Model of dynamics of the grouping states of radio electronic means in the problems of ensuring electromagnetic compatibility. Eastern-European Journal of Enterprise Technologies, 6(9–102), 12–20. https://doi.org/10.15587/1729-4061.2019.188976
[70] Alsaleem, N. Y. A., Moskalets, M., & Teplitskaya, S. (2016). The analysis of methods for determining direction of arrival of signals in problems of space-time access. Eastern-European Journal of Enterprise Technologies, 4(9–82), 36–44. https://doi.org/10.15587/1729-4061.2016.75716

9 Authors

Adnan Mohsin Abdulazeez President of Duhok Polytechnic University, Professor of Computer Engineering and Science. Dr. Abdulazeez holds Ph.D. in Computer Engineering, M.Sc. in Computer and Control Engineering, and his B.Sc. in Electrical and Electronic Engineering. He held the position of Dean of Duhok Technical Institute for several years. Before that, he was assigned as a head of several scientific departments and committees in various public and private universities in Kurdistan Region and Iraq. He has been awarded the title of Professor since 2013.He is keen to carry out his administrative and academic responsibilities simultaneously, and therefore he supervised and still supervises a large number of master and doctoral students. In addition, he focuses his attention on publishing scientific researches in valuable international scientific journals, so he has published many researches in these journals. His research interest areas include intelligence system, soft computing, multimedia, network security and coding and FPGA implementation. Also, Dr. Abdulazeez is a reviewer for several accredited international journals. He has created and led various research groups, as well as urged and encouraged them to publish research in different international journals.

Baraa Wasfi Salim PhD student in Duhok Polytechnic University. Holds M.Sc. in computer Science, Network Security, Zakho University, Iraq, 2011, B.Sc. in computer science, Mosul University, Lecturer in Nawroz University, College of Engineering, Communication & Computer Department. She has Published a number of papers on Networks, Security and Image Processing.

Diyar Qader Zeebaree was born in Akre city, Duhok, Kurdistan, Iraq in 1985. He received the B.S. degree in Computer Science from the University of Nawroz, in 2012 and the M.S. degree in Computer Information Systems (CIS) from the Near East University, North of Cyprus, Turkey, in 2014, and Ph.D. degree in Computer Science from University Technology Malaysia (UTM) in 2020.

Currently, he is working in Duhok Polytechnic University (DPU) as director of the research center. He is the author of one book, more than 20 articles. His research interests in artificial neural network, machine learning, deep learning, medical image analysis and image processing.

Dr. Diyar was a recipient of the IEEE-International Conference on Advanced Science and Engineering (ICOASE), Best Symposium Paper Award in 2019.

Dana Farhad Doghramachi PhD student in Duhok Polytechnic University. Holds M.Sc. In Computer Engineering, Image Compression, Near East University, Cyprus – Lefkosa ,2012, B.Sc. in Software Engineering, Salahuddin University, Asst. Lecturer in Erbil Polytechnic University, Erbil Technical Engineering college, Information System Engineering Department. He has published a number of articles and researches most of them focused on security.

Article submitted 2020-06-23. Resubmitted 2020-08-05. Final acceptance 2020-08-05. Final version published as submitted by the authors.