A Survey on Dynamic Multipoint Virtual Private Networks

Roumaissa Khelf [(1)], Nacira Ghoualmi-Zine [(2)]

[(1),(2)]Network and System Laboratory- LRS
Computer Science department
Badji Mokhtar-Annaba University

[(1)]khelfroumaissa@yahoo.com, [(2)]ghoualmi@yahoo.com

Abstract

A dynamic multipoint virtual private network (DMVPN) is a secure network that exchanges data between sites without needing to pass traffic through an organization's headquarter. It is in every company's advantage to make use of DMVPN where possible, to help reduce WAN costs and increase bandwidth and reliability. Therefore, many studies have been conducted to enhance the network performances, to demonstrate the optimal routing protocols and to define the suitable configuration. This article studies different works that have been made in the concept of DMVPN and demonstrate the limitations of existing solutions developed to fulfill the DMVPN issues. Furthermore a classification of these studies is presented according to their addressed issues. In addition, open questions and research challenges that could improve the capabilities and effectiveness of DMVPNs are also outlined.

1 Introduction

Virtual private network (VPN) technology allows the creation of a private path via the Internet [1]. This technology is widely used because of its cost effectiveness, availability, and high level of security. Conventional VPNs are preconfigured in a static manner with a manual configuration. Therefore, medium and large companies have tended to use Dynamic Multipoint VPNs (DMVPN) as an alternative solution to satisfy requirements arising from the expansion of enterprise networks and the high demand for mobility, dynamicity and flexibility.

DMVPN is the latest VPN solution devolved by Cisco Corporation. This client-server based solution is the best practice to ensure real time communication and higher security for enterprise businesses. Each DMVPN cloud has at least one server called "Hub" and several clients named "Spokes". Thus, the connection between the hub and its spokes must be carried out by permanent tunnels. On the other hand, the connection between two spokes is done dynamically on demand accompanied by the Hub assistance. Hence, DMVPN defines two deployment models: HUB to Spoke and Spoke to Spoke model (Fig.1). Noting that, security is ensured by using the Internet Protocol Security (IPsec) [2]. Among the DMVPN advantages, it reduces the configuration on the router, since a classic VPN requires the configuration of crypto map list and ACL for each remote spoke, which is a tedious and error-prone task [3]. In addition, it enables routers dynamic addressing using the Next Hop Routing Protocol (NHRP).

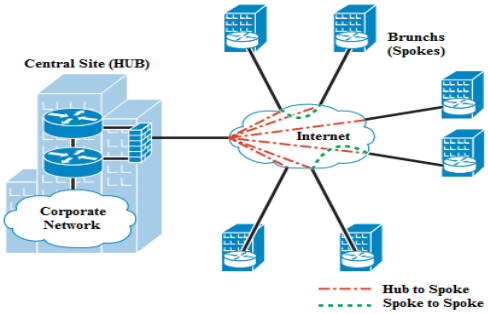

Figure 1: DMVPN Model

Various aspects of the DMVPN were discussed in the literature, such as the impact of the routing protocol choice on network performance [6-12]. In addition, research efforts are being made to address security-related issues, such as confidentiality threats on the transferred data between corporate Head Quarters (HQ) and Mobile Workers (MW) using open networks such as than the Internet [6, 11]. In addition, considerable efforts have been made to evaluate the performance of the DMVPN network [19, 20]. Some of these approaches target the scalability and availability issues [12], while other approaches aim to provide the optimal failure recovery mechanism [21].

The main motivation of this survey is to study different works that have been made in the concept of DMVPN, especially because the literature lacks this type of survey. Moreover, we aim to demonstrate the limitations of existing solutions developed to fulfill the DMVPN issues. Furthermore; we classify those studies according to their addressed issue. Hence, these solutions are analyzed and compared, in order to outline both open questions and research challenges that could improve the capabilities and effectiveness of DMVPNs

The remainder of this paper is organized as follows. Section II presents an overview of DMVPN components and phases. Section III a review of some typical studies on DMVPN is presented. Section IV classifies and compares the state of art articles. Section V gives perspectives about the open questions and the future research challenges. Finally, Section VI concludes the paper.

2 DMVPN Overview

The need for mobility and flexibility in corporate networks can be achieved through the use of dynamic routing in DMVPN. However, this solution has created a new challenge, securing data exchange. Knowing that, IPsec cannot secure or encrypt the multicast packets used in dynamic routing. DMVPN solution use a combination of several standard technologies together which are briefly explained below.

2.1 DMVPN Components

Dynamic multipoint VPN is based on the client / server model, it is a mechanism to establish IPsec/GRE (Generic Routing Encapsulation) tunnels directly between routers who want to interact with each other in a simplistic and totally dynamic way. GRE is an encapsulating protocol which can encapsulate multicast and broadcast packets in a unicast packet. Hence, it would be possible to encrypt it using IPsec. Basically, the solution is to implement multicast packets using GRE tunnels, and since GRE is not secure then IPsec is used for data encryption. Hence DMVPN components are as follow.

2.1.1 Next Hop Routing Protocol

In DMVPN two types of addresses are distinguished: Underlay and Overlay IP addresses. The underlay address is a public IP address used as the source or the destination address of the tunnel and the overlay address is a private IP address given to a GRE tunnel. Thus, the mapping between these addresses is done through the Next Hop Routing Protocol (NHRP). NHRP is based on the client-server standard [4]; the spokes (NHRP Clients) send periodic updates containing public and tunnels addresses to the hub (NHRP Server) of the network. Therefore, when spoke router comes to online, it automatically registers relational information with the hub router according to the external network public IP address of hub router and NHRP protocol.

2.1.2 Multipoint Generic Routing Encapsulation

Multipoint Generic Routing Encapsulation (mGRE) is responsible for the dynamic creation of tunnels. The use of mGRE is dependent to IPsec; since GRE tunnel can encapsulate multicast/broadcast packets into GRE packets, and GRE packets are unicast packets, so they can be encrypted by IPSec. That's the multi and broad cast packet are transferred with mGRE and encrypted with IPSec. Basically, a GRE header is added to each packet which changes either the broadcast or multicast packet into a unicast. Since GRE uses the same link as IPsec, the IPsec header is applied to encrypt all the GRE data (Fig.2). Nevertheless, it is incapable of changing the physical IP address since the IPsec needs a fixed IP address to create the IPSEC tunnel. Therefore, the GRE tunnel IP address is invariable.

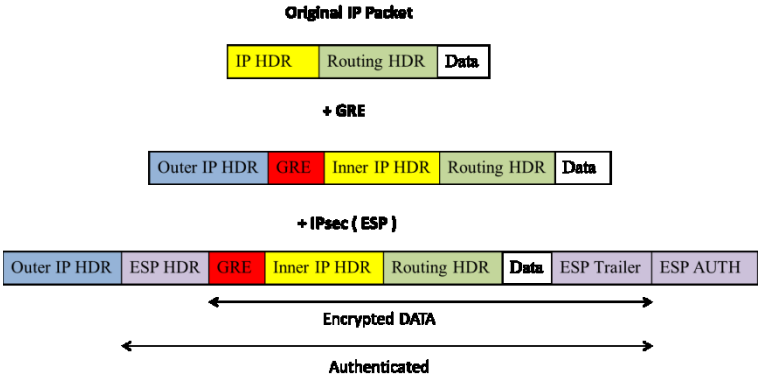

Figure 2: GRE/IPsec Encapsulation of an IP packet

2.1.3 Internet Protocol Security

The Internet protocol security (IPsec) itself is a set of protocols and mechanisms that provide the end-to-end security in term of encryption, authentication and integrity for all IP-enabled networks. IPsec is a flexible method to protect network traffic, it has relatively fewer vulnerabilities discovered and reported, and thus has become one of the most widely used VPN implementations [5]. Despite that the use of IPsec in DMVPN is optional; it has a great importance to ensure the security of communicated data since GRE tunnels are not secured at all. Conventionally, IPSec uses an access control list (ACL) to define what data are to be encrypted. That is, when a data packet matches the defining entry of an ACL, the IPSec encryption tunnel will be set up immediately. However, when using IPSec/mGRE tunnels, the mGRE tunnel configuration includes the mGRE tunnel peer address already, which is also the IPSec peer address.

2.1.4 Routing Protocol

Beside all technologies mentioned previously, a dynamic routing protocol is mandatory for DMVPN. Indeed, routing protocols present a main part of the DMVPN solution, they ensure the smooth establishment of tunnels and have a major impact on network's behavior and transported applications. Hence, several works have been conducted assessing the network performances in order to determine the most convenient routing protocol for DMVPN [6-8, 21-23]. Among the routing protocols used for DMVPN we cite:

- Enhanced Interior Gateway Routing Protocol (EIGRP): a distance-vector routing protocol which is only available on cisco routers. EIGRP is used on a router to share routes with other routers within the same autonomous system.
- Routing Information Protocol ('RIP'): a distance-vector routing protocol which employ the hop count as a routing metric. RIP implements the split horizon, route poisoning and hold-down mechanisms to prevent incorrect routing information from being propagated.
- Open Shortest Path First (OSPF): an IP based routing protocol which It uses a link state routing algorithm and falls into the group of interior gateway protocols, operating within a single autonomous system.

2.2 DMVPN Phases

When there is a data exchange between two Spokes, the first spoke contacts the Hub, in order to obtain the information required on the other end, in order to be able to create a dynamic IPsec VPN tunnel directly between them. If the spoke uses dynamic IP address, it must register with the headquarters router (Hub) while it joins the network every time. Then after

passing the confirmation step, both routers can implement direct communication between them. The communication between spokes is done according to one of the three phases of DMVPN.

2.2.1 Phase 1: Hub to Spoke

In this phase, each spoke is configured with the IP address of the hub as the network server. Hence, each spoke have a static tunnel with a fixed destination IP which represent the Hub's physical address. Consequently, spokes can only get to each other across the hub. The key advantage of DMVPN Phase 1 is the simplified Hub configuration. Additionally, the choice of routing protocol is much easier since almost any dynamic routing protocol would help with attaining reachability. The hub just needs to advertise a default route to spokes, while spokes should advertise their subnets dynamically to the hub. However, the main drawback is inability to establish spoke-to-spoke shortcut tunnels. NHRP Phase 2 resolves this issue and allows for spoke-to-spoke tunnels

2.2.2 Phase 2: Spoke to Spoke

This mode requires all the spokes to have complete routing information with the next-hop preserved. Since not all spokes may accept full load of routing updates, this requirement may limit the scalability especially in large networks. The second phase limitation occur in case of network with 1000 spokes for example, where the routing table on each spoke will have too many entries, which essentially isn't needed. Hence it becomes difficult for the routers to have such a huge routing table.

2.2.3 Phase 3: Spoke to Spoke with Scalable Infrastructure

Basically, this phase accomplishes the same things as phase 2, but it improves on some of its limitations. Phase 3 fixed this problem in the most effective way. Because all spokes see the entire network being learned from the hub. The solution is to summarize the network on the hub. Hence DMVPN phase 3 can be used for very large deployments and it is lot more scalable than DMVPN phase 2 and has a better hierarchy.

2.3 DMVPN Topologies

The simplest possible design of DMVPN allows each spoke site to have a single router and a single uplink. However, it is possible to have two hub routers (preferably with independent uplinks), which brings the following two topologies: Dual hub-single DMVPN cloud and Dual hub-dual DMVPN cloud. In both topologies, two hub routers are implemented for redundancy purposes. Thus, High availability is provided through the use of a second hub router, in a single DMVPN cloud topology, the hub may be on the same DMVPN subnet as the primary router. Knowing that, this topology is generally not recommended because it relies on mechanisms outside of the tunnel to determine the appropriate hub for failover. Otherwise, in a dual DMVPN cloud topology, the second hub router serves its own DMVPN subnet. It relies on routing protocols running inside of the tunnel to determine path selection.

3 Related works

In this section, a review of the proposed solutions is presented in a chronological order. As mentioned above, a lot of works aim to find out the best routine protocol for DMVPN such, it has a huge importance in term of performances. Namely, Jankuniene et al., [6] evaluate the performances of DMVPN spoke-to-spoke network when varying both the dynamic routing protocols (OSPF, RIP and EGIRP) and the size of intermediary's routers (the number of client side routers). According to the authors' finding, the least delay was obtained using RIP protocol. Hence, they conclude that it is purposeful to use RIP protocol when WAN cloud is not big (up to 15 transits); otherwise it is advisable to use EIGRP protocol. Thorenoor in [7] aims to find the best decision to make concerning the choice of routing protocol type, between protocols that involve distance vector or link state or the combination of both of them. The idea is to build up a network with RIP, OSPF and EIGRP as routing protocols respectively, and compare the network performances in each case. Meanwhile, VPN, network limitations were discussed in [8]. The authors stressed that GRE is highly criticized because of some packets dropped cases. Despite that the network improvement is not discussed, authors validate their theories by performing a network simulation in which they conclude that DMVPN gives more opportunities for enterprise to build up secure and economical networks.

In the network simulation area, Bahnasse et al. [9] propose a server-based architecture to automate the simulation of Dynamic Multipoint Virtual Private Networks (DMVPNs) under the OPNET Modeler simulator. They conceive a web-tool which provides the possibility to parameterize and customize the routing protocol used for the DMVPN network, the IPsec sub-protocols and GRE and NHRP tunneling protocols. However, this work is only compatible with a single simulator and do not allow the generation of a lot of scenarios based on specific factors. Additionally, the interpretation of the obtained results is a tedious and challenging task. Authors in [10] study the implementation of DMVPN and develops an algorithm for tunnel connections structure management in distributed and corporate network, in order to achieve a self-diagnosable DMVPN for the purpose of hubs 'load balancing. Authors' findings introduced a way to resolve a 'dead' IPsec session using cryptographic tunnels created by configuring the router with NHRP. However the experiment in this research seems to be supervised and manually controlled.

The issue of confidentiality was stressed by Nowosielski in [11] which can afford data transfer between corporate headquarters (HQ) and mobile workers (MW) using open networks such Internet. They proposed a DMVPN technique to improve previous versions defects. Simulation results allowed authors to conclude that DMVPN provides great flexibility and confidentiality associated with the use of IPSec tunnels. Hence, they demonstrate that DMVPN technique is the most convenient solution for large companies, where the mobility of workers and security play a major role. Authors in [12] focus on the reliability issue; they propose to use the link, routing and equipment redundancy to overcome the defect of reliability in IPsec-VPN technology. They propose to use redundant links and equipment so in case where one tunnel or gateway fails, the other tunnel and gateway works normally to provide a secure encrypted channel. However, authors didn't consider the impact of redundancy on DMVPN performances. This was stressed in [13] where an evaluation of DMVPN network high availability by the assessment of the network performances when using various routing protocols is done. According to the simulation results, the authors conclude that CPU performances can be improved by a duplicating HUB number. In addition, they proved that EIGRP protocol benefits from the increase in the number of HUBs, but not from the number of clouds. Bahamas et al. [14] enhances the previous research, by studying the scalability of the DMVPN network by varying number of sites and dynamic routing protocols using OSPF, BGP and EIGRP. The results of their experiments show that EIGRP protocol is the best in terms of initial convergence delay, Throughput and queuing delay, BGP shows its efficiency compared to OSPF, this letter is not recommended on DMVPN network.

The problem of the impracticality of DMVPN for users how need to obtain an IP address dynamically is addressed in [15]. As DMVPN depends on NHRP, where only nodes registered on the NHRP server will be connected to the network, this is inconvenient for users who move frequently. Authors propose to use an architecture that should support data encryption transmission, dynamic routing information encryption transmission and a variety of redundancies, including gateway and link redundancies. For these aims, they propose to use EZVPN to compensate the limitation of DMVPN. This solution is assumed to solve the issues of encryption, reliability and free remote access. According to the authors, the replacement of IPSec with EZVPN provides better alternative to remote access while retaining DMVPN.

In [16] authors designed a model of a smart adaptive quality of service management for the dynamic and multipoint Virtual Private Network; they create a web oriented application PB-SAQOS which aims to make it possible to adapt the QoS policy according to: Intermediate equipment, traffic class, or appropriate QoS policies to the type of the network access. Security issues related to each component of the DMVPN protocols were discussed in [17]. Authors' addresses the vulnerabilities associated with DMVPN technology and the countermeasures that can be taken to mitigate such damage. In another area, Angelescu et al. [18] presents a simulation of DMVPN based network, the simulation concern phase 2 of DMVPN networks with one hub and two spokes. They proved that the use of DMVPN reduces the number of hops which is translates to lower transit delays. Otherwise, regarding the Dual Hub, Dual DMVPN hub-to-spoke model, the authors in [19] demonstrate which routing protocol is most paramount. The results of their simulation have shown the efficiency of EIGRP over other protocols. However, they assume that OSPF is still a good alternative.

El-kamoun et al. [20] present a comparative study on the impact of conventional VPN and DMVPN technology on the performance of the 802.16e networks. Thus, the authors evaluated the Scalability of the protected DMVPN by IPsec in a WiMax Network. They use VOIP to evaluate the performances of the network, according to five scenarios, in each scenario the number of BTS is increased in order of 4. They assume that the increase in the number of IPsec tunnels has a direct influence on the performance of the whole system. Regarding routing protocols another evaluation was done in [21]. Author's presents a comparative performance evaluation between the two routing protocols OSPF and RIP, in order to determine which of these protocols recovers faster in the case of link failure. The authors stressed up the problem of failing to recover in mesh topology networks, where switching between the links in terms of failure and recovery takes a period of time depending on the routing protocol employed. Based on their results, the authors conclude that OSPF should be used in a network prone to frequent failure; hence RIP should be used in networks where failures are infrequent.

Bensalah et al. [22] study the impact of VPN technologies (GRE, GRE over IPsec, DMVPN, IPsec DMVPN, and IPsec site to site) on voice over IP performances and Determine the scalability of each technology with the load rise of the packets. Authors order the VPN technologies, according to their preference as follows: GRE, GRE over IPsec, IP, DMVPN, IPsec DMVPN and IPsec site to site. Bahnasse et al. [23] enhance their previous research and propose a new model of adaptive security called Smart Security Management for New Generation VPN. In order to evaluate their approach, the authors created a testbed of 5 sites, fully connected with securing IPsec tunnels and used VOIP traffic to evaluate the behavior of their model compared with traditional security by increasing the load of the packet. The optimization of the hub/spoke set to improve interdepartmental communication efficiency is discussed in [24]. The basic intend of this paper is to determine the optimal VPN communication structure, in other words the optimal set of hubs and spokes in a hub-and-spoke networks. Authors choose OSPF as the dynamic routing protocol used for broadcasting branches addresses prefixes.

4. Literature Classification and Comparison

According the related discussed issues in the researches cited in the previous section, we proposed a classification of DMVPN approaches which can categorize them into four main categories (Fig.3).

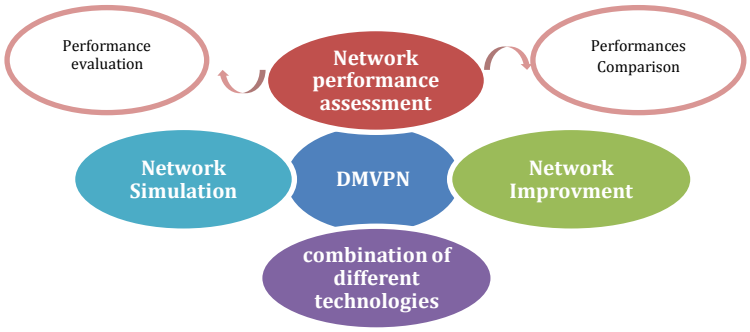

Figure 3: The proposed classification

4.1 Network performance assessment approaches

The richest category is the one which regroups works that have been the focus of DMVPN network performance assessment. This category itself is subdivided into two sub-categories. The first sub-category has two main purposes, the first one aim, to evaluate the impact of DMVPN on enterprise networks [8]. While the second focus on performances of real time application such as VoIP applications [22, 23].

The second sub-category presents the set of approaches which focus on the comparison the network performance in different situations. Namely, in case of utilization of various routing protocols such as EIGRP, OSPF, and RIP; where authors compared between routing protocols in terms of queuing delay [6], CPU utilization [7], network availability [12] and scalability [14], failure recovery [21], network convergence activity and duration [19] and even the impact of encryption protocol on DMVPN performance [11]. Major contributions of this first category are summarized in Table 1.

4.2 Network improvement Approaches

The second category in our literature classification is DMVPN network improvement. The relevant approaches aim to enhance DMVPN functionality and ameliorate the network performances. Among these improvements is the insurance of an optimal hub load balancing in order to ensure servers ‘availability [5]. The approach presented in [12] aim to resolve the reliability issue using routers and link redundancy. Additionally, the automatization of the QoS policy management is elaborated in [16] and [22]. Other studies focus on the improvement of security within DMVPN networks such in [17] where authors discuss the security issues related to each component of the DMVPN protocols, and [24] where authors aim to infer the set of hub and spokes in DMVPN implementations. The major contributions of this category are summarized in Table 2.

Table 1 Summary of DMVPN performance assessment approaches

Ref	Year	Objective	Contribution	Finding	Drawbacks
[7]	2010	Deduct the Optimal routing protocol type for DMVPN	Using different routing protocols (EGIRP, OSPF, RIP)	EIGRP provides Better network performances	The simulation scenarios are static.
[8]	2011	Validate DMVPN effectiveness in enterprise network	Proposing a scheme which provides a safe, efficient, flexible and economical way to build safe and low cost enterprise network	DMVPN gives more opportunities to enterprise to build up secure and economical networks	The improvement over the classic schema is not addressed.
[11]	2015	Demonstrate the encryption protocol Impact on performances.	Vary encryption protocol in order to resolve data confidentiality issues.	DMVPN/IPsec provides great flexibility and confidentiality	Only the Hub and Spoke implementation is verified
[19]	2017	Demonstrate the most performant routing protocol for Dual Hub DMVPN hub-to-spoke connection.	Compare the routing protocol performances in term of least delay, convergence time and link utilization	EIGRP is the most suitable protocol for this type of network.	Only the hub-to-spoke topology is considered
[21]	2017	Demonstrate which routing protocol recovers faster in the case of failure.	Compare the two routing protocols OSPF and RIP in term of failover recovery.	OSPF should be used in failure prone networks; RIP in networks where failures are infrequent	The study is based only on MAN

Table 2 Summary of DMVPN network improvement approaches

Ref	Year	Objective	Contribution	Finding	Drawbacks
[10]	2014	Automate the tunnel connections structure.	Proposition of an algorithm for automatic management of tunnel connections.	Introduced a way of resolving a 'dead' IPsec session.	Manually controlled experiments.
[12]	2015	Overcome the defect of reliability in IPsec-VPN technology.	The use of link, routing and equipment redundancy.	Redundancy ensures the network reliability and the continuity of its services.	the impact of redundancy on DMVPN performances is not considered
[16]	2016	Automate the management of the QoS policy in DMVPN network.	Design of smart adaptive quality of service management model for for DMVPN Network;	The simulation results proved PB-SAQOS efficiency due to its simplified and automatic resources management.	
[17]	2016	Addresses the security issues related to each component of DMVPN.	using ACLs to filter the IP option fields, and to protect against IP spoofing before encryption to overcome IPsec limitations	NHRP limits can be remedied by using the anti spoofing mechanisms.	The impact of the procedure on the convergence time is not mentioned

4.3 Network Simulation Approaches

Works regrouped in this category have two main objectives: automate the simulation of DMVPN [9] and demonstrate the efficiency of DMVPN [18]. The major contributions of this category are summarized in Table 3. To be mentioned that we didn't mention some network simulation approaches such as [16],[19] and [21] to avoid the redundancy because some these approaches were already mentioned in previous categories. Hence, in some cases one approach can belong to more than one category.

4.4 Technologies combination

The last category regroups approaches which combine other technologies with DMVPN such as [15] where authors replace IPsec with EZVPN technology in DMVPN and [20] where authors used DMVPN in WiMAX networks. The major contributions of this category are summarized in Table 4.

Table 3 Summary of DMVPN network simulation approaches

Ref	Year	Objective	Contribution	Finding	Drawbacks
[9]	2014	Automate the generation of dynamic scenarios DMVPN multi-architectures projects for OPNET modeler	Propose a server-based architecture to automate DMVPN simulation under the OPNET Modeler simulator. conceive a web-tool which provides the possibility to parameterize and customize the DMVPN parameters	The conceived web-tool provides the possibility of automatization of the simulation and also parameterize and customize all the DMVPN protocols	Complicated result interpretation and incompatibility with other simulators.
[18]	2017	Demonstrate the efficiency of the DMVPN technology over the classical VPN approach.	Simulate a DMVPN phase 2 in GNS3 simulator	The use of the DMVPN protocol reduces the number of hops which translates to lower transit delays	Only the phase tunnel on demand is simulated

Table 4 Summary of DMVPN network simulation approaches

Ref	Year	Objective	Contribution	Finding	Drawbacks
[15]	2016	Address the problem of impracticality of DMVPN for users how need to obtain an IP address dynamically	Propose to use EZVPN instead of IPsec-VPN to compensate the limitations of DMVPN such it does not provide dynamic IP address for rooming users	The combination of EZVPN with DMVPN provide safe, free remote access for users and low workload management for administrators.	EZVPN device restriction, (no heterogeneous devices). Issues of bandwidth and high cost
[20]	2016	Demonstrates the impact of conventional VPN and DMVPN technology on scalability of WiMAX network.	Use VOIP to evaluate the performances of the network according to five scenarios, in each scenario the number of BTS is increased in order of 4.	Both the increment of BTS or IPsec tunnels number has a negative impact on WiMAX network performances.	

5 Perspectives

Despite that DMVPN related studies and solutions are plenty; there are still a lot of lacks and open questions which could be a source of inspiration for future works. One of the major concerns in DMVPN is the choice of routing protocol. As demonstrated in the previous section, a lot of work focused on this issue. Regarding EIGRP, OSPF RIP or BGP, according to the literature the most recommended protocol is EIGRP. Nevertheless, there are some scenarios where the use of EIGRP is not optimal such in case of network prone to failure, where OSPF stand up as a better choice. Another case where RIP is a better choice is when the network density is low (Table 5). Hence, there is still no standard routing protocol conceived particularly for DMVPN. Another major limitation should be studied which is the problem of the impracticality of DMVPN in dynamic situation; where mobile users need a dynamic addressing. An important research challenge that must be taken into consideration is the security issues. Whether the WAN security which is related to IPsec or the LAN security which repose on the routing protocol security mechanisms. Another important issue in DMVPN is the use of VoIP over DMVPN regarding that the increase IPsec tunnels number has a direct influence on the whole system performance.

Table 5 Routing protocols Comparison

Criterion / Protocol	Memory capacity and delay	Network convergence	Hub Redundancy	Network density	Network failure situations
EIGRP	✓	✓	✓	×	×
OSPF	×	×	×	×	✓
RIP	×	×	×	✓	×

6 Conclusion

Given that the DMVPN technology is imposed recently, through this paper, we examined the different solutions, approaches and proposition related to Dynamic Multipoint Virtual Private Networks. We proposed a classification of a state of art in the context of DMVPN. Moreover, we compared the existing solutions developed to fulfill the DMVPN issues. According the related discussed issues in these researches, we proposed a classification of state of art. Moreover, we demonstrated the limitations of existing solutions developed to fulfill the DMVPN issues. Furthermore, we outlined both open questions and research challenges that could improve the capabilities and effectiveness of DMVPNs such as the security issues which can be detrimental to the proper functioning of the networks. Hence, According to our analysis, a standard efficient solution must be conceived to overcome prior approaches limitations in the context of Dynamic Multipoint Virtual Private Networks.

References

[1] Venkateswaran, Ramachandran. Virtual private networks. IEEE potentials, 2001, vol. 20, no 1, p. 11-15.

[2] S. Krishnan, "IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap", IETF RFC 6071 Ericsson, February 2011.

[3] Khelf, Roumaissa et Ghoualmi, Nassira. Intra and inter policy Conflicts Dynamic Detection Algorithm. In: Detection Systems Architectures and Technologies (DAT), Seminar on. IEEE, 2017. p. 1-6.

[4] Luciani, J., D. Katz, D. Piscitello, B. Cole, and N. Doraswamy. "Next hop resolution protocol (NHRP)." RFC2332 (2001).

[5] Jahan S, Rahman M S, Saha S. Application specific tunneling protocol selection for Virtual Private Networks[C]//Networking, Systems and Security (NSysS), 2017 International Conference on.IEEE, 2017: 39-44.3.

[6] Jankuniene, R., & Jankunaite, I. (2009, June). Route creation influence on DMVPN QoS. In Information Technology Interfaces, 2009. ITI'09. Proceedings of the ITI 2009 31st International Conference on (pp. 609-614). IEEE.

[7] Thorenoor, S. G. (2010, April). Dynamic routing protocol implementation decision between EIGRP, OSPF and RIP based on technical background using OPNET modeler. In Computer and Network Technology (ICCNT), 2010 Second International Conference on (pp. 191-195). IEEE.

[8] Chen, H. (2011, May). Design and implementation of secure enterprise network based on DMVPN. In Business Management and Electronic Information (BMEI), 2011 International Conference on (Vol. 1, pp. 506-511). IEEE.

[9] Bahnasse, Ayoub et EL Kamoun, Najib. Policy-Based Automation of Dynamique and Multipoint Virtual Private Network Simulation on OPNET Modeler. Policy, 2014, vol. 5, no 12.

[10] Malinowski, T., & Arciuch, A. (2014, September). The procedure for monitoring and maintaining a network of distributed resources. In Computer Science and Information Systems (FedCSIS), 2014 Federated Conference on (pp. 947-954). IEEE.

[11] Nowosielski, Leszek, Wielemborek, Radosław, Laskowski, Dariusz, et al. Confidentiality of data in backbone networks based on scalable and dynamic environment technologies. In : Communications and Networking (BlackSeaCom), 2015 IEEE International Black Sea Conference on. IEEE, 2015. p. 68-71.

[12] Yang, Fan et Zhao, Lizhen. IPSec-VPN Availability Research and Simulation. In : International Conference on Computational Science and Engineering (ICCSE). 2015. p. 290-295.

[13] Bahnasse, Ayoub et Elkamoun, Najib. Study and evaluation of the high availability of a Dynamic Multipoint Virtual Private Network. Revue MéDiterranéEnne Des TéLéCommunications, 2015, vol. 5, no 2.

[14] Bahnasse, A., & El Kamoun, N. (2015). Study and Analysis of a Dynamic Routing Protocols' Scalability over a Dynamic Multi-point Virtual Private Network. International Journal of Computer Applications, 123(2).

[15] Li, Hongru, Prasad, P. W. C., Alsadoon, Abeer, et al. An improvement of backbone network security using DMVPN over an EZVPN structure. In : Advances in Electrical, Electronic and Systems Engineering (ICAEES), International Conference on. IEEE, 2016. p. 203-207.

[16] Bahnasse, Ayoub et EL Kamoun, Najib. A policy based management of a smart adaptive QoS for the dynamic and multipoint virtual private network. Int. J. Control Autom, 2016, vol. 9, no 5, p. 185-198.

[17] BAHNASSE, Ayoub et EL Kamoun, Najib. Security of Dynamic and Multipoint Virtual Private Network. International Journal of Computer Science and Information Security, 2016, vol. 14, no 7, p. 100.

[18] Angelescu, N., Puchianu, D. C., Predusca, G., et al.DMVPN simulation in GNS3 network simulation software. In : Electronics, Computers and Artificial Intelligence (ECAI), 2017 9th International Conference on. IEEE, 2017. p. 1-4.

[19] TIZAZU, Gebere Akele, KIM, Ki-Hyung, et BERHE, Abraham Belay. Dynamic routing influence on secure enterprise network based on DMVPN. In: Ubiquitous and Future Networks (ICUFN), 2017 Ninth International Conference on. IEEE, 2017. p. 756-759.

[20] El kamoun, Najib, Bahnasse, Ayoub, et Bensalah, Faycal. Evaluation of the Scalability of the Protected Multipoint Dynamic VPN by IPsec in a WiMax Network. IJCSNS, 2017, vol. 17, no 12, p. 108.

[21] AJANI, Ayodeji Akeem, OJUOLAPE, Bilkisu Jimada, AHMED, Abdulkadir A., et al. Comparative performance evaluation of open shortest path first, OSPF and routing information protocol, RIP in network link failure and recovery cases. In: Electro-Technology for National Development (NIGERCON), 2017 IEEE 3rd International Conference on. IEEE, 2017. p. 280-288.

[22] Bensalah, F., El Kamoun, N., & Bahnasse, A. (2017). Analytical performance and evaluation of the scalability of layer 3 tunneling protocols: case of voice traffic over IP. International Journal of Computer Science and Network Secuirty (IJCSNS), 17(4), 361-369.

[23] Bahnasse, A., Louhab, F. E., Talea, M., Oulahyane, H. A., Harbi, A., & Khiat, A. (2017, November). Towards a new approach for adaptive security management in new generation virtual private networks. In Wireless Networks and Mobile Communications (WINCOM), 2017 International Conference on (pp. 1-6). IEEE.

[24] Malinowski T., Chudzikiewicz J. (2018) On Improving Communication System Performance in Some Virtual Private Networks. In: Gaj P., Sawicki M., Suchacka G., Kwiecień A. (eds) Computer Networks. CN 2018. Communications in Computer and Information Science, vol 860. Springer.