Alexander Moore

CEG 6422

Vance Saunders

11/24/21

Virtual Dispersive Networking

Virtual Dispersive Networking is a fairly novel cybersecurity technology that was introduced by Dispersive Solutions, Inc. in the early 2010s. “Dispersive Solutions, Inc, is led by Robert W. Twitchell Jr., CEO, and inventor of VDN technology” [1]. The company was founded in 2010 and develops, produces, and sells computer software. The company is fairly small in size and has not been reported as an ideal place to work because of nepotism. Alongside Twitchell Jr.’s many other granted patents, Virtual Dispersive Networking relates to wireless connection between multiple devices. Normally, multiple devices communicate with each other by sending and receiving full packets or complete files of data. However, Virtual Dispersive Networking divides “the message into multiple parts, encrypt those parts and route them over different protocols on independent paths” [4]. This immensely increases cybersecurity for any of the wireless communication happening between the devices using this new unique approach. The broken up data is transmitted separately which makes the entire message much harder to get ahold of. Even if someone who should not get ahold of one of the pieces of data does, it will be encrypted. Then if they decrypt it successfully, they will still only have a single, unintelligible piece of information. The entire message should still make its way to the intentional receiver unharmed, and the legitimate sender and/or receiver will be alerted that there was a breach in the transmission of their message.

“VDN follows the methods of traditional military radio spread spectrum security” [5]. This is most likely the result of the close proximity with which Dispersive Solutions, Inc. has worked with the United States military. Spread spectrum security was an implementation to increase security of radio transmissions from the conventional radio signals. This radio technology is an approach that the United States military has used for decades in the past. While they may still continue to use this technology, “some [techniques] have been declassified as recently as the 1980s” [6]. This means there is a good possibility that they have replaced it with an improved radio transmission technology. While normal radio signals are extremely concentrated in frequency, they are also easily susceptible to interference and being intercepted. “Spread spectrum radio (SSR) signals, in contrast, are spread over a broader portion of the radio frequency band and are typically much more resistant to interference—by other co-existent signals or by intentional jamming.” [6]. There are two different types of these spread spectrum radio signals: frequency-hopping spread spectrum (FHSS) and direct-sequence spread spectrum (DSSS). “FHSS is used in a variety of communication transmissions where the data signal is modulated with a narrowband carrier signal that "hops" in a random but predictable sequence from frequency to frequency as a function of time over a wide band of frequencies” [6]. Virtual Dispersive Networking is most similar to this type of spread spectrum technique but modifies digital data communications over networks, including the internet, instead of radio signals. “By doing this, only the intended recipient can reassemble the message properly” [7].

The incentive for the creation of Virtual Dispersive Networking was predominantly to combat man-in-the-middle cyber-attacks and cyber spying. “Man-in-the-Middle (MIM) attacks are nothing but cracking the encryption of messages and targeting the median nodes” [8]. Once the attacker breaks the encryption of the message communicated between two devices, they are able to spy on that communication without the deliberate parties’ knowledge. There are multiple different types of man-in-the-middle attacks, including rouge access points, ARP spoofing, and DNS spoofing. Exploiting rogue access points, attackers will take advantage of the fact that “devices equipped with wireless cards will often try to auto-connect to the access point that is emitting the strongest signal. Attackers can set up their own wireless access point and trick nearby devices to join its domain. All of the victim’s network traffic can now be manipulated by the attacker.” [10]. ARP spoofing involves the attacker pretending to be a legitimate host on a network, responding to requests from the victim’s device using its own MAC address. “When using a DNS spoofing attack, the attacker attempts to introduce corrupt DNS cache information to a host in an attempt to access another host using their domain name” [10]. This type of man-in-the-middle attack results in the victim unintentionally sending their confidential information to the attacker’s domain. Attackers mainly use this DNS spoofing attack to gain access to the victim’s passwords, but may also be seeking other personal data in the victim’s cache.

While the man-in-the-middle attack is often used in order to spy and collect information from the victims, it can also be used in order to modify information going between two devices without either of the victims’ knowledge. This type of modification of communication is “said to be an attack on integrity” [11]. Oftentimes, attackers will use this in order to plant a link to malware to infect the user receiving the communication. The receiver will trust that the message they are receiving is from the trusted source. However, since it was tampered with during the transmission, the integrity of the message is lost. If the receiver knows that the message has been tampered with, they should avoid opening the message. Unfortunately, the victims of these types of man-in-the-middle attacks often don’t realize that the data is corrupted until it is too late and the malware has already spread onto their computer.

Even though man-in-the-middle attacks are a concern globally from malicious users, they are additionally a concern in countries where citizens have restricted rights to speech or knowledge. “They are quite common in China, where the firewalls preventing internet traffic are also listening to everything coming through from outside of China” [7]. Users in authoritarian countries such as China must anticipate being spied on by their own government alongside any malicious attackers. Virtual Dispersive Networking can assist in preventing these man-in-the-middle attacks because the ”signal is transmitted in short bursts or quantum packets, which can't be covertly read without disrupting their content. No one can intercept data sent to you without introducing some noise in it” [12]. While Virtual Dispersive Networking helps prevent these man-in-the-middle attacks, it also helps monitor and log for the user whether or not there are any attempted attacks. “VDN also isolates attacks by changing identity while under attack and alerting peers. It then re-routes attacks for analysis and response” [9]. This means that even if the packets are attacked during transmission, Virtual Dispersive Networking technology still facilitates the transmission of the complete message from the legitimate sender to the legitimate receiver without any disruption.

Currently, there are several practices and methods in place to prevent man-in-the-middle attacks. General good cyber hygiene practices are heavily recommended for any cybersecurity, and this is no different when attempting to protect against these man-in-the-middle attacks. Some of these practices include keeping software up to date, creating strong passwords, using multi-factor authentication, using firewalls and credible antivirus software, etc. Other methods to protect against these types of cyber-attacks include educating users/employees about potential scams such as phishing emails or forcing the usage of HTTPS when browsing the internet rather than allowing the usage of less secure HTTP. Two more technical ways to minimize the risk of the man-in-the-middle attacks include using secure socket layer (SSL) certificates and a virtual private network (VPN). Secure socket layer certificates show evidence of a secure, encrypted connection. “SSL certificates have a key pair: a public and a private key. These keys work together to establish an encrypted connection. The certificate also contains what is called the ‘subject,’ which is the identity of the certificate/website owner” [15]. While browsing on the internet, a padlock will appear next to a website’s URL (uniform resource locator) if the website has a secure socket layer certification. Clicking on the padlock will display more information about the site and the certification. Virtual private networks are a technology that conveniently allows users to secure their internet traffic even when on unsecure networks. “VPNs create several subnets for securing communications through the use of encryption-based keys. This method prevents a hacker from deciphering the traffic in the VPN even if he can connect to the network” [12]. Virtual private networks have become more widespread and mainstream over the last several years, with major VPN companies gaining popularity.

Unfortunately, these methods are becoming outdated and less secure as time continues to pass. “Encryption-based MiM prevention technologies like SSL (secure sockets layer, now called TLS, or transport layer security) and virtual private networks (VPNs) are point-to-point, while today’s complex digital world requires secure end-to-end communications, where traffic might cross many intermediate nodes – all of which become weak points ripe for MiM attacks” [13]. The intermediary nodes in which the network traffic is passed across are vulnerabilities that can be easily taken advantage of by attackers. “Data that was once securely encrypted can now be broken by parallel processing power” [14]. This challenge of competing with increasing processing power has spawned the need for a new security technology, which is why Virtual Dispersive Networking was created. Virtual Dispersive Networking pushes the data “dynamically to optimum paths – both randomizing the paths the message take while simultaneously taking into the account congestion or other network issues” [14]. This new technique of communicating securely over the network is exceeding the abilities of the old communication methods, and may become the new commercialized practice.

Virtual Dispersive Networking has also been used to increase security in peer-to-peer networking. “A peer-to-peer network is a group of computers on the internet that have agreed to share files with one another” [2]. Because there are a large group of users all in a single network, peer-to-peer networks can raise some cybersecurity concerns. “When you join a peer-to-peer network, you are choosing to trust the very large group of strangers that make up the network” [2]. When you open certain ports on your personal computer to access the network, other users can gain access to your personal machine or network. These open ports are like invitations for attackers to infiltrate your system and place malware or steal information from you. “In peer-to-peer (P2P) networking, a group of computers are linked together with equal permissions and responsibilities for processing data” [3]. Because everyone has equal permissions and no device is specifically set as a client or a server, data exchange between the devices can be manipulated easily by attackers.

Although I could not find any specific real-life examples of anyone using the Virtual Dispersive Networking, the related company, Dispersive Solutions, Inc. has worked with many government entities. “Dispersive has been deployed by enterprises, government agencies and branches of the military due in part to the stringent security capabilities of its multi-path, software-defined networking overlay solution” [16]. One fictional example of this technology being used would include a military contractor who is attempting to send or receive some data or confidential information to/from a military base. The data is classified and is of high importance to United States security. In this example, a Russian spy is attempting to intercept the data being sent between the contractor and the military base so that he can record it and relay it back to his Russian authorities. If the contractor and military base were trusting simpler technologies such as SSL certifications or VPNs, then the data would be at higher risk of being collected by the Russian spy. However, they recently installed Virtual Dispersive Networking on their systems. The data is transmitted in small, indistinguishable parts with endpoints that are much harder for the hacker spy to gain access to. Even if the spy does get ahold of a single part of the data, it is encrypted and small enough that it would not reveal anything of any importance to him. Additionally, the Virtual Dispersive Networking would alert the contractor and military base that there was an infiltration and spying attempt so that they may take any further steps they desire to ensure that their method of communication continues to stay secure. Although this technology is mostly used by government entities, it can also be used by the private sector.

Another fictional example could include a private machinery company that has multiple locations. Because it has multiple locations, any updates to the software of the machinery or improvements on the specifications need to be shared between all of the locations. Although this information is not a concern of national security like the previous example, this private company wants to keep its software and specifications for its machinery secret. In this fictional example, this machinery company is far ahead of the competition because of their advancements, and any error that results in the release of their confidential information would likely shorten that gap and cause them to lose business. For this example, a lone hacker is attempting to hack into their systems in an attempt to find important data that he can use as leverage against the company. The hacker wants to hold the data for ransom and threaten to release the data to the public unless the company pays him. Although he has high quality decryption technology and is skilled at hacking, he is surprised that he cannot find any useful data. Fortunately, the company uses Virtual Dispersive Networking so the data the hacker is retrieving is broken up pieces that are not useful to him at all. On top of that, the company now has the knowledge that someone is attempting to hack into their systems.

A third fictional example includes an older employee that is currently working from home on his computer because of the pandemic. He doesn’t have much knowledge about computers in general, but his only option to continue working was to work on the computer. A lot of the employee’s work communication is done through email. Because the company that he works for did not have enough time to train all of their newly online employees about cybersecurity and secure computing practices, the employee is not aware of phishing attacks. Simultaneously, the pandemic has caused a lone hacker to be inspired to improve his skills, so he attempts to find easy targets for his phishing attacks. The hacker wants to make the phishing attack look legitimate like it came from someone else within the company. He attempts to gain access to a thread of communication between the older employee and his coworker. However, the Virtual Dispersive Networking software makes it so that the hacker cannot store any malicious data within the messa

Advantages of the Virtual Dispersive Networking technology includes the extreme improvement to overall cybersecurity. “Dispersing the data over multiple paths eliminates the Man-in-the Middle threat. Hackers can only obtain small pieces of the original file on any given pathway, rendering any data obtained meaningless.” [13]. Additionally, if any “connection is lost on any of the several streams due to network failure, data packets are then rerouted to an already existing path, or an additional path is established which drives in negligible network downtime” [5]. This results in incredible speed and performance compared to previous networking communication methods such as VPN. Because the Virtual Dispersive Networking “traffic is dispersed over multiple independent paths using unique methods, increasing available bandwidth and optimizing data flows on individual pathways” [13].

The main disadvantage that I have noticed with this technology is that it is extremely new so it is likely that most companies might be hesitant to put their faith in it yet. “As with any industry, change can be terrifying (especially when sensitive data is considered)” [5]. While the technology looks extremely effective in theory, it appears that there is extremely small amount of information about it or the company online. The company, Dispersive Solutions, Inc., seems to be fairly small still even though it has been in business for about ten years now, so it is possible that the companies or agencies that have used the product have not garnered the amount of success that they were hoping for. Or possibly the company’s marketing and advertising teams are not very effective. There is so little amount of content online about this technology and this business that it makes it difficult to even research about it. It is likely that most companies won’t start implementing this Virtual Dispersive Networking technology until it becomes more popular to the cybersecurity world. That being said, there didn’t appear to be any definitive disadvantages to this technology as far as software or cybersecurity is concerned. I believe that as time passes and the technology gains more attention, there may be some disadvantages that appear as it is used and tested more. However, the technology is so novel and unused that it is difficult to see any at this point in time.

Virtual Dispersive Networking is an awesomely powerful method for communicating between two devices across a network. “The balance of power in Cyber Security now shifts back in defense of the user” [1]. The technology, although adopting its design from old radio transmission techniques, is novel to cyber security and networking. It is ideally much more secure than current methods of communication across networks and is trusted even by the government for secure data transmission. If the United States military and government is using the technology, it will most likely be used within private sector soon if it is not already. In fact, COVID-19 could potentially be a driving factor that makes Virtual Dispersive Networking technology a mainstream software in the private sector. Because of the pandemic, more people have been staying home to work and have been relying heavily on computers and networks. The longer this expansion of employees stay home, the more necessary it is for them to find a secure method of communication over their network. Just as other companies, such as Zoom and Nord VPN, have taken advantage of this by increasing their advertising, Dispersive Solutions, Inc. can do the same thing. If they improve their marketing and advertising teams and take advantage of the fact that a lot of people are relying on secure networks right now, they could potentially become a popular cybersecurity software company. The technology appears to be extremely effective and is potentially the future of cybersecurity.

References

[1] Bell, Darin C. “Dispersive Solutions Announces a Revolutionary Technology That Changes The Balance of Power in Cyber SecurityD.” *CISION PRWeb*, Vocus PRW Holdings, LLC., 11 Dec. 2012, https://www.prweb.com/releases/cybersecurity/networksecurity/prweb10209088.htm.

[2] “Peer-2-Peer Networking.” *OSU.edu*, The Ohio State University, https://cybersecurity.osu.edu/cybersecurity-you/avoid-threats/peer-2-peer-networking.

[3] “What Is P2P Network Sharing?” *Webroot*, Webroot Inc., https://www.webroot.com/us/en/resources/glossary/what-is-peer-to-peer-networking.

[4] CyberDegrees.org Staff. “Hot Technologies in Cybersecurity.” *Cyber Degrees*, CyberDegrees.org, 29 Sept. 2021, https://www.cyberdegrees.org/resources/hot-technologies-cyber-security/.

[5] “Here’s How Virtual Dispersive Networking (VDN) Can Help Fight Man in the Middle Attacks.” Edited by Trixter, *Trixter*, Trixter Cyber Solutions Pvt Ltd., 9 Mar. 2021, https://trixter.in/heres-how-virtual-dispersive-networking-vdn-can-help-fight-man-in-the-middle-attacks/.

[6] Muenstermann, Stephen. “Interference and Security Considerations for Wireless Communications in an Industrial Environment .” *Honeywell Process Solutions*, Honeywell International Inc., June 2007, https://www.honeywellprocess.com/library/marketing/whitepapers/Interferenceand%20Security\_WP\_May08.pdf.

[7] “How 2020 Has Changed the IT Security Landscape.” *ITeam*, The ITeam, 2020, https://theiteam.ca/cybersecurity/emerging-cybersecurity-technologies/.

[8] Tank, Abhishek. “Cybersecurity Technologies You Should Be Aware of in 2020.” *DevsDay*, DevsDay.Ru, 3 Aug. 2020, https://devsday.ru/blog/details/22013.

[9] Mounts, William. “MT Transparency R&D Paper FINAL.” *ACADEMIA*, https://d1wqtxts1xzle7.cloudfront.net/32893857/MT\_Transparency\_R\_D\_Paper\_FINAL-with-cover-page-v2.pdf?Expires=1637636361&Signature=LA-IlrUbQne0b0-uQYylTbsWTWnpeMGOJ7PHnmIfVx2vzfhJ6E63XkHf2loa1NkA6eHIa9PBbdnEbMdrhGW5ifDtSPf8QXabcagiKetG9nXvsqtYZykt9nR0G3ypQHUvPE0ZmH5T00jEN7ztPPG-BpYtuN0IdaPoQ~oV9SOa4bYwBmnkz-Gbk2cj6205LYF1bP9bVEv46yIbhx~s5lX4OWPYnO2KbEqbalmCCKwH9tM2BvBF5bgbYgCKw3sbLmHKUihVARIueTMEZQD42h43-g2JRAY3FI1ZBhj0dj7P7M3OKjOq160kdnugnjPtghCDUTYOnILT0s-YqRjM65VotQ\_\_&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA.

[10] “Man in the Middle (MITM) Attacks.” *Rapid 7*, Rapid 7, https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/.

[11] M., Febna V. “Man-in-the-Middle (MITM) Attack: Types, Techniques and Prevention.” *Beagle Security*, Beagle Security, 3 Dec. 2020, https://beaglesecurity.com/blog/article/man-in-the-middle-attack.html.

[12] Ganapathy, Apoorva. “Virtual Dispersive Network in the Prevention of Third Party Interception: A Way of Dealing with Cyber Threat.” *ABC Journal of Advanced Research*, OJS/PKP, 31 Dec. 2020, https://i-proclaim.my/journals/index.php/abcjar/article/view/568.

[13] Bloomberg, Jason. “Cybersecurity: Turning the Tide on Hackers with Dispersive Technologies.” *Forbes*, Forbes, 16 Oct. 2014, https://www.forbes.com/sites/jasonbloomberg/2014/10/16/cybersecurity-turning-the-tide-on-hackers-with-dispersive-technologies/?sh=b7b5f348afc7.

[14] “Virtual Dispersive Networking.” *Arridae*, Arridae Infosec Pvt Ltd, 17 Jan. 2020, https://www.arridae.com/blogs/Virtual-Dispersive-Networking.php.

[15] “What Is an SSL Certificate?” *Digicert*, DigiCert, Inc., https://www.digicert.com/what-is-an-ssl-certificate.

[16] Robuck, Mike. “Dispersive Networks Targets SD-WAN Sector with Its Multi-Path Approach.” *Fierce Telecom*, Questex LLC, 13 May 2020, https://www.fiercetelecom.com/telecom/dispersive-networks-looks-to-disrupt-sd-wan-sector-its-multi-path-approach.