MAKING CYBER SPACE NETWORKS A SAFER WORK ENVIRONMENT AFTER COVID-19 USING SOFTWARE-DEFINED NETWORKS' TECHNOLOGIES

Ali AMEEN[24]

Abstract: *with the corona COVID-19 virus outbreak; the need for online jobs and working remotely has increased, many daily jobs that require face-to-face communications has converted into online jobs as well, with all that and especially with the ever-evolving cyber-threats; comes a bigger need to provide more security for the cyber-space for a better and more reliable work environment. For those reasons and for others; many researches have been conducted to assure the security of computer networks using various ideas and based on different aspects and one of them comes the Software-Defined Networks (SDN) paradigm which is merely a new way of managing the network more that it is a new technology but, this methodology despite its short lifespan proved to be more and more reliable and there are many researches that use SDN to secure or patch issues in some other fields of technology or use other fields of technology to secure SDN and that proves how SDN is not just important and effective but, its ability to be integrated with other technologies. Over the last few years of its age; SDN has proved to be effective in solving some network management issues and provided some quick solutions for some threats but, in the same time with its ability to cure some cyber-diseases; it gives the opportunity for other cyber-threats to emerge.*

Keywords: *corona, security level measurement, programming, centralization, API.*

1. Introduction

With the advent of internet service to the end-users, development of websites and programming, development of data storage system and clouds, internet turned the whole world into a small village as they say and it became the corner stone of everyday' s worldwide development in different fields. With the new evolving technologies emerged bigger needs for the internet; it

[24] student Technical University of Moldova

became the means for shopping, trade, socializing, business, etc. and that created new job opportunities that didn't exist in the human history before and with that came online jobs or working at home, etc. for all the previous reasons and others internet became like the spine for today's world technology and lives everywhere and securing it from ever-evolving threats that are called cyber threats is a huge necessity and to secure it; it is needed to secure its main infrastructure which is the networks that form it. Now networks in general and simple definition as well; could be described as a connection between more than one computer and that connection could be made using hubs, bridges or switches, while to connect more than one network with each other; then a router will be used and all those types of network nodes and others could form the known structure of the network. This kind of structure has remained for a long time with no prominent changes and it is posing great security threats especially when those networks are with huge number of nodes like hundreds of switches, computers, etc. the task of reconfiguring such a network where every device requires a reconfiguration from the beginning is tedious, error-prone and agonizing task and that may lead to more gaps and security issues that could be leveraged to infiltrate the network or disrupt it. Thencomes the Software-Defined Network (SDN) paradigm which is merely a new way of managing the computer networks by separating the brain or the controlling ability switches had from the forwarding ability in them and leaving the switches as merely packets forwarding devices with the ability to forward packets based on traffic rules predefined in the flow tables that there entries are issued by the controlling point that was extracted from the switches and raised to be a central controlling point and defined as a whole new plane or layer called the control plane and represented by a software-based or hardware-based controller/controllers. SDN has lots of advantages like:

- Cost saving: Despite that it is a new way of managing networks but, it has a backwards-compatibility with legacy network devices and that means that is possible to work with SDN environment using classical network devices so, there is no need to change the entire equipment hence a big reduction on cost.
- Dealing with growing technology needs: The amounts of the deployed internet connected devices like (Ipads, smartphones, and IoT devices etc) are really soaring up and with the new technologies like cloud technologies there is a growing need to develop computer networks to be able to keep up with these gigantic amounts of data that are created due to the previous reasons, and Software-defined networks could be a potential solution for that issue.
- Enhancing data flow: The SDN controller is capable of identifying multiple paths for each flow; meaning that this permits the flow's traffic to be distributed and divided among multiple network nodes. And that will give a better enhancement of the performance of the network.
- Flexibility: Due to its programmability; the SDN can open the domain to develop new apps as per user, administrator or enterprise requirements also, that will free the consumer from vendor-based equipment hence, more freedom.
- Security: The centralization provided in this new paradigm represented by the control plane which could be usually one controller and it could be multiple controllers means that there will be one entity or brain capable of controlling, monitoring and managing the status of the whole network with the ability to enforce policies in the network from a central point with no need to configure every single switch in the network which will reduce that time needed and takes a big amount of the burden of configuring or changing policies in every single network node and that means reduction of human error; not to forget that this single point of management will be capable

of filtering the data packets through restrict rules that will provide a granular control over the networks data.

On the other hand, SDN raises some security questions and poses some new cyber challenges like:

- Centralization*:* one of the main advantages software-defined networking technology presents is the ability to control the whole network from a single point of management which can be both time and cost efficient technique but, in the same time from the all the previously mentioned alongside with the combined extrapolation of other researches; it has shown that it could be a single point of failure in the structure of SDN.
- Connection: to solve the above issue some researches tend to use multiple controllers but in this case we'll have another issue to patch up which is the Application programming interface connection API between those controllers, which is named as the east-westbound API.
- Security level measurement: many researches have tried to measure the level of security of SDN but with the usage of a general network security level equations but, not with a specifically-designed equation to measure the security level of the SDN paradigm and some have used some kind of modelling for their own SDN models and environments.

2. Suggested Algorithms

Here are the main algorithmic solutions proposed by this research to be integrated together in a whole framework to solve the problems noticed in the research:

- Hydra: A framework that contains the next algorithms with some techniques incorporated alongside those methods like counter measurement precautions to deal with some prominent cyber-attacks like the Denial of

Service/ Distributed Denial of Service (DoS/DDoS) attacks [1]. This could be done by dictating the installation of botnets [2] into network computers that are connected to the controller that has the Hydra software installed within it; to make them as potential zombie guards to attack the attacker's IP.

- VPN: virtual private network (VPN) is has a great ability to secure connection between nodes using its technique internet protocol security (IPsec). Internet Protocol Security (IPsec) and Secure Socket Layer (SSL) are the two dominant VPN technologies being used today [3]. VPN can create secure communication virtual channels between connected nodes and since it is widely used in different networks then it is possible to include it into the proposed framework.Basically it is possible to connect two controllers using the secure channel of VPN even if they were in the same building and exchange the information between them securely.

- **RSA:** RSA (Rivest–Shamir–Adleman) is one of the first public-key cryptosystemsand is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and it is different from the decryption key which is kept secret (private). In RSA, this asymmetry is based on the practical difficulty of the factorizationof the product of two large prime numbers, the "factoring problem". The acronym RSA is made of the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who first publicly described the algorithm in 1977. Clifford Cocks, an English mathematician working for the British intelligence agency Government Communications Headquarters (GCHQ), had developed an equivalent system in 1973, but this was not declassified until 1997 [4]. This algorithm is already used in most network's communications nowadays but it was included here in this framework in a different way and that's by doubling the channel of cryptography; meaning that instead of using one public key and 2 private keys

for every encryption-decryption procedure; this framework will use 2 public keys and 4 private keys and every node will have a channel for sending encrypted information and a channel for receiving information hence; two channels of encrypted communications. The figure 1 below shows the idea of how the algorithm will be used.

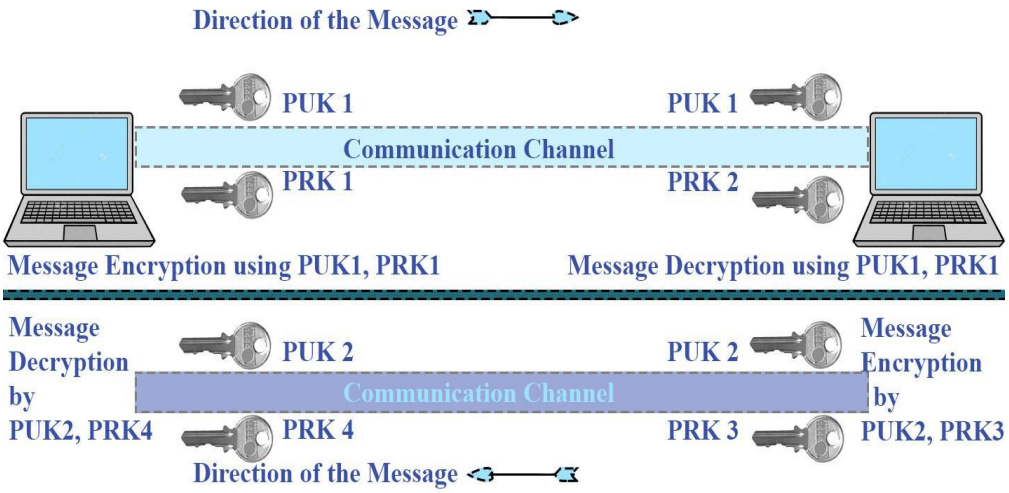

Figure 1. Double RSA algorithm in the Hydra framework

- **Blockchain:** As it is known blockchain's best and biggest participation is in cryptocurrencies like bitcoin but, it is also used in some other fields and it is already used in the Marconi protocol [5], blockchain is also incorporated with the aforementioned framework but in a different way than how it is used in the Marconi protocol. Here the blockchain will be used to secure the configuration updates between multiple controllers'.

3. Risk assessment and capacity utilization

Before going further in the mathematical path, it is important to explain here that it is possible to boost and assure the security of SDN using more than

one controller but in different ways of interaction between them and for that; it is possible to suggest the following SDN controllers' topologies:

- Serial topology: this topology contains 3 controllers, where there's a main controller and 2 backup ones just in case of an attack or a disruption that may stop the first or main controller. the main controller controls the whole network and its nodes and sends an update every 10 seconds that informs the backup controllers about any change in the topology or network configuration and it also acts like a beacon that alerts the controllers if there's a latency in the update message and it took more than 10 seconds then, it will be taken that the main controller has been infected by a DDoS attack or any type of threat hence, comes the role for the second controller which was a backup to become the next main controller and the same thing now goes between the new main controller and the third controller which now becomes the new 1st backup controller until the previous main one will be maintained and restored then everything goes back to its previous state.

- Parallel topology: in this topology we'll use also 3 controllers as well but, they'll work together as a whole one entity integrated together where the info is processed synchronously and each controller will deal with any area or slice of the network especially, if it was closer to this slice or segment than other controllers; which means each controller will give higher priority to closer network segments than the further or more distant segments (of course the distance will be calculated based on the number of hops in the path between the network slice and the controller), of course the updates will be also every 10 seconds. We call this topology as the parallel topology since all controllers work together in parallel so, there is no priority numbers here because they all behave like parts of one main controller where each one of its nodes will serve the closest switches to it first so, the priority for a switch in France to be served

by a controller in France will be higher than that of a switch in Russia based on the number of hops between the switch and the controller.

- Hybrid topology: this topology combines features of both the previous topologies where we have here 6 controllers. There will be 3 main controllers that work like one controller simultaneously and in a parallel way and each one will have a backup controller just in case if it's down then, the backup will take control instead of the infected one. The only update will be between each main controller and its backup one, and it will be every 10 seconds as well. Every backup controller will be connected to other backup controllers alongside with switches in the network and its own main controller that it assists as well. The priority numbers will be between every main controller and its backup one only.

To assess the risk or conversely the security level; it is possible to use the security risk assessment law [6] that states:

$$R = P * V \qquad (1)$$

Where R is the security risk assessment that quantifies and shows the possibility of a threat acts upon a vulnerability successfully and the severity of the results of that attack would be.

Where P represents the probability or likelihood of the vulnerability occurrence; V represents the value or cost of the asset.

In other words, using this formula we can estimate theoretically how much our proposed framework will reduce the security risk of a computer network, hence assuring its security. Logically speaking since a server is the most important part and has the highest value node in the network environment, which we will install our controller software on, then we can say it has the highest asset value or impact according to the same previous resource

[6] we can see that servers have the value V=100 as an asset impact, estimating that our framework will reduce the likelihood of attacks occurrence (like DoS/DDoS, MITM attacks) from P= 0.025 [6] to the following.

Before:

P= 0.025

V= 100

R= 2.5 [6]

R=P.V=0.025.100=2.5

Using the queueing theory for determining the capacity utilization law which describes the single server model and multiple server model queueing theories [7] which are used for calculating the capacity utilization of servers, which state that:

$$K = \lambda/\mu \rightarrow \mu \leq \lambda \qquad (2)$$

Where K = capacity utilization, λ= the number of hosts sending requests and μ = the number of hosts being served per unit of time.

But we can speed the process of the queueing theory a bit and reduce the time consumed by adding more controllers so, the law will be multiple server model and it states that:

$$K_n = \lambda/(n\,\mu) \qquad (3)$$

Where k_n: is the capacity utilization for multiple or n controllers, n: represents the number of controllers in the topology of a network.

Of course, the less capacity utilization, the better it is and the closer to 1 the more optimal it is [7].

So, we can apply the one controller ordinary topology and our proposed topologies and see the difference that they can make. Then in case of the ordinary topology we have:

$K_{n\ ordinary} = 6/(1*2) \rightarrow 6/2=3$

For 3 controllers and the same number of hosts like in serial and parallel topologies: $k_{n\ serial/parallel} = 6/(3*2) \rightarrow 6/6 = 1$

For 6 controllers and the same number of hosts like in the hybrid topology, then: $k_{n\ hybrid} = 6/(6*2) \rightarrow 6/12 = 1/2 < 1$

So this means that the capacity utilization is better or theoretically optimal [8]; because it means that the server is freer and more capable of dealing with requests and prepared in a better way for any DoS/DDoS attack.

Now we can use the following approach to show the relationship between capacity utilization and vulnerability likelihood as shown here. Let:

$$K_n = f(\lambda, n, \mu) \quad (4)$$ So,

$$P_n = P_0 * K_n \quad (5)$$

Where P_n is the new probability of vulnerability. Since that we reduced the capacity utilization and we are using this formula or law to get the percentage of how much we reduced the probability or likelihood of vulnerability. Where Pn is the new likelihood of vulnerability which is the result of the initial probability of likelihood multiplied by the capacity utilization. Of course, now we can compare the previous controller topologies and we can see that the security will be enhanced and the vulnerability will be reduced by using more controllers hence, the likelihood of the vulnerability to occur will be reduced to about 32% which means it will be about 68% less when using our 3 controllers' instead of using 1 controller in our proposed topology and to about 16%, which means that it will be about 84% less using

the 6 controllers' topology instead of using 1 controller topology, which is of course better.

That's why we can see that our probability could be reduced as compared to the 1 controller topology to:

$$R_n = (P_0 * K_n) * V \quad (6)$$

$$R_n = P_n * V \quad (7)$$

$$R_n = \frac{P_0 \cdot \lambda . V}{n\mu} \quad (8)$$ since that V is fixed in our research then let

$$R = f(n, P0, \lambda, \mu) \quad (9)$$

Another way to write this formula is:

$$R_n = \frac{P_0 \cdot K . V}{n} \exists K = \lambda/\mu \quad (10)$$

Where R_n is the new risk assessment resulting after reducing the probability of vulnerability.

We can see the relationship displayed in this figure 2:

Figure 2. the effect of number of controllers used on Security Risk Assessment

The above figure shows how can we reduce the security risk assessment just by adding more controllers to our experiment instead of using 1 controller regardless of their topology, behavior, the architecture of their work, their type and synchronization. So, we are calculating the security risk reduction based on the relation to the usage of one controller; How much percentage we have less capacity utilization to the initial capacity utilization when one controller was used. Which means that the capacity utilization of 3 controllers whether in serial or parallel topology, is 1/3 to the capacity utilization of the 1 controller topology which is approximately 32% less than the initial capacity utilization and that means more capable servers/controllers to deal with requests and better preparation and defense against DoS/DDoS attacks. The figure 3 shows the relationship between capacity utilization and Security Risk Assessment.

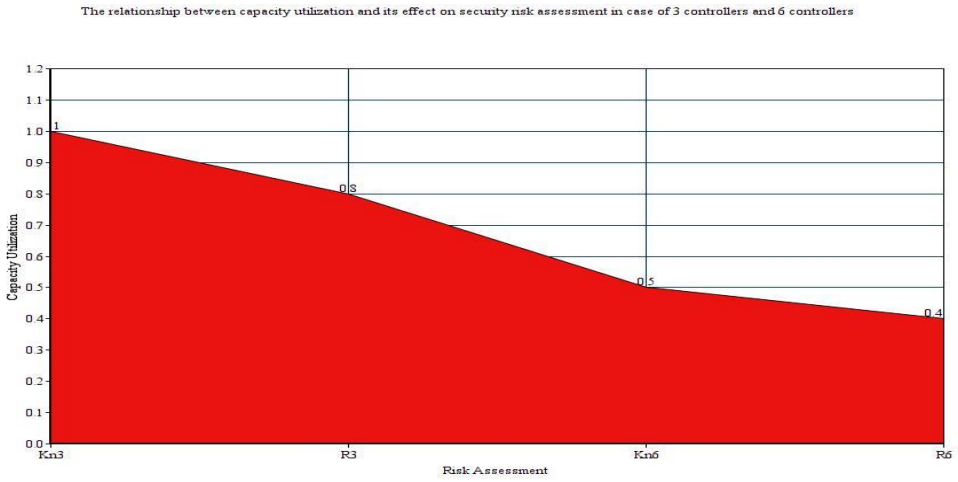

Figure 3. The relationship between capacity utilization and Security Risk Assessment

The above figure shows effect of reducing capacity utilization on reducing the risk assessment, by reducing how much percentage estimated to be after using 3 controllers or 6 controllers instead of a 1 controller which well

be done by reducing the probability of an attack or vulnerability to occur hence reduces the security risk assessment. The effect of vulnerability likelihood on security risk assessment is noticed after reducing it by reducing the capacity utilization of servers that contain the controllers' software which means increasing their ability to deal with attacks such as DoS/DDoS attacks.So, after the usage of 3 controllers in both the serial and parallel topologies, the probability and risk will be: $P_{n\ serial/parallel} = 0.025 * 0.33 \rightarrow P_{n\ serial/parallel} \approx 0.008$

$V = 100$

$R_{n\ serial/parallel} = 0.8$

After the usage of 6 controllers in the hybrid topology, the probability and risk will be:

$P_{n\ hybrid} = 0.025 * 0.16 \rightarrow P_{n\ hybrid} \approx 0.004$

$V = 100$

$R_{n\ hybrid} = 0.4$

Eventually we can conclude that according to the risk assessment modeling method, the 3rd topology which is the hybrid topology has the minimum risk assessment and that means it's the best of all the described topologies.

4. Conclusions

- In order to make the internet's environment a safer place for cyber day to day communications and life, then it is needed to secure its infrastructure which is basically the networks since internet itself is a network.

- There are different ways, technologies and methods used to secure or add some security level to the networks and protect them against some cyber-threats.
- One of those methodologies is the software-defined network paradigm which is a new approach of managing computer networks.
- The world today is depending on the cyber-space in a huge way and that dependence is soaring up more and more.
- SDN could be a booster for cyber world especially with this pandemic that struck the entire planet.
- This paper gives some new or modified algorithms that could be incorporated into a framework that will be used in the application plane to manage the control plane that in turn will manage the SDN infrastructure.
- Also some software-defined network controllers' topologies were formulated.
- To give a simple mathematical modelling for the proposed SDN topologies; capacity utilization and risk assessment laws were used to assess the security level of SDN environments that leverage those proposed topologies.

REFERENCES

1. Zakaria Bawany N., A. Shamsi J., Salah K., DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions, King Fahd University of Petroleum & Minerals, ISSUE 2017, Journal of Cryptology, 17-pages.

2. Osagie M., Enagbonma O., Inyang A., The Historical Perspective of Botnet Tools. Current Journal of Applied Science and Technology, Issue 6, Feb, 2019, Department of Physical Sciences, Faculty of Science, Benson Idahosa University. Volume 32, 8-pages.

3. Chawla B., Gupta O., Sawhney B., A Review on IPsec and SSL VPN. International Journal of Scientific & Engineering Research, 2014, Punjab Agricultural University, 5(11), pp. 21-24.

4. RSA. [online]. 2019, [accessed: 20.07.2019] available: https://en.wikipedia.org/wiki/RSA_(cryptosystem).

5. How blockchain will manage networks. [online]. 2019, [accessed: 26.08.2019] available: https://www.networkworld.com/article/3356496/how-blockchain-will-manage-networks.html.

6. N. vlajic, security risk management, computer security management assessment and forensics: Course material. York University-Canada, 2013.

7. Sztrik J., Basic queueing theory: Book. Faculty of informatics. University of Debrecen-Hungary, 2012.

8. Liu C., Tan C.K., Fang Y.S., Lok T.S., The Security Risk Assessment Methodology: symposium article. Tsinghua University- China, 2012.