Available online at: https://ijact.in

Date of Submission	28/05/2020
Date of Acceptance	15/07/2020
Date of Publication	31/07/2020
Page numbers	3755-3761 (7 Pages)

ISSN:2320-0790

compusoft
An International Journal of Advanced Computer Technology

ARCHITECTURE BASED ON TOR NETWORK FOR SECURING THE COMMUNICATION OF NORTHBOUND INTERFACE IN SDN

Osman Ahmed[1] and Mohammad Hafiz MohdYusof[2]

[1,2]INTI International University, Nilai, Malaysia
[1]Osmanalshaikh.cs@gmail.com
[2]mohammadhafiz.yusof@newinti.edu.my

Abstract: Software-defined networking (SDN) is an emerging technology that has separated its architecture into three layers. Applications layer and Control layer communicates through the Northbound Interface (NBI), these communications can be targeted to fingerprinting even with the encryption applied. With the growth of cyber-attacks and zero-day vulnerabilities in network environments, SDN is more open to security issues than other technologies due to the isolation of its architecture. In this paper, we proposed a new architecture to add an extra layer of Tor network to anonymize the communication of NBI, the development of the combination of SDN and Tor experiment using VMware virtual machines for SDN controller, GNS3 networks and Wireshark for NBI traffic analysis. In the results of maximizing the security of SDN, anonymous communication can prevent NBI from the fingerprinting by allowing the requests and response messages going through multiple nodes before reaching the destination comparing with the current SDN architecture that using direct communications. Lastly, we discussed the results towards the STRIDE model to show and ensure how the combination of SDN and Tor can provide the security and privacy to the SDN Network

Keywords: SDN Architecture; Northbound Interface Communications; SDN Security; TOR Network

I. INTRODUCTION

Software-defined Network (SDN) is a network technology that has advantages of providing security, performance, and control over the network [1]. It's being more common in recent years for many domains like Data Center Network and Cellular Networks. But SDN network is very sensitive to attacks due to separation of control and data plane [1]. However, security issues are involved in this technology and must be considered after being widely used [2]. According to Statistics, "Attackers are trying to find a new way to access SDN network due to vulnerabilities are existed in the SDN network protocols". (Shamugam, Murray, Leong & Sidhu, 2016)

In the SDN network, protocols are establishing trusted communications between the Controller and Application by passing the packets through encrypted traffic in the network to prevent any attacks [1]. But, it's still possible for the hackers to intercept these packets and watch the information because of the addressing wrappers in SSL or TLS is unencrypted [3]. This will give the ability to access and control all the information transmitted over the network. These days, hackers thought in a different way to find the weakness using traffic analysis tools to know some information about sources and destinations within the network. The information collected by the hacker can help them to compromise each point separately. Passive and Active attacks are techniques used by hackers to read information [1]. "Organizations' operations affected when hackers getting unauthorized access to the company's information". (Dacier et al. 2017). Since the Northbound Interface (NBI) is the way the controller used to access SDN applications. When an attacker gaining access to the Controller, the attacker can manipulate with contents, identifying more targets and isolating the network administrator from the Control plane [1]. Always, attackers going to oppose the weakness of communication security in the NBI between the SDN Controller and Applications. The

Controller must be secure when communicating with other layers because it is the central point of failure.

Securing the communication of Controllers is critical and where the Administrator set network rules and decisions for the traffic through the network [2]. SDN poses huge security challenges and finding an appropriate way to secure the SDN network [2] [4]. So, it is extremely important to apply security features along with the Northbound Interface to ensure that all the communications are secured. Enhancing the deployment and security against Northbound Interface attacks became a priority for many network Administrators [4]. With applying the Tor technique in SDN Controller, all the communications through Northbound APIs between SDN Controller and Application, this will make all the SDN Controller communications anonymous to have more security and privacy and be away from the attacks after multiple encryptions of the data and covering the packet's header that called "packet wrapper". In the result of anonymizing the transmitted packets. Tor is protecting communications against both eavesdropping and traffic analysis, and remove identifying information the data transmitting, and then having anonymity and privacy thus the communication can be more secured.

This paper will contain 4 sections: related work to review the recent researches of NBI security, the methodology used among this research, showing the experiment results and discussions.

II. Related work

Recent researches towards security the Northbound Interface ([5,6,7])shown efficient ways to secure this critical interface in the SDN networks.

First, Hien Do Hoang et al. [5]applied Blockchain technology to secure the NBI communication by using BlockAs (Novel Blockchain System). The functions of BlockAs is to provide Authentication, Authorization and Monitoring the Controller accessibility with characteristics of; unchangeable, decentralized, anonymity and audibility. Blockchain technology provides efficient security comparing with other technologies that show how the importance of privacy for each network to be secured. However, in this proposal, BlockAs applied complex modules of Blockchains with 7 steps to communicate, required database and additional fields to the Applications to allow users (permission fields). According to Radoslav Kobus's questions asked to BlockHunters CEO KamilGórski, says "Blockchains is more pseudonymous than being anonymous" (Nov 2019). This means the user who using Blockchain can be identified [8].

Also, Yuchia Tseng et al. [6], proposed a lightweight plugin called ControllerSEPA developed to secure and prevent SDN from five types of attacks; unauthorized access, illegal function calling, malicious rules injection, resources exhausting, man-in-the-middle attack. ControllerSEPA can eliminate these attacks only for small SDN network, the plugin needs the permissions from the Controller like verifying the digital signatures to apply actions, this will add another layer to the SDN the communication. Also, using a TLS protocol for the Communication between Application and Controller that may lead to the fingerprinting attack in the current SDN network. As mentioned, the Tor network will avoid the fingerprinting technique.

Lastly, SeyedBagher et al. [7]proposed the NTRU algorithm and the NSS digital signature for the security of NBI. This technique is providing the SDN network more powerful to the performance by increasing the speed, reducing the computing and power consumption in the SDN network. Also, it used Lattice-based cryptography that gives it more power than other methods. However, it has wrapping errors in the decryptions methods that provide plain texts, private keys and it can be exploited easily by the attackers [9].Its impacts of decryption failures cannot prove the security level without the knowledge of the private key [10].

Recent studies ([5,6])provide additional isolation to the SDN, which allows zero-days vulnerabilities in the communications of NBI. Another study [7]produces encryption using NTRU to secure the NBI communications that may face the traffics analysis even with the encryption applied [3]. After reviewing these researches, the proposed Architecture based on Tor network with SDN is efficient and effective on the NBI Interface Communications rather than the recently proposed solutions by providing Anonymous communication to avoid the information of the traffic can be gathered like amounts, length, incoming and outgoing of the Packets [3] and zero-day attacks. This will improve the security of the NBI communications by preventing it from all the possible attacks.

III. Research Methodology

This section will explain how the proposed Architecture of SDN based on Tor developed, traffic captured and show the initial results of the analysis. With the combination of Tor and SDN, the controller uses the Onion concept during communication with the Application as shown in Figure 1, this technique will allow it to have anonymity, privacy and security.

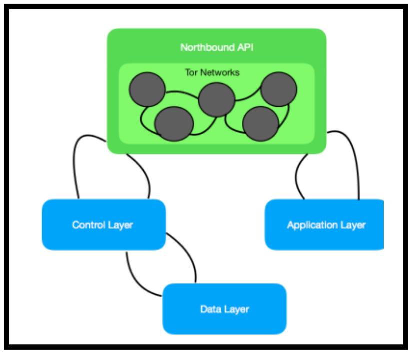


Figure 1: SDN based on Tor Architecture

A. Proposed NBI Communications

Northbound Interface using NETCONF protocol to automate the configuration of the SDN networks. It is based on Yang models that used in ODL applications to define NBI, the standards mechanism of the Web Applications, for accessing the network data, events configuration and notifications using the RESTCONF protocol that running over HTTP or HTTPS within the SDN network [11]. The RESTCONF protocol uses HTTP entities for message operations. Every single message of HTTP/HTTPS performs a single task [11]. The Request message is represented and identified as the operations, data or stream requested by the Administrator from the Controller to the Application that usually applied for data resources.

The purpose of the Response message is to provide the requested resources to the controller, this message contains descriptions of the data. So, with the operation of Tor and NETCONF in NBI, the SDN network will have multiple nodes within NBI that used Tor techniques to cover the connections and interactions of the Network Administrator. Using an onsurf tool to anonymize the network, enabling the Transparent Proxy by configuring IPv4 virtual network address, Socks, DNS. Transparent Proxy is redirecting the Requests and Responses messages without modifying them. All these configured as the:

kali-anonsurf/kali-anonsuf-deb-src/etc/tor/torrc.anon as:

```
    VirtualAddNetwork 10.192.0.0/10

    AutomapHostsOnResolve 1

    TransPort   9040

    SocksPort 9050

    DNSPort   53

RunAsDeamon 1
```

The above lines are shown Tor configuration. It provides a range of IP addresses (10.192.0.0./10) to the Tor network and it will assign unused IPs to use them for communication purposes, lookup for the requests, combination of Transparent and Socks Proxies connections via 9040 and 9050 ports. The Controller running as a Daemon (Background process of Tor traffics). The anonymity in the proposed SDN Architecture depends on the numbers of nodes or relays connected.

As shown below in Figure 3 and Figure 4, we assumed the Tor networks have only 3 nodes. During the communication of the Controller and Application contains Request Messages from ODL to the Dlux and Response Messages from the Dlux to the ODL through the NBI using application protocol. The diagrams showed the activities of the Request and Response Messages. These two diagrams will provide a better view of the proposed Architecture and understand the operation principle of it.

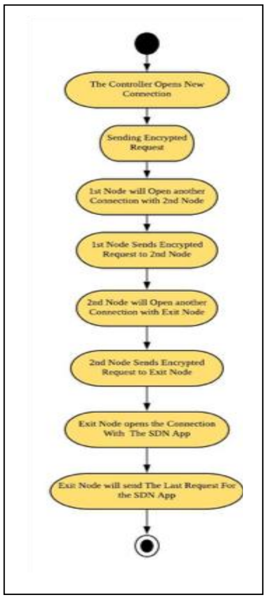

The Controller Opens New Connection
Sending Encrypted Request
1st Node will Open another Connection with 2nd Node
1st Node Sends Encrypted Request to 2nd Node
2nd Node will Open another Connection with Exit Node
2nd Node Sends Encrypted Request to Exit Node
Exit Node opens the Connection With The SDN App
Exit Node will send The Last Request For the SDN App

Figure 2: Request Message

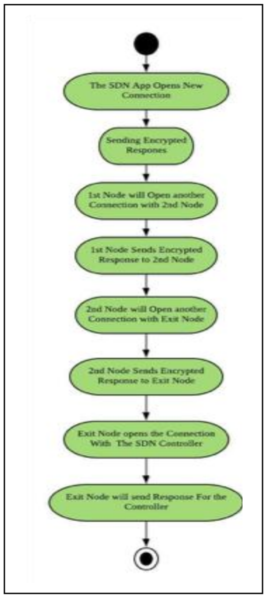

The SDN App Opens New Connection
Sending Encrypted Respones
1st Node will Open another Connection with 2nd Node
1st Node Sends Encrypted Response to 2nd Node
2nd Node will Open another Connection with Exit Node
2nd Node Sends Encrypted Response to Exit Node
Exit Node opens the Connection With The SDN Controller
Exit Node will send Response For the Controller

Figure 3: Response Message

B. *Experiment Setup*

This experiment running on the virtual environment and the physical host, the physical host is controlling the virtual environment. It is developed with setting up with the virtual environment through visualization software to apply virtual Operating Systems and network with required installations, configurations, implementations, operations and testing which are done on macOS (Host) using VMware Fusion to run VMs (Open Daylight Controller) and GNS3 network emulator that interact with VMs. As illustrated in Figure 4, will describe how the physical host interacting and linking to the virtual environment. During the setting up of the environments, installing the required VMs using VMware Fusion Professional Version 11.0.2 to install Ubuntu Linux 64-bit 18.04.2 as an SDN controller using the Open Source Controller (Open Daylight version Lithium 0.3.0) with multiple network adapters (vmnets). Also, GNS3 version 2.1.18 to build the SDN network and pulling OpenvSwitch (OVS) from Docker containers to the GNS3 network, will support and provides OpenFlow protocol. Another VM called GNS3 VM that runs to provide interaction between the virtual network and the virtual machines (GNS3 and VMware Fusion). Besides, Installing Wireshark version 3.0.2 for traffic filtering and analysis purposes on the physical host. After the ODL installed and installing the required features to run the Dlux application and install the security packages to apply Tor service by download "anonsurf" through Terminal on Ubuntu that will anonymize the entire system under Tor network within the ODL controller and Dlux application.

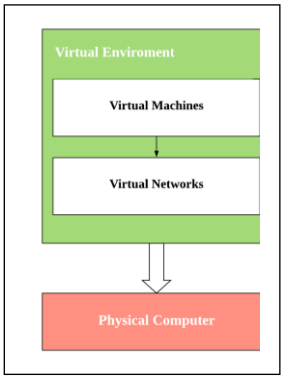


Figure 4: Experiment Setup

C. *Traffic Capture*

After the experiment setup, the virtual machines and virtual network are connected through GNS3 and VMware Fusion software. In this part of the research, we will capture the packets of the virtual network (vmnet) between the ODL Controller and Dlux Application using open source packet analysis Wireshark installed on the physical host.

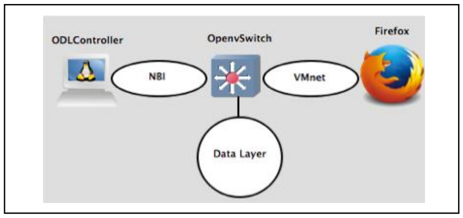


Figure 5: Network Topology

Figure 5 shows the network topology and how each network element is connected. In this experiment, we have used Firefox to access the Dlux Application via vmnet to OVS before reach to the ODL. Then, capturing the vmnet during the communication.

D. *NBI Traffics Analysis*

The captured traffic from vmnet has been analyzed and filtered to intercept and examine all the messages to collect the information patterns of the communications by using the below list of filtering expressions for both current and proposed SDN Architectures:

- *Current SDN Architecture*

Filtering all the TCP communications, IN and OUT Packets between Controller and Applications used the HTTP protocol:

```
ip.dst == 192.168.133.227 and

ip.src == 192.168.133.166 and http.
```

Filtering the communications by following the HTTP protocol data stream rule:

```
tcp.stream == 2
```

- *SDN Architecture based on Tor*

Filtering all the indirect communications between Controller and Applications used the below rule, shows the Flow Graph, IN and OUT Packets;

```
ip.dst == 192.168.133.229 or

ip.src == 192.168.133.234
```

Filtering Tor Traffics that use TLS protocol and 9001 port;

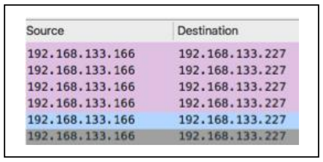
```
tls and tcp.port == 9001
```

IV. Results and Discussion

After all the required implementation is done for this experiment, we will show and discuss the comparison of the traffics captured & findings in two experiments, that is, proposed and the current NBI communications, view the results, review the anonymous communication and evaluate it toward STRIDE threat model.

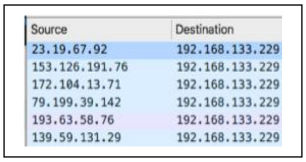
A. NBI Communications *Captured*

In this part of the paper, we will compare and discuss the NBI communication based on three main elements; IP Addresses, Protocols, Port numbers review and discuss the statistical information of NBI traffics during the Communications. The next Figures 6 and 7, it will show the IP Addresses in both Communications of NBI.



Source	Destination
192.168.133.166	192.168.133.227
192.168.133.166	192.168.133.227
192.168.133.166	192.168.133.227
192.168.133.166	192.168.133.227
192.168.133.166	192.168.133.227
192.168.133.166	192.168.133.227

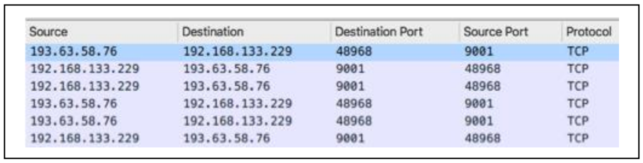
Figure 6: Current NBI IPs



Source	Destination
23.19.67.92	192.168.133.229
153.126.191.76	192.168.133.229
172.104.13.71	192.168.133.229
79.199.39.142	192.168.133.229
193.63.58.76	192.168.133.229
139.59.131.29	192.168.133.229

Figure 7: Tor NBI IPs

In the current NBI, the communication is direct that shows only two IP addresses; the controller 192.168.133.227 and the Firefox Browser; 192.168.133.166 (Source and Destination). However, the communication in the proposed NBI based on the Tor network is indirect that only show the IP Address of the controller; 192.168.133.229 and other multiple IP addresses of Tor Nodes, the data transmitting will encrypt and decrypt with changing of the IP address in each visited node.



Source	Destination	Destination Port	Source Port	Protocol
193.63.58.76	192.168.133.229	48968	9001	TCP
192.168.133.229	193.63.58.76	9001	48968	TCP
192.168.133.229	193.63.58.76	9001	48968	TCP
193.63.58.76	192.168.133.229	48968	9001	TCP
193.63.58.76	192.168.133.229	48968	9001	TCP
192.168.133.229	193.63.58.76	9001	48968	TCP

Figure 8: Tor Traffics

As shown in Figure 8, the traffic use TLS protocol and work over the TCP protocol during the communication between the Controller with the IP destination 192.168.133.254 of Ubuntu Linux Server, it uses these IPs and Port number 9001 that is known for Tor traffics. Also, the Dlux Application with port 8181 and port 6633 for the handshake of end-end communications. The operations of TLS over TCP using 443 port and other random port numbers like 48968 and random IPs such as 193.63.58.76 that indicates Web-Services of SDN are using Tor traffics to perform the requested actions by the Controller.

Tor traffic consuming more bits than other networks during the transmissions due to its nodes are used in the data flows. The following Figures 9 and 10 shows the data flow in both Architecture and how each node interacts with others. Figures explains the TCP flow, IPs involved in both communications, Ports and the purpose of the interaction between each node.

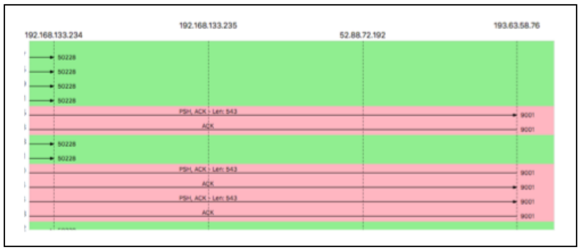


Figure 9. Data Flow of TCP in SDN based Tor

As we noticed, the Tor network has more IPs or nodes that are unknown (Figure 9) and the existed network has limited and known IPs (Figure 10) in the data flow.

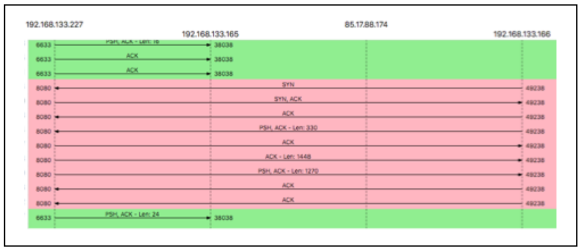


Figure 10. Data Flow of TCP in existed SDN

Figure 11 and 12 shows the I/O of the packets in SDN Architecture based on Tor and compare it with the normal data transmissions in the existed SDN Architecture.

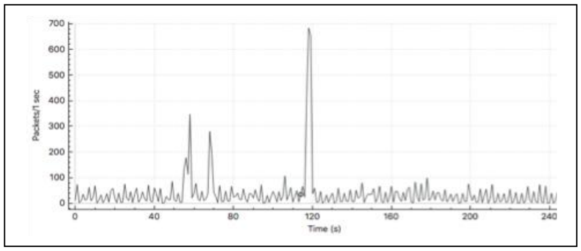


Figure 11. I/O Packets of the SDN based Tor

As Figure 11 has shown the I/O packets within the SDN Architecture based on the Tor network, we noticed that it is using many nodes to reach the destinations. The average of 60 to 70 I/O Packets per second. But the Figure 12, the existed SDN Architecture, the average of 20 to 30 I/O Packets per second.

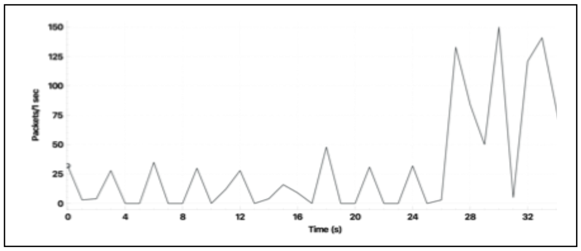


Figure 12. I/O Packets of the existed SDN

B. Final Results

With the combination of SDN and Tor networks, will provide anonymity to the network and prevent it from many threats and attacks. This section will also discuss and describe the STRIDE threats modelling to categorize and identify the threats in NBI as Table 1 has shown. With all the operations of NBI, after anonymized all the controller's communications the STRIDE model that categorizes and identified the threats into six Category Threats and Security model for Mitigations ([12,13]):

Table 1. STRIDE Threats Model

Category Threat	***Security Property***
Spoofing	Authentication
Tampering	Integrity
Repudiation	Non-repudiation
Information Disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

1. Spoofing: The ODL controller must identify and authenticate any users in the network and ensure only the authenticated users can enter the network to avoid spoofing attacks. These authenticators will use Tor to hide their actual IP Addresses. If the authentication not applied or it is weak, this may lead the attacker to use the credentials to authenticate himself to the controller. The authentication and unknown IP addresses applied within the ODL to access the Applications will help to prevent the attackers to listen, monitor or watching the traffic in the network by spoofing attacks of IP, ARP spoofing and others.

2. Tempering: Tor used multiple nodes that packets passed through the NBI before reaching to the Applications, that is will provide integrity to avoid the modification of the data sent over the network. The unknown sender and receiver will make the attackers confused to apply tempering attacks to the important data whether destroying or modifying that called Man-in-The-Middle-Attack. For example, attackers exploit the vulnerability to delete flows.

3. Repudiation: Always the attackers working hard to hide their activities to avoid the detection of the attacks. They use many techniques to repudiate their actions by deleting logs or spoofing another identity of the user. with multiple and strong encryptions methods used by Tor to make the source log of the NBI unknown, this is important to prevent this kind of attack.

4. Information Disclosure: The information that sent over the network can be sensitive or non-sensitive but it is highly valuable to the attackers to analysis it and trying to find vulnerabilities from it (fingerprinting), this may lead to the data breach in the system such as, scanning the physical memory of the controller to extract flow rules. This can be protected by using Tor.

5. Denial of Service: Another attack that hackers concern about shut down the system and trying to conflict the services provided in many ways like applying DDoS against the Controller or the services provided. In this case, the challenge is the availability of the system or network. So, with applied Tor network will make the Controller anonymous and then the attacker cannot or difficult determine the target to apply these kinds of attacks.

6. Elevation of Privilege: This related to other STRIDE model parts Tempering and Spoofing. The Dlux Application and other SDN Applications have their own privilege for the Administrator for the operations needed in the network like network topology, statistics information, network devices, and other operations but some other Administrator having more privilege of network configurations. In this case, the authorization and Tor is the best security to avoid attacks by given multiple IP addresses to the Controller.

The existing SDN network has several solutions to overcome the lack of security in Northbound Interface like ([5, 6,7, 14,15]). Many researchers produced security solutions within NBI that applied many encryption protocols to have a high level of security with consideration of the isolation in SDN. But these days, applying the encryptions, authentication and authorization are not enough to protect the network from the attacks. Hackers are going forward to collects network information instead of breaking the encryption connections ([3,16]). Even different vendors of the SDN controller are still working in the NBI security based on STRIDE. But with using Tor, it provides an additional layer of security and the chance of gathering information about the network minimizes because of the anonymizing of the SDN system with self-authentication. Tor uses multiple layers of TLS encryptions and streams integrity checking over TCP instead of working with UDP to provide more reliability as its transport protocol with 443 TLS port that known as Tor traffic. In addition, TLS requires all the data to be received to avoid recovering of corruption, dropped or lost packets. It is handling with the multiplex TCP and Socks proxies over circuits within the Application to ensure the anonymity of both Request and Response messages, Nguyen Phong Hoang et al. used Tor-based anonymous communication approach to prevent the IoT devices from possible attacks [17].

As a result, Tor providing an anonymous SDN controller for network communications is extremely important these days, especially with the growth of the cyber-attacks. In this paper, the proposed solution could serve to be a new method of cyber defence against the threats and attacks whether known or unknown within the NBI by made the communications anonymous that be more difficult to the hackers to determine the targets. Tor gives anonymity that can be the protection against strong, weak or zero-days attacks that is used by hackers, helps to prevent watching on the transmitted data and monitoring the habits or behaviours thereby making difficult to fingerprinting the system during the communication between Controller and Applications, block and avoid any third party trackers through the network traffic of the Administrator and producing multi-layers of encrypted traffics, multiple IP and MAC addresses that passed over the distributed network with identification of both connection side.

V. CONCLUSION

This paper is considered as the first step towards using a combination of the Tor technique and the SDN network. The paper starts with a brief introduction about SDN networks, architecture lacks security within NBI communication and how Tor can overcome this lack by providing anonymity network. Then it discusses recent research in NBI security. The methodology followed in this paper contains the design and implementation of the proposed security solution that explain operations and the virtual environment used to apply the experiment. Lastly, comparison and discussion on the NBI in both proposed and current architectures shows the results and findings of the experimental research. In future work, we look forward to the contribution of Open Daylight and Tor communities to develop and work on this project by providing it's Tor private instead of using structured way for the traffic to enhance the Northbound Interface security.

VI. References

[1] Dargin, M. 2018. Secure your SDN controller. Network World.

[2] Singh,D. and Kumar,S. 2019.Software Defined Networking (SDN) Challenges, issues and Solution. International journal of computer sciences and engineering, 7(1):884-889.

[3] Cao, J., Yang, Z., Sun, K., Li,Q., Xu,M. and. Han, P. 2019. Fingerprinting SDN Applications via Encrypted Control Traffic. Beijing, China: 22nd International Symposium on Research in Attacks, Intrusions and Defences.

[4] Hogg, S. 2014. SDN Security Attack Vectors and SDN Hardening. Network World.

[5] Do Hoang,H., Phan,D.and Pham,V. 2019.A Security-Enhanced Monitoring System for Northbound Interface in SDN using Blockchain. The Tenth International Symposium.

[6] Tseng,Y., Zhang,Z. and Nait-Abdesselam,F. 2016.ControllerSEPA: A Security-Enhancing SDN Controller Plug-in for OpenFlowApplications. 17th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT).

[7] Bagher,S., Natanzi,S. and Majma,M. 2017.Secure Northbound Interface for SDN Applications with NTRU Public KeyInfrastructure. Tehran, Iran: 4th International Conference on Knowledge-Based Engineering and Innovation (KBEI-2017).

[8] Kobus, R. 2019. Could the Blockchain Provide True Anonymity? Retrived from: Hackernoon.com. Last Accessed Date: 15 February, 2020.

[9] Meskanen, T. And Renvall, A. 2006. A wrap error attack against NTRUEncrypt. Discrete Applied Mathematics. Vol-154(2).

[10] Howgrave-Graham,N., Nguyen,P.Q., Pointcheval,D. and Proos,J.2003. the Impact of Decryption Failure on the Security OF NTRU encryption. 23rd Annual International Cryptology Conference.

[11] Bierman, A., YumaWorks, Bjorklund, M. 2014. Tail-f Systems. Watsen, Juniper Networks, Fernando R. and Cisco. 2014 RESTCONF Protocol.

[12] Laan, J.J. 2015. Securing the SDN northbound interface with the AID of anomaly detection. Master Research Report submitted Faculty of Science, University of Amsterdam. Retrived from: https://delaat.net/rp/2014-2015/p73/report.pdf.

[13] Ruffy,F., Hommel,W. and von Eye,F. 2016.A STRIDE-based Security Architecture for Software-Defined Networking. ICN2016: The Fifteenth International Conference on Networks.

[14] Oktian,Y.E., Lee, S.G., Lee, H.J. and Lam,J.H. 2015. Secure your Northbound SDN API. 2015 Seventh International Conference on Ubiquitous and Future Networks, Sapporo.

[15] Weng,J., Weng,J., Zhang,Y., Luo,W. and Lan,W., 2019"BENBI: Scalable and Dynamic Access Control on the Northbound Interface of SDN-Based VANET," in IEEE Transactions on Vehicular Technology, vol. 68, no. 1, Jan.

[16] Cui,H., Karame,G.O., Klaedtke,F. and Bifulco,R.2016.On the Fingerprinting of Software-Defined Networks. in IEEE Transactions on Information Forensics and Security.11(10), Oct.

[17] Hoang,N.P. and Pishva,D.2015.A TOR-based anonymous communication approach to secure smart home appliances. 2015 17th International Conference on Advanced Communication Technology (ICACT), Seoul.