(12) INNOVATION PATENT (11) Application No. **AU 2021103338 A4**
(19) AUSTRALIAN PATENT OFFICE

(54) Title
A METHOD FOR DETERMINING THE INDIVIDUAL AND MUTUAL RELATIONSHIP AMONG THE VULNERABILITIES OF SDN ENTITIES

(51) International Patent Classification(s)
H04L 41/28 (2022.01)

(21) Application No: **2021103338** (22) Date of Filing: **2021.06.14**

(45) Publication Date: **2022.03.24**
(45) Publication Journal Date: **2022.03.24**
(45) Granted Journal Date: **2022.03.24**

(71) Applicant(s)
Sudipta Roy

(72) Inventor(s)
Roy, Sudipta;Deb, Raktim

(74) Agent / Attorney
Sudipta Roy, Parcel Locker 1013253411 Shop 355 111 West Lakes Boulevard, West Lakes, SA, 5021, AU

2021103338 14 Jun 2021

ABSTRACT

The present disclosure relates to a method for determining the individual and mutual relationship among the vulnerabilities of SDN entities. The present disclosure presents the mathematical representation of Bayesian network methodology in the SDN environment for identifying the status of different entities while mutual exploitations take place for violating the network system. The CVSS is used in the first place to demonstrate the vulnerabilities and then the mutual relationship between the vulnerabilities are identifies using Bayesian network methodology. The first aim of this disclosure is to determine proper conditions to relate the CVSS for the SN entities and set the local conditional probabilities for each entity of SDN and then the use of Bayesian network us explored to determine the mutual relationship among the vulnerabilities of SDN entities.

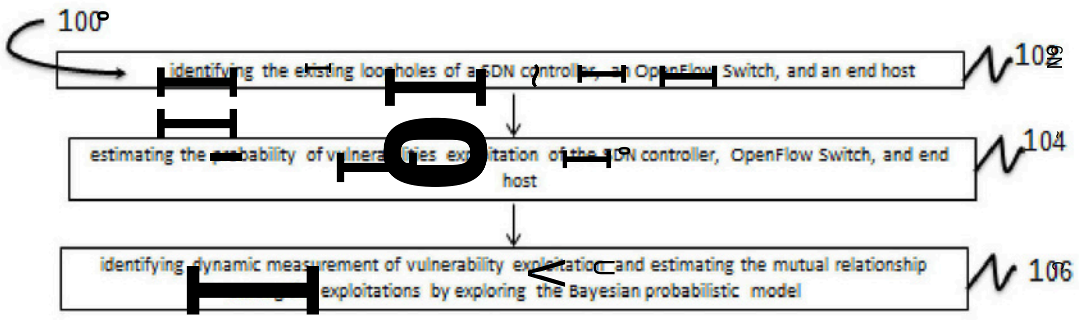

100
identifying the existing loopholes of a SDN controller, an OpenFlow Switch, and an end host
102
estimating the probability of vulnerabilities exploitation of the SDN controller, OpenFlow Switch, and end host
104
identifying dynamic measurement of vulnerability exploitation and estimating the mutual relationship
exploitations by exploring the Bayesian probabilistic model
106

Figure 1

A METHOD FOR DETERMINING THE INDIVIDUAL AND MUTUAL RELATIONSHIP AMONG THE VULNERABILITIES OF SDN ENTITIES

FILED OF THE INVENTION

The present disclosure relates to a method for determining the individual and mutual relationship among the vulnerabilities of SDN entities.

BACKGROUND OF THE INVENTION

SDN provides better flexibility, programmability, cost-effective, and on demand configuration control over the network resources as well as network architecture, but despite of having so many benefits there are many major security issues with SDN. To address these issues there are several researches but these researches do not support the vulnerabilities and risks that exist in different SDN entities. These risks may lead to serious impact on the organizational networking system.

A common vulnerability scoring system is used for measuring the risk of networking services of an organization. But the problem with this scoring system is that it only determines the risk with individual entity of a networking system and on the top of that it also don't gives a proper justification to relate this scoring system to SDN. The probability of individual vulnerabilities can be mutual or joint to compromise critical resources, and ignorance of such situation can be dangerous to any organization.

In one existing solution a security analysis of communication between OpenFlow switch and controller using STRIDE and Attack tree modeling method. In another existing solution, an migration scheme has been proposed, the scheme identifies the difference between the flow entropy and mean entropy of flow entries of a given node and compares with the threshold value to diminish the DoS attack. In another existing solution, an algorithm has been proposed for detecting and defending the DoS attack using switch port statistics analysis and identifying the attacking source. For the control plane attack, FlowRanger which is a buffer prioritizing solution for controllers to handle the routing request based on their likelihood to be attacking requests, and for this the service quality of any legitimate hosts will not be undermined during a DoS assault in SDN. In one prior art solution (KR101692155B1), the invention relates to a method for analyzing a vulnerability of a SDN network, and a control channel category, and acquiring a vulnerability database including an attack code for the vulnerability.

In another prior art solution (US9240976B1), the invention relates to providing security monitoring in computer network, more particularly, a service accessible via a network port of a network node within the network is identified. However, there are various existing solution regarding the countermeasures for illegal access of network resources but all the countermeasures are much focused on threat domains and none of the research showed individual vulnerabilities of SDN entities. Therefore there is a need for a method for determining the individual and mutual relationship among the vulnerabilities of SDN entities.

SUMMARY OF THE INVENTION

The present disclosure relates to a method for determining the individual and mutual relationship among the vulnerabilities of SDN entities. The present disclosure presents the mathematical implementation of Bayesian network methodology in the SDN environment for identifying the status of different entities while mutual exploitations take place for violating the network system. The intention of the current disclosure is to determine proper conditions to relate the CVSS for the SDN entities and set the local conditional probabilities for each entity of SDN and to use of a Bayesian network to determine the mutual relationship among the vulnerabilities of SDN entities. Initially the identification of the existing loopholes of SDN switch and control plane from SDN open standard and then estimation of likelihood of exploitation is done. To estimate the dynamic changes the concept of Bayesian network is adopted.

The present disclosure seeks to provide a method for determining the individual and mutual relationship among the vulnerabilities of SDN entities. The method comprises: identifying the existing loopholes of a SDN controller, an OpenFlow Switch, and an end host; estimating the probability of vulnerabilities exploitation of the SDN controller, OpenFlow Switch, and end host; and identifying dynamic measurement of vulnerability exploitation and estimating the mutual relationship among the exploitations by exploring the Bayesian probabilistic model.

An objective of the present disclosure is to a method for determining the individual and mutual relationship among the vulnerabilities of **SDN** entities.

Another object of the present disclosure is to demonstrate the vulnerabilities of **SDN** entities using **CVSS.**

Another object of the present disclosure is to identify the mutual relationship between the vulnerabilities using Bayesian network methodology.

Another object of the present disclosure is to determine proper conditions to relate the **CVSS** for the **SDN** entities and set the local conditional probabilities for each and every entity of **SDN.**

Another object of the present disclosure is to identify the existing loophole of **SDN** switch and control plane from **SDN** open standard and estimate the likelihood of estimation.

To further clarify advantages and features of the present disclosure, a more particular description of the invention will be rendered **by** reference to specific embodiments thereof, which is illustrated in the appended drawings. It is appreciated that these drawings depict only typical embodiments of the invention and are therefore not to be considered limiting of its scope. The invention will be described and explained with additional specificity and detail with the accompanying drawings.

BRIEF DESCRIPTION OF FIGURES

These and other features, aspects, and advantages of the present disclosure will become better understood when the following detailed description is read with reference to the accompanying drawings in which like characters represent like parts throughout the drawings, wherein:

Figure 1 illustrates a flow chart of a method for determining the individual and mutual relationship among the vulnerabilities of **SDN** entities in accordance with an embodiment of the present disclosure;

Figure 2 illustrates an Attack scenario in **SDN** in accordance with an embodiment of the present disclosure;

Figure 3 illustrates an attack graph for network attack in accordance with an embodiment of the present disclosure;

Figure 4 illustrates an updated exploitability metric for SDN in accordance with an embodiment of the present disclosure;

Further, skilled artisans will appreciate that elements in the drawings are illustrated for simplicity and may not have been necessarily been drawn to scale. For example, the flow charts illustrate the method in terms of the most prominent steps involved to help to improve understanding of aspects of the present disclosure. Furthermore, in terms of the construction of the device, one or more components of the device may have been represented in the drawings by conventional symbols, and the drawings may show only those specific details that are pertinent to understanding the embodiments of the present disclosure so as not to obscure the drawings with details that will be readily apparent to those of ordinary skill in the art having benefit of the description herein.

illustrate to help to improve

DETAILED DESCRIPTION

For the purpose of promoting an understanding of the principles of the invention, reference will now be made to the embodiment illustrated in the drawings and specific language will be used to describe the same. It will nevertheless be understood that no limitation of the scope of the invention is thereby intended, such alterations and further modifications in the illustrated system, and such further applications of the principles of the invention as illustrated therein being contemplated as would normally occur to one skilled in the art to which the invention relates.

It will be understood by those skilled in the art that the foregoing general description and the following detailed description are exemplary and explanatory of the invention and are not intended to be restrictive thereof.

Reference throughout this specification to “an aspect”, “another aspect” or similar language means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment of the present disclosure. Thus, appearances of the phrase “in an embodiment”, “in another embodiment” and similar language throughout this specification may, but do not necessarily, all refer to the same embodiment.

The terms "comprises", "comprising", or any other variations thereof, are intended to cover a non-exclusive inclusion, such that a process or method that comprises a list of steps does not include only those steps but may include other steps not expressly listed or inherent to such process or method. Similarly, one or more devices or sub-systems or elements or structures or components proceeded by "comprises...a" does not, without more constraints, preclude the existence of other devices or other sub-systems or other elements or other structures or other components or additional devices or additional sub-systems or additional elements or additional structures or additional components.

Unless otherwise defined, all technical and scientific terms used herein have the same meaning as commonly understood by one of ordinary skill in the art to which this invention belongs. The system, methods, and examples provided herein are illustrative only and not intended to be limiting.

Embodiments of the present disclosure will be described below in detail with reference to the accompanying drawings.

Figure 1 illustrates a flow chart of a method for determining the individual and mutual relationship among the vulnerabilities of SDN entities in accordance with an embodiment of the present disclosure. At step 102 the method 100 includes, identifying the existing loopholes of a SDN controller, an OpenFlow Switch, and an end host.

At step 104 the method 100 includes, estimating the probability of vulnerabilities exploitation of the SDN controller, OpenFlow Switch, and end host. There is a lack of trust between the controller and application running on it and this may lead to the open door for modifying the network behavior and get control over the controller activity, this indicated the existing exploits in SDN controller and in this circumstances the probability of exploitation of a SDN controller is $Pr(\mathrm{E}) = 0.97$, wherein AV = Network, AC = Low, PR and UI are none. The SDN controller may be exploited for failing to scale its computing resources and this may lead to resource saturation attack, in this case the probability of exploitation of SDN controller will be $\mathrm{Pr(E)} = 0.71$, wherein AV = Network, AC=Low, PR = None and UI = Required. The OpenFlow switch is used for packet movement only without verifying its authenticity, this creates a big problem cause the switch doesn’t provide a standard for Transport layer security and the input buffer receives untrusted data. This can cause DoS attack in the switch, since the switch are not scalable and input buffer remains buffered until controller made a decision about the received packet. This may lead to switch-to-controller attack if multiple switches are engaged in the exploitation in a similar manner. The vulnerabilities points suggest that the OpenFlow switch attack complexity is low, privilege is not required and use interaction is required. The attack complexity introduces three different cases network attack, adjacent network attack, and local attack. Wherein in the network attack the probability of exploitation will be Pr(E) = 0.71, where AV = Network, AC = Low, PR = None and UI = Required, in the case of adjacent attack the probability of exploitation will be Pr(E) = 0.52, where AV = Adjacent Network, AC = Low, PR = None and UI = Required, and in the case of local attack the probability of exploitation will be Pr(E) = 0.46, where AV = Local, AC = Low, PR = None and UI = Required. The end host is equally probable of exploitation and the probability of exploitation is given by switch exploitation divided by number of active end host.

At step 106 the method 100 includes, identifying dynamic measurement of vulnerability exploitation and estimating the mutual relationship among the exploitations by exploring the Bayesian probabilistic model. In Bayesian network each node is considered as Bernoulli random variable and a conditional probability table for the end host is represented. The conditional probability table can be obtained by the casual dependency of states of the parents and to obtain this, AND decomposition is used when multiple parents need to be compromised and OR decomposition is used when at least one parent need to be compromised to read the goal state. The prior and post probability conditions are computed resulting from mutual exploitation of vulnerability, wherein the prior probability accounts the mutual relationship between exploitation and represents a cumulative score and the post probability determines the current status of the OpenFlow switch in the controller due to changes in contributing factor or event of attack occurrence.

Figure 2 illustrates an Attack scenario in SDN in accordance with an embodiment of the present disclosure. This image illustrates 4 different attacks, controller saturation attack, network attack, adjacent network attack, and local network attack. The controller saturation attack is when any host which is connected to switch tries to exploit the controller. The network attack is where switches are involved in the exploitation of the controller and generate switch-to-controller link saturation. The probability of exploitation Pr (E) = 0.71, where AV = Network, AC = Low, PR = None and UI = Required. In the adjacent network attack a connected switch may try to exploit another switch in the same network. The probability of exploitation Pr (E) = 0.52, where AV = Adjacent Network, AC = Low, PR = None and UI = Required. In the local network attack any host connected to a switch tries to exploit the same switch for making resources unavailable for other hosts. However the probability of this scenario is rare, as no one tries to exhaust own resources. In this case, the probability of exploitation will be Pr(E) = 0.46, where AV = Local, AC = Low, PR = None and UI = Required.

Figure 3 illustrates an attack graph for network attack in accordance with an embodiment of the present disclosure. The figure illustrates an attack graph and corresponding conditional probability table. For estimating the mutual relationship among the exploitations, the concept of Bayesian belief probabilistic networks has been adopted. Each node of the attack graph represents a host with a specific violation state and also represents partial beliefs under conditions of uncertainty. In our case each node represents an SDN entity with a specific vulnerability.

Figure 4 illustrates a table of updated exploitability metric for SDN in accordance with an embodiment of the present disclosure. The table clearly shows that any unusual activity begins in the network when the OpenFlow status crosses the limit 0.648 under the mutual relationship among the vulnerabilities of SDN entities.

The drawings and the forgoing description give examples of embodiments. Those skilled in the art will appreciate that one or more of the described elements may well be combined into a single functional element. Alternatively, certain elements may be split into multiple functional elements. Elements from one embodiment may be added to another embodiment. For example, orders of processes described herein may be changed and are not limited to the manner described herein. Moreover, the actions of any flow diagram need not be implemented in the order shown; nor do all of the acts necessarily need to be performed. Also, those acts that are not dependent on other acts may be performed in parallel with the other acts. The scope of embodiments is by no means limited by these specific examples. Numerous variations, whether explicitly given in the specification or not, such as differences in structure, dimension, and use of material, are possible. The scope of embodiments is at least as broad as given by the following claims.

Benefits, other advantages, and solutions to problems have been described above with regard to specific embodiments. However, the benefits, advantages, solutions to problems, and any component(s) that may cause any benefit, advantage, or solution to occur or become more pronounced are not to be construed as a critical, required, or essential feature or component of any or all the claims.

2021103338 14 Jun 2021

WE CLAIM

1. A method for determining the individual and mutual relationship among the vulnerabilities of SDN entities, the method comprises:

   identifying the existing loopholes of a SDN controller, an OpenFlow Switch, and an end host;

   estimating the probability of vulnerabilities exploitation of the SDN controller, OpenFlow Switch, and end host; and

   identifying dynamic measurement of vulnerability exploitation and estimating the mutual relationship among the exploitations by exploring the Bayesian probabilistic model, and wherein an exploitability metric is composed of attack vector (AV), attack complexity (AC), privilege required (PR), and user interaction (UI).

2. The method as claimed in claim 1, wherein there is a lack of trust between the controller and application running on it and this may lead to the open door for modifying the network behavior and get control over the controller activity, this indicated the existing exploits in SDN controller and in this circumstances the probability of exploitation of a SDN controller is *Pr*(E) = 0.97, wherein AV = Network, AC = Low, PR and UI are none.

3. The method as claimed in claim 1, wherein the SDN controller may be exploited for failing to scale its computing resources and this may lead to resource saturation attack, in this case the probability of exploitation of SDN controller will be Pr(E) = 0.71, wherein AV = Network, AC=Low, PR = None and UI = Required.

4. The method as claimed in claim 1, wherein the OpenFlow switch is used for packet movement only without verifying its authenticity, this creates a big problem cause the switch doesn’t provide a standard for Transport layer security and the input buffer receives untrusted data. This can cause DoS attack in the switch, since the switch are not scalable and input buffer remains buffered until controller made a decision about the received packet. This may lead to switch-to-controller attack if multiple switches are engaged in the exploitation in a similar manner.

5. The method as claimed in claim 5, wherein vulnerabilities points suggest that the OpenFlow switch attack complexity is low, privilege is not required and use interaction is required.

6. The method as claimed in claim 6, wherein the attack complexity introduces three different cases network attack, adjacent network attack, and local attack. Wherein in the network attack the probability of exploitation will be Pr(E) = 0.71, where AV = Network, AC = Low, PR = None and UI = Required, in the case of adjacent attack the probability of exploitation will be Pr(E) = 0.52, where AV = Adjacent Network, AC = Low, PR = None and UI = Required, and in the case of local attack the probability of exploitation will be Pr(E) = 0.46, where AV = Local, AC = Low, PR = None and UI = Required.

7. The method as claimed in claim 1, wherein the end host is equally probable of exploitation and the probability of exploitation is given by switch exploitation divided by number of active end host, wherein a Bayesian network can be defined by two major properties directed acyclic graph and set of conditional probability distribution, and wherein each node is considered as Bernoulli random variable and a conditional probability table for the end host is represented.

8. The method as claimed in claim 7, wherein the conditional probability table can be obtained by the casual dependency of states of the parents and to obtain this , AND decomposition is used when multiple parents need to be compromised and OR decomposition is used when at least one parent need to be compromised to read the goal state.

9. The method as claimed in claim 1, wherein the prior and post probability conditions are computed resulting from mutual exploitation of vulnerability, and wherein the prior probability accounts the mutual relationship between exploitation and represents a cumulative score, wherein the cumulative score derived from the combination of one or multiple exploits.

10. The method as claimed in claim 9, wherein the post probability determines the current status of the OpenFlow switch in the controller due to changes in contributing factor or event of attack occurrence.

11

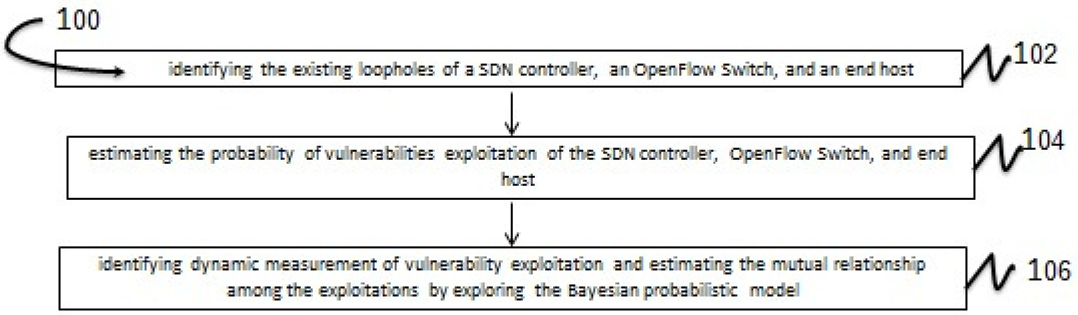

100
identifying the existing loopholes of a SDN controller, an OpenFlow Switch, and an end host
102
estimating the probability of vulnerabilities exploitation of the SDN controller, OpenFlow Switch, and end host
104
identifying dynamic measurement of vulnerability exploitation and estimating the mutual relationship among the exploitations by exploring the Bayesian probabilistic model
106

Figure 1

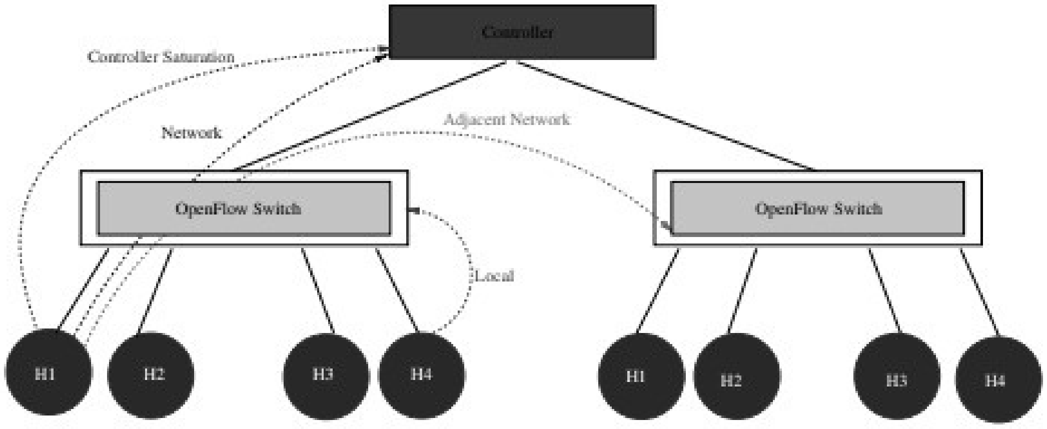
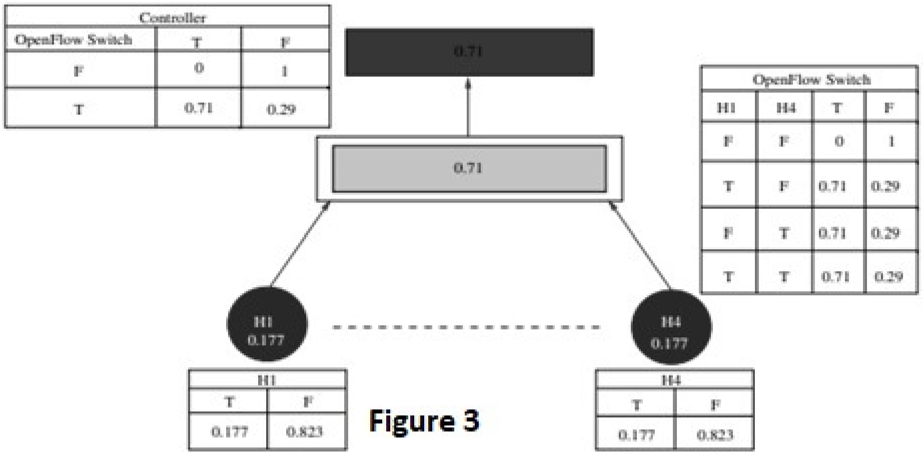

Controller
Controller Saturation
Network
Adjacent Network
OpenFlow Switch
OpenFlow Switch
Local
H1
H2
H3
H4
H1
H2
H3
H4

Figure 2



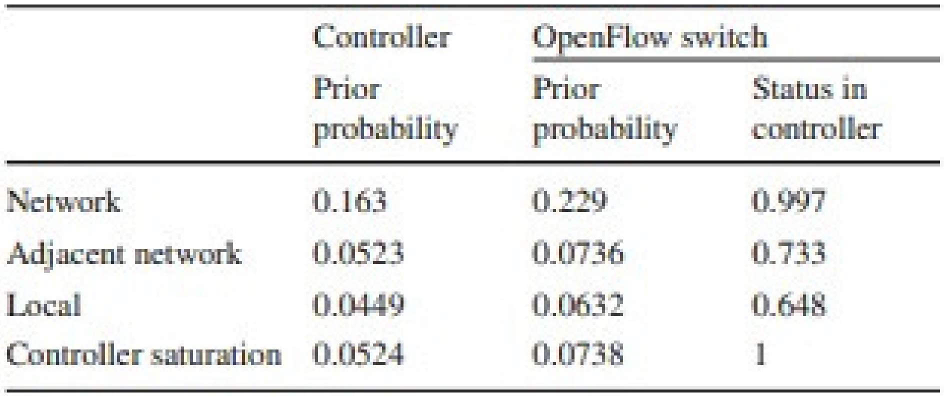
Controller		
OpenFlow Switch	T	F
F	0	1
T	0.71	0.29

OpenFlow Switch			
H1	H4	T	F
F	F	0	1
T	F	0.71	0.29
F	T	0.71	0.29
T	T	0.71	0.29

H1	
T	F
0.177	0.823

H4	
T	F
0.177	0.823

Figure 3



	Controller	OpenFlow switch	
	Prior probability	Prior probability	Status in controller
Network	0.163	0.229	0.997
Adjacent network	0.0523	0.0736	0.733
Local	0.0449	0.0632	0.648
Controller saturation	0.0524	0.0738	1

Figure 4