Diversity Modeling to Evaluate Security of Multiple SDN Controllers

Hellen Maziku  
Tennessee State University  
Nashville, TN

Sachin Shetty  
Old Dominion University  
Norfolk, VA

Dong Jin  
Illinois Institute of Technology  
Chicago, IL

Charles Kamhoua  
Army Research Lab  
Adelphi, MD

Laurent Njilla and Kevin Kwiat  
Air Force Research Lab  
Rome, NY

Abstract—Software Defined Networking (SDN) facilitates network orchestration and ability to reconfigure the network plane at run time. Despite ubiquitous adoption of SDN, there is also growing concern about security risks posed by SDN. The security risks stem from centralized controller, trust issues between network elements due to Open APIs and an insecure OpenFlow channel. However, SDN controllers are a common target since compromising SDN controllers has the capability of impairing the entire network. SDN controller protection efforts have centered around replicating controllers for redundancy and hardening host Operating Systems. There is lack of research efforts on the security impact of adopting multiple SDN controllers. In this paper, we present a network diversity modeling framework to assess impact on security risk due to multiple SDN controllers. Using attack graphs and diversity models, we explore the security impact of resource relationships to SDN multiple controller networks. Our results reveal that having similar resource instances in different multiple SDN controllers increases the security risk.

Index Terms—Cyber Resilience; Security Metrics; SDN security; Diversity Modeling; OpenFlow; Attack graphs

I. INTRODUCTION

Software defined networking (SDN) is a networking paradigm to provide automated network management at run time through network orchestration and virtualization. SDN is used primarily for quality of service (QoS) and automated response to network failures. SDN allows decoupling of the control and data plane, enabling logically centralized network controllers to manage whole networks [11]. Current critical infrastructures were designed with a static non adaptive nature which makes it practically infeasible to reconfigure a network to react to cyber attacks. Our previous work in [10], [8], and [9], demonstrates how SDN’s dynamic and real-time reconfigurability ability is the answer to cyber security and resilience of today’s critical infrastructures such as smart grids and cloud networks.

However, there is a growing concern about security risks in adopting SDN. SDN presents new security challenges due to centralized control logic that maybe prone to DoS attacks (single point of failure), trust issues between network elements due to Open APIs and an OpenFlow channel that may not be secure, depending on the configuration options enforced [14], [1]. There have been efforts proposed to secure SDN across all layers [5], [14], [4]. Specific approaches, such as, authentication mechanisms such as TLS, shared secret passwords and nonces to avoid eavesdropping and spoofed southbound communications have been proposed. However, the SDN controllers are a fairly common target because impairing the controllers can severely compromise large network segments. Security mitigation schemes to protect SDN controllers include replicating controllers for redundancy and hardening host Operating Systems. However, there needs to be a systematic understanding of the degree of security enhancements multiple SDN controllers can provide. Some of the key questions that need to be addressed include; Does overall security of SDN improve with multiple controllers? What is the optimal number of SDN controllers to provide the desired degree of protection? What are the cost implications of choosing a High Availability (HA) SDN controller configuration?

This paper provides a first step towards formally modeling SDN controller diversity. Using diversity modeling principles in [17], we investigate the hypothesis that adding multiple controllers improves the security of an SDN enabled network. We evaluate existing diversity metrics and analyze the applicability of diversity modeling to SDN multiple controller frameworks. We propose a framework with multiple controllers as depicted in Figure 1 for improving security and resilience of SDN enabled infrastructures. We adopt a high Availability (HA) hierarchical role-based controller architecture in the SDN control layer. Each controller is assigned specific roles by another controller that acts as master and delegator. The challenge is to come up with a cost model to determine optimal number of controllers. We use single-controller and three-controller networks to model diversity and our results demonstrate that adding multiple controllers improves the security of an SDN enabled network. We employ attack graphs to model the casual relationships between different resources running in the SDN network and use diversity models to evaluate the security impact of resource relationships to SDN multiple controller networks. We reveal that having similar resource instances in different SDN elements in the network lowers network diversity and permits reuse of exploits by attackers.

evaluating robustness of the network against zero day attacks. Drawing analogy from biodiversity in ecology, the authors in [17] propose three security metrics for modeling network diversity.

**Diversity metric 1:** Borrowing concepts from familiar mathematical models of biodiversity in ecology such as *species richness* and *Shannon-Wiener index*, Wang et al. propose the first diversity metric based on distinct number of resources in a network. Given a network \( G \) with a total number of hosts \( H = \{h_1, h_2, ..., h_n\} \) and a set of resource types \( R = \{r_1, r_2, ..., r_m\} \) with the resource mapping \( res(\cdot) \). Let the number of resource instances be given as \( t = \sum_{i=1}^{n} |res(h_i)| \) and relative frequency of each resource be given as \( p_i = \frac{|\{h_i, r_j \in res(h_i)\}|}{t} (1 \leq i \leq n, 1 \leq j \leq m) \). \( r(G) \) known as networks effective richness of resources is given as: \( r(G) = \prod_{r=1}^{n} p_r^p \). Network diversity based on effective richness is defined as \( d_1 \) in equation below. A higher value of \( d_1 \) represents a more diverse network.

\[
d_1 = \frac{r(G)}{t}
\]  

**Diversity metric 2:** The second diversity metric is derived from an attack graph of a network and reflects how attackers may compromise a critical asset, also known as a goal condition in a network, with the least effort. We model an attack graph which is syntactically equivalent to a resource graph in [17], but models known SDN vulnerabilities rather than zero day attacks. Given an attack graph \( G(E \cup C, R_e \cup R_c) \) with pre and post condition relations \( R_e, R_c \) and a goal condition \( c_g \in C \), for each \( c \in C \) and \( q \in seq(c) \) where \( seq(c) \) is a set of attack paths \( \{e_1, e_2, ..., e_n : (c_n, c) \in R_c\} \) for a given sequence of exploits \( e_1, e_2, ..., e_n \), denote \( R(q) \) for \( \{r : r \in R, r \text{ appears in } q\} \). Diversity based on least attacking effort is a ratio between minimum number of distinct resources on a path and minimum number of steps on a path. Network diversity based on least attacking effort is defined below as \( d_2 \). This ratio can never exceed 1.

\[
d_2 = \frac{\min_{q \in seq(c)} |R(q)|}{\min_{q' \in seq(c)} |q'|}
\]  

**Diversity metric 3:** The least attacking effort also known as the shortest path to the attacker’s target does not provide a full picture of the threat and hence carries insufficient information [17]. The third metric, with the help of probability, combines all paths in an attack graph and gives the average attacking effort. Assume \( p \) is the probability of achieving the final goal condition in a network where all resources are different (no exploit reuse), and \( p' \) is the probability of achieving the final goal condition in the same network but with the possibility of reusing an exploit. \( p \) and \( p' \) represent the attack likelihood with respect to the attacker’s goal condition and both probabilities are modeled using a Bayesian network derived from the attack graph. Network diversity based on average attacking effort is defined as:

\[
d_3 = \frac{p}{p'}
\]
III. IMPLEMENTATION OF SDN CONTROLLER DIVERSITY

This section uses two SDN controller configuration examples and diversity metrics from the previous section to evaluate and quantify the security in SDN multiple controller networks.

A. Single SDN Controller Configuration

Figure 2 represents a single OpenFlow controller network with three open vSwitches (X, Y, Z) and three hosts (A, B, C). The attacker is on host A and aims to attack switch Z or host C using two threat vectors eavesdropping and DoS. Suppose the controller is running firewall, REST API and Load Balancer services. The services running in the controller plus the OpenFlow instance trigger data plane flows such as: Packet_in, Flow_mod, Features_request, Features_reply, arp in the network, giving 5 total resource instances.

Effective Richness of Resources: Using equation 1, diversity based on the effective richness of resources in the SDN single controller network, $d_S$ is 3.789.

Least Attacking Effort: In order to compute network diversity based on the least attacking effort, we build an attack graph to model control plane vulnerabilities in our single controller network as depicted in Figure 3 (ignore probability values inside and outside the rectangles). A pair represents a security based condition (e.g., connectivity (source, destination) or privilege (privilege, host)). The triple tuple depicts potential exploit of resource, (resource, exploiting host, exploitable host). Edges flow from pre-conditions to exploits (e.g., from (A, X) and (user, A) to (arp, A, X)), and from that exploit to its post-conditions (e.g., from (arp, A, X) to (user, Y)). We observe five attack paths as illustrated by Table I. Using equation 2, diversity based on the least attacking effort in the SDN single controller network gives a ratio $d_S = \min(1,2,3) = 1$. This ratio indicates that the current network is not diverse and there is 100% potential improvement in diversity.

Average Attacking Effort: In order to compute the cumulative probability of successfully executing an exploit, in this case, the exploit is $<\text{features_reply}, A, Z>$, we update the attack graph in Figure 3 to include individual and cumulative probability scores for conditions and exploits. Given exploit $e$, condition $c$ and probabilities for individual scores $p(e)$ and $p(c)$, cumulative scores $P(e)$ and $P(c)$ can be obtained using equations:

$P(e) = p(e) \cdot \prod_{e \in R(c)} P(e)$ and $P(c) = p(c) \cdot \bigoplus_{e \in R(c)} P(e)$ for any $e \in E$ and $\bigoplus(S_1 \cup S_2) = \bigoplus S_1 + \bigoplus S_2 - \bigoplus S_1 \cap S_2$ for any disjoint and non-empty sets $S_1 \subseteq E$ and $S_2 \subseteq E$.

Cumulative scores in an attack graph factor in the casual relationships between exploits and conditions. This cumulative score exposes the difference in attack likelihood between two multiple SDN controller networks with same number of controllers but different configurations such as different topology setups, or different applications/software running within the controllers. For individual scores (probabilities inside the rectangles), we convert NVD and CVSS base scores [16] for SDN vulnerabilities. We use the above cumulative probability equations to obtain cumulative scores for the exploits and conditions in the one controller attack graph (probabilities outside the rectangles). The Conditional Probability Tables (CPT) in a Bayesian network help to calculate the joint probability function for achieving a certain goal. For example, in the single controller network configuration, Table II helps to calculate the probability of exploiting the $<\text{features_reply}, A, Z>$ resource at switch Z. As seen in Figure 3, 0.264 represents the cumulative probability score for achieving the final goal condition. This probability for exploiting the network includes the significance of causal relationships among resources running in the different controllers, therefore factoring in the effect of how the controllers are positioned in the network.

B. Three SDN Controller Configuration

Figure 4 represents a second degree SDN multiple controller network with six open vSwitches (X1, Y1, Z1,X2, Y2, Z2) and three OpenFlow controllers (C1, C2, C3). An attacker at X1 aims to attack switch Z2. Controllers C2 and C3 are running control plane firewalls while C1 runs REST API and Load Balancer applications. Similar to single controller network, the services running in the controllers plus the OpenFlow instance trigger data plane flows such as: Packet_in at C1, C2, C3, X2, Z2, Features at C3, X2, arp at Z1, Z2, firewall at C2, C3 in the network, giving 11 total resource instances.

Effective Richness of Resources: Using equation 1, di-

---

### TABLE I

<table>
<thead>
<tr>
<th>Attack Path</th>
<th>Steps</th>
<th>Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;features_reply, A, Z&gt;</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>&lt;arp, A, X&gt; → &lt;packet_in, Y, C&gt;</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>&lt;arp, A, X&gt; → &lt;flow_mod, C, Y&gt;</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>&lt;arp, A, X&gt; → &lt;packet_in, X, C&gt; → &lt;features_reply, A, Z&gt;</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>&lt;arp, A, X&gt; → &lt;flow_mod, C, Y&gt; → &lt;features_reply, A, Z&gt;</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

---

Fig. 2. Single SDN Controller Network Configuration
network.

With a probabilistic approach, diversity in a network refers to the probability, where if an attacker can successfully achieve a certain goal condition in the network, he/she can still achieve the targeted goal even if all of network’s resources were to be different across all components. Therefore we model the attack likelihood while considering the effect of reusing an exploit on different network components. Consider Figure 5, assume that reusing the packet_in exploit on controller C3 increases the probability from 0.5 to 0.9. Figure 6 shows the updated Bayesian network with the effect of reusing the exploit. Diversity based on the average attacking effort as discussed in equation 5 is a ratio between probability of achieving final goal condition with no exploit reuse and probability of achieving the same goal condition with exploit reuse. Looking at Figure 5 and Figure 6, \(d_3 = \frac{0.5}{0.9} = 0.556\). We observe that modeling diversity on the three-controller network using the least attacking effort gives a higher diversity value (60%) but masks the effect of re-using an exploit. The average attacking effort however, gives a lower metric value (51%) but exposes the effect of having different resource instances in the network (all resources appearing only once) as opposed to reusing exploits.

**IV. CONCLUSION AND FUTURE WORK**

This paper lays a foundation on methods of formally quantifying the security of SDN multiple controller networks. We extend existing network diversity modeling principles to Software Defined Networking. Using diversity modeling, we demonstrate that adding multiple controllers improves the security of an SDN enabled network. We use diversity models and attack graphs to evaluate the security impact of resource relationships to SDN multiple controller networks.
Our preliminary results reveal that having similar resource instances in different SDN elements in the network lowers network diversity. We are currently extending the probabilistic diversity metric to factor in higher degree SDN multiple controller networks and the cost of diversity. We are looking at how we can improve existing metrics to factor in degree of importance of each controller.

ACKNOWLEDGMENT

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000780 and Office of the Assistant Secretary of Defense for Research and Engineering agreement FA8750-15-2-0120.

REFERENCES


