Research Article

Moving Target Defense Based on Adaptive Forwarding Path Migration for Securing the SCADA Network

Yifan Hu ¹, Peng Xun ¹, Peidong Zhu ², Wenjie Kang ^{3,4,5}, Yinqiao Xiong ^{1,2},
Yufei Zhu ¹, Weiheng Shi ⁶, and Chenxi Hu ⁷

¹College of Computer, National University of Defense Technology, Changsha 410073, China

²Department of Electronic Information and Electrical Engineering, Changsha University, Changsha 410022, China

³Hunan Provincial Key Laboratory of Network Investigational Technology, Hunan Police Academy, Changsha 410138, China

⁴College of Systems Engineering, National University of Defense Technology, Changsha 410073, China

⁵Key Laboratory of Police Internet of Things Application Ministry of Public Security, Beijing 100089, China

⁶College of Meteorology and Oceanography, National University of Defense Technology, Nanjing 211101, China

⁷College of Electrical Engineering, National University of Defense Technology, Hefei 230037, China

Correspondence should be addressed to Peidong Zhu; peidong_nudt@163.com and Wenjie Kang; kangwenjie@nudt.edu.cn

Received 21 June 2021; Accepted 8 September 2021; Published 26 October 2021

Academic Editor: Shahram Babaie

Copyright © 2021 Yifan Hu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Static characteristics of supervisory control and data acquisition (SCADA) system are often exploited to perform malicious activities on smart grids. Most of the time, the success of cyberattacks begins with the profiling of the target system and follows by the analysis of the limited resources. To alleviate the asymmetry between attack and defense, network-based moving target defense (MTD) techniques have been applied in the network system to defend against cyberattacks by constructing a dynamic attack surface to the adversary. In this paper, we propose a novel MTD technique based on adaptive forwarding path migration (AFPM) that focuses on improving the defense capability and optimizing the network performance of path mutation. Considering the transient problems present in path mutation caused by the dynamic switching of the forwarding path, we formalize the mutation constraints based on the satisfiability modulo theory (SMT) to select the mutation path. Considering the limited defense capability of path mutation owing to the traditional mutation selection mechanism, we design the mutation path generation algorithm based on the network security capacity matrix to obtain an optimal combination of mutation path and mutation period. Finally, we compare and analyze various cyber defense techniques used in the SCADA network and demonstrate experimentally that our MTD technique can prevent more than 92% of passive monitoring under specified conditions while ensuring the quality of service (QoS) to be almost the same as the static network.

1. Introduction

Supervisory control and data acquisition (SCADA) system as an essential backbone of smart grids plays an important role in monitoring, controlling, and protecting critical infrastructure resources incorporated within the system. Figure 1 shows the architecture and the protocols in a SCADA system. In recent years, influential cyberattacks [1–3] that have led to massive power outages show more and more static network configurations or underlying vulnerabilities present in the cyber-physical system (CPS) that can

be exploited by the adversary. In addition, if some vulnerable firmware of the embedded devices involved in smart grids is left unpatched, backdoors can be installed to perform sophisticated automated attacks.

For example, the centrifuges inside Iran's Natanz uranium enrichment facility were destroyed by Stuxnet worm [1], which was a rootkit exploiting the Siemens programmable logic controllers (PLC). Although critical infrastructure resources involved in smart grids are already protected by conventional security measures like firewall, IDS, IPS, etc., there are still powerful attacks capable of

FIGURE 1: SCADA architecture and protocols.

circumventing them. On the other hand, static network configurations themselves are a potential cyber threat, which give the attacker a sitting target for malicious manipulations. Owing to the limited storage and computing resources, some smart devices that have installed such security measures cannot detect and prevent more complicated attacks like coordinated attacks.

In a traditional network, a large number of unauthorized IPs are screened out to prevent system overload every day. However, if the attacker escalates his or her privilege for the authorized IPs to flood the targeted devices in a SCADA network, the system will crash by denial of service (DoS) [4]. Suppose that the system is capable of handling the overload, the crash can be avoided by throttling the traffic at the cost of dropping legitimate packets with a huge impact on smart grids. However, a system with dynamic network configurations achieves the possibility of preventing some of these attacks, such as dynamically changing the network topology to mislead the attack target. In practice, this defense technique must ensure availability and synchronization for the communication entities.

To provide a random, dynamic, and heterogeneous environment, network-based moving target defense (MTD) was proposed to disrupt the cyber kill chain [10] by increasing apparent complexity and uncertainty in network communications with controlled change across multiple system dimensions. Table 1 shows some typical

network-based MTDs using different techniques. As the main object of network scanning and traffic monitoring, forwarding path is taken as one of the important network properties needing to be protected. To prevent the attacker from maliciously monitoring the forwarding path, path mutation is widely used for network-based MTD by dynamically changing the forwarding path between the communication entities. In current studies of path mutation, two major problems need to be addressed:

There exist transient problems [11] in path mutation because the performance constraints of the forwarding path are not considered.

The defense capability of path mutation is limited owing to an inappropriate combination of mutation path and mutation period.

In this paper, we propose a novel MTD technique based on adaptive forwarding path migration (AFPM) that achieves an optimal path selection mechanism for path mutation. Different from the traditional path selection mechanism that focuses on the selection of mutation path without considering mutation period, we improve the defense capability by incorporating both the selections of mutation path and mutation period into our technique. In addition, we formalize the performance constraints that routing nodes and forwarding links on the forwarding path need to satisfy to prevent the transient problems during path

TABLE 1: Typical network-based MTDs.

References	Technique	Contribution
[5]	Random host mutation	Providing high-speed and unpredictable IP mutation
[6]	SDN-based MTD analysis	Implementing MTDs using SDN
[7]	Dynamic address solution	Enlarging the changing scopes of terminal hosts
[8]	Collaborative mutation including end point mutation and routing mutation	Improving the defensive benefit brought about by network mutation
[9]	Attack graph-based MTD	Shuffling network configurations based on the criticality

mutation. The main contribution of this paper is to show how AFPM concepts provide a dynamic attack surface to the adversary against passive monitoring and maximize the defense benefits without compromising the availability of path mutation. Specifically,

To ensure the availability of path mutation, we formalize the mutation constraints based on the satisfiability modulo theory (SMT) to select the forwarding path that satisfies these constraints as the mutation path.

To achieve the maximum defense benefits, we design the mutation path generation algorithm based on the network security capacity matrix to obtain an optimal combination of mutation path and mutation period.

The remainder of this paper is organized as follows. Section 2 reviews the related work. Section 3 introduces the necessary background. Section 4 explains the AFPM technique. Section 5 presents the evaluation results. Concluding remarks are drawn in Section 6 with future work.

2. Related Work

The DARPA Information Assurance Program did initial research in the area of dynamic network defense for the purpose of confusing any would-be adversaries sniffing the network [12]. Thus, network defense technique transforms from “passive defense” to “proactive defense” and network-based MTD comes into being. Existing studies on path mutation technique mainly include multipath mutation [13–15] and random-path mutation [16–18].

2.1. Multipath Mutation. Multipath mutation is the concept of calculating all possible disjoint paths in advance and randomly selecting one of them as the mutation path. Duan et al. [13] presented a proactive random route mutation (RRM) technique to defend against reconnaissance, eavesdropping, and DoS attacks by modeling and solving a constraint satisfaction problem, where they formalized the mutation constraints using the SMT to identify the optimal forwarding path. Compared with the static network using a single forwarding path, RRM can prevent more than 90% of eavesdropped or disrupted packets. RRM was extended by Jafarian et al. [14] via optimizing the mutation strategy based on game theory and constraint satisfaction optimization to improve the defense capability of path mutation. To enhance the mutation efficiency and increase the complexity of attacks in scanning and poisoning, Zkik et al. [15] focused on modeling software defined network (SDN) architectures,

where two new modules were implemented to automatically calculate the suitable paths based on a pathfinder algorithm. However, owing to the deterministic nature of these multipath mutation techniques, the adversary who has acquired the routing algorithm can calculate the mutation path and hence endangers all packets forwarded over this path.

2.2. Random-Path Mutation. Random-path mutation is the concept of collecting all the available routing nodes in advance and randomly selecting one of them as the next hop. Different from the existing multipath mutation techniques, the adversary cannot pinpoint the routes traversed by each packet even if he or she has known the routing algorithm. Considering that traditional routing protocols forwarded packets over a single path, Bohacek et al. [16] presented a game-theoretic stochastic routing (GTSR) framework where all paths between a source-destination pair were discovered and next-hop probabilities were determined. By proactively forcing packets to probabilistically take alternate paths, GTSR mitigated the effect of packet interception and eavesdropping attacks. Instead of selecting the path from a pre-calculated set of routes like multipath mutation, Shu et al. [17] proposed a randomized multipath routing algorithm that generated randomized routes taken by the shares of different packets to secure wireless sensor networks (WSN) against compromised node and DoS. To invalidate the adversary’s knowledge and plan of attacks against critical network resources, Gillani et al. [18] employed virtual networks (VN) to proactively defend against sophisticated DDoS (Distributed DoS) attacks like Crossfire by dynamically reallocating network resources using VN placement and offering constant VN migration to new resources. Although these random-path mutation techniques can enhance security by increasing randomness, they still have problems that we have presented in Section 1.

3. Background and Motivation

In this section, we first explain the cyber risk of static cyber threats that exist in the SCADA network. Then, we state the security problems with static configurations in a specific attack scenario. Finally, we introduce the methodology of network-based MTD based on the cyber kill chain.

3.1. Static Cyber Threats. Network communications in smart grids are supported by the SCADA system where network configurations and facilities are usually static (or fixed) for the attacker. Even if the system is upgraded, it goes into a

step-by-step update including deploying new network configurations and facilities, which gives the attacker plenty of time to trace out these update steps. Many security measures have been deployed in the system to protect these static network resources [19]. However, when the scale of smart grids reaches the level at which critical infrastructures are integrated into the system, potential cyber threats become more dangerous and numerous. Maybe only a small loophole on which a backdoor can be established is needed for the attacker to penetrate the inside system where vulnerabilities can be exploited to launch a powerful attack. To measure the cyber risk, security experts give the following equation:

Cyber risk = Threats * Vulnerabilities * Consequences.

However, it is impossible that all threats including existing uncertain and unknown ones are factored into threat modeling, which means that the modeling result is not always accurate. Considering that there are so many vulnerabilities in such a large-scale system, it will take a considerable amount of time and effort to check system behaviors for them one by one. Even if all of these threats and vulnerabilities are counted, the results are still inconclusive considering false positives. Therefore, achieving a 100% secure system is always theoretical. Intrusions are inevitable in most cases of cyberattacks, where attack scripts or malware are implanted into the system and they can lie dormant for days, weeks, or even months [20]. However, the security of a system where reactive types of security measures have been deployed can be enhanced by applying proactive defense technique to mislead the attacker into developing ineffective attacks.

3.2. Cyberattack Identification. Figure 2 shows an abbreviated SCADA network consisting of three subnetworks connected by wide area networks (WAN). Since the WAN is exposed to the outside world, it is more likely that the traffic is vulnerable to attacks. For example, the attacker can trace out the IP addresses of the communication entities by monitoring and analyzing the traffic in the DNP3 communication established between the SCADA server in the control center and the remote terminal unit (RTU) in the substation. By targeting one of them, the attacker can maliciously trip open a relay that is connected to and controlled by the RTU via replaying the legitimate trip command issued by the control center to select an incorrect breaker to trip the breaker system.

Since the source IP addresses of the trip packets are unauthenticated, they are usually detected and dropped by the gateway router where a specific firewall or IDS rule is added in the substation. However, there may be smart attackers able to legitimize the source IP addresses such that these trip packets can bypass the detection of this added firewall or IDS rule without being dropped. This kind of attacks can be detected unless the IDSs are distributed with event correlations between the control center and the substation. However, it will be very costly and time-consuming to check for every event such that normal

legitimate communication cannot be guaranteed. And more seriously, DoS issues will be raised and the system will be unavailable. Therefore, distributed IDSs fail to prevent such an attack at an early stage because system availability is a primary consideration.

3.3. Network-Based MTD. To understand how network-based MTD can be effective against cyberattacks in the SCADA network, we start with the cyber kill chain, as shown in Figure 3, where the loop of a cyberattack is divided into five steps:

- (1) *Reconnaissance.* The attacker gathers topology information, such as host name, network address, and MAC address, to develop a blueprint of the system architecture and identify the key locations for the attack.
- (2) *Access.* The attacker tries to connect or communicate with the target to explore version numbers, configurations, operating system, and other system properties for vulnerability identification.
- (3) *Exploitation.* This is a weaponization step. The attacker exploits one of the vulnerabilities discovered in the system to establish a foothold for malicious activities, such as installing attack scripts or malware for specific types of attacks.
- (4) *Execution.* After being clear enough about the operation state of the system within a period of lurk, the attacker finds a right time to execute the attack scripts or malware through a network connection or an infected USB pendrive.
- (5) *Persistence (optional).* The attacker keeps the access channels and the inserted backdoors in the compromised system, which give chances for him or her to launch further more impactful attack in the future by repeating the above steps.

If we break one or more steps of the cyber kill chain, the development of the cyberattack will be disrupted. Especially in the first stage, if we mislead or delay the attacker's reconnaissance, i.e., obstructing the attacker's access to the knowledge about the system, the later steps become useless. This is where the idea of network-based MTD comes from, which achieves a kind of proactive defense technique against cyberattacks by extending the attack surface to alleviate the asymmetries between attack and defense, e.g.,

- (i) Narrow the attack window by increasing the uncertainty of the network composition to alleviate the information asymmetry between attack and defense.
- (ii) Delay the attack time by increasing the dynamics of the network topology to alleviate the time asymmetry between attack and defense.
- (iii) Raise the attack cost by increasing the diversity of the network elements to alleviate the cost asymmetry between attack and defense.

FIGURE 2: A specific attack in the SCADA network.

FIGURE 3: Network-based MTD against cyber kill chain.

However, network-based MTD may create additional performance overhead in the absence of cyber threats when system properties are dynamically changed. To maximize the defense benefits and lower the performance overhead, network-based MTD usually adopts a intelligent architecture by a combination of proactive mutation and reactive mutation. The basic principle of network-based MTD is described in Figure 3, which is introduced as follows:

- (1) Formulate the security policy and the functional tasks based on some kind of security objective and initialize the network resources.

- (2) Select mutation element and mutation period based on the formulated security policy and create mutation configurations by mutation configuration management.
- (3) Issue and deploy the mutation configurations to the corresponding devices of the target system by mutation implementation.
- (4) Perceive and analyze the current security state of the target system in the analysis engine and submit the result to the mutation triggering mechanism.

- (5) Determine the mutation strategy for the next mutation period based on the analysis of the current network security state by the mutation triggering mechanism.

4. Adaptive Forwarding Path Migration

Owing to the imperceptibility of passive monitoring, most path mutation methods employ an autonomous random mutation technique, which relies on a preset path selection algorithm to select the forwarding path for the next mutation [13, 18]. However, the quality of service (QoS) cannot be ensured because such technique fails to perform real-time adjustments for the network security state. Therefore, we design the adaptive forwarding path migration (AFPM) mechanism to optimize the selection of mutation path, as shown in Figure 4, where the dynamic switching of the forwarding path is realized by changing the routing deployment and the forwarding strategy. For ease of reference, nomenclatures are provided in Tables 2 and 3.

4.1. Forwarding Path Migration Constraints. Transient problem is the phenomenon of rapid decline in the network performance during path mutation. This will lead to an increased probability of packet disorder and packet loss. Packet disorder means that the packet sequence of forwarding data is out-of-order caused by forwarding path migration. Packet loss is caused by insufficient forwarding nodes and links, unreachable forwarding paths, and inconsistent update of flow tables. Since packet disorder and packet loss may trigger the TCP retransmission mechanism with the degradation of the TCP performance, the availability of path mutation is reduced. To ensure the QoS, we formalize the mutation constraints in terms of forwarding path capacity, forwarding path delay, and forwarding path accessibility.

Network resource capacity [21] refers to the remaining available resources of routing nodes and forwarding links in a network system. Among them, the remaining available resources of routing nodes mainly depend on the remaining available flow table entries because the CPU consumption and storage surplus of routing nodes are positively correlated with the number of the flow table entries [22], and the remaining available resources of forwarding links mainly depend on the remaining available bandwidth. In an actual network characterized by the multi-flow intersection, the overhead of a routing node or a forwarding link is equivalent to the sum of the costs of all the data flows passing through the node or the link at a time. We denote $b_v^{T_{RMP}}(k)$ as the Boolean variable whether routing node v forwards the k th data flow within mutation period T_{RMP} (if so, $b_v^{T_{RMP}}(k) = 1$; otherwise, $b_v^{T_{RMP}}(k) = 0$). Similarly, we denote $b_e^{T_{RMP}}(k)$ as the Boolean variable whether forwarding link e transmits the

k th data flow within mutation period T_{RMP} (if so, $b_e^{T_{RMP}}(k) = 1$; otherwise, $b_e^{T_{RMP}}(k) = 0$). Thus, path mutation needs to satisfy the following constraints.

4.1.1. Forwarding Path Capacity Constraint. This constraint aims to prevent packet loss caused by data overflow via selecting the routing node that can carry the accumulated flow tables and the forwarding link that can carry the accumulated data flows. We use the exponential function based on marginal cost to quantify the resource consumption of routing nodes and forwarding paths.

$$c_v(k) = C_v \left(\sigma^{1 - (C_v(k)/C_v)} - 1 \right), \quad (1)$$

$$\forall MR_v, \quad \text{If } C_v^{\max} - \sum_{i=1}^k b_v^{T_{RMP}}(i) c_v(i) \geq C_v^{\text{th}}, b_v^{T_{RMP}}(i) = 1, \quad (2)$$

$$c_e(k) = C_e \left(\sigma^{1 - (C_e(k)/C_e)} - 1 \right), \quad (3)$$

$$\forall ML_e, \quad \text{If } C_e^{\max} - \sum_{i=1}^k b_e^{T_{RMP}}(i) c_e(i) \geq C_e^{\text{th}}, b_e^{T_{RMP}}(i) = 1. \quad (4)$$

Equation (1) represents the marginal cost function for a newly added flow table entry, where C_v denotes the number of the remaining entries in the flow table, σ denotes the adjustment parameter whose value is set as $\sigma = 2n$ through a theoretical analysis [23], where n is the number of routing nodes, and $1 - c_v(k)/C_v$ denotes the flow table utilization after forwarding information of the k th data flow is added to routing node v . Equation (2) indicates that the accumulated marginal cost of the flow table must be within the capacity limit of the selected node $C_v^{\max}$, and the remaining flow table length should not be less than C_v^{th} to avoid data overflow. Equation (3) represents the marginal cost function of forwarding a data flow, where $1 - c_e(k)/C_e$ denotes the bandwidth utilization after the k th data flow passes through forwarding path e . Equation (4) indicates that the accumulated marginal cost of the bandwidth consumption must be within the capacity limit of forwarding path $C_e^{\max}$, and the remaining bandwidth should not be less than C_e^{th} such that the forwarding path has the residual capacity to deal with data fluctuation caused by load balance or network jitter.

4.1.2. Forwarding Path Delay Constraint. This constraint aims to prevent packet disorder via selecting the forwarding path whose total transmission delay is acceptable and whose mutation delay is less than the inter-packet delay.

$$\sum b_v^{T_{RMP}}(k) \leq L_{\max}, MR_v \in \{MR_S, MR_I, \dots, MR_D\}, \quad (5)$$

$$\text{If } \{L_{T_{RMP+1}} | (t(i+1, k) - t(i, k)) > \max[D(L_{T_{RMP}})] - \min[D(L_{T_{RMP+1}})]\}, \quad b_L^{T_{RMP+1}}(k) = 1. \quad (6)$$

FIGURE 4: Adaptive forwarding path migration mechanism.

TABLE 2: Variable notation.

Notation	Definition
T_{RMP}	Mutation period
$b_v^{\text{RMP}}(k)$	Boolean variable whether routing node v forwards the k th data flow within mutation period T_{RMP}
ML_e	Forwarding path e for mutation
ML_v	Routing node v for mutation
$C_e(k)$	Marginal cost of forwarding path e carrying data flow k
$C_v(k)$	Marginal cost of routing node v carrying data flow k
d_{v-D}^k	Set of the routing nodes on mutation path MR_e excluding the routing nodes with the source and destination addresses
$sc_{S,D}$	Distance from the current mutation node MR_v to the target routing node
$c_{S,D}$	Resource capacity of routing nodes and forwarding paths that ensures secure forwarding from source node S to destination node D
$\omega_{S,D}^s$	Maximum residual capacity from source node S to destination node D
$\mathbf{Q}[sc_{S,D}]_{n \times n}$	Security coefficient
σ	Network security capacity matrix from source node S to destination node D
	Adjustment parameter

TABLE 3: Constant notation.

Notation	Definition
C_e^{th}	Minimum amount of data to be retained by forwarding path e
C_e^{max}	Maximum cumulative marginal cost that forwarding path e can hold
C_v^{th}	Minimum amount of data to be retained by routing node v
C_v^{max}	Maximum cumulative marginal cost that routing node v can hold
L_{max}	The preset maximum length of the forwarding path

Equation (5) indicates that the length of each forwarding path should not exceed the preset maximum value L_{max} (in this paper, $L_{\text{max}} = 32$). Since the transmission delay is positively related to the number of routing nodes on the forwarding path [24], the deterioration in the QoS caused by excessive transmission delay can be prevented by limiting the length of the forwarding path. Before forwarding path migration, the minimum transmission delay of the alternative forwarding path in the next mutation period $L_{T_{\text{RMP}+1}}$ and the maximum transmission delay of the current

forwarding path $L_{T_{\text{RMP}}}$ are measured by the round trip time (RTT) [25]. Equation (6) indicates that the difference between the minimum transmission delay of $L_{T_{\text{RMP}+1}}$ and the maximum transmission delay of $L_{T_{\text{RMP}}}$ should be less than the average inter-packet delay to avoid packet disorder.

4.1.3. Forwarding Path Accessibility Constraint. This constraint aims to prevent the occurrence of forwarding loops that can cause packet loss via limiting the selection of mutation nodes.

$$\begin{aligned}
b_s^{T_{\text{RMP}}}(k) &= 1, \\
b_D^{T_{\text{RMP}}}(k) &= 1, \\
\sum_{i \in I} b_i^k &= \sum_{o \in O} b_o^k,
\end{aligned} \tag{7}$$

$$\begin{aligned}
\text{If } b_v^{T_{\text{RMP}}}(k) &= 1, \quad \forall MR_v \in \chi(MR_v), \\
\sum b_v^{T_{\text{RMP}}}(k) &= 2,
\end{aligned} \tag{8}$$

$$\text{If } MR_v \in \{MR | \text{next hop of } MR_{v-1}\}, \quad d_{v-D}^k \leq d_{(v-1)-D}^k. \tag{9}$$

Equation (7) indicates that the input and the output of all routing nodes on the forwarding path are the same. Equation (8) indicates that each routing node on the forwarding path is physically adjacent to the routing nodes of its previous and next hops, where $\chi(MR_v)$ denotes the set of routing nodes excluding the source and destination nodes on the forwarding path. Since accessibility cannot be guaranteed when a data flow is forwarded from one node to its next-hop neighbor, equation (9) limits the distance between the forwarding node and the target node, i.e., the distance between the next-hop node and the target node cannot exceed the distance between the current forwarding node and the target node, where d_{v-D}^k denotes the distance from MR_v to the target node. Equation (9) ensures that the data flow will not be forwarded again after reaching the target node.

4.2. Mutation Path Generation Algorithm. To achieve the maximum defense benefits of forwarding path migration, we calculate the optimal combination of mutation path and mutation period by referring to the idea of maximum flow-minimum cut [26]. Since the adversary usually monitors routing nodes and forwarding links for malicious purposes and the current network resource capacity has no consideration for security, the availability of routing nodes and forwarding links is reduced with the increase of cyber risks even if they satisfy the mutation constraints in Section 4.1. Therefore, we define the network security capacity matrix to obtain an optimal combination of mutation path and mutation period. The actual network can be abstracted as a directed graph $G(N, L)$, where N denotes the set of vertexes, i.e., the set of routing nodes $\{MR_v\}$, and L denotes the set of directed edges, i.e., the set of forwarding paths $\{ML_e\}$.

Definition 1. Weighted directed graph. Given a network $G(N, L)$, we represent $\vec{G}(N, L, W)$ as its weighted directed graph, where $W = (C, B)$, C denotes the security capacity of routing nodes, and B denotes the security bandwidth of forwarding links.

Definition 2. Network security capacity matrix. Given a network $\vec{G}(N, L, W)$, we represent $\mathbf{Q}[sc_{S,D}]_{n \times n}$ as its network security capacity matrix, where $n = |N|$ denotes the number of routing nodes, and $sc_{S,D}$ denotes the resource capacity of routing nodes and forwarding paths, which ensures secure forwarding from source node $S \in N$ to destination node $D \in N$ (i.e., $S-D$).

$$sc_{S,D} = c_{S,D} \omega_{S,D}^s,$$

$$\omega_{S,D}^s = 1 - \min_{d \in D} \max_{a \in A} \sum_{l_j \in L_+} f\left(\frac{R_A}{R_D} P_j^a P_j\right), \tag{10}$$

where $c_{S,D}$ denotes the maximum residual capacity [21] that can be calculated based on real-time online access to network status information, and $\omega_{S,D}^s$ denotes the security coefficient determined by the attacker and defender's strategies: the attacker adopts the monitoring strategy $a \in A$ to maximize the attack benefits (i.e., minimize $\omega_{S,D}^s$), and the defender adopts the mutation strategy $d \in D$ to maximize the defense benefits (i.e., maximize $\omega_{S,D}^s$). Thus, $\omega_{S,D}^s$ is related to the number of attacker's monitoring $R_A = T/r_A$, the number of mutations $R_D = T/T_{\text{RMP}}$, the probability of the attacker monitoring the j th path P_j^a , and the probability of data packets passing through the j th path P_j within time T .

Theorem 1. Given a weighted directed graph $\vec{G}(N, L, W)$, for $\forall l_j \in L_+$ with the constraint $W(l_j) = 1/P_j^a$, the value of $1 - \omega_{S,D}^s$ is equal to the reciprocal of the max-flow of $S-D$.

Proof. Since $1 - \omega_{S,D}^s$ is linearly dependent on the selection of the monitoring strategy $a \in A$ when the mutation strategy $d \in D$ is determined, $1 - \omega_{S,D}^s$ can be expressed by $\min_{a \in A, d \in D} \sum_{l_j \in L_+} \lambda$, where $\lambda \geq P_j^a P_j$. If we set $\bar{\lambda} = 1/\lambda$, $f_{S,D}^s = 1/(1 - \omega_{S,D}^s)$ and $f_{S,D}^s = \max \bar{\lambda}$ such that

$$\frac{1}{1 - \omega_{S,D}^s} = \max_{a \in A, d \in D, \bar{\lambda} P_j \leq 1/P_j^a} \bar{\lambda}. \tag{11}$$

Equation (11) represents the max-flow problem of $S-D$ for $\forall l_j \in L_+$ with the constraint $\bar{\lambda} P_j \leq 1/P_j^a$ in $\vec{G}$. Therefore, the solution to $1/(1 - \omega_{S,D}^s)$ can be transformed into the solution to the max-flow problem of $S-D$ with the constraint $W(l_j) = 1/P_j^a$.

Based on the network security capacity matrix, we calculate the optimal combination of mutation path and mutation period to achieve the maximum $\omega_{S,D}^s$. Figure 5 shows the flow chart of the mutation path generation algorithm, which is written as follows:

- (1) Initialize a combination queue Q of mutation path and mutation period;
- (2) Construct the breadth-first searching (BFS) tree of undirected graph G , where mutation node MR_S acts as the root node, and mutation nodes MR_i are sorted in descending order based on the distance from MR_i to MR_S and those of the same distance are placed in the same order;
- (3) Observe and rank MR_i, ML_i , where $i \in [1, n]$;
- (4) Select the set of MR_i, ML_i that satisfy the capacity constraint based on equations (1)–(4) using the SMT solver;
- (5) Calculate the max-flow of $c_{S,D}$;
- (6) Convert undirected graph G to weighted directed graph $\vec{G}$;

FIGURE 5: Mutation path generation algorithm.

- (7) Calculate the max-flow of $f_{S,D}^s$;
- (8) Transform $f_{S,D}^s$ into $w_{S,D}^s$ based on Theorem 1;
- (9) Construct network security capacity matrix $\mathbf{Q}[sc_{S,D}]_{n \times n}$;
- (10)
 - (1) For each $MR_i, i \in [1, n]$ do
 - (2) If $i = 1$ then
 - (3) Select MR_S ;
 - (4) Else
 - (5) Select the set of routing nodes $\{MR_i\}^i$ physically adjacent to MR_{i-1} that satisfy the accessibility constraint based on equations (7)–(9);
 - (6) End if
 - (7) End for;
- (11) Select the mutation path that satisfies the delay constraint based on equations (5) and (6);
- (12) Add the alternative combinations of mutation path and mutation period that satisfy the mutation constraints into queue Q ;

- (13) Sort the alternative combinations of mutation path and mutation period in descending order;
- (14) Take the highest ranked combination as the optimal one for the next mutation;
- (15) Return the optimal combination of mutation path and mutation period;

In this algorithm, we first traverse the mutation nodes using the BFS algorithm, and select the set of routing nodes and forwarding links that satisfy the forwarding path capacity constraint in steps (2)–(4). Next, we calculate the max-flow of $c_{S,D}$ using the Hao–Orlin algorithm [27] in step (5), and calculate the max-flow of $f_{S,D}^s$ and transform it into $w_{S,D}^s$ based on Theorem 1 in steps (6)–(8). Then, we construct network security capacity matrix $\mathbf{Q}[sc_{S,D}]_{n \times n}$ in step (9), and screen out the possible forwarding paths in $\mathbf{Q}[sc_{S,D}]_{n \times n}$ by the forwarding path delay constraint and the forwarding path accessibility constraint in steps (10)–(12). Finally, we rank the alternative combinations of mutation path and mutation period in steps (13) and (14), and return the optimal one to achieve the maximum defense benefits in step (15).

4.3. Path Mutation Security Analysis

4.3.1. Mutation efficiency analysis. Suppose that there is a data flow f transmitted within time T in which case the data flow transmitted in each mutation period is denoted as f/R_D , there are r routing nodes included in set V_R monitored by the attacker, there are s routing nodes included in set V_T between source node S and destination node D , and the successful probability of the attacker monitoring a data flow is independently distributed as $x = P_j^a P_{j \cdot}$.

Case 1: $R_A \leq R_D$. When the successful probability of the attacker monitoring a data flow obeys binomial distribution $B(R_A, x)$, the data flow monitored by the attacker is fxR_A/R_D .

Case 2: $R_A > R_D$. The attacker achieves a higher frequency of passive monitoring, $z = \lceil R_A/R_D \rceil$ times in each mutation period, which obeys geometric distribution $G(x)$. If the attacker successfully penetrates a routing node by an attack, he or she can monitor the data flow through this node for the rest of the mutation period. When the successful probability of the attacker monitoring a data flow obeys binomial distribution $B(R_A, x)$, the data flow monitored by the attacker is $f \sum_{k=1}^z x(1-x)^{k-1} [z - (k-1)]/z$.

In the static network, we have that $z = R_A$ since there is no path mutation. The successful probability of the attacker monitoring the j th path is $P_j^a = C_n^r - C_{n-s}^r / C_n^r$, and the data flow monitored by the attacker is $f \sum_{k=1}^{R_A} x(1-x)^{k-1} [R_A - (k-1)]/R_A$.

In the RRM network [13], the attacker can monitor the path from S to D when $MR_S \in V_R$ or $MR_D \in V_R$ while the attacker can do that when $MR_S \notin V_R$ and $MR_D \notin V_R$ if and only if the routing nodes on the path from S to D in G can be divided in x interconnected subgraphs $G_1, G_2, \dots, G_x$ by the cut set V_C , i.e., $V_C \subseteq V_R$. Thus, the successful probability of the attacker

monitoring the j th path is $P_j^a = C_2^1 C_{r-2}^{r-1} + C_2^2 C_{r-2}^{r-2} + n_{V_R} / C_n^r$, where n_{V_R} denotes the number of V_R . Since RRM has a fixed mutation period, the data flow monitored by the attacker is $\min(R_A, R_D) p_{\min(R_A, R_D)} \cdot f \sum_{k=1}^z x(1-x)^{k-1} [z - (k-1)] / z R_D$, where $p_{\min(R_A, R_D)}$ denotes the probability of $R_A \leq R_D$ when $\min(R_A, R_D) = R_A$ or the probability of $R_A > R_D$ when $\min(R_A, R_D) = R_D$.

In the AFPM network, similarly, the successful probability of the attacker monitoring the j th path is $P_j^a = C_2^1 C_{r-2}^{r-1} + C_2^2 C_{r-2}^{r-2} + n_{V_R} / C_n^r$. Since AFPM can adjust the mutation period as the frequency of the attacker's passive monitoring changes, the data flow monitored by the attacker is fxR_A/R_D .

Therefore, the successful probability of the attacker monitoring the data flow can be significantly reduced in the AFPM network compared with the two other networks.

4.3.2. Network Performance Analysis. According to Section 4.1, packet disorder caused by path mutation is the reason for the performance consumption, which reduces the availability of path mutation. Therefore, we have imposed the forwarding path delay constraint on path mutation to prevent such transient problem.

Theorem 2. $\{L_{T_{RMP+1}} | (t(i+1, k) - t(i, k)) > \max[D(L_{T_{RMP}})] - \min[D(L_{T_{RMP+1}})]\}$ ensures that packet disorder does not occur in the AFPM network.

Proof. Since the selected mutation path in the next mutation period satisfies $\{L_{T_{RMP+1}} | (t(i+1, k) - t(i, k)) > \max[D(L_{T_{RMP}})] - \min[D(L_{T_{RMP+1}})]\}$, we have that $D(f_k^{T_{RMP}}) \geq \min[D(L_{T_{RMP}})]$ holds for any data flow f_k . Suppose that data packet x_i of data flow f_k is transmitted by forwarding path $L_{T_{RMP}}$ and data packet x_{i+1} of data flow f_k is transmitted by forwarding path $L_{T_{RMP+1}}$, we set $\Delta t = t(i+1, k) - t(i, k)$.

Case 1: $\max[D(L_{T_{RMP}})] = D(f_k^{T_{RMP}})$. The maximum transmission delay of data packet x_i transmitted by forwarding path $L_{T_{RMP}}$ satisfies $\max[D(f_k^{T_{RMP}})] < \min[D(L_{T_{RMP+1}})] + \Delta t$.

Case 2: $\max[D(L_{T_{RMP}})] > D(f_k^{T_{RMP}})$. The maximum transmission delay of data packet x_i transmitted by forwarding path $L_{T_{RMP}}$ still satisfies $\max[D(f_k^{T_{RMP}})] < \min[D(L_{T_{RMP+1}})] + \Delta t$.

Given that $\min[D(L_{T_{RMP+1}})] \leq D(f_k^{T_{RMP+1}})$ holds, we still have that $\max[D(f_k^{T_{RMP}})] < \min[D(f_k^{T_{RMP+1}})] + \Delta t$ holds based on Case 1 and Case 2. Therefore, any data flow will not cause packet disorder during path mutation.

Considering that differential flow table configurations resulting from inconsistent update of flow tables may lead to packet loss that also affects the network performance, we prevent this transient problem by updating the flow tables based on the principle of reverse adding and forward deleting: the mutation controller adds new flow table rules for the routing nodes in reverse order (i.e., from the destination node to the source node) while deleting old flow table rules for the routing nodes in order (i.e., from the source node to the destination node).

Theorem 3. The principle of reverse adding and forward deleting during the update of flow tables ensures the packet accessibility during path mutation.

Proof. Suppose that the principle of reverse adding and forward deleting during the update of flow tables cannot ensure the packet accessibility during path mutation. This means that there must be a mutation node MR_i that cannot forward packets to the other nodes. All possible mutation nodes can be classified as follows:

Case 1: $MR_i \notin MR_{\text{new}} \wedge MR_i \notin MR_{\text{old}}$. This indicates that the mutation node is not included in the set of the routing nodes in the current mutation period nor is it included in the set of routing nodes in the next mutation period. In this case, MR_i does not receive any packets.

Case 2: $MR_i \in MR_{\text{new}} \wedge MR_i \notin MR_{\text{old}}$. This indicates that the mutation node is only included in the set of the routing nodes in the next mutation period. In this case, MR_i does not receive packets in the current mutation period and only forwards packets in the next mutation period based on the updated flow table.

Case 3: $MR_i \in MR_{\text{new}} \wedge MR_i \in MR_{\text{old}}$. This indicates that the mutation node is not only included in the set of the routing nodes in the current mutation period but also included in the set of the routing nodes in the next mutation period. In this case, MR_i receives packets in the current mutation period and forwards them according to the updated flow table.

Case 4: $MR_i \notin MR_{\text{new}} \wedge MR_i \in MR_{\text{old}}$. This indicates that the mutation node is only included in the set of the routing nodes in the current mutation period. In this case, MR_i only receives packets in the current mutation period and forwards them according to the original flow table. However, MR_i does not receive any packets after the RTT, which means that all packets have been forwarded within the current mutation period [13].

Therefore, the packets forwarded by mutation node MR_i are still reachable during path mutation, which contradicts this supposition.

5. Evaluation

To demonstrate the significance and necessity of network-based MTD, we first compare the strengths and weaknesses of various cyber defense techniques by analyzing their defense capability and system performance. Based on the security analysis in Section 4.3, we then discuss the security performance and transient problems of our proposed MTD technique against passive monitoring through case studies.

We simulated communication networks of the kinds used by SCADA to deliver smart grid commands and measurements. We used real SDN-enabled hardware routers and switches in different physical locations to build a backbone network, which supported communications between the control center and the substations. Figure 6 shows

FIGURE 6: Network-based MTD test bed.

the network topology of our test bed, where network-based MTD strategies are deployed in the backbone network that is targeted by the attacker.

5.1. Cyber Defense Technique Comparison. In a network system, there are many network security applications for preventing different types of cyber threats. In this paper, we will discuss some of them that are most commonly and significantly used in the SCADA network. Based on the defense mechanism, cyber defense techniques can be classified into four categories: (a) obfuscation (e.g., network-based MTD), (b) end point filter (e.g., firewall/IDS/IPS), (c) secure protocol (e.g., DNP3sec), and (d) crypto encapsulation (e.g., scalence/VPNsec/GRE tunnelling). Table 4 shows security features, threats addressed and unaddressed for various cyber defense techniques used in the SCADA network.

Based on the defense performance in Table 4 and through extensive investigations, we quantify the defense capability of these cyber defense techniques against cyber-attacks in Figure 7, which is graded from 0 to 10.

Overall, each of the cyber defense techniques performs differently for different attacks and no one is one-size-fits-all. However, we can observe that network-based MTD shows better performance on most attacks, such as targeted attack, APT, command injection, MITM/hijacking, and IP spoofing intrusion. This is because the dynamic change of the system properties increases the difficulty for the attacker to identify the target, thereby reducing the probability of a successful attack. On the other hand, we also find that network-based MTD has poor performance on some attacks, such as random attack, timing attack, and data leakage. We guess that this may be the result of the attacker knowing that network-based MTD is activated and the system properties are changed. To compensate for this, it is wise to have a combination of network-based MTD and other cyber defense techniques to prevent various attacks. Therefore, network-based MTD is often adopted as a complement rather than a replacement for existing passive defense techniques.

Since defense capability comparison alone cannot represent a comprehensive analysis of these cyber defense

techniques, we quantify the system performance of them against performance parameters in Figure 8, which is graded from 0 to 10.

Overall, all the cyber defense techniques are unevenly distributed in the radar chart and they differ greatly in shape from one another. Compared to the other cyber defense techniques, network-based MTD has a relatively smooth distribution for all the performance parameters. Although some of the cyber defense techniques that are customized for the system have more optimal performance in certain aspects, additional overhead is still introduced owing to their inherent operation mechanism. For example, the latency must be introduced when the firewall or the IDS installs new rules or checks all rules in the gateway routers. Network-based MTD manipulates the network to be less static, less homogeneous, and less deterministic by dynamically changing the network topology and configurations in ways that are manageable by the defender to create an unpredictable attack surface to the adversary. Therefore, network-based MTD is also referred to as an adaptive cyber defense as it involves shifting the defense strategies from reactive to proactive technique by employing dynamic momentum to the system from its static counterparts.

5.2. Passive Monitoring Attack Test. To demonstrate the feasibility and effectiveness of AFPM in disrupting the steps of the cyber kill chain, we used OpenVSwitRC [28] as the mutation switch and OpenDaylight [29] as the mutation controller. AFPM was deployed on the OpenVSwitRC and OpenDaylight with Z3 SMT solver [30] to solve the mutation constraints. In the test, the volume of data flow is set as 8×10^5 whose rate is 1.6×10^3 pps, and the probability of the attacker monitoring a forwarding link or a routing node P^a obeys random uniform distribution on $[0.5, 0.95]$.

For comparison, we design the attack tests in different cases with respect to the length of the forwarding path: $L_T = 10, 20$ and the application of MTD: (a) static network (i.e., no MTD application), (b) MTD-RRM (i.e., MTD based on RRM), and (c) MTD-AFPM (i.e., MTD based on AFPM).

Figure 9 shows the relationship between the successful probability of passive monitoring and the network size on

TABLE 4: Difference between various cyber defense techniques.

Technique	Security features	Threats addressed	Threats unaddressed
Network-based MTD	Operational confidentiality, state obfuscation, attack surface extension	DoS, MitM, spoofing, insider threat, targeted attack	Replay and random attacks
Firewall/IDS/IPS	Monitoring, exfiltration, signature analysis, anomalous behavior detection	Malicious traffic filtering	Masquerade, authentication attack
DNP3sec	Authentication and integrity check	Replay, spoofing, modification, nonrepudiation	DoS, traffic attack, zero day exploits
Scalence/VPNsec/GRE tunnelling	Confidentiality, transparent application-level security	IPSec-application layer attack	APT, rootkit, trapdoor, stealth DoS, phishing attack, network layer attack, SSLSec-application layer attack

FIGURE 7: Defense capability comparison of different cyber defense techniques.

FIGURE 8: System performance comparison of different cyber defense techniques.

FIGURE 9: Attack test against different network sizes.

the condition that $R_A = R_D$ and the attacker can passively monitor 100 routing nodes simultaneously.

Overall, the successful probability of passive monitoring is reduced as the network size increases when the length of the forwarding path is fixed. In each case, the longer the forwarding path, the higher the successful probability of passive monitoring, when the network size is fixed. Since the static network has no strategic protection, the successful probability of passive monitoring reaches the highest among the three cases, which remains above 70%. In the two MTD cases, there is a significant reduction in the successful probability of passive monitoring. Compared to MTD-RRM, MTD-AFPM is more capable of preventing passive monitoring and especially when $L_T = 10$ and the network size is large enough, it can prevent more than 92% of passive monitoring. This is because MTD-AFPM optimizes the selection of mutation path based on the network security capacity matrix such that an optimal combination of mutation path and mutation period can be obtained according to the current network security state.

Figure 10 shows the relationship between the successful probability of passive monitoring and the number of routing nodes monitored by the attacker on the condition that $R_A = R_D$, $n = 1000$.

FIGURE 10: Attack test against different number of routing nodes monitored by the attacker.

Reverse to Figure 9, the successful probability of passive monitoring gets increased as the number of routing nodes monitored by the attacker increases when the length of the forwarding path is fixed. In each case, the longer the forwarding path, the higher the successful probability of passive monitoring, when the number of routing nodes monitored by the attacker is fixed. Compared with the static network, MTD-RRM and MTD-AFPM are advantageous against passive monitoring when the number of routing nodes monitored by the attacker is less than half of the total number of routing nodes in the network. In addition, MTD-AFPM is more effective than MTD-RRM because the optimal combination of mutation path and mutation period is adopted.

Figure 11 shows the relationship between the successful probability of passive monitoring and the attack frequency on the condition that $n = 1000$ and the attacker can passively monitor 100 routing nodes simultaneously.

We can observe that the successful probability of passive monitoring gets increased as the attack frequency increases on the condition that $R_A \leq R_D$ when the length of the forwarding path is fixed. In each case, the longer the forwarding path, the higher the successful probability of passive monitoring, when the attack frequency is fixed. Because of the fixed mutation period, MTD-RRM is equally capable of preventing passive monitoring as the static network regardless of the increase in the attack frequency on the condition that $R_A > R_D$. Different from MTD-RRM, MTD-AFPM has an optimal combination of mutation path and mutation period according to the current network security state. Therefore, even if the attacker increases the attack frequency, MTD-AFPM can still adjust the mutation period such that $R_A \leq R_D$.

Considering the impact of path mutation on network performance, we evaluate the network performance by recording the number of out-of-order packets. Figure 12 shows the proportion of out-of-order packets in different cases.

Since MTD-RRM randomly selects a feasible forwarding path for the next mutation, the proportion of the difference

FIGURE 11: Attack test against different attack frequencies.

FIGURE 12: Network test for packet disorder.

between the minimum transmission delay of the forwarding path in the next mutation period $L_{T_{RMP+1}}$ and the maximum transmission delay of the current forwarding path $L_{T_{RMP}}$ greater than the minimum inter-packet delay gets increased as the mutation frequency increases, which results in a gradual increase in the proportion of out-of-order packets. However, MTD-AFPM does not have such packet disorder problem because of our imposed forwarding path delay constraint on path mutation. This is the reason why the curve of MTD-AFPM is very close to that of the static network.

6. Conclusion and Future Work

In this paper, we propose an AFPM-based MTD technique and demonstrate through simulations that it optimizes the network performance and improves the defense capability of path mutation. In our technique, we presented solutions to the two existing problems in path mutation, respectively. First, we formalized the mutation constraints in three terms

based on the SMT to select the appropriate forwarding path. Second, we designed the mutation path generation algorithm based on the network security capacity matrix to calculate the optimal combination of mutation path and mutation period. Simulation results show that AFPM can prevent more than 92% of passive monitoring when $L_T = 10$ and 1/20 of routing nodes are monitored. In addition, the probability of packet disorder in the AFPM network is almost equivalent to that in the static network. Therefore, AFPM can maximize the defense benefits with the guarantee of the QoS.

In the future, we will incorporate IP hopping and network port hopping to increase the attack complexity and cost. Such an integrated technique can extend the attack surface to a considerable extent, even for sophisticated attack scenarios.

Data Availability

The data used to support the findings of this study are available from the corresponding authors upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors would like to acknowledge the support from NSFC (61572514), Hunan NSF (2020JJ5621), Changsha NSF (kq2007088), High-Tech Industry Sci. and Tech. Innovation Leading Plan (2020GK2029), Fund of Hunan Education Department (19C0160, 20B064), Fund of Hunan Key Lab. of Network Investi. Tech. (2020WLZC003), research plan of National University of Defense Technology (ZK21-41), and Key Laboratory of Police Internet of Things Application Ministry of Public Security, People's Republic of China.

References

- [1] R. Langner, "Stuxnet: dissecting a cyberwarfare weapon," *IEEE Security and Privacy Magazine*, vol. 9, no. 3, pp. 49–51, 2011.
- [2] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: implications for false data injection attacks," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317–3318, 2017.
- [3] C. Osborne, "Industroyer: An in-depth look at the culprit behind ukraine's power grid blackout," *ZDNet.com*, vol. 28, 2018.
- [4] M. Bogdanoski, T. Suminoski, and A. Risteski, "Analysis of the syn flood DoS attack," *International Journal of Computer Network and Information Security*, vol. 5, no. 8, pp. 1–11, 2013.
- [5] E. A. Shaer, Q. Duan, and J. H. Jafarian, "Random host mutation for moving target defense," in *Proceedings of the International Conference On Security And Privacy In Communication Systems*, pp. 310–327, Springer, Padua, Italy, September 2012.
- [6] P. Kampanakis, H. Perros, and T. Beyene, "SDN-based solutions for moving target defense network protection," in *Proceedings of IEEE International Symposium On a World Of Wireless, Mobile and Multimedia Networks 2014*, pp. 1–6, IEEE, Sydney, NSW, Australia, June 2014.
- [7] S. Wang, L. Zhang, and C. Tang, "A new dynamic address solution for moving target defense," in *Proceedings of the 2016 IEEE Information Technology, Networking, Electronic and Automation Control Conference*, pp. 1149–1152, IEEE, Chongqing, China, May 2016.
- [8] H. Q. Zhang, C. Lei, D. X. Chang, and Y. J. Yang, "Network moving target defense technique based on collaborative mutation," *Computers & Security*, vol. 70, pp. 51–71, 2017.
- [9] S. Yoon, J. H. Cho, D. S. Kim, T. J. Moore, F. F. Nelson, and H. Lim, "Attack graph-based moving target defense in software-defined networks," *IEEE Transactions on Network and Service Management*, vol. 17, no. 3, pp. 1653–1668, 2020.
- [10] T. Yadav and A. M. Rao, "Technical aspects of cyber kill chain," *Communications in Computer and Information Science*, Springer, in *Proceedings of the International Symposium On Security In Computing And Communication*, pp. 438–452, April 2015.
- [11] S. Nelakuditi, S. Lee, Y. Yu, Z. L. Zhang, and C. N. Chuah, "Fast local rerouting for handling transient link failures," *IEEE/ACM Transactions on Networking*, vol. 15, no. 2, pp. 359–372, 2007.
- [12] D. Kewley, R. Fink, J. Lowry, and M. Dean, "Dynamic approaches to thwart adversary intelligence gathering," in *Proceedings DARPA Information Survivability Conference and Exposition II. DISCEX'01*, vol. 1, pp. 176–185, Anaheim, CA, USA, June 2001.
- [13] Q. Duan, E. Al-Shaer, and H. Jafarian, "Efficient random route mutation considering flow and network constraints," in *Proceedings of the 2013 IEEE Conference On Communications And Network Security (CNS)*, pp. 260–268, Washington D.C., USA, October 2013.
- [14] J. H. Jafarian, E. A. Shaer, and Q. Duan, "Formal approach for route agility against persistent attackers," in *Computer Security-ESORICS 2013*, J. Crampton, S. Jajodia, and K. Mayes, Eds., Springer, Berlin, Heidelberg, pp. 237–254, 2013.
- [15] K. Zkik, A. Sebbar, Y. Baddi, and M. Boulmalf, "Secure multipath mutation snpm in moving target defense based on SDN," *Procedia Computer Science*, vol. 151, pp. 977–984, 2019.
- [16] S. Bohacek, J. Hespanha, J. Lee, C. Lim, and K. Obraczka, "Game theoretic stochastic routing for fault tolerance and security in computer networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 18, no. 9, pp. 1227–1240, 2007.
- [17] T. Shu, M. Krunz, and S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," *IEEE Transactions on Mobile Computing*, vol. 9, no. 7, pp. 941–954, 2010.
- [18] F. Gillani, E. A. Shaer, S. Lo, Q. Duan, M. Ammar, and E. Zegura, "Agile Virtualized Infrastructure to Proactively Defend against Cyber Attacks," in *Proceedings of the 2015 IEEE Conference on Computer Communications*, pp. 729–737, INFOCOM, Hong Kong, China, April 2015.
- [19] W. Stallings, *Network Security Essentials Applications And Standards, 5/E*, vol. 22, Second edition, 2003.
- [20] P. G. Teodoro, J. D. Verdejo, G. M. Fernández, and E. Vázquez, "Anomaly-based network intrusion detection: techniques, systems and challenges," *Computers & Security*, vol. 28, no. 1–2, pp. 18–28, 2009.
- [21] M. Yu, Y. Yi, J. Rexford, and M. Chiang, "Rethinking virtual network embedding," *ACM SIGCOMM - Computer Communication Review*, vol. 38, no. 2, pp. 17–29, 2008.

- [22] R. Cohen, L. E. Lewin, J. S. Naor, and D. Raz, "On the effect of forwarding table size on SDN network utilization," in *Proceedings of the IEEE INFOCOM 2014-IEEE Conference on Computer Communications*, pp. 1734–1742, IEEE, Toronto, ON, Canada, April 2014.
- [23] M. Huang, W. Liang, Z. Xu, W. Xu, S. Guo, and Y. Xu, "Dynamic routing for network throughput maximization in software-defined networks," in *Proceedings of the IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications*, pp. 1–9, IEEE, San Francisco, CA, USA, April 2016.
- [24] B. Peng, A. H. Kemp, and S. Boussakta, "QoS routing with bandwidth and hop-count consideration: a performance perspective," *JCM*, vol. 1, no. 2, pp. 1–11, 2006.
- [25] V. Jacobson, "Congestion avoidance and control," *ACM SIGCOMM Computer Communication Review*, vol. 18, no. 4, pp. 314–329, 1988.
- [26] S. Han, Z. Peng, and S. Wang, "The maximum flow problem of uncertain network," *Information Sciences*, vol. 265, pp. 167–175, 2014.
- [27] J. X. Hao and J. B. Orlin, "A faster algorithm for finding the minimum cut in a directed graph," *Journal of Algorithms*, vol. 17, no. 3, pp. 424–446, 1994.
- [28] N. McKeown, T. Anderson, H. Balakrishnan et al., "Open-Flow: enabling innovation in campus networks," *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 2, pp. 69–74, 2008.
- [29] J. Medved, R. Varga, A. Tkacik, and K. Gray, "QoS: towards a model-driven SDN controller architecture," in *Proceedings of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014*, pp. 1–6, IEEE, Sydney, NSW, Australia, June 2014.
- [30] L. D. Moura and N. Bjørner, "Z3: an efficient SMT solver," in *Proceedings of the International Conference on Tools And Algorithms for the Construction and Analysis of Systems*, pp. 337–340, Springer, Budapest, Hungary, March 2008.