

DVA-IR: Runtime Integrity Attestation for Secure VNF Operation in NFV

DOI: <https://doi.org/10.54654/isj.v1i27.1160>

Vu Ngoc Hoa, Nguyen Viet Phan, Nguyen Tuan Hung, Ngo Hai Anh*

Abstract— Network Function Virtualization (NFV) improves flexibility and cost efficiency, but it also creates new security risks at the virtualization, VNF, service-chain, and orchestration layers. This paper focuses on a specific NFV security problem: detecting and containing runtime compromise of Virtual Network Functions (VNFs), including unauthorized binary, configuration, or memory-state modification, invalid attestation responses, and no-response events. We propose Dynamic VNF Attestation and Instant Response (DVA-IR), a framework that combines periodic remote attestation of running VNFs with MANO-driven isolation and replacement of compromised VNFs. Unlike access-control-only or signature-based mechanisms, DVA-IR verifies runtime VNF integrity and immediately updates service-chain forwarding behavior when compromise is detected. A Monte Carlo simulation compares DVA-IR with manual monitoring, signature-based IDS/IPS, and DVA-only attestation. The results show that DVA-IR achieves high detection quality, rapid containment, and significantly reduced service downtime, while its centralized orchestration overhead remains manageable for small-to-medium and medium-to-large NFV deployments.

Tóm tắt— Ảo hóa chức năng mạng (Network Function Virtualization - NFV) giúp nâng cao tính linh hoạt và hiệu quả chi phí trong triển khai hạ tầng mạng, nhưng đồng thời cũng làm phát sinh các rủi ro an toàn mới tại các lớp ảo hóa, VNF, chuỗi dịch vụ và điều phối. Bài báo này tập trung vào một

vấn đề bảo mật cụ thể trong môi trường NFV, phát hiện và cô lập các chức năng mạng ảo (Virtual Network Functions - VNFs) bị xâm phạm trong quá trình vận hành, bao gồm các trường hợp mã nhị phân, cấu hình hoặc trạng thái bộ nhớ bị sửa đổi trái phép, phản hồi chứng thực không hợp lệ hoặc VNF không phản hồi. Trên cơ sở đó, bài báo đề xuất khung xác thực VNF động và phản hồi tức thì (DVA-IR), kết hợp cơ chế chứng thực từ xa định kỳ đối với các VNF đang chạy với khả năng cô lập và thay thế VNF bị xâm phạm thông qua hệ thống quản lý và điều phối MANO. Khác với các cơ chế chỉ dựa trên kiểm soát truy cập hoặc phát hiện theo chữ ký, DVA-IR kiểm tra trực tiếp tính toàn vẹn của VNF trong thời gian vận hành và cập nhật ngay hành vi chuyển tiếp của chuỗi dịch vụ khi phát hiện dấu hiệu xâm phạm. Kết quả mô phỏng Monte Carlo, trong đó DVA-IR được so sánh với giám sát thủ công, IDS/IPS dựa trên chữ ký và cơ chế chứng thực DVA đơn lẻ, cho thấy phương pháp đề xuất đạt chất lượng phát hiện cao, khả năng cô lập nhanh và giảm đáng kể thời gian gián đoạn dịch vụ, trong khi chi phí điều phối tập trung vẫn ở mức có thể chấp nhận đối với các triển khai NFV quy mô nhỏ đến trung bình và trung bình đến lớn.

Keywords— NFV; security; DVA-IR; AIR.

Từ khóa— NFV; an toàn thông tin; DVA-IR; AIR.

I. INTRODUCTION

The development of next-generation networks, especially 5G, has driven a revolution in network architecture, where flexibility, scalability, and cost-effectiveness are key factors [1–3]. In this context, NFV has emerged as a foundational technology, enabling Service Providers (SPs) to transition network services from dedicated, proprietary hardware infrastructure to a more agile virtualized

This manuscript was received on October 15, 2025. It was reviewed on March 2, 2026, revised on May 20, 2026 and accepted on June 8, 2026.

* Corresponding author.

environment [2, 4, 5]. NFV decouples Network Functions (NFs) such as firewalls, load balancers, and Intrusion Detection/Prevention Systems (IDS/IPS) from physical hardware devices and deploys them as software entities called VNFs [2, 6]. These VNFs can run on Commercial-Off-The-Shelf (COTS) servers, significantly reducing both Capital Expenditure (CAPEX) and Operating Expenditure (OPEX) [4, 5, 7].

The NFV architecture, standardized by the European Telecommunications Standards Institute (ETSI), consists of three main components: NFV Infrastructure (NFVI), VNFs, and Management and Orchestration (MANO) [4, 5, 8]. VNFs are often connected in a logical sequence to create complete network services, a concept known as Service Function Chaining (SFC) [2], [9, 10]. SFC provides high flexibility in routing traffic through various network functions according to service and policy requirements [11, 12]. Software-Defined Networking (SDN) is often integrated with NFV to provide centralized control and orchestration, making the creation and management of service chains more efficient [13–15].

Although NFV offers numerous outstanding benefits such as cost-effectiveness, flexibility, and reduced energy consumption [4, 5], the transition to a virtualized environment is also accompanied by new and complex security challenges [5, 16]. The attack surface is expanded due to the emergence of new virtualization layers like the hypervisor, virtual machines (VMs), and containers [4, 5]. Threats come not only from external sources but also from within the system (malicious insiders), where administrators with privileged access to the virtualization layer can cause serious damage [5, 17]. The complex architectural layers and the involvement of multiple vendors in an NFV ecosystem also make identifying and remedying security vulnerabilities more difficult [5, 18].

Topological risks, where misconfiguration of virtual network components can lead to security holes, are also a significant concern [5, 19]. Furthermore, ensuring the integrity, availability, and confidentiality of data and VNFs in a dynamic and flexible environment like NFV requires advanced and comprehensive security solutions

[6, 20]. Traditional security mechanisms, designed for static hardware-based networks, are often not effective enough to protect the NFV environment [21]. Therefore, researching and developing new security frameworks, advanced algorithms, and techniques to address these challenges is an urgent requirement, ensuring that the benefits of NFV can be leveraged safely and sustainably [22 - 24].

II. BACKGROUND, NFV SECURITY THREATS AND RELATED WORK

The field of NFV security has attracted significant attention because NFV shifts network functions from dedicated appliances to software components running on shared virtualized infrastructure. This shift improves programmability and scalability, but it also changes the threat model. In addition to conventional network attacks, NFV systems must address threats arising from the hypervisor, virtual machines or containers, VNF images, service-function chains, and Management and Orchestration (MANO) components [5, 16, 24].

A. NFV security threats and the scope of this work

Several studies have surveyed NFV architectures, service function chaining (SFC), and open security challenges. Mijumbi et al. [27] identified early NFV research challenges, while Pattaranantakul et al. [16] analyzed NFV security from use-case-driven threats to countermeasures. Adoga and Pezaros [2] reviewed NFV and SFC frameworks, including resilience and fault recovery, and Zhang et al. [6] classified NFV platforms and discussed future security directions. More recently, Zoure et al. [24] surveyed anomalies in NFV network services and verification methods. Related studies published in the *Journal of Science and Technology on Information Security* are also relevant to the detection-and-response perspective of this work. Dung et al. investigated deep-learning-based network reconnaissance attack detection, while Hai et al. proposed UET.SIR as an information-security incident-handling support solution for e-government. These studies do not address runtime VNF attestation directly, but they provide useful domestic references on network-attack detection and incident response,

which are related to the motivation of DVA-IR [25, 26].

The threat surface of NFV can be grouped into four layers. First, the NFVI layer includes risks related to shared physical resources, hypervisors, virtualization isolation, and privileged administrators [5, 20]. Second, the VNF layer includes vulnerable images, malicious or compromised VNFs, unauthorized runtime changes, and tampered configurations. Third, the SFC layer includes incorrect traffic steering, bypassed security functions, and compromised VNFs inside a service chain [10, 11]. Fourth, the MANO layer includes orchestration abuse, insecure APIs, and delayed or inconsistent response actions [22, 31].

This paper does not claim to solve all NFV security issues. Its scope is narrower and more verifiable: runtime VNF integrity protection. Specifically, it targets cases in which a running VNF is modified, becomes untrustworthy, fails to provide a valid integrity proof, or must be isolated from active SFCs to prevent further impact.

B. Existing countermeasures

Existing NFV security countermeasures can be summarized into four groups. Encryption and strong authentication protect data in transit, control administrative access, and reduce credential-based compromise [5, 20]. Zero Trust architectures apply the principle of “never trust, always verify” by enforcing least privilege, contextual access decisions, and micro-segmentation [5, 32]. Standardized interfaces and APIs, including ETSI NFV-based interfaces and REST-style management APIs, reduce heterogeneity and support consistent policy enforcement in multi-vendor environments [5, 8]. Availability-oriented techniques, such as VNF state replication, fault-tolerant chaining, and fast failover, improve service continuity when failures occur [29, 30, 38].

These mechanisms are important but have different primary objectives. Encryption and MFA protect communication and access, but they do not continuously verify the integrity of a running VNF. Zero Trust focuses mainly on identity, access, and policy enforcement, but additional mechanisms are required to attest runtime state. IDS/IPS mechanisms are useful for

traffic-level attacks, but signature-based detection can miss internal VNF tampering or insider-induced state changes. Fault-tolerant SFC mechanisms improve availability, but they usually do not decide whether a VNF is trustworthy at runtime.

C. Research gap and positioning

The related work shows a gap between integrity verification and operational response. Some approaches can detect anomalies or improve resilience, while others enforce security policies, but fewer solutions integrate continuous runtime VNF integrity attestation with immediate SFC-level containment and VNF replacement. The proposed DVA-IR framework is positioned to fill this gap by linking three functions: runtime attestation, trust-state decision, and MANO-driven response.

III. PROPOSED DVA-IR FRAMEWORK

A. Design objective and threat model

The objective of DVA-IR is to detect runtime integrity compromise of VNFs and rapidly contain its impact on active service chains. The assumed attacker can modify a VNF binary, configuration, or critical runtime state; cause an attestation timeout; or attempt to return an invalid or forged attestation response. The attacker may also be an insider with access to part of the virtualization environment. However, the NFVO-side baseline repository, public-key registry, and orchestration control logic are assumed to be trusted and protected.

DVA-IR consists of two coupled algorithms. The first algorithm, Dynamic VNF Attestation (DVA), periodically challenges each active VNF and verifies its signed integrity measurement. The second algorithm, Attestation-based Instant Response (AIR), consumes DVA trust states and performs isolation, forwarding-rule update, and VNF replacement through MANO and the Service Function Forwarder (SFF).

B. Algorithm 1: Dynamic VNF Attestation

DVA verifies whether a running VNF remains consistent with its trusted baseline. A mismatch between the current integrity measurement and the baseline, an invalid signature, or a timeout is treated as evidence that the VNF is no longer trustworthy.

Algorithm 1 Dynamic VNF Attestation (DVA)

Require: $V, B_v, T_{attest}, \tau, K_{pub,v}, K_{priv,v}$
Ensure: $S_v \in \{\text{TRUSTED}, \text{COMPROMISED}\}$ for each $v \in V$

```

1: procedure NFVO_ATTEST_LOOP
2:   while true do
3:      $\text{sleep}(T_{attest})$ 
4:     for all  $v \in V$  do
5:        $n_v \leftarrow \text{Nonce}()$ 
6:        $\text{Request}(v, n_v)$ 
7:     end for
8:     for all  $v \in V$  do
9:        $R \leftarrow \text{Listen}(v, \tau)$ 
10:      if  $R$  is received then
11:         $(M_v, \sigma_v, n_v) \leftarrow R$ 
12:         $ok \leftarrow \text{Verify}(\sigma_v, M_v || n_v, K_{pub,v})$ 
13:        if  $ok$  then
14:           $H_v \leftarrow \text{HashFrom}(M_v)$ 
15:           $H_v^0 \leftarrow \text{HashFrom}(B_v)$ 
16:          if  $H_v = H_v^0$  then
17:             $S_v \leftarrow \text{TRUSTED}$ 
18:          else
19:             $S_v \leftarrow \text{COMPROMISED}$ 
20:          end if
21:        else
22:           $S_v \leftarrow \text{COMPROMISED}$   $\triangleright$  Invalid proof
23:        end if
24:      else
25:         $S_v \leftarrow \text{COMPROMISED}$   $\triangleright$  No response
26:      end if
27:    end for
28:  end while
29: end procedure

30: procedure VNF_HANDLE_REQUEST( $v, n_v$ )
31:    $C_v \leftarrow \text{CollectState}()$   $\triangleright$  Binary/config/memory
32:    $H_v \leftarrow \text{Hash}(C_v)$ 
33:    $M_v \leftarrow \text{Measure}(H_v)$ 
34:    $\sigma_v \leftarrow \text{Sign}(M_v || n_v, K_{priv,v})$ 
35:    $\text{Send}(M_v, \sigma_v, n_v)$ 
36: end procedure

```

Algorithm 2 Attestation-based Instant Response (AIR)

Require: V, S_v, C, F_c, B_v , SFF/MANO APIs
Ensure: Compromised VNFs are isolated, replaced, and SFC rules are updated

```

1: procedure MANO_MONITOR_AND_REACT
2:   for all  $v \in V$  do
3:     if  $S_v = \text{COMPROMISED}$  then
4:        $\text{LogEvent}(v)$ 
5:        $I \leftarrow \text{FindChains}(v, C)$ 
6:       for all  $c \in I$  do
7:          $\text{SetSFF}(F_c, \text{"DROP"})$ 
8:       end for
9:        $v' \leftarrow \text{NewCleanVNF}(B_v)$ 
10:      if  $v'$  is created then
11:        for all  $c \in I$  do
12:           $c' \leftarrow \text{Replace}(c, v, v')$ 
13:           $\text{SetSFF}(F_c, \text{"FORWARD"}, c')$ 
14:        end for
15:         $\text{Terminate}(v)$ 
16:         $V \leftarrow (V \setminus \{v\}) \cup \{v'\}$ 
17:      else
18:         $\text{AlertOperator}(v)$ 
19:      end if
20:       $S_v \leftarrow \text{HANDLED}$ 
21:    end if
22:  end for
23: end procedure

```

The proposed method is not intended to replace encryption, authentication, IDS/IPS, or fault-tolerant SFC mechanisms. Instead, it complements them by addressing a security gap that is difficult for those mechanisms to cover: runtime integrity compromise of VNFs after deployment.

IV. SECURITY SCOPE AND COMPARISON WITH EXISTING METHODS

C. Algorithm 2: Attestation-based Instant Response

AIR connects the trust decision from DVA with orchestration actions. When a VNF is marked as compromised, AIR finds all SFCs that contain the VNF, updates SFF rules to block or redirect affected traffic, instantiates a clean replacement VNF, and updates service chains to restore service continuity.

D. Operational interpretation

DVA-IR implements an integrity-oriented form of continuous verification. The nonce in Algorithm 1 prevents replay of old valid measurements, while the signature check prevents forged measurements from being accepted. A hash mismatch indicates that the running VNF no longer matches the trusted baseline. Algorithm 2 then translates this trust decision into operational defense by isolating affected flows and replacing the compromised VNF.

A. Security issues addressed by DVA-IR

Table I clarifies how the proposed algorithms address concrete NFV security issues. This mapping also defines the boundary of the contribution: DVA-IR focuses on runtime VNF trust and response, not on every possible NFV security threat.

B. Comparison with existing approaches

Table II compares DVA-IR with representative approaches discussed in the related work. The comparison shows why the proposed framework is different from purely preventive, traffic-inspection, or availability-oriented mechanisms.

The comparison addresses the central concern that the proposed algorithm must be linked to concrete security issues. DVA-IR is most suitable for cases where the main risk is that a VNF

TABLE I. MAPPING BETWEEN NFV SECURITY ISSUES AND DVA-IR MECHANISMS

NFV security issue	DVA-IR mechanism	Main algorithmic component	Expected security effect
Unauthorized modification of VNF binary, configuration, or critical memory state	Periodic measurement and comparison with trusted baseline B_v	DVA	Runtime integrity compromise is detected rather than only deployment-time integrity being checked
Invalid or forged attestation response	Public-key signature verification and nonce-based challenge-response	DVA	Forged or replayed measurements are rejected
No response or timeout from a VNF	Timeout threshold τ and fail-closed trust-state assignment	DVA	Unresponsive VNFs are treated as unsafe and escalated for response
Compromised VNF inside an active SFC	Identification of affected chains and immediate SFF rule update	AIR	Traffic is dropped or redirected before lateral movement can continue
Need to restore service after isolation	Instantiation of clean replacement VNF and chain update	AIR	Security response is combined with service restoration

TABLE II. QUALITATIVE COMPARISON WITH EXISTING NFV SECURITY AND RESILIENCE APPROACHES

Approach	Runtime integrity check	Insider tampering detection	Automated isolation	Clean replacement	Main limitation
Encryption and MFA [5], [20]	No	Limited	No	No	Protect access and communication, but not VNF runtime state
Zero Trust access control [5], [32]	Partial	Limited	Policy-dependent	No	Verifies access context, but usually not VNF memory or binary integrity
Signature IDS/IPS	No	Weak	Partial	No	Effective for known traffic patterns, weak against internal VNF state modification
Fault-tolerant SFC / replication [29], [30], [38]	No	Weak	Failure-oriented	Partial	Improves availability, but does not decide whether a VNF is compromised
DVA-only attestation	Yes	Yes	No	No	Detects integrity violation but requires separate response process
DVA-IR	Yes	Yes	Yes	Yes	Adds attestation and orchestration overhead; requires trusted baseline management

remains active in an SFC after its runtime state has become untrusted. In such cases, detection time alone is insufficient; the response mechanism must also reduce containment delay and service exposure.

V. EVALUATION OF THE IMPROVED ALGORITHM

A. Evaluation objectives and scope

The evaluation assesses four aspects that directly correspond to the design goals of DVA-IR: detection quality, containment and recovery performance, service availability impact, and scalability under increasing orchestration load. The purpose of the simulation is not to prove that the proposed method solves all NFV security issues. Instead, it evaluates a narrower claim: DVA-IR is effective for runtime VNF integrity compromise detection, rapid containment of affected service chains, and service restoration through automated remediation.

B. Simulation setup

We implemented a Python-based Monte Carlo simulation to emulate an NFV environment with one NFVO, multiple active VNFs, and multiple SFCs. In the default configuration, the simulation includes 50 VNFs and 10 SFCs, where each SFC consists of 3–5 VNFs. To evaluate scalability, the number of VNFs is further increased up to 1000.

The simulation includes multiple event types relevant to integrity-oriented NFV security:

- binary tampering;
- configuration tampering;
- critical memory tampering;
- benign state updates;
- timeout/no-response events;
- invalid signature events.

The main simulation parameters are: base environment of 50 VNFs and 10 SFCs; attestation intervals $T_{attest} \in \{5, 10, 30, 60\}$ seconds; 2000 runs for detection and timing experiments; 1200 runs for scalability

experiments; and VNF scale values of 50, 100, 250, 500, and 1000 VNFs.

We compare four methods: Manual monitoring, signature-based IDS/IPS, DVA-only attestation, and the proposed DVA-IR. Manual monitoring has no automatic attestation or automated response. IDS/IPS represents traffic-signature-based detection. DVA-only performs integrity attestation but does not automatically isolate or replace compromised VNFs. DVA-IR combines attestation with MANO-driven isolation and replacement.

C. Evaluation metrics

The revised evaluation uses the following metrics:

- **Detection quality:** Precision, Recall, F1-score, and False Positive Rate (FPR);
- **Containment performance:** mean containment delay, measured from the moment a VNF is compromised to the moment affected traffic is isolated;
- **Availability impact:** mean service downtime, measured in flow-seconds;
- **Scalability:** attestation overhead, NFVO CPU demand, and queue delay as the number of VNFs increases.

D. Detection quality results

Table III and Figure 1 summarize detection quality across methods. DVA-IR achieves the best overall balance between precision and recall. It reaches a precision of 0.999, recall of 0.962, F1-score of 0.980, and FPR of 0.002. DVA-only also achieves high recall (0.967), but its false positive rate is higher (0.119), indicating that integrity attestation without confirmation and response logic may generate more unnecessary alarms. In contrast, signature-based IDS/IPS obtains lower recall (0.368), showing that it misses many integrity-compromise events that do not match predefined signatures.

These results indicate that integrity-oriented attestation is better suited than conventional signature-based inspection for detecting runtime VNF compromise, especially in scenarios involving insider tampering or unauthorized internal state modification.

TABLE III. DETECTION QUALITY ACROSS METHODS

Method	Precision	Recall	F1-score	FPR
IDS/IPS	0.966	0.368	0.533	0.029
DVA-Only	0.947	0.967	0.957	0.119
DVA-IR	0.999	0.962	0.980	0.002

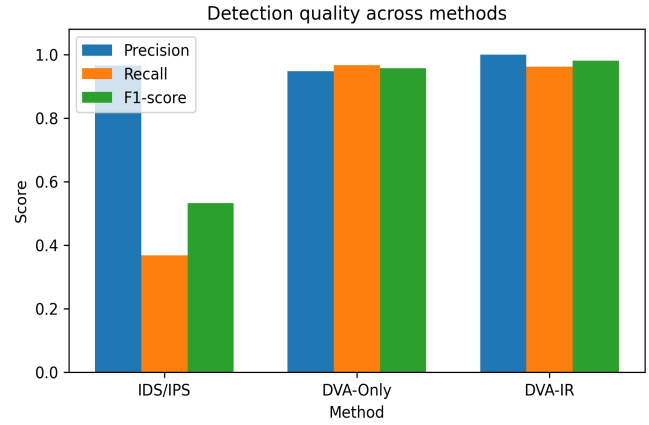


Figure 1. Detection quality across methods in terms of precision, recall, and F1-score

E. Containment performance

To evaluate operational response, we measured the time required to contain compromised VNFs after compromise. Figure 2 shows the mean containment delay as a function of T_{attest} . At $T_{attest} = 10$ s, DVA-IR achieves a mean containment delay of 5.16 s, whereas DVA-only requires 495.50 s and manual response requires 8970.20 s.

This result highlights an important distinction between detection and security response. DVA-only can identify integrity violations, but without orchestration-driven automated mitigation, its containment time remains too large for practical protection. The integration of AIR with DVA therefore provides a major practical advantage by rapidly updating the forwarding behavior of affected SFCs, isolating the compromised VNF, and triggering replacement from a clean image.

F. Availability impact

In addition to detection and containment, we evaluated the effect of the proposed method on service continuity. Table IV and Figure 3 show that DVA-IR substantially reduces service downtime. At $T_{attest} = 10$ s, the mean downtime of DVA-IR is

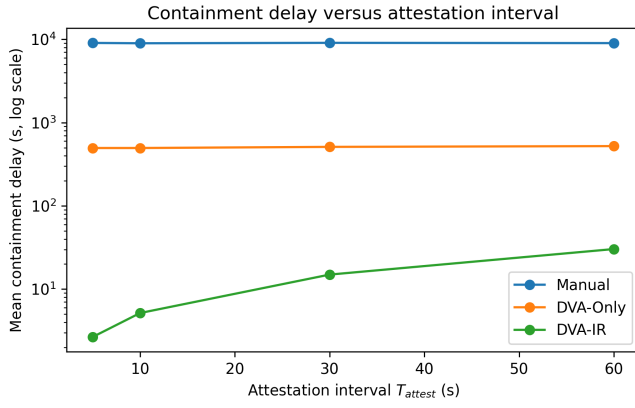


Figure 2. Mean containment delay versus attestation interval T_{attest} for different methods

TABLE IV. CONTAINMENT AND AVAILABILITY RESULTS AT $T_{attest} = 10$ s

Method	Mean containment delay (s)	Mean downtime (flow-seconds)
Manual	8970.20	–
DVA-Only	495.50	2157367.30
DVA-IR	5.16	22394.85

22394.85 flow-seconds, compared with 2157367.30 flow-seconds for DVA-only.

This reduction indicates that the proposed automated response mechanism is not only a security enhancement but also a resilience mechanism. By isolating and replacing compromised VNFs quickly, the framework reduces the duration during which service flows remain disrupted or exposed to a compromised chain.

G. Scalability and overhead

Fig. 4 presents the scalability behavior of DVA-IR. The results indicate that the framework remains practical at moderate scale, but orchestration overhead increases with the number of VNFs. At 1000 VNFs, the mean attestation overhead reaches 1957.48 ms, normalized NFVO CPU demand reaches 112.51%, and the queue delay is 1.60 ms.

These findings suggest that the proposed method is feasible for small-to-medium and medium-to-large deployments, but a centralized NFVO may become a bottleneck at very large scale. Therefore, future work should investigate distributed attestation, hierarchical orchestration, or parallel verification to improve scalability.

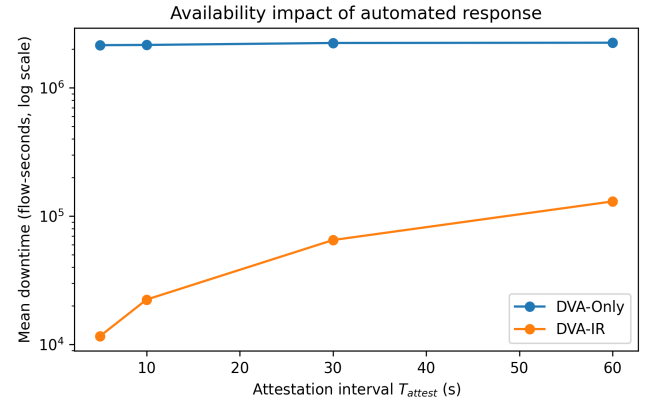


Figure 3. Availability impact versus attestation interval, measured as mean downtime in flow-seconds

TABLE V. SCALABILITY SNAPSHOT OF DVA-IR AT 1000 VNFs

Number of VNFs	Attestation overhead (ms)	NFVO CPU demand (%)	Queue delay (ms)
1000	1957.48	112.51	1.60

H. Summary of findings

Overall, the simulation supports three findings. First, runtime integrity attestation improves detection of VNF compromise events that are difficult for signature-based traffic inspection. Second, detection alone is insufficient; automated MANO-level containment substantially reduces exposure time. Third, DVA-IR can improve service continuity by replacing compromised VNFs, although very large deployments may require distributed attestation to avoid a centralized NFVO bottleneck.

VI. DISCUSSION

The simulation results provide a clearer understanding of the actual contribution of DVA-IR. The comparison with IDS/IPS shows that traditional signature-based detection is not sufficient for runtime integrity compromise in VNFs, especially when the attack manifests as an internal state modification rather than as a known traffic signature. This observation is consistent with the design motivation of DVA, which verifies the integrity of running VNFs rather than only inspecting traffic patterns.

The comparison between DVA-only and DVA-IR demonstrates that accurate detection alone is not enough. DVA-only achieves high

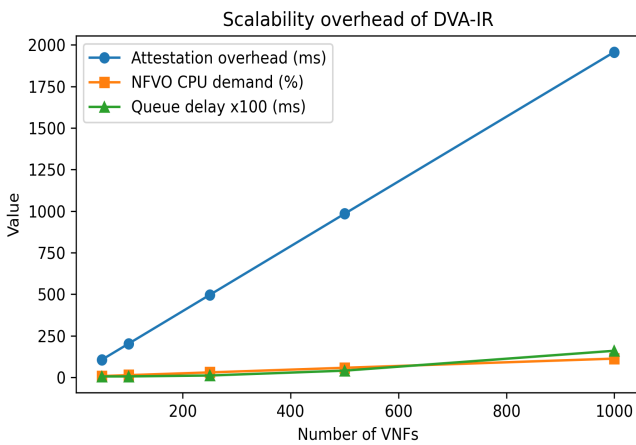


Figure 4. Scalability of DVA-IR in terms of attestation overhead, NFVO CPU demand, and queue delay

recall, but its containment delay and service downtime remain substantially larger because it lacks immediate orchestration-driven remediation. This result highlights the practical significance of AIR as the component that translates integrity detection into rapid operational defense.

The availability results show that automated replacement is an important property of the proposed framework. In NFV environments, security mechanisms should ideally preserve service continuity rather than only report anomalies. By instantiating a clean VNF and rerouting the affected service chain, DVA-IR acts not only as a security control but also as a self-healing mechanism.

At the same time, the evaluation clarifies the limitations of the method. The scalability experiment shows that as the number of VNFs becomes very large, centralized orchestration overhead can become significant. This means that the proposed approach should be interpreted as a viable integrity-protection framework for small-to-medium and medium-to-large NFV deployments, while very large-scale environments may require a distributed attestation architecture.

Another limitation is that the present study is based on simulation rather than on a real NFV testbed. Although the simulation includes multiple event types, baseline methods, and service-chain effects, the results should still be interpreted as evidence of potential effectiveness under the assumed orchestration and threat model, rather than as a complete proof of production performance.

VII. CONCLUSION

This paper addressed the problem of runtime VNF integrity protection in NFV environments. Instead of claiming to solve all NFV security issues, the work focused on detecting and containing compromised VNFs that may have undergone unauthorized binary, configuration, or memory-state modification, or that fail to provide valid attestation responses. The proposed DVA-IR framework combines dynamic VNF attestation with MANO-driven instant response. DVA verifies the runtime integrity of active VNFs, while AIR isolates compromised VNFs, updates service-chain forwarding rules, and triggers replacement from clean images.

The comparison and evaluation directly show how the proposed method differs from previous approaches. Compared with signature-based IDS/IPS, DVA-IR better addresses internal VNF integrity compromise. Compared with DVA-only attestation, DVA-IR reduces containment delay and service downtime through automated response. The simulation results show high detection quality, fast containment, and significant availability improvement, with manageable overhead at moderate scale. Future work will focus on validating the framework in a real NFV testbed, improving secure baseline update procedures, reducing false positives, and designing distributed attestation for very large-scale deployments.

REFERENCES

- [1] F. Z. Yousaf, M. Bredel, S. Schaller, and F. Schneider, "NFV and SDN-Key technology enablers for 5G networks," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 11, pp. 2468–2478, Nov. 2017.
- [2] H. U. Adoga and D. P. Pazaros, "Network Function Virtualization and Service Function Chaining Frameworks: A Comprehensive Review of Requirements, Objectives, Implementations, and Open Research Challenges," *Future Internet*, vol. 14, no. 2, pp. 59, Feb. 2022.
- [3] A. Kak, "Towards 6G Through SDN and NFV-Based Solutions for Terrestrial and Non-Terrestrial Networks," Ph.D. Thesis, Georgia Institute of Technology, Atlanta, GA, USA, 2021.
- [4] A. A. A. Shittu, "Network Function Virtualization Technology Adoption Strategies," Doctoral Study, Walden University, 2021.
- [5] N. A. S. binti Suhaimi, "Network Function Virtualization Security Challenges and Solutions," *arXiv preprint*, July 16, 2024.

- [6] T. Zhang, H. Qiu, L. Linguaglossa, W. Cerroni, and P. Giaccone, "NFV platforms: Taxonomy, design choices and future challenges," *IEEE Trans. Netw. Serv. Manag.*, vol. 18, no. 1, pp. 30–48, Mar. 2021.
- [7] I. Morris, "NFV Promises Cost Savings of Nearly 70% Study" (2015), Access time: 22/05/2026, *Light Reading*.
- [8] ETSI, "Network Functions Virtualisation (NFV): Architectural Framework," Technical Report 002 V1.1.1, 2013.
- [9] K. Kaur, V. Mangat, and K. Kumar, "A comprehensive survey of service function chain provisioning approaches in SDN and NFV architecture," *Comput. Sci. Rev.*, vol. 38, pp. 100298, 2020.
- [10] A. M. Medhat, T. Taleb, A. Elmangoush, G. A. Carella, S. Covaci, and T. Magedanz, "Service function chaining in next generation networks: State of the art and research challenges," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 216–223, Feb. 2017.
- [11] H. Hantouti, N. Benamar, T. Taleb, and A. Laghrissi, "Traffic steering for service function chaining," *IEEE Commun. Surv. Tutor.*, vol. 21, no. 1, pp. 487–507, 2018.
- [12] B. Dab, I. Fajjari, M. Rohon, C. Auboin, and A. Diquélou, "An Efficient Traffic Steering for Cloud-Native Service Function Chaining," in *Proc. 2020 23rd Conf. on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*, Paris, France, pp. 71–78, 2020.
- [13] M. S. Bonfim, K. L. Dias, and S. F. Fernandes, "Integrated NFV/SDN architectures: A systematic literature review," *ACM Comput. Surv. (CSUR)*, vol. 51, no. 6, pp. 1–39, 2019.
- [14] Y. Li and M. Chen, "Software-defined network function virtualization: A survey," *IEEE Access*, vol. 3, pp. 2542–2553, 2015.
- [15] D. E. Sarmiento, A. Lebre, L. Nussbaum, and A. Chari, "Decentralized SDN Control Plane for a Distributed Cloud-Edge Infrastructure: A Survey," *IEEE Commun. Surv. Tutor.*, vol. 23, no. 1, pp. 256–281, 2021.
- [16] M. Pattaranantakul, R. He, Q. Song, Z. Zhang, and A. Meddahi, "NFV security survey: From use case driven threat analysis to state-of-the-art countermeasures," *IEEE Commun. Surv. Tutor.*, vol. 20, no. 4, pp. 3330–3368, 2018.
- [17] V. Khera, "Are you aware of the security risks of Network Function Virtualization?" (2019), Access time: 22/05/2026, *Cybersecurity Magazine*.
- [18] S. Cherrared, S. Imadali, E. Fabre, G. Gössler, and I. G. B. Yahia, "A survey of fault management in network virtualization environments: Challenges and solutions," *IEEE Trans. Netw. Serv. Manag.*, vol. 16, no. 4, pp. 1537–1551, 2019.
- [19] L. Maojun, "Securing NFV the smart way" (2017), Access time: 22/05/2026, *Huawei*.
- [20] Thales, "Virtualized Networks and Real Risks: Best Practices for Securing Network Function Virtualization Environment," White Paper, 2019.
- [21] Z. Yan, P. Zhang, and A. V. Vasilakos, "A security and trust framework for virtualized networks and software-defined networking," *Secur. Commun. Netw.*, vol. 9, no. 15, pp. 3059–3069, 2016.
- [22] A. J. Gonzalez, G. Nencioni, A. Kamisinski, B. E. Helvik, and P. E. Heegaard, "Dependability of the NFV Orchestrator: State of the Art and Research Challenges," *IEEE Commun. Surv. Tutor.*, vol. 20, no. 4, pp. 3307–3329, 2018.
- [23] L. De Simone, A. Lanzaro, D. Cotroneo, A. Iannillo, R. Natella, W. Ping, and J. Fan, "Network Function Virtualization: Challenges and Directions for Reliability Assurance," in *Proc. 2014 IEEE 25th International Symposium on Software Reliability Engineering Workshops*, pp. 370–375, 2014.
- [24] M. Zoure, T. Ahmed, and L. Réveillère, "Network Services Anomalies in NFV: Survey, Taxonomy, and Verification Methods," *IEEE Trans. Netw. Serv. Manag.*, vol. 19, no. 2, pp. 1567–1584, 2022.
- [25] N. T. Dung, N. V. Quan, and N. V. Hung, "Application of deep learning model in network reconnaissance attack detection," *Journal of Science and Technology on Information Security*, vol. 2, no. 16, pp. 60–72, Feb. 2023. DOI: 10.54654/isj.v1i16.922.
- [26] L. H. Hai, N. N. Hoa, P. V. On, T. M. Duc, and N. Q. Huy, "UET.SIR: An e-Government Information Security Incident Management Support Solution," *Journal of Science and Technology on Information Security*, vol. 2, no. 16, pp. 14–23, Feb. 2023. DOI: 10.54654/isj.v1i16.267.
- [27] R. Mijumbi, J. Serrat, J. L. Gorricho, N. Bouten, F. De Turck, and S. Latré, "Network function virtualization: State-of-the-art and research challenges," *IEEE Commun. Surv. Tutor.*, vol. 18, no. 1, pp. 236–262, 2016.
- [28] A. Hmaity, M. Savi, F. Musumeci, M. Tornatore, and A. Pattavina, "Virtual network function placement for resilient service chain provisioning," in *Proc. 2016 8th International Workshop on Resilient Networks Design and Modeling (RNDM)*, pp. 245–252, 2016.
- [29] S. G. Kulkarni, G. Liu, K. Ramakrishnan, M. Arumathurai, T. Wood, and X. Fu, "REINFORCE: Achieving Efficient Failure Resiliency for Network Function Virtualization-Based Services," *IEEE/ACM Trans. Netw.*, vol. 28, no. 2, pp. 695–708, 2020.
- [30] M. Ghaznavi, E. Jalalpour, B. Wong, R. Boutaba, and A. J. Mashtizadeh, "Fault tolerant service function chaining," in *Proc. Annual Conference of the ACM Special Interest Group on Data Communication on the Applications, Technologies, Architectures, and Protocols for Computer Communication*, pp. 198–210, 2020.
- [31] C. Basile, F. Valenza, A. Liroy, D. R. Lopez, and A. P. Perales, "Adding support for automatic enforcement of security policies in NFV networks," *IEEE/ACM Trans. Netw.*, vol. 27, no. 2, pp. 707–720, 2019.
- [32] ASEE, "What is Zero Trust Security? Zero trust architecture model explained" (2024), Access time: 22/05/2026, *Cybersecurity ASEE*.
- [33] G. A. Carella and T. Magedanz, "Open baton: A framework for virtual network function management and orchestration for emerging software-based 5G networks," *Newsletter 2015*, pp. 190, 2016.

- [34] G. Sun, Z. Xu, H. Yu, X. Chen, V. Chang, and A. V. Vasilakos, "Low-latency and resource-efficient service function chaining orchestration in network function virtualization," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 5760–5772, 2019.
- [35] H. Huang, C. Zeng, Y. Zhao, G. Min, Y. Y. Zhu, W. Miao, and J. Hu, "Scalable Service Function Chain Orchestration in NFV-enabled Networks: A Federated Reinforcement Learning Approach," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 8, pp. 2558–2571, 2021.
- [36] M. Hamdan, E. Hassan, A. Abdelaziz, A. Elhigazi, B. Mohammed, S. Khan, A. V. Vasilakos, and M. N. Marsono, "A comprehensive survey of load balancing techniques in software-defined network," *J. Netw. Comput. Appl.*, vol. 174, pp. 102856, 2021.
- [37] H. Hantouti, N. Benamar, and T. Taleb, "Service Function Chaining in 5G and Beyond Networks: Challenges and Open Research Issues," *IEEE Netw.*, vol. 34, no. 5, pp. 320–327, 2020.
- [38] H. B. Nguyen, N. T. Dinh, J. Oh, and Y. Kim, "An Openflow-based Scheme for Service Chaining's High Availability in Cloud Network," in *Proc. International Conference on ICT Convergence*, 2019.

ABOUT THE AUTHORS



Vu Ngoc Hoa

Workplace: Hanoi College of Industrial Economics, Vietnam

Email: hoavn@hiee.edu.vn

Education: PhD student, Graduate University of Science and Technology (GUST), Vietnam Academy of Science and Technology (VAST).

Recent research interests: computer networking, algorithm, programming, information systems.

Tên tác giả: **Vũ Ngọc Hòa**

Cơ quan công tác: Trường Cao đẳng Kinh tế Công nghiệp Hà Nội, Việt Nam.

Email: hoavn@hiee.edu.vn

Quá trình đào tạo: tốt nghiệp cử nhân tại Đại học Quốc gia Thành phố Hồ Chí Minh, thạc sĩ tại Trường Đại học Công nghệ thông tin và truyền thông - Đại học Thái Nguyên, hiện đang là nghiên cứu sinh tại Học viện Khoa học và Công nghệ - Viện Hàn lâm Khoa học và Công nghệ Việt Nam

Hướng nghiên cứu hiện nay: mạng máy tính, thuật toán, lập trình, hệ thống thông tin.



Nguyen Viet Phan

Workplace: Center for Information Technology and Network Security Monitoring, Vietnam Government Information Security Commission

Email: nvphan@bcy.gov.vn

Education: received engineering degree in 2008 and the Ph.D. degree

in 2011 from the Federal Protective Service Academy (FSO), Russian Federation.

Recent research direction: His research interests include Information security and privacy, cyberattacks.

Tên tác giả: **Nguyễn Việt Phan**

Cơ quan công tác: Trung tâm Công nghệ thông tin và Giám sát an ninh mạng, Ban Cơ yếu Chính phủ, Việt Nam

Email: nvphan@bcy.gov.vn

Quá trình đào tạo: Tốt nghiệp kỹ sư năm 2008, Tiến sĩ năm 2011 tại trường Học viện Cơ quan bảo vệ liên bang (FSO), Liên bang Nga.

Hướng nghiên cứu hiện nay: An toàn và bảo mật thông tin, phòng chống tấn công mạng.



Nguyen Tuan Hung

Workplace: University of Engineering and Technology, Vietnam National University

Email: 25025069@vnu.edu.vn

Education: Received bachelor degree in 2025 in University of Engineering and Technology

Recent research direction: His research interests include: information system, artificial intelligence, algorithm.

Tên tác giả: **Nguyễn Tuấn Hưng**

Cơ quan công tác: Trường đại học Công nghệ, Đại học Quốc gia Hà nội

Email: 25025069@vnu.edu.vn

Quá trình đào tạo: Tốt nghiệp cử nhân vào năm 2025 tại trường Đại học Công nghệ, Đại học Quốc gia Hà Nội

Hướng nghiên cứu hiện nay: hệ thống thông tin, trí tuệ nhân tạo, thuật toán.



Ngo Hai Anh

Workplace: Institute of Information Technology (IOIT), Vietnam Academy of Science and Technology (VAST), Vietnam

Email: ngohaianh@ioit.ac.vn

Education: PhD, Vietnam Academy of Science and Technology (VAST).

Recent research interests: computer, networking, telecommunication, cybersecurity, cloud computing, artificial intelligence.

Tên tác giả: **Ngô Hải Anh**

Cơ quan công tác: Viện Hàn lâm Khoa học và Công nghệ Việt Nam.

Email: ngohaianh@ioit.ac.vn

Quá trình đào tạo: tốt nghiệp cử nhân tại Đại học Kinh tế quốc dân, thạc sĩ tại Trường Đại học Công nghệ - Đại học Quốc gia Hà Nội, tiến sĩ tại Học viện Khoa học và Công nghệ - Viện Hàn lâm Khoa học và Công nghệ Việt Nam.

Hướng nghiên cứu hiện nay: mạng máy tính, mạng viễn thông, an ninh mạng, điện toán đám mây, trí tuệ nhân tạo.