

Adaptive Mitigation of Blackhole Attacks in Blockchain-Enhanced Software Defined Networks

Mehmed K. Uludag^{*}, Murat Karakus[†], Evrim Guler[‡], Suleyman Uludag[§]

^{*} Department of Computer Science and Engineering, University of Michigan - Ann Arbor, muludag@umich.edu

[†] Department of Software Engineering, Ankara University, Ankara, Türkiye, 06830, mrtkarakus@ankara.edu.tr

[‡] Department of Computer Engineering, Bartın University, Bartın, Türkiye, 74110, evrimguler@bartin.edu.tr

[§] Department of Computer Science, University of Michigan - Flint, MI, USA 48502, uludag@umich.edu

Abstract—Software-Defined Networking (SDN) and Blockchain (BC) are transformative technologies reshaping network management and security, utilizing their synergies. SDN’s centralized control enhances flexibility and efficiency but introduces vulnerabilities due to its single point of control. With its decentralized and immutable ledger, BC offers a solution by distributing control and providing a tamper-proof audit trail. This paper integrates these technologies to address blackhole attacks—a critical vulnerability where compromised SDN controllers disrupt network performance. We propose *Blockchain-Enhanced SDN for Adaptive Path Finding (BeS4APF)* algorithm against blackhole attacks in the multidomain SDNs. The algorithm maintains a high Packet Delivery Ratio (PDR) by dynamically adjusting network paths in response to node failures. The *BeS4APF* algorithm presented effectively maintains a high PDR by dynamically adjusting paths in response to node failures. The methodology involves monitoring the network, detecting compromised nodes, and recalculating optimal paths using Dijkstra’s algorithm and node-disjoint path selection. Experiments with synthetic networks of varying sizes (from 60 to 120 domains) demonstrate that the algorithm successfully handles domain-compromising node attacks, maintaining high PDR even with increasing stochastic disruptions. Our preliminary results show that, while PDR slightly deviates and recovers in smaller networks, it stabilizes towards almost 100% in larger networks after initial adjustments. This work advances the integration of SDN and BC, offering a robust approach to securing modern networks against evolving stochastic attack scenarios and threats.

Index Terms—Software Defined Networking, blockchain, adaptive mitigation, blackhole attacks, multipath routing, security

I. INTRODUCTION

Software Defined Networking (SDN) and Blockchain (BC) are two of the most disruptive technologies of the past few decades. As an innovative networking paradigm decoupling the control plane from the data plane, SDN enables centralized and programmable network management. By separating these two functions, SDN allows dynamic adjustment of network configurations and optimization of resource utilization through high-level programming abstractions. This architectural shift addresses the limitations of traditional network infrastructures, which are often rigid and complex to manage. SDN’s programmability facilitates rapid deployment of new services, enhances network flexibility, and improves overall efficiency, making it a pivotal technology in the evolution of modern network architectures [1], [2]. As a result, SDN is gaining

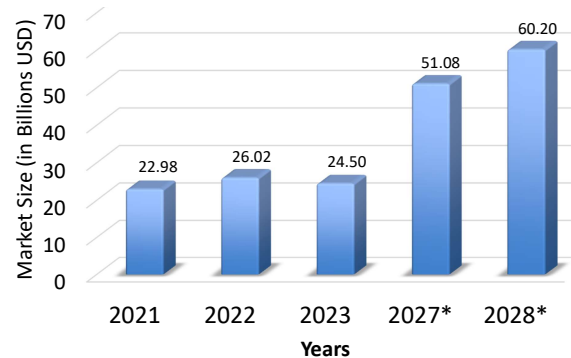


Fig. 1. SDN market size worldwide from 2021 to 2028 [3].

traction across various sectors, including data centers, telecommunications, and enterprise networks, driving significant advancements in network performance and operational agility.

BC, on the other hand, as conceptualized by Satoshi Nakamoto in 2008 for Bitcoin, has rapidly evolved into a transformative technology with applications extending far beyond cryptocurrencies. BC is a decentralized and distributed ledger that ensures secure, transparent, and immutable recording of transactions across a network of computers. The decentralized nature of BC eliminates the need for intermediaries, thereby reducing transaction costs and increasing efficiency. Moreover, its potential for smart contracts—self-executing contracts with the terms of the agreement directly written into code—opens new avenues for automation and trustless transactions in various sectors, including finance, supply chain management, healthcare, and governance.

The global SDN market has experienced significant growth over the past few years and is projected to continue expanding robustly as shown in Fig. 1. In 2023, the SDN market was valued at approximately USD 28.2 billion, and it is expected to reach USD 120.5 billion by 2032, growing at a Compound Annual Growth Rate (CAGR) of about 17%. This growth is driven by several factors, including the increased adoption of SDN in various industries, the need for simplified network management, and the integration of advanced technologies such as artificial intelligence and cloud computing [4].

The global BC technology market is also projected to continue a similar growth over the next decade, as shown in

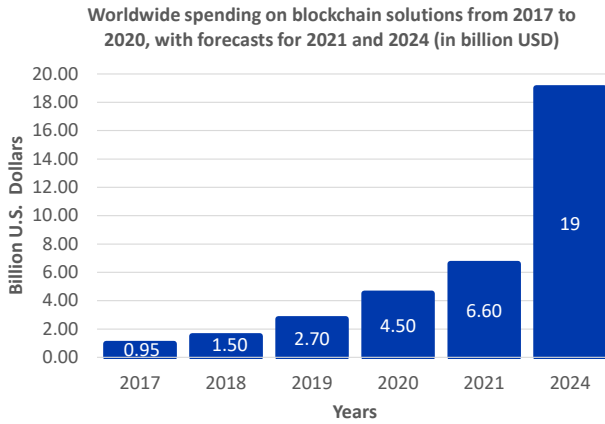


Fig. 2. Global BC solutions spending 2017-2020, with 2021 and 2024 forecasts [5].

Fig. 2. In 2023, the market was valued at approximately USD 17.46 billion, and 19 billion in 2024 to USD 248.9 billion by 2029 at a CAGR of 65.5% [6]. The increasing demand for secure, transparent transactions across various industries drives this growth, including finance, healthcare, supply chain management, and more.

Integrating BC with SDN presents a compelling advancement in network management and security. SDN’s separation of the control plane from the data plane allows for centralized control and programmability, significantly enhancing network flexibility and efficiency [1]. However, this centralization introduces potential vulnerabilities, as a single point of control can become a target for attacks. With its decentralized and immutable ledger, BC technology offers robust solutions to these security concerns. By integrating BC with SDN, the network’s control plane can be decentralized, distributing control among multiple nodes and thereby reducing the risk of a single point of failure [7]. This integration can enhance the trustworthiness of network configurations and operations, ensuring that changes are verified and recorded on a tamper-proof ledger, which mitigates the risk of unauthorized access or alterations [8]. Moreover, BC can facilitate secure and transparent resource management in SDN environments. The immutable nature of BC ensures that all transactions and configurations are recorded permanently, providing an audit trail that can be crucial for troubleshooting and compliance [9]. Smart contracts, another feature of BC, can automate and enforce network policies dynamically, leading to more responsive and adaptive network management [10].

In our previous work, we have exploited the synergies mentioned above in different contexts to develop this integrated framework [11]–[17], under the assumption of a fully secure operating paradigm with no compromises in the system. In this work, we release the attack-free operating environment and start our endeavor to study various aspects of our system under different vulnerability models. This study is the first to delve into vulnerabilities and attacks on the BC-enhanced SDN framework. We start with a simple threat model, *blackhole*

attack [18]–[24], where one or more SDN controllers are assumed to be compromised and develop corresponding problem formulations. We delineate many potential countermeasure approaches and focus on one in this study due to the page limit. We plan to continue our initial work with different countermeasures and add other threat models.

The rest of the paper is organized as follows: Section II provides the related work. Section III presents a synopsis of the underlying technologies. Section IV explains the threat model, develops the problem formulation, and discusses the high-level countermeasures. Section V explains the details of the methodology to mitigate blackhole attacks through adaptive algorithms in terms of the packet delivery ratio. Experiments and results are provided in Sections VI and VII, respectively. Concluding remarks are in Section VIII.

II. RELATED WORK

A. Blackhole Attacks on SDN Systems

The architecture of SDN presents novel security dynamics, which might be advantageous or perilous. The authors in [25] present an extensive examination of several vulnerabilities in SDN, such as blackhole attacks. They also describe the corresponding methods for detecting and mitigating these attacks. In [26], the authors analyze the security risks and possible solutions to mitigate them in SDN. The study conducts a comparative analysis of the security aspects of SDN and traditional networks. It highlights the novel security capabilities and dangers that arise as a result of implementing SDN. The authors in [27] concentrate on SDN-enabled Vehicular Ad Hoc Networks (VANETs), presenting techniques to identify and eliminate malicious blackhole attackers. The study emphasizes the incorporation of SDN into automotive networks to promote road safety and optimize communication efficiency. In [28], the authors suggest a “blackhole mechanism” to decrease the amount of switch-controller traffic overhead in SDN. The authors analyze the conventional beliefs regarding packet flow to the controller, which can result in substantial additional costs. They provide a method to address and reduce these costs. The study quantifies the burden on the controller resulting from various forms of traffic. It demonstrates how the blackhole mechanism can substantially decrease this load, hence improving the overall effectiveness of SDN operations.

B. Exploring the Relationship Between BC and Blackhole Attacks

Utilizing BC technology to bolster network security against blackhole attacks is increasingly gaining momentum. The authors in [29] examine the risks associated with SDN-enabled Wireless Sensor Networks (WSN) and provide a detailed analysis of blackhole attacks. The authors suggest implementing a security model that is not resource-intensive, utilizing a blockchain-block method to safeguard flow tables in every node. This technique effectively prevents unauthorized modifications and guarantees the secure transmission of data. This technique generates an immutable fingerprint for flow entries,

also known as a signature token. The researchers in [30] propose Blackhole/Greyhole Routing Protocol for Low Power and Lossy Networks (GBG-RPL). This method combines the Gini index and BC technology to identify and address blackhole and greyhole attacks in smart health monitoring Cyber-Physical Systems (CPSs). The study utilizes the Gini index’s analytical capabilities and BC technology’s security attributes to safeguard CPSs from advanced threats. The suggested method demonstrates significant enhancements in packet loss ratio, residual energy use, attack-detection rate, and overall network management efficiency, establishing it as a resilient option for safeguarding CPSs. In [31], the authors present a paradigm for smart contracts based on BC technology to improve trustworthiness and security in vehicle networks. The study employs Self-Classification Blockchain-Based Contracts (SCBC) and Voting-Classification Blockchain-Based Contracts (VCBC) to identify and reduce the occurrence of blackhole and greyhole assaults. The results indicate that VCBC outperforms in terms of packet delivery ratio and throughput, even in the presence of attacks, confirming its efficacy in increasing network security. The researchers in [32] propose a hybrid framework that integrates BC and the Internet of Things (IoT) devices to enhance the security of data transmission in IoT networks. The architecture specifically targets DoS attacks, including black hole attacks. The HFSDT-IoT framework employs a two-step methodology: the initial step involves the detection of malevolent devices through the utilization of the Ethereum Proof of Stake (PoS) protocol and Intrusion Detection Systems (IDSs), while the subsequent step enables the exchange of information between BCs through encryption.

C. Blackhole Attacks on Multi-Domain Systems

The vulnerabilities inherent in the Border Gateway Protocol (BGP), despite the implementation of measures such as BGPsec, continue to be a major cause for worry. The authors in [18] examine these vulnerabilities and show that, despite enhancements in security, there are still inherent exploitable weaknesses, leading to the possibility of black hole attacks. In [33], the researchers measure the efficacy of several BGP security protocols in reducing traffic-attraction attacks. The evaluated protocols include origin authentication, soBGP, S-BGP, and data-plane verification. The assessment reveals that even if these protocols have improved security protections, attackers can still find ways to bypass them. To mitigate black hole attacks in multi-domain network systems, it is necessary to implement comprehensive techniques encompassing many technologies. The authors in [34] suggest a method to protect VANETs from blackhole attacks by identifying and eliminating rogue nodes in the network. The extensive body of research on blackhole attacks across various network paradigms underscores the persistent and evolving threat they pose. From traditional BGP vulnerabilities to the nuanced challenges in SDN and the innovative defenses offered by BC technology, each study contributes valuable insights into mitigating these attacks. However, existing literature often addresses these threats in isolation, focusing on specific tech-

nologies without integrating solutions across different network environments. We aim to bridge this gap by developing a comprehensive framework to address blackhole attacks in a unified manner, encompassing SDN, BC, and multi-domain network systems. Our goal in this preliminary study is to unearth the potential security issues in BC-enhanced SDNs to draw research community’s attention, highlight simple, but potentially fatal, threat vectors, open up a discussion for some potential countermeasures, and develop and evaluate one simple adaptive mitigation strategy in terms of the packet delivery ratio.

III. OVERVIEW OF SDN AND BLOCKCHAIN

SDN and BC are distinct technologies employed across various industries and applications, each presenting unique advantages and limitations. This section provides a concise examination of SDN and BC.

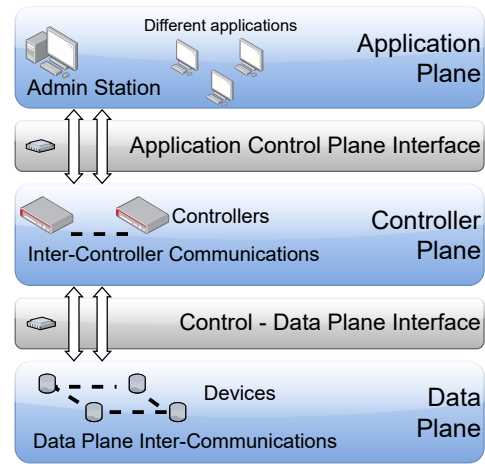


Fig. 3. Main layers and interfaces in SDN architectures.

A. Overview of SDN

SDN represents a network framework that facilitates centralized and intelligent network control and management through the use of software. SDN typically comprises three layers: the controller layer, the data layer, and the application layer. In this architecture, software applications are employed to program and regulate the behavior of the entire network and its devices. These applications interact with the data layer to accomplish this task. As illustrated in Fig. 3, the SDN architecture offers a structured framework that enhances the flexibility and widespread adoption of SDN in the management of network devices. SDN enables operators to decouple the control and management of individual networking devices from the underlying network technology.

The data layer encompasses the physical infrastructure, such as switches, routers, and access points. When an SDN controller operates at this level, it leverages interfaces like OpenFlow to facilitate communication [35]. The controller layer houses the SDN controllers, which interact with both the data and application layers through designated interfaces.

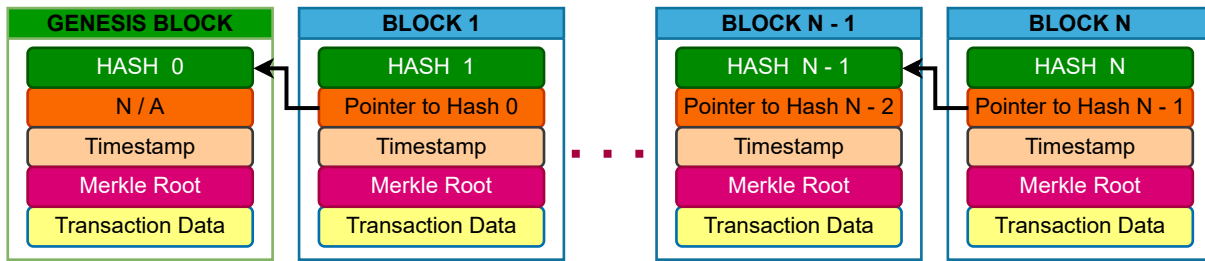


Fig. 4. High-level representation of block and blockchain data structures.

These controllers orchestrate network operations based on predefined protocols. The application layer hosts various programs responsible for managing network functions. Multiple applications can coexist within this layer, interacting with the SDN controller to execute their respective tasks [36].

B. Overview of Blockchain

BC technology represents a distributed ledger or database that is shared among multiple participants within a network. While it is most commonly associated with cryptocurrencies, its applications extend to various fields such as banking, voting, supply chain management, and networking [13]. Data recorded on a BC is immutable, verifiable, and securely documented, ensuring privacy and widespread distribution as transactions are stored in a shared ledger accessible to all network members.

The process starts with collecting and recording transaction data into a block, beginning with the Genesis block. Through cryptographic techniques, a hash is generated and added to the header of the next block, creating a chain of interconnected blocks. All participating nodes in the network can view and verify these transactions. BC achieves consensus among all participants using consensus algorithms, which allow network peers to validate transactions according to predetermined rules. BCs can be classified into private networks, requiring permission from an authoritative entity for access, or public networks, where any node can join and participate in mining without prior approval. Typically, as illustrated in Fig. 4, a BC includes a reference to the previous block, a hash, a sequential number, a timestamp, and transaction data.

IV. THREAT MODEL AND PROBLEM FORMULATION

As mentioned earlier, we consider threat scenarios for the BC-enhanced SDN systems. This section first introduces potential vulnerabilities, followed by developing threat models and potential countermeasures, focusing on one in this study; the rest is left for future work.

A. Threat Model

The traditional Internet routing subsystems have many vulnerabilities that have been well studied for a long time [33], [37]. The threat models and attack vectors from these studies include attacks of blackhole [18]–[20], wormhole [18], [19], mole [18], [19], attraction [33], [37], interception [18], [24],

[33], [37], [38], man-in-the-middle (MITM) [24], data falsification [39], protocol manipulation and tampering [18], [20], [39], data misuse [39], fake routing [18], and traffic hijacking [18] to name the most prominent ones. In many of these, as simple as a simple compromised node or manipulator [20], [37] has been the starting point for studying the implications and developing mitigation approaches.

As for the SDN, there have been many studies about vulnerabilities and attacks. The attacks and vulnerabilities studied for SDN include authentication issues [40], malicious code injection [21], [40], vulnerable controllers [22], forged control packet injection [21]–[23], [40]–[43], abuse of privileges [22], poisoned network view [22], MITM [22], [23], controller hijacking [44], spoofing [45], tampering flow table rules [21], [23], [41], [42], [45], [46], privilege escalation [45], blackhole [21], DDoS [23], buffer overflow [23], topology forgery [23], [47], [48], link fabrication [47], [48], cluster splitting attack [47], cluster amnesia attack [47], and control channel hijacking [46].

In this study, as a result of one or more of the aforementioned attacks and/or vulnerabilities, one or more nodes is/are compromised, and an attacker may use this node to launch a blackhole attack. While the attacker may prevent any number of packets passing through it, for the sake of simplicity and as a starting point, in this study, we will assume that *all* packets are dropped. In our future work, we will address stealthier and fractional packet-dropping scenarios. We aim to maintain the packet delivery ratio (PDR) between a source-destination pair by finding alternate paths when PDR goes below some predefined stepwise threshold values. A detailed description of our approach is given in Section V together with our algorithm.

B. Problem Formulation and Adaptive Mitigation

Here is our high-level, informal problem definition:

Definition 1: Given a set of BC-enhanced SDNs, administered by mutually distrustful entities, find alternate path(s) when one or more nodes is/are compromised, as manifested through a reduction in packet delivery ratio that can be escalated to multipath transmission after the depletion of alternate paths.

Potential countermeasures may be given as follows: (1) Detect and isolate the node, (2) Simple alternate path (3) Node-disjoint alternative path (4) Pathlet-disjoint path selection, (5) Domain-disjoint alternate path. Since we are under

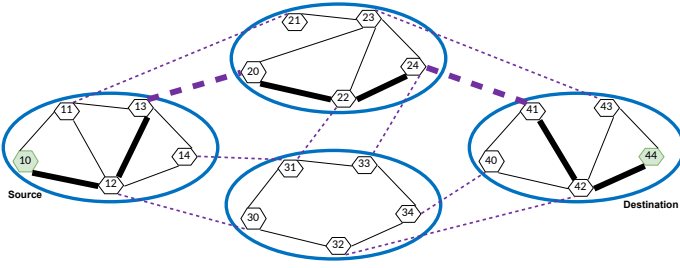


Fig. 5. Threat Model Sample network scenario. Original Path.

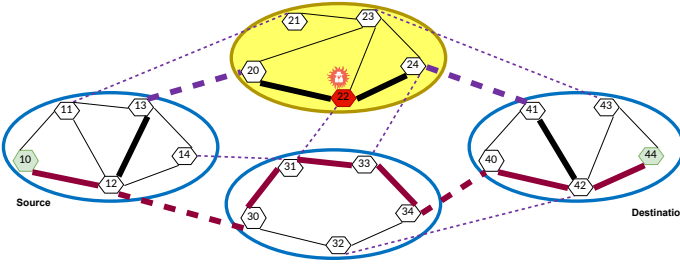


Fig. 6. Threat Model sample network with a domain-disjoint path.

the mutually distrustful model among the SDNs, the first option may not be possible. A simple alternate path is a possibility if networks cooperate with each other. The node-disjoint path will also require close coordination and disclosure of confidential topology information. In our earlier studies, we have relied on a novel concept of *pathlets*, see [17] for details. A pathlet-disjoint path would be the ideal situation, but we defer this option to future work due to the complexity. Due to the page limit, we are left with the last option, in this study, of finding a domain-disjoint alternate path to ensure a quick recovery from the reduced PDR, of course, at the expense of completely removing some potentially good paths from consideration. Again, our goal is to intervene to maintain high PDR by sacrificing some good links, which is the tradeoff.

We will illustrate our potential countermeasure as follows, skipping the others for brevity: Fig. 5 shows a simplified BC-enhanced SDN network with four domains, node 10 as the source and 44 as the destination, with the path 10 – 12 – 13 – 20 – 22 – 24 – 41 – 42 – 44. Let us assume that node 22 is compromised. Soon, we will notice a PDR decline for the above connection and try to find an alternate path. Fig. 5 We aim to find a domain-disjoint path to bring the PDR back up to as close to the initial levels as possible within the shortest time. Please note that the domain-disjoint path cannot skip the source and the destination domains for obvious reasons. Fig. 6 shows a possible alternate under the domain-disjoint path approach where the new path is 10 – 12 – 30 – 31 – 33 – 34 – 40 – 42 – 44.

V. BLOCKCHAIN-ASSISTED SECURE PATHFINDING FOR BLACKHOLE ATTACKS IN MULTIDOMAIN SDNS

This section details our adaptive mitigation algorithm, called Blockchain-Enhanced SDN for Adaptive Path Find-

ing (*BeS4APF*) against blackhole attacks in the multidomain SDNs, to efficiently transmit data packets using fewer resources than conventional methods by utilizing rerouting techniques to enhance network resilience against system attacks. Our method aims to dynamically adjust paths in response to node failures, maintaining a high packet delivery ratio (PDR). Our assumptions are:

Network Visibility: The algorithm has access to the entire network topology,

Compromise Detection: The system can detect which nodes have been compromised,

Performance Metrics: The algorithm can monitor network performance metrics such as PDR,

Real-time Adaptation: The system can adapt paths in real-time.

Our algorithm, *BeS4APF*, as shown in Algorithm 1, is designed to monitor the network, detect node failures, and adapt paths to mitigate performance drops. It leverages a combination of shortest path finding and node-disjoint path selection to ensure network robustness. The algorithm uses Dijkstra’s algorithm to find the shortest path and continuously monitors for performance drops, dynamically recalculating the optimal path between the source and destination nodes.

Algorithm 1 Blockchain-Assisted Path-finding for Blackhole Attacks in Multidomain SDNs

```

1: procedure BES4APF(Network, Src, Dst, BC)
2:   currentPaths  $\leftarrow$  PriorityQueue(BC)
3:   initialPath  $\leftarrow$  FINDBESTPATH(Network, Src, Dst)
4:   Update currentPaths with initialPath
5:   pdr  $\leftarrow$  CALCULATEPDR(Network, initialPath)
6:   while Network is operational do
7:     if Node failure detected then
8:       DEACTIVATENODE(Network, FailedNode)
9:       pdr_current  $\leftarrow$  CALCULATEPDR(Network, currentPaths)
10:      pdr_drop  $\leftarrow$  pdr – pdr_current
11:      if pdr_drop = 0 then
12:        Continue with current path
13:      else if pdr_drop < 2.0 then
14:        newPath  $\leftarrow$  FINDBESTPATH(Network, Src,
15:          Dst)
16:        UPDATEPATHS(currentPaths, newPath)
17:      else if pdr_drop  $\geq$  2.0 then
18:        newPath  $\leftarrow$  FINDNODEDISJOINT-
19:          PATH(Network, Src, Dst, currentPaths)
20:        if newPath is found then
21:          UPDATEPATHS(currentPaths, newPath)
22:        else
23:          newPath  $\leftarrow$  ADDNEWPATH(Network, Src,
          Dst)
          currentPaths.push(-pdr1, newPath)
24:        pdr  $\leftarrow$  CALCULATEPDR(Network, currentPaths)

```

The *BeS4APF* algorithm dynamically adjusts secure paths in multi-domain networks to maintain a high end-to-end PDR despite node failures as follows:

Initialize: Create a priority queue for current paths that uses a given performance metric to prioritize the best paths by considering the pathlet transactions in BC. Find the initial shortest path between the source and destination, and calculate the initial PDR by calling `FINDBESTPATH()` and `CALCULATEPDR()` methods, respectively.

Monitor and Detect Failures: Continuously monitor network status and search for node failures as indicated by drops in performance.

Failure Handling: (a) *No PDR Drop:* If PDR remains unchanged, continue with the current path, (b) *Small PDR Drop:* If the PDR drops by less than 2%, find a new shortest path that avoids the failed node, and replace the least priority path in the current paths, (c) *Significant PDR Drop:* If PDR drops by 2% or more, find a completely node-disjoint path by calling `FINDNODEDISJOINTPATH()` method. If no such path is available, then add the last best path back to the priority queue.

Update PDR: Recalculate the PDR with the updated paths and continue monitoring until the network is no longer operational.

VI. EXPERIMENTS

In this section, we present our simulations to evaluate the performance of our *BeS4APF* algorithm. The experiments aim to validate the effectiveness of the proposed algorithm in maintaining a high PDR under varying network conditions.

A. Graph Generation

This subsection describes the methodology used for generating the network topologies employed in our study. The graphs were created using the Erdős–Rényi model, which is well-suited for random graph generation and widely used in network research due to its simplicity and versatility.

Inter-Network Topologies. We have generated three inter-network topologies consisting of 60, 90, and 120 nodes, respectively. For each of these inter-networks, we ensured a connectivity probability of 0.7. This connectivity probability indicates that there is a 70% chance that any given pair of nodes will have a direct link between them, ensuring a robust and interconnected network structure.

Intra-Domain Topologies. Within each inter-network topology, we further created six different intra-domain topologies. These intra-domain topologies were generated for 5, 6, 7, 8, 9, and 10 nodes. Similar to the inter-networks, the intra-domain topologies were generated with a connectivity probability of 0.7, maintaining a high level of connectivity within each domain.

Link Characteristics. To simulate realistic network conditions, we assigned random values to the various link parameters within both the primary and intra-domain topologies:

Bandwidth: Each intra-domain link was assigned a random bandwidth availability within the range of 5 to 55 units. Links that interconnect different domains were assigned a significantly higher random bandwidth availability, ranging from 500 to 1000 units. This reflects the typically higher capacity of backbone links in multi-domain network environments.

Delay: Each intra-domain link was assigned a random delay within the range of 1 to 5 ms. This range represents typical delay values for intra-domain environments.

Reliability: Each intra-domain link was assigned a random reliability value between 0.99 and 0.999. This high-reliability range is representative of well-maintained and stable network links within a domain.

By using the Erdős–Rényi random graph generator and setting these parameters, we aimed to create network topologies that are both complex and realistic, providing a robust foundation for evaluating the performance and resilience of our proposed framework against black hole attacks in SDN, BC, and multi-domain environments.

B. Simulation Setup

The simulation setup is designed to test the efficacy of the adaptive pathfinding algorithm under various network conditions and attack scenarios. This section outlines the distinct components of the simulation:

PDR Calculation and Algorithm Separation: PDR calculation and the adaptive pathfinding algorithm are constructed as separate systems. The PDR calculation system is responsible for evaluating network performance and determining the impact of node failures on packet delivery. The adaptive algorithm focuses on adjusting paths to mitigate performance degradation. This separation allows for independent testing and optimization of each component.

Attack Simulation: The attack simulation is conducted over a predefined time period. At each time step, a number of nodes, denoted as k , are randomly selected and attacked. The steps involved in the simulation are:

- 1) **Node Attack:** At each time step, k nodes are chosen at random from the network and are corrupted such that any path using those nodes is affected.
- 2) **PDR Drop Calculation:** After the nodes are attacked, the PDR is recalculated to determine the performance impact of the node failures.
- 3) **Algorithm Decision:** The adaptive algorithm uses the computed PDR drop to make decisions on how to proceed. It assesses whether the drop in PDR is minimal or significant and selects an appropriate strategy to maximize the PDR for subsequent iterations.

The algorithm then recalculates the best path(s) and updates the network paths to optimize performance based on the current network conditions. This process is repeated at each time step to continuously adapt to the evolving network state.

VII. RESULTS

Our experiments demonstrate the *BeS4APF*'s effectiveness in maintaining a high PDR despite disruptions from stochastic domain attacks. The algorithm adeptly identifies and utilizes alternative and node-disjoint paths, preserving network performance under various attack scenarios.

A. Algorithm Performance

The algorithm was tested across different network configurations and attack scenarios. It successfully identified alternative paths during domain failures and utilized node-disjoint paths to ensure robust network performance. When faced with significant performance drops, the algorithm effectively managed multiple paths to uphold a high PDR.

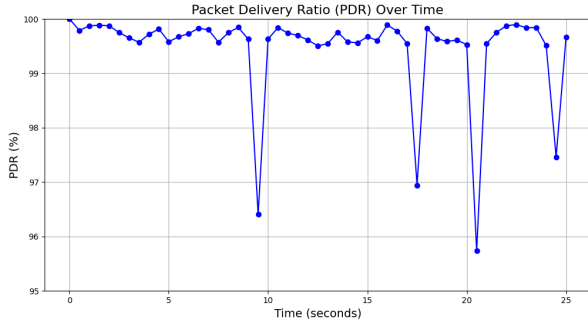


Fig. 7. PDR Over Time for 60-Domain

B. Figures and Analysis

a) *60-Domain Configuration*: Fig. 7 illustrates the *PDR Over Time for the 60-Domain* configuration. The graph shows slight deviations in PDR as attacks progress, with PDR falling slightly, recovering, and maintaining this pattern throughout. Fig. 8 depicts the *PDR vs. Number of Domains Attacked*, revealing that as more domains are attacked, the PDR decreases and recovery time extends as the number of attacked domains approaches the total number of domains in the network.

b) *120-Domain Configuration*: Fig. 9 shows the *PDR for the 120-Domain* configuration. The algorithm performs well, with PDR stabilizing at 100% after approximately 30 seconds, demonstrating its ability to handle multiple paths and compensate for a high number of attacked domains. Fig. 10 illustrates the *PDR vs. Number of Domains Attacked*, showing that as more domains are attacked, the algorithm's performance remains robust, although recovery time increases as the number of attacked domains approaches the total number.

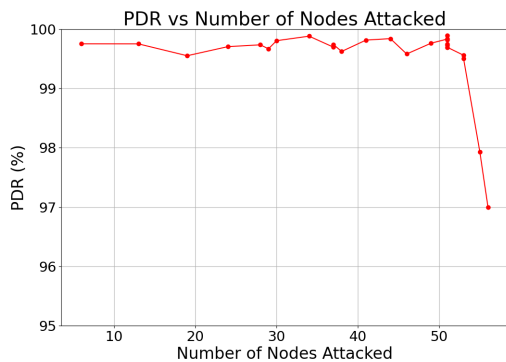


Fig. 8. PDR vs. Number of Domains Attacked for 60-Domain

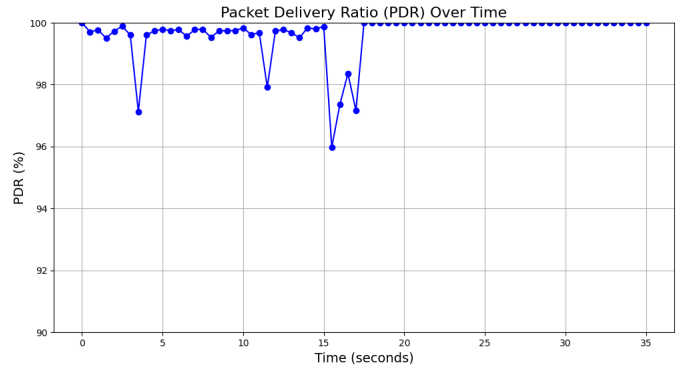


Fig. 9. PDR Over Time for 120-Domain

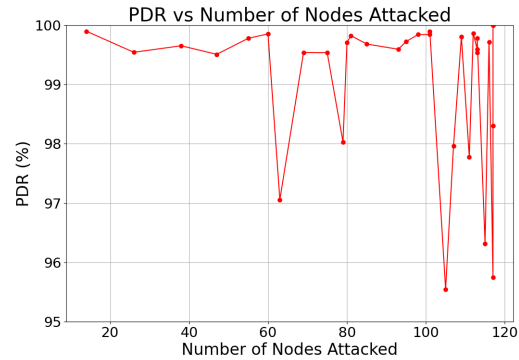


Fig. 10. PDR vs. Number of Domains Attacked for 120-Domain

C. Summary

Overall, the results validate the *BeS4APF* algorithm's ability to maintain network robustness and performance. Its capacity to switch to alternative and node-disjoint paths and to manage multiple paths effectively is crucial for sustaining a high PDR under varying attack conditions.

VIII. CONCLUSION

This study has presented our Blockchain-Enhanced SDN for Adaptive Path Finding (*BeS4APF*) algorithm against blackhole attacks in the multidomain SDNs, designed to maintain a high PDR despite node attacks and failures. The algorithm effectively identifies and utilizes alternative and node-disjoint paths, ensuring robust network performance under various attack scenarios. The results demonstrate the algorithm's capability to sustain high PDR by dynamically adjusting paths and deferring to multiple paths when necessary.

Future research can expand upon this work by incorporating additional performance metrics to provide a more comprehensive evaluation of network robustness. An interesting direction would be to adapt the algorithm to handle nodes that recover from attacks, allowing for the reuse of previously used paths. Enhancing the algorithm to consider and reintegrate older paths as they become available could further improve network efficiency and resilience. Additionally, exploring more complex scenarios and performance criteria could offer deeper

insights into the algorithm's capabilities and limitations in diverse network environments.

REFERENCES

- [1] D. Kreutz, F. M. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolkly, and S. Uhlig, "Software-defined networking: A comprehensive survey," *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14–76, 2014.
- [2] B. A. A. Nunes, M. A. S. Santos, B. T. de Oliveira, C. B. Margi, K. Obraczka, and T. Turetli, "Software-defined-networking-enabled capacity sharing in user-centric networks," *Communications Magazine, IEEE*, vol. 52, no. 9, pp. 28–36, September 2014.
- [3] L. S. Vaishery, "Software-defined networking (SDN) market size worldwide from 2021 to 2028," Mar 2024, Statista.
- [4] "Software Defined Networking Market," February 2024, global Markets Insights, Report ID: GMI2395.
- [5] "Worldwide spending on blockchain solutions from 2017 to 2020, with forecasts for 2021 and 2024 (in billion U.S. dollars)," April 2021, Statista.
- [6] "Blockchain Market - Global Forecast to 2029," July 2024, Markets and Markets, Report ID: TC 4638.
- [7] Q. Zhang, L. Yang, and X. Chen, "A survey on blockchain technology and its potential applications for securing iot networks," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 491–535, 2018.
- [8] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 858–880, 2018.
- [9] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain for iot security and privacy: The case study of a smart home," *PerCom Workshops*, pp. 618–623, 2017.
- [10] N. Fotiou, G. Marias, and G. C. Polyzos, "Smart contracts for the internet of things: Opportunities and challenges," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 2243–2255, 2021.
- [11] A. B. Gorgulu, H. O. Kamali, M. Karakus, E. Guler, and S. Uludag, "A proof of concept for Blockchain-Enhanced smart parking system with SDN: BePaS," in *IEEE BlackSeaCom 2024*, Tbilisi, Georgia, Jun. 2024.
- [12] M. Karakus, E. Guler, and S. Uludag, "SmartContractChain (SC²): Cross-ISP QoS traffic management framework with SDN and blockchain," *Peer-to-Peer Netw. & Applications*, pp. 1–18, Oct 2023.
- [13] S. W. Turner, M. Karakus, E. Guler, and S. Uludag, "A promising integration of sdn and blockchain for iot networks: A survey," *IEEE Access*, vol. 11, pp. 29 800–29 822, 2023.
- [14] E. Guler, M. Karakus, and S. Uludag, "Blockchain-enhanced cross-isp spectrum assignment framework in sdn: Spectrumchain," *Computer Networks*, p. 109579, 2023.
- [15] E. Guler, M. Karakus, and S. Uludag, "Evaluating path selection strategies with blockchain-based routing in Multi-Domain SDNs," in *(BalkanCom'22)*, Sarajevo, Bosnia and Herzegovina, Aug 2022.
- [16] E. Guler, M. Karakus, and S. Uludag, "SpectrumChain: An Efficient Spectrum Management Framework in Blockchain-Enabled Flexible SDNs," in *IEEE ICC*, May 2022.
- [17] M. Karakus, E. Guler, and S. Uludag, "QoSChain: Provisioning Inter-AS QoS in Software-Defined Networks with Blockchain," *IEEE Trans. on Netw. & Service Mngmnt*, vol. 18, no. 2, pp. 1706–1717, Jun 2021.
- [18] Q. Li, J. Liu, Y.-C. Hu, M. Xu, and J. Wu, "Bgp with bgpsec: Attacks and countermeasures," *IEEE Network*, vol. 33, no. 4, pp. 194–200, 2018.
- [19] Q. Li, Y.-C. Hu, and X. Zhang, "Even rockets cannot make pigs fly sustainably: Can bgp be secured with bgpsec," in *Workshop SENT'14, 23 February 2014, San Diego, USA, Copyright 2014 Internet Society: Proceedings*. Internet Society, 2014.
- [20] Y. Song, A. Venkataramani, and L. Gao, "Identifying and addressing reachability and policy attacks in "secure" bgp," *IEEE/ACM Transactions on Networking*, vol. 24, no. 5, pp. 2969–2982, 2016.
- [21] Y. Maleh, Y. Qasmaoui, K. El Gholami, Y. Sadqi, and S. Mounir, "A comprehensive survey on sdn security: threats, mitigations, and future directions," *Jrnal of Reliable Intell. Env.*, vol. 9, no. 2, pp. 201–239, 2023.
- [22] J. C. C. Chica, J. C. Imbachi, and J. F. B. Vega, "Security in SDN: A comprehensive survey," *Journal of Network and Computer Applications*, vol. 159, p. 102595, 2020.
- [23] Z. A. Bhuiyan, S. Islam, M. M. Islam, A. A. Ullah, F. Naz, and M. S. Rahman, "On the (in) security of the control plane of sdn architecture: A survey," *IEEE Access*, 2023.
- [24] A. Pilosov and T. Kapela, "Stealing the internet: An internet-scale man in the middle attack," *NANOG-44*, pp. 12–15, 2008.
- [25] S. Singh and S. Jayakumar, "A study on various attacks and detection methodologies in software defined networks," *Wireless Personal Communications*, vol. 114, no. 1, pp. 675–697, 2020.
- [26] Z. Shu, J. Wan, D. Li, J. Lin, A. V. Vasilakos, and M. Imran, "Security in software-defined networking: Threats and countermeasures," *Mobile Networks and Applications*, vol. 21, pp. 764–776, 2016.
- [27] M. Erritali, B. Cherkaoui, H. Ezzikouri, and A. Beni-hssane, "Detection of the black hole attack on sdn-based vanet network," in *Proceedings of ICDSIS 2020*. Springer, 2022, pp. 67–74.
- [28] A. Favaro and E. P. Ribeiro, "Reducing sdn/openflow control plane overhead with blackhole mechanism," in *2015 Global Information Infrastructure and Networking Symposium (GIIS)*, 2015, pp. 1–4.
- [29] E. Karakoç and C. Çeken, "Black hole attack prevention scheme using a blockchain-block approach in sdn-enabled wsn," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 37, no. 1, pp. 37–49, 2021.
- [30] M. Javed, N. Tariq, M. Ashraf, F. A. Khan, M. Asim, and M. Imran, "Securing smart healthcare cyber-physical systems against blackhole and greyhole attacks using a blockchain-enabled gini index framework," *Sensors*, vol. 23, no. 23, p. 9372, 2023.
- [31] A. Alabdulatif, M. Alharbi, A. Mchergui, and T. Moulahi, "Mitigating blackhole and greyhole routing attacks in vehicular ad hoc networks using blockchain based smart contracts," *CMES-Computer Modeling in Engineering & Sciences*, vol. 138, no. 2, 2024.
- [32] M. H. Salih Mohammed, "A hybrid framework for securing data transmission in internet of things (iots) environment using blockchain approach," in *(IEMTRONICS)*, 2021, pp. 1–10.
- [33] S. Goldberg, M. Schapira, P. Hummon, and J. Rexford, "How secure are secure interdomain routing protocols?" *Computer Networks*, vol. 70, pp. 260–287, 2014.
- [34] J. Tobin, C. Thorpe, and L. Murphy, "An approach to mitigate black hole attacks on vehicular wireless networks," in *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*, 2017, pp. 1–7.
- [35] M. Karakus and A. Durrezi, "Quality of Service (QoS) in Software Defined Networking (SDN): A Survey," *Journal of Network and Computer Applications*, vol. 80, pp. 200 – 218, 2017.
- [36] M. Karakus and A. Durrezi, "A Survey: Control Plane Scalability Issues and Approaches in Software-Defined Networking (SDN)," *Computer Networks*, vol. 112, pp. 279 – 293, 2017.
- [37] S. Goldberg, M. Schapira, P. Hummon, and J. Rexford, "How secure are secure interdomain routing protocols," *ACM SIGCOMM Computer Communication Review*, vol. 40, no. 4, pp. 87–98, 2010.
- [38] R. Hiran, N. Carlsson, and P. Gill, "Characterizing large-scale routing anomalies: A case study of the china telecom incident," in *Passive and Active Measurement: 14th Int'l Conf.* Springer, 2013, pp. 229–238.
- [39] A. Mitseva, A. Panchenko, and T. Engel, "The state of affairs in bgp security: A survey of attacks and defenses," *Computer Communications*, vol. 124, pp. 45–60, 2018.
- [40] R. Deb and S. Roy, "A comprehensive survey of vulnerability and information security in sdn," *Comp. Netw.*, vol. 206, p. 108802, 2022.
- [41] A. N. Alhaj and N. Dutta, "Analysis of security attacks in sdn network: A comprehensive survey," *Contemporary Issues in Communication, Cloud and Big Data Analytics: Proceedings of CCB 2020*, pp. 27–37, 2022.
- [42] S. Scott-Hayward, S. Natarajan, and S. Sezer, "A survey of security in software defined networks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 623–654, 2015.
- [43] T. Han, S. R. U. Jan, Z. Tan, M. Usman, M. A. Jan, R. Khan, and Y. Xu, "A comprehensive survey of security threats and their mitigation techniques for next-generation sdn controllers," *Concurrency and Computation: Practice and Experience*, vol. 32, no. 16, 2020.
- [44] A. Pradhan and R. Mathew, "Solutions to vulnerabilities and threats in software defined networking (sdn)," *Procedia Computer Science*, vol. 171, pp. 2581–2589, 2020.
- [45] M. B. Jimenez, D. Fernandez, J. E. Rivadeneira, L. Bellido, and A. Cardenas, "A survey of the main security issues and solutions for the sdn architecture," *IEEE Access*, vol. 9, pp. 122 016–122 038, 2021.
- [46] M. S. Farooq, S. Riaz, and A. Alvi, "Security and privacy issues in software-defined networking (sdn): A systematic literature review," *Electronics*, vol. 12, no. 14, p. 3077, 2023.
- [47] S. Deng, W. Dai, X. Qing, and X. Gao, "Vulnerabilities in sdn topology discovery mechanism: Novel attacks and countermeasures," *IEEE Transactions on Dependable and Secure Computing*, 2023.
- [48] S. Soltani, A. Amanlou, M. Shojafar, and R. Tafazolli, "Security of topology discovery service in sdn: Vulnerabilities and countermeasures," *IEEE Open Journal of the Communications Society*, 2024.