Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 5693962, 10 pages
https://doi.org/10.1155/2022/5693962

Research Article

Intelligent Blockchain-Based Secure Routing for Multidomain SDN-Enabled IoT Networks

Zhihao Zeng, Xiaoning Zhang, and Zixiang Xia

School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu, China

Correspondence should be addressed to Zhihao Zeng; zengzh688@outlook.com

Received 26 December 2021; Accepted 21 January 2022; Published 24 February 2022

Academic Editor: Xiaojie Wang

The development of fifth-generation (5G) mobile communication technology has become a major driver to the growth of Internet of Things (IoT) applications. As a promising networking paradigm, software-defined networking (SDN) makes IoT more flexible and agile by decoupling control plane from data plane. With a large number of heterogeneous devices accessing to the network, we need to divide the network into several domains and each domain is managed by an SDN controller. Controllers share topologies with each other to form global view of the entire network, which is used for crossing-domain path routing. However, crossing-domain routing requires global trust between multiple controllers. The reason is that if the malicious controller shares misleading topologies, the rest of controllers may calculate mistaken crossing-domain paths. As a result, packets are forwarded to the domain that is managed by the malicious controller and dropped deliberately, which is known as the black-hole attack. To this end, we present a blockchain-based architecture to ensure secure routing among multiple domains in SDN-enabled IoT networks. All SDN controllers are equipped with blockchains, and they upload abstract topologies to the blockchain via the smart contract. Thus, the genuine view of the entire network can be gained from the blockchain due to its consensus and immutability. In addition, we use the concept of reputation that consists of the local reputation and the global reputation to further protect routing reliability, and the global reputation is reserved in the blockchain. Compared with benchmark architectures, the emulation results show that our proposed method can effectively build trust between multiple controllers and ensure secure routing among multiple domains.

1. Introduction

Fifth-generation (5G) [1] mobile communication technology has significantly expanded the scope and scale of Internet of Things (IoT) [1] by providing high-speed connections and communications, where billions of smart devices can access to the Internet. These smart devices with heterogeneous characteristics (such as phones, sensors, and virtual reality devices) have generated volumes of data [2]. Meanwhile, machine learning (ML), as another important field, has achieved important success in many aspects, such as computer version, pattern classification, and natural language processing [3, 4]. Recently, there has been a rising trend of employing ML to improve IoT applications [5]. Edge IoT devices upload their raw data to a remote data center and perform the training in a centralized manner [6], which brings new technical challenges for the IoT network.

As a promising networking paradigm, software-defined networking (SDN) [7] is compatible to IoT [8, 9]. Heterogeneous devices need to transmit data, but they have different needs for network routing and forwarding. Based on the central architecture, the SDN network can easily implement these requirements. Controllers configure switches directly through OpenFlow protocol, which makes configuration and expansion easier and cheaper. Switches only need to forward packets. On the other hand, in the traditional IP network, switches and routers require to be configured manually as they belong to different manufacturers.

Since the SDN-enabled IoT network contains a large number of devices, how to efficiently perform packet

delivery is an important problem. In the large-scale environment, a single SDN controller cannot deal with transmission requests of switches when it remains in a heavy load condition, which reduces the forwarding capability [10]. Thus, we divide the network into several domains and deploy multiple controllers for management [11]. In Figure 1, we illustrate the architecture of SDN-enabled multidomains IoT networks. In the architecture, heterogeneous IoT devices [12] are connected to SDN switches through wireless or wired links, such as 5G, WiFi, and WLAN. Multiple controllers work together to manage the entire network.

Since the controller can only sense the structure of its own managed network, the SDN controllers share topologies that are used for crossing-domain routing with each other to set up a global view of the SDN-enabled multidomain IoT network. However, trust issues between multiple controllers are critical for the crossing-domain routing. For example, a malicious controller may distribute misleading topology. Generally speaking, the malicious controller often claims that its managed domain has low latency and high bandwidth in order to achieve this deceptive matter. As a consequence, other controllers will compute out mistaken paths and packets will be forwarded throughout the malicious domain [13, 14]. So the malicious controller can configure switches to deliberately drop the passing packets, which is known as the black attack, causing packet loss problem and threatening routing security.

The blockchain, an emerging decentralized technology, provides us with solutions to the above security problems. The blockchain contributes a distributed peer-to-peer network where untrusted individuals can interact in a verifiable manner with each other [15] without a trusted intermediary. The blockchain can be considered an immutable and decentralized digital ledger. Each block is mainly composed of the hash value of the previous block, the transaction records, and the timestamp. Due to the inherent cryptographic chaining, the malicious behavior can be easily detected via the hash value [16].

To this end, we leverage the method of blockchain to protect secure routing in SDN-enabled multi-controller IoT networks. Controllers interact with the blockchain nodes to build the global trust via the smart contract. The smart contract is a self-executing contract with the terms of agreement, which is written into lines of code in the blockchain. The SDN controllers upload their abstract topologies to the blockchain [17]. The abstract topology only consists of intra-domain virtual links and inter-domain links [18], which protects network privacy from disclosure as well as reduces the size of information. The abstract topology should be validated by other controllers before finally reserved in the blockchain. We use the concept of reputation to further promote routing reliability. The reputation concept consists of the local reputation and the global reputation, and the global reputation is reserved in the blockchain [19]. We use the combination of ONOS, Mininet, and hyperledger Fabric to conduct our experiments. Compared with the benchmark architecture, the emulation results show that our proposed method can effectively build trust between multiple controllers and ensure secure routing among multiple domains.

In this article, our main contributions are summarized as follows:

(1) We apply the blockchain technology to the SDN controllers to ensure secure routing among multiple domains.

(2) We use the local reputation and the global reputation to further promote the routing reliability, and the global reputation is reserved in the blockchain.

(3) We develop a testbed composed of ONOS, Mininet, and hyperledger Fabric to emulate networks.

The rest of this article is organized as follows. In Section 2, we briefly review the literature related to this article. In Section 3, we present a blockchain-based SDN-enabled network architecture. In Section 4, we propose the reputation mechanism. We evaluate the emulation results in Section 5 and conclude this article in Section 6.

2. Related Work

The main purpose of this article is to ensure secure routing among multiple domains in SDN-enabled IoT networks. In this area, there are some existing works. These works mainly focus on the following two parts.

For the first part, several mechanisms have been proposed to optimize the routing path among multiple domains. Deng et al. [10] proposed a path selection algorithm of multi-controller SDN networks, which has considered topologies synchronization and user requests. Xiao et al. [11] applied communicating sequential processes to model the routing service of multi-controller SDN architectures. Jamal et al. [20] proposed a management method for the control layer in the SDN multi-controller scene, which optimizes the controller placement by maximizing the flexibility and scalability of inter-domain connections. Fan et al. [21] introduced K-means clustering algorithm to optimize multi-controller deployment, which aims at minimizing the time delay between a controller and switches. Bagci et al. [22] proposed a multi-controller open exchange architecture in the SDN network by optimizing crossing-domain paths dynamically, which enables the ability that the single controller can provide inter-domain services. Although these above approaches optimize the deployment of multiple controllers and the path selection among domains, they do not consider trust problem between multiple controllers.

For the second part, several mechanisms have applied blockchain to protect SDN security. Chattaraj et al. [23] presented a scheme named BACC-SDN, which enables secure access between SDN applications, and SDN controllers and switches based on blockchain. Liu et al. [24] proposed a framework called BS-IoT, which supports the cooperative IoT networking management using blockchain technology. Fernando et al. [17] designed a two layers infrastructure, which consists of multi-controller SDN networking layer and blockchain-based autonomy layer. It enhances the integrity of the control and management commands. Singh et al. [13]

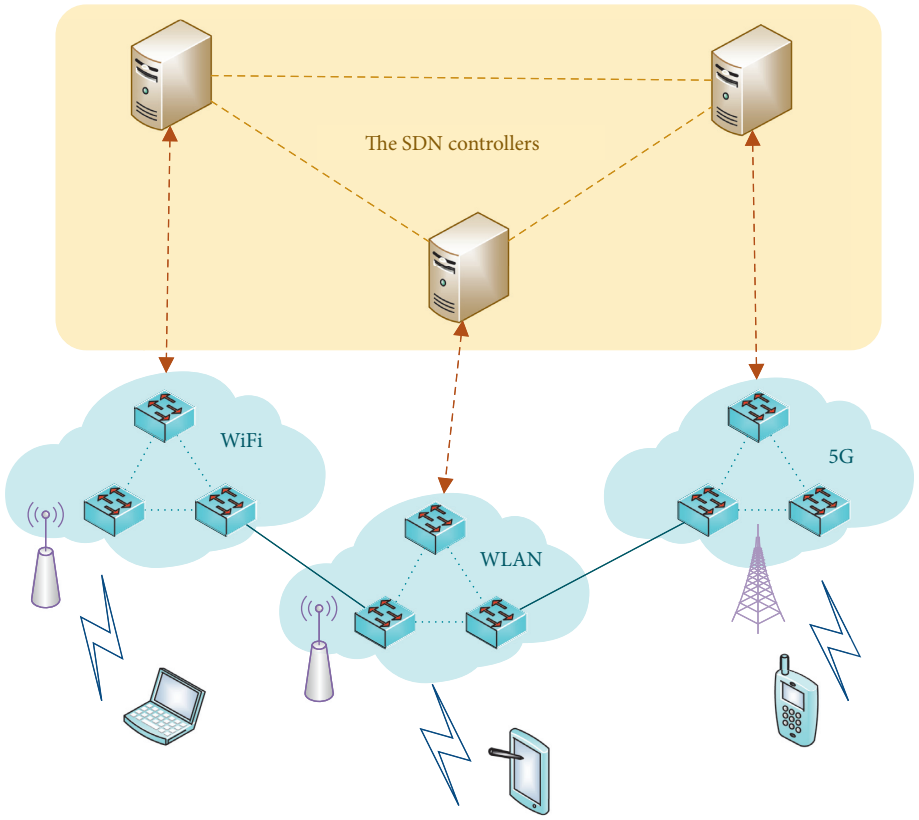

Figure 1: The SDN-enabled multi-controller IoT network.

integrated the blockchain with switches in the forwarding layer, which prevents uncontrolled traffic flows. Alemany et al. [25] presented a blockchain-based SDN architecture to integrate multiple domains in the SDN network, avoiding the reliance upon the SDN controllers.

There are three main differences between this article and the existing literature. Compared with the previous work, the first difference is that we deeply design the architecture to ensure secure routing among multiple domains using the blockchain technology, which is more specific and practical. Another difference is that we use the abstract topologies to meet the network privacy concerns. The final difference is that based on this architecture, we propose the concept of reputation and combine it with the blockchain.

3. A Blockchain-Based Architecture for Secure Routing in SDN-Enabled IoT Networks

In this section, we use abstract topologies to hide the precise information of the network, and we record the abstract topologies in the blockchain. We implement a verification process in the application layer and a voting mechanism in the smart contract to filter mistaken abstract topologies, and the verification results affect reputations of the SDN controllers.

3.1. The Abstract Topology. In the SDN-enabled multi-controller IoT network, controllers share their local topologies to form the global view of the entire network. The global topology can help the SDN controllers compute crossing-domain paths. However, local topologies shared with other controllers usually contain precise information of the network, which may result in privacy disclosure. For example, competitors can figure out the specific structure (such as the number of switches and link connections) of the network from the precisely shared local topology, which may cause privacy concerns.

Figure 2(a) shows the precise view of the entire network [26]. The SDN controllers are denoted by grey points. The red points and blue points denote the edge switches and intra-domain switches, respectively. And the red lines and blue lines denote the inter-domain links and intra-domain links, respectively. To protect the privacy of the network, we simplify the precise topology into the abstract topology. Several intra-domain links and switches are compressed as a virtual link, which hides the details of the network. So the abstract network only consists of inter-domain links and intra-domain virtual links.

As illustrated in Figure 2(b), controller $c1$ receives the abstract topology of controllers $c2$ and $c3$ [26]. In this figure, the red virtual lines denote the intra-domain virtual links. Controller $c1$ can compute crossing-domain paths by this simplified information without the details of $c2$ and $c3$ networks.

3.2. System Model. The blockchain-based SDN architecture consists of four layers, which are blockchain layer, application layer, control layer, and forwarding layer. The

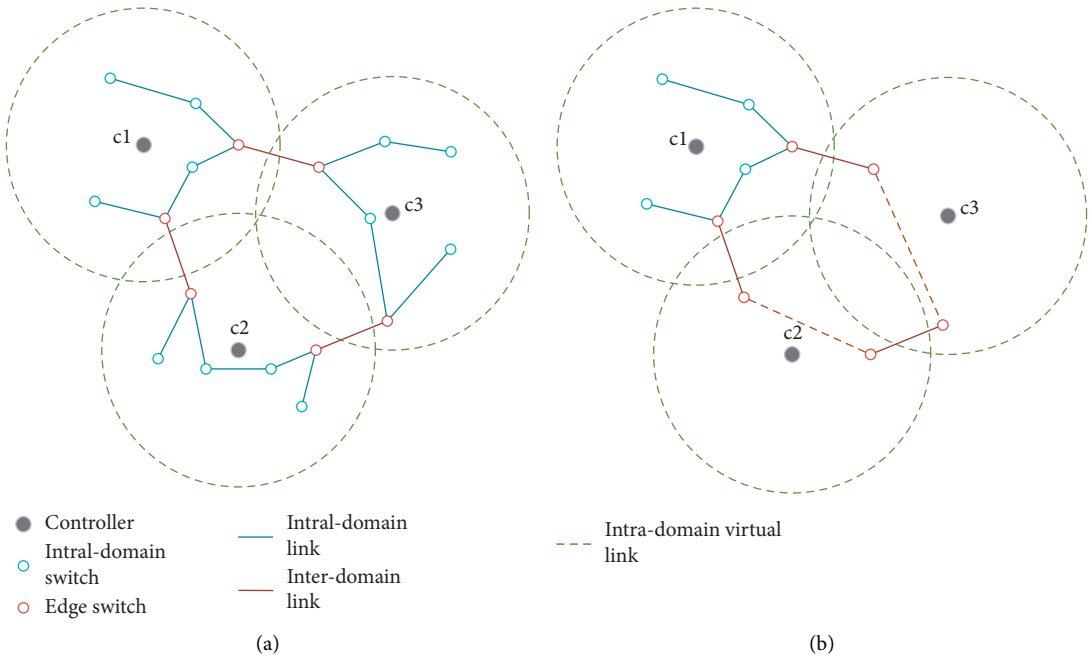

Figure 2: The abstract topology. (a) The precise view of the entire network. (b) Controller c1's view of the entire network.

architecture is illustrated in Figure 3. Compared with the conventional SDN architecture, we use the blockchain technology to equip the SDN controllers.

In the blockchain layer, we implement a smart contract that stores the abstract topologies and the SDN controllers' reputations as state variables. The SDN controllers upload their abstract topologies to the smart contract [17] through Google Remote Procedure Call (gRPC). Because the smart contract is part of the blockchain, which is called the chain code, in other words, the abstract topologies and reputations are reserved in the blockchain. The stored information is illustrated in Figure 4. The abstract topologies are composed of inter-domain links and intra-domain virtual links. And we use the reputation concept to reflect the reliability of the domain managed by the SDN controllers. The links and reputations are reserved in (key, value) format. Although the information stored in the blockchain is immutable, we should make sure that the information is correct. To achieve this, we implement a vote mechanism in the smart contract. When a controller uploads the abstract topology to the blockchain, the rest of controllers will verify it. If and only if over a half of the controllers prove correctness of the abstract topology, the smart contract will reserve it finally. Otherwise, the smart contract will clear it. The verification results also affect the reputations, which we will describe in Section 4.

In the application layer, we develop an application to interact with the smart contract. The application simplifies the precise topology to the abstract topology. Then, it uploads the abstract topology to the smart contract. As we stated above, the rest of controllers will verify the abstract topology by sending the ICMP packets to detect the edge switches.

Control layer is composed of link layer discovery protocol (LLDP) module and traffic routing module. The controller applies the LLDP module to discover

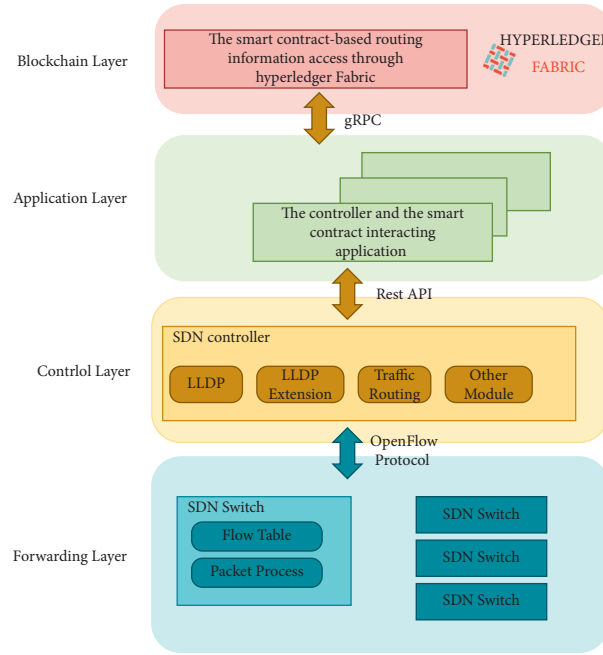

Figure 3: The blockchain-based SDN architecture.

intra-domain link and executes the traffic module to configure flow tables in the SDN switches. Since the LLDP module cannot find inter-domain links, we add the LLDP extension to advance the discovery [18]. And the forwarding layer processes and forwards packets in terms of flow tables.

3.3. Workflow. In Figure 5, we show the collaborating process of the smart contract and the controllers. At first, the controller uploads the abstract topology to the smart

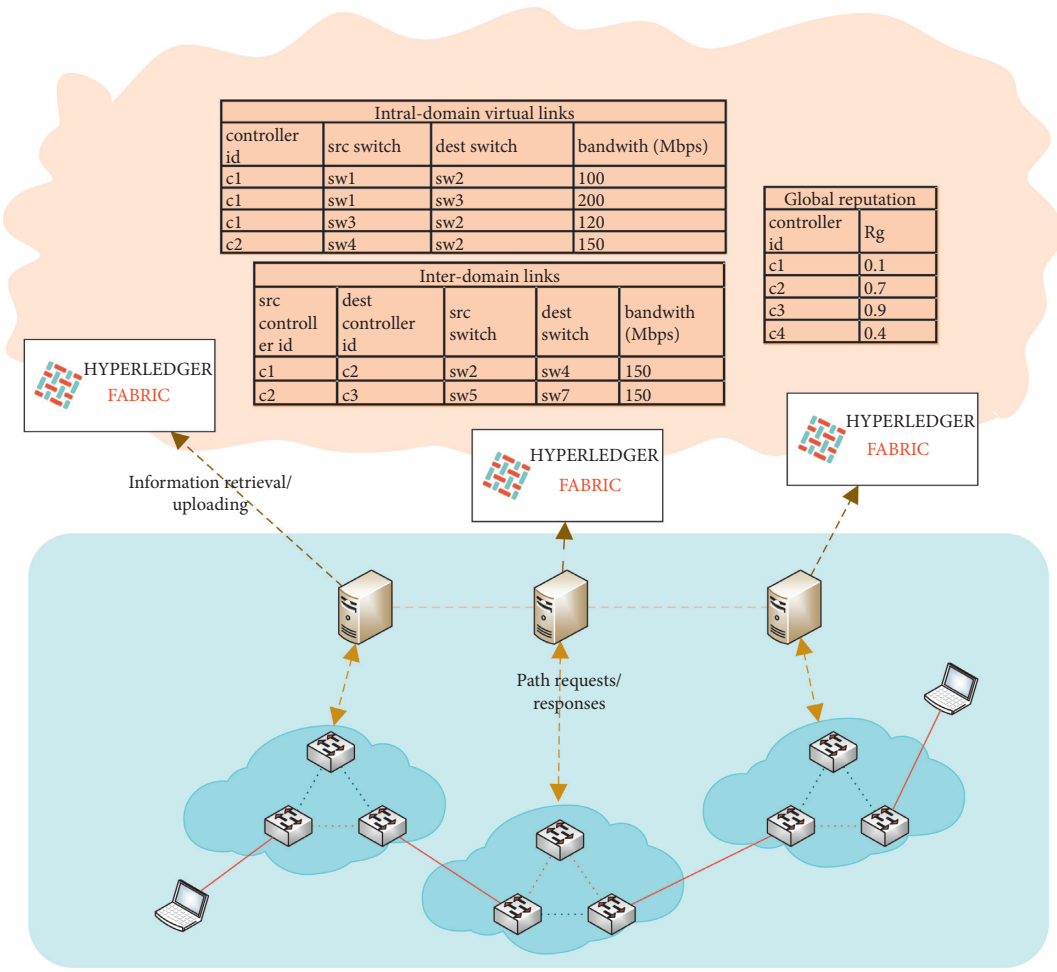

Figure 4: Blockchain-based SDN-enabled IoT networks.

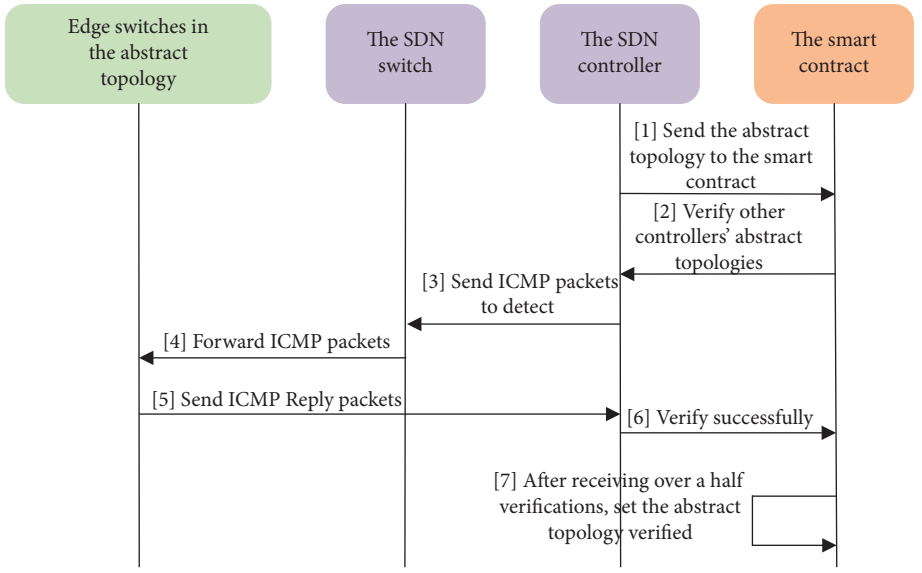

Figure 5: The validation and voting process.

contract. Since the uploading topology may be mistaken, we need to validate it. The validation method is sending probing packets, such as ICMP packets. Controllers send ICMP packets to detect edge switches exposed in the abstract topologies. If controllers receive ICMP replies, we can prove the existence of inter-domain links. But this method cannot

detect intra-domain virtual links. To make up for this shortcoming, we stipulate that if and only if over a half of the controllers prove the correctness of the abstract topology and vote it via the smart contract, the smart contract could finally reserve it, which increases the accuracy of the validation. Otherwise, if not over a half, the smart contract will clear the abstract topology. We further propose the reputation concept according to the verification results, consisting of the global reputation and local reputation. The smart contract will increase the global reputation of the controller that shared correct abstract topology, which we will describe in Section 4. The reputations can reflect controller's reliability based on its sharing behavior.

As shown in Figure 4, the interaction between the SDN controllers and the smart contract is the information retrieval and uploading, and the interaction between the SDN controllers and the switches is path request and response. When a device starts a connection to another device in the remote domain, the verified abstract topologies and the global reputations in the blockchain can protect devices against packet loss and data leakage. Figure 6 illustrates the procedure of the path request. First, the SDN switches request the controller for flow tables. Then, the controller takes all verified abstract topologies and global reputations in the blockchain to compute a reliable path. The path avoids low reputation domains as well as performs the shortest distance under bandwidth constrains. Next, the controller configures the path as flow tables to the SDN switches. Finally, the packets could be forwarded among multiple domains in security.

4. The Reputation Mechanism

In this section, according to the validation results of the abstract topologies in Section 3, we further propose a mechanism that leverages the reputation concept that consists of the local reputation and the global reputation to reflect the behavior of the SDN controllers. We apply Bayesian theory to estimate the local reputation, and we use blockchain to reserve the global reputation. All the notations used in this article are listed in Table.1.

4.1. The Reputation Components. Our reputation mechanism consists of two indicators: the local reputation and the global reputation [19]. Controllers validate abstract topologies to generate the local reputations and send them to the smart contract. Then, the smart contract counts these local reputations to form the global reputation. The global reputation in the blockchain can be used as a metric for reliable path computation. We use R_l to denote the local reputation, which is reserved in the controller's local storage. Every controller evaluates other controllers' reputations locally, which is performed by sending ICMP packets to validate the correctness of the abstract topology uploaded to the blockchain. $R_{l_{ij}}$ denotes controller i's evaluation to controller j. We use R_g to denote the global reputation, which is reserved in the blockchain. R_{g_i} denotes the global reputation of controller i. Since the R_{g_i} is stored in the blockchain, it can be obtained by all controllers.

4.2. Bayesian Estimation of the Local Reputation. According to the analysis and investigation of the mistaken routing information of NANOG's administration e-mail lists [27], the occurrence that malicious controller uploads mistaken abstract topology is randomly, and this bad behavior would last for a period time once it happens. For example, we do not know the time when the controller becomes malicious, but when the controller behaves badly, it will sustainably distribute misleading abstract topologies. As the abstract topology is either correct or incorrect, we consider this event as a Bernoulli incident.

Based on the Bayesian theory, the conjugate prior probability distribution of Bernoulli incident is Beta distribution [28]. We set α as the number of times that the SDN controller uploads correct topologies and β as the number of times that the SDN controller uploads mistaken topologies. We can get Beta distribution as follows:

$$\begin{aligned} f(x;\alpha,\beta) &= \frac{x^{\alpha-1}(1-x)^{\beta-1}}{\int_0^1 u^{\alpha-1}(1-u)^{\beta-1}\mathrm{d}x} \\ &= \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)}x^{\alpha-1}(1-x)^{\beta-1}, \end{aligned} \tag{1}$$

where x denotes the realization of a random process X, which is the probability of the correct abstract topology, and $\alpha > 1$, $\beta > 1$. The expected value of the Beta distribution random variable is as follows:

$$\begin{aligned} R_{l_{ij}} = \mu = E[X] &= \int_0^1 x f\left(x;\alpha_{ij},\beta_{ij}\right)\mathrm{d}x \\ &= \frac{\alpha_{ij}+1}{\alpha_{ij}+\beta_{ij}+2}, \end{aligned} \tag{2}$$

where α_{ij} denotes the correct times of controller i's validation to controller j and β_{ij} denotes the incorrect times of controller i's validation to controller j. μ denotes the expected value, which is the probability of the next correct abstract topology. As a result, we use μ to reflect the controller's reputation. For example, controller i validates that there are α_{ij} times and β_{ij} times that controller j uploads correct and mistaken topologies, respectively, to the blockchain, so the local $R_{l_{ij}}$ calculated by controller i is $(\alpha_{ij}+1)/(\alpha_{ij}+\alpha_{ij}+2)$.

4.3. The Blockchain-Based Global Reputation. With the local reputation estimation, every controller has the rest of controllers' reputations locally. But local reputations are weak of taking account of real behaviors. Based on the blockchain architecture, we propose the global reputation R_g to further take account. Controllers send their R_l to the smart contract, and the smart contract would calculate the global reputation R_g by the weighted mean of local reputations R_l as follows:

$$R_{g_i} = \sum_{k=1,k\neq i}^{n} w_k R_{l_{ki}}, \tag{3}$$

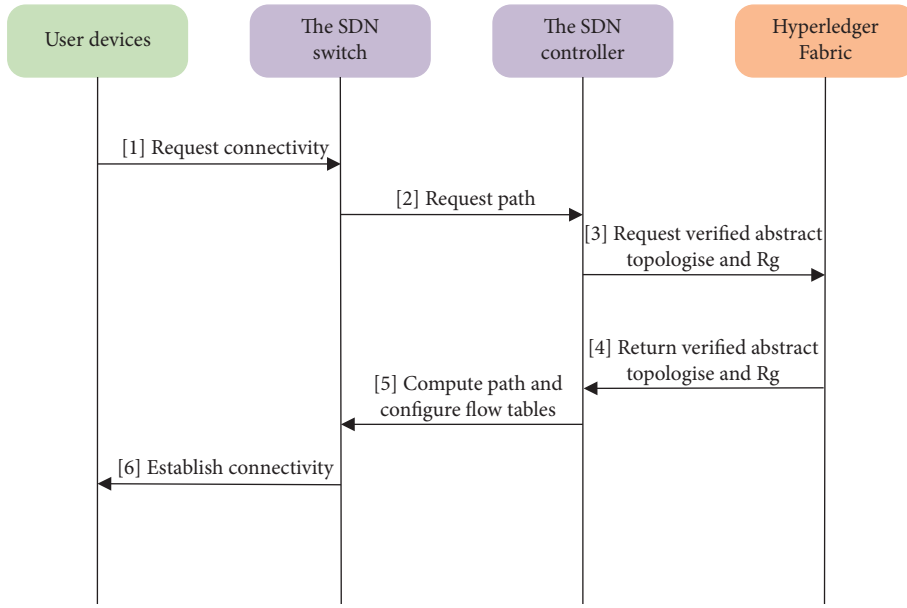

Figure 6: The crossing-domain path request process.

Table 1: Notations used in the article.

Notation	Description
topo_i	The abstract topology of controller i
C	The set of controllers
c_i	The controller i
$R_{l_{ij}}$	The local reputation estimation form controller i to j
R_{g_i}	The global reputation of controller i
$R_{g_{it}}$	The time decay global reputation of controller i
α_{ij}	The correct times that controller i has validated controller j's abstract topology
β_{ij}	The incorrect times that controller i has validated controller j's abstract topology
w_k	The weighted factor of controller k
λ_i	The decay rate of the global reputation of controller i
NUM	The number of edge switches

where R_{g_i} denotes the global reputation of controller i and $R_{l_{ki}}$ denotes the local reputation that controller k sends to the smart contract. Also we use the weight value w to reflect the influence factor of controller k. The weight value w is as follows:

$$w_k = \frac{R_{g_k}}{\sum_{j=1}^{n} R_{g_j}}, \tag{4}$$

where R_{g_k} denotes controller k's current global reputation, and we can also leverage R_{g_k} as an influence factor of estimated local reputation about other controllers by controller k because the controller with a higher global reputation would give a more convincing estimated local reputation about other controllers.

In addition, we apply time decay function to the global reputation computation as the global reputation only captures temporal information of the controller and the old global reputation cannot reflect the current situation [29, 30]. We use exponential function to express time decaying, which is given as follows:

$$N_t = N_0 e^{-\lambda t}, \tag{5}$$

where $N(t)$ denotes the decaying quantity, N_0 denotes the initial quantity, and λ denotes the decay rate.

According to (5), the time decay global reputation can be formulated as

$$R_{g_{it}} = R_{g_{i0}} e^{-\lambda_i t} = \left(\sum_{k=1, k \neq i}^{n} w_k R_{l_{ki}} \right) e^{-\lambda_i t}, \tag{6}$$
$$\lambda_i \propto \text{NUM}_{\text{edge switches}},$$

where $R_{g_{it}}$ denotes the decaying global reputation and $R_{g_{i0}}$ denotes the initial global reputation. We use $_{\text{NUM edge switches}}$ to denote the number of edge switches. And the decay rate λ_i is proportional to $\text{NUM}_{\text{edge switches}}$. Because a large-scale domain handles amounts of packets, it should update its global reputation frequently to maintain its global reputation at a fine level. And a large-scale domain has numbers of edge switches. So we build a connection between the number of edge switches and the decay rate. The reason is that a large-scale domain handles amounts of packets and the controller should often upload its abstract topology, being validated by other controllers.

Input: The unverified abstract topology topo_i in the blockchain uploaded by controller i; the set of controllers $C = \{c_1, c_2, \ldots, c_n\}$
Output: the global reputation $R_{g_{it}}$ of controller i
1: The smart contract informs controllers to validate topo_i
2: **for all** $c_k \in C, k \neq i$ **do**
3: Send ICMP packets to validate edge switches
4: **if** controller k receives ICMP relies **then**
5: Beta distribution parameter $\alpha_{ki} \longleftarrow \alpha_{ki} + 1$
6: **else**
7: Beta distribution parameter $\beta_{ki} \longleftarrow \beta_{ki} + 1$
8: **end if**
9: Estimate the local reputation $R_{l_{ki}} \longleftarrow \alpha_{ki} + 1/\alpha_{ki} + \beta_{ki} + 2$
10: Controller k send $R_{l_{ki}}$ to the smart contract
11: **end for**
12: The smart contract calculates controller i's global reputation $R_{g_{i0}} \longleftarrow \sum_{k=1,k\neq i}^{n} w_k RV_{l_{ki}}$
13: The smart contract makes the global reputation time decay, $R_{g_{it}} \longleftarrow R_{g_{i0}} e^{-\lambda_i t}$
14: **return** R_{g_i}

Algorithm 1: Reputation update algorithm.

Through the estimation of local reputation R_l and the calculation of global reputation R_g, we design the Reputation Update Algorithm that is illustrated in Algorithm 1. First, when controller i uploads the abstract topology topo_i to the blockchain, the smart contract will inform the rest of controllers to validate topo_i. Then, the rest of controllers apply ICMP packets to detect the edge switches of topo_i. If receiving ICMP replies, controllers update the Beta distribution parameters, α_{ki} and β_{ki}, based on Bayesian estimation. Next, controllers calculate local reputations $R_{l_{ki}}$ based on the expected value and send it to the smart contract. Finally, the smart contract gathers all local reputations $R_{l_{ki}}$, $k = \{1, 2, \ldots, n\}$, $k \neq j$, and calculates their weighted mean value, obtaining the time decay global reputation $R_{g_{it}}$.

5. Performance Evaluation

In this section, the performance of blockchain-based SDN-enabled secure routing (BSDNSR) model is studied. We first introduce the simulation setting. After that, the simulation results are presented.

5.1. Methodology and Simulation Setting

5.1.1. Setup. We implement a test network that is illustrated in Figure 7. Initially, all controllers' local reputations and global reputations are set to 1.0. All hosts send data packets with each other. After a period of time, the controller c3 will start uploading mistaken abstract topologies to the blockchain. To eliminate statistical fluctuations, each group of results is obtained by averaging on 10 experiments.

5.1.2. Benchmark Solutions. (1) Pure SDN-enabled inter-domain routing (PSDNIR) model: in PSDNIR, controllers just declare local topologies with each other without any security protections for crossing-domain routing; (2) AS cooperative inter-domain reputation (ASCIR) model: in ASCIR [19], based on the Bayesian theory, nodes establish local reputations according to forwarding behaviors and

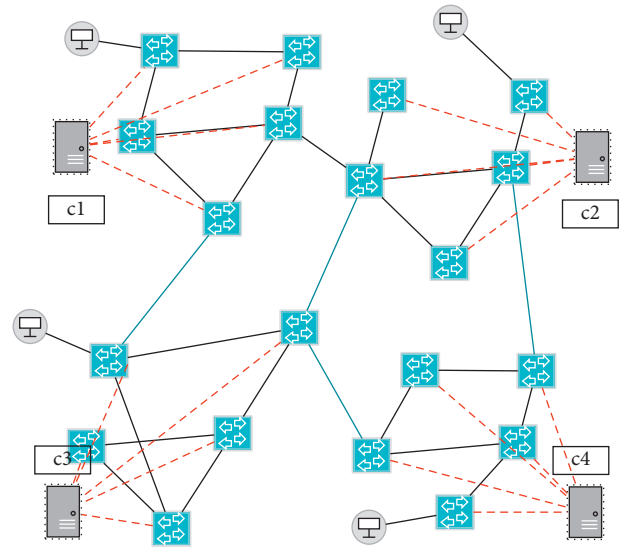

Figure 7: Test network with malicious controller c3.

summarize global reputations by the weighted mean of local reputations on the basis of the domain's features. It should be emphasized that we use controllers to represent nodes in this experiment in ASCIR.

The main difference between BSDNSR and other benchmarks is that BSDNSR applies the blockchain technology and the reputation method to jointly protect the routing security among multiple domains in the SDN-enabled network. PSDNIR is regarded as the most basic model, from which we can figure out the worst scenario without any protections in crossing-domain routing. ASCIR adds the reputation method into routing, which makes the scenario better. BSDNSR uses the blockchain tonology and the reputation method to further improve the performance.

5.1.3. Performance Metrics. (1) The efficiency of the global reputation *reputation*: how efficiently the reputation mechanism reacts against controllers' malicious behavior.

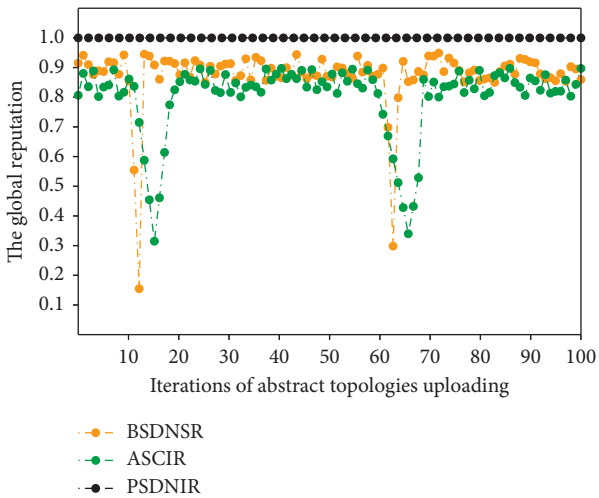

Figure 8: The efficiency analysis of the global reputation.

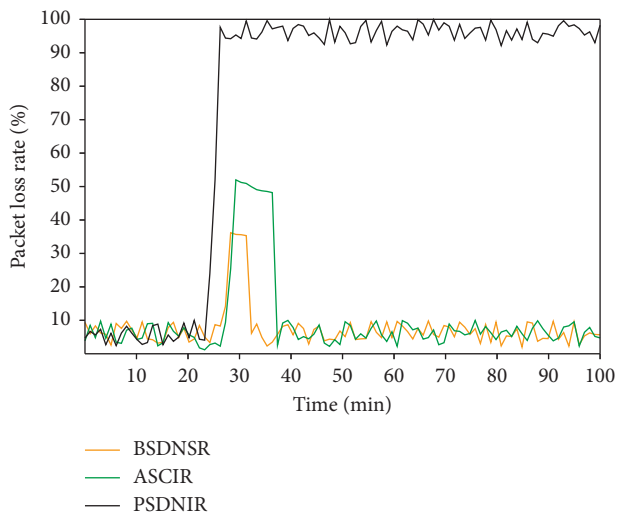

Figure 9: The packet loss of a crossing-domain path.

(2) The packet loss of a crossing – domain path: the packet loss rate under different security methods when some controllers become malicious.

5.2. Results

5.2.1. The Efficiency of the Global Reputation. Figure 8 shows the performance of different reputation mechanisms to handle malicious behaviors. The results in the figure are trends of the global reputation of controller c3 with the iteration of abstract topologies uploading. In PSDNIR, global reputations are always 1.0, because PSDNIR obviously has no reputation mechanism, which treats all controllers equally despite bad actions. Global reputations in BSDNSR and ASCIR both have been decreased at iterations 9 and 57, which tells that controller c3 has uploaded mistaken abstract topologies at these two periods. The global reputation in BSDNSR has started decreasing about 11% earlier than ASCIR when the controller behaved badly and also started increasing about 15% earlier than ASCIR when the controller returned normal. As a result, we can tell that BSDNSR is more sensitive than ASCIR against malicious behaviors.

5.2.2. The Packet Loss of a Crossing-Domain Path. Figure 9 shows the packet loss rate of a crossing-domain path when times increase. The host in the controller c1's domain continued to send packets to the host in the controller c4's domain. Initially, we set the path passing the controller c3's domain. After a period of time, the controller c3 became malicious. From the results, we can tell that packet loss rates increased sharply in PSDNIR, up to nearly 100%, which indicates that all packets that passed through the malicious domain were dropped. Both BSDNSR and ASCIR have shifted their paths to pass the controller c2's domain at the time $t = 22$ min when the controller c3 became malicious. But the packet loss in BSDNSR has been recovered faster than that in ASCIR, and the reduction in loss rates has improved about 20%.

From the results above, two metrics, the efficiency of reputation mechanism and the packet loss rate of a crossing-domain path, have both indicated that BSDNSR is more sensitive than ASCIR against risky domains. The reason is that the smart contract has collected information of all controllers in BSDNSR, and controllers can obtain trusted and verified information directly under the bridge of the blockchain, whereas in ASCIR, controllers need to communicate with each other one by one to summarize their reputations, which slows down recoveries to security problems.

6. Conclusion

In this article, we study the secure routing among multiple domains in the SDN-enabled IoT network. We first propose a blockchain-based SDN-enabled network architecture. In this architecture, the SDN controllers simplify the local topologies into the abstract topologies and upload them to the blockchain via the smart contract. We add the validation process and the voting mechanism to confirm the correctness of the abstract topologies. According to the validation of abstract topologies, we use the reputation concept, that consists of the local reputation and the global reputation to further protect routing reliability. The global reputation is reserved in the blockchain. Compared with benchmark architectures, our architecture can effectively build global trust between multiple controllers and protect routing reliability among multiple domains.

Data Availability

The data are available at https://gitee.com/zhihaozeng/hyperledger-fabric-and-onos and https://gitee.com/zhihaozeng/TopoBuilder.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] S. Li, L. D. Xu, and S. Zhao, "5g internet of things: a survey," *Journal of Industrial Information Integration*, vol. 10, pp. 1–9, 2018, https://www.sciencedirect.com/science/article/pii/S2452414X18300037.

[2] F. Li, R. Xie, Z. Wang et al., "Online distributed iot security monitoring with multidimensional streaming big data," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4387–4394, 2020.

[3] X. Wang, Z. Ning, S. Guo, M. Wen, and P. Vincent, "Minimizing the age-of-critical-information: an imitation learning-based scheduling approach under partial observations," *IEEE Transactions on Mobile Computing*, 2021.

[4] L. Cui, S. Yang, F. Chen, Z. Ming, N. Lu, and J. Qin, "A survey on application of machine learning for internet of things," *International Journal of Machine Learning and Cybernetics*, vol. 9, no. 8, pp. 1399–1417, 2018.

[5] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for internet of things (iot) security," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1646–1685, 2020.

[6] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated blockchain and edge computing systems: a survey, some research issues and challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1508–1532, 2019.

[7] T. Huang, F. R. Yu, C. Zhang, J. Liu, J. Zhang, and Y. Liu, "A survey on large-scale software defined networking (sdn) testbeds: approaches and challenges," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 891–917, 2017.

[8] Z. Ning, Y. Yang, and X. Wang, "Dynamic computation offloading and server deployment for uav-enabled multi-access edge computing," *IEEE Transactions on Mobile Computing*, 2021.

[9] Z. Lv and W. Xiu, "Interaction of edge-cloud computing based on sdn and nfv for next generation iot," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 5706–5712, 2020.

[10] Y. Deng, Y. Wang, X. He, and H. Feng, "An inter-domain transmission path selection approach of multi-controller sdn network based on fpga," in *Proceedings of the 2018 14th International Conference on Computational Intelligence and Security (CIS)*, pp. 66–70, Hangzhou, China, November 2018.

[11] L. Xiao, H. Zhu, S. Xiang, and P. Cong Vinh, "Modeling and verifying sdn under multi-controller architectures using csp," *Concurrency and Computation: Practice and Experience*, vol. 33, no. 2, https://onlinelibrary.wiley.com/doi/abs/10.1002/cpe.5334, Article ID e5334, 2021.

[12] X. Wang, Z. Ning, and S. Guo, "Dynamic uav deployment for differentiated services: a multi-agent imitation learning based approach," *IEEE Transactions on Mobile Computing*, vol. 1–1, 2021.

[13] M. Singh, G. S. Aujla, A. Singh, N. Kumar, and S. Garg, "Deep-learning-based blockchain framework for secure software-defined industrial networks," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 1, pp. 606–616, 2021.

[14] F. Oliviero and S. P. Romano, "A reputation-based metric for secure routing in wireless mesh networks," in *Proceedings of the IEEE GLOBECOM 2008 - 2008 IEEE Global Telecommunications Conference*, pp. 1935–1939, New Orleans, LA, USA, November 2008.

[15] P. K. Sharma, S. Singh, Y.-S. Jeong, and J. H. Park, "Distblocknet: a distributed blockchains-based secure sdn architecture for iot networks," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 78–85, 2017.

[16] Z. Ning, S. Sun, and X. Wang, "Blockchain-enabled intelligent transportation systems: a distributed crowdsensing framework," *IEEE Transactions on Mobile Computing*, 2021.

[17] P. Fernando and W. Jin, "Blockchain-powered software defined network-enabled networking infrastructure for cloud management," in *Proceedings of the 2020 IEEE 17th Annual Consumer Communications Networking Conference (CCNC)*, pp. 1–6, Las Vegas, NV, USA, January 2020.

[18] P. Lin, J. Bi, and Y. Wang, "Webridge: west-east bridge for distributed heterogeneous sdn noses peering: webridge for distributed heterogeneous sdn noses peering," *Security and Communication Networks*, vol. 8, 2014.

[19] D. Chen, H. Qiu, and K. J. Zhu, "An inter-domain routing reputation model based on autonomous domain collaboration (in Chinese)," *The Science of Sin*, vol. 51, pp. 1540–1558, 2021.

[20] M. Saalim Jamal, A. Hirwe, and K. Kataoka, "Vibhajan: a lightweight and scalable control plane management for multi-controller SDN," in *Proceedings of the 2018 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, pp. 1–7, Verona, Italy, November 2018.

[21] M. Fang, Y. Wang, and M. Ye, "A multi-controller deployment method of sdn network based on FPGA," in *Proceedings of the 2019 15th International Conference on Computational Intelligence and Security (CIS)*, pp. 262–266, Macao, China, December 2019.

[22] K. Tolga Bagci and A. Murat Tekalp, "Sdn-enabled distributed open exchange: dynamic qos-path optimization in multi-operator services," *Computer Networks*, vol. 162, 2019 https://www.sciencedirect.com/science/article/pii/S1389128618308387, Article ID 106845.

[23] D. Chattaraj, S. Saha, B. Bera, and A. K. Das, "On the design of blockchain-based access control scheme for software defined networks," in *Proceedings of the IEEE INFOCOM 2020—IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 237–242, Toronto, ON, Canada, July 2020.

[24] L. Liu, W. Feng, and C. Chen, "Bs-iot: blockchain based software defined network framework for internet of things," in *Proceedings of the IEEE INFOCOM 2020—IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 496–501, Toronto, ON, Canada, July 2020.

[25] P. Alemany, R. Vilalta, R. Muñoz, R. Casellas, and R. Martínez, "Blockchain-based connectivity provisioning in multiple transport sdn domains," in *Proceedings of the 2021 International Conference on Optical Network Design and Modeling (ONDM)*, pp. 1–3, Gothenburg, Sweden, June 2021.

[26] F. Deng, "Design and implementation of multi-controller system based on sdn in mobile communication scene," Master's thesis, p. 6, Chongqing University of Posts and Telecommunications, Chongqing, China, Chongqing University of Posts and Telecommunications, 2019.

[27] N. Hu, P. Zou, and P. D. Zhu, "Reputation-based collaborative management method for inter-domain routing security," *Journal of Software*, vol. 21, pp. 505–511, 2010.

[28] A. Josang and R. Ismail, "The beta reputation system," in *Proceedings of the 15th bled electronic commerce conference*, vol. 5, pp. 2502–2511, Bled, Slovenia, June 2002.

[29] J. Lee and J. C. Oh, "A node-centric reputation computation algorithm on online social networks," in *Lecture Notes in Social Networks Applications of Social Media and Social Network Analysis*, pp. 1–22, Springer, Berlin, Germany, 2015.

[30] A. Melnikov, J. Y. Lee, V. Rivera, M. Mazzara, and L. Longo, "Towards dynamic interaction-based reputation models," in *Proceedings of the 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA)*, pp. 422–428, Krakow, Poland, May 2018.