IEICE TRANS. INF. & SYST., VOL.E103–D, NO.2 FEBRUARY 2020

INVITED PAPER *Special Section on Security, Privacy, Anonymity and Trust in Cyberspace Computing and Communications*

Towards Blockchain-Based Software-Defined Networking: Security Challenges and Solutions

Wenjuan LI[†,††], **Weizhi MENG**[††a)], **Zhiqiang LIU**[†††], ***and*** **Man-Ho AU**[††††], ***Nonmembers***

SUMMARY Software-Defined Networking (SDN) enables flexible deployment and innovation of new networking applications by decoupling and abstracting the control and data planes. It has radically changed the concept and way of building and managing networked systems, and reduced the barriers to entry for new players in the service markets. It is considered to be a promising solution providing the scale and versatility necessary for IoT. However, SDN may also face many challenges, i.e., the centralized control plane would be a single point of failure. With the advent of blockchain technology, blockchain-based SDN has become an emerging architecture for securing a distributed network environment. Motivated by this, in this work, we summarize the generic framework of blockchain-based SDN, discuss security challenges and relevant solutions, and provide insights on the future development in this field.

key words: *software defined networking, blockchain technology, security challenges, attack and defence, Internet-of-Things*

1. Introduction

Due to the rapid development, computer networks are currently becoming more speedy, intelligent, resource-rich as well as complicated. For example, Internet-of-Things (IoT) has been gradually adopted by many organizations and business networks, the Gartner report made a prediction that there will be over 20 billion of connected devices worldwide by the end of 2020 [11]. The IoT architecture often contains a large amount of devices, servers and middleboxes, making the network management and configuration much difficult and error-prone, i.e., it is very laborious to add new devices and modify services as traditionally both control and data plane are integrated inside the network devices [38]. In addition, it is usually a difficult task to deploy new services without halting the ongoing services. This issue could become even worse with the increasing size of a network [17].

To address this issue, Software-Defined Networking (SDN) is a promising solution, which separates the network control from the data plane [33]. In such network, IT administrators can configure network policies from a software-based controller without the need of changing settings in each switch. In other words, the centralized SDN controller can direct the switches to deliver network services according to the requirements, regardless of the specific connections between a server and devices. This centralized control can help simplify network management and reduce the workload of configuration [38]. However, SDN is still confronted with many security challenges in practice, i.e., the SDN controller itself could become a single point of failure under adversarial scenarios [20], while distributed controllers may also face reliability and reputation issues [43].

Motivation. With the big success of Bitcoin cryptocurrency, blockchain technology has received tremendous attention from both academia and industry [49]. A blockchain holds a record of all data exchanges, in which the record is also known as 'ledger' and the data exchange is known as 'transaction'. It can use a peer-to-peer network to verify each new transaction, which can be added to the blockchain only after a successful verification. In this case, blockchain is believed to allow mutually unknown parties to exchange information or data without the need of a trusted third party [28]. Currently, some studies have tried to combine SDN with blockchain technology. For example, Sharma et al. [43] introduced DistBlockNet, a distributed model by integrating SDN and blockchains to improve the system performance and capability. Steichen et al. [46] presented a security mechanism named *ChainGuard*, which takes advantage of SDN functionalities to refine traffic and protect blockchain applications against flooding attacks from illegitimate sources.

Comparison and Contributions. In the literature, there are already many surveys on either SDN or blockchains. In the aspect of blockchain, Alsmadi and Xu [4] provided a survey to analyze the security issues in SDN, especially the robustness against several attacks like tampering, repudiation, data disclosure, etc. Meanwhile, Ahmad et al. [3] focused on the same topic and introduced some security threats that may compromise the control, application or data layer of SDN. For blockchain technology, Neudecker and Hartenstein [32] summarized several attacks on the permissionless blockchains, and discussed the demand for cost, anonymity and DoS resistance. Salman et al. [41] introduced some security issues on blockchains relating to confidentiality, authentication, privacy protection, data provenance, access control and so on. Some other recent reviews and surveys on either SDN or blockchains can be referred but not limited to [2], [5], [7], [9], [15], [22],

Manuscript received March 9, 2019.
Manuscript revised July 6, 2019.
Manuscript publicized November 8, 2019.

[†]The author is with the Department of Computer Science, City University of Hong Kong, Hong Kong SAR, China.
[††]The authors are with the Department of Applied Mathematics and Computer Science, Technical University of Denmark, Denmark.
[†††]The author is with the Department of Computer Science and Engineering, Shanghai Jiao Tong University, China.
[††††]The author is with the Department of Computing, The Hong Kong Polytechnic University, Hong Kong SAR, China.
a) E-mail: weme@dtu.dk (Corresponding author)

DOI: 10.1587/transinf.2019INI0002

Copyright © 2020 The Institute of Electronics, Information and Communication Engineers

[24], [34], [40].

The application of blockchain has been discussed in several domains like intrusion detection [28], Artificial Intelligence [39], IoT [25] and healthcare industry [35]. However, there are few surveys discussing the combination of SDN and blockchain technology. In this work, we try to complement this gap and review the existing security issues & solutions for blockchain-based SDN. In particular, we summarize the generic framework of blockchain-based SDN and discuss the recent research studies in this field. We also provide some insights on the development of blockchain-based SDN. Our work attempts to stimulate more research on designing a practical and secure blockchain-based SDN.

Organization. The remaining parts of this article are structured as follows. Section 2 introduces the basic information of both SDN and blockchain technology. Section 3 presents the generic framework of blockchain-based SDN and Sect. 4 discusses relevant security challenges and solutions. Section 5 describes some future directions and concludes our work.

2. Background on SDN and Blockchain Technology

In this part, we introduce the background on SDN like the basic architecture and major components, and describe how a blockchain works.

2.1 SDN

Software-Defined Networking (SDN) is an emerging networking architecture, in which the network control is independent of the data plane [33]. It can make the network directly programmable, more flexible and agile to support the virtualized server and storage in a modern data center. In a typical SDN environment, network management is logically centralized in a software-based controller, while network devices like switches can be considered as forwarding device, which can process traffic based on the defined flow tables [38]. These forwarding devices can be configured by the controller with the help of predefined standards.

In particular, OpenFlow (OF) is the first standardized communication protocol in an SDN environment between the control layer and the infrastructure layer. It enables the centralized controller handling switches without the need of disclosing any source code of their devices [20]. In other words, it allows network operators to directly access and modify both physical or virtual switches and routers. Figure 1 shows the three-layer architecture of SDN: the application layer, the control plane and the data plane.

- **The application layer.** This layer provides an open platform for various SDN applications and devices to leverage network recourses like topology and statistics. Different applications can communicate with each other as well as with the SDN controller via the northbound APIs. These applications can also offer end-to-end solutions for practical organizations.

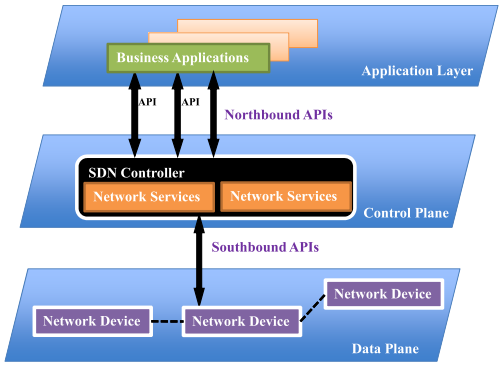


Fig. 1 The typical SDN architecture with three layers.

- **The control plane.** This layer is responsible for managing the whole network infrastructure via the centralized SDN controller, i.e., collecting network information, topology details, etc. It can configure the network devices in the data plane layer via the southbound APIs.
- **The data plane.** This layer contains many network equipment and devices that can help forward network traffic, e.g., network switches and routers. This also includes forwarding and processing of the data path.

The Northbound interface is defined as the connection between the controller and applications, whereas the Southbound interface is the connection between the controller and the physical networking hardware. Such SDN architecture is believed to provide many advantages and merits [4], [33].

- As the controllers are decoupled from the forwarding plane, the network control can become directly programmable.
- IT administrators or network operators can configure network traffic easily and dynamically according to different requirements.
- Network management is logically centralized in the SDN controllers with a global vision of the whole network environment.
- It helps simplify the process of design and operation in a network, as instructions are provided by the centralized controllers rather than various single devices or separate protocol.
- It can provide an open platform for various organizations to collaborate in many applications with the support of open APIs.

To summarize, SDN provides network administrators with the capability of writing programs via open APIs and configuring a network according to different requirements in an easy and flexible way.

2.2 Blockchain Technology

With the popularity of Bitcoin and other cryptocurrencies, blockchain technology has received much attention. It is an ingenious combination of multiple technologies

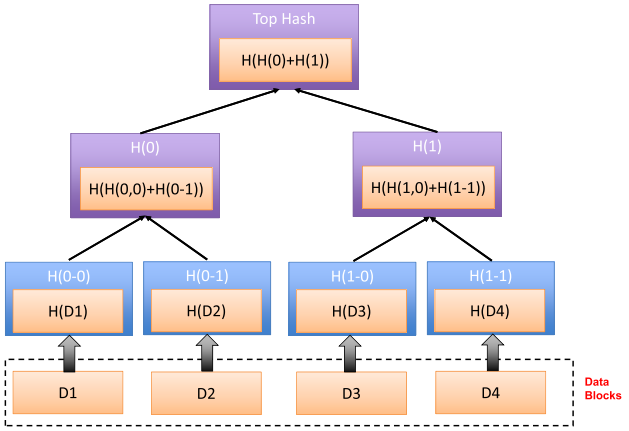


Fig. 2 Merkle tree of four hashes.

such as peer-to-peer network, consensus protocol over a distributed network, cryptographic schemes, distributed database, smart contract and game theory. It provides a decentralized way to build trust in social and economic activities, and thus holds a huge promise to change the future of financial transactions, and even the way of computation and collaboration.

For the block structure, the Merkle tree is a basis for the blockchain form and was used to create a 'secured chain of blocks' in around 1991. The chain is a series of data records, in which each of them connects to the foremost one [27]. The most recent (or newest) record in the chain would contain the history of the entire chain. Figure 2 presents an example structure of four hashes in a Merkle tree. The top hash serves as a combined representation of all data blocks before. This structure is very helpful to verify and manage records in a peer-to-peer network, ensuring that no modified or false data is transferred.

Then Satoshi Nakamato tuned the concept of distributed blockchain in 2008 [31]. It can include a secure chain of historical exchanged data by verifying each data exchange via a time-stamp in a peer-to-peer network. Thus, the data exchange can be handled without a central authority. More specifically, a blockchain saves a record of all data exchanges, where the record is known as 'ledger', and each data exchange is known as 'transaction'. Each verified transaction can be added to the ledger as a 'block'. In a real scenario, an entity should firstly obtain a pair of public and private key, in which the public key is used to represent the wallet address while the private key can help digitally sign and authorize different operations.

A consensus mechanism is applied in blockchain-based systems to make the necessary agreement on how to validate or add a data block. Some known consensus mechanisms are listed as follows.

- **Proof of Work (PoW).** This is the most widely known consensus mechanism that is being used by Bitcoin. In short, it secures the blockchain and creates a new block according to the level of computational power. Miners (or mining devices) have to compute the hash value of the next block containing both header data and transactions. The first miner that figures out the correct solution (target hash) can obtain reward with a block added. In Bitcoin cryptocurrenry, a new block is generated in every 10 minutes.
- **Proof of Stake (PoS).** This is a well-known alternative mechanism to PoW, which is featured with low cost and low energy consumption. It allocates the responsibility of refreshing the public ledger to a node in proportion to the number of virtual currency tokens. It means that more coins a node carries, the more possibilities it could be selected to maintain the ledger. This also means that the more participating nodes, the more decentralized the system becomes. As compared with PoW, one limitation of this mechanism is to encourage more on coin saving rather than spending.
- **Proof of Importance (PoI).** This mechanism is very similar to PoS, but can help prevent the issue of 'nothing at stake' through using an 'importance score', which can consider both the balance and the transaction frequency in deciding the final possibility of harvesting a new block. It thus can make a balance of saving and spending coins.
- **Proof of Capacity (PoC).** This mechanism enables miners (or mining devices) to mine and commit new blocks by taking advantage of free available hard-drive space. A list of potential solutions can be saved on minor's side to improve the mining possibility. In this case, the more solutions saved, the higher possibility of mining a new block. Rewards would be granted proportionally according to the free hard-drive space.
- **Proof of Elapsed Time (PoET).** This mechanism was introduced by the Intel, which tries to reach the distributed consensus without the need of consuming too much energy. In a peer-to-peer network, a number of participating nodes randomly create a value of waiting time, whereas only the node with the smallest value can have the chance to commit a new block. In each round, a new block is added, and it works similarly to PoW except that no mining activity occurs.

3. Framework of Blockchain-Based SDN

As described above, SDN can provide much global visibility and flexibility of network configuration by decoupling the network control from the data plane. However, SDN still suffers many limitations, i.e., the centralized controller may become a single point of failure [20], whereas distributed controllers might be vulnerable to insider attacks [29], [30]. As blockchain technology can encourage unknown entities to communicate with each other without a trusted third party, research community has already started investigating the performance of combining SDN with blockchains. Figure 3 depicts a generic framework of blockchain-based SDN by applying blockchains to the SDN architecture.

The SDN environment is similar to Fig. 1, but employs

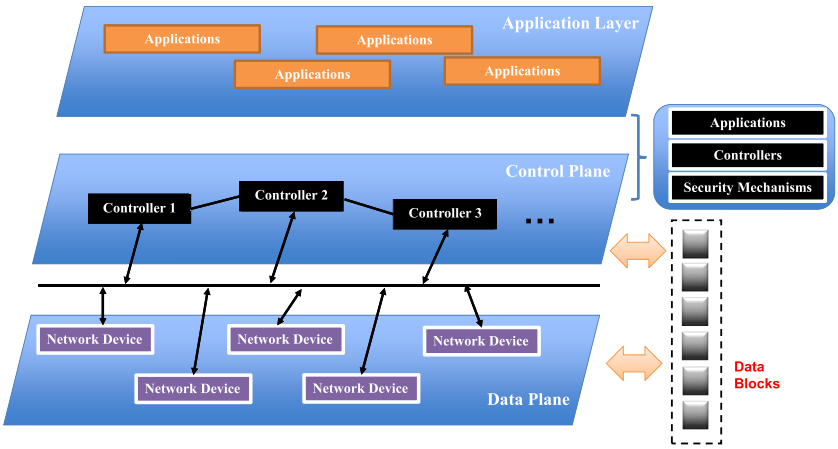


Fig. 3 The generic framework of blockchain-based SDN.

distributed controllers with the purpose of enhancing the robustness against the problem of single point of failure. Based on the requirements, the control plane and the application layer can be simplified as two large components (denote as application and controller component), where particular security mechanisms can be implemented to provide protection. Blockchain technology can be used to help enhance the security of distributed controllers and various forwarding devices in the data plane.

To implement the framework, it is very important to design the structure among applications, controller, security mechanisms and the relevant interactions. As an example, Sharma et al. [43] proposed DistBlockNet, a distributed IoT architecture that combines both SDN and blockchain technology. They particularly designed several security mechanisms like OrchApp and Shelter modules to defeat attacks.

- *OrchApp.* The purpose of this module is to provide programming characterized fortifications at the appropriate application layer, and ensure the adaptability to the new and dynamic network settings. Various security policies and threat intelligence can be deployed here, in relation to access control, data protection and many detection algorithms. For instance, it adopts a security convention model for access control among various devices in the IoT network. The threat intelligence monitors and examines both external and internal sources.
- *Shelter.* This module is used to protect the SDN environments against various attacks like insider attacks. It contains two major components: a flow control analyzer and a packet migration component. The former manages the main functionality of the network infrastructure including any malicious events, which can be deployed as a control application in the controller layer. The latter helps reduce the impact of malicious events. For example, during saturation attack [6], it can create new flow rules and migrate the missing table packet in the data cache. Therefore, it can protect the controller from being overloaded under adversarial scenarios like flooding attacks, by migrating all missing packets to the data cache when generating and updating the flow rules.

Referred to DistBlockNet [43], the generic framework of blockchain-based SDN can inherit many benefits from both SDN and blockchains, including adaptability, availability, reliability, scalability, and security.

- *Adaptability.* Thanks to the SDN characteristics, the generic framework is adaptive to the changing environment. This factor is vital to ensure the growth of the whole network with the increasing amount of underlying devices.
- *Availability.* The framework is able to provide high availability (with good fault tolerance), especially for the SDN controller under some adversarial scenarios. It allows the use of blockchain technology to safeguard the controller with mitigation mechanisms, i.e., *Shelter* can help protect the controller from being overloaded under attacks.
- *Reliability.* For a large-scale distributed network, the generic framework is able to reach linear performance with the deployment of appropriate mechanisms. It can make a balance between the expected performance and the achieved performance, under different environmental conditions.
- *Scalability.* This represents the capability of managing or accommodating a size-increasing network. Thanks to the SDN controllers, the generic framework is flexible and scalable when the network devices and services increase, i.e., reducing the cost of configuring network settings.
- *Security.* This is a very important factor for any type of network. By deploying appropriate security mechanisms and blockchain technology, the generic framework has the capability to secure the environment under attacks, in the aspects of confidentiality, integrity, and availability.

4. Security Challenges and Solutions

Though blockchain-based SDN can provide many benefits and advantages, it may still suffer various security issues and challenges. This could be caused by the limitations of either SDN itself or blockchain technology. In this part, we discuss some potential security challenges with relevant solutions.

4.1 Vulnerabilities and Attacks

By exploiting SDN vulnerabilities, attackers can try to compromise the network in the aspects of confidentiality, integrity and availability [3], [4], [20].

- *Scanning.* This is usually the first step that is utilized by cyber-criminals to understand the network status, such as network topology, host IP, server deployment, etc. Attackers can passively monitor all layers and their communication channels to collect the required information.
- *Spoofing attack.* Attackers can try to masquerade as either a legitimate external or an internal entity to gain unauthorized access to the SDN network. Based on the data obtained by scanning, they can impersonate as a device, a switch or even the controller through manipulating relevant data. Generally, there are two major types of spoofing attacks: Address Resolution Protocol (ARP) spoofing [23] and IP spoofing [8].
- *Hijacking attack.* With a successful attack, a hacker can control an element in the SDN environment. For example, if an intruder can successfully hijack the main controller, then the entire network could be under control. For example, Hong et al. [12] introduced a hijacking attack named *Host Location Hijacking*, which can hijack the location information of an identity in an OpenFlow controller. This attack has to first make a successful spoofing attack on the target.
- *DoS attack.* The major purpose of a denial-of-service attack is to render a network resource, SDN applications or any devices unavailable to the legitimate users. Shin and Gu [44] presented an early DoS attack, called *data plane resource consumption*, which is specific for SDN networks. Attackers first have to figure out whether a network employs OpenFlow switches, and then started generating manipulated flow requests from the data plane to the control plane. This can overload the data plane by delivering a large amount of useless rules.
- *MITM attack.* Man-in-the-middle attack allows an intruder to perform eavesdropping on the communication between two parties in the SDN network. For instance, Li et al. [19] introduced an MITM attack on OpenFlow channels, which allows hackers to collect data, rewrite flow tables, and poison the global view of controllers.

In addition to the above attacks, there are some other challenges in an SDN environment. For example, there is no trust management mechanism among distributed SDN controllers, which could be vulnerable to insider attacks [29]. On the other hand, as an emerging technology, blockchain also has many limitations that need to improve in practice, and itself could become an attractive target by cyber-criminals [22], [28].

- *Security issues.* As blockchain itself lacks of security by design, many traditional attacks are still feasible like DoS [46]. In addition, the shared ledger often has to be stored in a centralized place, which might be vulnerable as the single point of failure. Further, unauthorized access may become an issue, with the increase of participants and the complexity of trust management [50].
- *Privacy issues.* The challenges are mainly caused by that every transaction ever recorded on a public blockchain would be visible to anyone; however, such information could be sensitive in many domains like financial and medical sectors. Identity privacy could also be compromised if blockchain-based applications require the transaction to be associate with a known identity.
- *Latency issues.* In practice, a blockchain may need a period of time, or even several hours to complete the update of all ledgers. This may cause a delay and raise uncertainty for participating nodes. Attackers can utilize this to launch a DoS attack and compromise the availability.
- *Cost issues.* Taking Bitcoin as a concrete example, miners have to spend much computational power and energy if PoW is adopted as the consensus mechanism [42]. This would cause a big burden on the organizations or groups that have an interest in adopting blockchain technology.

Due to these issues and challenges, there is a great need to deploy appropriate security mechanisms to protect blockchain-based SDN against various threats. It is also a good option to choose private chain to increase the difficulty for attackers.

4.2 Defence and Solutions

To protect blockchain-based SDN in an adversarial environment, it is very important to deploy appropriate security mechanisms and enforce security policies.

- *Traffic and Flow control.* Firewalls and intrusion detection systems (IDSs) are two most commonly used mechanisms to control and refine traffic. For example, Suh et al. [45] introduced a firewall for an SDN controller, allowing IT staff to add new rules against malicious flows. Meng et al. [29] presented a collaborative IDS in a healthcare environment that can help fast detect insider attacks.
- *Policy enforcement.* To enforce security policies in an automatic way is a very important solution to secure SDN. Lara and Ramamurth [18] introduced an

OpenFlow-based framework named OpenSec, which helps maintain pre-defined security policies, i.e., guiding how it responds when malicious events are identified. Matias et al. [26] designed FlowNAC to authenticate participants and service-level access control according to the flow status.

- *DoS defend.* Such type of attack is indeed one of the most challenging threats for a centralized system. For protection, it is important to monitor and analyze the traffic by using the flexibility and programmability of SDN. As an example, Fichera et al. [10] introduced OPERETTA, a mechanism to defeat TCP SYNFLOOD attacks, through examining incoming TCP TYN packets and discarding untruthful connection requests.

The protection of blockchain-based SDN is not an easy task, it is vital to defeat unauthorized access, data leakage, data modification, DoS attack, malicious applications, as well as enhance configuration issues and many design issues. More promising solutions can refer to relevant studies and surveys [2], [5], [7], [9], [15], [22], [24], [34], [40], [48].

5. Future Trend and Conclusion

At this stage, the combination of SDN and blockchain faces many security challenges and issues, but they can complement each other in many practical scenarios, either by applying SDN to blockchain applications or applying blockchain to SDN applications.

- *The application of blockchain to SDN.* Blockchain can be an important factor for securing SDN- or IoT-related applications [47]. In the literature, Abbasi and Z.A. Khan [1] provided VeidBlock that could apply blockchain technique for SDN in order to validate identities against tampering attack. Sharma et al [43] introduced a scheme that utilized a blockchain to securely validate the flow rule table for IoT or SDN forwarding devices. Kataoka et al. [16] presented a method called Trust List, which could be used to establish the trust among various IoT and SDN devices, and prevent attacks & abuses by using both public and private blockchains. Qiu et al. [36] designed an approach of using a permissioned blockchain to help verify data flows and reach consensus in a distributed software defined vehicular network (SDVN).
- *The application of SDN to blockchains.* SDN has been studied as a solution to address many security issues in blockchain applications. For instance, Steichen et al. [46] identified that an attacker can halt the blockchain operation on particular nodes and proposed ChainGuard, a mechanism that could filter network traffic for blockchains. Houda et al. [14] introduced an SDN-based solution called ChainSecure, which could help defend blockchain nodes from DNS amplification attacks. Hou et al. [13] described how to use SDN to transfer flows in a more flexible way for consortium blockchains.

It is worth noting that we can also use replication techniques to avoid the issue of single point of failure, but it may cause the Byzantine Failure. Thus the use of blockchains can bring some more benefits like reasonable incentive models, smart contract operations, scalability and so on.

Overall, our work summarizes the generic framework of blockchain-based SDN, discusses potential security issues and relevant solutions. We figure out that the trend of combining SDN and blockchain seems positive and will continue. Thanks to many benefits like management flexibility, scalability and data flow verification, blockchain-based SDN can have a broad application in various domains like intrusion detection [21], [37], healthcare industry [30], [35], vehicular [36], etc. Meanwhile, we advocate that more future efforts could be made on exploring how to improve the security and performance of blockchain-based SDN.

Acknowledgments

This work was partially supported by H2020-SU-ICT-03-2018: CyberSec4Europe.

References

[1] A.G. Abbasi and Z. Khan, "VeidBlock: Verifiable Identity using Blockchain and Ledger in a Software Defined Network," Proc. UCC Companion, pp.173–179, 2017.
[2] A. Abdou, P.C. van Oorschot, and T. Wan, "Comparative Analysis of Control Plane Security of SDN and Conventional Networks," IEEE Communications Surveys and Tutorials, vol.20, no.4, pp.3542–3559, 2018.
[3] I. Ahmad, S. Namal, M. Ylianttila, and A. Gurtov, "Security in Software Defined Networks: A Survey," IEEE Communications Surveys and Tutorials, vol.17, no.4, pp.2317–2346, 2015.
[4] I. Alsmadi and D. Xu, "Security of Software Defined Networks: A Survey," Computers & Security, vol.53, pp.79–108, 2015.
[5] R. Alvizu, G. Maier, N. Kukreja, A. Pattavina, R. Morro, A. Capello, and C. Cavazzoni, "Comprehensive Survey on T-SDN: Software-Defined Networking for Transport Networks," IEEE Communications Surveys and Tutorials, vol.19, no.4, pp.2232–2283, 2017.
[6] M. Ambrosin, M. Conti, F. De Gaspari, and R. Poovendran, "LineSwitch: Tackling Control Plane Saturation Attacks in Software-Defined Networking," IEEE/ACM Trans. Netw., vol.25, no.2, pp.1206–1219, 2017.
[7] F. Bannour, S. Souihi, and A. Mellouk, "Distributed SDN Control: Survey, Taxonomy, and Challenges," IEEE Communications Surveys and Tutorials, vol.20, no.1, pp.333–354, 2018.
[8] K. Benton, L.J. Camp, T. Kelley, and M. Swany, "Filtering IP source spoofing using feasible path reverse path forwarding with SDN," Proc. IEEE Conference on Communications and Network Security (CNS), pp.733–734, 2015.
[9] I. Farris, T. Taleb, Y. Khettab, and J. Song, "A Survey on Emerging SDN and NFV Security Mechanisms for IoT Systems," IEEE Communications Surveys and Tutorials, vol.21, no.1, pp.812–837, 2019.
[10] S. Fichera, L. Galluccio, S.C. Grancagnolo, G. Morabito, and S. Palazzo, "OPERETTA: An OPEnflow-based REmedy to mitigate TCP SYNFLOOD Attacks against web servers," Computer Networks, vol.92, pp.89–100, 2015.
[11] Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016 (access on 20 Feb. 2019)

https://www.gartner.com/newsroom/id/3598917

[12] S. Hong, L. Xu, H. Wang, and G. Gu, "Poisoning Network Visibility in Software-Defined Networks: New Attacks and Countermeasures," Proceedings of NDSS, San Diego, USA, 2015.

[13] W. Hou, Z. Ning, L. Guo, and P. Guo, "SDN-based Optimizing Solutions for Multipath Data Transmission Supporting Consortium Blockchains," Proc. CITS, pp.1–5, 2018.

[14] Z.A.E. Houda, L. Khoukhi, and A. Hafid, "ChainSecure - A Scalable and Proactive Solution for Protecting Blockchain Applications Using SDN," Proc. GLOBECOM, pp.1–6, 2018.

[15] M. Karakus and A. Durresi, "A survey: Control plane scalability issues and approaches in Software-Defined Networking (SDN)," Computer Networks, vol.112, pp.279–293, 2017.

[16] K. Kataoka, S. Gangwar, and P. Podili, "Trust list: Internet-wide and distributed IoT traffic management using blockchain and SDN," Proc. WF-IoT, pp.296–301, 2018.

[17] H. Kim, T. Benson, A. Akella, and N. Feamster, "The evolution of network configuration: a tale of two campuses," Proc. 2011 ACM Conference on Internet Measurement Conference, pp.499–514, 2011.

[18] A. Lara and B. Ramamurthy, "OpenSec: A Framework for Implementing Security Policies using OpenFlow," Proc. GLOBECOM, pp.781–786, 2014.

[19] C. Li, Z. Qin, E. Novak, and Q. Li, "Securing SDN Infrastructure of IoT-Fog Networks From MitM Attacks," IEEE Internet of Things Journal, vol.4, no.5, pp.1156–1164, 2017.

[20] W. Li, W. Meng, and L.F. Kwok, "A Survey on OpenFlow-based Software Defined Networks: Security Challenges and Countermeasures," Journal of Network and Computer Applications, vol.68, pp.126–139, Elsevier, 2016.

[21] W. Li, S. Tug, W. Meng, and Y. Wang, "Designing Collaborative Blockchained Signature-based Intrusion Detection in IoT environments," Future Generation Computer Systems, In Press, Elsevier, vol.96, pp.481–489, 2019.

[22] I.-C. Lin and T.-C. Liao, "A survey of blockchain security issues and challenges," International Journal of Network Security, vol.19, no.5, pp.653–659, 2017.

[23] B. Liu, J. Bi, and Y. Zhou, "Source Address Validation in Software Defined Networks," Proceedings of the ACM SIGCOMM, pp.595–596, 2016.

[24] F.A. Lopes, M. Santos, R. Fidalgo, and S. Fernandes, "A Software Engineering Perspective on SDN Programmability," IEEE Communications Surveys and Tutorials, vol.18, no.2, pp.1255–1272, 2016.

[25] I. Makhdoom, M. Abolhasan, H. Abbas, and W. Ni, "Blockchain's adoption in IoT: The challenges, and a way forward," Journal of Network and Computer Applications, vol.125, pp.251–279, 2019.

[26] J. Matias, J. Garay, A. Mendiola, N. Toledo, and E. Jacob, "FlowNAC: Flow-based network access control," Proc. EWSDN, pp.79–84, 2014.

[27] R.C. Merkle, "Protocols for public key cryptosystems," Proc. 1980 IEEE Symposium on Security and Privacy, pp.122–134, 1980.

[28] W. Meng, E.W. Tischhauser, Q. Wang, Y. Wang, and J. Han, "When Intrusion Detection Meets Blockchain Technology: A Review," IEEE Access, vol.6, no.1, pp.10179–10188, IEEE, 2018.

[29] W. Meng, K.-K.R. Choo, S. Furnell, A.V. Vasilakos, and C.W. Probst, "Towards Bayesian-based Trust Management for Insider Attacks in Healthcare Software-Defined Networks," IEEE Transactions on Network and Service Management, vol.15, no.2, pp.761–773, IEEE, 2018.

[30] W. Meng, W. Li, Y. Wang, and M.H. Au, "Detecting Insider Attacks in Medical Cyber-Physical Networks based on Behavioral Profiling," Future Generation Computer Systems, In Press, Elsevier 2018.

[31] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," http://bitcoin.org/bitcoin.pdf, 2008.

[32] T. Neudecker and H. Hartenstein, "Network Layer Aspects of Permissionless Blockchains," IEEE Communications Surveys and Tutorials, vol.21, no.1, pp.838–857, 2019.

[33] "Software-defined networking: The new norm for networks," Open Networking Foundation, SDN Security Considerations in the Data Center, Techical report, 2012 (access on 20 Feb. 2019) https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf

[34] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and IoT Integration: A Systematic Survey," Sensors, vol.18, no.8, pp.1–37, 2018.

[35] C. Pirtle and J. Ehrenfeld, "Blockchain for Healthcare: The Next Generation of Medical Records?," Journal of Medical Systems, vol.42, no.9, pp.172:1–172:3, 2018.

[36] C. Qiu, F.R. Yu, F. Xu, H. Yao, and C. Zhao, "Blockchain-Based Distributed Software-Defined Vehicular Networks via Deep Q-Learning," Proc. DIVANet, pp.8–14, 2018.

[37] G. Sagirlar, B. Carminati, E. Ferrari, "AutoBotCatcher: Blockchain-Based P2P Botnet Detection for the Internet of Things," Proc. CIC, pp.1–8, 2018.

[38] R. Sahay, W. Meng, and C.D. Jensen, "The Application of Software Defined Networking on Securing Computer Networks: A Survey," Journal of Network and Computer Applications, vol.131, pp.89–108, 2019.

[39] K. Salah, M.H.U. Rehman, N. Nizamuddin, and A.I. Al-Fuqaha, "Blockchain for AI: Review and Open Research Challenges," IEEE Access, vol.7, pp.10127–10149, 2019.

[40] O. Salman, I. Elhajj, A. Chehab, and A.I. Kayssi, "IoT survey: An SDN and fog computing perspective," Computer Networks, vol.143, pp.221–246, 2018.

[41] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security Services Using Blockchains: A State of the Art Survey," IEEE Communications Surveys and Tutorials, vol.21, no.1, pp.858–880, 2019.

[42] S. Sankaran, S. Sanju, and K. Achuthan, "Towards Realistic Energy Profiling of Blockchains for Securing Internet of Things," Proc. ICDCS, pp.1454–1459, 2018.

[43] 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.

[44] S. Shin and G. GU, "Attacking Software-Defined Networks: A First Feasibility Study," Proc. 2nd Workshop on Hot topics in Software Defined Networks (HotSDN), Hong Kong, China, pp.165–166, 2013.

[45] M. Suh, S.H. Park, B. Lee, and S. Yang, "Building firewall over the software-defined network controller," Proc. ICACT, pp.1–5, 2014.

[46] M. Steichen, S. Hommes, and R. State, "ChainGuard — A firewall for blockchain applications using SDN with OpenFlow," Proc. IPTComm, pp.1–8, 2017.

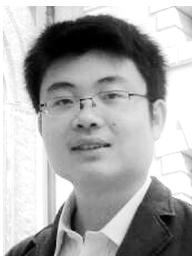
[47] C. Tselios, I. Politis, and S. Kotsopoulos, "Enhancing SDN security for IoT-related deployments through blockchain," Proc. NFV-SDN, pp.303–308, 2017.

[48] J. Xie, F.R. Yu, T. Huang, R. Xie, J. Liu, C. Wang, and Y. Liu, "A Survey of Machine Learning Techniques Applied to Software Defined Networking (SDN): Research Issues and Challenges," IEEE Communications Surveys and Tutorials, vol.21, no.1, pp.393–430, 2019.

[49] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where Is Current Research on Blockchain Technology?—A Systematic Review," PLoS ONE, vol.11, no.10, pp.1–27, 2016.

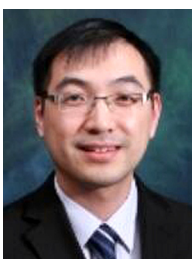
[50] Y. Yu, Y. Li, J. Tian, and J. Liu, "Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things," IEEE Wireless Communications, vol.25, no.6, pp.12–18, 2018.

Wenjuan Li is currently a Ph.D. student in the Department of Computer Science, City University of Hong Kong (CityU), and is holding an exchanged role at Technical University of Denmark (DTU), Denmark. Prior to this, she worked as a Research Assistant in CityU from 2013 to 2014, and was previously a Lecturer in the Department of Computer Science, Zhaoqing Foreign Language College, China. She was a Winner of Cyber Quiz and Computer Security Competition, Final Round of Kaspersky Lab "Cyber Security for the Next Generation" Conference in 2014. Her research interests include network management and security, collaborative intrusion detection, spam detection, trust computing, web technology and E-commerce technology.



Weizhi Meng is currently an assistant professor in the Cyber Security Section, Technical University of Denmark (DTU), Denmark. He obtained his Ph.D. degree in Computer Science from the City University of Hong Kong (CityU), Hong Kong. Prior to joining DTU, he worked as a research scientist in Infocomm Security (ICS) Department, Institute for Infocomm Research, A*Star, Singapore, and as a senior research associate in CS Department, CityU. He won the Outstanding Academic Performance Award during his doctoral study, and is a recipient of the Hong Kong Institution of Engineers (HKIE) Outstanding Paper Award for Young Engineers/Researchers in both 2014 and 2017. His primary research interests are cyber security and intelligent technology in security, including intrusion detection, smartphone security, biometric authentication, HCI security, trust computing, blockchain in security, and malware analysis.

Zhiqiang Liu is currently an Associate Professor in Department of Computer Science and Engineering, Shanghai Jiao Tong University, China. He received the Ph.D. degree in Computer Science from Shanghai Jiao Tong University (2012.01). He had about 7-year working experience (2001.03–2008.07) in several companies such as ZTE, Alcatel Shanghai Bell, and so on. He did post-doc program in Shanghai Jiao Tong University (2012.02–2015.04) as well as in KU Leuven, Belgium (2013.09–2014.09). His research interests focus on symmetric-key cryptography, cryptocurrency and blockchain.



Man-Ho Au is an associate professor at the Department of Computing, the Hong Kong Polytechnic University. His research interests include information security, applied cryptography, accountable anonymity and blockchain. Before joining PolyU in July 2014, he was a lecturer with the School of Computer Science and Software Engineering, University of Wollongong, Australia. His papers appeared at major conferences, including ACM CCS, NDSS and ACM SIGMOD. Currently, he is serving as a committee member of the ISO/IEC JTC 1/SC 27 working group 2 - Cryptography and security mechanisms. He is also a committee member of the Hong Kong Blockchain Society R&D division.