Trust-Enhanced Content Delivery in Blockchain-Based Information-Centric Networking

Huining Li, Kun Wang, Toshiaki Miyazaki, Chenhan Xu, Song Guo, and Yanfei Sun

Abstract

With the fast-growing demands for efficient and scalable content distribution, information-centric networking (ICN) can be a promising candidate for future networks. ICN promises direct retrieval of the content using its unique, persistent, and location-independent name. In ICN, all nodes work together to scale up content delivery, but security issues caused by malicious behaviors of ICN nodes cannot be avoided. To this end, in this article we develop a trust-enhanced blockchain based ICN (BICN) architecture for content delivery. In our proposed architecture, the whole process of content delivery is first traced in an implicitly trusted way by exploiting the excellent properties of the blockchain, so that the malicious ICN nodes can be located. Second, we leverage transactions to record the mapping between human-readable name and self-certifying name in BICN, which supports convenient and trusted alteration for users' requirements. Moreover, we present a case study in BICN based smart grid for energy data delivery, where we perform security analysis and conduct experiments. Numerical results show the superior performance of our proposal. Finally, we present open issues for future work.

Introduction

Recently, the Cisco Visual Networking Index has predicted that annual global Internet Protocol (IP) traffic will increase approximately threefold by 2021, up from 1.2 Zettabyte (ZB) in 2016 [1]. For adapting to future traffic trends, it is of great significance to redesign a new Internet architecture. Consequently, information-centric networking (ICN) emerges, inspired by the increasing demand for content distribution and retrieval [2, 3]. Compared with the traditional host-centric communication paradigm, where all the content requests are realized by accessing the host based on its IP address, ICN focuses on decoupling named content objects from the hosts. Specifically, the named content is regarded as the first-class citizen in ICN and is independent of its location [4, 5].

The whole process of content delivery in ICN is shown in Fig. 1. A publisher first sends a *register message* with the object's name to the local name resolution executor (NRE), and this *register message* will be sent to another parent or peering NRE afterward. Then, a subscriber who requires a specific object's content will send a *discover message* to its local NRE and propagate this discover message to the parent NRE, until the matching *register message* of this content is discovered. After that, the *discover message* follows the reverse direction of the *register message* until it reaches an appropriate publisher. Finally, the desired content is forwarded to the subscriber by content routers (CRs) along a regular IP address or reverse direction of *discover message*'s path. Unfortunately, some threats may inevitably happen in ICN for content delivery, which are illustrated as follows:

- A *register message, discover message*, or data are possibly tampered with, and then the tampered information is delivered to other ICN nodes.
- One malicious ICN node can refuse to forward any message or data to other ICN nodes.
- A *register message, discover message*, or data may be overheard and broadcast by malicious ICN node.

To tackle these malicious behaviors, we study possible solutions in ICN. Using a self-certifying naming scheme in content delivery can verify the provenance of data and protect data integrity, because this form of self-certifying name realizes name-publisher and name-content bindings via a cryptographic hash function [6]. Thus, the first malicious behavior, that is, tampering, can be discovered using a self-certifying naming scheme, but who is responsible for this is unknown. The second and third malicious behaviors can be located by tracing ICN nodes in the whole process of content delivery.

Although these two solutions provide a promising prospect, there still exist some challenges. On the one hand, self-certifying names are difficult to understand and cannot aggregate routing information for the system's scalability. On the other hand, although the tracing mechanism records the behaviors of ICN nodes, malicious ICN nodes still have the possibility to deny their malicious behaviors and even claim that the tracing mechanism fails, because the tracing mechanism is not implicitly trustworthy.

To this end, we develop a trusted blockchain based ICN (BICN) architecture for content delivery. Specifically, the blockchain is a public append-only ledger carrying all transactions that have been executed [7], where transactions record the behaviors of ICN nodes. For one thing, every block carrying the record of ICN node

Huining Li and Yanfei Sun (corresponding author) are with Nanjing University of Posts and Telecommunications and Jiangsu Engineering Research Center of HPC and Intelligent Processing; Chenhan Xu is with Nanjing University of Posts and Telecommunications; Kun Wang is with the University of California Los Angeles; Toshiaki Miyazaki is with The University of Aizu; Song Guo is with The Hong Kong Polytechnic University.

Digital Object Identifier:
10.1109/MNET.2019.1800299

0890-8044/19/$25.00 © 2019 IEEE

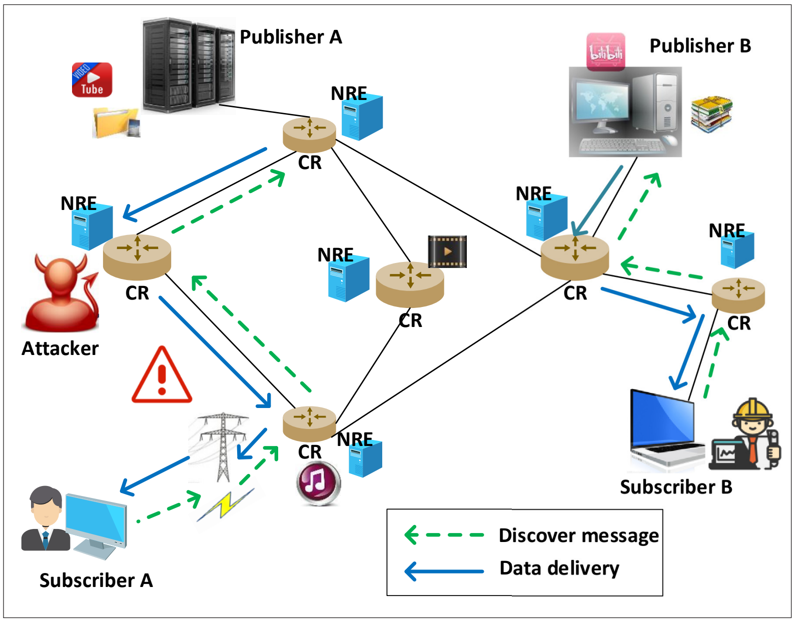

FIGURE 1. Content delivery in ICN.

behaviors is committed to the global blockchain where every logical blockchain host (LBH) will have a copy, and thus, every ICN node cannot deny the behaviors that have been recorded. For another, the blockchain can achieve global consensus on the whole sequence of records so that a conflicting record will be dropped once it is committed. Thus, these non-repudiation and non-tamping properties of the blockchain guarantee trusted content delivery in ICN. Our contributions are summarized as follows:

- We propose a trust-enhanced blockchain based tracing mechanism for the whole content delivery process in ICN. This mechanism can feed the records of behaviors on ICN nodes to the blockchain faithfully, which is the key to guaranteeing the tracing of the malicious ones.
- We design a trust-enhanced mapping between a human-readable name and a self-certifying name in the blockchain. Thus, these two forms of name can conveniently alternate with each other to satisfy different demands of publishers, subscribers, and ICN nodes.

The rest of the article is organized as follows. The following section gives an overview of security issues in ICN. The blockchain based ICN architecture and technical details for content delivery are then shown. A case study is then presented. We then discuss the open issues. Finally, we conclude this article.

Security Issues in Information-Centric Networking

Potential security issues in ICN are illustrated as follows.

Denial of Service (DoS) Attack: Different from traditional DoS attacks, the DoS attacks in ICN abuse the stateful forwarding plane, targeting either the intermediate CRs, NREs, or the content publishers [8]. Specifically, DoS attacks overwhelm the services in ICN via massive amounts of requests, such as interest flooding. As for interest flooding, attackers deliver interests for multiple content objects which may not exist in the caches of targeted CRs or NREs. On the one hand, the fake content object whose name has a valid prefix and an invalid suffix, can force the content publisher to drop the interest. On the other hand, dynamic content requests are always served by the content publisher, but these requests will overload the CRs for forwarding, and they cannot be aggregated, which can finally result in DoS attacks to the publisher.

Jamming: When an adversary masquerades as a legitimate subscriber to deliver an unnecessary or malicious content request, the publisher will reply, but the content will be sent to the destination with no receiver in ICN.

Hijacking: A malicious ICN node can declare invalid paths for any content as a publisher. Under this circumstance, content requests near the malicious node will not be replied because they have been direct toward the declared invalid paths in ICN.

Cache Pollution: Caching is independent of applications, which can be applied to content owners for accelerating the rate of data retrieval and promoting the availability of data [9]. In ICN, more popular content can be cached to decrease request latency and network load. An adversary can frequently request less popular content to destroy the popularity-based caching in ICN.

Design and Implementation of Blockchain-Based ICN

In this section, we first present the design of a blockchain based ICN architecture to tackle malicious attacks, and then the technique details about blockchain implementation are discussed.

Blockchain Based ICN Architecture

BICN consists of subscribers, publishers, NREs, CRs, and LBHs, as shown in Fig. 2. They all work together to maintain a trust-enhanced BICN architecture, which has the features of trusted name mapping and traceable content delivery. Generally, Youtube, Spotify, Instagram, Facebook, and so on can all act as the publishers in practice. Based on our group's previous work in reducing the storage resources occupied by the blockchain [10, 11], the proposed BICN system is embedded with a novel transaction offloading module, which will lead to more resources left for content transmission or other operations. In this way, the delay in content transmission can be decreased and our proposed system can support real-time content delivery for those providers.

For content delivery, on the one hand, the publisher who intends to deliver its content to the subscriber should first generate a pair of names, that is, a hierarchical name $\mathcal{H}$ (human-readable) and a flat name $\mathcal{F}$ (support self-certifying but not human-readable) for the content. Then, the $\mathcal{H}$:$\mathcal{F}$ pair must be uploaded to the blockchain as a transaction. After the pair is recorded by the blockchain, the NRE will be open to the publisher for registration. The *register message* is able to carry either $\mathcal{H}$ or $\mathcal{F}$, depending on the demands of the publisher's region. As Fig. 2 shows, the publisher sends the *register message* to a local NRE (arrow 1), and the NRE propagates the message to its parent NRE until the root NRE receives (arrow 2).

On the other hand, the subscriber usually obtains the name, which can be either hierarchical or flat. To fetch the content, the subscriber sends a *discover message* with the content name (arrow 3), and the message is also propagated (arrow 4). Even if the subscriber uses a hierarchical name, the self-certification is capable of being performed via the corresponding flat name recorded in the blockchain. Once the *discover message* matches a registration, it will follow the reverse path of the *register message* to reach the publisher (arrows 5–6). Every time the *discover message* goes through an NRE, the corresponding CR will be informed of the way back to the subscriber (arrows 3a, 4a, and 5a). Thus, the content is finally delivered from the publisher to the subscriber (arrows 7-10). Note that message transmission, propagation, and data delivery should be uploaded to the blockchain for traceability. In the next subsection, we will discuss the technical details of BICN.

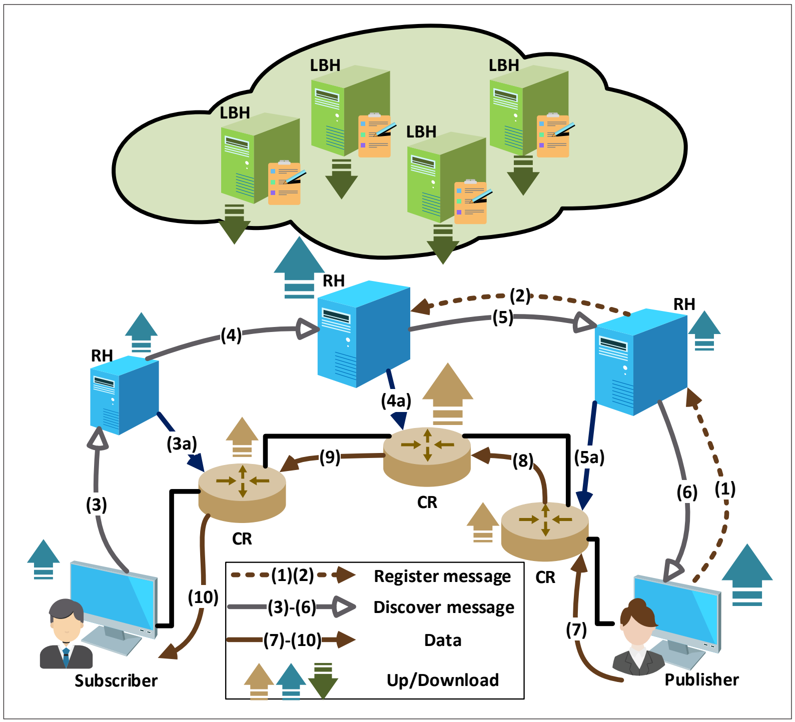

FIGURE 2. The architecture of blockchain based ICN for content delivery.

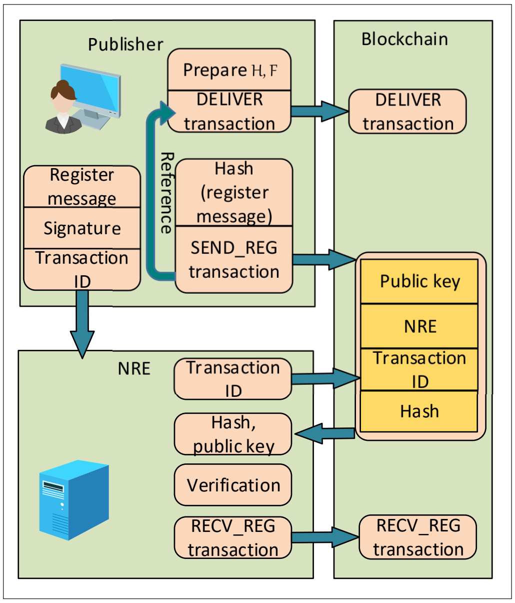

FIGURE 3. The process of sending a register message in BICN.

Blockchain Implementation

The data structure of the blockchain is maintained by all participants, which is non-tampering and undeniable. It was proposed by S. Nakamoto to run Bitcoin on the trustless Internet [12, 13]. Blocks are naturally generated in chronological order, and every block carries some transactions, which record the asset transferring. Mainstream organizations and enterprise markets have formally approved blockchain technology. The blockchain network is always maintained by a community, which is supported by technical committees, management boards, and the Linux Foundation. The trust mechanism in our proposed BICN is illustrated as follows.

Hybrid Naming: The design of the name in BICN is hybrid. To obtain the hybrid name, the publisher is required to prepare both a hierarchical and a flat name of the content to be delivered. After the preparation, the publisher is expected to construct a transaction using a pair of hierarchical name and flat name, that is, $\mathcal{H}$:$\mathcal{F}$, where $\mathcal{F}$ consists of the public key $\mathcal{P}$ of the publisher and the hash value $\mathcal{L}$ of content. Since a transaction itself contains the public key of its constructor, the publisher writes $\mathcal{H}$ and $\mathcal{L}$ in the **DELIVER** transaction. Finally, the transaction is uploaded to the blockchain, and the publisher can begin the registration later.

Trust Name Resolution and Data Routing: In order to register content, sending a *register message* is required. As Fig. 3 shows, the registration begins with a **SEND_REG** transaction, which contains the hash of the *register message*. It indicates that the publisher is going to send the message. The **SEND_REG** transaction should reference the previous delivering transaction to illustrate that the name of the content is valid. Moreover, the **SEND_REG** transaction should also mark the local NRE as a receiver. Uploading of the **SEND_REG** transaction is followed by sending the *register message* together with its signature from the publisher and the transaction ID of the previous uploaded **SEND_REG** transaction to a local NRE. Once the local NRE receives a *register message*, it stores the message in the buffer, and verifies that the referenced **SEND_REG** transaction:

a)is stored in the blockchain;

b) contains the same hash of the received message;

c)carries the public key that can validate the signature right.

If a), b), and c) are validated by this local NRE, it will upload a **RECV_REG** transaction and prepare for the next propagation.

Concluded from the above process of sending the *register message*, behaviors of nodes in BICN need to follow four procedures.

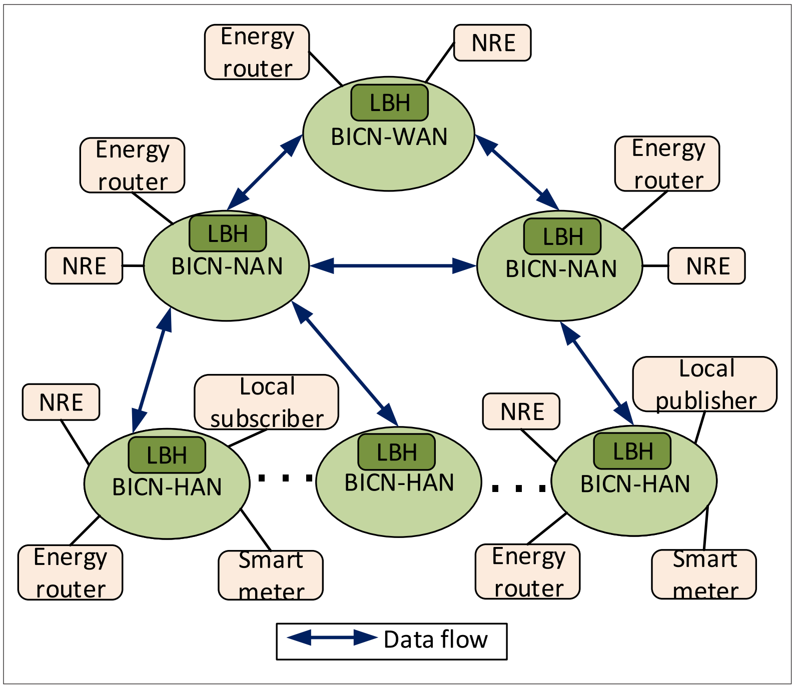

FIGURE 4. The BICN-SG platform for energy data delivery.

P1: The sender should upload a transaction (with prefix SEND, for example, SEND REG) that asserts they are going to send a payload to the receiver, and get a transaction ID from the LBH as a return. Specifically, for the register, discover, and content transmitting processes, the payloads are *register message*, *discover message*, and data of content, respectively. We stipulate that the receiver should be in the *Output* field of the transaction, and the transaction should carry the hash of the payload. Also, similar to general transactions in other blockchain applications, this transaction is required to reference a previous one, which is able to grant the validation of the transaction.

P2: The sender sends the payload to the receiver. In this procedure, the signature of the payload from the sender is sent together with the payload. Moreover, the transaction ID that was described in **P1** is attached as the extra data of the payload.

P3: The receiver receives the payload. The receiver stores the payload, transaction ID, and signature sent by the sender in a staging area (buffer). Then it looks up the received transaction ID in the blockchain immediately. If the transaction exists, the receiver will retrieve the public key and the hash value stored in it.

P4: The receiver uses the retrieved public key to decrypt the received signature, and the result is denoted with $hash_\alpha$. Also, we use $hash_\beta$ to represent the retrieved hash value stored in the referenced transaction. Then, the receiver must verify if $hash(payload) = hash_\alpha = hash_\beta$ is correct or not. If it is true, a transaction (with prefix **recv**) should be uploaded to assert that the payload is validated and received.

The other parts of the name resolution and data routing also use **P1-P4** to guarantee trust. The NRE propagates the *register message* to the parent NRE region by region. When a subscriber intends to fetch content, a *discover message* is required. Similar to the *register message*, the *discover message* follows the **FETCH** transaction. The difference is that a **FETCH** transaction does not contain a pair of names. Note that when the *discover message* reaches the publisher, the publisher will use **SEND_DATA** transaction to start data sending. This transaction directly references the **RECV_DCV** transaction which is uploaded by the publisher when he receives a *discover message*. In this way, the subscriber can trace the entire process from sending the *discover message* to receiving data.

Case Study: Secure BICN based Smart Grid for Energy Data Delivery

For security requirements, our proposed BICN architecture can support many IoT applications that are information-centric in nature, including smart grid [14, 15], smart transport, smart home, smart healthcare, and so on. In this section, we mainly study BICN based smart grid (BICN-SG).

BICN-SG Platform

We deploy blockchain in ICN-SG, where transactions record the hashes of energy data to be requested, the public keys of senders and receivers, and the signatures of senders. Our proposed blockchain based ICN-SG (BICN-SG) platform is divided into three layers, including the BICN based home area network (BICN-HAN), BICN based neighborhood area network (BICN-NAN), and BICN based wide area network (BICN-WAN), as shown in Fig. 4. In our proposed platform, subscribers and publishers are set in local BICN-HAN. Additionally, operations of name resolution and energy data delivery often start from a local BICN-HAN, and extend to BICN-NAN and BICN-WAN.

Specifically, we take an example of the whole transmission process of electricity price content in BICN-SG. The publisher of electricity price content, for example, the grid operator, should first generate a pair of hierarchical name and flat name, where the hierarchical name is human-readable and can be written such as */grid/<city>/<year>/<date>/<hourly>. json*, and the flat name is not human-readable, often written as *P:L*. Second, the mapping between the hierarchical name and the flat name of electricity price content is uploaded to the blockchain as a transaction. Then, the grid operator starts to send *register message* carrying a flat name of electricity price to a local NRE, and propagates to the parent NREs until the root NRE meets. Additionally, the *register message* is recorded in the transaction of the blockchain as well. After that, a commercial user in the BICN-HAN who intends to subscribe the electricity price content, sends a *discover message* carrying a hierarchical name via smart meters to a local NRE and propagates to other parent NREs in the BICN-SG. Once the matching *register message* is found, the *discover message* will follow the reverse path of the matching one to reach the grid operator. Note that the human-readable property of a hierarchical name makes it easier and more friendly for human users to participate in the BICN-SG system. When the *discover message* carrying the hierarchical name is transmitted to the WAN with no local human users, the hierarchical name can be changed into the flat name in the blockchain,

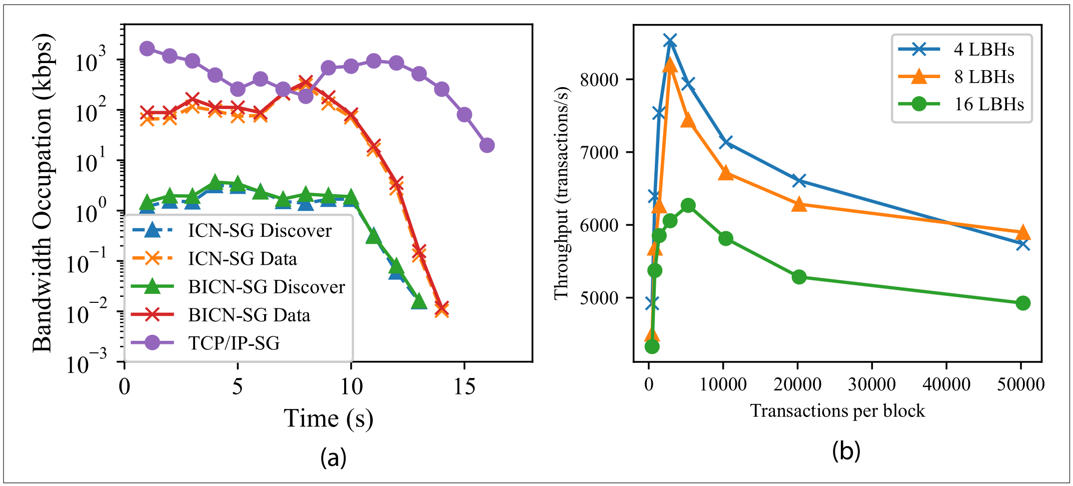

FIGURE 5. Bandwidth and throughput: a) Comparison of bandwidth occupation in BICN-SG, ICN-SG, and TCP/IP-SG; b) Comparison of blockchain's throughput under 4, 8, 16 LBHs in BICN-SG.

supporting self-certifying. Finally, the electricity price content is forwarded to smart meters on the commercial user side by energy routers along the reverse direction of the *discover message*'s path. Moreover, the whole process of name resolution and date routing of the electricity price is recorded as multiple transactions in the blockchain. This means that every LBH has a copy and no node can deny or tamper its past behavior in the BICN-SG system. By exploiting the non-reputation and non-tamping characteristics of the blockchain, we can enable an implicitly trusted tracing mechanism in the BICN-SG. How to analyze the records of nodes' behaviors and locate the malicious ones is illustrated in the next subsection.

Security Analysis

This subsection gives a security analysis of how the introduced blockchain helps to address the security issues that ICN-SG faces.

First, the blockchain prevents malicious tampering. The tampering is located and marked as a *conflict* in BICN-SG, and it consists of two cases. For one thing, a malicious smart meter sends tampered energy data to a normal one. In this case, the $hash(payload) = hash_\alpha = hash_\beta$ is not satisfied. For another, a malicious smart meter tampers the data from a normal one, where $hash(payload) = hash_\alpha = hash_\beta$ is satisfied. However, the malicious smart meter cheats LBHs that it receives tampered energy data in procedure **P4**. In the above cases, the blockchain can locate the malicious and normal meters as a pair of *conflicts*. The pair of *conflicts* can be solved by the enabled mechanism of the BICN-SG architecture.

Second, DoS attacks can be easily traced by analyzing the blockchain. In ICN-SG, malicious smart meters can launch DoS attacks, as aforementioned, by constructing *discover messages* with an efficient prefix and inefficient suffix. However, this *discover message*'s pending interest table entry will not be removed until a long expiration time. By exploiting the blockchain, tracing back to the attackers is allowed. When the sizes suddenly increase, CRs and NREs can sort the pending interest table entries in chronological order. Then, the malicious smart meter can be located by recursively checking the input field of transactions that correspond with the pending interest table entries.

Third, the blockchain also traces cache pollution. Different from DoS attacks, a malicious smart meter constructs a large number of *discover messages* of valid content, but the content is unpopular. In BICN-SG, the hashes of the *discover message* are recorded in the blockchain. Hence, the hash of unpopular content rarely appears in the blockchain. Any abnormal frequency changes of content hashes can be sensed by the BICN-SG. Thus, cache pollution makes no sense.

In addition, jamming attacks and hijacking attacks can be prevented. When an adversary masquerades as a legitimate subscriber to deliver an unnecessary or malicious content request, it first needs to send a *discover message* to its local RH and propagate this *discover message* to the parent RH. When the local RH and parent RH receive the *discover message*, they both need to upload this discover message and the address of the subscriber to the blockchain. After that, the blockchain will verify the legitimacy of the address and the *discover message*. If it is not legal, this unnecessary or malicious content request will be canceled. In this way, jamming attacks can be prevented. As for the hijacking attack, the proposed BICN system can help locate the malicious ICN node. Specifically, when a malicious ICN node declares invalid paths for any content as a publisher, our proposed system can help to dig out the *register message* recorded in the blockchain. Then, the malicious ICN node as a publisher can be traced according to the propagation path of the register message.

Experiments

To illustrate the feasibility of BICN-SG, we conduct several experiments. Our experiment platform is based on Python 3.6, where the hash operation is performed by the hashlib.sha256() library. We multiplex the I/O by select() system call, and the storage of the blockchain is implemented by SQLite. 500 smart meters are placed in BICN-SG, ICN-SG, TCP/IPSG, respectively. The blockchain network consists of LBHs, each of which has an Intel Core i7 3770K CPU, 8 GB RAM. Additionally, the ICN content chunk size and TCP maximum segment size are both set to 1000 Bytes.

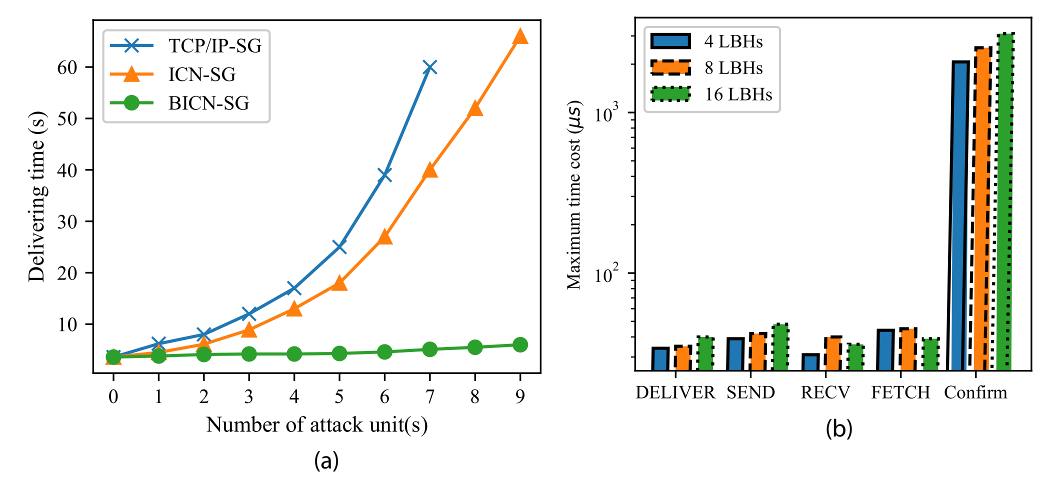

FIGURE 6. Time cost: a) Comparison of data delivering time under attacks in BICN-SG, ICN-SG, and TCP/IP-SG; b) Comparison of maximum time cost of different transaction operations with 4, 8, 16 LBHs in BICN-SG.

We first investigate the bandwidth occupation of the discovery process and data delivery process in BICN-SG, ICN-SG, and TCP/IP-SG, and the results are shown in Fig. 5a. When sending the same *discover messages* to request the same content, both bandwidth occupations of the data delivery process in BICN-SG and ICN-SG are lower than that of TCP/IP-SG due to the in-network cache. However, the bandwidth occupation of BICN-SG is a little bit higher than that of ICN-SG, because the blockchain is used to provide traceability and trust name mapping in this process, which occupies some extra bandwidth in the BICN-SG system. Then, we study the throughput of our proposed blockchain in BICN-SG, depicted in Fig. 5b. When the transactions per block are 5000, the throughput in the 4-LBHs network can reach up to 8500 transactions per second. In the networks with 4, 8, and 16 LBHs, the throughput is hundreds of times higher compared with Bitcoin.

Moreover, we observe the time consumption of retrieving a data object under attacks, whose size is 70 KB, as shown in Fig. 6a. An attack unit consists of five malicious smart meters to launch DoS attacks and five smart meters to perform cache pollution. With the number of attack groups increasing, the delivery in TCP/IP-SG and ICN-SG faces more resistance. However, the delivery time in BICN-SG is not affected by the attacks, because the blockchain helps BICN-SG to trace and exclude the malicious meters quickly. Finally, we study the time cost of different operations in BICN-SG with different amounts of LBH, including transaction construction of **DELIVER**, **SEND**, **RECV**, **FETCH**, and transaction confirmation, as shown in Fig. 6b. For one thing, the changes in the amount of LBHs do not affect the maximum time cost of transaction construction, taking less than 50 m s. For another, as the amount of LBH increases, the process of transaction confirmation consumes more time, but to bring more computational resources to enhance the security level. Meanwhile, the confirm time can reach 3000 m s, far less than 15s [15], which is the basic communication requirement of the smart grid. The above security analysis and experiment results indicate that the proposed BICN-SG can perform secure content delivery.

Open Issues

Inspired by the properties of the blockchain, we consider several open issues in our proposed ICN as follows.

Privacy Concerns: Blockchains are used as a record of various participants' behaviors, which is open for every participant to read. Although the transaction only carries the hash of the payload, some patterns of users' behaviors may still be dug out by data mining or statistical methods. Moreover, with the help of big data technology, the encryption technology of blockchains is indeed confirmed that there may exist risks. It has been proved that the anonymization of the transaction address still cannot guarantee the anonymity of the users, and some deliberate attacks can still cause threats.

Communication Requirement: An enormous number of behaviors are recorded in the blockchain, which may result in a critical demand on communication networks. For instance, Bitcoin now has more than 140 GiB of data, consisting of 270 million transactions. These transactions go through the entire network by broadcasting and cost tremendous resources of the communication network. Compared with Bitcoin, the amount of transactions in BICN is far more. Hence, the communication network of LBHs is challenged by broadcasting transactions.

Content Caching: Similar to the knowledge of users, the knowledge of content is contained in the blockchain as well. How to make use of content knowledge is an open issue. When some content has been popular recently, the hashes of this content frequently appear in the blockchain. CRs can use this temporal pattern to adjust their caches.

Conclusion

In this article, we propose a trust-enhanced blockchain based tracing mechanism for the whole content delivery process in ICN. This mechanism analyzes the records of behaviors on ICN nodes and locates the malicious ones. We design trust-enhanced mapping between a human-readable name and a self-certifying name in the blockchain, where the two forms of the name can conveniently alternate with each other to satisfy different demands of publishers, subscribers, and ICN nodes. The implementation of BLCN is mainly from the aspects of naming, name resolution, and data forwarding. We conduct a case study to realize secure energy data delivery in a BICN based smart grid, where we perform security analysis and conduct experiments. Numerical results show that our proposal is promising. Additionally, we illustrate the open issues in our proposed BICN system.

Acknowledgments

This work is supported by NSFC (61772286, 61872195, 61572262, 61872310); the "333" Project of Jiangsu Province(BRA2017401); the China Postdoctoral Science Foundation (2017M610252) and China Postdoctoral Science Special Foundation (2017T100297); the Shenzhen Basic Research Funding Scheme under research (JCYJ20170818103849343); the Strategic Information and Communications R&D Promotion Programme (SCOPE No.162302008), MIC, Japan; the Open Research Fund of the Jiangsu Engineering Research Center of Communication and Network Technology, NJUPT; and the National Engineering Research Center of Communications and Networking (Nanjing University of Posts and Telecommunications) (TXKY17014).

References

[1] Cisco visual networking index: Forecast and methodology. Accessed on Apr. 2017; available: https://www.cisco.com/c/en/us/solutions/collateral/serviceprovider/ visual-networking-index-vni/complete-white-paper-c11- 481360.html.

[2] X. He *et al.*, "Green Resource Allocation Based on Deep Reinforcement Learning in Content-centric IoT," *IEEE Trans. Emerging Topics in Computing*, 2018, pp. 1–1.

[3] K. Wang *et al.*, "Toward Trustworthy Crowdsourcing in the Social Internet of Things," *IEEE Wireless Commun.*, vol. 23, no. 5, Oct. 2016, pp. 30–36.

[4] B. Ahlgren *et al.*, "A Survey of Information-Centric Networking," *IEEE Commun. Mag.*, vol. 50, no. 7, July 2012, pp. 26–36.

[5] K. Wang *et al.*, "Crowdsourcing-Based Content-Centric Network: A Social Perspective," *IEEE Network*, vol. 31, no. 5, 2017, pp. 28–34.

[6] T. Koponen *et al.*, "A Data-Oriented (And Beyond) Network Architecture," *ACM SIGCOMM Computer Communication Review*, vol. 37, no. 4, Oct. 2007, pp. 181–92.

[7] M. Swan, *Blockchain: Blueprint for a New Economy*, O'Reilly Media, Inc., 2015.

[8] R. Tourani *et al.*, "Security, Privacy, and Access Control in Information-Centric Networking: A Survey," *IEEE Commun. Surveys Tutorials*, vol. 20, no. 1, 2018, pp. 566–600.

[9] E. G. AbdAllah, H. S. Hassanein, and M. Zulkernine, "A Survey of Security Attacks in Information-Centric Networking," *IEEE Commun. Surveys Tutorials*, vol. 17, no. 3, Third Qtr. 2015, pp. 1441–54.

[10] C. Xu *et al.*, "Making Big Data Open in Collaborative Edges: A Blockchain-Based Framework with Reduced Resource Requirements," *Proc. 2018 IEEE Int'l. Conf. Commun. (ICC)*, May 2018, pp. 1–6.

[11] C. Xu *et al.*, "Making Big Data Open in Edges: A Resource-Efficient Blockchain-Based Approach," *IEEE Trans. Parallel and Distributed Systems*, 2018, pp. 1–1.

[12] I. Eyal *et al.*, "Bitcoin-ng: A Scalable Blockchain Protocol," *NSDI*, 2016, pp. 45–59.

[13] C. Xu, K. Wang, and M. Guo, "Intelligent Resource Management in Blockchain-Based Cloud Datacenters," *IEEE Cloud Computing*, vol. 4, no. 6, Nov. 2017, pp. 50–59.

[14] K. Wang *et al.*, "A Survey on Energy Internet Communications for Sustainability," *IEEE Trans. Sustainable Computing*, vol. 2, no. 3, July 2017, pp. 231–54.

[15] K. Yu *et al.*, "A Key Management Scheme for Secure Communications of Information Centric Advanced Metering Infrastructure in Smart Grid," *IEEE Trans. Instrumentation and Measurement*, vol. 64, no. 8, Aug. 2015, pp. 2072–85.

> With the help of big data technology, the encryption technology of blockchains is indeed confirmed that there may exist risks. It has been proved that the anonymization of the transaction address still cannot guarantee the anonymity of the users, and some deliberate attacks can still cause threats.

Biographies

Huining Li [S'17] received the B.Eng. degree in electronic science and technology from Nanjing University of Information Science and Technology in 2016. Since 2016 she has been pursuing a Ph.D. degree in information acquisition and control at Nanjing University of Posts and Telecommunications. She is currently a joint Ph.D. student at the State University of New York at Buffalo, USA. Her research interests include big data analysis, information and network security, and energy management.

Kun Wang [SM'17] received two Ph.D. degrees from Nanjing University of Posts and Telecommunications, China in 2009 and from the University of Aizu, Japan in 2018, respectively, both in computer science. He was a postdoc fellow at UCLA, USA from 2013 to 2015, and a research fellow at the Hong Kong Polytechnic University, Hong Kong, from 2017 to 2018. He is currently a research fellow at UCLA, USA. His current research interests are mainly in the area of big data, machine learning systems, blockchain, and information security technologies.

Toshiaki Miyazaki [SM'13] is a professor at the University of Aizu. His research interests are in reconfigurable hardware systems, adaptive networking technologies, and autonomous systems. He received his Ph.D. degree from Tokyo Institute of Technology in 1994. He was a visiting professor at Niigata University in 2004, and a part time lecturer at the Tokyo University of Agriculture and Technology in 2003-2007. He is a senior member of IEICE and IPSJ.

Chenhan Xu is an undergraduate student in the School of Internet of Things, Nanjing University of Posts and Telecommunications, China. His current research interests include big data, cloud computing, blockchain, and machine learning.

Song Guo [SM'11] is a full professor in the Department of Computing, Hong Kong Polytechnic University. He has published over 300 papers in refereed journals/conferences and received multiple IEEE/ACM best paper awards. He is an editor of *IEEE Transactions on Green Communications and Networking* and the Secretary of the IEEE Technical Committee on Big Data. He is a Senior Member of the ACM and an IEEE Communications Society Distinguished Lecturer.

Yanfei Sun received the Ph.D. degree in communication and information systems from Nanjing University of Posts and Telecommunications, Nanjing, China, in 2006. He is currently a full Professor in the School of Internet of Things, Nanjing University of Posts and Telecommunications. He is also a director of the Jiangsu Engineering Research Center of HPC and Intelligent Processing. His current research interests are mainly in the areas of future networks, industrial Internet, energy Internet, big data management and analysis, and intelligent optimization and control.