Designing collaborative blockchained signature-based intrusion detection in IoT environments

Li, Wenjuan; Tug, Steven; Meng, Weizhi; Wang, Yu

Published in:
Future Generation Computer Systems

Link to article, DOI:
10.1016/j.future.2019.02.064

Publication date:
2019

Document Version
Peer reviewed version

Citation (APA):

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.
Designing Collaborative Blockchained Signature-based Intrusion Detection in IoT environments

Wenjuan Li, Steven Tug, Weizhi Meng, Yu Wang

Abstract

With the rapid development of Internet-of-Things (IoT), there is an increasing demand for securing the IoT environments. For such purpose, intrusion detection systems (IDSs) are one of the most important security mechanisms, which can help defend computer networks including IoT against various threats. In order to achieve better detection performance, collaborative intrusion detection systems or networks (CIDNs) are often adopted in a practical scenario, allowing a set of IDS nodes to exchange required information with each other, e.g., alarms, signatures. However, due to the distributed nature, such kind of collaborative network is vulnerable to insider attacks, i.e., malicious nodes can generate untruthful signatures and share to normal peers. This may cause intruders to be undetected and greatly degrade the effectiveness of IDSs. With the advent of blockchain technology, it provides a way to verify shared signatures (rules). In this work, our motivation is to develop CBSigIDS, a generic framework of collaborative blockchained signature-based IDSs, which can incrementally build and update a trusted signature database in a collaborative IoT environment. CBSigIDS can provide a verifiable manner in distributed architectures without the need of a trusted intermediary. In the evaluation, our results demonstrate that CBSigIDS can enhance the robustness and effectiveness of signature-based IDSs under adversarial scenarios.

Keywords: Intrusion Detection System, Internet-of-Things, Signature-based Detection, Collaborative Network, Blockchain Technology, Insider Attacks.

1. Introduction

The Internet-of-Things (IoT) refers to a system of internet-enabled computing devices, mechanical and digital machines, and objects that have the capability to transfer data over a network without requiring human-to-human or human-to-computer interaction [14]. More and more organizations are using IoT to improve their performance, i.e., operating more efficiently, better understanding, improving decision-making, etc. While the interrelated IoT devices are also threatened by many attacks, i.e., the threat-tread states moving from manipulating information to controlling actuations [2].

To safeguard various IoT devices and critical infrastructures, intrusion detection systems (IDSs) are one of the most essential and important tools that can help identify potential anomalies and policy violations [37, 42]. Based on the deployment, an IDS can be classified as either host-based IDS (HIDS) that focuses on local system logs, or network-based IDS (NIDS) that monitors network state and traffic. Further, there are two typical detection approaches: signature-based detection and anomaly-based detection. The former like [50, 40] (also known as misuse detection) uses a signature matching process to compare the stored signatures and the observed events like payload and system record. The latter like [49, 12] identifies a potential threat by discovering a significant deviation between its pre-defined normal profile and the observed events for a period of time. If any security violations are found, an alarm would be sent to notify security administrators. Figure 1 depicts the high-level detection workflow of both signature-based and anomaly-based approach.

With the rapid development of cyber attacks, it has...
become much difficult for separated IDSs to accurately discover complicated attacks, as they only have limited information on the protected environments. Therefore, traditional IDSs could be easily bypassed by both well-prepared attackers and complex attacks, e.g., Denial-of-Service (DoS) attack. To enhance the detection performance in practice, collaborative intrusion detection systems or networks (CIDSs or CIDNs) are employed, which encourages a set of IDS nodes to request and retrieve data from other nodes [53]. As an example, IDS nodes can share their signatures (also named rules) with others in a CIDN, with the purpose of improving detection accuracy and reducing unwanted alarms [25, 30, 24]. However, such type of collaborative intrusion detection is usually vulnerable to insider attacks, due to the distributed nature, i.e., malicious nodes can provide false rules to affect the detection performance of other nodes. In this case, there is a great need for designing appropriate security mechanisms to secure the process of signature sharing in a CIDN/CIDN.

Motivations. Inspired by a broad adoption of Bitcoin, blockchain technology has attracted much more attention from both academia and industry, allowing untrusted individuals to connect with others in a verifiable manner without the need of a trusted centralized entity [55]. A blockchain is an ordered list of blocks, in which each of them has a cryptographic pointer to their precursor. New blocks can be appended to the blockchain using a consensus protocol, which eventually allows sets of blockchain nodes to synchronize their copies of blockchain locally. By taking advantage of consensus mechanisms, blockchains can provide a transparent and integrity protected data storage, whereas the recorded data in any given block cannot be modified retroactively without the modification of all subsequent blocks. This characteristic of blockchains is desirable for sharing IDS signature in a secure way for CIDN and IoT environments.

Contributions. Motivated by the recent development and applications of blockchains, in this work, we focus on signature-based IDSs and design CBSigIDS, which is a generic blockchain-based framework for securing signature sharing against malicious nodes in IoT environments. The key idea behind is to apply blockchain technology for incrementally building a trusted signature database. This can ensure the detection effectiveness by adopting only trusted and verified signatures in a collaborative network. Our contributions can be summarized as follows:

- To reduce the influence of malicious nodes, we propose a blockchain-based framework called CBSigIDS by combining blockchains with distributed signature-based IDSs in an IoT environment. Our approach enables various IDS nodes to incrementally generate and verify a signature database in CIDNs. With the use of blockchains, CBSigIDS can provide a verifiable manner for sharing signatures among different nodes without the need of a trusted intermediary.

- In the evaluation, we study the performance of CBSigIDS in different environments and adversarial scenarios, e.g., in a simulated and a real CIDN environment respectively. We further compare our approach with a blockchain-based SDN application called DistBlockNet [43] in a practical IoT environment. The obtained results demonstrate that CBSigIDS can enhance the robustness and effectiveness of signature sharing in a CIDN through building a trusted signature database, i.e., it can protect DistBlockNet against malicious nodes.

It is worth noting that this work focuses mainly on signature-based detection, which has a larger implementation in practice as compared with anomaly detection [46]. This is because anomaly-based IDSs often result in a high false alarm rate due to the difficulty of building an accurate profile. While the combination of blockchain technique and anomaly detection is one of our future work. The major purpose of this work is to explore the feasibility of applying blockchain technology in CIDNs, and to stimulate more research in designing robust signature sharing in CIDNs.

The remainder of this paper is organized as follows. Section 2 introduces related research studies in relation to distributed and collaborative intrusion detection. In
Section 3, we introduce the background of blockchain technology and describe CBSigIDS in detail, e.g., the high-level architecture on how participating nodes construct a consortium blockchain. Section 4 presents our evaluation settings and discusses the obtained results. Section 5 presents some limitations and challenges in this field. Finally, we conclude our work in Section 6.

2. Related Work

Traditionally, a separated IDS often has no information about the deployed network where it tries to protect, leaving an opportunity for attackers to bypass its examination. For instance, cyber intruders can launch some complex attacks like DoS attack to compromise a single IDS, as it cannot have an overview of the whole traffic status in a network. In this case, there is a great need for a collaborative system or IDS network to leverage the detection performance of a single IDS [53].

**Distributed systems.** In the literature, distributed monitoring systems have been developed for decades. For example, distributed Intrusion Detection System (DIDS) [44] was introduced in 1991, which could utilize distributed monitoring and data reduction with centralized data analysis module to analyze a heterogeneous computer network. Event Monitoring Enabling Responses to Anomalous Live Disturbances (EMERALD) [39] was also developed in 1997, which could track malicious activity across abstract layers in a large network. It combines models from distributed high-volume events with traditional intrusion detection. COSSACK system [38] was designed for mitigating DDoS attack in an automatic way. This system does not require human intervention and supports independent attack signature generation.

In addition, DOMINO (Distributed Overlay for Monitoring InterNet Outbreaks) [33] was another type of distributed IDS, which enhances collaboration among heterogeneous nodes in a network. The overlay design enables this system to be heterogeneous, scalable, and robust to attacks and failures. It has the capability of detecting spoofed IP sources, reducing false positives, and classifying threats in a timely manner. Then, PIER [13] was an Internet-scale query engine, which supports massively distributed, database-style dataflows for snapshot and continuous queries. It can serve as a building block for a set of diverse Internet-scale information-centric applications.

**Collaborative intrusion detection.** In order to achieve better detection performance, a CIDS or CIDN enables an IDS node to exchange required information with other nodes. In 2006, Li et al. [15] argued that most distributed IDSs were relying on either centralized fusion, or distributed fusion that are not scalable. Motivated by this issue, they proposed a type of CIDS based on the emerging decentralized location and routing infrastructure. However, their mechanism assumes that all peers in the network are trusted, which would be vulnerable to insider attacks. In the field of collaborative intrusion detection, insider attacks are considered as one of the biggest threats, where an intruder has the right to consume resources in a network.

To protect CIDS against insider threats, a promising solution is to design appropriate trust mechanisms to evaluate the reputation levels among IDS nodes. As an example, Li et al. [20] introduced a P2P-based overlay method for IDSs (shortly Overlay IDS), which uses a trust-aware engine for correlating alerts and an adaptive scheme for managing trust. They concluded that if a reputation system was not incentive compatible, the more numbers of peers in the system, the less likely that a malicious will be reported correctly.

Based on this observation, Fung et al. [8] proposed a challenge-based CIDN, where the trustworthiness of an IDS node depends on the received answers to the challenges. They first introduced a Host-based IDS framework that enables each HIDS to evaluate the trustworthiness of others based on its own experience and uses a forgetting factor to give more emphasis on the recent experience of each peer. To improve the performance of such mechanism, Li et al. [16] identified that different IDS nodes may have different levels of sensitivity in detecting different types of intrusions. They then proposed a notion of intrusion sensitivity (IS) that measures the detection sensitivity of an IDS in detecting different kinds of intrusions. Accordingly, they proposed an intrusion sensitivity-based trust management model [17] that could allocate the values of IS by means of machine learning classifiers (e.g., a knowledge-based KNN classifier [30], ensemble classifier [25]). As a study, they described how to apply intrusion sensitivity for alarm aggregation and investigated its effect on defeating pollution attacks, in which a group of malicious peers cooperate together by providing false alert rankings [19].

The experimental results indicated that their method can decrease the trust values of malicious nodes in a fast manner.

Li et al. [20, 22] further identified intruders could use some advanced attacks to compromise a challenge...
mechanism. They introduced a passive message fingerprint attack (PMFA), which enable malicious nodes sending malicious feedback to only normal request and their trust values. They also developed a special On-Off attack (called SOOA) [23], in which malicious nodes could keep responding normally to one node while acting abnormally to another node. In addition, how to reduce the overload in communication is a critical issue for challenge mechanisms in different scenarios, e.g., healthcare [21, 34]. Some other related work regarding how to enhance the performance of an IDS can be referred to [6, 7, 18, 26, 27, 28, 29, 31, 32, 35].

Blockchain-based intrusion detection. How to apply blockchains in the field of intrusion detection is an interesting and important topic. Many studies have started researching in this area. Alexopoulos et al. [3] described a framework of a blockchain-based CIDS, where they considered a set of raw alarms produced by each IDS as transactions in a blockchain. Then, all collaborating nodes employed a consensus protocol to ensure the validity of the transactions before delivering them in a block. This can guarantee the stored alerts are tamper resistant in the blockchain, but they did not implement and evaluate their method in practice.

Focused on this issue, Meng et al. [33] provided some early insights regarding the intersection of IDSs and blockchains, and discussed some challenges in this area. They believed that blockchains can have a positive impact on distributed intrusion detection in the aspects of data sharing, alarm exchange and trust computation. Golomb et al. [11] then introduced CIoTA, a framework that uses the blockchain concept to perform distributed and collaborative anomaly detection for those devices with limited resources. On the other hand, IDS technique can also help protect blockchain applications. Steichen et al. [47] proposed ChainGuard, an OpenFlow-based firewall for securing blockchain-based SDN, which requires all traffic to be blockchain nodes should be forwarded by the switches controlled by ChainGuard. This could help reduce the malicious behavior from the participating nodes. Sharma et al. [43] proposed DistBlockNet, a distributed secure SDN architecture for IoT by integrating the blockchain technology, allowing a node to interact with others without the need of a trusted central controller.

How to share rules in a secure way is an important issue in the field of intrusion detection [9]. Our previous work [1] introduced how to achieve this by leveraging blockchain technology. In this work, we further consider DistBlockNet in the evaluation, and evaluated both CBSigIDS and DistBlockNet in a practical IoT environment. It is found that CBSigIDS can be used to enhance the robustness of DistBlockNet in defending against malicious nodes.

3. Our Approach

In this section, we begin by introducing the background of blockchain technology, and then introduce how to design CBSigIDS for CIDNs in detail.

3.1. Blockchain Technology

Blockchains can be considered as a distributed data structure, allowing information to be shared and verified among different entities in a peer-to-peer network, without the need of a trusted third party. In other words, blockchain technology is a decentralized ledger that enables recording transactions across various participating nodes, and protecting data integrity via strong cryptographic tools. The recorded data in any given block cannot be altered retroactively without the alteration of all subsequent blocks [33, 54]. A typical blockchain contains a list of records (called blocks) that can be chronologically ordered by discrete time-stamps. In particular, each block is linked to the previous block via a cryptographic hash, and the first one is called genesis block. A block usually contains a payload, a time-stamp and a cryptographic hash value of the entire previous blocks in the chain. Thus, blockchains can be treated as an implementation of a shared secure distributed ledger, where the participants have the right to read and write without any constraints in most cases.

According to specific types of permission control, existing approaches of blockchain implementation can be categorized into three types: public, consortium, and private. More specifically, a public blockchain allows every entity to act as a reader and a writer without any constraints, like Bitcoin [36] and Ethereum [52]. A consortium blockchain only allows registered entities or a small group of verified entities to have the right to read or write on the blockchain. A private blockchain is often controlled by a single entity, but still can be distributed in different locations. A blockchain can be updated via a consensus protocol, which ensures all participating entities to agree on a uniform view of the ledger. A consensus protocol can be dependent on specific blockchain implementation and threat model [33].

- Proof of work. This method allows a node to successfully accept a block, when a pre-defined amount of computational resources (known as ‘work’) can be proved to spent.
3.2. CBSigIDS

As discussed earlier, collaborative intrusion detection encourages IDS nodes to share required information with each other in order to enhance the detection capability. For example, a signature-based IDS can update its own rule database and then share some rules to help other nodes improve their detection performance in a network. However, we notice that CIDNs are typically vulnerable to various insider attacks; thus, an insider can share false signatures to degrade the effectiveness of detection, i.e., hiding external attackers.

Motivated by the wide adoption of blockchain technology, in this work, we focus on insider threats and propose CBSigIDS, which is a generic framework of collaborative blockchained signature-based IDSs. It mainly leverages blockchains to help build a trusted rule database in a collaborative network environment. Figure 2 depicts the high-level architecture of CBSigIDS, in which the participating nodes can construct a consortium blockchain.

It is worth noting that consortium blockchains are applicable in existing CIDNs, where only a group of verified nodes can join and interact with each other in the network. For instance, challenge-based CIDNs require a node to register to a trusted certificate authority (CA) and obtain its unique proof of identity (e.g., a public key and a private key), before it can join a CIDN. This attempts to provide a first layer of defence against malicious nodes, i.e., avoiding a participant to register many identities.

As depicted in Figure 2, a signature-based IDS node often contains three major components, including P2P communication component, collaboration component and trust management component [8, 16, 17].

- **Proof of stake.** This method ensures a consensus to be achieved by considering both random selection and the influence (known as 'stake') of the participating entities. It is assumed that entities would guarantee the integrity of blocks when they have a large stake in the blockchained network.

- **Proof of elapsed time.** This method ensures a consensus to be achieved by requesting every potential verifier to share a secure and random waiting time from a trusted execution environment.

- **CBSigIDS blockchain.** In CBSigIDS, each IDS node (or blockchain node) in the consortium blockchain can monitor the network traffic, identify attacks and periodically share a set of signatures (rules) with others. This set of rules has to be signed by a private key from a node, in order to understand the source of rules. Other nodes will only accept these rules by verifying them against their local database. In this case, the blockchain can be only expanded if the majority of nodes have verified that the received block contains trusted rules.

**Figure 2: The high-level architecture of CBSigIDS, where the participating nodes can construct a consortium blockchain.**
4. Evaluation

In this section, we evaluate the performance of CB-SigIDS under some adversarial scenarios in a simulated and a real CIDN environment, respectively.

4.1. Experiment-1

In this experiment, our goal is to investigate the performance of CBSigIDS against worm attack and flooding attack in a simulated CIDN. Our simulated network contains a total of 50 nodes that were randomly distributed in a $10 \times 10$ grid region. We used Snort \cite{snort} as the signature-based IDS and adopted its default rule database. The experiment could be started when all IDS nodes built a list of neighbors and established a stable connection. When an IDS node updates its rules, it can share the rules with others via the blockchain.

Flooding attack. To test the performance of CBSigIDS, we randomly selected two outside nodes (not belong to our CIDN) to launch a flooding attack, while an IDS node inside the CIDN started sharing two related rules against such attack. Figure 3 presents the packet rate during the flooding period. The attack was started from 4s and stopped at 44s, in which the maximum packet rate could reach around 3200 packets/s.

Worm attack. Under this attack, it is assumed that three IDS nodes updated its rules and started sharing related rules with others via the blockchain, and that the other nodes were not capable of detecting the worm at that time (denote as vulnerable node). Only the vulnerable nodes those who accepted the rules before being hit by the worm, could immediately protect themselves (denote as survived node) and mitigate such attack by reacting in a proper way, i.e., closing the vulnerable port or disconnecting from the network until the vulnerability is fixed. During the attack period, worm would be distributed to IDS nodes in every 2 seconds.

Figure 5 depicts the number of survived nodes under the worm attack. It is found CBSigIDS could gradually increase the number of survived nodes to 32, with a survival rate of 66.7%. In \cite{overlay_2005}, they used a P2P-based overlay for intrusion detection that addresses the worm attack using both a trust-aware engine for correlating alerts and an adaptive scheme for managing trust. They evaluated their method with a virtual network with 36 clients and an Internet worm attack. The overlay IDS can produce an alarm if it receives three similar alert messages from other nodes. In our experiment, our work could achieve a similar but better result (66.7%), as compared with the overlay IDS (a survival rate of 60%). These results demonstrate that the feasibility and performance of our approach in securing the CIDNs under attacks.
4.2. Experiment-2

In this experiment, we collaborated with an IT company to study the performance of CBSigIDS in a real CIDN with a total of 46 nodes. The IDS nodes could connect with the Internet through a server that could also provide many computing resources. We implemented our approach with a proof-of-concept blockchain, and Snort [45] was deployed in each node.

**Flooding attack.** Similar to the first experiment, we also utilized some external nodes to launch a flooding attack, while an IDS node inside the CIDN started sharing relevant rules to defeat such attack. Figure 6 shows that the period of attacking traffic was started from 2s and stopped at 80s, in which the maximum packet rate could reach around 3450 packets/s. Figure 7 describes the number of infected nodes during the period of flooding attack. It is found that our approach could steadily reduce the number of infected nodes from 49 to 0 (means that all nodes could produce alarms for the flooding attack), when the time reached 66s.

**Insider exploration.** To explore the effectiveness of signature sharing, we randomly selected one node inside the CIDN to be malicious, which could share false rules with other nodes. We mainly manipulated the patterns in these signatures (rules) that are used to detect flooding attack and worm attack. The main purpose behind this exploration is to study the impact of malicious nodes on CBSigIDS. We repeat such exploration several times, and found that these false rules would not be accepted by other nodes, as they could not bypass the verification in the blockchained signature database. Our obtained results validate that an attacker cannot compromise our approach of CBSigIDS, if he fails to manage the majority of blockchain nodes in a CIDN.

4.3. Experiment-3

In this experiment, we collaborated with another IT organization and established an SDN-based IoT environment. Figure 8 shows the high-level network architecture, including a controller layer and an IoT device layer. In particular, the controller layer contains three SDN controllers that could synchronize information, and device layer consists of 56 IoT devices, like PCs, laptops and smartphones, which are managed by the controllers. Snort was deployed in each node to perform signature-based detection.
DistBlockNet. In this experiment, we consider DistBlockNet [43], which employs distributed network control in the IoT network by using the blockchain technology to improve security, scalability, and flexibility, without the need for a central controller. In particular, they applied blockchain technique for updating a flow rule table, in order to securely verify a flow-rule table. To mitigate different types of attacks, it could deploy some additional security mechanisms for threat prevention, data protection, and access control. For example, it implemented two modules called Shelter and OrchApp in each local network to help handle the security attacks at a different level. OrchApp mainly works at the management or application layers, the controller-application interface, and the control layer. Shelter handles the data layer, the controller-data interface, and the control layer. However, we found there was no particular mechanism in the IoT device layer to identify false data that may be sent by malicious nodes. Their evaluation results indicated that DistBlockNet could detect malicious traffic under flooding attacks.

Flooding attack. Similarly, we used some external nodes to conduct a flooding attack and deliver malicious traffic to such IoT environment. As shown in Figure 9, the period of malicious traffic was started from 3s and stopped at 100s, in which the maximum packet rate could reach around 3772 packets/s.

Different from the above two experiments, this time we assume that all insider nodes have one effective rule in detecting this attack and set up two malicious nodes to started spreading malicious rules that attempt to replace the effective rule with a false one from 3s. Figure 10 depicts the number of infected nodes during the period of flooding attack. ‘Infected’ here refers to the nodes who adopt the false rule during the attacking period. It is found that DistBlockNet was vulnerable to such attack, where the infected nodes could increase gradually and all nodes become infected at around 80s. This is because DistBlockNet did not employ a particular mechanism to check the signatures sent by insider nodes.

As a comparison, we applied our approach into DistBlockNet and re-performed the experiment three times. We found that the false rule would not be accepted by insider nodes under CBSigIDS, as the false one could not bypass the verification of our blockchained rule database. Our results demonstrate that our approach of CBSigIDS can help enhance the robustness of a collaborative signature-based CIDN by building a trusted signature database.

5. Discussion and Limitations

To the best of our knowledge, this is the first work in discussing the application of blockchains with collaborative signature-based IDSs. There are many issues and open challenges in this emerging area.
• **Signature-based detection.** As signature-based
IDSs often produce fewer false alarms than an
anomaly-based IDS, it has been more extensively
used in practice [46]. Therefore, this work mainly
focuses on signature-based IDSs and explores
how to share rules in a verifiable way. It is worth
noting that Golomb et al. [11] has tried to combine
blockchains with anomaly-based detection through
building a trusted training model. Based on the re-

results obtained in this work, it is one of our future
topics to consider how to build a more effective and
robust collaborative anomaly-based IDS.

• **CIDN environments and CBSigIDS blockchain.** In
this work, we explored the performance of CB-
SigIDS in a simulated and a practical CIDN, re-
respectively. In practice, CIDNs have been wide-
ly implemented, whereas blockchains are still un-
der construction especially in the field of intrusion
detection. As a result, we only adopted a proof-
of-concept blockchain in current work. In future
work, we plan to validate our approach using more
practical and well-developed anomaly-based IDS.

• **Adversarial scenarios.** Similar to other studies in
the area of intrusion detection, this work mainly
considers several common attacks like flooding at-
tack and worm attack. The obtained experimental
results demonstrated the feasibility and effec-
tiveness of our approach. In future work, it is an in-
teresting topic to consider other attacks including
advanced attacks, and different network settings.

• **Trust mechanisms.** Currently, most CIDNs are
likely to deploy at least one trust-based mechanism
to help identify insider attacks, like challenge-
based mechanism that evaluates the trustworthi-
ness of target nodes by comparing the received feedback with the expected answers. In future
work, we plan to conduct a comparison among sev-
eral trust mechanisms with blockchain technology
in securing CIDN environments.

• **Large-scale evaluation.** To investigate the scal-
ability of a security mechanism. It is very im-
portant to perform a large and systematic evaluation by
considering various variables and scenarios. How-
ever, blockchain-based intrusion detection is an e-
merging topic, some special conditions should be
considered on how to design such kinds of experi-
ments, i.e., which type of blockchains can be used
in the evaluation.

Intuitively, blockchain technology can help improve
intrusion detection in the aspects of data sharing and
alarm exchange, but it still suffers from some inherent challenges and limitations according to [33].

• **Energy and cost.** The computational power is a
concern for blockchain applications in real-world
scenarios. For instance, Wang and Liu [51] iden-
tified that the required computational power could
be added on single miners at first, while could be
greatly increased afterwards when the network e-
volved.

• **Security and privacy.** Most existing blockchain ap-
lications require smart transactions and contracts
to be linked to known identities. This could in-
crease both privacy and security concerns when s-
sharing the data on the shared ledger. In addition,
blockchain technology can be threatened / hacked
by any traditional attacks like distributed denial-
of-service (DDoS) attacks.

• **Latency and complexity.** Depending on different s-
cenarios and architectures, blockchain application-
s possibly require several hours to finish until all
parties update their corresponding ledgers, which
may open a hole for cyber-criminals. In this work,
we only used a proof-of-concept blockchain in-
stead of an existing blockchain, hence the achieved
speed could much faster than that in a practi-
cal blockchain application. While the proof-of-
concept blockchain is still valid to investigate the
robustness of our approach in terms of our goal-
s. In future, we plan to construct a more practical
blockchain and re-evaluate our results.

• **Organization and block size.** Due to the wide adop-
tion of blockchain applications, many different or-
ganizations may develop their own blockchain re-
lated standards. Due to the increasing size of dis-
tributed ledgers, this may greatly degrade the per-
formance and make the blockchains less efficient
than current frameworks.

6. Conclusion
Collaborative intrusion detection has become an im-
portant and essential security solution to safeguard IoT
environments, which allows various IDS nodes to ex-
change information with each other, e.g., rules. Howev-
er, malicious nodes in a CIDN may generate untruth-
ful signatures and share to others, which can greatly
degrade the effectiveness and robustness of detec-
tion. In the literature, blockchain technology is believed to provide a verifiable manner for sharing information without the need of a trusted centralized entity. Motivated by the recent blockchain applications, in this work, we focus on signature-based detection and develop \textit{CBSigIDS}, a generic framework for collaborative blockchain signature-based IDSs, which adopts blockchains to help incrementally share and build a trusted signature database. In the evaluation, our experimental results in both simulated and real IoT environments demonstrate that \textit{CBSigIDS} can enhance the robustness and effectiveness of signature-based detection under adversarial scenarios (e.g., flooding attacks) by sharing the signatures in a verifiable way.

Our work is an early research study in this area, showing how to use blockchains to improve the effectiveness of collaborative signature-based IDSs. The main purpose is to complement the literature and stimulate more research on this topic. Future work includes building a secure IDS framework via blockchains for anomaly-based detection and developing a strong mechanism in defending IDS nodes against advanced insider attacks.

Acknowledgment

The authors would like to thank security administrators and managers from the participating organizations for their help and support during the evaluation. This work was partially supported by H2020-SUCCESS-03-2018: CyberSec4Europe and the Young Scientists Fund of the National Natural Science Foundation of China (No. 61802077).

Reference


[23] W. Li, W. Meng, L.F Kwok, “Investigating the Influence of


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. She is a student member of IEEE.

Steven Tug is an exchanged student at Department of Applied Mathematics and Computer Science, Technical University of Denmark (DTU), Denmark. He has a broad interest in network and system security, like malware detection and smartphone security. Before, he got some programming experiences from industry.

Weizhi Meng is currently an assistant professor in the Department of Applied Mathematics and Computer Science, 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. He was known as Yuxin Meng and prior to joining DTU, he worked as a research scientist in Infocomm Security (ICS) Department, Institute for Infocomm Research, Singapore. His primary research interests include intrusion detection, smartphone security, biometric authentication, HCI security, blockchain security, trust management, and vulnerability analysis. He is a member of IEEE.

Yu Wang received his Ph.D. degree in computer science from Deakin University, Victoria, Australia. He is currently an associate professor with the School of Computer Science, Guangzhou University, China. His research interests include network traffic analysis, mobile networks, social networks, and cyber security.
Highlights

1. We propose CBSigIDS, a framework by combining blockchains with signature-based IDSs in a collaborative IoT environment.
2. Our framework enables various IDS nodes to incrementally produce and verify a signature (or rule) database without the need of a trusted intermediary.
3. We evaluated CBSigIDS in different environments and adversarial scenarios including both a simulated and a real CIDN environment.
4. We also compare and apply our approach into a blockchain-based SDN application in a practical IoT environment.