Towards Blockchained Challenge-based Collaborative Intrusion Detection

Wenjuan Li[1], Yu Wang[2⋆], Jin Li[2], and Man Ho Au[3]

[1] Department of Computer Science, City University of Hong Kong, Hong Kong
[2] School of Computer Science, Guangzhou University, China
[3] Department of Computing, The Hong Kong Polytechnic University, Hong Kong
yuwang@gzhu.edu.cn

Abstract. To protect distributed network resources and assets, collaborative intrusion detection systems / networks (CIDSs / CIDNs) have been widely deployed in various organizations with the purpose of detecting any potential threats. While such systems and networks are usually vulnerable to insider attacks, so that some kinds of trust mechanisms should be integrated in a real-world application. Challenge-based trust mechanisms are one promising solution, which can measure the trustworthiness of a node based by sending challenges to other nodes. In the literature, challenge-based CIDNs have proven to be robust against common insider attacks, but it may still be susceptible to advanced insider attacks. How to further improve the robustness of challenge-based CIDNs remains an issue. Motivated by the recently rapid development of blockchains, in this work, we aim to combine these two and provide a blockchained challenge-based CIDN framework. Our evaluation shows that blockchain technology has the potential to enhance the robustness of challenge-based CIDNs in the aspects of trust management (i.e., enhancing the detection of insider nodes) and alarm aggregation (i.e., identifying untruthful inputs).

Keywords: Intrusion Detection, Collaborative Network, Insider Attack, Blockchain Technology, Challenge-based Trust Mechanism.

1 Introduction

Due to the connectivity and sensing features, Internet-of-Things (IoT) has been gradually adopted by many organizations. The Gartner manager predicted that the IoT would keep delivering new opportunities for digital business innovation over the next decade, many of which can be further boosted by newly developed technologies like artificial intelligence [12]. Their report forecasts that up to 14.2 billion things will be connected by the end of 2019, and will finally reach a total of 25 billion devices by the end of 2021 [11].

The rapid growth of IoT devices bring many benefits, i.e., facilitating our daily lives, but it also becomes a major target by cyber criminals. The Symantec

[⋆] Corresponding Author

security report indicated that the overall volume of IoT attacks remained consistent and high in 2018 [51]. In particular, connected cameras and routers were the most infected devices - there is an increase on the infection vector. While worms and bots are still the most commonly detected IoT attacks. For example, the Mirai distributed denial of service (DDoS) worm remained an active threat and, account for a 16 percent of the detected attacks, which was the third most common IoT threat in 2018.

To help protect the security of IoT, intrusion detection systems (IDSs) are a basic and essential security mechanism. To fit the distributed nature, collaborative intrusion detection systems / network (CIDSs / CIDNs) are often deployed in a distributed environment, which allow a set of IDS nodes to exchange required messages and understand the protected environment [54, 59]. A detector could be either rule-based (signature-based) or anomaly-based. The former has to compare its stored rules with incoming events, in order to identify an attack [44, 55]. The latter discovers a potential threat through identifying an anomaly between its pre-built benign profile and the current profile [45].

Insider attacks are one major threat to distributed networks and environments, some trust mechanisms are often implemented to protect CIDSs / CIDNs. In the literature, challenge-based trust mechanism is one promising solution, which evaluates a node's reputation by sending challenges and receiving the corresponding feedback [8]. A series of research like [8, 9] has proven its effectiveness against common insider attacks; however, some studies demonstrated that such challenge-based CIDNs may still be susceptible to advanced attacks [23–25, 27]. For instance, the Passive Message Fingerprint Attacks (PMFA) [23] enables suspicious nodes to cooperate in identifying normal messages and remain their reputation without being detected. Thus, there is a great need to design a more robust challenge-based CIDNs to ensure its detection effectiveness. Below are two desirable attributes for a new CIDN framework.

- To avoid the issue of a single point of failure (SPOF), the CIDN framework should not rely mainly on a centralized server.
- The CIDN framework should provide a robust trust management process, which can evaluate the trustworthiness of nodes in an accurate way.
- The CIDN framework should be able to identify malicious inputs, which are even from some trusted nodes.

Recently, blockchain technology has become quite popular encouraged by the success of cryptocurrency Bitcoin. The Gemalto report [10] indicates that the adoption of blockchains has doubled from 9% to 19% in the early 2019, and this trend is likely to continue in the next year and beyond. They also described a survey that up to 23% of respondents believed that blockchain technology would be an ideal solution to use for securing IoT devices, and 91% of organisations are likely to consider it in the future. For instance, Amazon announced its new managed service, Amazon Managed Blockchain, which allows users to set up and configure a scalable blockchain network with just a few clicks [2]. With a huge number of devices, blockchains can increasingly be used to monitor and record those communications and transactions in an IoT environment [29].

Currently, blockchains have been applied into many domains like IoT [28, 48], transportation [17, 22], energy [47]. The strong encryption used to secure blockchains can greatly increase the difficulty for cyber criminals to brute-force their way into private and sensitive environments. Due to these merits, some research has started trying to combine blockchains with CIDSs / CIDNs. An initial blockchain-based framework was proposed by Alexopoulos et al. [1], aiming to protect the alarm exchange among the collaborating nodes. They regarded raw alarms generated by the monitors are stored as transactions in a blockchain, replicated among the participating nodes of peer-to-peer network. While they did not show any experimental implementation or results. Tug et al. [52] introduced CBSigIDS, a framework of collaborative blockchained signature-based IDSs, by incrementally sharing and building a trusted signature database via blockchains in a CIDN network. They mainly targeted the combination of blockchains with signature-based IDSs, but remained anomaly-based detection as future work. On the other hand, a blockchain-based framework called CIoTA was proposed by Golomb *et al.* [13], which focused solely on anomaly detection via updating a trusted detection model.

Contributions. Though some studies have discussed the intersection between CIDSs and blockchains, to the best of our knowledge, most existing work was initialized at the high level, without specifying a concrete CIDS / CIDN. In addition, there is no work focusing on a specific trust-based detection system. To make up this gap, in this work, we focus on the challenge-based trust mechanism, and develop a blockchained challenge-based CIDN framework. Our contributions can be summarized as below.

- To combine the blockchain technology with a concrete type of trust-based CIDN, we propose a blockchained challenge-based CIDN framework, which can be workable under both signature-based and anomaly-based detection. In particular, blockchains can be served as an additional layer to provide the flexibility in practical deployment.
- Under our framework, we show how to use blockchains to enhance the robustness of trust management against attacks, as well as protect the alarm aggregation process from malicious inputs. The enhancement is valid for both signature-based and anomaly-based detection.
- In the evaluation, we exploit the performance of our framework in the aspects of trust computation and alarm aggregation. Our results demonstrate that our framework can become more robust via the implementation of blockchains, i.e., identifying malicious nodes and untruthful inputs.

Paper organization. Section 2 introduces research studies on collaborative intrusion detection and the background of blockchains. Section 3 describes our framework of blockchained challenge-based CIDNs that can be suitable for both signature-based and anomaly-based detection. We show how to use blockchains to enhance the trust management and alarm aggregation. Section 4 shows our experimental settings and analyzes the collected results. We discuss some challenges in Section 5 and conclude the work in Section 6.

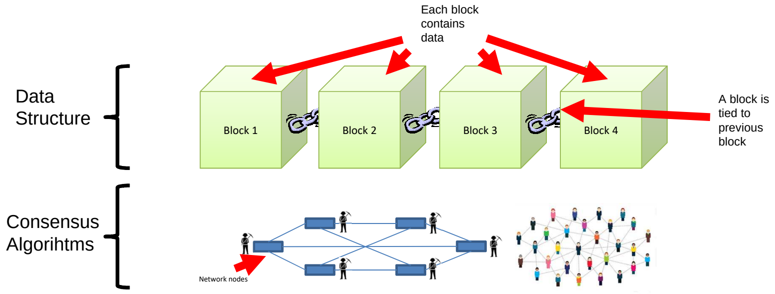

Fig. 1. The high-level review of blockchains.

2 Background and Related Work

In this section, we introduce the background of blockchain technology and review research studies on distributed detection systems, collaborative intrusion detection and blockchain-based detection.

2.1 Background of Blockchains

The original purpose of blockchains is to make payments between entities without a trust relationship and build a temper-resistant blockchain. Cryptocurrencies like Bitcoin have proven to be a phenomenal success. The underlying blockchain technique, which is an ingenious combination of multiple technologies such as peer-to-peer network, consensus protocol over a distributed network, cryptographic schemes, distributed database, smart contract and game theory, provides a decentralized way to build trust in our social and economic activities, and thus holds a huge promise to change the future of financial transactions, and even our way of computation and collaboration. As one of hottest topics in the fields of IT and Fintech, blockchain has drawn much attention from researchers, as well as IT and fintech industry. So far, both research community and industry community have made significant progresses in blockchain technologies and applications.

A blockchain node often maintains a list of records (known as blocks), which are organized in a chronological order based on discrete time stamps [60]. A block is typically comprised of a payload, a timestamp and a cryptographic hash value. The first block is called genesis block, and the node behind can connect to the previous one via a hash value. New blocks are added in a sequential manner with the next block containing a hash of the previous block. A new block can be generated once the previous block enters in the blockchain. The big feature of a block is that the recorded data in any block could not be modified without the alteration of all subsequent blocks [38]. The high-level review of blockchains is depicted in Fig. 1.

A blockchain can be generally classified into two categories: public blockchain and permissioned blockchains [60]. The former enables anyone to join and contribute to the network like Bitcoin [39] and Ethereum [58]. A public blockchain is completely open and anyone is free to join & leave. Everyone can participate in the major activities of the blockchain network including reading, writing and auditing the ongoing activities on the public blockchain network. The latter allows only verified entities to join the network, and perform only certain activities on the network like Hyperledger [15]. For example, Such blockchains would grant special permissions to each participant to have permissions to read, access and write pre-defined information on the blockchains. Blockchain nodes can make a decision-making process via consensus algorithms. There are some requirements for consensus algorithms in blockchains. For instance, the algorithm should collect all the agreements from chain nodes. Each node should aim at a better agreement to fit a whole interest.

There are may related studies focused on consensus mechanism. Badertscher et al. [3] put forth the first global universally composable (GUC) treatment of PoS-based blockchains in a setting that captures arbitrary numbers of parties that may not be fully operational (i.e., dynamic availability, which naturally captures decentralized environments within which real-world deployed blockchain protocols are assumed to operate). They proposed a new PoS-based protocol called "Ouroboros Genesis" which enables new or offline parties to safely (re-)join and bootstrap their blockchain from the genesis block without any trusted advice (such as checkpoints) or assumptions regarding past availability. With the model allowing adversarial scheduling of messages in a network with delays and captures the dynamic availability of participants in the worst case, the authors proved the GUC security of Ouroboros Genesis against a fully adaptive adversary controlling less than half of the total stake. Kiffer et al. [16] developed a simple Markov-chain based method for analyzing consistency properties of blockchain protocols. This method could be used to address a number of basic questions about consistency of blockchains such as providing a tighter guarantee on the consistency property of Nakamoto's protocol, analyzing a family of delaying attacks and extending them to other protocols, giving the first rigorous consistency analysis of GHOST, and so on. Wan et al. [56] presented a novel hybrid consensus protocol named Goshawk, in which a two-layer chain structure with two-level PoW mining strategy and a ticket-voting mechanism are elaborately combined. They showed that Goshawk is the first blockchain protocol with three key properties such as high efficiency, strong robustness against 51

Pass et al. [42] proposed a new paradigm called Thunderella for achieving state machine replication by combining a fast, asynchronous path with a (slow) synchronous "fall-back" path. With this paradigm, they provided a new resilient blockchain protocol (for the permissionless setting) assuming only that a majority of the computing power is controlled by honest players, and optimistically, transactions could be confirmed as fast as the actual message delay in the network if 3/4 of the computing power is controlled by honest players, and a special player called the accelerator is honest. Daian et al. [4] presented a provably secure proof-of-stake protocol called Snow White. As a matter of fact, Snow White was publicly released in 2016. It provides a formal, end-to-end proof of a proof-of-stake system in a truly decentralized, open-participation network. The authors identified a core “permissioned” consensus protocol suitable for proof-of-stake, and proposed a robust committee re-election mechanism such that as stake switches hands, the consensus committee can evolve in a timely manner and always reflect the most recent stake distribution. They also introduced a formal treatment of costless simulation issue and gave both upper- and lower-bounds that characterize exactly what setup assumptions are needed to resist costless simulation attacks.

2.2 Related Work

In real-world applications, a separate IDS often has no information about its deployed and protected environment, opening a chance for attackers and cyber-criminals. Due to the lack of contextual information, it becomes very hard for an IDS to figure out complicated attacks. Focus on this issue, there is a great need for building a distributed system or collaborative network to enhance the detection performance [59].

Distributed systems. Distributed systems have been widely used in various domains over many years. For example, Prras et al. [43] introduced EMERALD (Event Monitoring Enabling Responses to Anomalous Live Disturbances) in 1997, which aimed to monitor malicious behaviors across different layers in a large network. It can model distributed high-volume events and correlate them using traditional IDS techniques. Snapp et al. [46] presented a distributed Intrusion Detection System (DIDS), which could improve the monitoring process with data reduction method and centralized data analysis. Then, COSSACK system [41] was developed to reduce the impact of DDoS attack, which could work without the support and inputs from humans, i.e., it could generate rules and signatures in an automatic way. Then, DOMINO (Distributed Overlay for Monitoring InterNet Outbreaks) [61] was proposed, aiming to enhance the collaboration process among different nodes. They particularly used an overlay design to achieve a heterogeneous, scalable, and robust mechanism. PIER [14] was an Internet-scale query engine and a kind of querying-based system. It could help distribute dataflows and queries in a better way.

Collaborative intrusion detection. A collaborative system encourages an IDS node to collect and exchange information with other nodes. Li *et al.* [18] found that most distributed intrusion detection architectures could not be scalable under different communication mechanisms. Thus, they proposed a distributed detection system by means of a decentralized routing infrastructure. However, one big limitation is that all nodes in their approach should be intra trusted. This may lead to insider attacks, which are one common threat for various distributed systems and collaborative networks.

To protect distributed / collaborative systems against insider attacks, it is very important to design suitable trust mechanisms to measure the reputation in such systems and networks. As an example, a overlay IDS was proposed by Duma *et al.* [5], which could identify insider attacks. It consists of a trust-aware engine for correlating alarms and an adaptive trust mechanism for handling trust. Then

Tuan [53] applied game theory to help enhance the detection performance in a P2P network. They found that if a trust system was not incentive compatible, the more numbers of nodes in the system, the less likely that a malicious node would be identified.

Fung *et al.* [8] proposed a kind of challenge-based CIDNs, which could evaluate the trustworthiness of an IDS node based on the received answers to the challenges. They first proposed a collaboration framework for host-based IDSs with a forgetting factor, which can emphasize on the recent behavior of a node. To enhance such challenge mechanisms, Li *et al.* [19] claimed that IDS nodes may have different sensitivity levels in identifying particular intrusions. Then they proposed a concept of *intrusion sensitivity (IS)* that measures the detection sensitivity of an IDS for a particular intrusion. They also designed an *intrusion sensitivity-based trust management model* [20] that could automatically allocate the values by using machine learning classifiers like KNN classifier [34]. They also performed a study to investigated the effect of intrusion sensitivity on detecting pollution attacks, where a set of malicious nodes collaborate to affect alert rankings by offering untruthful information [21]. They indicated that *IS* can help decrease the reputation of malicious nodes quickly. Other related work regarding how to improve the performance of intrusion detection can refer to [6, 7, 30–33, 36, 37, 57].

Blockchain-based intrusion detection. The application of blockchains in the field of intrusion detection has been studied, but it is still an emerging topic. Alexopoulos *et al.* [1] described a framework to show how to combine a blockchain with a CIDS. They considered a set of raw alarms produced by each IDS as transactions in a blockchain. Then, all collaborating nodes could use a consensus protocol to ensure the transaction validity before delivering them in a block. This can make sure that the stored alarms are tamper resistant in the blockchain. The major limitation is that they did not provide any results or implementation detail.

Then Meng *et al.* [38] provided the first review regarding the intersection of blockchains and intrusion detection, and introduce the potential application of such combination. They indicated that blockchains can help enhance an IDS in the aspects of data sharing, trust computation and alarm exchange. For anomaly detection, Golomb *et al.* [13] described a framework called CIoTA, which could apply blockchains to perform anomaly detection in a distributed manner for IoT devices. by contrast, Li et al. [26] demonstrated how to use blockchains to enhance the performance of collaborative signature-based IDSs via building a verifiable rule database. On the other hand, some studies investigated how an IDS can help protect blockchain applications. Steichen *et al.* [50] introduced an OpenFlow-based firewall named ChainGuard, which could help protect blockchain-based SDN and identify malicious traffic and behavior in the network.

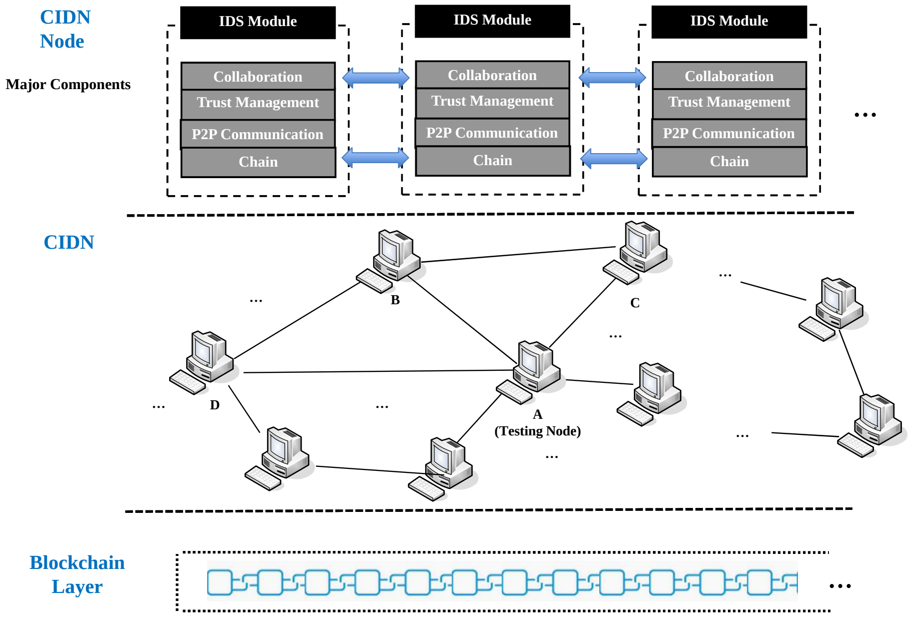

Fig. 2. Blockchained challenge-based CIDN framework: a high-level review.

3 Our Proposed Framework

As discussed above, there are already some studies investigating the intersection of collaborative intrusion detection and blockchains. While most of them (e.g., [1]) focused on a generic CIDS without considering a particular trust mechanism. In practice, the implementation of blockchains may depend on the specific types of trust mechanisms. In this section, we propose a blockchain-based framework for challenge-based CIDNs particularly.

3.1 Framework Design

Fig. 2 shows the high-level framework of blockchained challenge-based CIDNs. Under a CIDN, an IDS module is a basic component. There are some more major components: *collaboration component*, *trust management component*, *P2P communication*, and *chain component*.

- *Collaboration component* is mainly responsible for assisting a node in computing the trust values of another node by sending out *normal requests* or *challenges*, and receiving the relevant *feedback*. This component can help a tested node deliver its feedback when receiving a request or challenge. For instance, Fig. 1 shows that when node A sends a *request* or *challenge* to node B, it can receive relevant feedback.

- *Trust management component* is responsible for evaluating the reputation of other nodes via a specific trust approach. Challenge-based mechanism is a kind of trust approach that computes the trust values through comparing the received feedback with the expected answers. Each node can send out either normal requests or challenges for alert ranking (consultation). To further protect challenges, the original work [8] assumed that challenges should be sent out in a random manner and in a way that makes them difficult to be distinguished from a normal alarm ranking request.
- *P2P communication.* This component is responsible for connecting with other IDS nodes and providing network organization, management and communication among IDS nodes.
- *Chain component.* This component aims to connect the node with the blockchain, i.e., uploading information, voting and receiving decisions.

Blockchain layer. This layer makes the framework different from traditional CIDN frameworks, by allowing to establish a consortium blockchain. A separate layer can facilitate the migration from the traditional framework to our blockchain-based framework, without the need of changing the infrastructure much. This framework is also workable under both signature-based and anomaly-based detection. That is, this layer provides an interface for both detection approaches to connect with blockchains. Taking malicious feedback as an example, each chain node can check and share the suspicious feedback to the chain, and other chain nodes can help verify the feedback. This can help either build a trusted rule database [26] or enhanced profile [13].

In such network, every IDS node can select its own partners according to defined policies, and maintain a list called *partner list.* When a node wants to join the CIDN, it first has to apply and get a unique proof of identity (e.g., a public and a private key pair) via a trusted certificate authority (CA). As depicted in Fig. 1, if node B asks for joining the network, it has to send a request to a CIDN node, say node A. Then, node A makes a decision and sends back an initial *partner list*, if node C is accepted. A CIDN node can typically send two types of messages: *challenge* and *normal request.*

- A *challenge* mainly contains a set of IDS alarms, where a testing node can send these alarms to the tested nodes for labeling alarm severity. Because the testing node knows the severity of these alarms in advance, it can judge and compute the satisfaction level for the tested node, based on the received feedback.
- A *normal request* is sent by a node for alarm aggregation, which is an important feature of collaborative networks in improving the detection performance of a single detector. The aggregation process usually only considers the feedback from highly trusted nodes. As a response, an IDS node should send back alarm ranking information as their feedback.

3.2 Trust Management

Node expertise. In this work, we consider three expertise levels for an IDS node as low (0.1), medium (0.5) and high (0.95). The expertise of an IDS can be using a beta function described as below:

$$\begin{aligned} f(p'|\alpha,\beta) &= \frac{1}{B(\alpha,\beta)} p'^{\alpha-1}(1-p')^{\beta-1} \\ B(\alpha,\beta) &= \int_0^1 t^{\alpha-1}(1-t)^{\beta-1}dt \end{aligned} \tag{1}$$

where $p'(\in[0,1])$ is the probability of intrusion examined by the IDS. $f(p'|\alpha,\beta)$ means the probability that a node with expertise level l responses with a value of p' to an intrusion examination of difficulty level $d(\in[0,1])$. A higher value of l means a higher probability of correctly identifying an intrusion while a higher value of d means that an intrusion is more difficult to detect. In particular, α and β can be defined as [9]:

$$\begin{aligned} \alpha &= 1 + \frac{l(1-d)}{d(1-l)} r \\ \beta &= 1 + \frac{l(1-d)}{d(1-l)} (1-r) \end{aligned} \tag{2}$$

where $r \in \{0,1\}$ is the expected result of detection. For a fixed difficulty level, the node with higher level of expertise can achieve higher probability of correctly detecting an intrusion. For example, a node with expertise level of 1 can accurately identify an intrusion with guarantee if the difficulty level is 0.

Node Trust Evaluation. To measure the reputation of a target node, a testing node can deliver *challenges* via a random generation process. Then the testing node can calculate a score to indicate the satisfaction. According to [8], we can evaluate the reputation of a node i according to node j as follows:

$$T_i^j = (w_s \frac{\sum_{k=0}^n F_k^{j,i} \lambda^{tk}}{\sum_{k=0}^n \lambda^{tk}} - T_s)(1-x)^d + T_s \tag{3}$$

where $F_k^{j,i} \in [0,1]$ is the score of the received feedback k and n is the total number of feedback. λ is a *forgetting factor* that assigns less weight to older feedback response. w_s is a *significant weight* depending on the total number of received feedback, if there is only a few feedback under a certain minimum m, then $w_s = \frac{\sum_{k=0}^n \lambda^{tk}}{m}$, otherwise $w_s = 1$. x is the percentage of "don't know" answers during a period (e.g., from $t0$ to tn). d is a positive incentive parameter to control the severity of punishment to "don't know" replies. More details about equation derivation can be referred to [8].

Satisfaction Evaluation. Intuitively, satisfaction can be measured between an expected feedback ($e \in [0,1]$) and an actual received feedback ($r \in [0,1]$). In addition, we can construct a function F ($\in [0,1]$) to derive the satisfaction score as follows [8, 9]:

$$F = 1 - (\frac{e-r}{max(c_1 e, 1-e)})^{c_2} \quad e > r \tag{4}$$

$$F = 1 - (\frac{c_1(r-e)}{max(c_1 e, 1-e)})^{c_2} \quad e \leq r \tag{5}$$

where c_1 controls the degree of penalty for wrong estimates and c_2 controls satisfaction sensitivity. A large c_2 means more sensitive. In this work, we set $c_1 = 1.5$ and $c_2 = 1$ based on the simulation in [9].

In combination with blockchains. The blockchained challenge-based CIDN can be treated as a consortium blockchain, as each node should be verified by a *CA* and get their key pair. It is a key to enhance the robustness of trust computation by measuring the received feedback. In this case, we can submit the received feedback to the chain for verification. If it is not passed, then the feedback can be considered as a suspicious one.

3.3 Alarm Aggregation

Alarm aggregation is a critical process, which can help a CIDS / CIDN make a decision. Intuitively, a node performing the process can request the alarm rankings from other trusted nodes in its *partner list.* For instance, node j can aggregate the feedback $R_j(a)$ from others, and make a decision, e.g., the aggregated ranking of alert a, by using a weighted majority method as below.

$$R_j(a) = \frac{\sum_{T \geq r} T_i^j D_i^j R_i(a)}{\sum_{T \geq r} T_i^j D_i^j} \tag{6}$$

where $R_i(a)(\in [0,1])$ indicates the aggregated ranking of alert a by node i, r means a trust threshold that node j only accepts the alarm ranking from those nodes whose reputation is higher than this threshold. $T_i^j(\in [0,1])$ indicates the reputation of node i according to node j. $D_i^j(\in [0,1])$ describes how many *hops* between these two nodes.

In combination with blockchains. The alarm aggregation is a critical process in CIDNs, in which an IDS node decides whether there is an intrusion or not. In real-world applications, some malicious nodes may have high reputation at first (e.g., betrayal nodes) and can send untruthful alarm feedback. To avoid the negative impact, the blockchained challenge-based CIDN can submit the received alarm ranking to the chain for validation. If any suspicious clues are found, then the received alarm feedback can be discarded.

4 Evaluation: A Case Study

In this section, as a first study, our purpose is to evaluate the initial performance of our framework in a simulated environment, where malicious nodes could perform an advanced collusion attack, called random poisoning attack [35]. It enables malicious nodes making untruthful feedback in a possibility. In practice, the possibility can be tuned according to the requirements from different environments and networks. The simulated environment contains 50 nodes that are randomly distributed in a 12×12 grid region. We deployed an IDS, e.g., Snort [49] and Zeek [62] in each node, and all IDS nodes can find their own partners after communicating with others within a time period. The consortium blockchain was deployed in a mid-end computer with Intel(R) Core (TM)i6, CPU 2.5GHz with 100 GB storage.

To evaluate the trustworthiness of partner nodes, each node can send out challenges randomly to its partners with an average rate of ε. There are two levels of request frequency: ε_l and ε_h. For the nodes that have a unclear trust value around the threshold, the frequency should be set as high ε_h. The detailed parameters are shown in Table 1. All the settings are maintained similar to relevant work [8, 20, 24].

Table 1. Parameter settings in the experiment.

Parameters	Value	Description
λ	0.9	Forgetting factor
m	10	Lower limit of received feedback
d	0.3	Severity of punishment
ε_l	10/day	Low request frequency
ε_h	20/day	High request frequency
r	0.8	Trust threshold
T_s	0.5	Trust value for newcomers

Trust evaluation under attack. We randomly selected three expert nodes to perform the random poisoning attack. A malicious node under random poisoning attack enjoys a possibility of 1/2 in sending out malicious feedback. Fig. 3 depicts the reputation of malicious nodes under both traditional framework and our blockchain-based framework.

- It is observed that the trustworthiness of malicious nodes could be reduced faster under our framework than that under the traditional framework. This is because traditional framework cannot identify all malicious feedback nodes as the malicious nodes only behave untruthfully with a possibility.
- By contrast, our framework leverages the application of blockchains and each feedback could be verified by all chain nodes. This can greatly increase the successful rate of detecting malicious feedback. Thus, our framework can decrease the reputation of malicious nodes in a fast manner.

Alarm aggregation under attack. Similarly, we also selected three expert nodes randomly to deliver false alarm rankings to a node that performs alarm

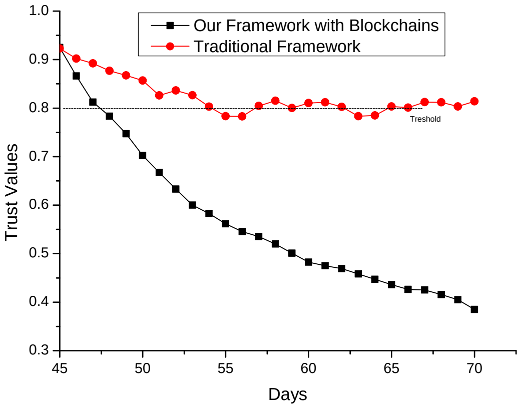

Fig. 3. The trust values of malicious nodes: under traditional and our framework.

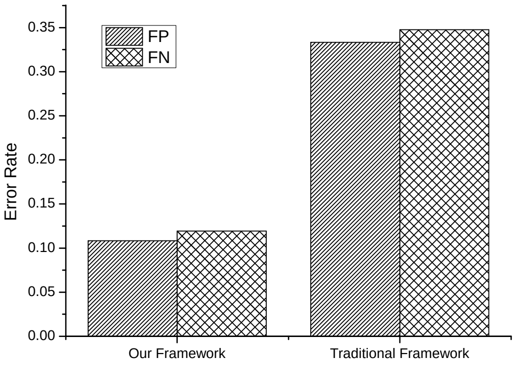

Fig. 4. Classification errors during the alarm aggregation process.

aggregation. We mainly consider a false negative (FN) rate and a false positive (FP) rate. Fig. 4 shows the errors of alarm aggregation under both traditional framework and our framework.

- It is found that the errors under the traditional framework are generally high with FN=33.3% and FP=34.8%. This is because as the traditional framework cannot identify malicious nodes efficiently, e.g., under the random poisoning attack, so that these malicious nodes could still make a negative impact on the alarm aggregation.
- In the comparison, our framework could reduce the error rates significantly, i.e., with FN=10.8% and FP=11.9%. There are two major reasons. One is that our framework can help identify malicious nodes in a quick manner, e.g., under the random poisoning attack. Also, in our framework, the received alarm rankings can be submitted to the chain for verification, and it is easier to detect untruthful inputs, even from trusted nodes, i.e., betrayal nodes.

Overall, our study indicates that our framework can enhance the robustness of challenge-based CIDNs in the aspects of both trust management and alarm aggregation, through integrating with blockchains.

5 Discussion and Challenges

Though blockchain technology can bring a lot of benefits, it is still at a developing, which may suffer many challenges from both inside and outside [38].

- *Energy and cost.* The computational power is a concern for blockchain applications in real-world scenarios. For example, Proof of Work (PoW) may require huge amounts of energy while doing bitcoin mining, where the electricity consumption could rise to 7.7GW by the end of 2018, which is almost half a percent of the world's electricity consumption.

- *Security and privacy.* Though Bitcoin has been widely adopted, it does not mean that it is safe. There are existing some types of attacks. Taking eclipse attack as an example, as the chain nodes have to keep constant communication to compare data, an attacker can fool it into accepting false data if he / she has successfully compromised that node [40]. This results in wasting network resources or accepting fake transactions. There is a need to enhance the security of blockchain itself.
- *Complexity and speed.* Blokchain is a complex system that is hard to be established from scratch. A single mistake may cause the whole system to be compromised. Due to the complexity, it also suffers data storage and transaction speed issues. As a study, we only tried a proof-of-concept chain to investigate the performance. It is an important topic to exploit the performance when the blockchain runs for a while.
- *Blockchain size.* In the beginning of a blockchain, the node number may be in a small scale, which makes it vulnerable to many attacks during the growth. For instance, assume there are only 30 nodes, if a single entity successfully controls just or more than 51 percent of the blockchain nodes, then it has a high probability to control the whole outputs.

6 Conclusion

Challenge-based Collaborative intrusion detection provides a promising solution to safeguard assets from being compromised; however, it may still be vulnerable to advanced attacks in practical deployment. Motivated by the fast development of blockchains, in this work, we propose a blockchained challenge-based CIDN framework by leveraging the benefits offered by the blockchain technology. Our framework enables nodes to form a consortium chain and improve the robustness of challenge-based CIDNs. In the evaluation, our results demonstrate that our framework can enhance the robustness in the aspects of trust management by detecting advanced malicious nodes, and alarm aggregation through identifying untruthful inputs and reducing error rates.

Acknowledgments. This work was funded by the National Natural Science Foundation of China (NSFC) Grant No. 61772148, 61802080 and 61802077.

References

1. Alexopoulos, N., Vasilomanolakis, E., Ivanko, N.R., Muhlhauser, M.: Towards blockchain-based collaborative intrusion detection systems. In: Proceedings of the 12th International Conference on Critical Information Infrastructures Security, pp. 1-12 (2017)
2. Amazon Managed Blockchain: Easily create and manage scalable blockchain networks. (accessed on 10 April 2019).
`https://aws.amazon.com/managed-blockchain/`

3. Badertscher, C., Gazi, P., Kiayias, A., Russell, A., Zikas, V.: Ouroboros Genesis: Composable Proof-of-Stake Blockchains with Dynamic Availability. In: Proceedings of ACM Conference on Computer and Communications Security (CCS), pp. 913-930 (2018)
4. Daian, P., Pass, R., Shi, E.: Snow White: Robustly Reconfigurable Consensus and Applications to Provably Secure Proofs of Stake. Financial Cryptography and Data Security (FC), 2019.
5. Duma, C., Karresand, M., Shahmehri, N., Caronni, G.: A Trust-Aware, P2P-Based Overlay for Intrusion Detection. In: DEXA Workshop, pp. 692–697 (2006)
6. Fadlullah, Z.M.,Taleb, T.,Vasilakos, A.V.,Guizani, M.,Kato, N.: DTRAB: combating against attacks on encrypted protocols through traffic-feature analysis. IEEE/ACM Transactions on Networking, vol. 18, no. 4, pp. 1234-1247 (2010)
7. Friedberg, I., Skopik, F., Settanni, G., Fiedler, R.: Combating advanced persistent threats: From network event correlation to incident detection. Computers & Security, vol 48, pp. 35-47 (2015)
8. Fung, C.J., Baysal, O., Zhang, J., Aib, I., Boutaba, R.: Trust Management for Host-Based Collaborative Intrusion Detection. In: De Turck, F., Kellerer, W. Kormentzas, G. (eds.): DSOM 2008, LNCS 5273, pp. 109–122 (2008)
9. Fung, C.J.; Zhu, Q., Boutaba, R., Basar, T.: Bayesian Decision Aggregation in Collaborative Intrusion Detection Networks. In: NOMS, pp. 349–356 (2010)
10. Almost half of companies still can't detect IoT device breaches, reveals Gemalto study (accessed on 10 April 2019). `https://www.gemalto.com/press/Pages/Almost-half-of-companies-still-can-t-detect-IoT-device-breaches-reveals-Gemalto-study.aspx`
11. Leading the IoT: Gartner Insights on How to Lead in a Connected World (accessed on 22 March 2019). `https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf`
12. Gartner Identifies Top 10 Strategic IoT Technologies and Trends (accessed on 22 March 2019). `https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends`
13. Golomb, T., Mirsky, Y., Elovici, Y.: CIoTA: Collaborative IoT Anomaly Detection via Blockchain. In: Proceedings of workshop on Decentralized IoT Security and Standards (DISS), pp. 1-6 (2018)
14. Huebsch, R., Chun, B.N., Hellerstein, J.M., Loo, B.T., Maniatis, P., Roscoe, T., Shenker, S., Stoica, I., Yumerefendi, A.R.: The Architecture of PIER: an Internet-Scale Query Processor. In: Proceedings of the 2005 Conference on Innovative Data Systems Research (CIDR), pp. 28–43 (2005)
15. Hyperledger C Open Source Blockchain Technologies. `https://www.hyperledger.org/`
16. Kiffer, L., Rajaraman, R., Shelat, A.: A Better Method to Analyze Blockchain Consistency. In: Proceedings of ACM Conference on Computer and Communications Security (CCS), pp. 729-744 (2018)
17. Lei, A., Cruickshank, H.S., Cao, Y., Asuquo, P.M., Ogah, C.P.A., Sun, Z.: Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems. IEEE Internet of Things Journal 4(6), pp. 1832-1843 (2017)
18. Li, Z., Chen, Y., Beach, A.: Towards Scalable and Robust Distributed Intrusion Alert Fusion with Good Load Balancing. In: Proceedings of the 2006 SIGCOMM Workshop on Large-Scale Attack Defense (LSAD), pp. 115–122 (2006)
19. Li, W., Meng, Y., Kwok, L.-F.: Enhancing Trust Evaluation Using Intrusion Sensitivity in Collaborative Intrusion Detection Networks: Feasibility and Challenges.

In: Proceedings of the 9th International Conference on Computational Intelligence and Security (CIS), pp. 518–522, IEEE (2013)

20. Li, W., Meng, Y., Kwok, L.-F.: Design of Intrusion Sensitivity-Based Trust Management Model for Collaborative Intrusion Detection Networks. In: Proceedings of the 8th IFIP WG 11.11 International Conference on Trust Management (IFIPTM), Springer, pp. 61-76 (2014)
21. Li. W., Meng, W.: Enhancing Collaborative Intrusion Detection Networks Using Intrusion Sensitivity in Detecting Pollution Attacks. Information and Computer Security 24(3), pp. 265-276, Emerald (2016)
22. Li, L., Liu, J., Cheng, L., Qiu, S., Wang, W., Zhang, X., Zhang, Z.: CreditCoin: A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles. IEEE Trans. Intelligent Transportation Systems 19(7), pp. 2204-2220 (2018)
23. Li, W., Meng, W., Kwok, L.F., Ip, H.H.S.: PMFA: Toward Passive Message Fingerprint Attacks on Challenge-based Collaborative Intrusion Detection Networks. In: Proceedings of the 10th International Conference on Network and System Security (NSS 2016), pp. 433-449 (2016)
24. Li, W., Meng, W., Kwok, L.F.: SOOA: Exploring Special On-Off Attacks on Challenge-Based Collaborative Intrusion Detection Networks. In: Proceedings of GPC, pp. 402-415 (2017)
25. Li, W., Meng, W., Kwok, L.-F.: Investigating the Influence of Special On-Off Attacks on Challenge-based Collaborative Intrusion Detection Networks. Future Internet, vol. 10, no. 1, pp. 1-16 (2018)
26. Li, W., Tug, S., Meng, W., Wang, Y.: Designing Collaborative Blockchained Signature-based Intrusion Detection in IoT environments. Future Generation Computer Systems, In Press, Elsevier.
27. Li, W., Kwok, L.-F.: Challenge-based Collaborative Intrusion Detection Networks under Passive Message Fingerprint Attack: A Further Analysis. Journal of Information Security and Applications, In press, Elsevier.
28. Makhdoom, I., Abolhasan, M., Abbas, H., Ni, W.: Blockchain's adoption in IoT: The challenges, and a way forward. Journal of Network and Computer Applications 125, pp. 251-279 (2019)
29. Marr, B.: 5 Blockchain Trends Everyone Should Know About (accessed on 10 April 2019). https://www.forbes.com/sites/bernardmarr/2019/01/28/5-blockchain-trends-everyone-should-know-about/#30c1ab523bb9
30. Meng, Y., Kwok, L.F.: Enhancing False Alarm Reduction Using Voted Ensemble Selection in Intrusion Detection. International Journal of Computational Intelligence Systems, vol. 6, no. 4, pp. 626-638, Taylor & Francis (2013)
31. Meng, Y., Li, W., Kwok, L.F.: Towards Adaptive Character Frequency-based Exclusive Signature Matching Scheme and its Applications in Distributed Intrusion Detection. Computer Networks, vol. 57, no. 17, pp. 3630-3640, Elsevier (2013)
32. Meng, W., Li, W., Kwok, L.-F.: An Evaluation of Single Character Frequency-Based Exclusive Signature Matching in Distinct IDS Environments. In: Proceedings of the 17th International Conference on Information Security (ISC), pp. 465-476 (2014)
33. Meng, W., Li, W., Kwok, L.-F.: EFM: Enhancing the Performance of Signature-based Network Intrusion Detection Systems Using Enhanced Filter Mechanism. Computers & Security, vol. 43, pp. 189-204, Elsevier (2014)
34. Meng, W., Li, W., Kwok, L.-F.: Design of Intelligent KNN-based Alarm Filter Using Knowledge-based Alert Verification in Intrusion Detection. Security and Communication Networks 8(18), pp. 3883-3895, Wiley (2015)

35. Meng, W., Luo, X., Li, W., Li, Y.: Design and Evaluation of Advanced Collusion Attacks on Collaborative Intrusion Detection Networks in Practice. In: Proceedings of the 15th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2016), pp. 1061-1068 (2016)
36. Meng, W., Li, W., Xiang, Y., Choo, K.K.R.: A Bayesian Inference-based Detection Mechanism to Defend Medical Smartphone Networks Against Insider Attacks. Journal of Network and Computer Applications, vol. 78, pp. 162-169, Elsevier (2017)
37. Meng, W., Li, W., Kwok, L.-F.: Towards Effective Trust-based Packet Filtering in Collaborative Network Environments. IEEE Transactions on Network and Service Management, vol. 14, no. 1, pp. 233-245 (2017)
38. Meng, W., Tischhauser, E.W., Wang, Q., Wang, Y., Han, J.: When Intrusion Detection Meets Blockchain Technology: A Review. IEEE Access, vol. 6, no. 1, pp. 10179-10188 (2018)
39. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. `http://bitcoin.org/bitcoin.pdf` (2008)
40. Orcutt, M.: How secure is blockchain really? (accessed on 22 March 2019) `https://www.technologyreview.com/s/610836/how-secure-is-blockchain-really/`
41. Papadopoulos, C., Lindell, R., Mehringer, J., Hussain, A., Govindan, R.: COSSACK: Coordinated Suppression of Simultaneous Attacks. In: Proceedings of the 2003 DARPA Information Survivability Conference and Exposition (DISCEX), pp. 94–96 (2003)
42. Pass, R., Shi, E.: Thunderella: Blockchains with Optimistic Instant Confirmation. In: Proceedings of the 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 3-33 (2018)
43. Porras, P.A., Neumann, P.G.: Emerald: Event Monitoring Enabling Responses to Anomalous Live Disturbances. In: Proceedings of the 20th National Information Systems Security Conference, pp. 353–365 (1997)
44. Roesch, M.: Snort: Lightweight intrusion detection for networks. In: Proceedings of Usenix Lisa Conference, pp. 229-238 (1999)
45. Scarfone, K., Mell, P.: Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication 800-94 (2007)
46. Snapp, S.R., et al.: DIDS (Distributed Intrusion Detection System) - Motivation, Architecture, and An Early Prototype. In: Proceedings of the 14th National Computer Security Conference, pp. 167–176 (1991)
47. Sharma, V.: An Energy-Efficient Transaction Model for the Blockchain-Enabled Internet of Vehicles (IoV). IEEE Communications Letters 23(2), pp. 246-249 (2019)
48. Singh, S., Ra, I.H., Meng, W., Kaur, M., Cho, G.H.: SH-BlockCC: A Secure and Efficient IoT Smart Home Architecture based on Cloud Computing and Blockchain Technology. International Journal of Distributed Sensor Networks, In Press, SAGE.
49. Snort: An an open source network intrusion prevention and detection system (IDS/IPS). Homepage: `http://www.snort.org/`
50. Steichen, M., Hommes, S., State, R.: ChainGuard - A firewall for blockchain applications using SDN with OpenFlow. In: Proceedings of International Conference on Principles, Systems and Applications of IP Telecommunications (IPTComm), pp. 1-8 (2017)
51. Symantec 2019 Internet Security Threat Report (accessed on 22 March 2019). `https://www.symantec.com/security-center/threat-report`
52. Tug, S., Meng, W., Wang, Y.: CBSigIDS: Towards Collaborative Blockchained Signature-based Intrusion Detection. In: Proceedings of The 1st IEEE International Conference on Blockchain (Blockchain) (2018)

53. Tuan, T.A.: A Game-Theoretic Analysis of Trust Management in P2P Systems. In: Proceedings of ICCE, pp. 130–134 (2006)
54. Vasilomanolakis, E., Karuppayah, S., Muhlhauser, M., Fischer, M.: Taxonomy and Survey of Collaborative Intrusion Detection. ACM Computing Surveys 47(4), pp. 55:1-55:33 (2015)
55. Vigna, G.,Kemmerer, R.A.: NetSTAT: A Network-based Intrusion Detection Approach. In: Proceedings of Annual Computer Security Applications Conference (ACSAC), pp. 25-34 (1998)
56. Wan, C., Tang, S., Zhang, Y., Pan, C., Liu, Z., Long, Y., Liu, Z., Yu, Y.: Goshawk: A Novel Efficient, Robust and Flexible Blockchain Protocol. In: Proceedings of Inscrypt, pp. 49-69 (2018)
57. Wang, Y., Meng, W., Li, W., Liu, Z., Liu, Y., Xue, H.: Adaptive Machine Learning-based Alarm Reduction via Edge Computing for Distributed Intrusion Detection Systems. Concurrency and Computation: Practice and Experience, Wiley.
58. Wood, G.: Ethereum: A secure decentralised generalised transaction ledger. EIP-150 Revision (2016)
59. Wu, Y.-S., Foo, B., Mei, Y., Bagchi, S.: Collaborative Intrusion Detection System (CIDS): A Framework for Accurate and Efficient IDS. In: Proceedings of the 2003 Annual Computer Security Applications Conference (ACSAC), pp. 234–244 (2003)
60. Wüst, K., Gervais, A.: Do you need a blockchain? In: CVCBT, pp. 45-54 (2018)
61. Yegneswaran, V., Barford, P., Jha, S.: Global Intrusion Detection in the DOMINO Overlay System. In: Proceedings of the 2004 Network and Distributed System Security Symposium (NDSS), pp. 1-17 (2004)
62. The Zeek Network Security Monitor. `https://www.zeek.org/`