Journal Pre-proof

A blockchain-empowered authentication scheme for worm detection in wireless sensor network

Yuling Chen, Xiong Yang, Tao Li, Yi Ren, Yangyang Long

PII: S2352-8648(22)00056-6

DOI: https://doi.org/10.1016/j.dcan.2022.04.007

Reference: DCAN 396

To appear in: *Digital Communications and Networks*

Received Date: 26 May 2021

Revised Date: 1 April 2022

Accepted Date: 7 April 2022

Please cite this article as: Y. Chen, X. Yang, T. Li, Y. Ren, Y. Long, A blockchain-empowered authentication scheme for worm detection in wireless sensor network, *Digital Communications and Networks* (2022), doi: https://doi.org/10.1016/j.dcan.2022.04.007.

Digital Communications and Networks(DCN)

HOSTED BY

ELSEVIER

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/dcan

A blockchain-empowered authentication scheme for worm detection in wireless sensor network

Yuling Chen[a], Xiong Yang[a,*], Tao Li[a], Yi Ren[b], Yangyang Long[a]

[a]State Key Laboratory of Public Big Data, College of Computer Science and Technology, Guizhou University, Guiyang 550025, China
[b]School of Computing Science, University of East Anglia, Norwich NR5 7TJ, U.K

Abstract

Wireless Sensor Network (WSN) is a distributed sensor network composed a large number of nodes with low cost, low performance and self-management. The special structure of WSN brings both convenience and vulnerability. For example, a malicious participant can launch attacks by capturing a physical device. Therefore, node authentication that can resist malicious attacks is very important to network security. Recently, blockchain technology has shown the potential to enhance the security of the Internet of Things (IoT). In this paper, we propose a Blockchain-empowered Authentication Scheme (BAS) for WSN. In our scheme, all nodes are managed by utilizing the identity information stored on the blockchain. Besides, the simulation experiment about worm detection is executed on BAS, and the security is evaluated from detection and infection rate. The experiment results indicate that the proposed scheme can effectively inhibit the spread and infection of worms in the network.

KEYWORDS:
Wireless sensor network (WSN)
Node authentication
Blockchain
Tangle
Worm detection

1. Introduction

The wireless sensor network is the underlying technology of IoT, which receives more and more attention. WSN is a multi-hop self-organized network formed by abundant sensor nodes deployed in the monitoring area [1, 2], which can collect environmental information and help participants in the decision-making process. WSN eliminates the limitation of cables and realizes wireless communication, so it is widely utilized in environmental monitoring, military monitoring, building security monitoring, medical care, and other fields.

However, the sensor devices are often deployed without protection, which allows attackers to physically capture WSN nodes, read sensor data, and even control nodes for network transmission [3]. For example, the attacker injects self-propagating malicious code (worm-type virus) into the captured node to infect the benign nodes, and finally control the network. To resist worm attacks, an attack detection scheme usually requires the cooperation of two components: firstly, collecting and analyzing the information in the network to detect current attacks; secondly, generating alarms and responding after an attack detected. The optimal response method is to directly move malicious nodes in the WSN network. Scilicet, the nodes register with the identity database to obtain a license, and then the network can manage the nodes by modifying the identity information. So WSN needs a node authentication scheme that only allows legitimate nodes to participate in the network to ensure the effectiveness

of node management capability. Nevertheless, how to secure the identity registry, if the network has already been attacked, is a key challenge.

Recently, blockchain technology has emerged as an ideal approach for secure data storage and distributed computing, which records transactions in the decentralized network in a verifiable and immutable manner [4]. It has the characteristics of decentralization, immutability, transparency, and system autonomy, which can effectively tackle the problems of privacy protection, equipment security, and inter-network cooperation caused by malicious nodes in WSN. To be specific, the identity information for node authentication in WSN can be stored in a decentralized blockchain network, which provides a transparent and secure way to manage data. So blockchain enables mutual trust between different participating nodes in WSN and greatly reduces the cost of reshaping or maintaining trust.

In this paper, we propose a blockchain-enabled node authentication scheme in WSN, which utilizes a new data structure, Trust Relationship Graph (TR-Graph), to store these nodes' identity information in the authentication. In our proposed scheme, the required information can be divided into two parts: traditional authentication information and relationship information. The traditional authentication information includes the nodes' certificates, ID, etc. And the relationship information is the binary relationships of valid nodes and their neighbor nodes. Besides, we construct a blockchain network among sink nodes to store and maintain the TR-Graph. To be specific, we adopt the transitive signature technology to represent the relationship information nodes, and then, the relationship and TR-Graph can be calculated and updated by the sink nodes. Finally, we conduct a comprehensive experiment of worm detection based on our proposed BAS scheme to evaluate the security of the scheme. The experimental results indicate that the proposed scheme effectively limits the spread and infection of worms, and our proposed BAS scheme performs well in node management and attack resistance.

The contributions of this paper are as follows:

1. We propose a new data structure, which is called the TR-Graph, to represent the nodes' identity authentication information. Compared with the traditional identity information, TR-Graph stores the nodes' relationship and enables trusted nodes to save communication interaction.

2. Based on the TR-Graph, we adopt blockchain to store the authentication information and introduce a new network (BAS). And in this network, the sink node authenticates the nodes in the local network domain by the transitive signature and TR-Graph. Therefore, the sink node bears most of the storage and computing overhead required, which makes BAS have the potential to be applied in resource scarcity networks. Besides, The BAS stores and maintains the node's identity authentication information through the Directed Acyclic Graph (DAG) blockchain built by all sink nodes to ensure the security of the scheme.

3. Based on BAS in WSN, worm detection experiments are carried out. The experiment divides the network into multiple independent network domains. Each sink node executes worm detection on the local network domain, and then inter-domain communication and node management are carried out through the blockchain. Meanwhile, we prove the security and application potential of the scheme.

2. Related work

In this section, we review three categories of related works to position our work in the research community.

2.1. Worm detection in WSN

Due to the limited resources of most sensor devices in WSN, traditional worm detection on the Internet is not suitable for WSN. AbuHmed [5] et al. proposed a simple remote code attestation based on software, and Yang [6] et al. proposed a memory attestation to verify the integrity of device hardware; both of them can effectively detect the worm nodes for resource-limited sensor network. Qiang [7] et al. proposed an improved Sequential Probability Ratio Analysis (SPRA) to detect the spread of worms based on the idea of the worm propagation chain.

In the WSN, the communication ability of the node is limited [8], so the infection of malicious code will cause the repeated transmission of data packets. The worm propagation chain is a special communication pattern that means worm infection. If a specific communication pattern is detected, we can dynamically select a threshold to determine whether the network has a worm infection by SPRA.

2.2. Node authentication in WSN

The RPL in 6LoWPAN first provides an authentication [9]: a device may initially join the network using a preconfigured key and the preinstalled security mode, and next obtain a different cryptographic key from a key authority. To strengthen the security of network authentication, Grajal [10] et al. proposed architecture for end-to-end secure communication of IoT devices, which effectively supports ECC-based identity authentication and key agreement. The conclusion of this scheme is that when using low-power sensor platform, even if the additional overhead of the authentication protocol is required, it will be more advantageous to entrust the expensive ECC calculations to more powerful devices. More solutions, which ensure security by complex calculations, have been proposed due to the improvement of resource availability. Wang [11] et al. proposed an efficient multi-factor user authentication protocol, which met various security goals, for real-time data access in WSNs. Lin [12]

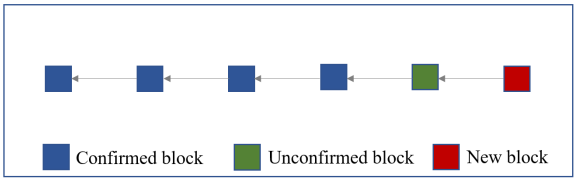


Fig. 1: Schematic diagram of Blockchain

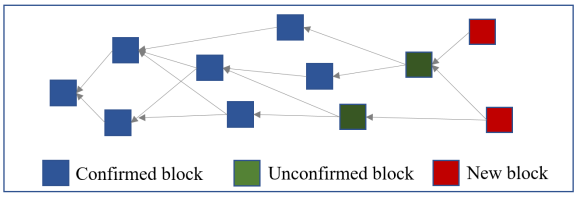


Fig. 2: Schematic diagram of DAG Blockchain

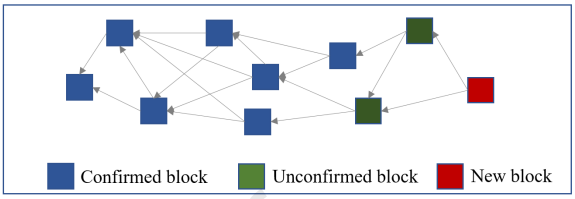


Fig. 3: Schematic diagram of IOTA

et al. proposed an identity management system based on transitive closed undirected graph authentication, which utilized transitive signature technology to authenticate nodes.

Compared with standard digital signatures, transitive signatures can be calculated by a third party [13]. Specifically, suppose there is a graph $G = (V, E)$, a set of nodes $V = \{v_0, v_1, \ldots, v_n\}$, the set of edges $E = V \times V$, the signature of any edge $(v_i, v_{(i+1)})$is denoted as $\sigma_{(i,i+1)}$. Thus, any one can calculate the $\sigma_{(i-1,i+1)}$ as long as they get the $\sigma_{(i-1,i)}$ and $\sigma_{(i,i+1)}$ without knowing the private key of the signer. The transitive signature can solve the problem of efficiency and security of signature in practical applications [14]. For example, Lin [15] et al. proposed a transitive signature algorithm based on the classic RSA algorithm, which was used to authenticate a large number of dynamically growing graphics data. Moreover, the transitive signature can transfer the computational pressure to high-performance nodes in the authentication.

2.3. Integration of blockchain and WSN

Blockchain is a distributed ledger that combines data blocks into a chain data format in chronological order. Nodes in the network layer, without mutual trust, achieve verification through a certain consensus mechanism such as Proof of Work (PoW), Proof of Stake (PoS), and the Practical Byzantine Fault Tolerance algorithm (PBFT). These mechanisms provide solid foundations for the smooth implementation of the contract layer and the application layer [16]. Its structure is shown in Fig.1.

Blockchain provides a new trust model under the open network, enabling system participants to achieve trust under decentralized conditions. To ensure trust and decentralization at the same time, the blockchain must sacrifice the performance of the system. However, lower system throughput will limit the large-scale application of blockchain in commercial activities. The distributed ledger technology based on the DAG is a kind of solution to this problem. It transforms the single-chain structure in the blockchain into a directed acyclic graph structure. DAG avoids the serialization write limitation caused by the single-chain structure, so it has the characteristics of supporting high concurrency, no mining, faster transaction speed, and lower resource consumption [17]. DAG structure is shown in Fig.2.

IOTA is a third-generation shared distributed ledger based on the DAG structure. It calls the special DAG structure it adopts as Tangle. The block in IOTA is a single transaction, and each new block refers to the previous two blocks. IOTA does not reach an immediate consensus. When a transaction involves the first two transactions, it means that the first two transactions have been verified [18]. Therefore, IOTA does not need miners, which avoids mining attacks such as [19, 20]. In IOTA, users can verify the transactions by themselves, and the transaction cost is only the computational cost of verifying the other two transactions [21]. Its structure is shown in Fig.3.

The blockchain is a kind of IoT security solution worthy of in-depth study, it can solve the trust problem between unreliable devices [22]. Hu [23, 24] et al. respectively proposed the attack detection strategies applied to multiple microgrids and the Internet of vehicles. They utilize the Dpos consensus and a multi-layer structure blockchain to safely share detection results. Zhen [25] et al. proposed a distributed privacy protection strategy for wireless body area networks, which leverages the blockchain-based decentralized mobile edge computing paradigm to support efficient transmission of privacy information. For WSN, Feng [26, 27] et al. proposed a new consensus protocol and encryption mechanism, and then constructed a lightweight blockchain to store sensor data in a distributed manner to ensure data security. Zeng [28, 29] et al. adopted the blockchain network to store sensor data efficiently through high-performance nodes and sliding windows. Cui [30] et al. proposed a hybrid blockchain-based identity authentication scheme, which is constructed among different types of nodes, for multi-WSN. For the node management in WSN, Hammi [31] et al. proposed a security authentication mechanism applied to sensor networks, which allowd nodes to migrate among different clusters by blockchain. They then applied the smart contracts to the identity authentication [32], which authenticate the IoT devices by a distributed system called the trust bubble. Shi [33] et al. proposed a blockchain-

empowered authentication scheme in the large-scale heterogeneous network for data security. However, the focus of the above work is on the authentication mechanism, and there is a lack of research on how to build a more suitable blockchain structure and consensus for WSN. BAS saves the communication interaction of authentication through the transitive signature technology, and shortens the consensus cycle of distributed nodes through Tangle. While ensuring the security of cross-domain authentication, it has more application potential than previous scheme.

3. Threat model

We define the worm attack model that satisfies the following assumptions:

Assuming that the sensor network is static, the location of sensor nodes will not change after deployment, and the nodes are bidirectional links, which can communicate with each other. Frequent communication among nodes will reduce network life, so the network always transmits fewer packets. However, the worm detection experiment [34] proves that the worm code needs to send multiple data packets when spreading, so the packet retransmission is the key to worm detection.

Suppose that the nodes captured by at tackers can spread worms in the network. All sensor nodes have only two states: vulnerable or infected. Except for the infected initiator, all sensor nodes are initially vulnerable state. Because of the dense deployment of WSN nodes, each node has enough neighboring nodes that can be transmitted. Attackers usually adopt a hop-by-hop propagation strategy to reduce detection probability.

4. The blockchain-based node authentication scheme in the WSN

We propose a blockchain-based scheme for node authentication in WSN. As shown in Fig.4, the proposed scheme mainly involves five entities: base station, sink node, sensor node, wireless sensor network, and blockchain network, and includes two processes: generation of identity information, and interaction process with blockchain. Next, the introduction of each entity is as follows:

Base station: It mainly provides wireless communication for the network, collects sensor data of the entire network, and connects the wireless sensor network to the external network.

Sink node: Compared with sensor nodes, it has stronger computing and storage capabilities. It is responsible for collecting the sensor data, which is uploaded by sensor nodes in the local network and sent to the base station. Also, the sink node authenticates local sensor nodes through the data that are stored on the blockchain.

Sensor node: It is the basic functional unit of a wireless sensor network, which has low price, low power consumption, and poor performance. Sensor nodes send the data, which is collected from the environment to the sink node through multiple hops by adjacent nodes.

Wireless sensor network: WSN is divided into several local networks, and each local network has a sink node and several sensor nodes. The sensor nodes collect the physical information in real-time and send it to the sink nodes. Sink nodes converge and fuse local sensor information and send it to the base station.

Blockchain network: A special blockchain structure, called Tangle, is utilized to store the identity information of the nodes. All sink nodes participate in the blockchain network and publish the blocks, including the nodes' identity information, to the blockchain for storage after the consensus. During the authentication, sink nodes periodically update the local TR-Graph by the identity information from the Tangle.

4.1. Generation of identity information

Two types of identity information, which include nodes' certificates and the relationships among nodes, are required for the BAS. Therefore, we propose the TR-Graph to store the identity information of nodes. The TR-Graph is denoted as $G = (V, E)$, which is an undirected graph, where V is a set of finite points; $E \in V \times V$ is a set of finite edges. The point v represents the trusted entity sensor node in WSN, including the unique ID (UID), the certificate (Σ), etc. The edge (u, v) corresponds to the trusted relationship between the two nodes, which is a transitive signature ($Sign$). The details are as follows:

1) Certificates: Each sensor node in WSN registers with the sink node through its UID. The legal node in WSN is described as $N = \{1, \ldots, n, \ldots N\}$. Then, each legal node will obtain its own key pair and private label as $\{PK_n, SK_n, \lambda_i\}$ from the sink node, where the public key PK_n is open to the entire network, and the private key SK_n and private label λ_i are secretly stored by the node itself. Next, the sink node calculates $w_n = Sig_{(SK_{SN})}(UID_n \| PK_n)$ as the public label of node n, where $Sig(.)$ is the standard digital signature algorithm, and SK_{SN} is the private key of the sink node; Finally, $\sigma_n = Sig_{(SK_n)}(\lambda_n \| w_n)$ is calculated as the standard signature of n; the certificate $\Sigma_n = (\lambda_n, w_n, \sigma_n)$ is generated for n.

2) Relation signature: The legal node with the key pair can write signature. If node m is in the neighbor routing table of node n, and the registration of m is completed through the transfer of n, then n can sign a transitive signature on the relation between the two nodes:

$$Sign_{(n,m)} = TSig(SK_n, \Sigma_n, \Sigma_m) \tag{1}$$

$TSig(.)$ is a transitive signature algorithm. The signature will be uploaded to the sink node. Based on the

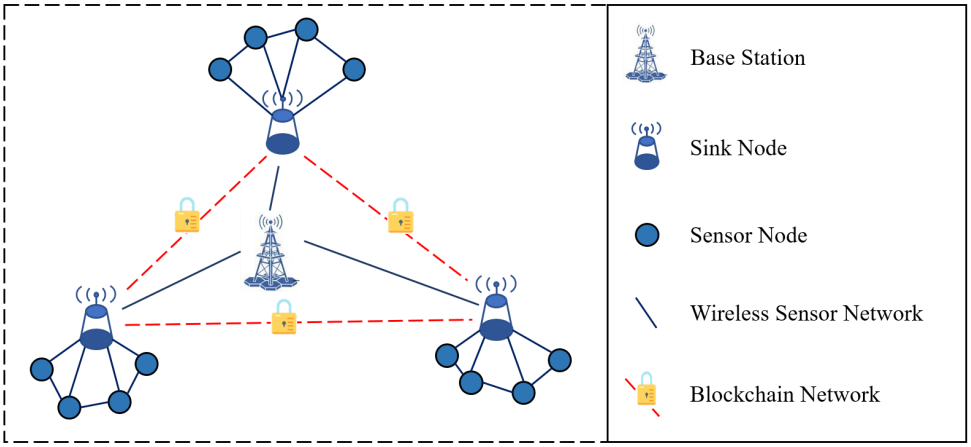


Fig. 4: System model of BAS

characteristics of the transitive signature technology, the sink node can verify the signature:

$$\{0,1\}TVer \leftarrow (pk_n, Sign_{(i,j)}) \tag{2}$$

$TVer(.)$ is a verification algorithm for transitive signature. The algorithm will verify whether the signature is legal and return 1 or 0. The sink node can also synthesize two signatures that have transitive relation:

$$Sign_{(n,k)} = Comp(Sign_{(n,m)}, Sign_{(m,k)}) \tag{3}$$

$Comp(.)$ is a synthesis algorithm for transitive signature, which combines two transitive signatures and returns a synthesized signature.

The purpose of additional storage, which is the trust relationship among nodes, is to save the communication overhead when nodes authenticate each other. For the traditional authentication scheme, when node A wants to communicate with node B, A needs to confirm the identity information of the B through a Certificate Authority (CA). Then A first encrypts the transmitted data with the B's public key and then encrypts it with its private key. Through the above method, the two nodes can authenticate each other and negotiate a session key for communication. But for the BAS that additionally stores the trust relationship, the communication between trusted nodes can omit key negotiation and communicate through a constant session key. Therefore, the scheme can save the communication interaction of mutual authentication between nodes.

4.2. Interaction process

Fig.5 describes the interaction process between nodes and blockchain in BAS. The process is divided into two stages: registration stage and authentication stage.

In the registration phase, the sink node submits the identity information of the legal nodes to the blockchain network: First, sensor node A sends a registration request to the sink node (step 1); the sink node verifies the legitimacy of the node through the request containing a device's inherent message. The legitimate nodes obtain their keys (step 2); Node A signs a transitive signature on the relationship between itself and neighbors nodes (step 3); The sink node verifies the previous block according to the Tips (step 4); The sink node packages the identity information of node A into a block, which quotes the blocks in the List, and publishes it(step 5).

In the authentication phase, the sink node periodically generates a local TR-Graph according to the blockchain: First, the sink node downloads the information, which is about the local network, on the blockchain (step 6); The sink node calculates the downloaded information into the TR-Graph, then calls it directly during the authentication (step 7); Sensor node B sends an authentication request to the sink node (step 8); The sink node responds to the request of the B according to TR-Graph (step 9).

The sink node undertakes most of the work of BAS. On the one hand, it acts as a registration agency, reviews the registration requests of nodes, distributes keys to legitimate nodes, and submits the node's identity information to the blockchain; on the other hand, it also acts as a certification authority, regularly downloads identity information from the blockchain, and updates the local TR-Graph to authenticate local nodes. The maintenance process is divided into parts, including storing identity information on the blockchain and downloading it to update the TR-Graph.

4.2.1. Update the blockchain

All sink nodes in BAS are the participants of the blockchain, which chooses the Tangle for data storage. The consensus mechanism of Tangle is that every new transaction needs to verify the first two unconfirmed transactions and quote them. Verification means that the sink node checks the previous block content (node identification and signature) in BAS. Then, the sink nodes packages the new information and quote the

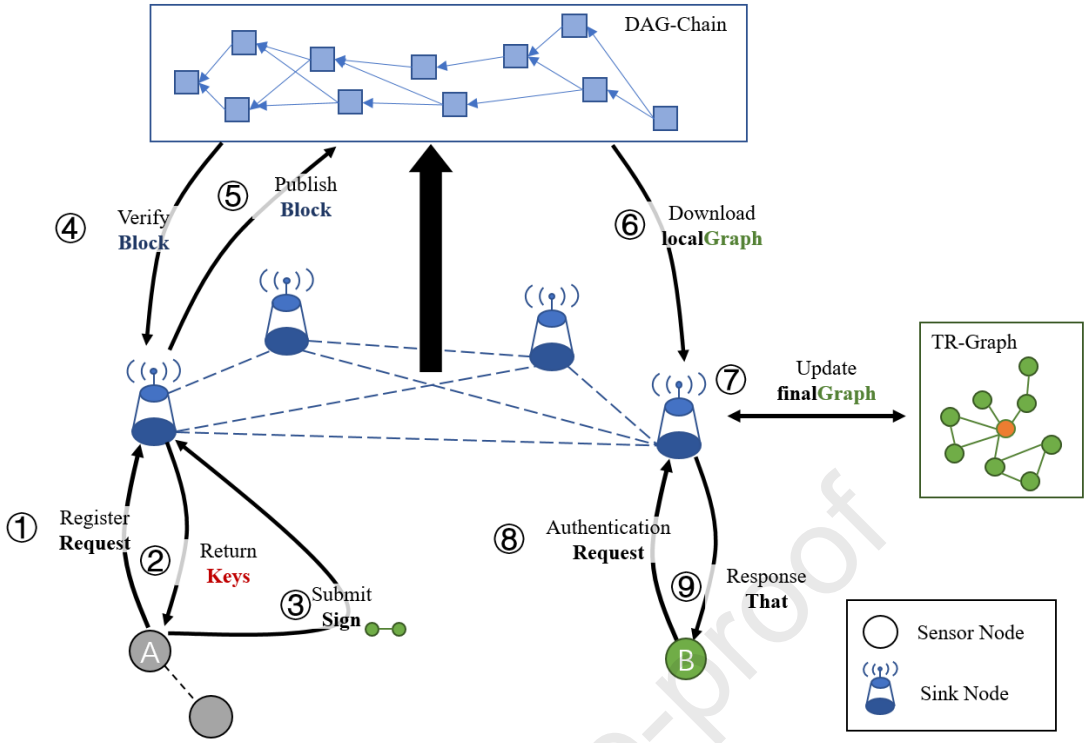


Fig. 5: Interaction process in BAS

verified blocks. The uploading identity information to the blockchain is described as follows:

1) Verify transaction: The sink node firstly visits its $Tips$ (a list of unconfirmed blocks in the network), and randomly selects blocks for verification. The content of the block includes the certificate and signature of the node. For the node certificate Σ_n, query the public key $PK_{(SN_n)}$ of the sink node in the local network where n is located, then verify the public label w_n. Thus, the sink node can judge whether the node is legal. For the signature Sign, the sink node judge it by the algorithm $TVer(.)$. When a block is verified, the sink node puts it into the *List*, including the blocks that can be quoted, and ends this work after the *List* is added to 2 elements.

2) Generate block: The new blocks must quote the two verified blocks. The content of the block includes $timeStamp$, ID of the block, *hash* value of the current block and previous blocks, and the *data*. The block structure is:

$$Block = [timeStamp||blockId||hashPre||hashCur||data] \quad (4)$$

The *data* includes the node's identity information Σ_n, relation signature $Sign_{(n,m)}$ and status $flag$. The data structure is:

$$Data = [\Sigma_n||Sign_{(n,m)}||flag] \quad (5)$$

The $flag$ is utilized to remove the identity information, the details will be introduced in 4.2.2.

3) Publish block: The sink node calculates the hash value of the new block and quotes the previous blocks according to the *List*. Then the sink node encrypts the new block with a private key and broadcasts it to the blockchain network. The new block is added to the end of the Tangle through the recognition of the format and source by the network participants. And, the release of a new block will update the *List*. After several rounds of consensus, subsequent quotations to a block will prove the credibility of the block.

4.2.2. Update the TR-Graph

The authentication does not directly call the data stored on the blockchain because it cannot be modified. The TR-Graph, which is generated by the sink node based on the Tangle, is utilized for final authentication. Therefore, the BAS can delete designated identity information to disable malicious nodes, which were originally trusted. The details are as follows:

1) Generate local TR-Graph: The sink node only authenticates the nodes in the local network, so TR-Graph just contains the information of this local network. The sink node traverses the identity information stored in the blockchain, and judges whether the identity information belongs to itself according to the node's public label w_n. Then the sink node downloads the identity information Σ_n belonging to it and the relation signature $Sign_{(n,m)}$ signed by the local nodes. Finally, the sink node calculates the TR-Graph by the downloaded information. To solve the redundancy caused by repeated relation signatures, the sink node ignores the repeated signatures and synthesizes

the transitive signature. Thus TR-Graph is a transitive reduction.

2) Update TR-Graph: The BAS adds a status $flag$ to the block format, which indicates whether the purpose of the block is to register identity information or delete identity information. The flag in a new block will be changed from 0 to 1 if we want to delete the identity information rather than register. Other sink nodes can also verify the block after the disabling reason is written to the mechanism. The sink nodes will read the block in a new cycle, then ignore the previous identity information of the node in the block. Therefore, the sink node will not generate the node's identity information when updating the TR-Graph.

Tangle maintains an identity that has been agreed by the entire network. The existence of this identity information is a linked list of DAG structures. The sink nodes will periodically download the data on the Tangle, and generate a partial TR-Graph. The graph only contains the identity information required for local authentication, and the sink node will directly call it during the authentication.

4.3. Algorithm description

As shown in Fig.6, the sink node submits identity information to the blockchain. Then the blockchain maintains the identity information through the consensus. Finally, the sink node periodically downloads the required information from the blockchain and updates the TR-Graph. The update algorithm of TR-Graph in BAS is exhibited in Algorithm 1.

Algorithm 1: Updating mechanism of TR-Graph

input : registerRequests and transitive signatures
output: Updating the TR-Graph

```
1  begin:
2      SN ← this ;
3      Rmsg ← recieveRegister(); // SN recieve
           the registerRequests
4      forall elements of Rmsg do
5          request = decode(element);
6          if judge(request.SID)==1 then
7              Send Keys to request.address ;
8          else
9              return errors()
10         end
11     end
12     Smsg ← recieveSignature() ; // SN
           recieve the Signatures
13     forall elements of Smsg do
14         msg = decode(Smsg) ;
15         list = verify(blockChain) ;
16         publish(list,msg)
17     end
18     Update(blokChain,TR-Graph) ;
19 end
```

In the algorithm, SN represents the sink node, $Rmsg$ represents the registration information sent by the sensor node, $Smsg$ represents the signature information sent by the sensor node, and TR-Graph represents the final trust relation graph. The function $Judge()$ is used to judge whether the node is legal, $Verify()$ is used to verify the legitimacy of the previous block, and returns the latest list of trusted blocks, and $Publish()$ can package the identity information into blocks, and $Update()$ can update the local TR-Graph according to the blockchain. The specific process of the algorithm is as follows:

After initialization (line 1), the sink node will collect registration requests from all surrounding nodes (line 3), and then traverse all registration requests (line 4). The sink node decrypts the request according to the inherent UID of the device (line 5) and then judges whether the requesting device can be registered according to the pre-deployed default configuration. If the registration request is passed, the node will obtain a key pair randomly distributed by the sink node (lines 6-7). The sink node collects the relation signatures submitted by the sensor nodes (line 12), then traverses all signatures (line 13). In this process, the sink node does not verify the current signature but verifies the previous signatures according to Tips (line 15). The receiver node then publishes the current signatures according to the List (line 16). Moreover, in each cycle, the sink node will update the local TR-Graph (line 18) based on the blockchain.

5. Security analysis

This section will analyze the security of BAS from three aspects: certification, detection rate, and transmission rate.

Authentication: The BAS uses the device's inherent UID to authenticate the sensor nodes. After the node is authenticated by the system, it obtains the certificate and key and becomes a legal node. Then the node can encrypt the data and sign the relation signature. The UID of the deployed device has already been written to the memory of the sink node, and the sensor node cannot obtain this UID list. Therefore, it is difficult for a disabled device to forge a new legal UID to join the network again. Digital signature technology prevents attackers from pretending legal entities or forging false information; adding a timestamp prevents attackers from launching replay attacks. The above encryption technology makes the system have good ability to resist traditional security attacks.

Detecion rate: Collect the communication patterns and use the dynamic detection algorithm SPRA to detect the worm propagation in the network. The scheme effectively addresses the worm propagation characteristics in WSN. Under the condition that the false alarm rate α' and the missed alarm rate β' are continuously

reduced, the detection rate of worms will continue to increase.

Infection rate: The BAS divides WSN into several network groups, and these groups communicate through blockchain. The worm do not spread horizontally between network groups. When an attacker selects a sensor node to launch a worm attack, the node will quickly spread the worm in the local network, but the worm will be limited to the local network and cannot spread in a large area. At the same time, the detection strategy will detect the spread of worms in a short time, and then trigger the system to manage the nodes. Therefore, BAS can isolate the origin of the worm, effectively limiting the spread of the worm.

6. Simulation and experiment

This section conducts worm detection simulation and compares two WSNs that have been attacked by worms. One of them only runs a traditional worm detection scheme, and the other can manage detected malicious nodes by BAS. This proves the potential of BAS to integrate other attack detection strategies and the security of BAS.

6.1. Environment setting

The sink node monitors the communication patterns of the local network domain. When a *fusion communication pattern* is detected, the sink node runs the SPRA algorithm to calculate the possibility of worm propagation. Set the user false alarm value and the missed alarm value to 0.01, the lower threshold γ_0 and the upper threshold γ to 0.1 and 0.9, respectively, the election probability of monitoring nodes $\rho_d = 0.1$, and the probability of random broadcast of packets $\rho_f = 0.02$. The simulation is carried out in the Matlab environment: with 90-time slots as a cycle, 300 sensor nodes are placed in a square area of 300m×300m, and the communication radius of each sensor node is 50m.

In the experiment, the packet sent by each node is either benign or malicious. Normal network traffic satisfies the Poisson distribution, the interval time of packets transmission satisfies the exponential distribution of the parameter λ, and the packet size sent in each time slot is 50 bytes.

6.2. Experimental analysis

6.2.1. Infection rate

We utilize the epidemic spread model to simulate the spread of worms in sensor networks. The epidemic spread model can predict the number of infected nodes in the network well. Literature [35] gives a simple epidemic spread model and infection rate of worms in discrete time.

$$\frac{dI_t}{I_t} = \rho \mathrm{I}_t(N - I_t) \tag{6}$$

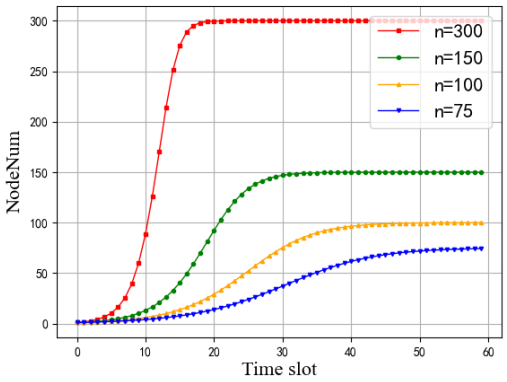


Fig. 6: Diagram of change in the number of infected nodes

As exhibited in formula (6), the unit of time is a time slot t, I_t represents the number of infected nodes in the network at time t, N represents the number of summary nodes in the network, and ρ represents the infection rate between sensor nodes.

The infection rate is set to a fixed probability ρ. Within different total numbers of nodes, the number of infected nodes varies with time, as shown in Fig.6. As the time increases, the number of infected nodes increases. The network with a smaller number of nodes is fully infected at a slower speed. The communication between groups of BAS uses blockchain technology, and the worm will not spread horizontally in each network group, so the total number of nodes that the worm can infect is the number of network nodes divided by the number of network groups. Therefore, BAS, which clusters the network, has more advantages in resisting worm infection.

6.2.2. Detection rate

Assuming that n samples are detected when the SPRA algorithm terminates, and the time spent for detection is r, then the probability that the worm node is detected before the time $r + 1$ is $P_r = 1 - e^{-\sum_{i=1}^{r} P_S^i}$, where P_S^i is the maximum probability that the worm is not detected in each time slot, as shown in formula (7):

$$P_S^i = 1 - \frac{\ln \frac{1-\beta'}{\alpha'} + n \ln \frac{1-\gamma_0}{1-\gamma_1}}{n(\ln \frac{\gamma_1}{\gamma_0} - \ln \frac{1-\gamma_1}{1-\gamma_0})} \tag{7}$$

In each round of time slots, the SPRA accepts hypothesis H_1 when $\varphi_n \geq l_1(n)$, and determines that there is worm propagation in the network. The probability that a malicious node is detected is $P_r = 1 - \prod_{i=1}^{r}(1 - P_S^i)$ before the time $r + 1$. In addition, since $(1 + x) \leq e^x$, the probability expression can be expressed as formula (8):

$$P_r = 1 - \prod_{i=1}^{r}(1 - P_S^i) \geq 1 - e^{-\sum_{i=1}^{r} P_S^i} \tag{8}$$

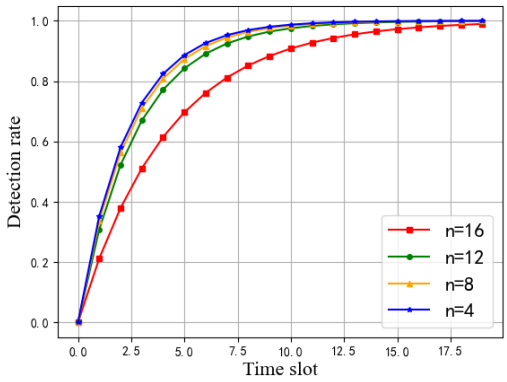


Fig. 7: Diagram of changes in detection rate

From Equations 7-8, we could conclude that not only the detection rate is affected by the number of nodes, but the change rate of the detection rate is also affected by the number of nodes. Fig.7 exhibits that the worm detection rate is related to the number of nodes in the network. It indicates that as the number of nodes increases, the rate of decline of the detection rate also increases, the detection rate will take more time to reach an acceptable level. Since BAS divides WSN into multiple network groups, the number of detection nodes is only the number of nodes in a single local network. Therefore, the detection loaded with BAS can detect the spread of the worm in a shorter time.

7. Conclusions

We propose a blockchain-based node authentication scheme for WSN. The scheme divides the WSN into multiple independent local networks. Each sink node authenticates the sensor nodes in the local network, and then the blockchain stores the identity information to ensure security. Based on the node management capabilities of BAS, we simulated worm detection, and proved the security and application potential of BAS through experimental comparison. However, the application of blockchain-based authentication in WSN still faces some technical challenges and limitations. For example, how to balance storage and communication overhead in the solution, and how to group dynamic nodes. In addition, blockchain technology is still in its infancy, which may face new problems and challenges when applied to WSN. In the future, we will strive to address these topics.

Acknowledgements

This work was supported by the Natural Science Foundation under Grant No. 61962009, Major Scientific and Technological Special Project of Guizhou Province under Grant No. 20183001, and Foundation of Guizhou Provincial Key Laboratory of Public Big Data under Grant No. 2018BDKFJJ003, 2018BDKFJJ005 and 2019BDKFJJ009.

[1] L. Qiang, H. Xiaohong, L. Supeng, L. Longjiang, M. Yuming, Deployment strategy of wireless sensor networks for internet of things, China Commun. 8 (2011) 111–120.
[2] N. Marriwala, P. Rathee, An approach to increase the wireless sensor network lifetime, Proc. 2012 World Congr. Inf. Commun. Technol. WICT 2012. (2012) 495–499. https://doi.org/10.1109/WICT.2012.6409128.
[3] P.Ö. and H.S. Butun, Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures, IEEE Commun. Surv. Tutorials. 22 (2020) 616–644. https://doi.org/10.1145/3023924.3023943.
[4] Y. Yuan, F.Y. Wang, Blockchain: The state of the art and future trends, Zidonghua Xuebao/Acta Autom. Sin. 42 (2016) 481–494. https://doi.org/10.16383/j.aas.2016.c160158.
[5] T. AbuHmed, N. Nyamaa, D.H. Nyang, Software-based remote code attestation in wireless sensor network, GLOBECOM - IEEE Glob. Telecommun. Conf. (2009). https://doi.org/10.1109/GLOCOM.2009.5425280.
[6] P.H. Yang, S.M. Yen, Memory attestation of wireless sensor nodes through trusted remote agents, IET Inf. Secur. 11 (2017) 338–344. https://doi.org/10.1049/iet-ifs.2016.0556.
[7] G. Qiang, Z. Chongyang, Worm detection based on remote software attestation and sequential probability ratio analysis, J. Cent. China Norm. Univ. Sci. 52 (2018) 461–467.
[8] Y. Chen, J. Sun, Y. Yang, T. Li, X. Niu, H. Zhou, PSSPR: A source location privacy protection scheme based on sector phantom routing in WSNs, Int. J. Intell. Syst. (2021). https://doi.org/10.1002/int.22666.
[9] C. Mahmoud, S. Aouag, Security for internet of things: A state of the art on existing protocols and open research issues, ACM Int. Conf. Proceeding Ser. 17 (2019) 1294–1312. https://doi.org/10.1145/3361570.3361622.
[10] J. Granjal, E. Monteiro, J.S. Silva, End-to-end transport-layer security for Internet-integrated sensing applications with mutual and delegated ECC public-key authentication, 2013 IFIP Netw. Conf. IFIP Netw. 2013. (2013) 1–9.
[11] Di. Wang, P. Wang, C. Wang, Efficient Multi-Factor User Authentication Protocol with Forward Secrecy for Real-Time Data Access in WSNs, ACM Trans. Cyber-Physical Syst. 4 (2020). https://doi.org/10.1145/3325130.
[12] C. Lin, D. He, X. Huang, M. Khurram Khan, K.K.R. Choo, A New Transitively Closed Undirected Graph Authentication Scheme for Blockchain-Based Identity Management Systems, IEEE Access. 6 (2018) 28203–28212. https://doi.org/10.1109/ACCESS.2018.2837650.
[13] H. Engi, Survey on Transitive Signature Schemes, (2002) 6–11.
[14] C.G. Peng, Y.L. Tian, B. Zhang, Z.P. Xu, General transitive signature scheme based on homomorphic encryption, Tongxin Xuebao/Journal Commun. 34 (2013) 18–25. https://doi.org/10.3969/j.issn.1000-436x.2013.11.003.
[15] C. Lin, W. Wu, X. Huang, L. Xu, A new universal designated verifier transitive signature scheme for big graph data, J. Comput. Syst. Sci. 83 (2017) 73–83. https://doi.org/10.1016/j.jcss.2016.06.003.
[16] T. Li, Y. Chen, Y. Wang, Y. Wang, M. Zhao, H. Zhu, Y. Tian, X. Yu, Y. Yang, Rational Protocols and Attacks in Blockchain System, Secur. Commun. Networks. 2020 (2020). https://doi.org/10.1155/2020/8839047.
[17] Z.F. Gao, J.L. Zheng, S.Y. Tang, Y. Long, Z.Q. Liu, Z. Liu, D.W. Gu, State-of-the-art Survey of Consensus Mechanisms on DAG-based Distributed Ledger, Ruan Jian Xue Bao/Journal Softw. 31 (2020) 1124–1142. https://doi.org/10.13328/j.cnki.jos.005982.
[18] I. Makhdoom, M. Abolhasan, H. Abbas, W. Ni, Blockchain's adoption in IoT: The challenges, and a way forward, J. Netw. Comput. Appl. 125 (2019) 251–279. https://doi.org/10.1016/j.jnca.2018.10.019.
[19] T. Li, Z. Wang, G. Yang, Y. Cui, Y. Chen, X. Yu, Semi-selfish

mining based on hidden Markov decision process, Int. J. Intell. Syst. (2021) 1–17. https://doi.org/10.1002/int.22428.

[20] T. Li, Z. Wang, Y. Chen, C. Li, Y. Jia, Y. Yang. Is semi-selfish mining available without being detected?. Int. J. Intell. Syst. (2021). https://doi.org/10.1002/int.22656

[21] W.F. Silvano, R. Marcelino, Iota Tangle: A cryptocurrency to communicate Internet-of-Things data, Futur. Gener. Comput. Syst. 112 (2020) 307–319. https://doi.org/10.1016/j.future.2020.05.047.

[22] C. Machado, C.M. Westphall, Blockchain incentivized data forwarding in MANETs: Strategies and challenges, Ad Hoc Networks. 110 (2021) 102321. https://doi.org/10.1016/j.adhoc.2020.102321.

[23] B. Hu, C. Zhou, Y. Tian, Y. Qin, X. Junping, Using Blockchain for Multimicrogrid Systems, IEEE Trans. Syst. Man, Cybern. Syst. 49 (2019) 1720–1730.

[24] H. Liang, J. Wu, S. Mumtaz, J. Li, X. Lin, M. Wen, MBID: Micro-Blockchain-Based Geographical Dynamic Intrusion Detection for V2X, IEEE Commun. Mag. 57 (2019) 77–83. https://doi.org/10.1109/MCOM.001.1900143.

[25] Y. Zhen, H. Liu, Distributed privacy protection strategy for MEC enhanced wireless body area networks, Digit. Commun. Networks. 6 (2020) 229–237. https://doi.org/10.1016/j.dcan.2019.08.007.

[26] L. Feng, H. Zhang, L. Lou, Y. Chen, for ' ata 6 ecurity 3 rocess 3 latform of WSN, 2018 IEEE 22nd Int. Conf. Comput. Support. Coop. Work Des. (2018) 75–80.

[27] W. Tiberti, A. Carmenini, L. Pomante, D. Cassioli, A Lightweight Blockchain-based Technique for Anti-Tampering in Wireless Sensor Networks, Proc. - Euromicro Conf. Digit. Syst. Des. DSD 2020. (2020) 577–582. https://doi.org/10.1109/DSD51259.2020.00095.

[28] Y. Zeng, X. Zhang, R. Akhtar, C. Wang, A Blockchain-Based Scheme for Secure Data Provenance in Wireless Sensor Networks, Proc. - 14th Int. Conf. Mob. Ad-Hoc Sens. Networks, MSN 2018. (2018) 13–18. https://doi.org/10.1109/MSN.2018.00009.

[29] S. Kushch, F. Prieto-Castrillo, A rolling blockchain for a dynamic WSNs in a smart city, ArXiv. (2018) 29–34.

[30] Z. Cui, F. Xue, S. Zhang, X. Cai, Y. Cao, W. Zhang, J. Chen, A Hybrid BlockChain-Based Identity Authentication Scheme for Multi-WSN, IEEE Trans. Serv. Comput. 13 (2020) 241–251. https://doi.org/10.1109/TSC.2020.2964537.

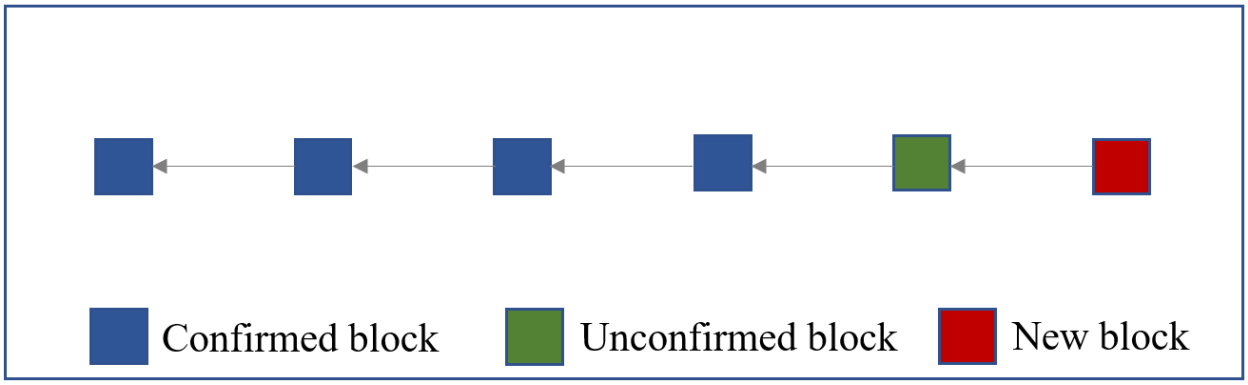
[31] M.T. Hammi, P. Bellot, A. Serhrouchni, BCTrust: A decentralized authentication blockchain-based mechanism, IEEE Wirel. Commun. Netw. Conf. WCNC. 2018-April (2018) 1–6. https://doi.org/10.1109/WCNC.2018.8376948.

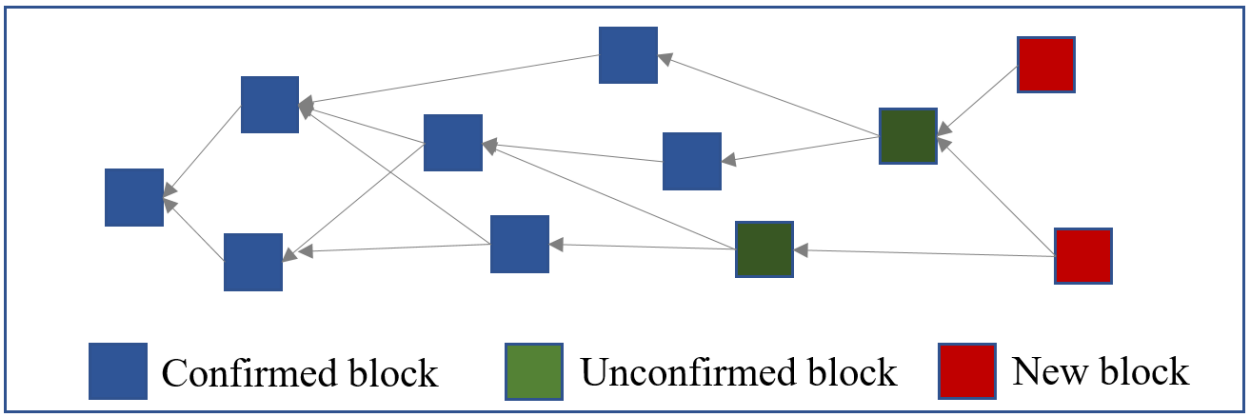
[32] M.T. Hammi, B. Hammi, P. Bellot, A. Serhrouchni, Bubbles of Trust: A decentralized blockchain-based authentication system for IoT, Comput. Secur. 78 (2018) 126–142. https://doi.org/10.1016/j.cose.2018.06.004.

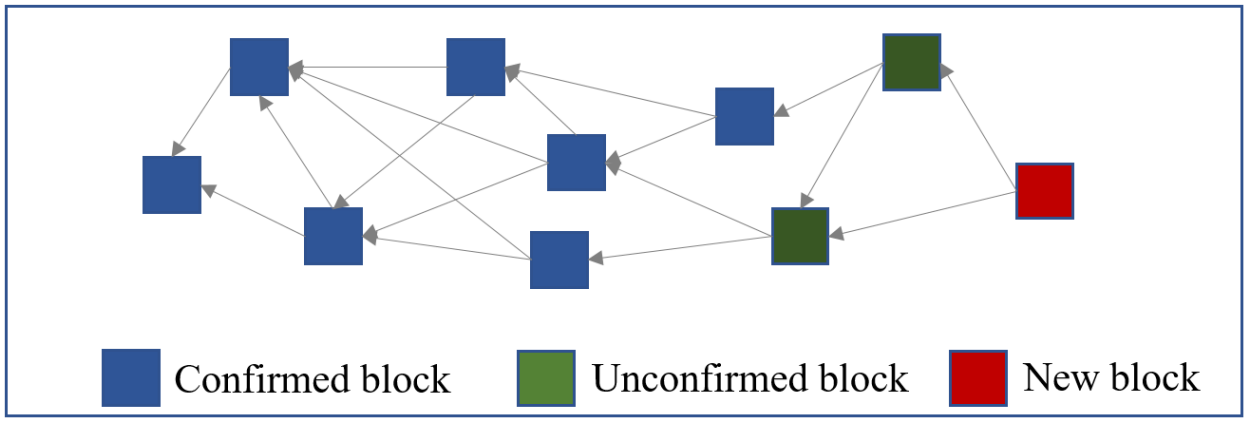
[33] N. Shi, L. Tan, W. Li, X. Qi, K. Yu, A blockchain-empowered AAA scheme in the large-scale HetNet, Digit. Commun. Networks. (2020). https://doi.org/10.1016/j.dcan.2020.10.002.

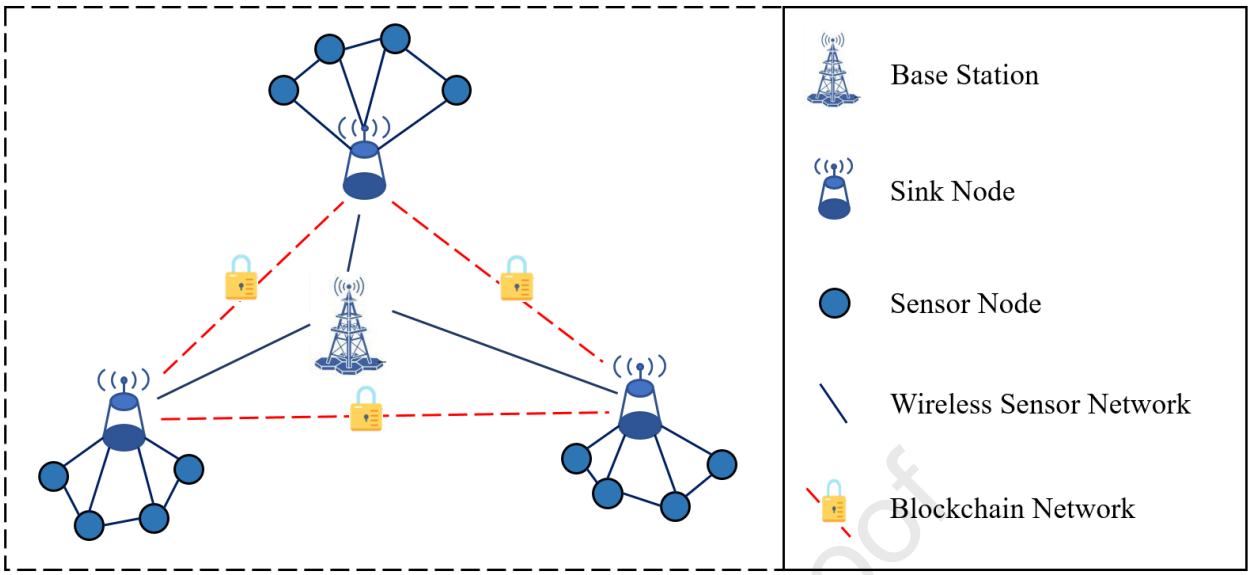
[34] C.C. Zou, L. Gao, W. Gong, D. Towsley, Monitoring and early warning for internet worms, Proc. ACM Conf. Comput. Commun. Secur. (2003) 190–199. https://doi.org/10.1145/948134.948136.

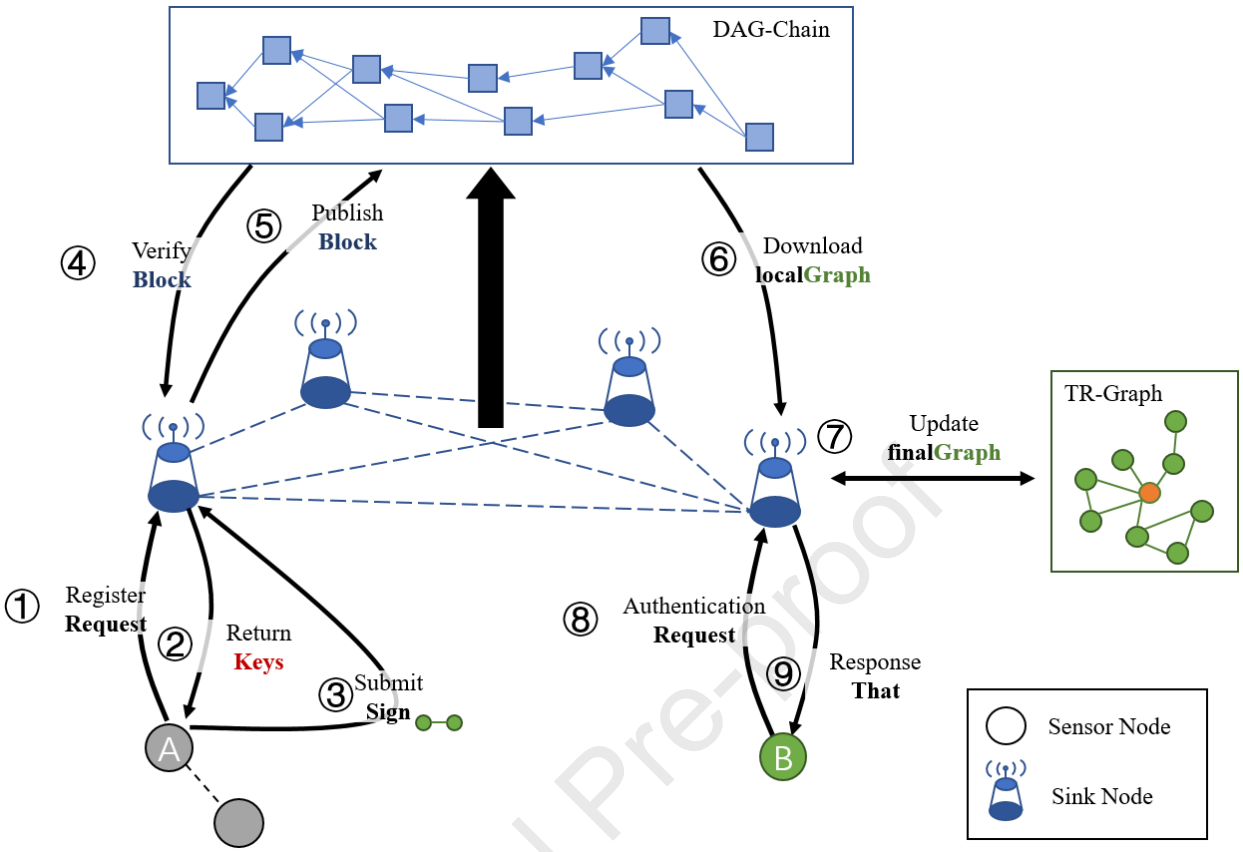
[35] J.W. Ho, M. Wright, S.K. Das, Fast detection of mobile replica node attacks in wireless sensor networks using sequential hypothesis testing, IEEE Trans. Mob. Comput. 10 (2011) 767–782. https://doi.org/10.1109/TMC.2010.213.

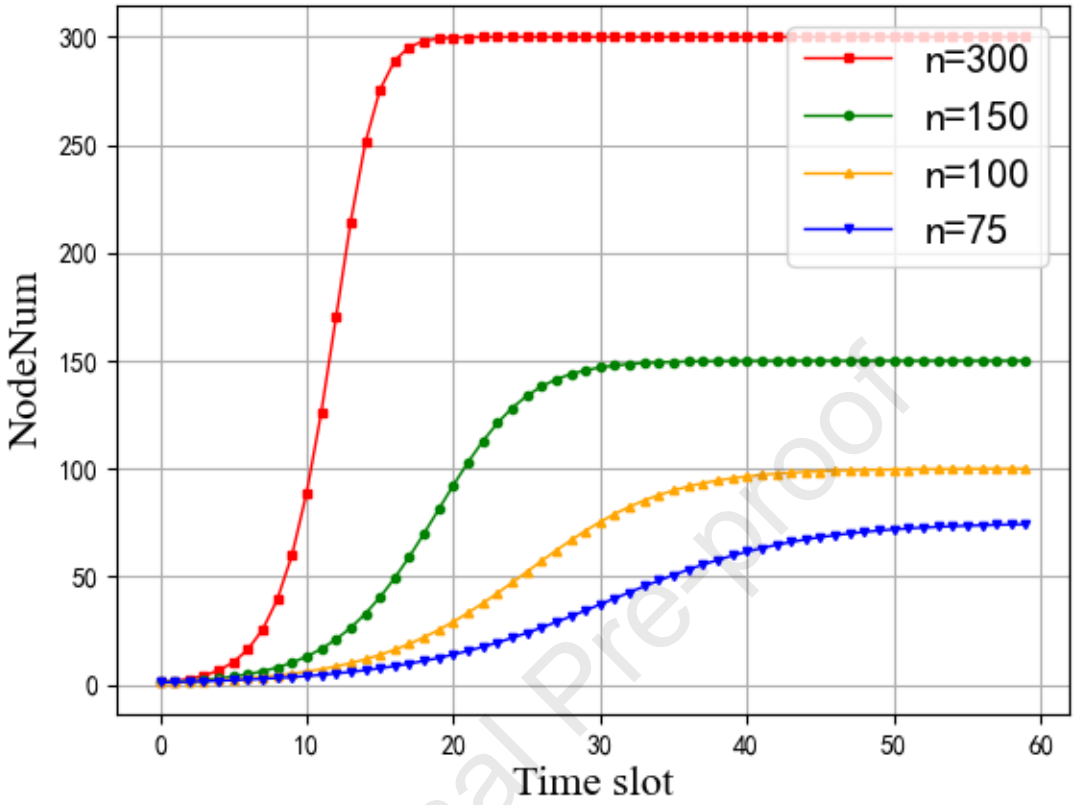


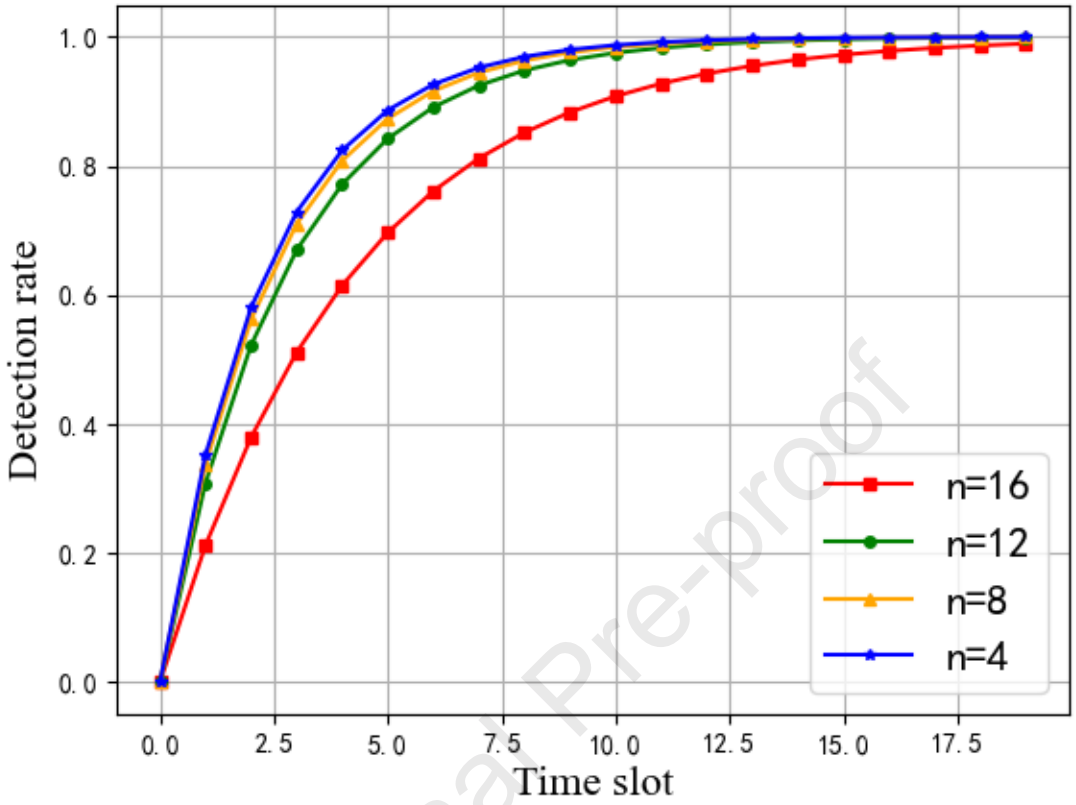












Declaration of interests

We declare that we have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.