Postprint: A Node Clone Attack Detection Scheme for Data Dissemination in Wireless Sensor Networks

Authors: Zhang Qian, Hongbin Chen, Hongbin Chen

Date: 2022-06-07T00:00:00+00:00

Abstract

In wireless sensor networks (WSNs), data dissemination constitutes a critical transmission paradigm that must satisfy three fundamental requirements: reliability, energy efficiency, and scalability. Nevertheless, existing research has devoted limited attention to attacks targeting data dissemination, substantially undermining its reliability. To detect node clone attacks in WSNs data dissemination and ensure high reliability, we propose a node clone attack detection scheme based on single-round zero-knowledge proof. Our scheme constructs disjunctive-superimposed codes to generate unique digital fingerprints for each node, and verifies these fingerprints within a single-round zero-knowledge proof protocol to detect cloned nodes lacking valid digital fingerprints. Simulation results demonstrate that the proposed scheme can guarantee high reliability for WSNs during the data dissemination process.

Full Text

Preamble

A Node Cloning Attack Detection Scheme for WSNs Data Dissemination

ZHANG Qian, CHEN Hongbin
(School of Information and Communication, Guilin University of Electronic Technology, Guilin 541004, China)

Abstract: In wireless sensor networks (WSNs), data dissemination is an essential transmission mode that must meet three key requirements: reliability, energy efficiency, and scalability. However, existing research pays little attention to attacks targeting data dissemination, resulting in significant degradation

of reliability. To detect node clone attacks in WSNs data dissemination and ensure high reliability, this paper proposes a node clone attack detection scheme based on single-round zero-knowledge proof. The scheme generates unique digital fingerprints for each node by constructing superimposed disjunct codes, then verifies these fingerprints through a single-round zero-knowledge proof protocol to detect cloned nodes lacking correct digital fingerprints. Simulation results demonstrate that the proposed scheme can ensure high reliability of WSNs during the data dissemination process.

Keywords: data dissemination; node clone attack; superimposed disjunct code; zero knowledge proof; reliability

Introduction

In wireless sensor networks (WSNs), the most common operation involves base stations or sink nodes collecting sensed data from nodes scattered throughout the monitoring area [1]. In contrast to this many-to-one data collection pattern, one-to-many data transmission represents another critical aspect of WSNs operations [2]. This transmission mode is referred to as data dissemination, where base stations or sink nodes send configuration parameters to sensor nodes during network updates to maintain consistency, or transmit commands and warning messages to control sensor nodes [3]. A crucial metric in data dissemination is reliability—all nodes in the WSN must receive the disseminated data to maintain network uniformity. The presence of captured nodes during data dissemination severely compromises this reliability. Therefore, considering node capture attacks in data dissemination protocol research constitutes meaningful work.

WSNs data dissemination must satisfy three requirements: reliability, energy efficiency, and scalability [4]. Typical data dissemination methods fall into two categories: structure-based schemes and unstructured schemes. Structure-based approaches include CORD [5], CoCo [6], and CDS [7]. These schemes leverage network structural information (such as location and topology) to construct efficient dissemination-specific structures [8]. Consequently, structure-based schemes meet reliability and energy efficiency requirements but suffer from poor scalability. Unstructured schemes, by contrast, do not utilize network structural information nor form dedicated dissemination structures, offering excellent scalability. Unstructured schemes can be further divided into: (1) non-negotiation schemes (e.g., flooding [9], Gossip [10], Trickle [11]); and (2) negotiation-based schemes (e.g., SPIN [12], MOAP [13], Deluge [14]). Non-negotiation schemes without control information enable relatively fast dissemination but struggle to provide high reliability and may cause broadcast storm problems. Negotiation-based schemes aim to control redundant transmissions and guarantee high reliability [15], but the control information introduces additional communication and time overhead, making them less energy-efficient than non-negotiation schemes.

Node cloning attacks represent a highly destructive attack form in WSNs data dissemination: attackers capture legitimate nodes to obtain sensitive network

information, replicate this information onto cloned nodes, and redeploy these clones into the network [16]. Such cloned nodes can easily participate in WSNs data dissemination and other operations as legitimate nodes, enabling more destructive insider attacks. This paper investigates detection schemes for node cloning attacks, with existing approaches detailed below.

The first commonly used technique in node cloning attack detection compares information held by neighboring nodes: each node compares its stored information with all neighbors' information, detecting cloning attacks by identifying inconsistencies [17]. Reference [18] proposed a clone attack detection protocol for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN), where a mapping function assigns identity (ID) and rank information to all nodes, enabling parent nodes to identify anomalies between node IDs and rank information using mapper characteristics. However, this approach fails when attackers capture and clone parent nodes. Reference [19] presented a clone node detection scheme for the Internet of Things using a fingerprint-based zero-knowledge proof mechanism for two-level authentication of sensor devices. The base station computes fingerprints for each node and sends them to cluster heads, detecting cloned nodes by comparing device fingerprints with base station records. This incurs substantial computational overhead at the base station when verifying numerous sensor nodes simultaneously and only applies to static networks, increasing communication overhead between cluster heads and the base station.

The second common technique employs witness discovery: witness nodes detect cloned nodes during communication, with detection efficiency achieved by strategically modifying witness node selection [20]. Reference [21] proposed four clone attack detection methods: node-to-network broadcast, deterministic multicast, random multicast, and line-selected multicast. Node-to-network broadcast floods location information throughout the network, effectively selecting all nodes as witnesses to detect identity conflicts. Deterministic multicast selects specific node subsets as witnesses to reduce communication costs. Random multicast distributes node location information to randomly chosen witnesses, preventing attackers from obtaining fixed witness node information and leveraging the birthday paradox [22] to detect replicated nodes. Line-selected multicast utilizes network topology to detect replicated nodes at intersection points of witness node paths, though detection performance is limited by the number and distribution of these intersection points.

The proposed detection scheme belongs to the first category, deriving detection results by comparing information held by original and cloned nodes. The innovation lies in applying a single-round zero-knowledge proof scheme based on elliptic curve discrete logarithms, which minimizes communication overhead and thus energy consumption compared to multi-round zero-knowledge proof schemes.

1.1 Sensor Network Model

As shown in Figure 1 [Figure 1: see original paper], this paper considers static WSNs deploying one sink node and numerous ordinary nodes. The sink node is positioned at the monitoring area' s center, intermittently disseminating data to or collecting data from ordinary nodes via multi-hop transmission. Serving as a gateway between the WSN and the Internet, the sink node manages the entire WSN. Compared with ordinary sensors, the sink node' s energy and memory can be considered unlimited. Ordinary nodes are responsible for sensing monitoring area information, processing sensed data, and transmitting data.

1.2 Data Dissemination Model

This paper adopts the Sensor Protocol for Information via Negotiation (SPIN) as the data dissemination routing protocol, an unstructured, flat routing scheme illustrated in Figure 2 [Figure 2: see original paper]. Nodes broadcast ADV messages to inform neighbors about forthcoming data dissemination; neighbors requiring the data reply with REQ messages, and nodes already possessing the disseminated data send DATA messages to those without it. This routing scheme reduces redundant packet transmission during dissemination. ADV and REQ messages are small packets consuming minimal energy resources while ensuring data dissemination reliability. The connections established through ADV and REQ message exchanges satisfy reliability requirements while maintaining scalability.

1.3 Node Clone Attack Detection Model

A key reason for WSNs' widespread application is the use of low-cost microsensors. Consequently, all sensor nodes lack tamper-proof hardware, and when a node suffers a capture attack, its memory contents become available to attackers. Attackers may deploy multiple nodes with identical identity IDs into the network to cooperate in evading detection. As in most research models, cloned nodes cannot create new IDs without base station or sink node approval; thus, this paper assumes cloned nodes can only participate in the network using original node IDs.

2 Algorithm Description

To address node cloning attacks in data dissemination, this paper proposes a Single-Round Zero-Knowledge Proof detection scheme (SR-ZKP). The algorithm constructs superimposed-disjunct codes using node deployment location information and identity proof codes assigned by the sink node to generate unique digital fingerprints for legitimate nodes. These digital fingerprints then serve as the basis for distinguishing legitimate nodes from clones, with proof conducted via a single-round zero-knowledge proof scheme based on elliptic curve discrete logarithms. Relevant theoretical foundations are presented below.

2.1.1 Superimposed Codes

Superimposed codes have been extensively studied and applied across various fields, including multiple-access communication, cryptography, pattern matching, circuit complexity, and many computer science domains. Their cryptographic applications offer low complexity and high resistance to cracking. We first introduce fundamental definitions and properties of superimposed codes.

For matrix X, the following definitions apply:

Definition 1 (Covering). Given two binary codewords $y = (y_1, y_2, \cdots, y)$ and $z = (z_1, z_2, \cdots, z)$, if the Boolean sum (logical OR) of y and z equals y, then y covers z, denoted as y z = y.

Definition 2 ((s, L, M) Superimposed Code). If any s columns of an M×N binary matrix X have a Boolean sum that covers at most L−1 columns outside these s columns, then X defines a superimposed code of length M, size N, and strength s ($1 < s \leq N$) with list size l ($1 \leq l \leq N$), denoted as an (s, l, M) superimposed code of size N.

Definition 3 (Disjunct Property). If the Boolean sum of any s columns in X cannot cover any column outside this set of s columns, X is called an s-disjunct code.

Based on these definitions, an (s, 1, N) superimposed code is also an s-disjunct code, referred to as a superimposed-disjunct code. Matrix X in equation (3) represents a (3, 1, 13) superimposed-disjunct code. According to the disjunct property of superimposed-disjunct codes, the following property holds:

Given an (s, 1, N) superimposed-disjunct code X, for any subset of s columns in X, there exists at least one row where all elements are zero.

2.1.2 Zero-Knowledge Proof

Zero-knowledge proof enables one party (the prover, denoted as P) to demonstrate knowledge of certain information to another party (the verifier, denoted as V) without revealing any useful information. This approach prevents third-party eavesdroppers from obtaining the knowledge, protecting its integrity and confidentiality. This characteristic suits verifying secret information of nodes over open wireless channels. The zero-knowledge proof procedure involves:

Step 1: P sends commitment information (Commit) related to the proven knowledge to V, enabling V to determine whether P violates this commitment in subsequent proofs.

Step 2: After receiving the commitment, V randomly selects a question from the question set (problems solvable only with secret knowledge) and sends it to P.

Step 3: P solves the problem using secret knowledge and sends the solution to V for verification.

Step 4: V makes an identity judgment about P based on the verification information.

Due to random question selection in Step 2, zero-knowledge schemes require multiple repetitions of these four steps to ensure correctness. In contrast, the single-round zero-knowledge scheme based on elliptic curves requires only one round to achieve the required correctness, substantially reducing communication costs [23].

2.2 Digital Fingerprint Generation

This phase constructs superimposed-disjunct codes using environmental information and unique identity proof codes to generate node digital fingerprints (DID). Using DID during data dissemination enables clone detection. Compared with conventional public-key protocols, this superimposed-disjunct code construction algorithm involves smaller computational overhead, requiring only simple binary operations.

Some schemes digitize node deployment location neighborhood information into binary code strings, filling them into the matrix' s first row, then using cyclic right-shift operations to fill subsequent rows until achieving equal column weights. However, most sensor networks deploy numerous nodes, resulting in redundant nodes. This matrix construction may cause redundant nodes with identical neighborhood information and neighbors to compute identical superimposed-disjunct codes, creating conflicts.

Therefore, this scheme uses binary code strings representing neighborhood information as part of the matrix. The sink node assigns each node a unique identity proof code (also represented as a binary code string), which is appended to the last column of the current partial matrix, followed by the complement of the identity proof code string. This satisfies the constant weight property of the matrix. This approach yields a unique matrix containing both node deployment environment characteristics and a numerical string symbolizing the node' s unique identity, known only to the sink node and the individual node.

The digital fingerprint is then constructed using superimposed-disjunct code properties. The fingerprint computation method has been introduced in existing work, with the process illustrated in Figure 3 [Figure 3: see original paper].

2.3 Single-Round Zero-Knowledge Proof Detection

This phase employs a single-round zero-knowledge scheme based on elliptic curve discrete logarithms for clone detection, verifying node identity without directly exposing identity credentials.

We first describe the elliptic curve discrete logarithm problem: Given a finite field F and an elliptic curve E over F , for a base point G on E, the operation m · G = M defines the problem of solving for m given G, M, and the elliptic curve prime p (typically a large prime). The single-round zero-knowledge scheme

based on elliptic discrete logarithms operates with both prover and verifier sharing G, M, and p, where prover P demonstrates knowledge of the solution m to verifier V. Solving elliptic curve discrete logarithm problems requires exponential time, making it computationally infeasible for provers lacking secret knowledge to pass verification, thus ensuring clones almost never evade detection.

During network initialization, each node generates commitment message Commit and exchanges it with one-hop neighbors along with its digital fingerprint. Neighbor nodes store these messages in memory. The commitment message takes the form Commit = {G, M}, where G is a randomly selected base point on the elliptic curve, p is the large prime of the elliptic curve, and M is computed via equation (5):

$$M = \mathrm{DID} \cdot G$$

In zero-knowledge proof, upstream nodes (including the sink node) during data dissemination serve as verifier V, while downstream nodes serve as prover P. After exchanging commitment information, both parties share p, G, and M.

During data dissemination, verifier V initiates verification of downstream nodes: V computes B using G selected in the commitment message and a randomly chosen r (r F), where "·" denotes elliptic curve multiplication, and sends it to P:

$$B = r \cdot G$$

Upon receiving the verification message, prover P generates K using the DID known only to legitimate nodes and sends it to V:

$$K = \mathrm{DID} \cdot B$$

After receiving K, verifier V checks the condition using equation (8):

$$\mathrm{flag}_N = K - r \cdot M$$

2.4.1 Security Analysis

We first analyze the completeness, soundness, and zero-knowledge property of the zero-knowledge proof scheme.

1. **Completeness:** The scheme clearly satisfies completeness—if the prover genuinely knows DID and follows the protocol instructions, the verifier will always accept the proof.

2. **Soundness:** Assuming a cloned node lacks knowledge of DID and attempts to deceive the upstream verifier, it must guess the value of DID in the elliptic curve domain. The probability of correct guessing is only 1/p, an extremely small value, thus satisfying soundness.

3. **Zero-Knowledge Property:** During the proof process, V can only obtain information about whether P possesses the secret DID, acquiring no additional knowledge, thereby satisfying the zero-knowledge property.

We next analyze the scheme' s resistance to two common attacks:

1. **Man-in-the-Middle Attack:** This prevalent wireless network attack involves the attacker masquerading as an intermediary between communicating parties—posing as the receiver to legitimate senders and as the sender to legitimate receivers to control communication. In the proposed detection scheme, attackers attempting to establish independent connections with WSN nodes will fail to masquerade successfully without legitimate nodes'digital fingerprints. Node digital fingerprints possess zero-knowledge properties in this scheme, preventing illegal attackers from obtaining legitimate fingerprints. Even if attackers guess a fingerprint with minimal probability, they cannot pass zero-knowledge proof because each iteration generates new random challenge questions.

2. **Replay Attack:** In this attack, adversaries attempt to replay previous communications to consume network resources and authenticate themselves to verifiers. However, since verifiers send different challenge values for each communication, replaying previous communications will fail verification.

2.4.2 Complexity Analysis

Digital fingerprint computation using superimposed-disjunct codes involves only simple binary operations.

In zero-knowledge proof, prover P performs one elliptic curve multiplication, while verifier V performs two elliptic curve multiplications and one comparison. During each data dissemination round, every node participates once as prover; correspondingly, its upstream node on the dissemination path participates once as verifier. Therefore, in a WSN with N nodes, N zero-knowledge proofs are conducted to determine whether nodes are redeployed clones. Each zero-knowledge proof requires three elliptic curve multiplications, yielding overall computational complexity of O(N).

For attackers, solving the elliptic curve discrete logarithm problem has time complexity $O(\sqrt{p})$ [24], requiring exponential time, thus providing high security for the scheme.

2.4.3 Scalability Analysis

The proposed scheme performs clone detection based on SPIN data dissemination, belonging to the unstructured category. As analyzed above, unstructured schemes do not depend on network topology and exhibit good scalability, manifested as slowly increasing completion time and energy consumption with network scale.

3.1 Experimental Simulation Setup

This experiment configures a 100 m × 100 m square monitoring area with the sink node placed at the center and nodes deployed randomly. To demonstrate node cloning attacks' impact on data dissemination, simulations were conducted for scenarios with no clone attacks and with 5 and 10 clone nodes affecting the SPIN dissemination protocol. The proposed Single-Round Zero-Knowledge Proof node clone attack detection scheme (SR-ZKP) was applied to SPIN (denoted as ZKP-SPIN) by adding three data items related to node digital fingerprints to the three messages in data dissemination, with performance compared across scenarios. Twenty WSNs were randomly generated, each undergoing 400 rounds of data dissemination, with average network performance metrics shown in subsequent figures. Experimental parameters and values are listed in Table 1 .

Table 1: Simulation Parameter Settings

Parameter	Value
Monitoring Area (Length × Width)	100 m × 100 m
ADV Message Size	100 bit
REQ Message Size	100 bit
DATA Message Size	30-35 kbit
ZKP Data Size	128 bit
Initial Node Number	400
Clone Node Number	5, 10
E_{elec}	50 nJ/bit
_{fs}	12 pJ/(bit · m^2)
_{mp}	0.0012 pJ/(bit · m^4)

3.2 Simulation Analysis

Figure 4 [Figure 4: see original paper] shows average residual energy variation. Since the SPIN dissemination protocol in this simulation fixes dissemination routes, energy consumption per round remains relatively consistent. The four curves appear approximately linear before round 160. Compared with the no-clone scenario (SPIN curve), networks with more clone nodes exhibit smaller slopes, indicating that more clone nodes result in more nodes failing to complete data dissemination and poorer reliability. After approximately round 240,

coverage holes emerge as some nodes exhaust their energy, causing the descent rate to slow. Because zero-knowledge proof data is extremely small compared to disseminated data, even with single-round zero-knowledge proof detection applied to SPIN, energy consumption remains nearly equal to SPIN without clone detection, making the average residual energy curves almost identical. This is reflected in other simulation figures, demonstrating that applying single-round zero-knowledge proof detection does not degrade SPIN data dissemination protocol performance. In scenarios with 5 and 10 clone nodes, SPIN dissemination protocol success rates decline severely, while ZKP-SPIN can detect clone nodes immediately during dissemination, preventing performance degradation from clone attacks.

Figure 5 [Figure 5: see original paper] shows the increase in dead nodes with dissemination rounds, where nodes under clone attacks are marked as dead. The four curves begin rising around round 80 because nodes near the sink bear heavy forwarding loads and gradually exhaust energy; around round 240, the ascent slows as the sink' s neighboring nodes are nearly depleted, forming coverage holes that allow only a few nodes with surviving neighbors to receive data.

Figures 6 [Figure 6: see original paper] and 7 [Figure 7: see original paper] respectively show the increase in nodes failing to complete data dissemination and the decrease in dissemination success rate with rounds. Nodes failing dissemination include three types: clone nodes, dead nodes, and nodes unable to connect with the sink due to coverage holes. In no-clone-attack scenarios, energy-limited nodes inevitably fail dissemination as energy depletes over time. In clone-node scenarios, since clone attacks occur randomly in simulation, clone deployment positions are also random. When clones are randomly deployed between legitimate nodes and the sink, legitimate nodes may use clones as intermediate nodes to the sink while actually disconnecting from the sink, preventing data reception. In practice, intelligent attackers could strategically place clone nodes to affect more legitimate nodes, causing greater damage to dissemination reliability. Although random clone deployment in simulation results in random impacts on legitimate nodes, the figures clearly show that scenarios with more clone nodes cause stronger disruption to dissemination completion.

4 Conclusion

This paper proposes a node clone attack detection scheme based on single-round zero-knowledge proof (SR-ZKP) and applies it to the SPIN data dissemination protocol. The scheme detects node cloning attacks by requiring downstream nodes to prove information possession to upstream nodes in the dissemination model. Superimposed-disjunct codes generate digital fingerprints, enabling complex encryption through simple binary operations. For fingerprint verification, the scheme employs a single-round zero-knowledge proof protocol based on elliptic curves to ensure that knowledge representing node identity is not transmitted over wireless channels between provers and verifiers, guaranteeing zero-knowledge property against illegal third parties in WSNs while resisting

man-in-the-middle and replay attacks. Simulation results demonstrate that the algorithm not only detects clone nodes and ensures dissemination reliability but also incurs minimal energy overhead that does not affect other dissemination performance metrics.

References

[1] SUN L M, ZHANG S Q, LI Z, et al. *Wireless Sensor Network Theory and Applications* [M]. Beijing: Tsinghua University Press, 2018: 11-13.

[2] CHEN H B, CHEN Q. Energy-balanced dynamic clustering algorithm for data collection in wireless sensor networks [J]. *Journal of Guilin University of Electronic Technology*, 2020, 40(4): 286-291.

[3] XU Z R, HU T L, SONG Q S. Bulk data dissemination in future low power sensor networks: present and directions [J]. *Sensors*, 2017, 17(12): 156-186.

[4] ZHENG X L, WAN M. A survey on data dissemination in wireless sensor networks [J]. *Journal of Computer Science and Technology*, 2014, 29(3): 470-486.

[5] HUANG L J, SETIA S. CORD: Energy-efficient reliable bulk data dissemination in sensor networks [C]// INFOCOM 2008. 27th IEEE International Conference on Computer Communications. Piscataway, NJ: IEEE Press, 2008: 574-582.

[6] ZHAO Z W, DONG W, BU J J, et al. Exploiting link correlation for core-based dissemination in wireless sensor networks [C]// Eleventh Annual IEEE International Conference on Sensing, Communication, and Networking (SECON). Piscataway, NJ: IEEE Press, 2014: 372-380.

[7] ZHU X R, TAO X P, GU T, et al. Target-aware, transmission power-adaptive, and collision-free data dissemination in wireless sensor networks [J]. *IEEE Transactions on Wireless Communications*, 2015, 14(12): 6911-6925.

[8] YU J G, WANG N N, WANG G H, et al. Connected dominating sets in wireless ad hoc and sensor networks—a comprehensive survey [J]. *Computer Communications*, 2013, 36(2): 121-134.

[9] TSENG Y C, NI S, CHEN Y, et al. The broadcast storm problem in a mobile ad hoc network [J]. *Wireless Networks*, 2002, 8(2-3): 153-167.

[10] HASS Z J, HALPERN J Y, LI L. Gossip based ad-hoc routing [C]// IEEE Annual Joint Conference: INFOCOM, IEEE Computer and Communications Societies. Piscataway, NJ: IEEE Press, 2002: 1707-1716.

[11] LEVIS P, PATEL N, CULLER D, et al. Trickle: a self-regulating algorithm for code propagation and maintenance in wireless sensor networks [C]// Conference on Symposium on Networked Systems Design & Implementation-volume. Berkeley, CA: USENIX Association, 2004: 1-14.

[12] KULIK J, HEINZELMAN W R. Negotiation-based protocols for disseminating information in wireless sensor networks [J]. *Wireless Networks*, 2002, 8(2/3): 169-185.

[13] STATHOPOULOS T, HEIDEMANN J, ESTRIN D. A remote code update mechanism for wireless sensor networks [R/OL]. (2003-11-01)[2022-04-24] https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.

[14] HUI J W, CULLER D. The dynamic behavior of a data dissemination protocol for network programming at scale [C]// SenSys: ACM Conference on Embedded Networked Sensor Systems. New York: ACM, 2004: 81-95.

[15] ZHENG X L, WANG J L, DONG W, et al. Bulk data dissemination in wireless sensor networks: analysis, implications and improvement [J]. *IEEE Transactions on Computers*, 2016, 65(5): 1428-1439.

[16] AL-RIYAMI A, ZHANG N, KEANE J. An adaptive early node compromise detection scheme for hierarchical WSNs [J]. *IEEE Access*, 2019, 4: 4183-4206.

[17] XING K, LIU F, CHENG X Z, et al. Real-time detection of clone attacks in wireless sensor networks [C]// The 28th International Conference on Distributed Computing Systems. Piscataway, NJ: IEEE Press, 2008: 3-10.

[18] RAZA S, WALLGREN L, VOIGT T. SVELTE: Real-time intrusion detection in the Internet of Things [J]. *Ad Hoc Networks*, 2013, 11(8): 2661-2674.

[19] SHANMUGAM A, PARAMASIVAM J. A two-level authentication scheme for clone node detection in smart cities using Internet of Things [J]. *Computational Intelligence*, 2020, 36(3): 1-21.

[20] LOU Y X, ZHANG Y, LIU S L. Single hop detection of node clone attacks in mobile wireless sensor networks [J]. *Procedia Engineering*, 2012, 29: 2798-2803.

[21] PARNO B, PERRIG A, GLIGOR V. Distributed detection of node replication attacks in sensor networks [C]// 2005 IEEE Symposium on Security and Privacy. Piscataway, NJ: IEEE Press, 2005: 49-63.

[22] CORMEN T H, LEISERSON C E, RIVEST R L, et al. *Introduction to Algorithms* [M]. Boston: MIT Press, 2001: 89-91.

[23] MENG Y, HOU Z F, ANG D Y, et al. Single-round zero-knowledge proof scheme based on elliptic curves [J]. *Computer Technology and Development*, 2007, 17(12): 147-150.

[24] BALASUBRAMANIAN R, KOBLITZ N. The improbability that an elliptic curve has subexponential discrete log problem under the menezes-okamoto-vanstone algorithm [J]. *Journal of Cryptology*, 1998, 11(2): 141-145.

Note: Figure translations are in progress. See original paper for figures.