Encrypted Broadcast Protocols in Device Cooperative Relay Environments

Authors: Wei Zixuan

Date: 2025-11-19T00:00:00+00:00

Abstract

In large-scale IoT deployments, terminal nodes are often constrained by power consumption, cost, and installation location, preventing direct Internet connectivity and forcing reliance on nearby devices for data forwarding. In the absence of security mechanisms in the forwarding path, user privacy is readily exposed and data is vulnerable to tampering by malicious nodes. To address this issue, this paper designs a decentralized device collaboration relay encryption broadcast protocol for the scenario of "how non-networked devices can securely communicate through nearby networked devices." The protocol integrates broadcast encryption based on interpolation polynomials with a hierarchical μTESLA authentication mechanism, enabling non-networked devices to accomplish encrypted broadcasting and authenticated forwarding via nearby networked devices without additional hardware. The paper first presents the complete procedures for system initialization, key distribution, data broadcasting, and relay forwarding, and subsequently introduces dynamic polynomial updates and a group key chain strategy to accommodate frequent node joining and departure. Theoretical analysis demonstrates that the protocol achieves data confidentiality, collusion resistance, and forward and backward security while maintaining controllable communication overhead; compared with typical schemes, user-side key storage is reduced from O(log N) to constant O(1), and relay node caching requirements are effectively constrained. Further discussion reveals that the distribution density of networked devices directly impacts latency and delivery rate, and that routing optimization and node incentive mechanisms remain necessary in extremely sparse network scenarios, constituting the primary direction for future work. Overall, this protocol provides a practical secure communication solution for IoT deployments in constrained scenarios such as emergency communications and underground facility monitoring.

Full Text

Abstract

In large-scale IoT deployments, terminal nodes are often constrained by power consumption, cost, and installation location, preventing direct Internet connectivity and forcing reliance on nearby devices for data forwarding. When forwarding paths lack security mechanisms, user privacy becomes vulnerable to exposure and malicious tampering. Addressing this challenge, this paper designs a decentralized encrypted broadcast protocol with device-collaborative relays that enables offline devices to communicate securely without requiring additional hardware modules. The protocol combines broadcast encryption based on interpolation polynomials with a hierarchical μTESLA authentication mechanism, and specifies a complete workflow including system initialization, key distribution, data broadcasting, and relay forwarding. To cope with user churn, we further introduce dynamic polynomial updates and grouped key chains to maintain lightweight key management on resource-constrained nodes. Theoretical analysis demonstrates that the protocol achieves confidentiality, collusion resistance, and forward/backward security while keeping communication overhead manageable. Compared with typical schemes, user-side key storage is compressed from O(log N) to constant O(1), and relay node buffer requirements are effectively bounded. Further discussion reveals that the density of connected devices directly impacts latency and delivery ratio; in extremely sparse network scenarios, complementary routing optimization and node incentive mechanisms remain necessary, constituting the main direction for future work. Overall, this protocol provides a practical security communication approach for IoT deployments in constrained scenarios such as emergency communications and underground facility monitoring.

In many real-world IoT deployments, a considerable portion of sensing devices cannot maintain direct Internet connectivity because of battery constraints, hardware cost, or harsh installation environments. These "offline" nodes must rely on nearby connected devices to reach remote servers, raising serious concerns about confidentiality and message integrity along the relay path. Focusing on this practical setting, this paper designs a decentralized encrypted broadcast protocol with device-collaborative relays that allows offline devices to communicate securely without adding extra hardware modules. We examine how the density of connected devices affects latency and delivery ratio, and identify extremely sparse networks as the main limitation where complementary routing and incentive mechanisms are needed. These results suggest that the proposed protocol is a practical candidate for secure communication in emergency response systems and large-scale IoT deployments in remote areas.

Keywords: Broadcast encryption; Device-collaborative relay; Relay transmission; IoT security; Key management

1. Introduction

With the deep integration of 5G/6G and IoT technologies, sensing terminals have been widely deployed in industrial control, urban infrastructure, and environmental monitoring scenarios. Unlike traditional Internet terminals, these devices are often installed in mines, inside mountains, or enclosed factories, relying long-term on battery or energy harvesting power supplies, making them extremely sensitive to communication module power consumption. Practical deployments show that a significant portion of nodes, to save cost and energy, are not equipped with cellular or Ethernet interfaces, but instead interact with nearby devices via short-range wireless technologies such as Bluetooth and ZigBee, placing them in a logically "offline" state.

In emergency communications and remote area monitoring tasks, these offline nodes form "information islands" that are difficult to reach in a timely manner. On one hand, traditional satellite links or dedicated relay equipment are expensive and complex to maintain; on the other hand, centralized architectures suffer from single-point failures that can cause entire regions to lose data reporting capabilities. Apple' s "Find My" network leverages massive user devices to build a decentralized Bluetooth relay system, validating the feasibility of using existing terminals for collaborative forwarding, though its protocol details are not publicly disclosed and security analysis remains limited.

Broadcast encryption mechanisms require simultaneous satisfaction of confidentiality, collusion resistance, and dynamic user management. Typical schemes can be divided into stateful and stateless categories: the former, such as LKH multicast solutions, have short ciphertexts but incur high re-keying overhead during user join and revocation; the latter attempt to reduce central management pressure through pre-distributed keys or polynomial methods [1, 5]. Wang Shangping et al. proposed an interpolation polynomial-based scheme that reduces central storage burden, but computational complexity remains high in large-scale scenarios [2].

In relay communication, Lei Weijia et al. studied anti-eavesdropping collaborative relay transmission schemes under partial channel state information, enhancing security through physical layer design [4]; the μTESLA protocol achieves lightweight broadcast authentication through delayed key disclosure, finding extensive application in sensor networks. Qi Junfeng et al.' s hybrid multi-level μTESLA protocol supports hierarchical broadcasting for different node types [3], while Yang Ting et al.' s survey systematically summarized security assumptions and time synchronization challenges in IoT authentication protocols [6]. Overall, existing work offers respective advantages in broadcast encryption and authentication, but systematic solutions targeting the specific "offline-device to online-device" collaborative relay scenario remain insufficient.

presents a performance comparison of different broadcast encryption schemes.

3. System Model and Protocol Design

3.1 System Architecture

The protocol involves offline devices (source/destination nodes), connected devices (relay nodes), and a trusted center (KGC). As shown in [Figure 1: see original paper], offline devices initiate requests, and connected devices perform local legitimacy verification before relaying ciphertext to the server. Response messages return via the reverse path. When network links are temporarily interrupted, relay nodes employ a store-and-forward mechanism to cache packets, resuming forwarding once connectivity is restored.

3.2 Broadcast Encryption Scheme

Let the user set be $\mathcal{U}$, with $|\mathcal{U}| = N$, authorized set $\mathcal{S} \subseteq \mathcal{U}$, and revoked set $\mathcal{R} = \mathcal{U} \setminus \mathcal{S}$. The core idea utilizes interpolation polynomials for session key generation, enabling legitimate users to decrypt with constant storage overhead [2].

The trusted center selects a large prime p and randomly generates a $(k-1)$-degree polynomial:

$$F(x) = a_0 + a_{1x} + \cdots + a_{k-1}x^{k-1} \pmod{p},$$

and selects k distinct points (x_i, y_i) as system public parameters. User U_i receives secret parameters $H_i = (H_i^x, H_i^y)$ and prime P_i, satisfying $P_{0P}1 \cdots P_N > p$. These parameters enable local reconstruction of polynomial points and session keys.

Confidentiality: Based on the interpolation polynomial structure, unauthorized users possessing fewer than k valid point pairs cannot recover polynomial $F(x)$, making session key computation infeasible [2]. Combining session keys with symmetric encryption algorithms $SEnc$ ensures ciphertext indistinguishability under IND-CCA2 (formal proof omitted).

Collusion Resistance: Even if fewer than k unauthorized users collude, they cannot uniquely determine $F(x)$ and thus cannot recover legitimate session keys. This property ensures the protocol resists multi-user joint attacks under reasonable parameter selection.

Forward and Backward Security: Through polynomial version updates and key chain unidirectionality, revoked users cannot decrypt subsequent session keys while newly joined users cannot deduce historical keys, thereby achieving both forward and backward security simultaneously.

3.3 Hierarchical μTESLA Authentication

To ensure data integrity and source authentication along relay paths, the protocol employs a two-layer key chain: a high-level chain manages multiple low-

level chains, with different message types bound to different low-level chains to achieve hierarchical authentication [3].

The main steps include: key chain initialization, time synchronization, MAC-based message authentication, and delayed key disclosure verification. Through key chain grouping and rolling updates, the protocol supports multiple service types and limits the impact scope of single key leakage without imposing excessive communication burden [3, 6].

3.4 Collaborative Relay Process

The collaborative relay workflow roughly includes request verification, secure connection establishment, ciphertext forwarding, temporary caching, and response backhaul. Relay nodes process only ciphertext and authentication information without accessing plaintext content. For temporarily unreachable destination servers, relay nodes adopt store-and-forward strategies combined with simple incentive mechanisms (such as forwarding credits or local statistics) to encourage connected devices to participate in relaying [4].

4. Security Analysis

summarizes the primary security properties [3, 6].

Security Property	Implementation Mechanism	Attack Type Resistance
Confidentiality	Interpolation polynomial encryption	Eavesdropping
Authentication	Hierarchical multi-level μTESLA	Data tampering
Integrity	Digital signatures/time synchronization	Replay attacks
Forward Security	Parameter updates	Revoked user attacks
Backward Security	Key chain unidirectionality	New user historical cracking
Collusion Resistance	Polynomial threshold k	Multi-user joint attacks

5. Performance Analysis

Communication overhead primarily comprises encryption parameters, MACs, and relay control information. Benefiting from polynomial methods and hierarchical key chain design, user-side key storage is compressed to constant $O(1)$, while relay node caching scales only linearly with local traffic volume. In terms of computational complexity, polynomial interpolation and evaluation costs are lower than typical public-key schemes, making them suitable for resource-constrained terminals [1, 2, 5]. provides a comparison with several representative schemes.

Scheme	User Key Storage	Encryption Communication Overhead	Decryption Computation Overhead	Dynamic User Management
This Protocol	$O(1)$	$O(k)$	Polynomial evaluation	Supported
RSA-based Scheme	$O(\log N)$	$O(\log N)$	Modular exponentiation	Supported
Bilinear Pairing Scheme	$O(\log N)$	$O(\log N)$	Pairing operations	Limited support
LKH Scheme	$O(\log N)$	$O(r \log N)$	Symmetric encryption	Supported

6. Conclusion

This paper proposes an encrypted broadcast protocol for device-collaborative relay environments to address secure access for offline devices. By combining interpolation polynomial broadcast encryption with hierarchical multi-level μTESLA authentication, the protocol achieves confidentiality, collusion resistance, and forward/backward security while maintaining low communication and storage overhead. Theoretical analysis and comparative results demonstrate the scheme' s potential for emergency communications and remote-area IoT deployments [1–3, 6].

Future work will proceed along two directions: first, designing more sophisticated relay selection and routing algorithms for actual scenarios to reduce latency in extremely sparse networks; second, exploring integration with post-quantum cryptographic techniques such as lattice-based cryptography to enhance long-term security against quantum computing threats.

References

[1] Chen Yanli, Yang Geng, Cao Xiaomei. Research on broadcast encryption schemes. *Computer Technology and Development*, 2010, 20(10): 189–194.

[2] Wang Shangping, Xie Kangle, Wang Xiaofeng, et al. A broadcast encryption scheme based on interpolation polynomials. *Journal of Electronics & Information Technology*, 2008, 30(12): 2996–2998.

[3] Qi Junfeng, Pan Wenlun, Leng Zijie. Hybrid multi-level μTESLA protocol for multi-type nodes. *Journal of University of Electronic Science and Technology of China*, 2025, 54(2): 233–241.

[4] Lei Weijia, Zuo Lijie, Xie Xianzhong. Anti-eavesdropping collaborative relay transmission scheme under partial channel state information. *Journal of Jilin University (Engineering and Technology Edition)*, 2015, 45(5): 1658-1664.

[5] Zhang Jinman. Research and application of broadcast encryption schemes [D]. Hangzhou Dianzi University, 2013.

[6] Yang Ting, Zhang Guanghua, Liu Ling, Zhang Yuqing. Survey on IoT authentication protocols. *Journal of Cryptologic Research*, 2020, 7(1): 87-101.

Author Biography: Zixuan Wei (born 2007), male, native of Ganzhou, Jiangxi, undergraduate student, research interests include computer applications.

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