Secure Cryptographic Broadcast Network Concept

1. Overview

This document describes a highly secure broadcast network designed for maximum privacy, integrity, and resistance against traffic analysis, spam, and replay attacks. The network enforces constant traffic from all users, uses strong cryptographic primitives, and obfuscates timing and metadata.

2. Network Architecture

The network is decentralized, with no central server. Each user node communicates over a broadcast channel, routing packets to all other users either directly or via a gossip-based routing protocol to maintain scalability.

3. Message (Packet) Sending Rules

- Each user must send exactly one packet every interval, where the interval is a random time between 1 and 5 minutes.
- If the user has no real message, a packet with random data is sent (dummy traffic).
- This ensures a constant and uniform traffic pattern to resist traffic analysis.
- Each packet has a fixed size of 1024 bytes to prevent size-based inference.

4. Packet Format

Each packet consists of the following structure:
1. First byte: Sender info flag
   - 0x01: Sender includes their public key and signs the packet.
   - 0x00: Sender is anonymous; no public key or signature included.
2. AES key and IV: Symmetric keys for encrypting the data, encrypted asymmetrically with the recipient's public key.
3. Encrypted receiver public key hash (to identify incoming packets).
4. Encrypted message data.
5. Optional sender public key (if sender info flag = 0x01).
6. Digital signature of the message data and the sender's + receiver's public key (if not anonymous).
7. Padded with random bytes to achieve a fixed packet size (1024 bytes).
8. Proof of Work

5. Cryptographic Technologies

- Symmetric Encryption: AES-256-GCM or ChaCha20-Poly1305 for authenticated encryption.
- Asymmetric Encryption: RSA-4096 or Elliptic Curve (e.g., Curve25519) to encrypt AES key and IV.
- Digital Signatures: Ed25519 or ECDSA for authenticating sender messages.
- Hash Functions: SHA3-256 or Blake2b for data integrity and proof of work.
- Proof of Work: Hashcash-style PoW requiring packet hash to have at least 5 leading zeros in binary.

6. Replay Protection and Packet Identification

- The packet hash (from the Proof of Work) (SHA3-256 or Blake2b) of the entire packet is used as the unique packet ID.
- Each receiver maintains a cache of recent packet IDs to reject duplicates, preventing replay attacks.
- Cache entries expire after a configurable time window to save memory.

7. Traffic Obfuscation and Timing

- Random delay between 1 and 5 minutes before sending to the next packet.
- Continuous dummy traffic ensures uniform traffic patterns.
- Fixed packet size (1024 bytes) prevents packet size-based analysis.
- Random padding used inside packets to maintain constant size.

8. Security Considerations

- Anonymous packets (flag=0x00) are not signed and carry no sender public key.
- PoW is required for all packets to prevent spam and DoS attacks.
- Replay attacks prevented via packet ID caching.
- Forward secrecy is recommended via ephemeral keys and key rotation.

9. Scalability and Routing

- Direct one-to-one sending to all users does not scale.
- Gossip-based broadcast enables efficient dissemination of packets across the network.
- Nodes forward packets to all neighbors until all receive them.

10. Summary

This network design ensures strong cryptographic protections, anonymity options, traffic pattern obfuscation, and spam prevention.
Technologies such as AES-GCM, Ed25519, SHA3, and PoW are combined to provide confidentiality, authenticity, integrity, and DoS resistance.
Random delays and fixed packet sizes mask traffic analysis vectors.
Future work includes scalable routing, sybil resistance, and forward secrecy implementations.