[PIXPATCH]

A encrypted and resilient dispatch system

Arin Upadhyay
HackYeah 2025 (4-5 Oct)

Problem

- In conflict zones, traditional network infrastructure like cables and routers are common points of failure and attack by adversaries because static network architecture is unable to work with changing topology. This makes communication and connectivity faulty and unreliable.
- A solution for this is flood networking. However, existing solution do not provide substantial security and are vulnerable to eavesdropping or other attacks. Security of information is paramount in conflict zones because they can contain sensitive information like military strategies
- Flood networks are very useful broadcast type messages like news, disaster warnings or rescue calls.

Why existing solutions fail

- Satellite phones: Expensive, requires clear sky view, limited bandwidth, traceable location.
- WhatsApp/Signal: Requires internet infrastructure, centralized servers can be blocked, not topology-agnostic.
- Military tactical radios: Expensive, limited range, can be jammed, requires specific hardware.
- Ham radio: Not encrypted, no spam resistance, easy to trace.

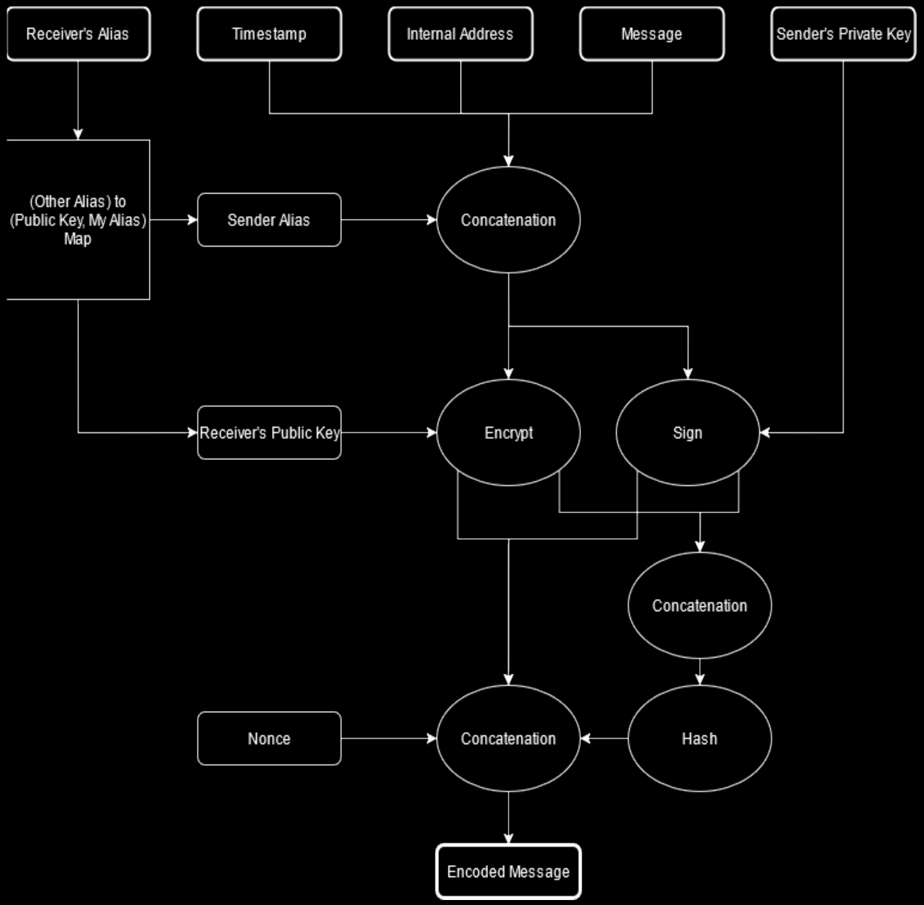
Solution

- PIXPATCH uses a novel encrypted flood protocol that combats all of these issues and more.
- The protocol is a zero-trust, encrypted flood protocol that uses a modern crypto stack to provide resilient and untraceable peer-to-peer messaging in degraded network environments.
- Its topology-agnostic and fault-resilient flooding design along with maximum security makes it a perfect fit for the application.
- It also has features like built-in spam resistance and perfect forward secrecy.
- It can also be used in inter-satellite communication which presents similar requirements.

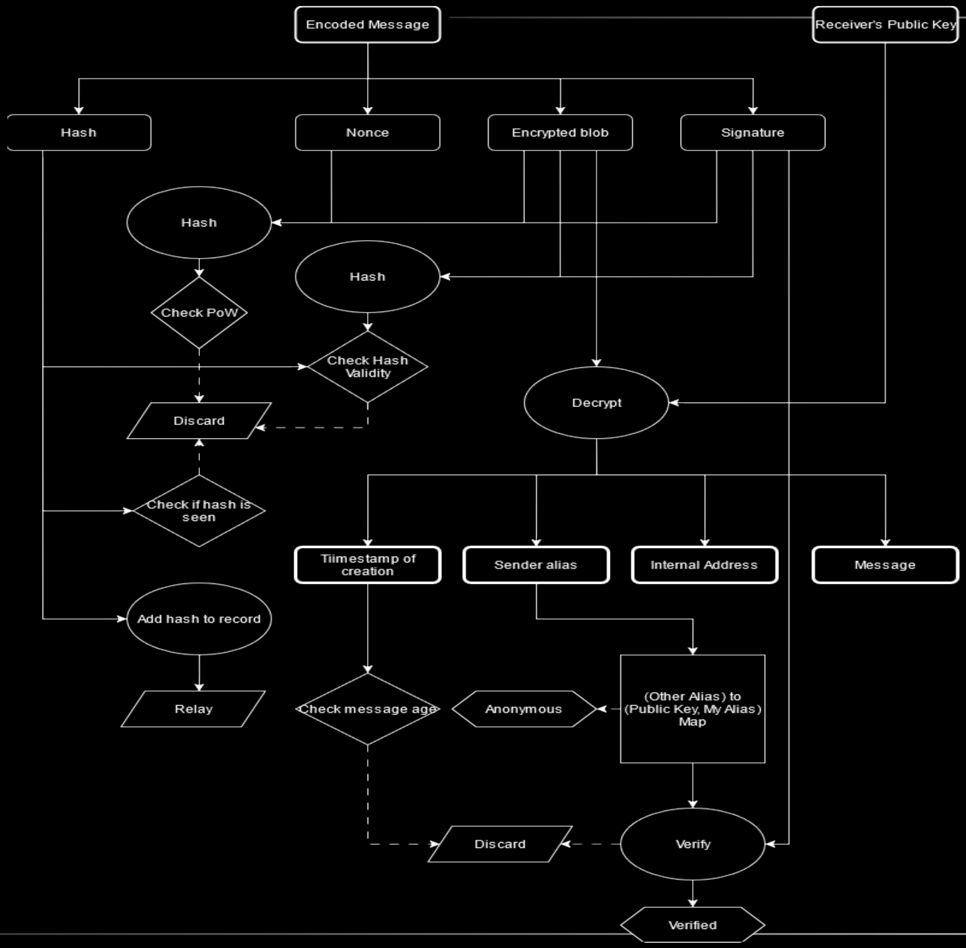
How it works

- A unicast message is encoded (as specified by the protocol) and relayed to any and all nodes.
- This message is flooded all throughout the network in way that only the intended recipient is able to decrypt the message. It is also designed to make it impossible to eavesdrop or observe the network to find out the involved nodes. Metadata is also hidden from those not involved.
- This design makes it invulnerable to many attack vectors used today.
- It has emphemeral keys for forward secrecy, proof-of-work for spam resistance and deduplication, elliptical curve cryptography for fast encryption, written in C for maximum performance using industry standard library Monocypher.

How it works


Receiver's Alias
Timestamp
Internal Address
Message
Sender's Private Key
(Other Alias) to (Public Key, My Alias) Map
Sender Alias
Concatenation
Receiver's Public Key
Encrypt
Sign
Concatenation
Nonce
Concatenation
Hash
Encoded Message

How it works


Encoded Message
Receiver's Public Key
Hash
Nonce
Encrypted blob
Signature
Hash
Hash
Check PoW
Check Hash Validity
Decrypt
Discard
Check if hash is seen
Tiimestamp of creation
Sender alias
Internal Address
Message
Add hash to record
Relay
Check message age
Anonymous
(Other Alias) to (Public Key, My Alias) Map
Discard
Verify
Verified

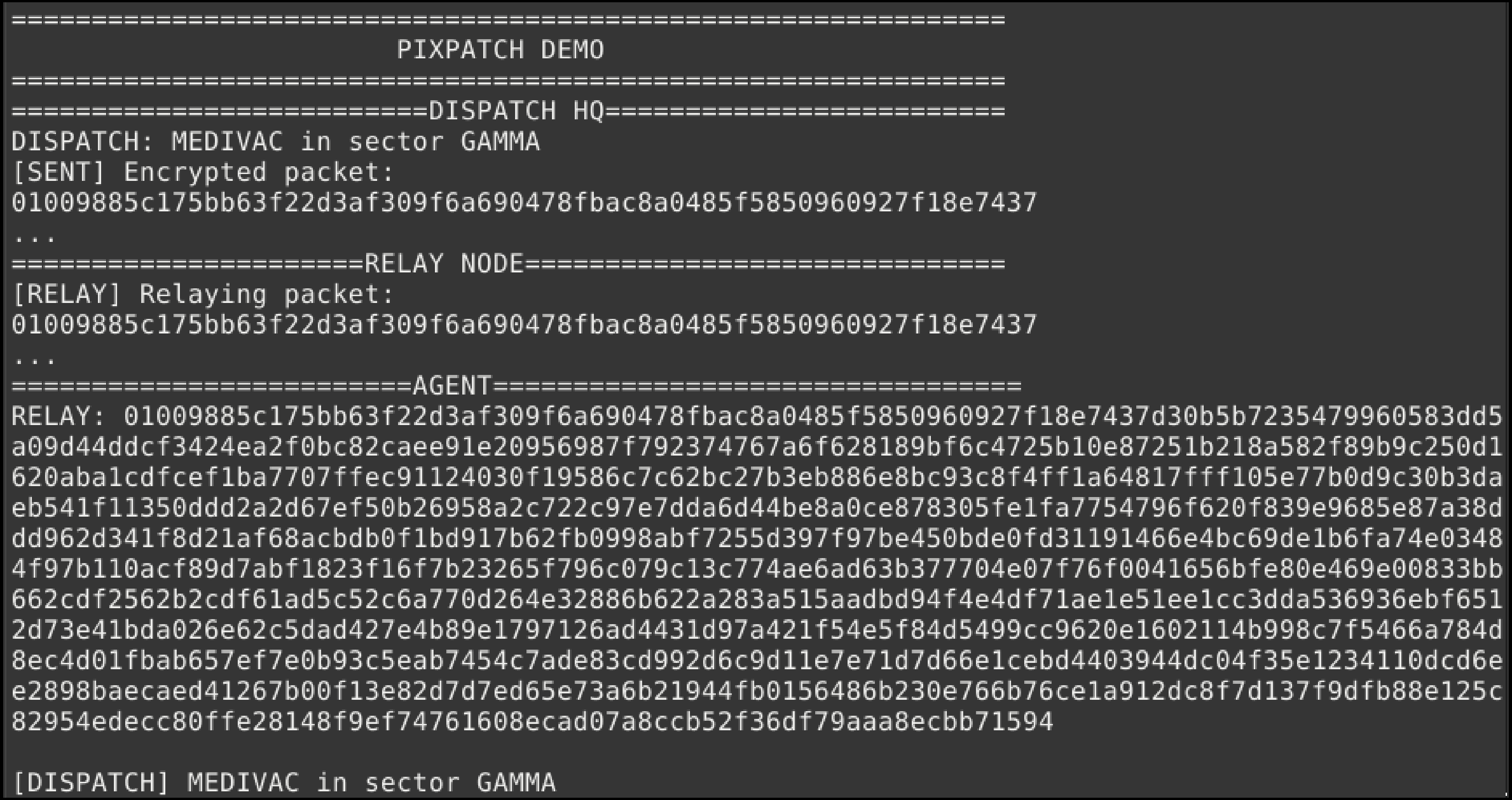
Key features

- Zero infrastructure dependency: Works without any central servers or internet.
- Topology-agnostic: Adapts to any network structure automatically.
- End-to-end encrypted: Military-grade encryption using X25519 and ChaCha20-Poly1305.
- Untraceable: Impossible to determine sender or recipient from network traffic.
- Spam resistant: Built-in proof-of-work prevents message flooding.
- Perfect forward secrecy: Compromising one message doesn't compromise others.
- High performance: Written in C with industry-standard Monocypher library.

Use cases

- Military operations: Secure command and control in degraded networks. Cannot be jammed, intercepted, or traced to source.
- War correspondents: Send reports from areas without infrastructure. Source protection and censorship resistance.
- Humanitarian aid: Coordinate relief efforts in disaster zones. Works when cellular towers are down.
- Emergency broadcasts: Disaster warnings, rescue calls, public alerts spread rapidly through all connected devices.
- Whistleblowers & activists: Censorship-resistant communication with complete anonymity.
- Space & research: Inter-satellite or remote research station communication where central servers are infeasible.

Demo



```
==============================================================
                        PIXPATCH DEMO
==============================================================
==========================DISPATCH HQ=========================
DISPATCH: MEDIVAC in sector GAMMA
[SENT] Encrypted packet:
01009885c175bb63f22d3af309f6a690478fbac8a0485f5850960927f18e7437
...
======================RELAY NODE==============================
[RELAY] Relaying packet:
01009885c175bb63f22d3af309f6a690478fbac8a0485f5850960927f18e7437
...
=========================AGENT=================================
RELAY: 01009885c175bb63f22d3af309f6a690478fbac8a0485f5850960927f18e7437d30b5b7235479960583dd5
a09d44ddcf3424ea2f0bc82caee91e20956987f792374767a6f628189bf6c4725b10e87251b218a582f89b9c250d1
620aba1cdfcef1ba7707ffec91124030f19586c7c62bc27b3eb886e8bc93c8f4ff1a64817fff105e77b0d9c30b3da
eb541f11350ddd2a2d67ef50b26958a2c722c97e7dda6d44be8a0ce878305fe1fa7754796f620f839e9685e87a38d
dd962d341f8d21af68acbdb0f1bd917b62fb0998abf7255d397f97be450bde0fd31191466e4bc69de1b6fa74e0348
4f97b110acf89d7abf1823f16f7b23265f796c079c13c774ae6ad63b377704e07f76f0041656bfe80e469e00833bb
662cdf2562b2cdf61ad5c52c6a770d264e32886b622a283a515aadbd94f4e4df71ae1e51ee1cc3dda536936ebf651
2d73e41bda026e62c5dad427e4b89e1797126ad4431d97a421f54e5f84d5499cc9620e1602114b998c7f5466a784d
8ec4d01fbab657ef7e0b93c5eab7454c7ade83cd992d6c9d11e7e71d7d66e1cebd4403944dc04f35e1234110dcd6e
e2898baecaed41267b00f13e82d7d7ed65e73a6b21944fb0156486b230e766b76ce1a912dc8f7d137f9dfb88e125c
82954edecc80ffe28148f9ef74761608ecad07a8ccb52f36df79aaa8ecbb71594

[DISPATCH] MEDIVAC in sector GAMMA
```

Future work

- Making the setup process easier for a non-technical person to setup and use.
- Using it with radio comm hardware for wireless and geography-free communication.
- Mobile application for easier deployment in the field.
- Add better TUI

Thank you