[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: Some static infrastructure is still present. Need to blindly trust the relayers and routing is involved.
- Ham radio: Not encrypted, no spam resistance, easy to trace.

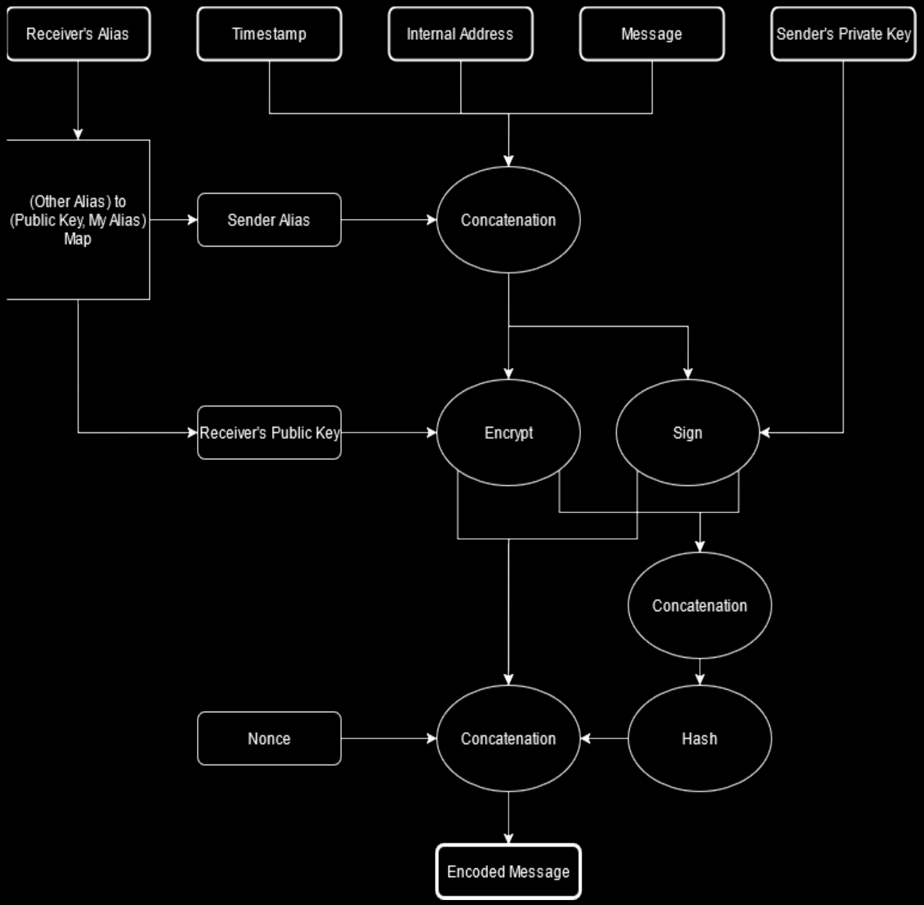
Solution

- 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.

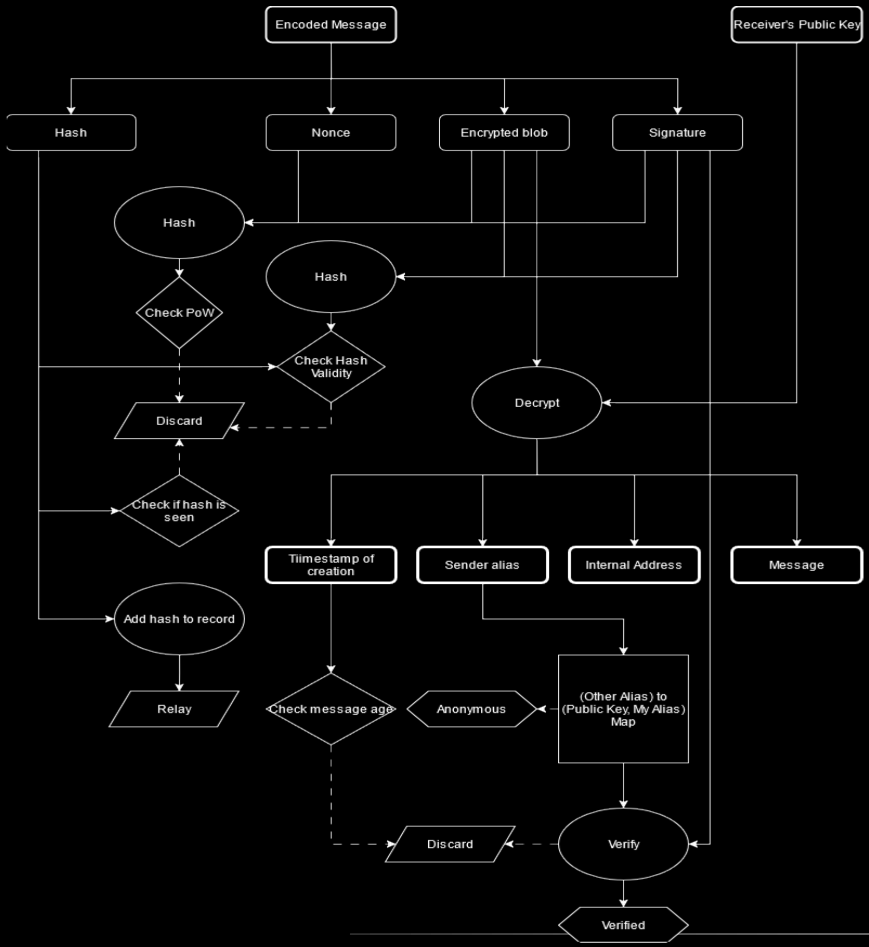
How it works

- 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.
- Replay attacks are countered with max age, PoW hashes and can be further mitigated with higher layer methods like message counters etc.
- 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.

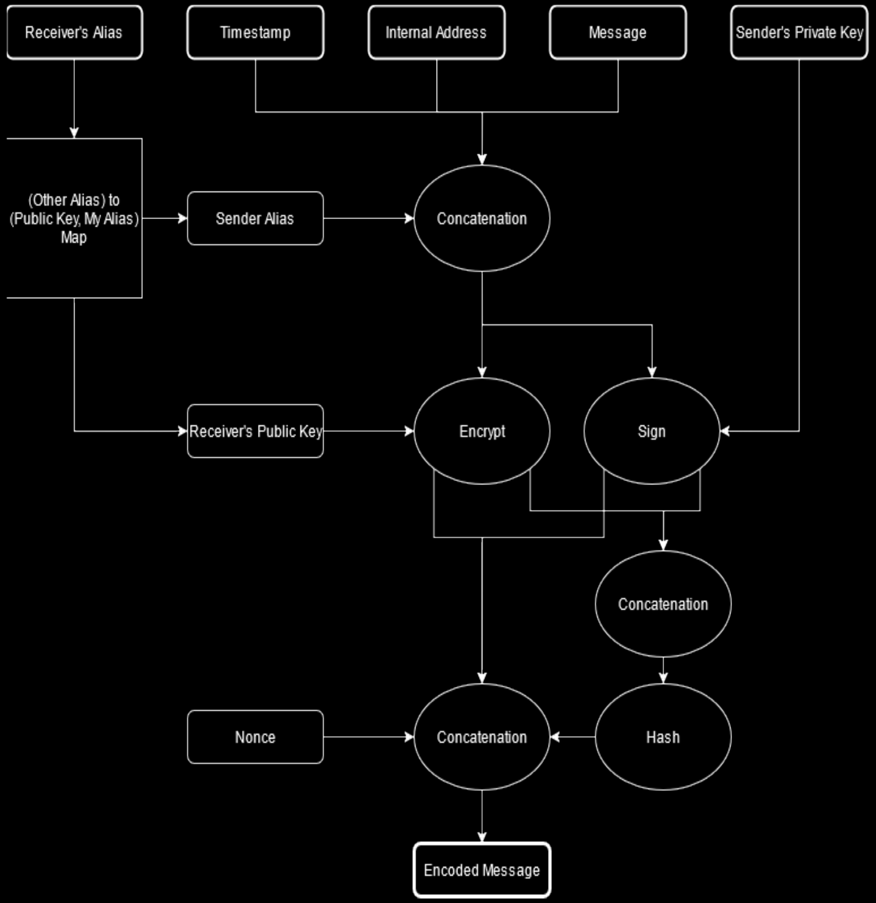
How it works


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



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

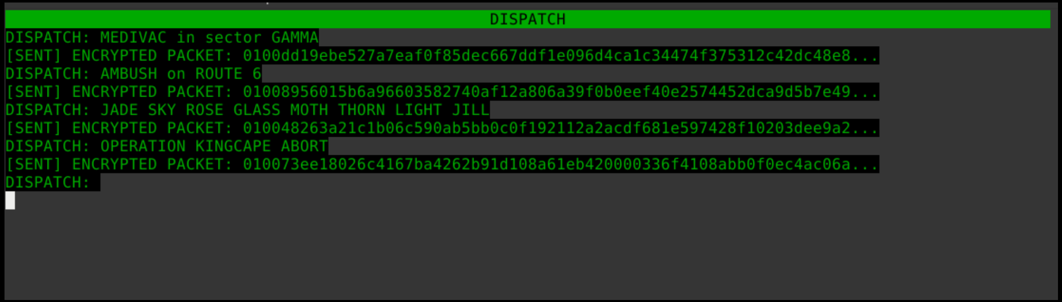
Key features

- Zero infrastructure dependency: Works without any central servers or internet.
- Topology-agnostic: Adapts to any network structure automatically.
- End-to-end encrypted: Modern encryption stack 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.

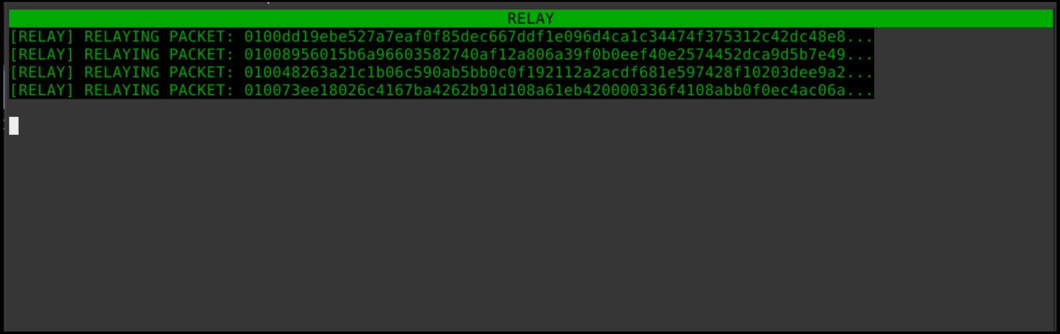
Use cases

- 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.

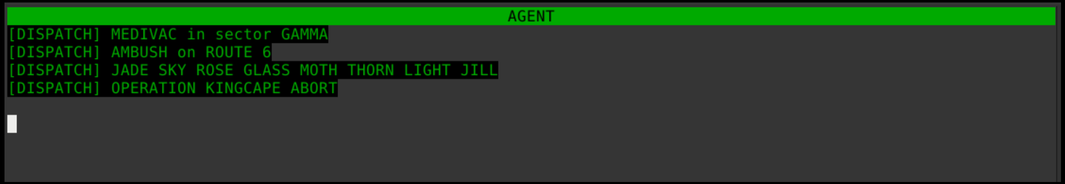
Demo



```
DISPATCH: MEDIVAC in sector GAMMA
[SENT] ENCRYPTED PACKET: 0100dd19ebe527a7eaf0f85dec667ddf1e096d4ca1c34474f375312c42dc48e8...
DISPATCH: AMBUSH on ROUTE 6
[SENT] ENCRYPTED PACKET: 01008956015b6a96603582740af12a806a39f0b0eef40e2574452dca9d5b7e49...
DISPATCH: JADE SKY ROSE GLASS MOTH THORN LIGHT JILL
[SENT] ENCRYPTED PACKET: 010048263a21c1b06c590ab5bb0c0f192112a2acdf681e597428f10203dee9a2...
DISPATCH: OPERATION KINGCAPE ABORT
[SENT] ENCRYPTED PACKET: 010073ee18026c4167ba4262b91d108a61eb420000336f4108abb0f0ec4ac06a...
DISPATCH:
```



```
[RELAY] RELAYING PACKET: 0100dd19ebe527a7eaf0f85dec667ddf1e096d4ca1c34474f375312c42dc48e8...
[RELAY] RELAYING PACKET: 01008956015b6a96603582740af12a806a39f0b0eef40e2574452dca9d5b7e49...
[RELAY] RELAYING PACKET: 010048263a21c1b06c590ab5bb0c0f192112a2acdf681e597428f10203dee9a2...
[RELAY] RELAYING PACKET: 010073ee18026c4167ba4262b91d108a61eb420000336f4108abb0f0ec4ac06a...
```



```
[DISPATCH] MEDIVAC in sector GAMMA
[DISPATCH] AMBUSH on ROUTE 6
[DISPATCH] JADE SKY ROSE GLASS MOTH THORN LIGHT JILL
[DISPATCH] OPERATION KINGCAPE ABORT
```

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