[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.

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.

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.

Thank you