Communication Pattern Privacy for Teams

Linda Briesemeister, SRI International

Karim Eldefrawy, Confidencial, Inc.

July 2023

SRI International®

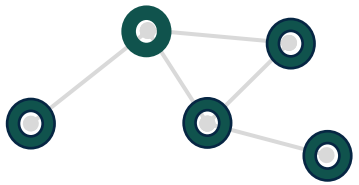
Communication patterns can expose a mission

Communication patterns can reveal sensitive team organization or mission information

…despite encrypted message contents!

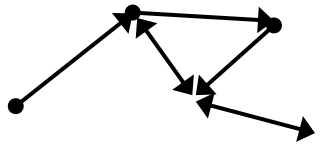
Network watchers may observe and infer

Communication Endpoints



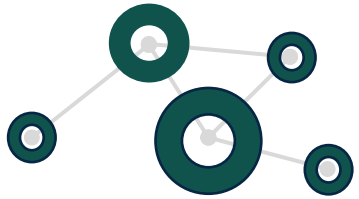
"who is talking to whom?"

Communication Direction



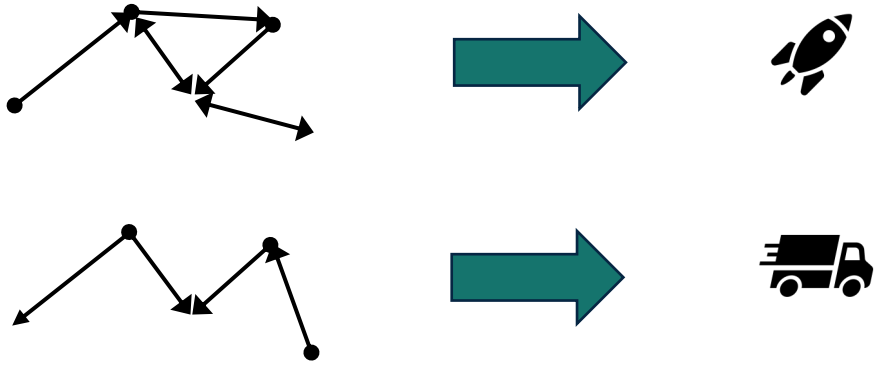
"who sends and who receives?"

Communication Hub



"critical node for team functions"

Correlation of Patterns with Events



"this chatter usually precedes a missile launch"

pico

The ***pico Conceal*** **network overlay**

obscures team messaging patterns

to **ensure communication pattern privacy**

even on ordinary devices while

communicating over untrusted networks.

Communication confidentiality versus pattern privacy

Message Content Confidentiality

A network observer cannot…

+ read the contents of an encrypted message unless the observer has the corresponding decryption key

Communication Pattern Privacy

A network observer cannot…

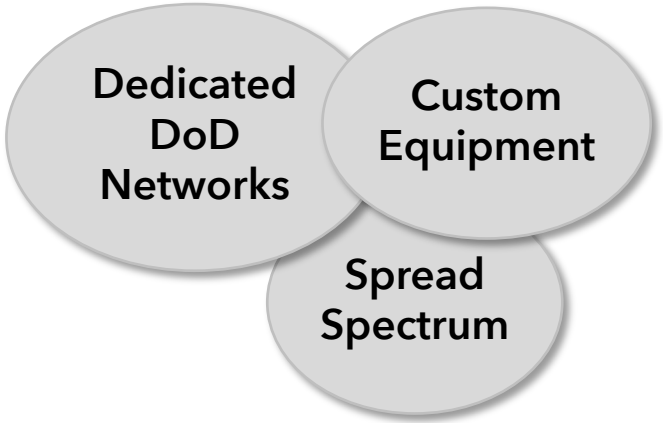
+ determine who is sending to whom
+ distinguish message senders from recipients
+ detect communication hubs
+ correlate communication patterns with other events

Who needs communication pattern privacy?

- Teams involved in intelligence and military missions
- Corporate executives or attorneys preparing for a merger
- Diplomats negotiating to diffuse an international crisis
- Police communicating with informants in large-scale criminal investigation
- Journalists and whistleblowers

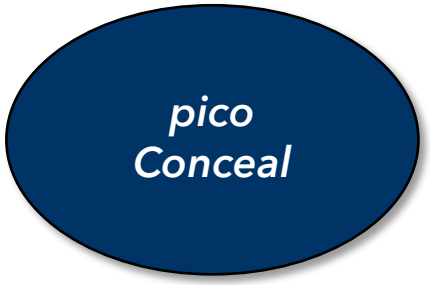
Technology for communication pattern privacy

Current Military Technology



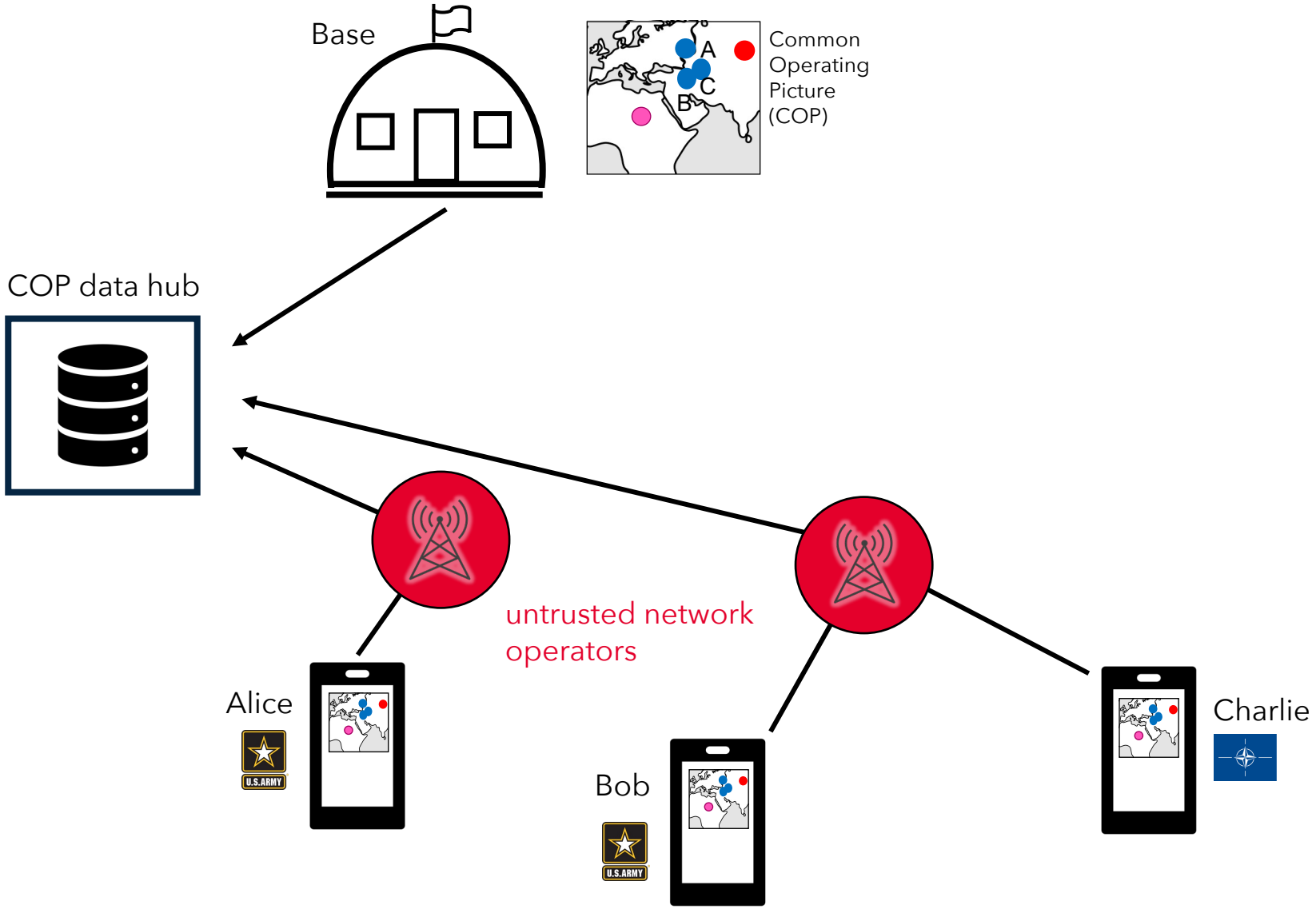
- Hides physical communication signals
- Special-purpose equipment: difficult to manage and share with mission partners

pico Conceal Technology

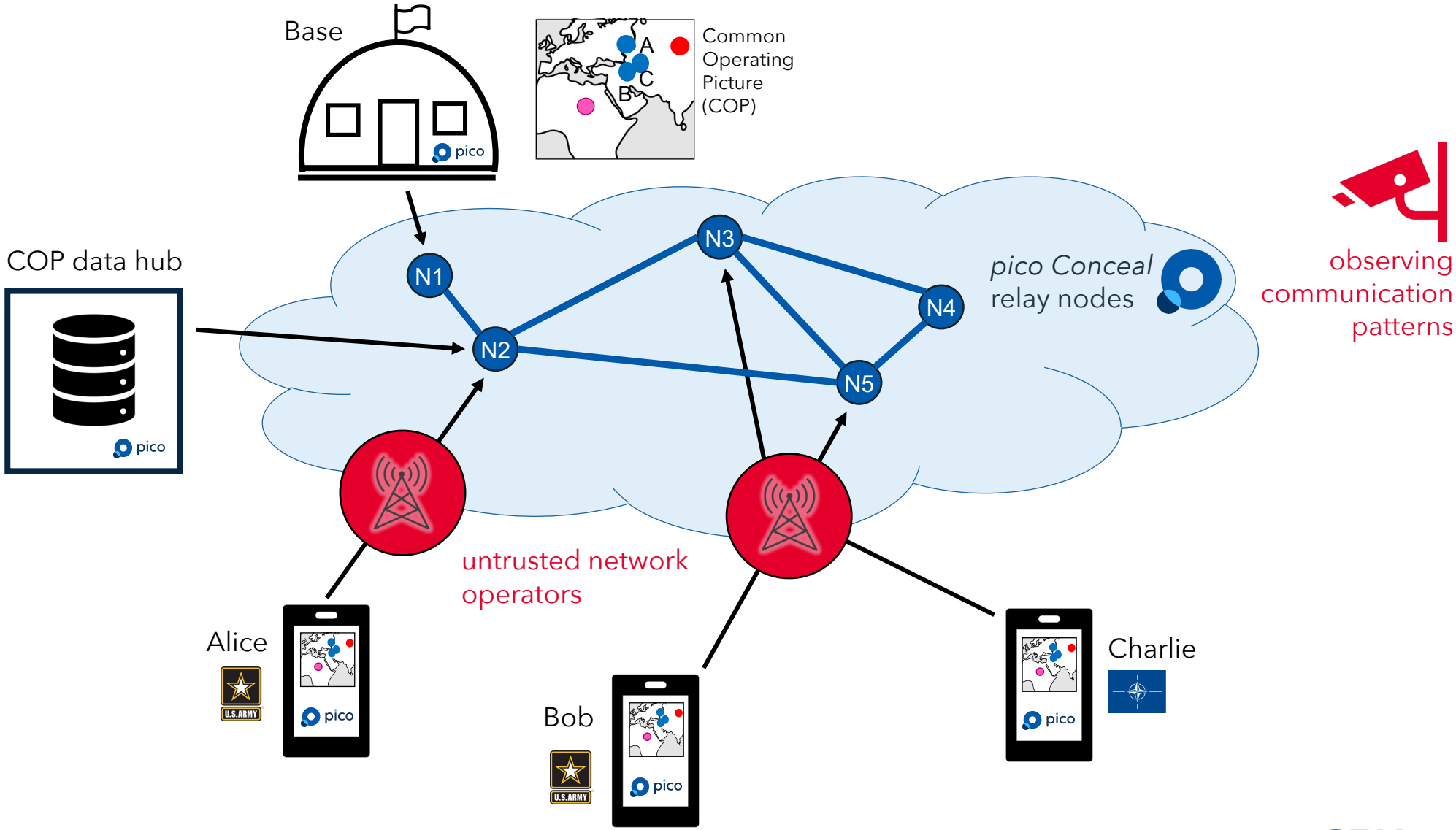


- Hides IP communication endpoints
- Software-based: endpoint application interacts with middleware-layer network overlay
- Deploys onto common software platforms
- Share with mission partners; de-provision after mission completion

Blue Force Tracking today



Blue Force Tracking with *pico Conceal*



SRI International®

Why use *pico Conceal*?

- **Hides communication patterns** from network observers, including untrusted 5G operators
- **Resilient** to node and link failures
- **Stealthy operation** of overlay network

pico Conceal Components and Roadmap

Today

- Client software written in Python and running in Docker containers
- Relay node server software written in Python and running in Docker containers
- Management scripts for local or cloud-based container deployments

Roadmap

- Port client software to mobile platforms such as Android
- Re-write software in Rust
- Develop application programming interface (API) for overlay access
- Develop sample application and documentation to aid technology integrators
- Develop operator dashboard including dynamic stealth management

Summary

pico

- Communication pattern privacy is essential for many critical missions
- *pico Conceal* technology obscures message patterns to protect high-consequence team communication

To learn how *pico Conceal* technology can enhance your communication security offering, contact us at pico-conceal@sri.com