Tactical Computing and Communications (TCC)

Grace Lewis

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM-0004099

Agenda

Motivation

Previous Work

- Tactical Cloudlets
- Delay-Tolerant Networking (DTN)

Trusted Identities in Disconnected Environments

Secure Service VM Migration

Delay-Tolerant Data Sharing

Summary

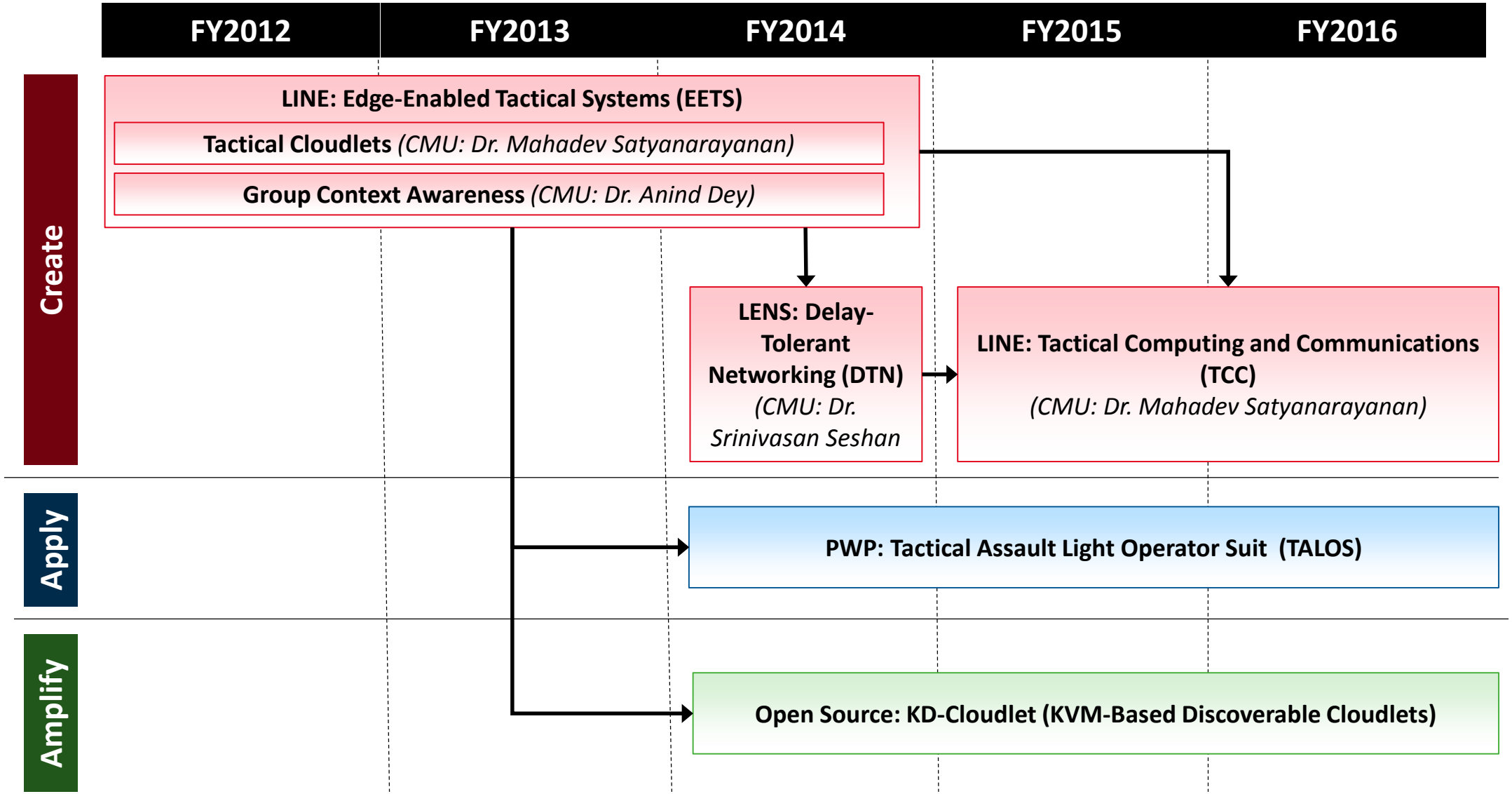
Motivation

Soldiers and first responders operating in tactical environments increasingly make use of mobile systems for mission support

However, dynamic context, limited computing resources, disconnected-intermittent-limited (DIL), network connectivity, and high levels of stress pose a challenge

TCC develops architectures and technologies that provide efficient and secure computing and communications for teams operating in tactical environments

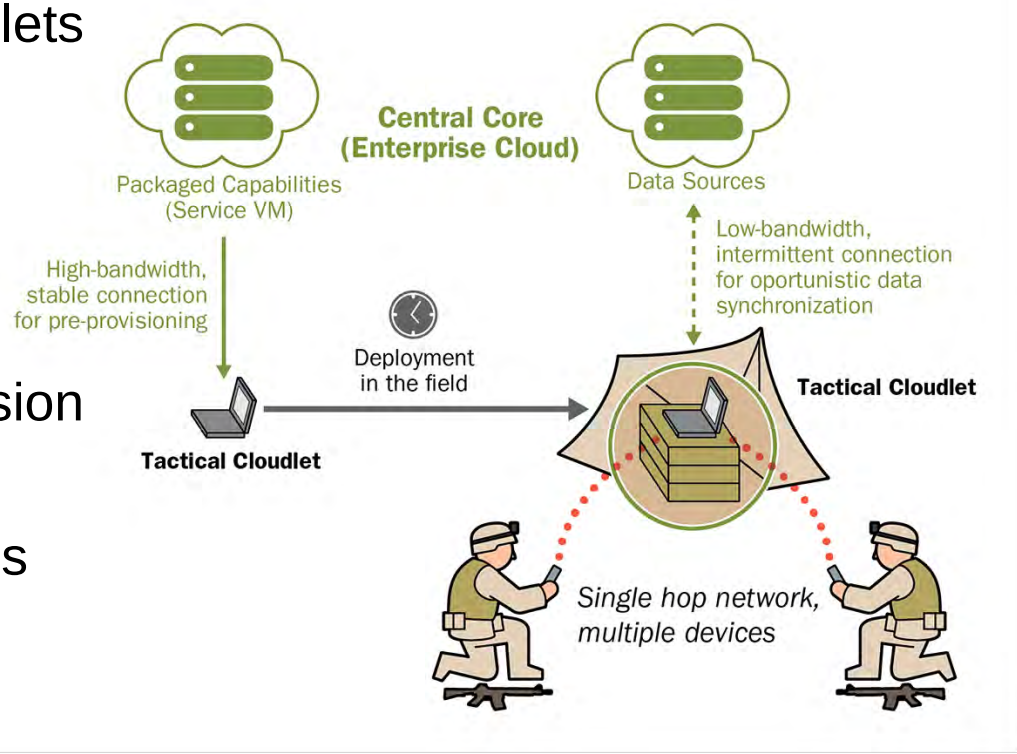
Overview of Results



Previous Work: Tactical Cloudlets

Forward-deployed, discoverable, virtual machine (VM) based cloudlets that can be hosted on vehicles or other platforms to provide

- infrastructure to offload computation
- forward data-staging for a mission
- data filtering to remove unnecessary data from streams intended for dismounted warfighters
- collection points for data heading for enterprise repositories



Features

- Pre-Provisioned Cloudlets with App Store
- Standard Packaging of Service VMs
- Optimal Cloudlet Selection
- Cloudlet Management Component
- Cloudlet Handoff/Migration
- Secure Key Generation and Exchange

Previous Work: Delay-Tolerant Networking (DTN)

Extensions to the existing DTN standard for priorities, staleness, replacement, and redundancy monitoring to increase bandwidth efficiency in DIL environments

	Connected	Disconnected	Reconnecting
GOALS	**Maintain shared group context** **Make best use of available bandwidth**	**Applications continue to function** **Predict state where possible**	**Re-establish shared group context as quickly and accurately as possible**
DTN NODE TASKS	Pre-cache data likely to be relevant later in the mission Delay transmission of noncritical data	Predict location of teams based on mission plan Provide connectivity map to help the user reconnect	Prioritize synchronization of critical messages Eliminate redundant messages

Used DTN metadata extension block to attach key-value pairs to bundles

- Time and location
- Priority
- Type of payload (image, voice, video, text, …)
- Set of tags describing payload content (building, crowd, fire, injured person, …)

Trusted Identities in Disconnected Environments [1]

Motivation

- Common solution for establishing trust is to create and share credentials in advance, and then use an online trusted authority for validation
- However, characteristics of tactical environments do not consistently provide access to a credential repository or online authority

Solution Requirements

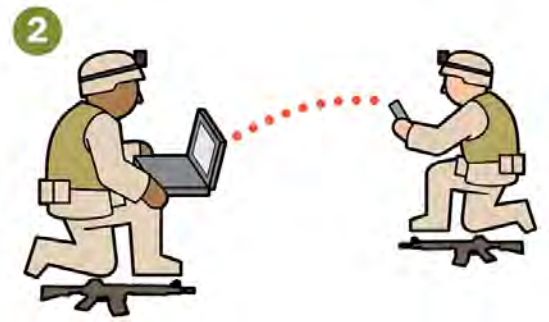
1. Cannot require network connectivity to a third party for credential generation or validation
2. Cannot place any specific security requirements on hardware
3. Cannot require pre-provisioning of credentials on the mobile devices
4. Must address the threats of a tactical environment

Trusted Identities in Disconnected Environments 2

Admin logs into the Cloudlet Manager to start the Bootstrapping process

Bootstrapping

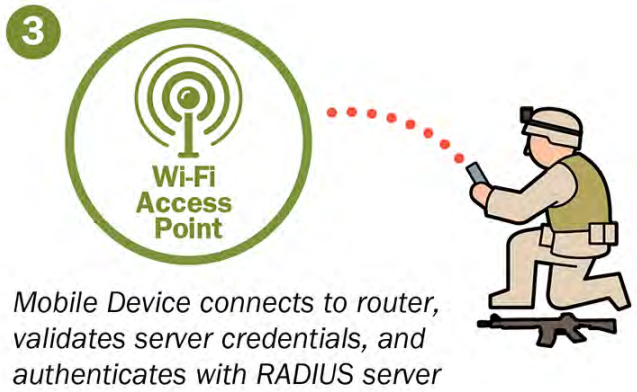
- Generation of *Cloudlet Credentials* using IBE (Identity-Based Encryption)
- Setup of *RADIUS Server* with *Cloudlet Credentials*



User connects mobile device to the cloudlet, and upon visual confirmation the admin starts the pairing process

Pairing

- Generation of *Device Credentials* using IBE
- Transfer to device using Bluetooth or USB, plus visual confirmation
- Transfer to *RADIUS Server*

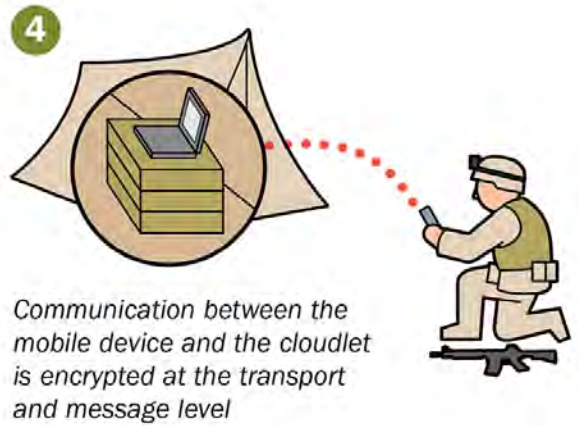


Mobile Device connects to router, validates server credentials, and authenticates with RADIUS server

Wi-Fi Authentication

RADIUS Server implements Wi-Fi WPA2-Enterprise 802.1X EAP-TTLS with PAP

- Device receives cloudlet credentials and validates
- Devices sends its credentials for validation



Communication between the mobile device and the cloudlet is encrypted at the transport and message level

API Requests

- Device exchanges encrypted messages with the cloudlet
- Each exchange is validated against authorized device list

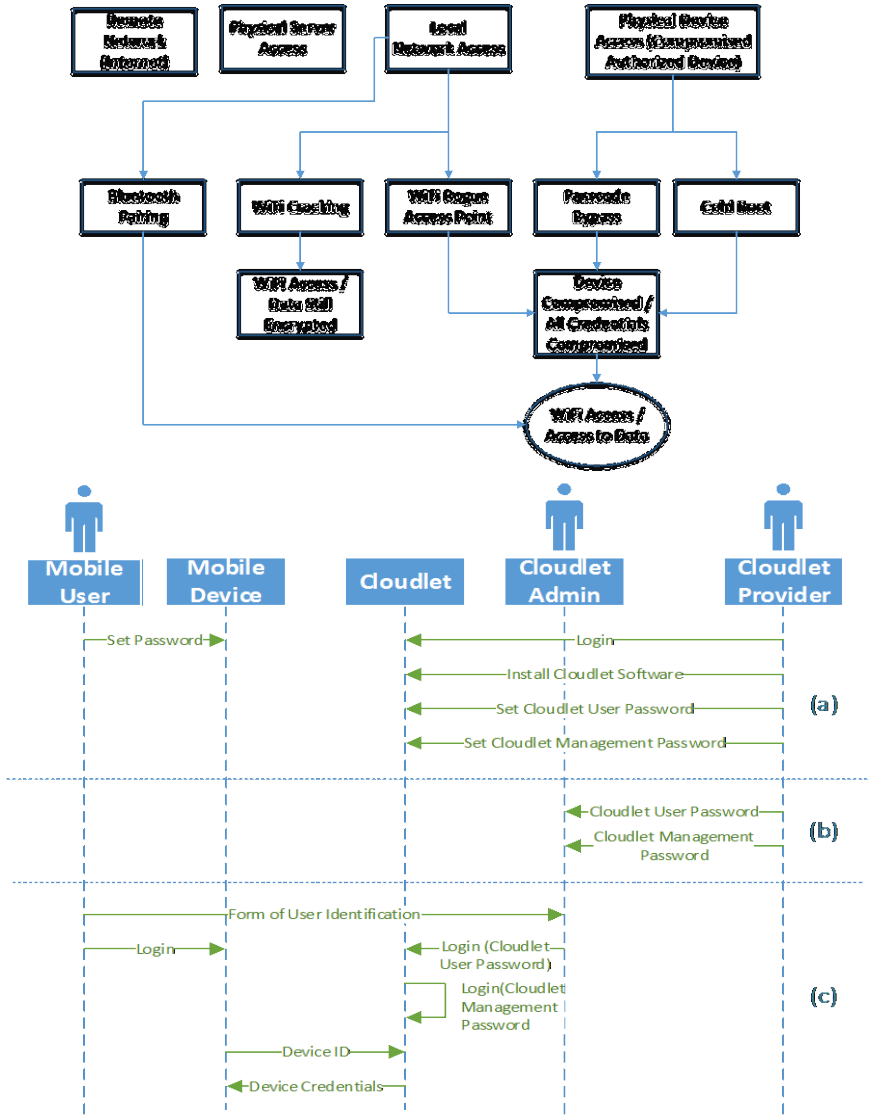
Device Credential Revocation

- Automatic due to timeout: Bootstrapping requires setting up mission duration
- Manual due to known loss or compromise: Cloudlet Manager component has revocation option

Trusted Identities in Disconnected Environments 3

Validation

- Threat modeling
  - Identified and prioritized 14 threats
  - Solution addresses 12 threats (directly or indirectly)
- Vulnerability analysis
  - Architectural and technical analysis of possible vulnerabilities using a simple attack tree based on the threat model
- Ceremony analysis
  - Ceremonies include all protocols, applications with a user interface, and security provisioning workflows — nothing is out of band



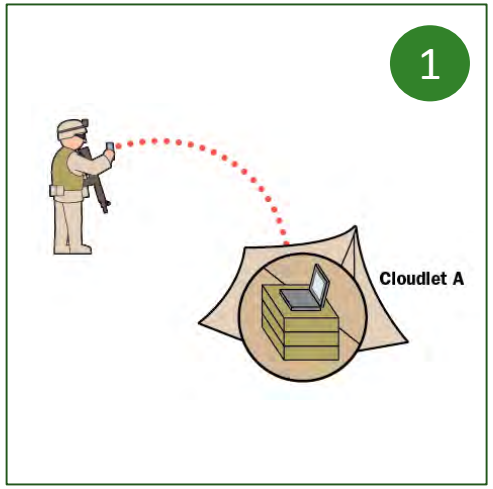
Secure Service VM Migration [1]

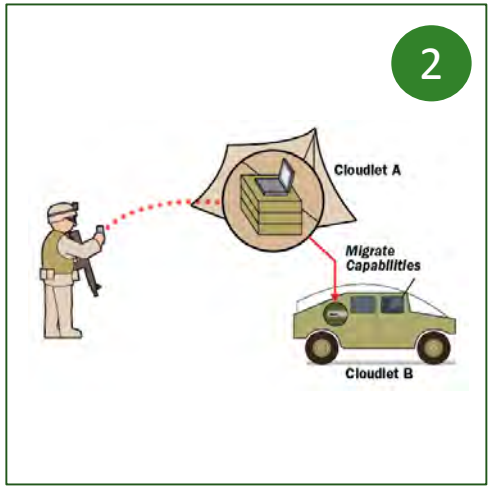
Service VM Migration involves transferring a running service VM on a source cloudlet to a target cloudlet

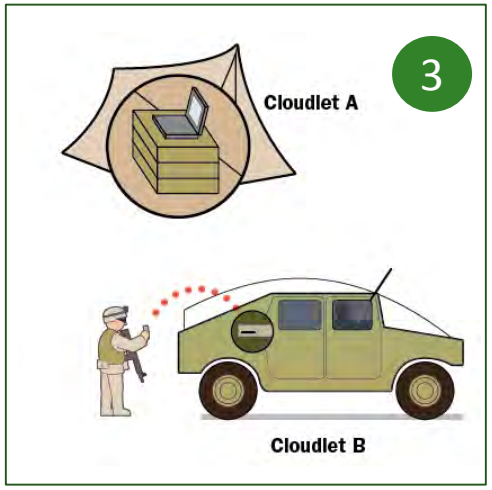
- VM migration
- Device “migration”

Challenges

- Establishing trust between cloudlets for credential exchange
- Transferring device trust from source to target cloudlet





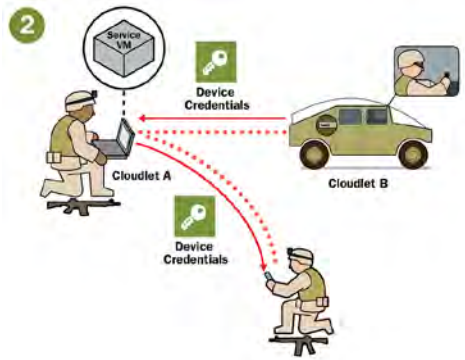


Secure Service VM Migration 2

Cloudlet Admins exchange temporary keys using their radios

Cloudlet Pairing

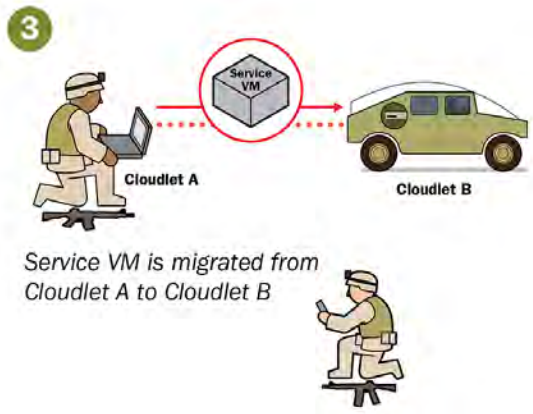
- Cloudlet Admins exchange temporary keys over voice
- Keys are used to setup a temporary channel
- Cloudlet credentials are exchanged over the temporary channel



Cloudlet B generates and sends device credentials to Cloudlet A

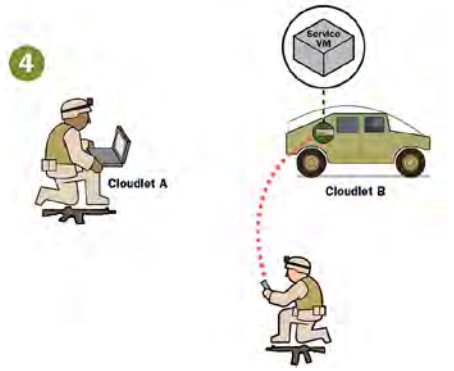
Device Credential Generation

- Cloudlet A discovers and connects to Cloudlet B using exchanged credentials
- Cloudlet B generates new credentials for Device
- Cloudlet B sends credentials to Device via Cloudlet A



Service VM Migration

- Cloudlet A migrates Service VM to Cloudlet B



Device connects to the migrated Service VM on Cloudlet B

Device Connection

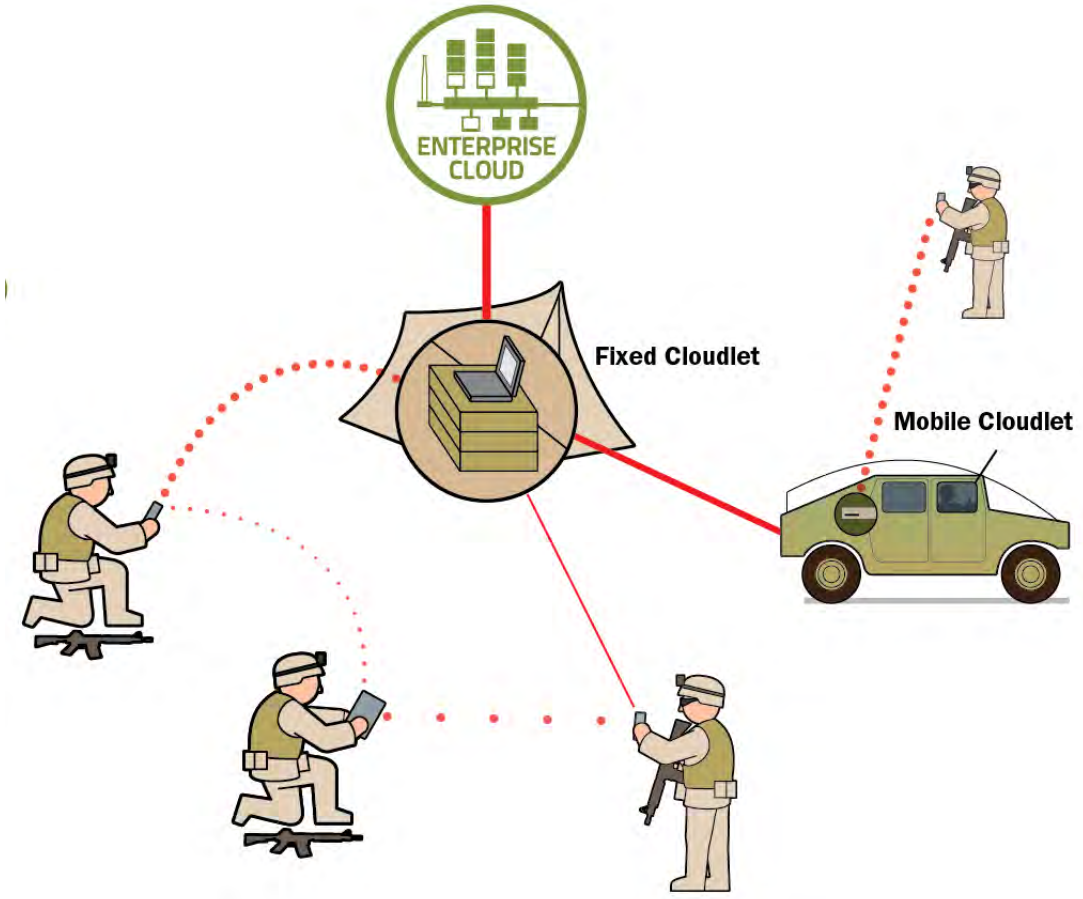
- Device connects to Cloudlet B using new credentials
- Client App on Device connects to Service VM running on Cloudlet B

Delay-Tolerant Data Sharing [1]

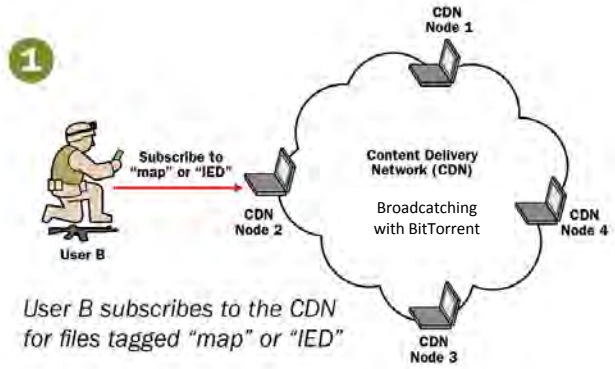
There is a large amount of information generated and needed in the field

However …

- DIL environments make it challenging to share information due to connectivity and bandwidth limitations
- Not all nodes need all information
- Not all connections between nodes have the same latency and bandwidth

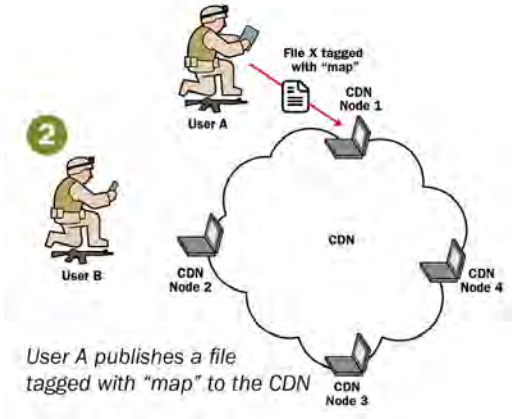


Delay-Tolerant Data Sharing 2



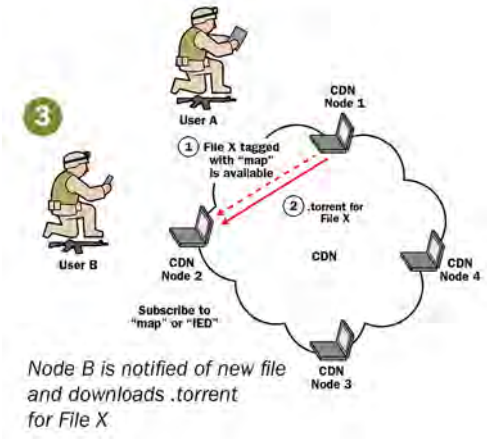
Subscription

- User B subscribes to the Content Delivery Network (CDN) for files tagged “map” or “IED”
- CDN uses RSS to discover files



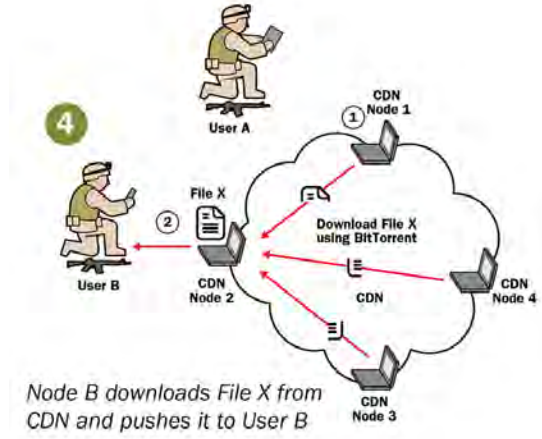
Publication

- User A sends File X tagged with “map” to the CDN
- CDN uses RSS to publish files



Notification and .torrent Download

- CDN Node 2 is notified via RSS that CDN Node 1 has published a file tagged with “map"
- CDN Node 2 downloads .torrent file for File X from Node 1



File Download using BitTorrent

- CDN Node 2 downloads File X using BitTorrent
- CDN Node 2 pushes File X to User B’s device

Summary

Tactical Computing and Communications (TCC) develops architectures and technologies that provide efficient and secure computing and communications for teams operating in tactical environments

- *Trusted Identities in Disconnected Environments* for establishing trust between nodes in tactical environments
- *Secure VM Migration* for enabling secure migration of capabilities between nodes in tactical environments
- *Delay-Tolerant Data Sharing* for efficient information sharing between nodes in tactical (DIL) environments

We advocate the effectiveness of combined threat modeling, vulnerability analysis and ceremony analysis to develop end-to-end secure software systems

Contact Information

Principal Investigator

Grace A. Lewis

Principal Researcher (SSD/AMS)

Telephone: +1 412.268.5851

Email: glewis@sei.cmu.edu

Team

Jeff Boleng (SSD/AMS)

Sebastían Echeverría (SSD/AMS)

Dan Klinedinst (CERT/VUL)

Marc Novakouski (SSD/AMS)

Keegan Williams (SSD/AMS)