

Tactical Computing and Communications (TCC)

Grace Lewis



Copyright 2016 Carnegie Mellon University

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.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

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

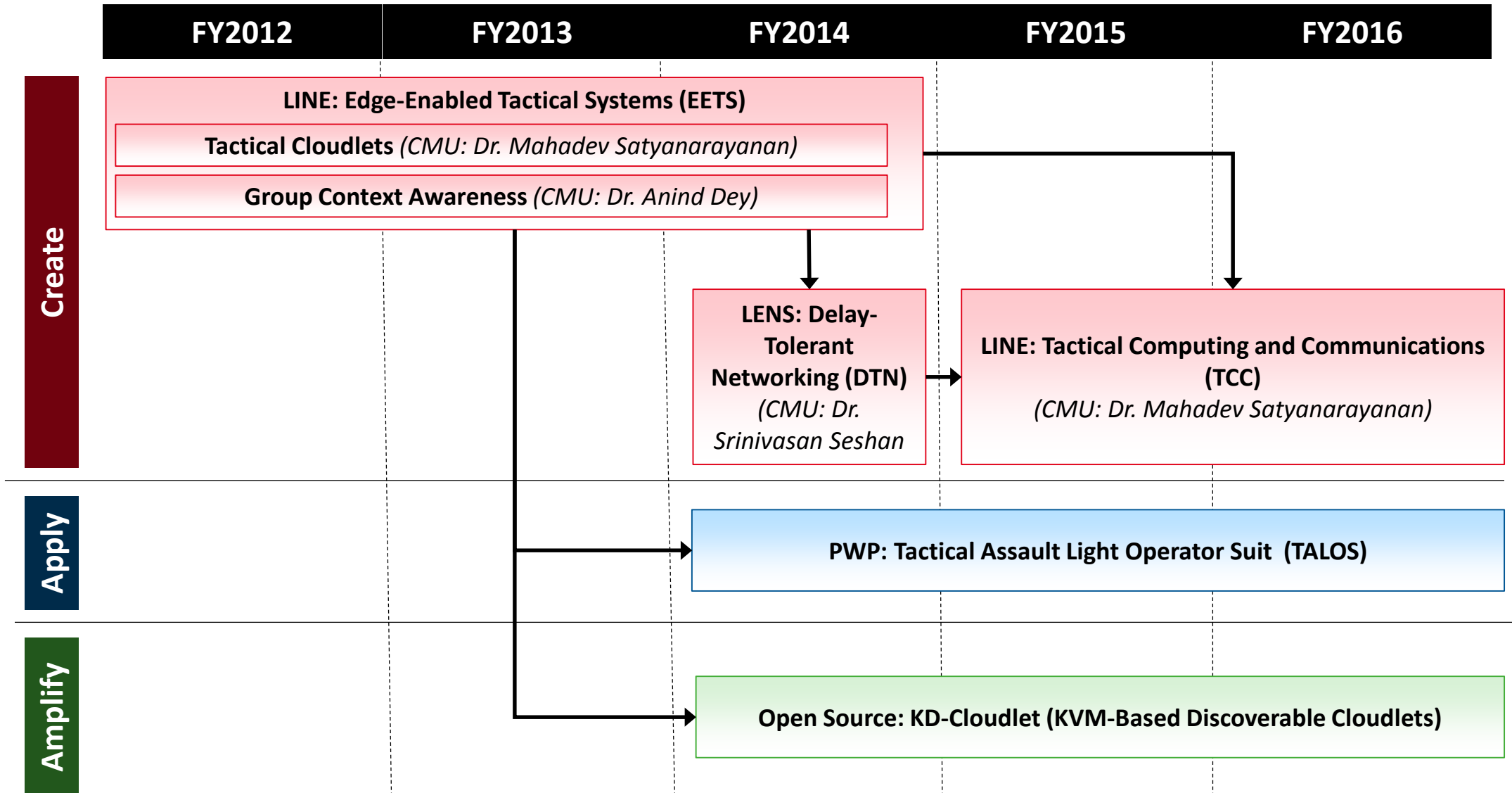
Soldiers and first responders operating in tactical environments increasingly make use of mobile systems for mission support

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



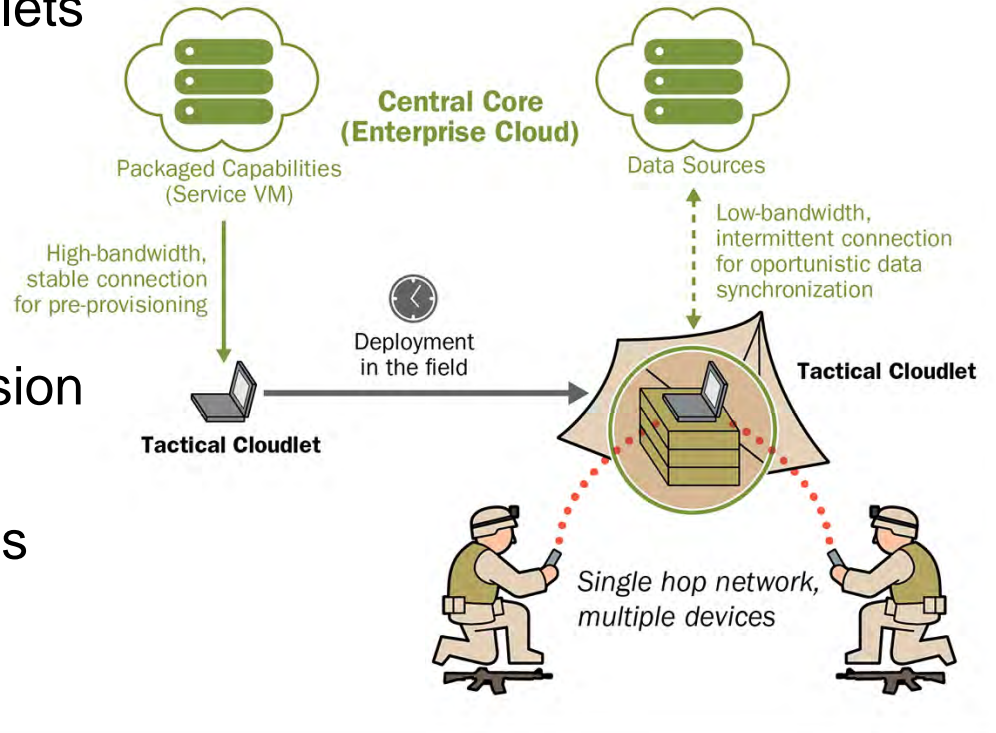
Overview of Results



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



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

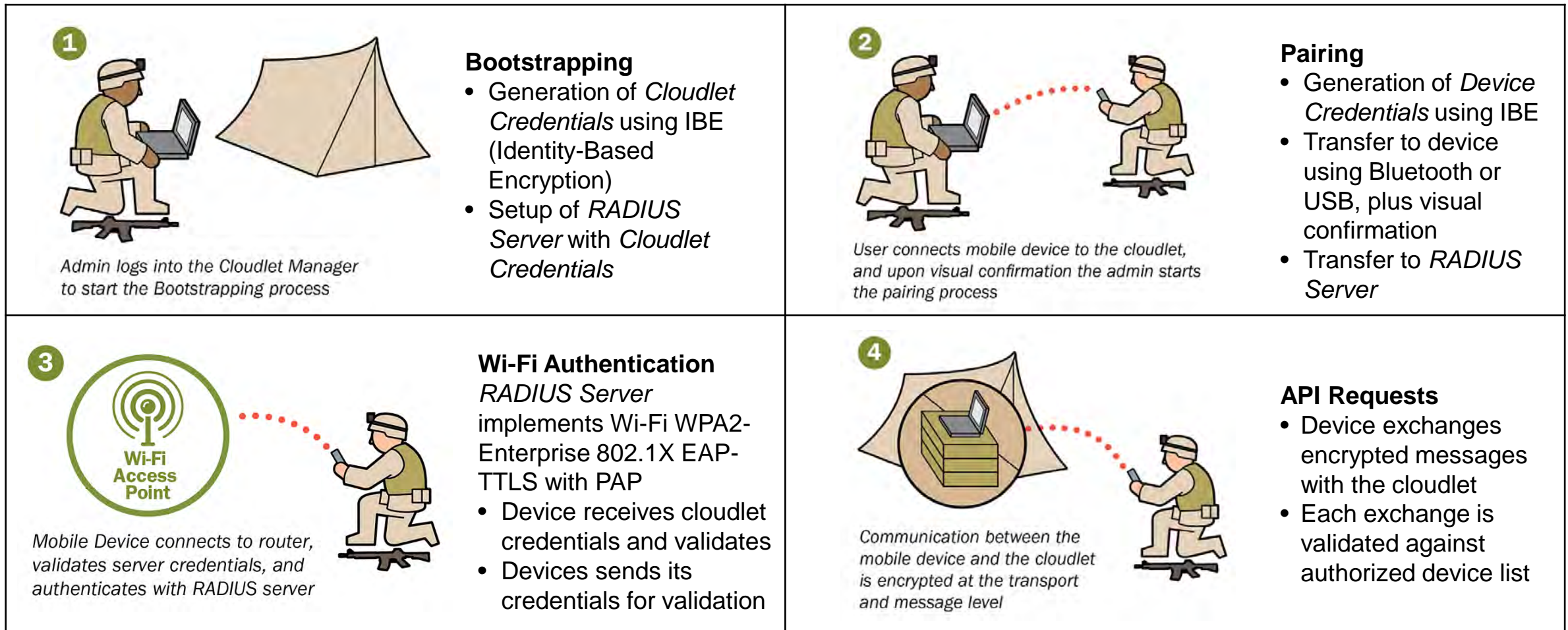
Motivation

- 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



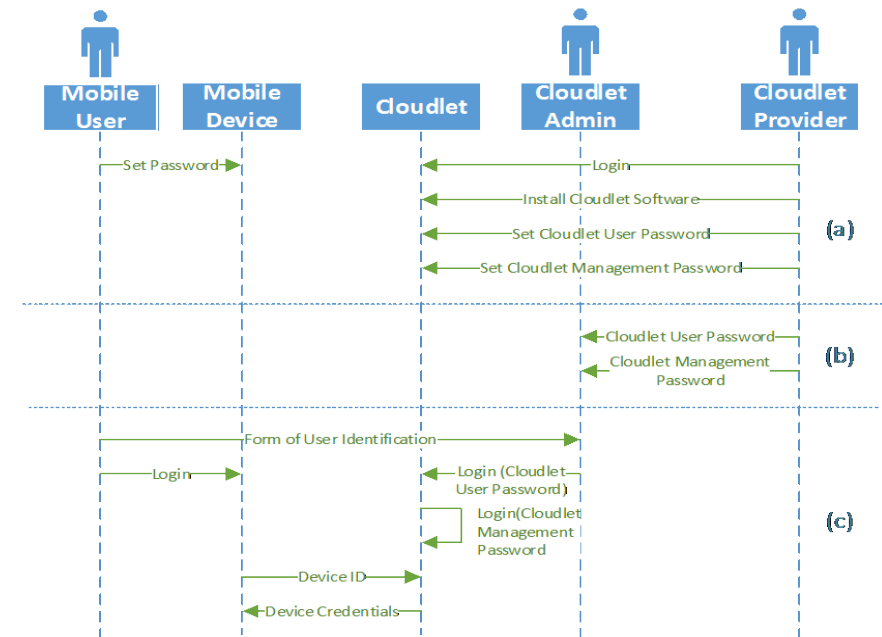
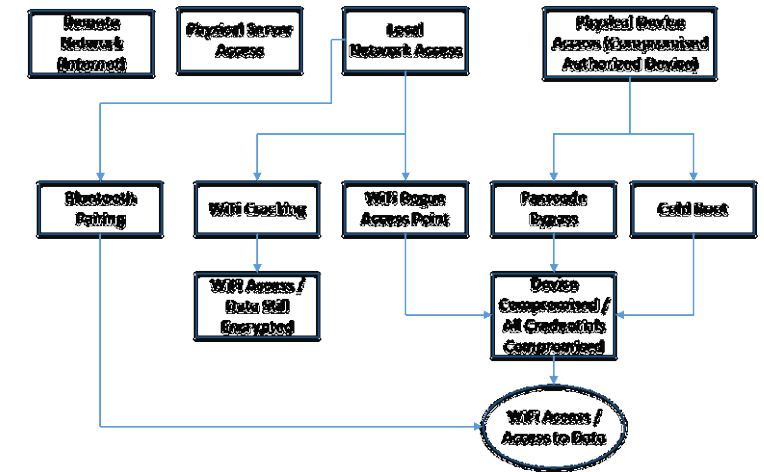
Device Credential Revocation

- 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



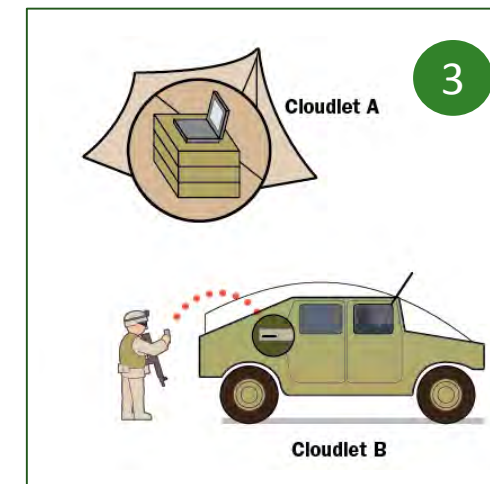
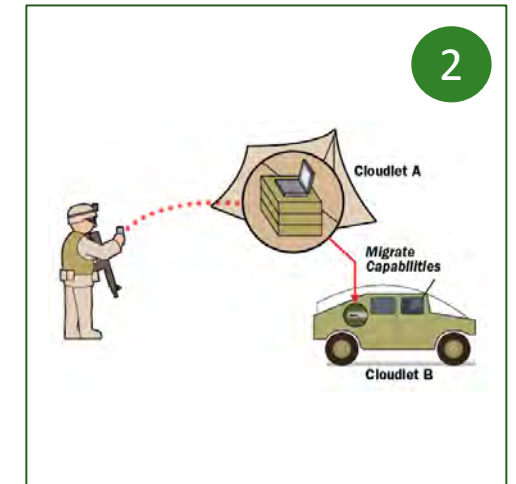
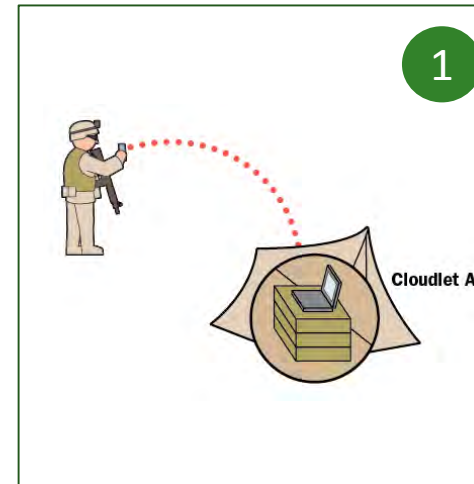
Secure Service VM Migration ₁

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

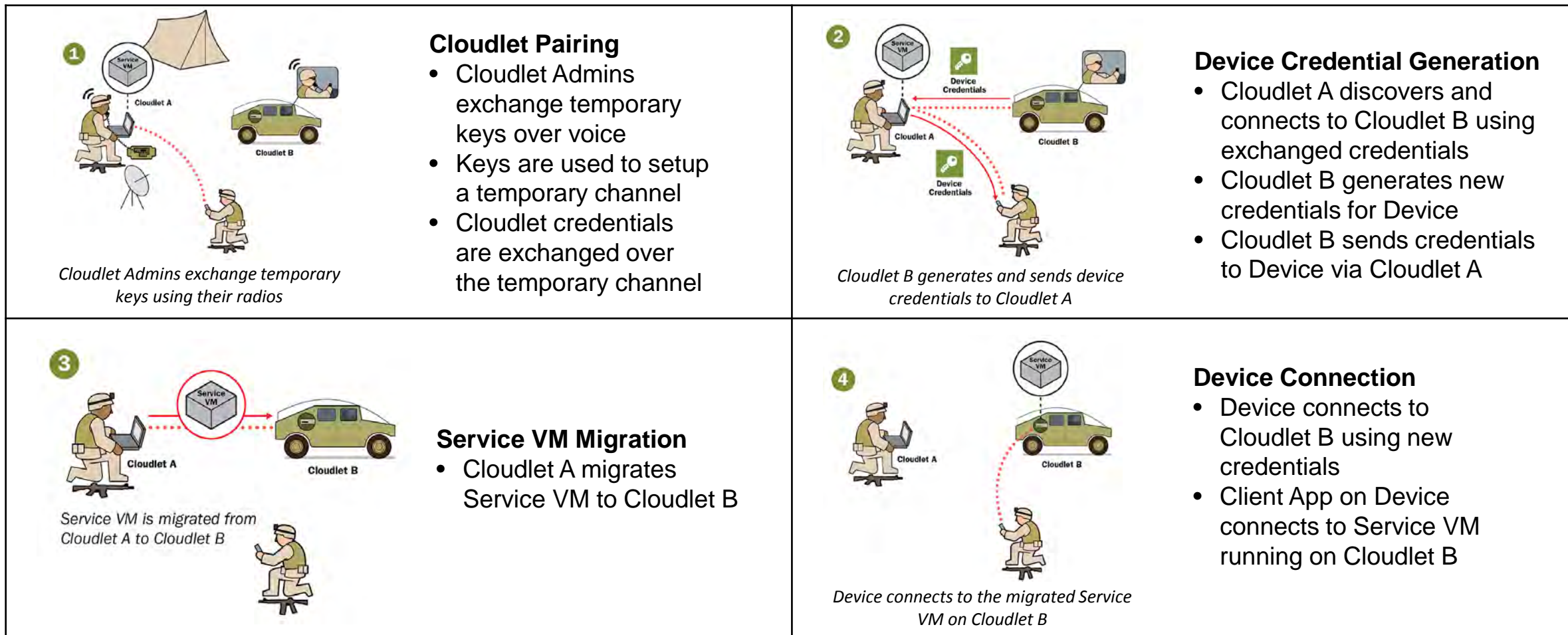
- VM migration
- Device “migration”

Challenges

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



Secure Service VM Migration ₂

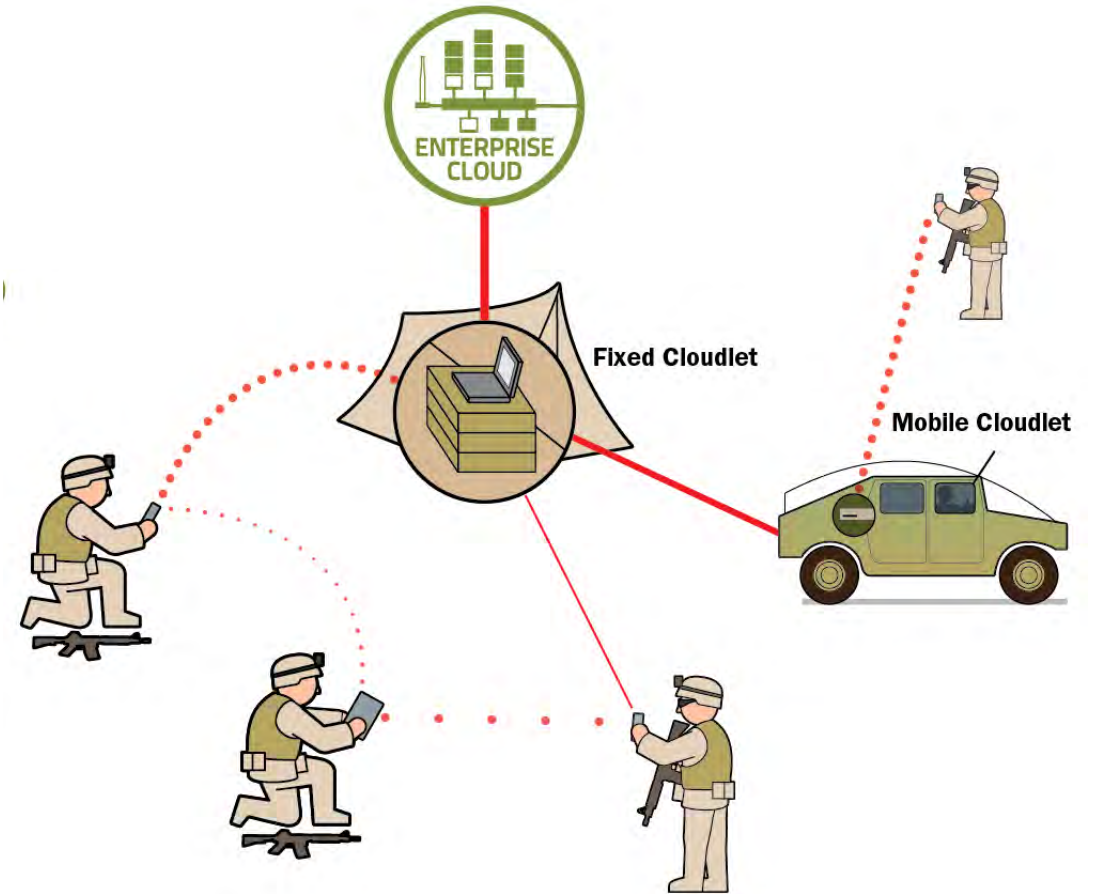


Delay-Tolerant Data Sharing ₁

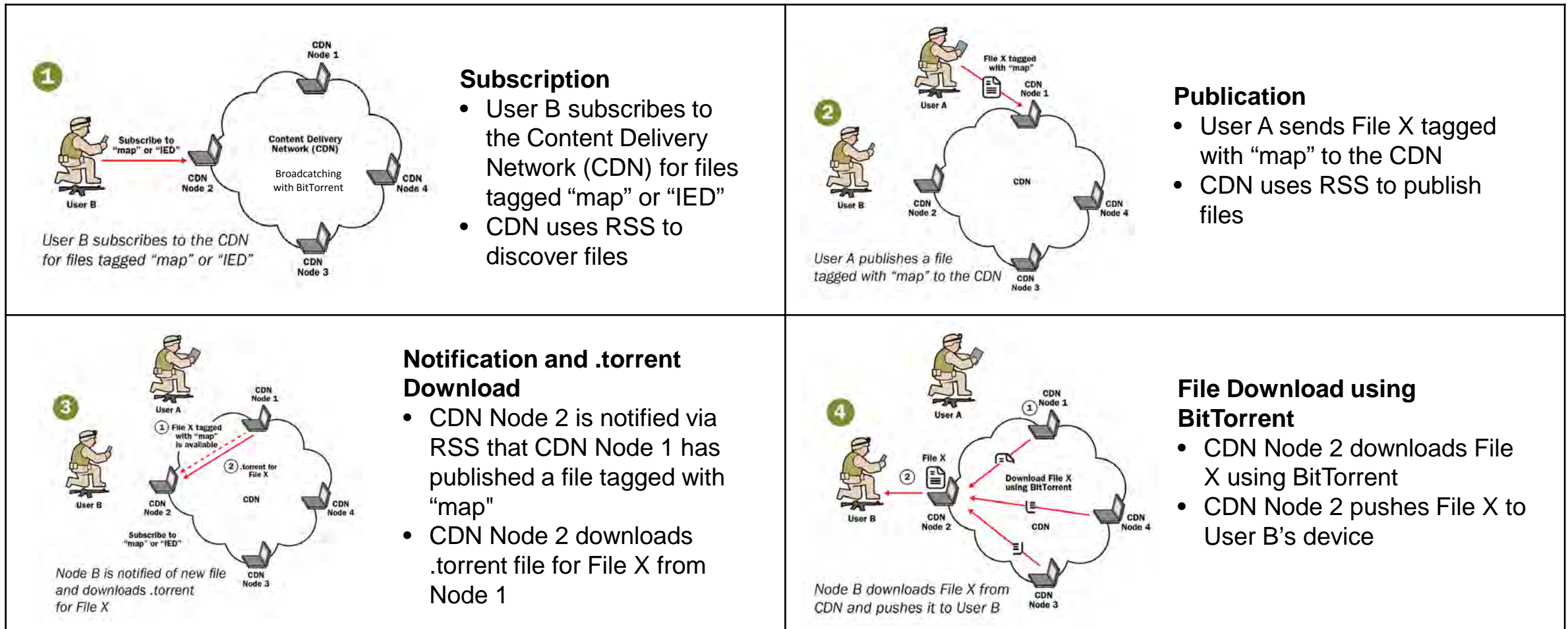
There is a large amount of information generated and needed in the field

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



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)

Sebastián Echeverría (SSD/AMS)

Dan Klinedinst (CERT/VUL)

Marc Novakouski (SSD/AMS)

Keegan Williams (SSD/AMS)

