Experimentation in the Use of Service Orientation in Resource-Constrained Environments

May 18, 2011

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Joe Seibel
Dan Plakosh
Soumya Simanta
Ed Morris
William Anderson

Scope

Current & Future Reality

- "Last Mile" users in tactical military situations & early responders in crisis situations desire
  - — mobile, dismounted, interoperating coalitions, using ad hoc and wireless networks, to improve situational capabilities

Purpose & Goals of the IRAD

- Determine if SOA is applicable and implementable in tactical environments

Success Criteria

- Sound understanding, environment characterization, functioning prototypes, and documented lessons

Related Work

Apps for the Army

- Competition to encourage app development (non-tactical)

MITRE

- Counter-Insurgency Intelligence Collection

U.S. Department of Homeland Security and NASA

- Chemical detection using sensors on smartphone

General Dynamics

- Militarized wearable computer (GD300) based on Android

Raytheon

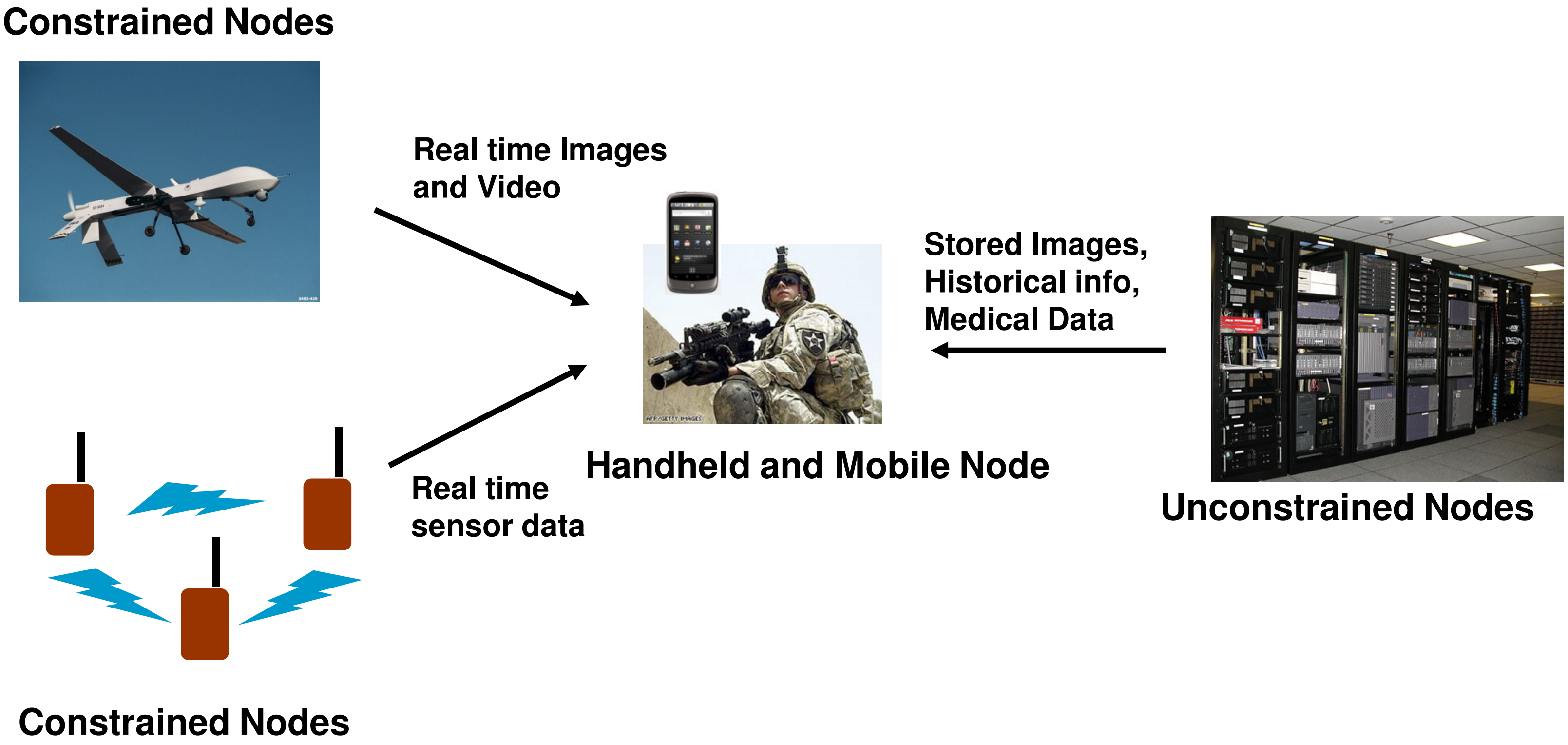
- Modification of Android for military use

Related Work

DARPA

- Transformative Apps program (DARPA-BAA-10-41)
  - Marketplace, infrastructure and apps
  - App Issues:
    - frequent disconnection, limited bandwidth
    - distributed compute/storage nodes in vehicles or outposts.
    - security tradeoffs with usability, performance, and complexity.

Feasibility Study: Communication Architecture Using Web Services



Constrained Nodes

Real time Images and Video

Handheld and Mobile Node

Stored Images, Historical info, Medical Data

Unconstrained Nodes

Real time sensor data

Constrained Nodes

Arrows represent communication via web services

Engineering Decision: Transport Layer Protocol

Transport layer protocol defines interfaces available to applications that allow end-to-end communications; TCP is the most familiar

- TCP provides reliable transmission – data guaranteed to reach destination in correct order and without duplication.
- TCP is suited for situations with reliable transmission (solid network infrastructure)
- Not suited to situations where packet loss, mis-ordering, or garbling are more common

We selected UDP as the preferred protocol for:

- better for time-sensitive applications
- *but* UDP does not provide error correction

Engineering Decision: Message Protocol

SOA uses two common messaging protocols

- Traditional WS-* based web services employing SOAP messages
- Representational State Transfer (REST) web services using URI's, and HTTP operations

REST is simpler and increasingly more common

- Better support on the Android platform
- Close tie to HTTP and therefore TCP meant we could not use it

We selected SOAP also hoping to take advantage of well-defined specifications, open source implementations, and support for security.

Engineering Decision: SOAP Engine

SOAP is a platform/language independent XML-based protocol for encoding messages

- Variety of open source SOAP engines that serialize in-memory data structures to XML messages and vice versa
- Machines at the other end of the wire perform inverse operation

SOAP engines selected

- gSOAP on the CoT router-side supports SOAP over UDP and C++ development
- We modified kSOAP on the Android side to support UDP, but problems remain
  - We had to manually develop code to marshal/unmarshal Java objects to SOAP messages
  - kSOAP for Android omits important features (XML attributes, limited parsing, WS-Addressing)

Reduced bandwidth on GPRS networks later necessitated a change to a binary format

Engineering Decision: Security

Typical strategy for web services over the internet is

- Network level security (encryption) based on IPsec
- Transport level security built on transport mechanisms such as HTTP
- Application level security strategies such as WS-Security

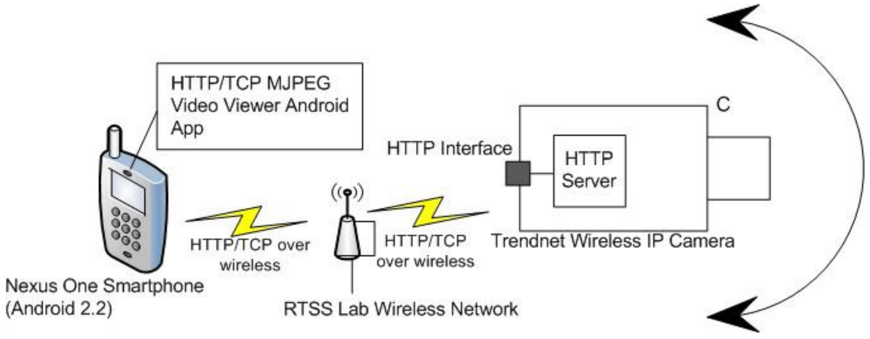
We considered WS-Security, but rejected it due to lack of kSOAP support

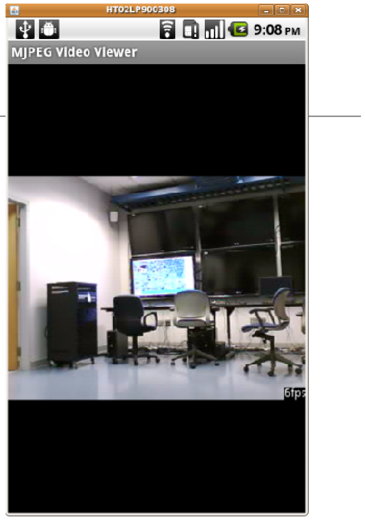
Our approach

- Network level security: existing internet and wireless protocol WPA/WPA2 with pre-shared key (PSK)
- Transport level security: Datagram Transport Layer Security (DTLS) was immature when we evaluated it
- Application level security: AES-256 bit encryption with WPA2 passphrase generation

Not perfect, but this solution provides a reasonable level of security

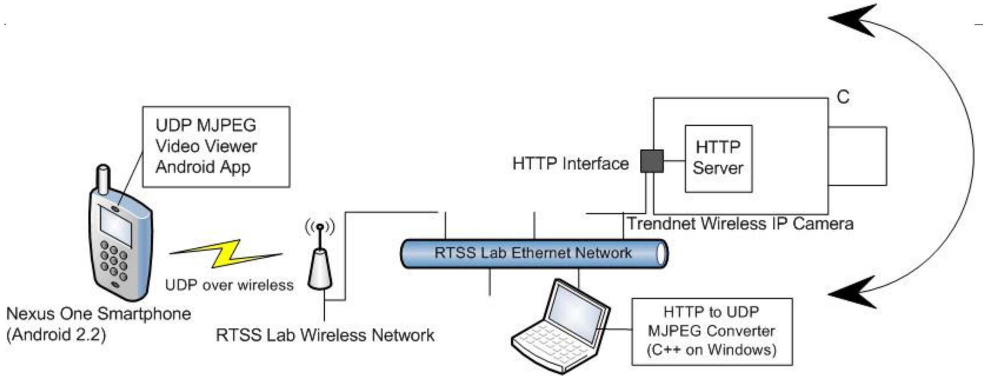
Test 1 – HTTP/TCP MJPEG Video Viewer App

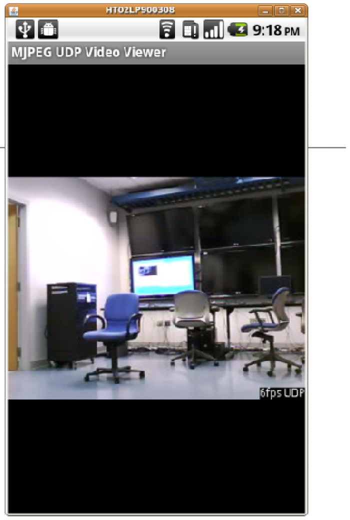

HTTP/TCP MJPEG Video Viewer Android App
HTTP Interface
HTTP Server
C
HTTP/TCP over wireless
HTTP/TCP over wireless
Trendnet Wireless IP Camera
Nexus One Smartphone (Android 2.2)
RTSS Lab Wireless Network



- Trendnet wireless IP Camera and Nexus One smartphone are connected to RTSS wireless network
- The smartphone receives video in Motion JPEG (MJPEG) format over a wireless HTTP/TCP connection

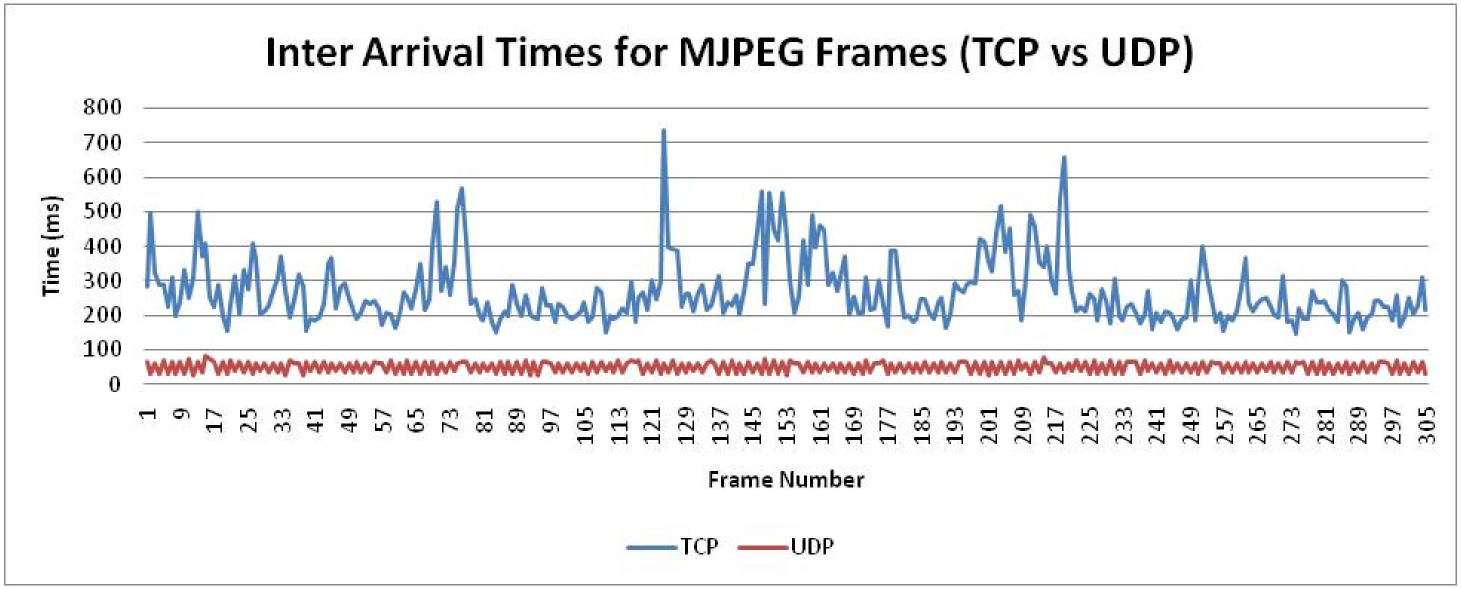
Test 2 – UDP MJPEG Video Viewer App



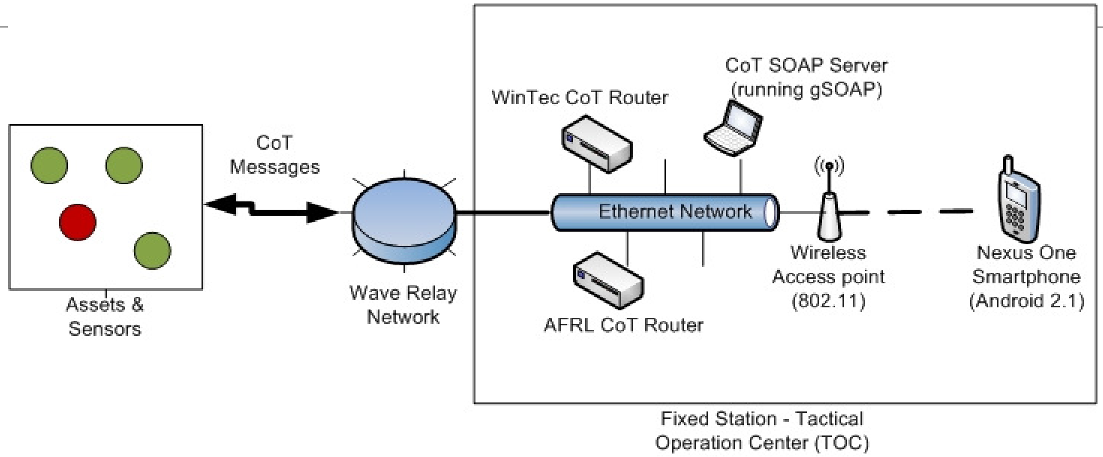


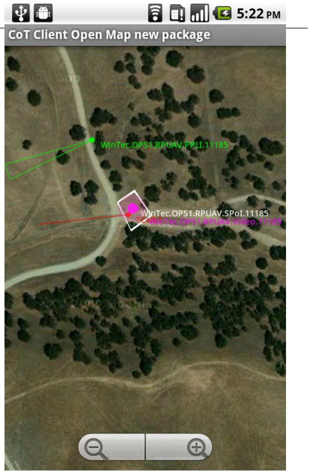
- Trendnet wireless IP Camera is connected to a Windows machine running a TCP to UDP MJPEG converter (C++) through a wired Ethernet network
- The TCP to UDP converter gets MJPEG image data over TCP and retransmits that same data using UDP to the RTSS Lab wireless network.
- The Android smartphone is connected to the RTSS lab wireless network and can receive these MJPEG frames over UDP and display it using an Android application

Performance of TCP vs UDP for Video Data on the Phone

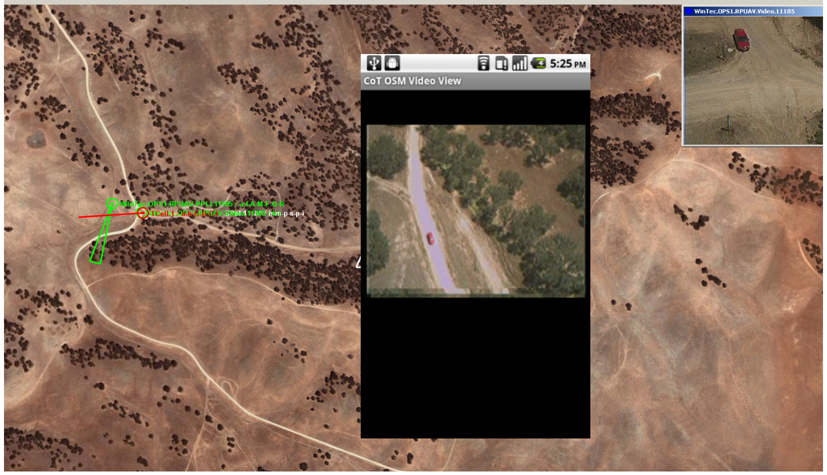


Prototype 1 – CoT SOAP UDP App V1 (Camp Roberts – May 2010 TNT) – Fixed Station

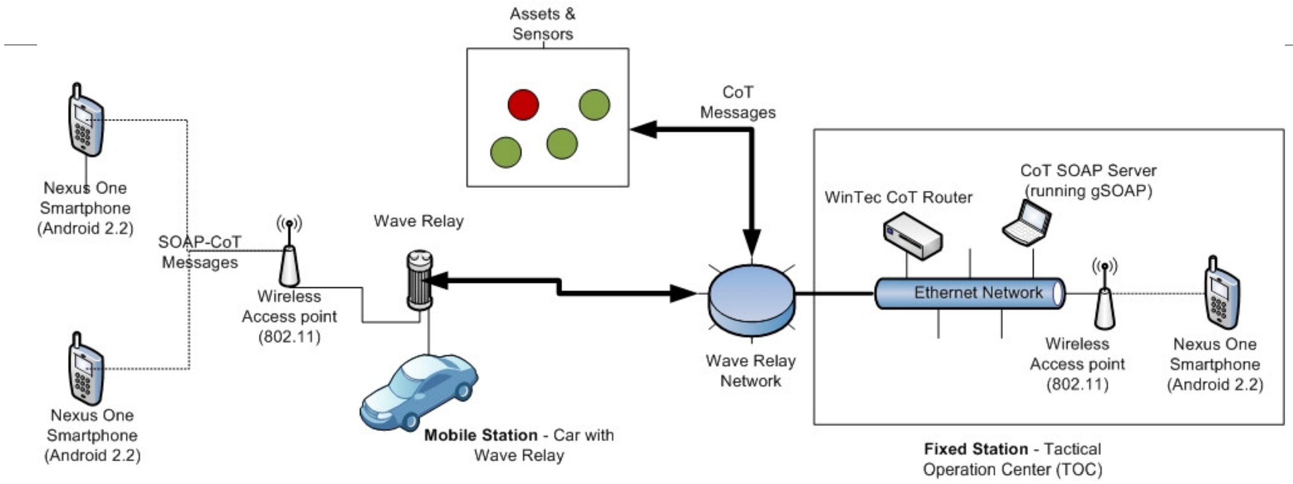

CoT Messages
Assets & Sensors
Wave Relay Network
WinTec CoT Router
CoT SOAP Server (running gSOAP)
Ethernet Network
AFRL CoT Router
Wireless Access point (802.11)
Nexus One Smartphone (Android 2.1)
Fixed Station - Tactical Operation Center (TOC)


5:22 PM
CoT Client Open Map new package
WinTec.OPS1.RPUAV.PPLI.11185
WinTec.OPS1.RPUAV.SPoI.11185
TCell.1
WinTec.OPS1.RPUAV.Video.11185

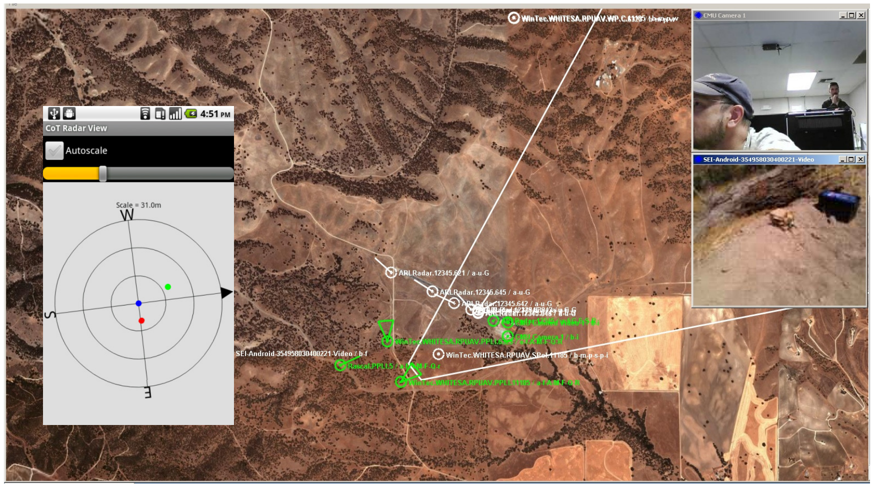
- Assets (UAVs, cars) track a hostile vehicle and post CoT messages (video, location etc) to the CoT SOAP Server
- CoT SOAP Server consume raw CoT messages and provides CoT data as SOAP-over-UDP web service
- Android phone consume SOAP messages, processes and displays them



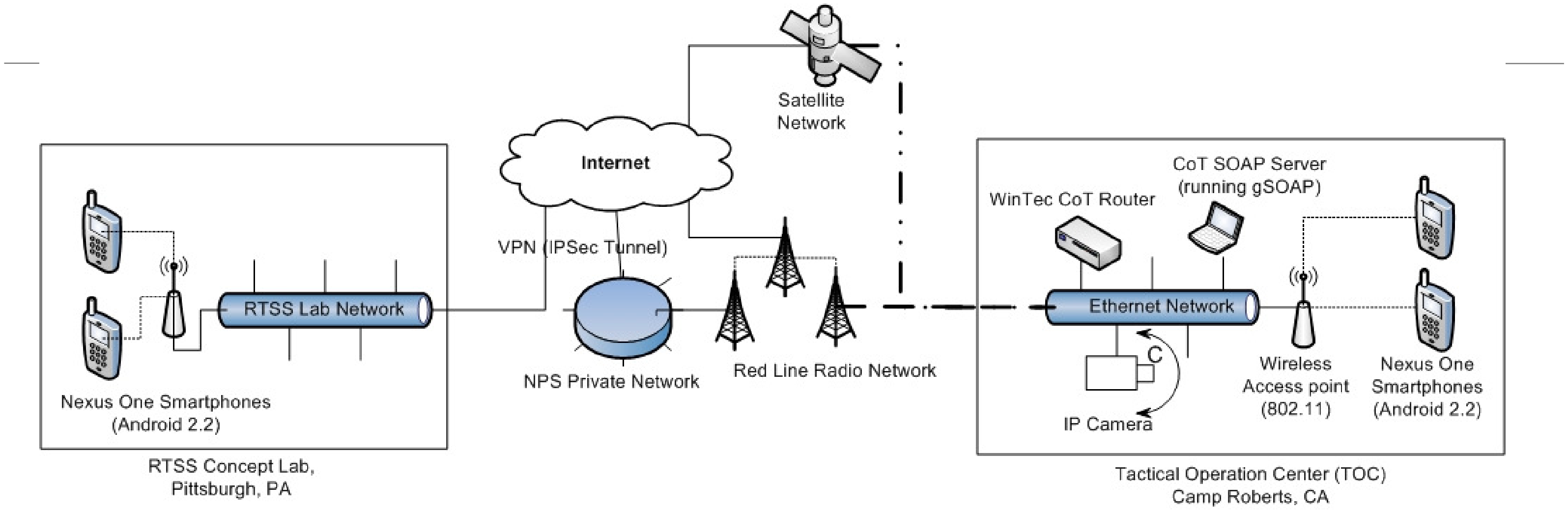
Prototype 2 – CoT SOAP UDP App V2 (Camp Roberts August 2010 TNT) – Mobile Station


Assets & Sensors
CoT Messages
Nexus One Smartphone (Android 2.2)
SOAP-CoT Messages
Wireless Access point (802.11)
Wave Relay
Nexus One Smartphone (Android 2.2)
Mobile Station - Car with Wave Relay
Wave Relay Network
WinTec CoT Router
CoT SOAP Server (running gSOAP)
Ethernet Network
Wireless Access point (802.11)
Nexus One Smartphone (Android 2.2)
Fixed Station - Tactical Operation Center (TOC)

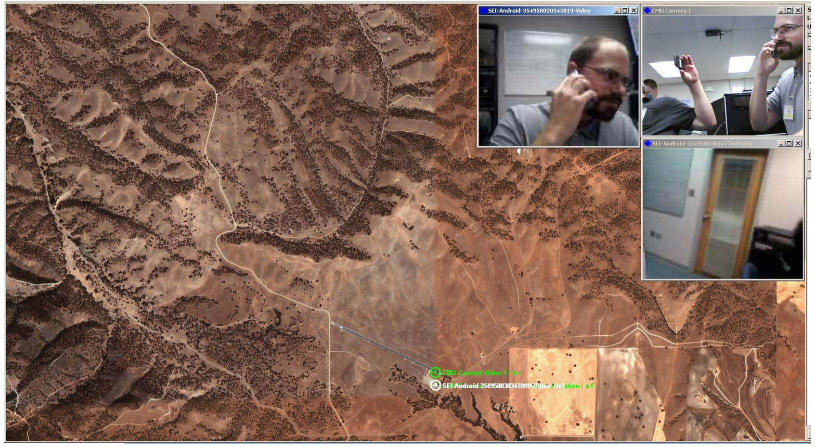
- “Warfighers” disguised as civilian tourists have Android phones that are connected to a Wi-Fi access point (connected to a wave relay via ethernet) on a mobile station (car)
- Phones consume CoT Messages from other assets (UAV)
- Phones also broadcast live video feeds to other phones and the TOC


4:51 PM
CoT Radar View
Autoscale
Scale = 31.0m
W
S
E
CMU Camera 1
SEI-Android-354958030400221-Video
ARLRadar.12345.621 / a-u-G
ARLRadar.12345.645 / a-u-G
ARLRadar.12345.642 / a-u-G
SEI-Android-354958030400221-Video / b-f
Rascal.PPLI.5
CMU Camera 1 / b-i
WinTec.WHITESA.RPUAV.SPoI.11185 / b-m-p-s-p-i
WinTec.WHITESA.RPUAV.PPLI.11185 / a-f-A-M-F-Q-R

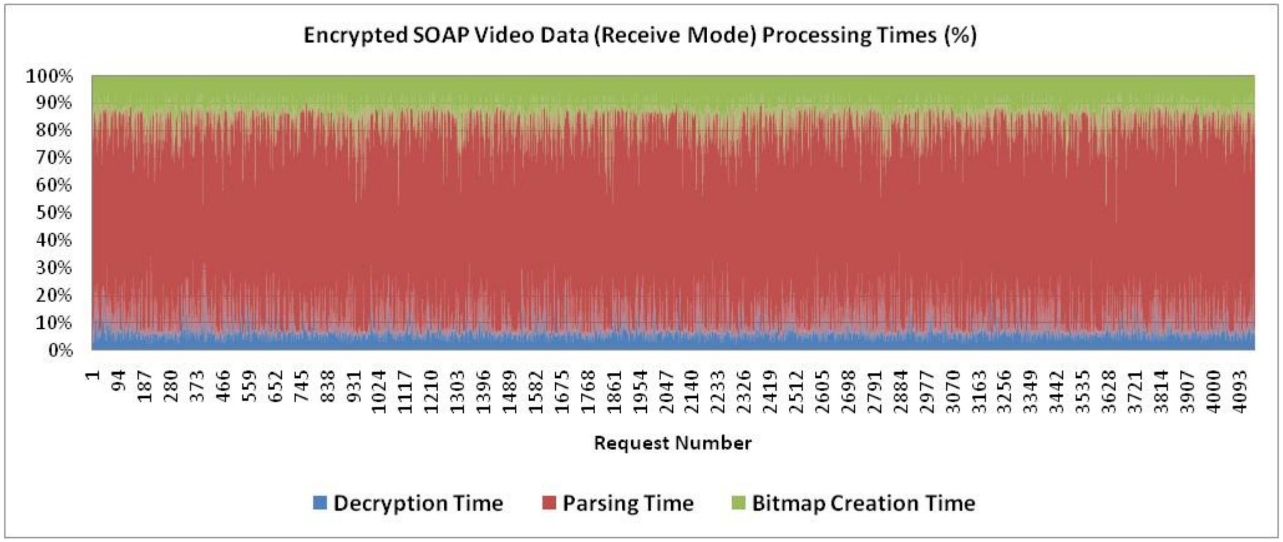
Prototype 3 – CoT SOAP UDP App V2 (Camp Roberts August 2010 TNT) – Two-way Video over VPN


Satellite Network
Internet
VPN (IPSec Tunnel)
NPS Private Network
Red Line Radio Network
RTSS Lab Network
Nexus One Smartphones (Android 2.2)
RTSS Concept Lab, Pittsburgh, PA
WinTec CoT Router
CoT SOAP Server (running gSOAP)
Ethernet Network
C
IP Camera
Wireless Access point (802.11)
Nexus One Smartphones (Android 2.2)
Tactical Operation Center (TOC) Camp Roberts, CA

- IP camera and Android phones (inside the TOC, Camp Roberts) capture video frames and convert them into SOAP-over-UDP CoT messages.
- These SOAP messages are sent to both local service consumers (other phones and CoT display) as well as remote service consumers (phones inside the RTSS lab network, Pittsburgh)
- Remote Phones (inside the RTSS lab) can also broadcast live video feeds as SOAP-over-UDP CoT messages to the TOC in Camp Roberts via the RTSS Lab VPN connection

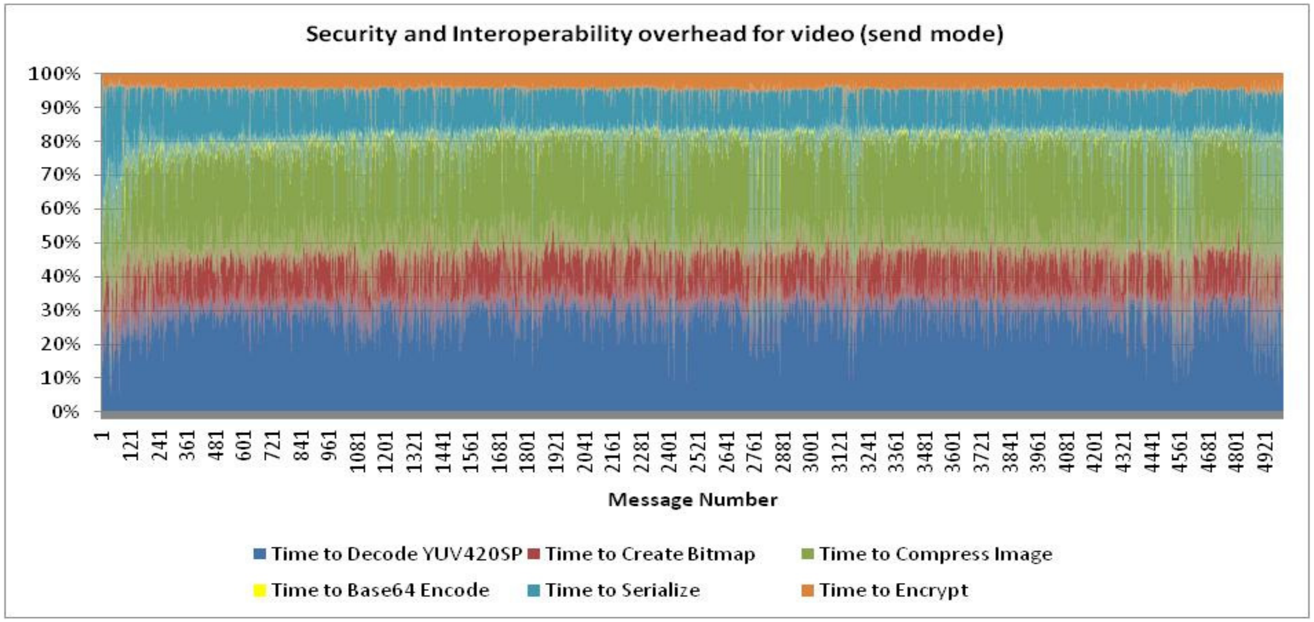

SEI-Android-354958030343819-Video
CMU Camera 1
SEI-Android-354958030347760Video

Security and Interoperability overhead for SOAP Video Messages (Receive Mode)



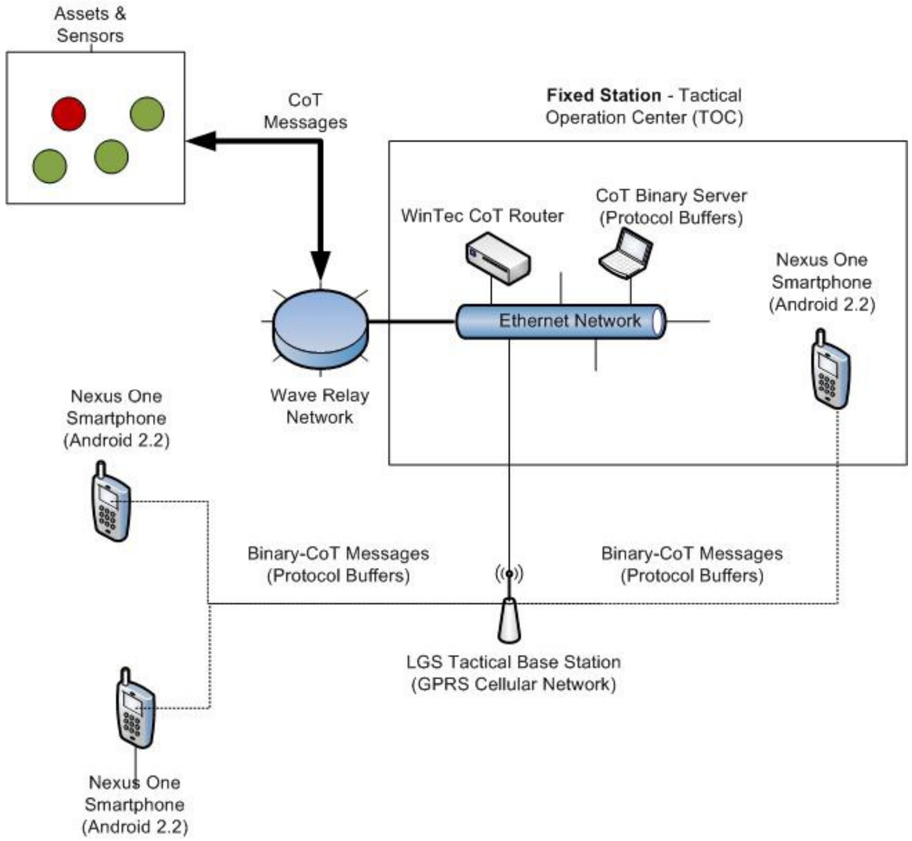
	Average	Std Dev	Median
Decryption Time (ms)	6.074469	4.149628	3.997803
Parsing Time (ms)	52.68427	21.83106	44.12842
Bitmap Creation Time (ms)	10.33385	6.397927	7.141113

Security and Interoperability overhead for SOAP Video Messages (Send Mode)



	Average	Std Dev	Median
Time to Decode UV420SP (ms)	5.485956	1.301711	5.310059
Time to Create Bitmap (ms)	2.659412	0.935272	2.288818
Time to Compress Image (ms)	4.55023	1.458631	5.401611
Time to Base64 Encode (ms)	0.177075	0.785067	0.122071
Time to Serialize (ms)	2.954358	4.221974	2.075196
Time to Encrypt (ms)	0.815698	0.499913	0.701904

Prototype 4 – CoT UDP, Binary Protocol, GPRS (Camp Roberts October 2010 TNT)


Assets & Sensors
CoT Messages
Fixed Station - Tactical Operation Center (TOC)
WinTec CoT Router
CoT Binary Server (Protocol Buffers)
Nexus One Smartphone (Android 2.2)
Ethernet Network
Wave Relay Network
Nexus One Smartphone (Android 2.2)
Binary-CoT Messages (Protocol Buffers)
Binary-CoT Messages (Protocol Buffers)
LGS Tactical Base Station (GPRS Cellular Network)
Nexus One Smartphone (Android 2.2)

- CoT data including imagery sent to and from Android phones are transmitted via an LBS Tactical Base Station using GPRS
- Due to reduced bandwidth, real-time video was not attempted, only still imagery (snapshots) were sent.
- Performance with still images was quite good (approximately 30-40 kbits/sec)

Summary of Observations

Security overhead

- 256 bit AES encryption and decryption at line speed
- Accelerated by use of “native” code
- Significantly less as compared to interoperability overhead (SOAP/XML serialization de-serialization overhead)

Variation in processing time (especially for Java only function such as parsing) is due to

- JVM automatic garbage collection
- Variation in message size for video frames
- Potential problem with kSOAP implementation

IRAD Results – Technical $_1$

A subset of SOA is practical in tactical environments where bandwidth is high

- Performance of video feeds (using SOAP-based CoT format) is comparable (visually) with the video feed on a standard desktop machine for a threshold of video feeds

To make SOA practical in these situations, we had to make some non-typical SOA choices

- UDP rather than customary TCP to improve video performance
- SOAP vs. REST based web services
  - Currently, REST is built on HTTP/TCP, but there has been some work on REST-UDP
- Use of WS-Security is not easy since implementations are lacking

Moved to binary formats in situations with low bandwidth

IRAD Results – Technical $_2$

Smartphone (Nexus One) far exceeded our expectations

- Roughly as powerful as a circa 2000 desktop
- Sophisticated software development platform
- Phones with dual core processors are now being developed and released

Our current solution does not address

- Architectural changes to the way CoT data is distributed (that may be need to improve performance)
  - Video frame size (with UDP)
  - UDP is not reliable – not a problem of real-time video but is a problem for text
  - Current phone hardware can be overwhelmed by too many video feeds
  - Not clear if the parsing overhead can be fixed using a better implementation or modifying the existing parser on the phone
- Non-software issues in the field – screen visibility in bright light, radio interference

IRAD Results - Non-technical

May 2010 TNT (Camp Roberts)

- Good feedback from Special Forces personnel
- Requested for more features

August 2010 TNT (Camp Roberts)

- General feeling that we were ahead of others in our development of smartphone capabilities for situational awareness
- By November 2010, we were leapfrogged
- Other consumers of CoT data using our CoT web service

October/November 2010

- Worked with NPS, Naval Special Warfare (NSW) experts to make technology available on proprietary GPRS network
- GPRS sufficient for single images but not for video

Lessons Learned – Mobile Computing

Android is good and open development platform

However, the platform is still evolving

- Performance improvements with new OS versions
- User interface needs to be more responsive
- Lack for hardware-base support for security, but this changing all the time

Architecture must take into account constraints of mobile devices

- The CoT architecture mayneed to be adapted to support constrained devices
  - For example, “on demand” video feeds can reduce bandwidth usage as well as unwanted processing on the phone

Lessons Learned – SOA on Smartphones

Immaturity of SOAP implementations

- kSOAP
  - Lack of support of generated code from WSDL
  - Many key XML features missing or are not directly supported
  - No support for UDP transport, security and other WS standards
- gSOAP
  - Poor architecture for supporting applications that need low-level networking control
  - Problems with UDP support

Reduction in Development time

- Using SOAP can reduce development time by reusing services only if mature implementations are available for the target platform(s)
- Using SOAP can result in unacceptable performance for some class of applications

Current Capabilities of the Android App

Online and cached maps

Asset’s geo-location, field of view (FOV) and video feed displayed on a map

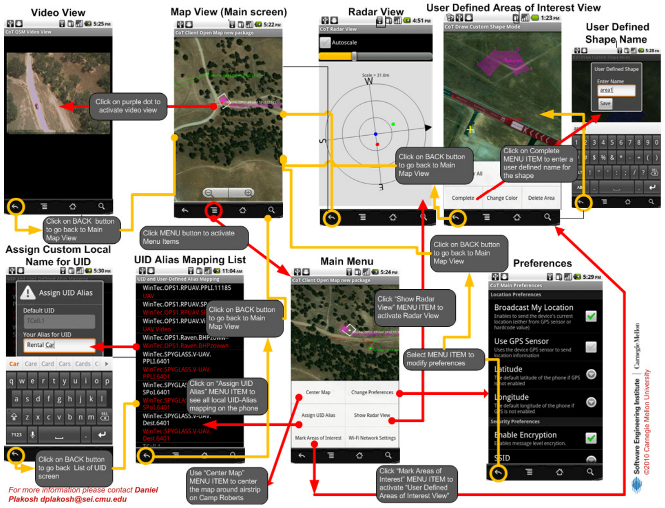
Radar and compass view

User-defined “area of interest” that can be shared in real-time

Real-time video feed from phones

Phone’s current geo-location in real-time

256-bit AES encryption



Video View

Map View (Main screen)

Radar View

User Defined Areas of Interest View

User Defined Shape Name

Assign Custom Local Name for UID

UID Alias Mapping List

Main Menu

Preferences

Click on purple dot to activate video view

Click on BACK button to go back to Main Map View

Click MENU button to activate Menu Items

Click on BACK button to go back to Main Map View

Click on Complete MENU ITEM to enter a user defined name for the shape

Click on BACK button to go back to Main Map View

Click “Show Radar View” MENU ITEM to activate Radar View

Select MENU ITEM to modify preferences

Click on BACK button to go back to Main Map View

Click on “Assign UID Alias” MENU ITEM to see all local UID-Alias mapping on the phone

Click on BACK button to go back List of UID screen

Use “Center Map” MENU ITEM to center the map around airstrip on Camp Roberts

Click “Mark Areas of Interest” MENU ITEM to activate “User Defined Areas of Interest View”

UID and User-Defined Alias Mapping

WinTec.OPS1.RPUAV.PPLI.11185
UAV
WinTec.OPS1.RPUAV.SP
WinTec.OPS1.RPUAV.SP
WinTec.OPS1.RPUAV.Vi
UAV Video
WinTec.OPS1.Raven.BHPzoww=
WinTec.OPS1.Raven.BHPzoww=
WinTec.SPYGLASS.V-UAV.
PPLI.6401
WinTec.SPYGLASS.V-UAV.
PPLI.6401
WinTec.SPYGLAS
SPoI.6401
WinTec.SPYGLA
SPoI.6401
WinTec.SPYGLASS.V-UAV.
Dest.6401
WinTec.SPYGLASS.V-UAV.
Dest.6401

Assign UID Alias

Default UID: TCell.1

Your Alias for UID: Rental Car

User Defined Shape

Enter Name: area1

CoT Main Preferences

Location Preferences

Broadcast My Location ☑
Enables to send the device's current location (either from GPS sensor or hardcode value)

Use GPS Sensor □
Uses the device GPS sensor to send location information

Latitude
The default latitude of the phone if GPS is not enabled

Longitude
The default longitude of the phone if GPS is not enabled

Security Preferences

Enable Encryption ☑
Enables message level encryption.

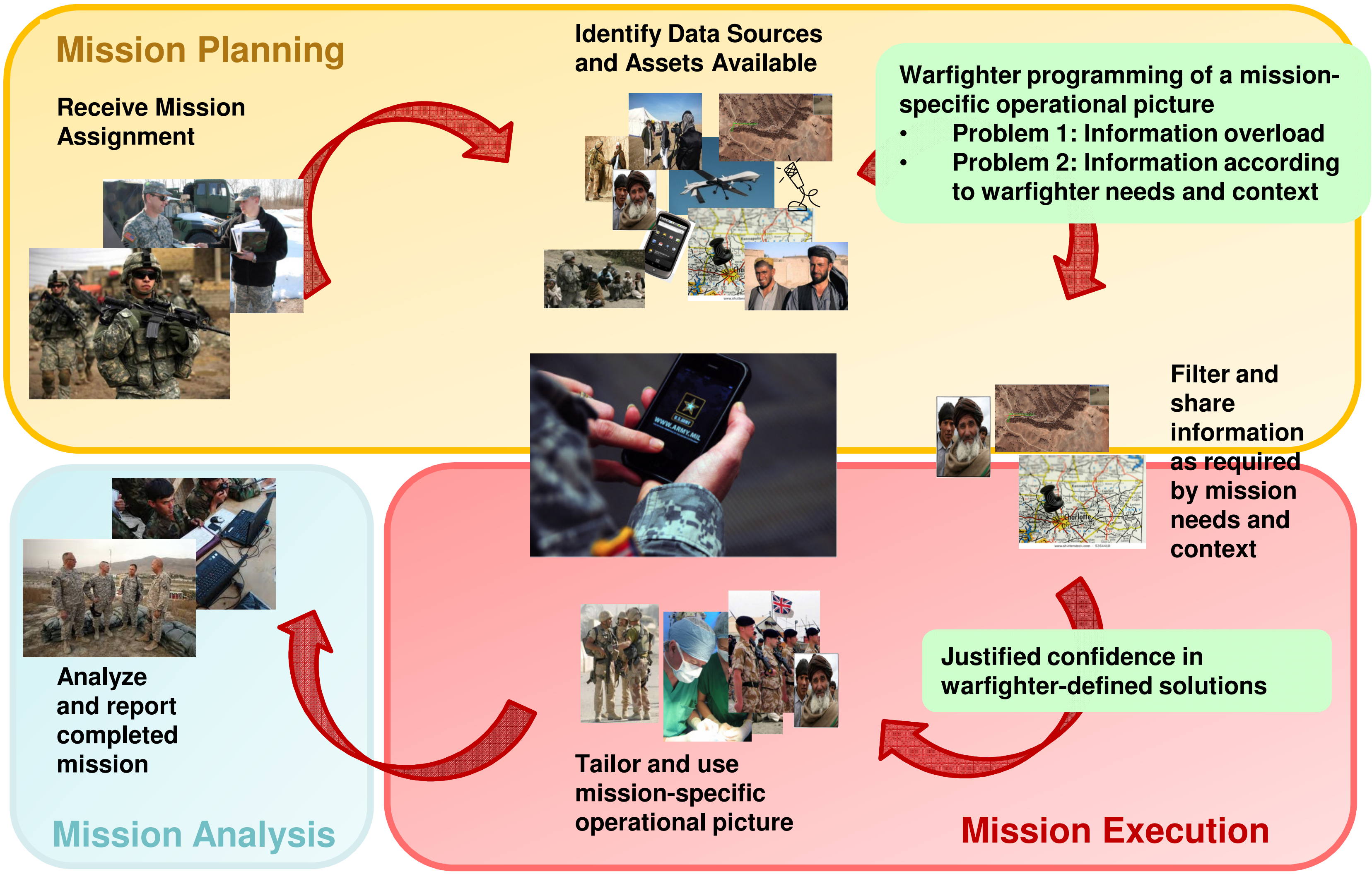
SSID

*For more information please contact **Daniel Plakosh dplakosh@sei.cmu.edu***

Software Engineering Institute | Carnegie Mellon

©2010 Carnegie Mellon University

FY11: Warfighter (Edge) Programming of Handheld Devices



Mission Planning

Receive Mission Assignment

Identify Data Sources and Assets Available

Warfighter programming of a mission-specific operational picture

- Problem 1: Information overload
- Problem 2: Information according to warfighter needs and context

Filter and share information as required by mission needs and context

Justified confidence in warfighter-defined solutions

Tailor and use mission-specific operational picture

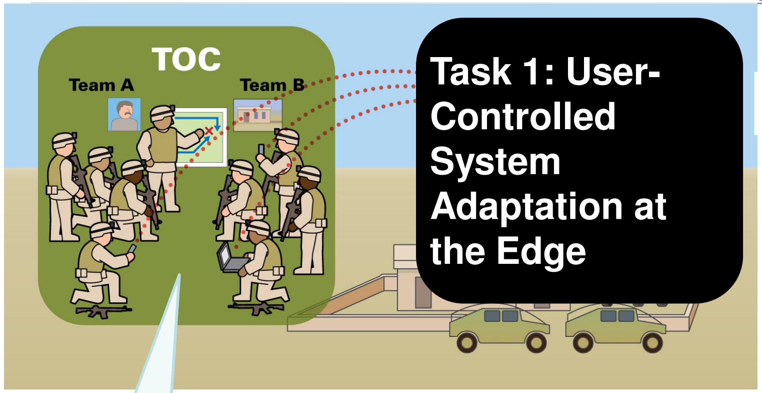
Mission Execution

Analyze and report completed mission

Mission Analysis

FY12 Planned Work

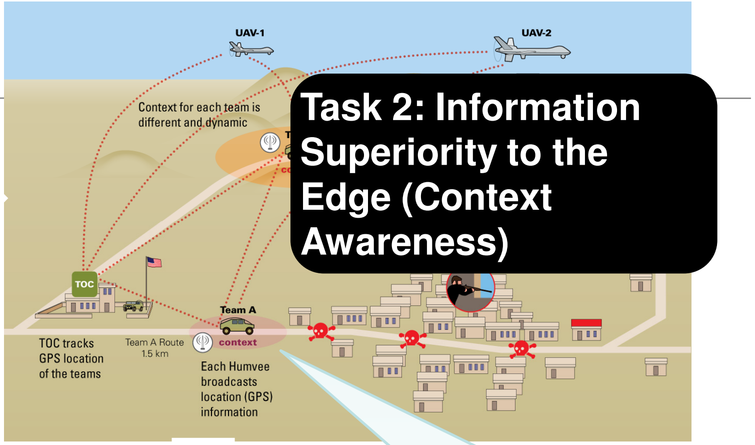
Mission Planning



Task 1: User-Controlled System Adaptation at the Edge

A group of warfighters receives a new mission. Inevitably, the systems they have are not ideally suited to support that mission.

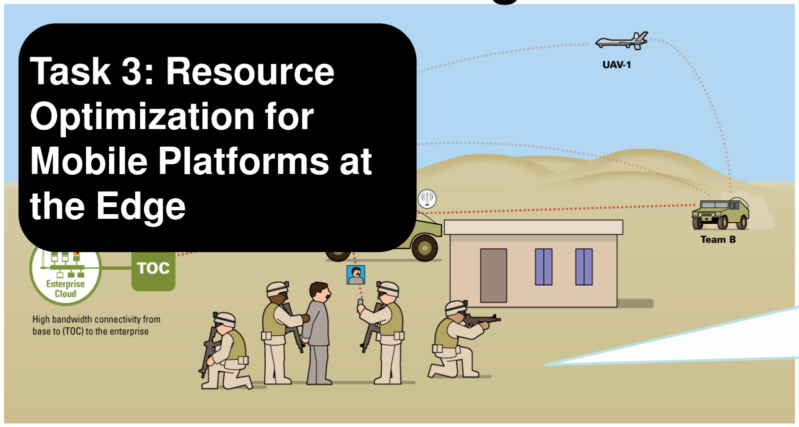
Emerging Situation


UAV-1
UAV-2
Context for each team is different and dynamic
TOC
Team A
context
TOC tracks GPS location of the teams
Team A Route 1.5 km
Each Humvee broadcasts location (GPS) information

Task 2: Information Superiority to the Edge (Context Awareness)

Once the warfighters embark on the mission, the circumstances and crucial data for each team changes rapidly.

Dismounted Warfighters


UAV-1
Team B
Enterprise Cloud
TOC
High bandwidth connectivity from base to (TOC) to the enterprise

Task 3: Resource Optimization for Mobile Platforms at the Edge

In the field, as warfighters move further away from the enterprise and TOC, computational resources decrease.