# SECURELY CONNECTING INSTANT MESSAGING SYSTEMS FOR AD HOC NETWORKS TO SERVER BASED SYSTEMS

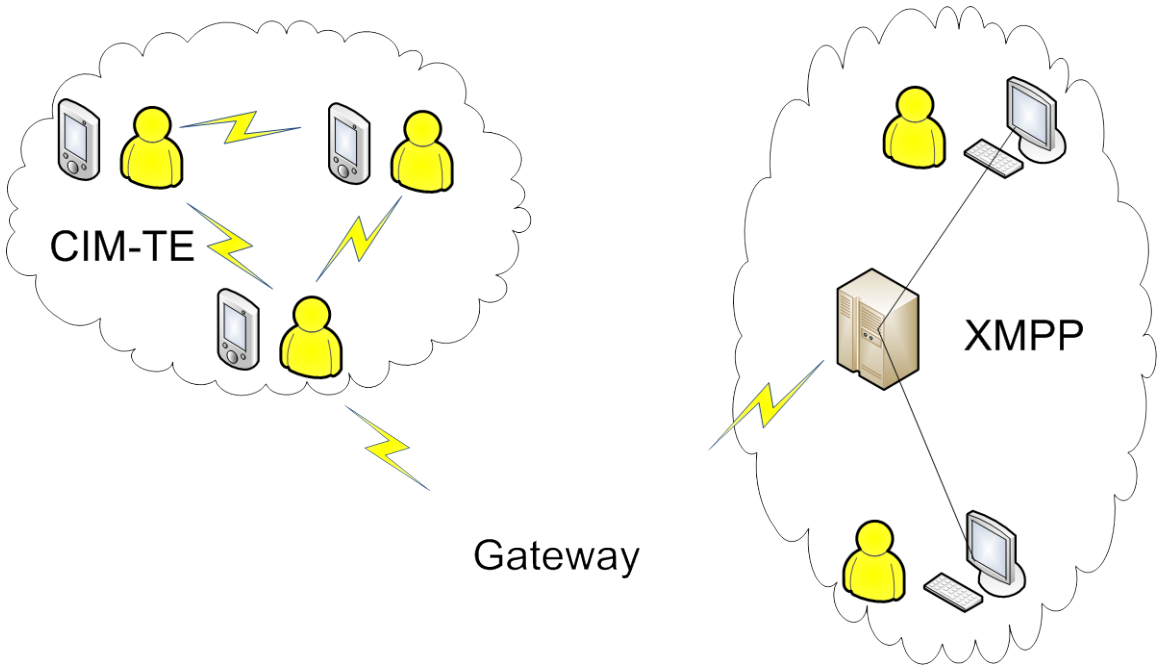
Philipp Steinmetz

# Introduction

- Motivation for Tactical Instant Messaging
  - Bandwidth-efficient
  - Silent information exchange
  - Message history
- Motivation for connection to strategic networks
  - Connection to commanders and technical specialists at HQ

# Goals

- Provide instant messaging in tactical networks
- Connect the tactical instant messaging protocol to XMPP



# Requirements

- Tactical Instant Messaging requirements
  - Distributed system without a server
  - Security
  - Efficiency

# The CIM-TE protocol

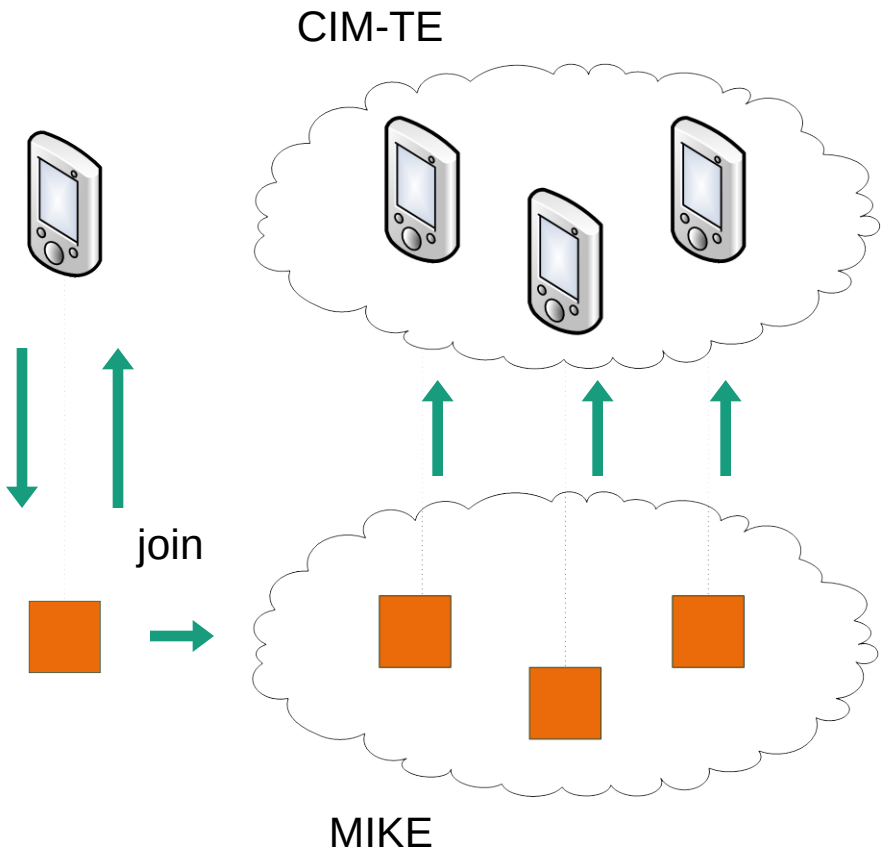
- Instant Messaging protocol for tactical environments
- Distributed system
- Uses IP multicast to distribute messages among a group of users
- Text messages
- Presence messages: status updates

# The CIM-TE protocol

- Signature: Digital signature to provide authenticity
- Message: Symmetric message encrypted with AES
- SenderID, MsgID: Unique message identification
- KeyID, TMFlag: Used by MIKE protocol

# The MIKE protocol

- The encryption key is provided by the MIKE protocol
- MIKE: Group key distribution protocol based on Diffie-Hellman key exchange
- Key is provided to all group members
- Key changes when members join or leave






Fraunhofer FKIE

# The XMPP protocol

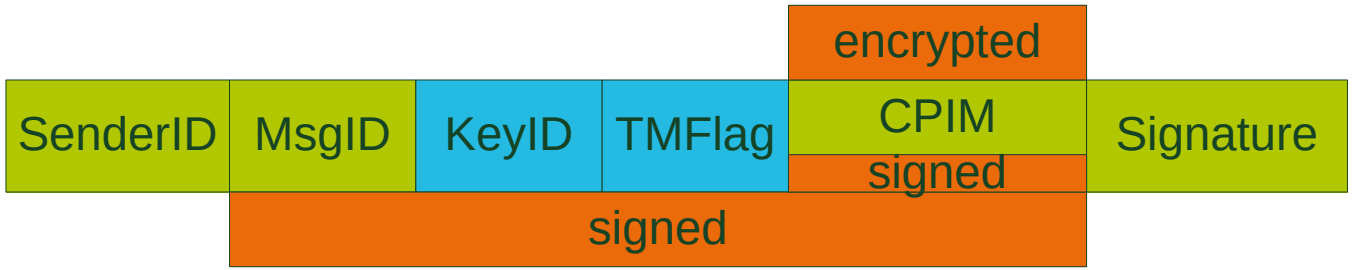
- Used in strategic networks
- Popular instant messaging standard
- XML streams between client and server
- Standards process for extensions (XEPs)

# CIM-TE/XMPP gateway requirements

- Connect tactical and strategic messaging
- Maintain security features
  - confidentiality, authenticity, integrity, non-repudiation
- Limit effects of malicious gateway

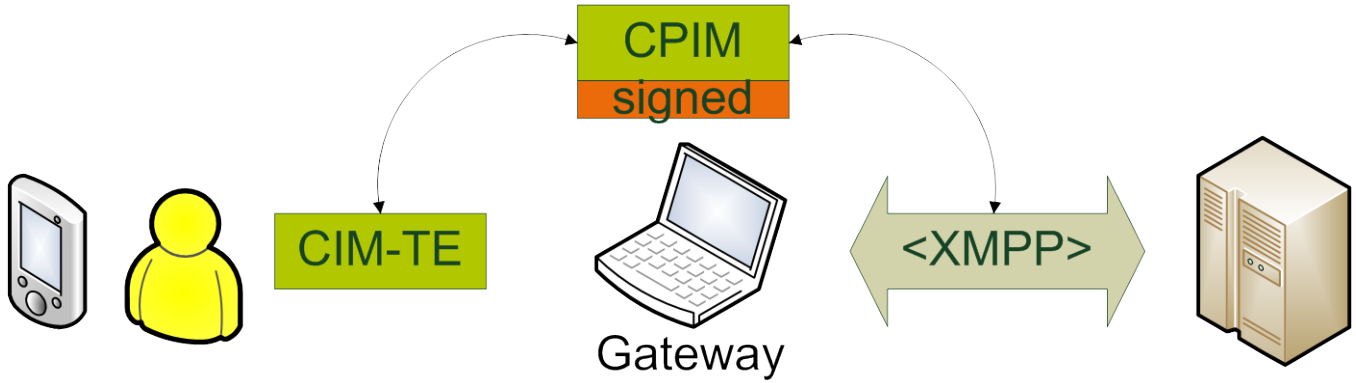
# CIM-TE/XMPP gateway

- Mechanism described in RFC 3923 “End-to-end signing and object encryption for XMPP“
- Sender generates signed messages in CPIM format
- Both protocols use CPIM elements instead of plain text



# CIM-TE/XMPP gateway

- Gateway translates between CIM-TE messages and XMPP XML stanzas without modifying the CPIM elements
- Receiver can verify the original sender's signature
- Gateway cannot forge text messages



# CIM-TE/XMPP gateway

- Symmetric decryption and re-encryption at gateway
- Gateway is group member: access to all messages anyway
- Low computational cost for encryption
- Independent key management for each protocol

# Implementation

- CIM-TE
  - Implemented in Java ME
- CIM-TE with XMPP gateway functionality
  - Implemented in Java SE
- Java advantages
  - Runs on PDAs
  - Libraries available for crypto operations, XML and XMPP

# Optimization

- Possible CIM-TE optimization:
  - Replace CIM-TE signature with keyed MAC, since it contains a signed CPIM element
  - Use pre-distributed MAC key
- Message content is still signed by the sender
- Message flags are protected

# Cryptographic operations

- Asymmetric crypto operations (signing, verification) are expensive
- Optimization (orange) reduces them for CIM-TE and gateway nodes

| Node activity | Signing operations | Verification operations |
|---|---|---|
| CIM-TE send | 2 1 | |
| CIM-TE receive | | 2 1 |
| XMPP send | 1 | |
| XMPP receive | | 1 |
| CIM-TE to XMPP | | 2 1 |
| XMPP to CIM-TE | 1 0 | 1 |

# Summary

- Gateway between XMPP and CIM-TE, our tactical IM
- Gateway maintains security features with end-to-end signing and re-encryption
- Java implementation

# Thank you!

philipp.steinmetz@fkie.fraunhofer.de