On Trust Establishment in Mobile Ad-Hoc Networks

Laurent Eschenauer, Virgil D. Gligor and John Baras

ECE Department, University of Maryland

Proceedings of the Security Protocols Workshop (2002)

Trust

– reliance on the integrity, strength, ability, surety, etc., of a person or thing.

Real Life

- Trusting a Colleague
- Trusting a Colleague's Trust about another Colleague

Computer Network

- Trusting a Node
- Trusting a Node's Trust about another Node

Transitivity

A -> B -> Y

How Things work in Internet

Internet

- Certification Authority certifies someone.
- That Certificate is stored in a Directory Server
- People contact the Directory Server to fetch that Certificate in order to establish “Trust” on “Someone”

Real Life

- Your Trusted Friend trusts someone
- “Someone” contacts you with Reference to your “Trusted Friend”
- You call your “Trusted Friend” to confirm his Trust

What's Odd and What's Not

Similarity

- Transitivity of Trust Establishment
- Uncertainty in Trust Establishment
- Guaranteed Connectivity to Trust-Infrastructure Servers

Oddity

- Trust Establishment without a Trust Infrastructure
- Short-lived, Fast, and On-line-only Trust Establishment
- Trust Establishment with Incomplete Evidence

What's Required in a MANET

Peer-to-Peer, independent of a pre-established trust infrastructure (i.e. Certification Authority and Directory Servers)

Short, fast, and on-line; and

Flexible, support uncertain and incomplete trust evidence.

Scenario 1

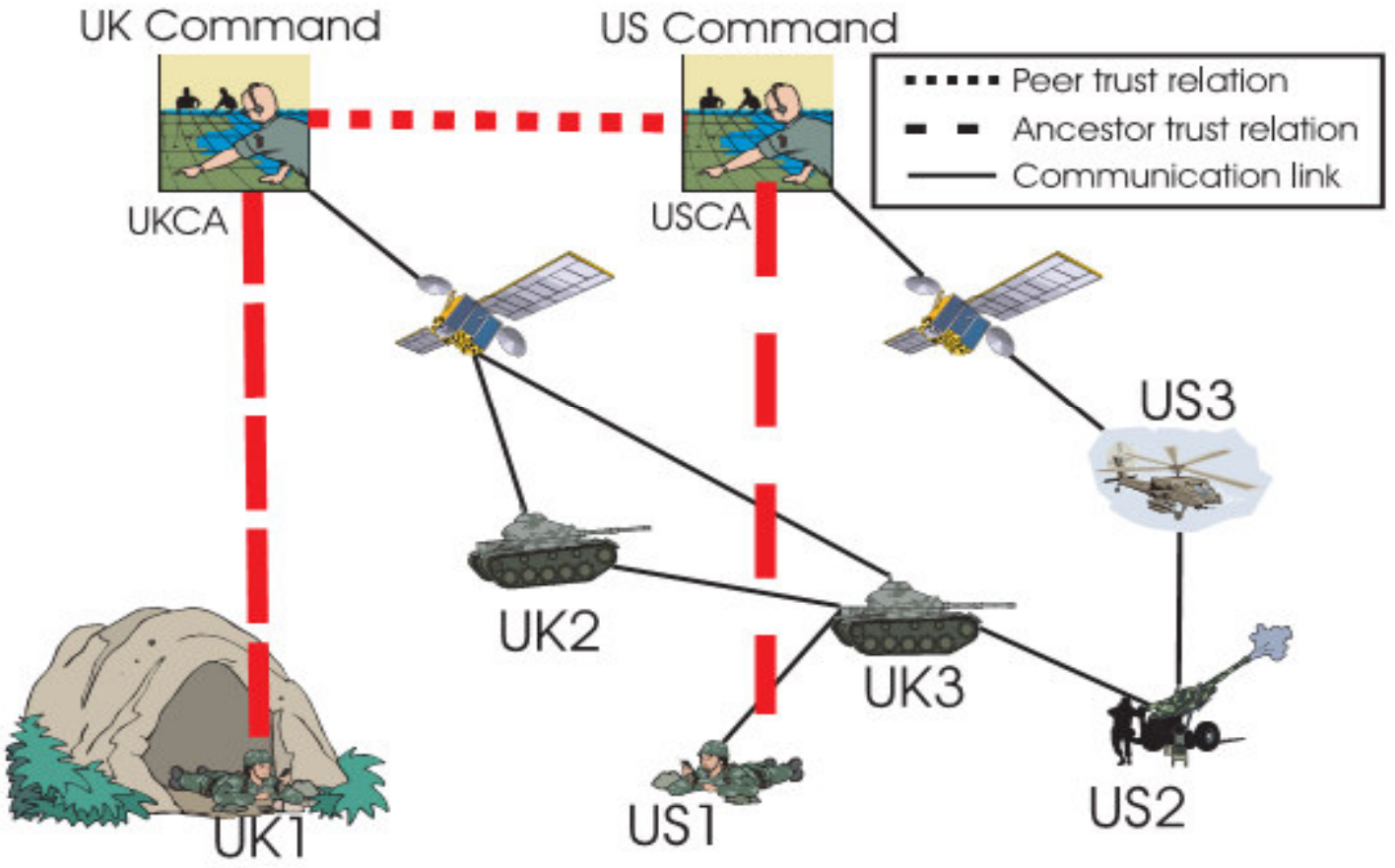


Fig. 1. A battlefield scenario. UK1 is lost and can only communicate with US1

Scenario 2

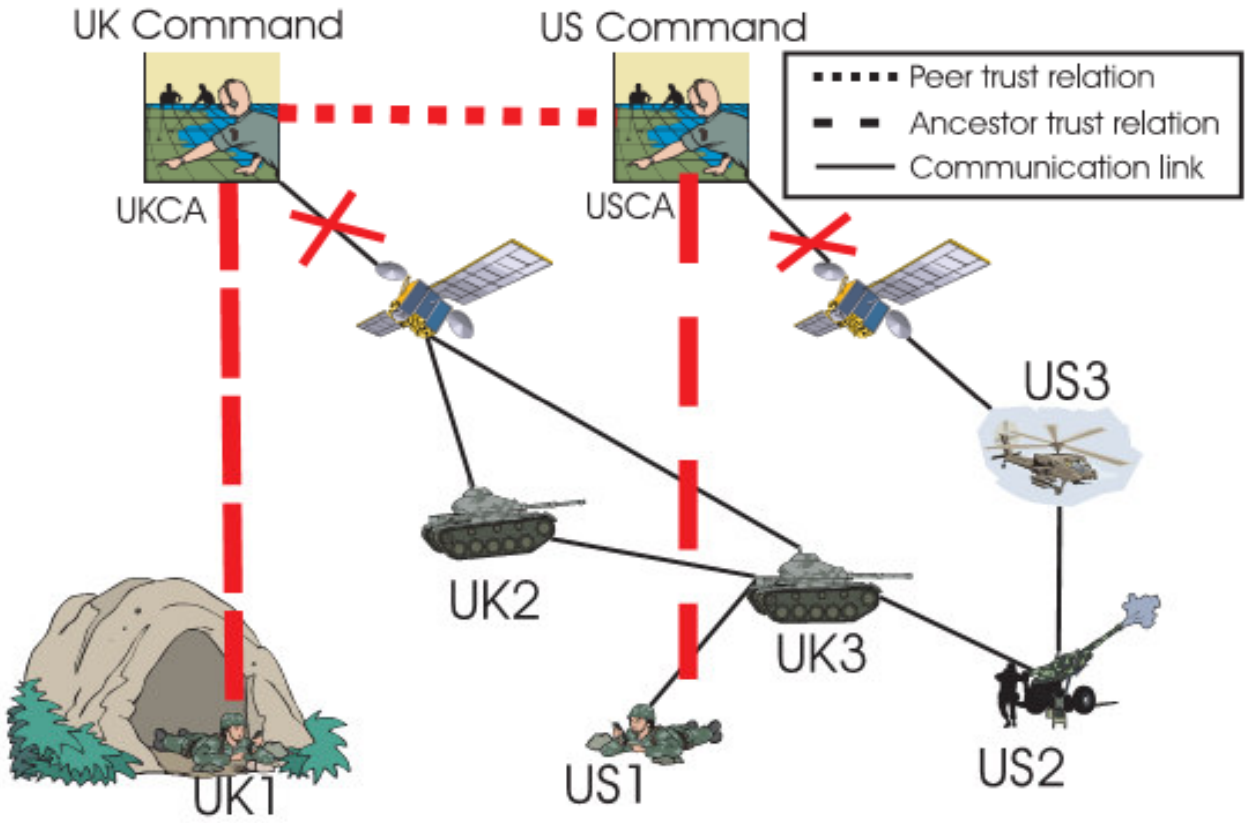


Fig. 2. A battlefield scenario. UK1 is lost and can only communicate with US1. The satellite links are down due to inclement weather

Scenario 3

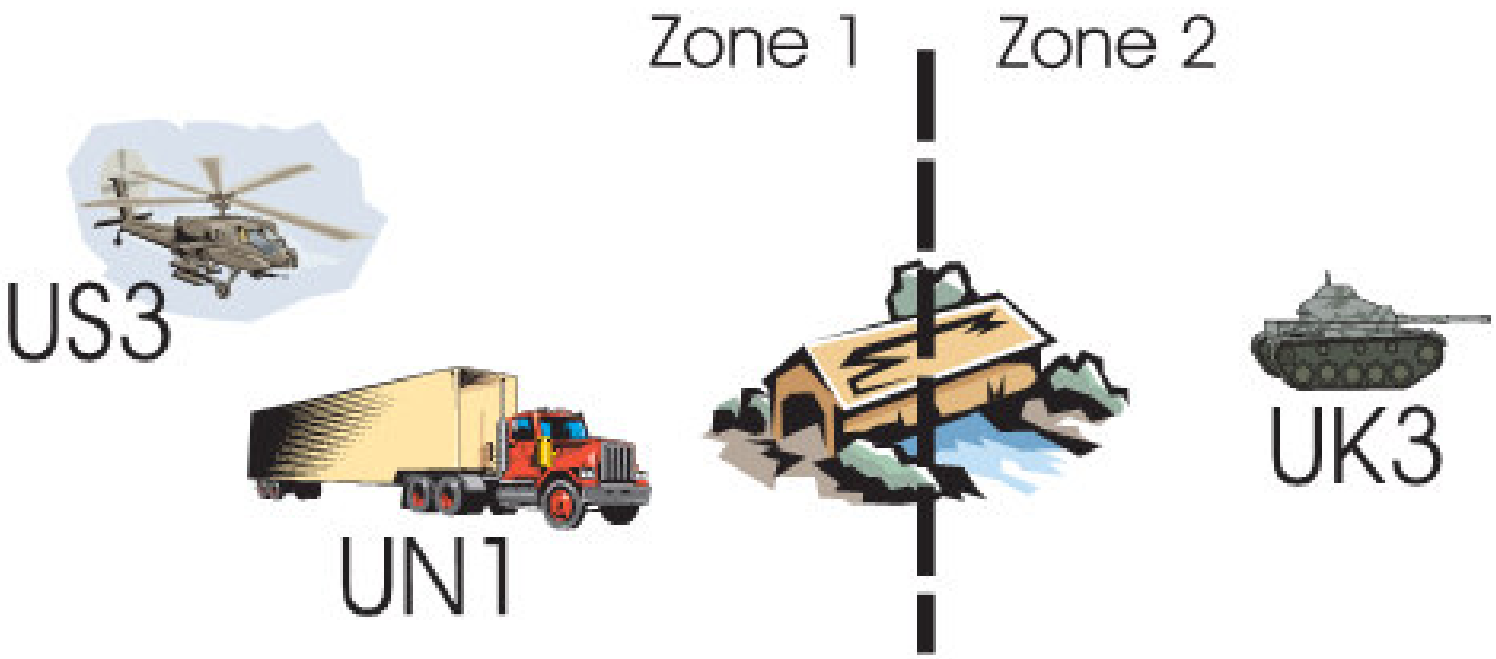


Fig. 3. A battlefield scenario

Solution Proposed

Generation of Trust Evidence

- Any Node can generate trust evidence about any other Node.
- Evidence can be generated Off-Line or On-Line.
- Principal generates a piece of evidence and Signs it specifying its Lifetime.
- Principal distributes the Evidence and has the Right to Revoke.

Solution Proposed

Distribution of Trust Evidence

- Peer-to-peer file sharing for evidence distribution
- Freenet File Sharing – REQUEST (ALICE/*)
- Swarm intelligence for trust evidence distribution

Solution Proposed

Application of Evaluation Metric to Body of Evidence

Active Research - Trust metrics to evaluate uncertain/incomplete sets of evidence.

Only Implemented Trust Metric - PGP - Web of Trust

PGP handles only the evaluation of trust in a chain of keys, with limited "levels of trust"

EG. – A Key is marginally trusted if signed by two independent, marginally trusted keys.

Conclusion

Pros

- Comprehensive comparison of Internet and MANET Trust Model.
- Nice Explanation of Transitivity concept.
- Discussed Scenarios are Practical.

Cons

- No Implementation
- Freenet Modification Idea not complete.
- No Simulations
- No Experiments

Other Papers

- Establishing Trust In Pure Ad-hoc Networks
- Cooperation in Wireless Ad Hoc Networks

Fitting All Pieces Together

Reno Varghese - GeoCast

- GFG and GFPG
- GeoTORA
- GeoGRID
- Location Based MultiCast
- Voronoi Based GeoCast

Fitting All Pieces Together

Pavneet Singh - Localization

GPS Free Node Localization in Mobile Wireless Sensor Networks

Algorithms for Nodes Localization in Wireless Ad-Hoc Networks Based on Cost Function

Fitting All Pieces Together

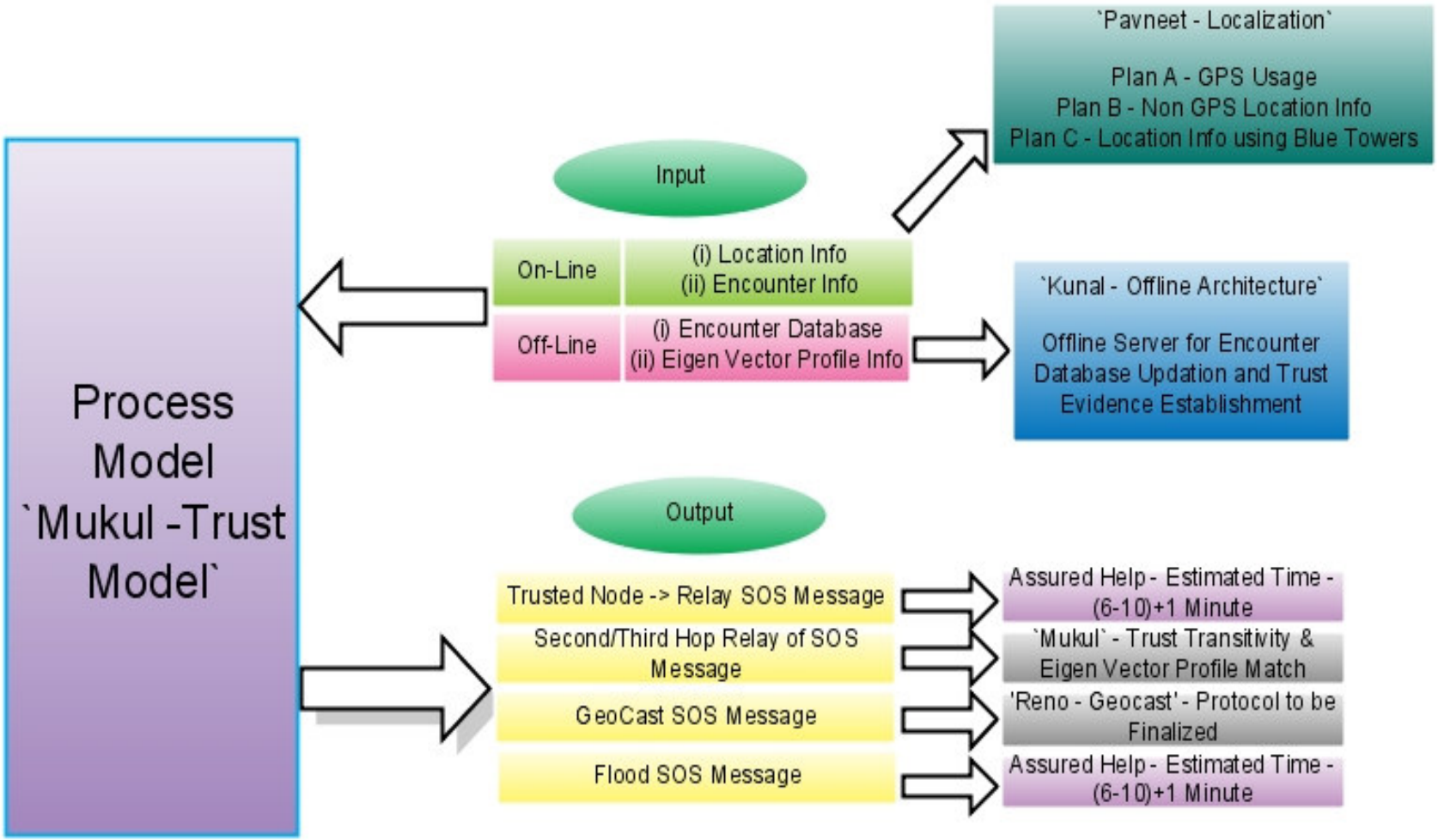
Kunal Sawlani- Architecture

CarTel: A Distributed Mobile Sensor Computing System

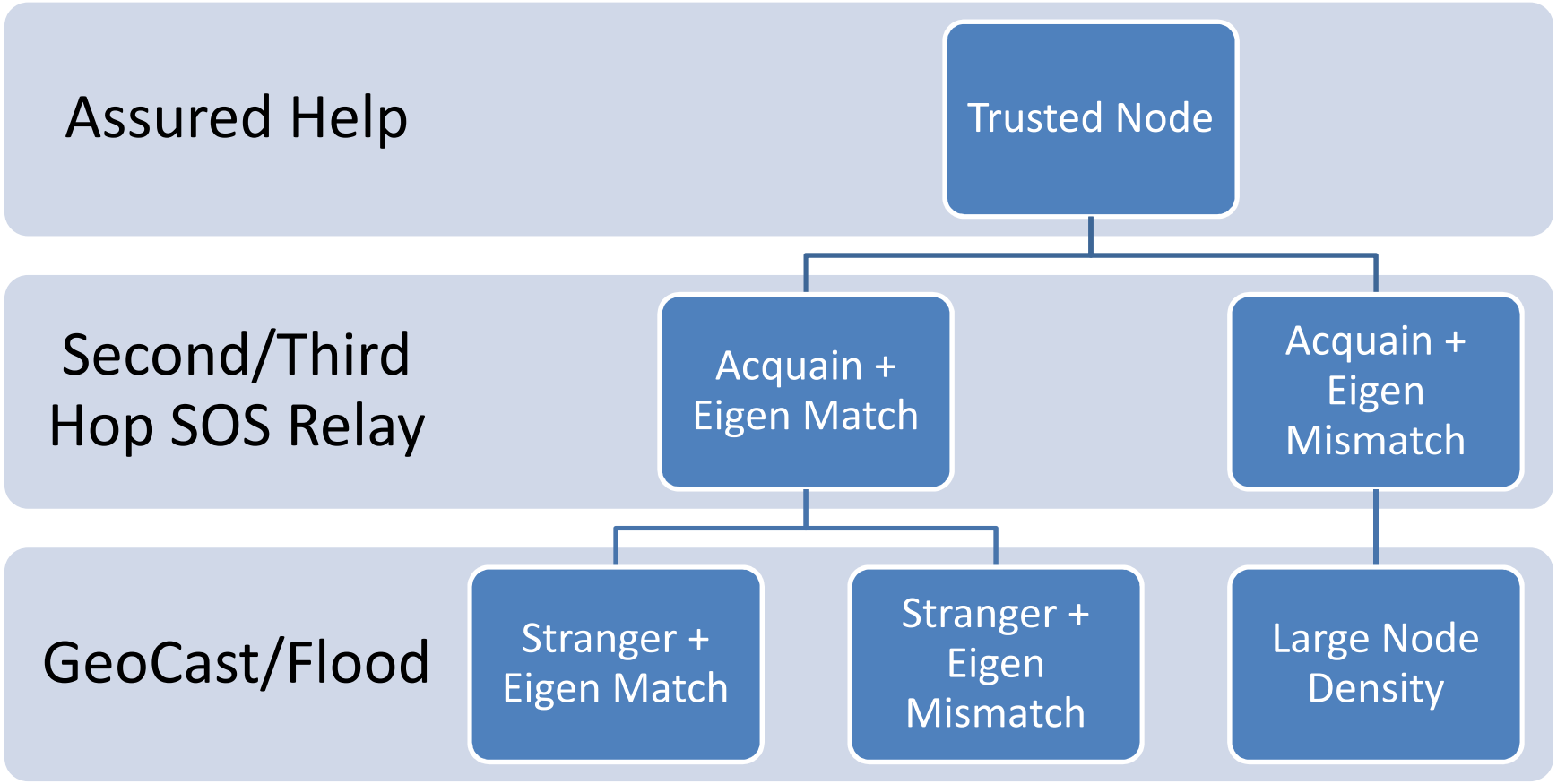
Mukul Sharma – Trust Model

On Trust Establishment in Mobile Ad-Hoc Networks

Process Model



Trust Hierarchy



System View

On Drawing Board

Thanks!!

Questions or Comments!!