Mobile Ad-Hoc Networks (MANETs)

Ad-hoc = > no designated infrastructure prior to deployment

- no predetermined access points or topology, no allocation of nodes to administrative services
  - no dedicated router nodes, name servers, certification authorities, etc.
- no distinction between trusted and untrusted nodes
  - no physical and administrative protection of trusted nodes
  - nodes are subject to capture

- Mobile => topology changes dynamically

- Wireless => connectivity among nodes is not guaranteed
  - broadcast to one-hop neighbors is inexpensive
  - limited power and energy traded-off for connectivity

…. are very different from Mobile IP v6

Trust Establishment in MANETs

- *Trust:* a *relation* among entities (e.g., domains, principals, components)
  - established by evidence evaluation using specified metrics, and
  - required by
    - *specified policies* (e.g., by administrative procedures, business practice, law)
    - *specified design goals* (e.g., composition correctness via use of layering, abstraction)

Example: An Authentication-Trust Relation

"A *accepts* CA_B's *signature* on X's *PK certificate"*

Basis for *A's acceptance of* CA_B's *signature :* off-line *evaluation* of *evidence*

- CA_B's authentication of X is done using "*acceptable*" mechanisms and policies (i.e., A *trusts*^{AU} CA_B)
- CA_B's registration database (including X's registration) is protected using "*acceptable*" mechanisms and policies (i.e., A *trusts the Registration DBMS*)
- CA_B's server is managed using "*acceptable*" administrative, physical and personnel policies (i.e., A *trusts* CA_B's administrators)

What Do We Mean By Trust Establishment ?

Trust establishment (in general):

- *application of an **evaluation metric** to a body of **evidence**,*
- ***on-** or **off-line**, on **short-** or **long-terms**, and*
- *where the evidence may include **already established trust relations**.*

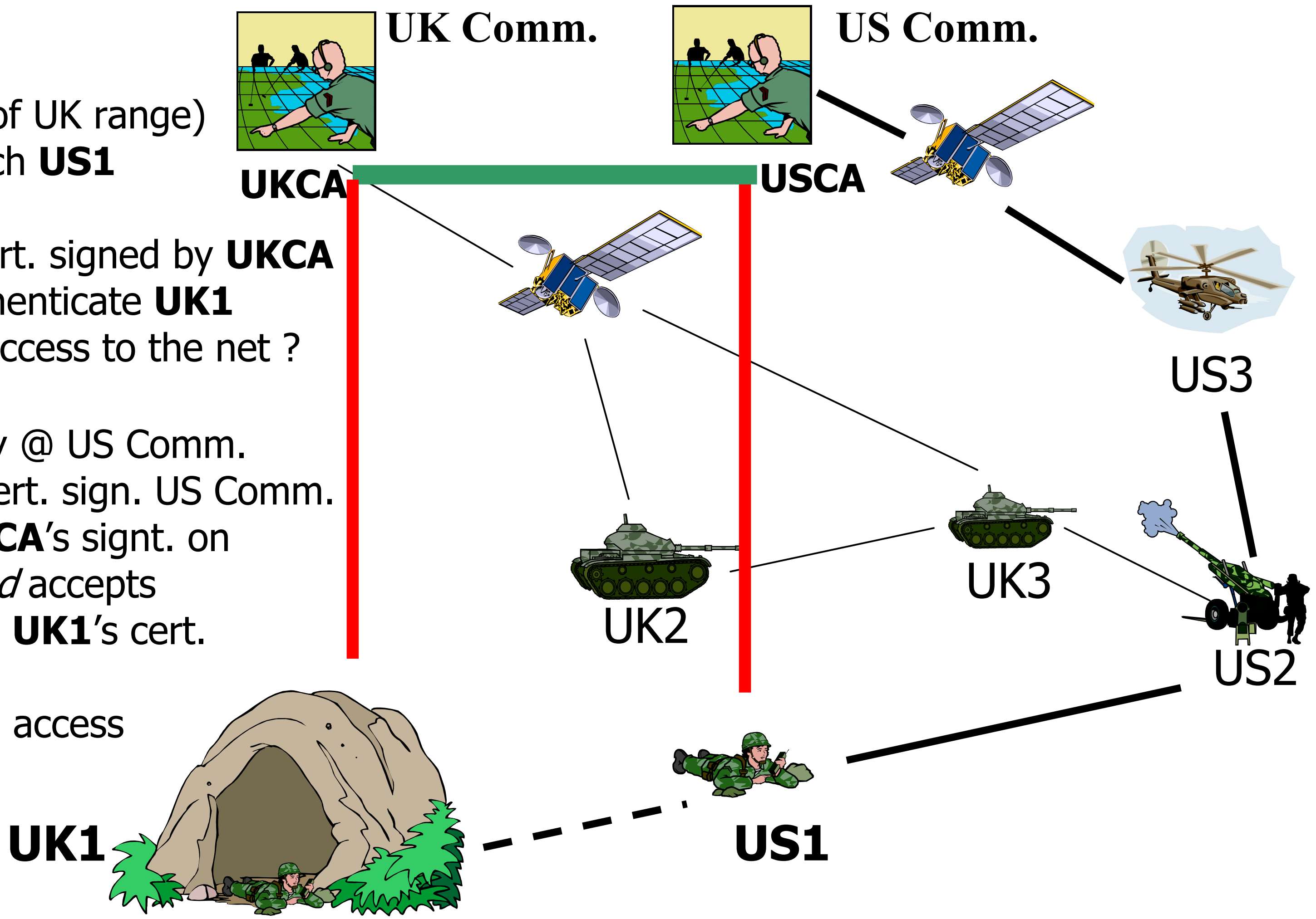
Old Focus: The Internet…

Scenario 1:
UK1 is lost (out of UK range) and can only reach **US1**

UK1 b-casts a cert. signed by **UKCA**
• Could **US1** authenticate **UK1** and grant him access to the net ?

- **US1** -> Directory @ US Comm.
- **US1** <- **UKCA** cert. sign. US Comm.
- **US1** accepts **USCA**'s signt. on **UKCA**'s cert. *and* accepts **UKCA**'s signt. on **UK1**'s cert.

• **US1** grants **UK1** access



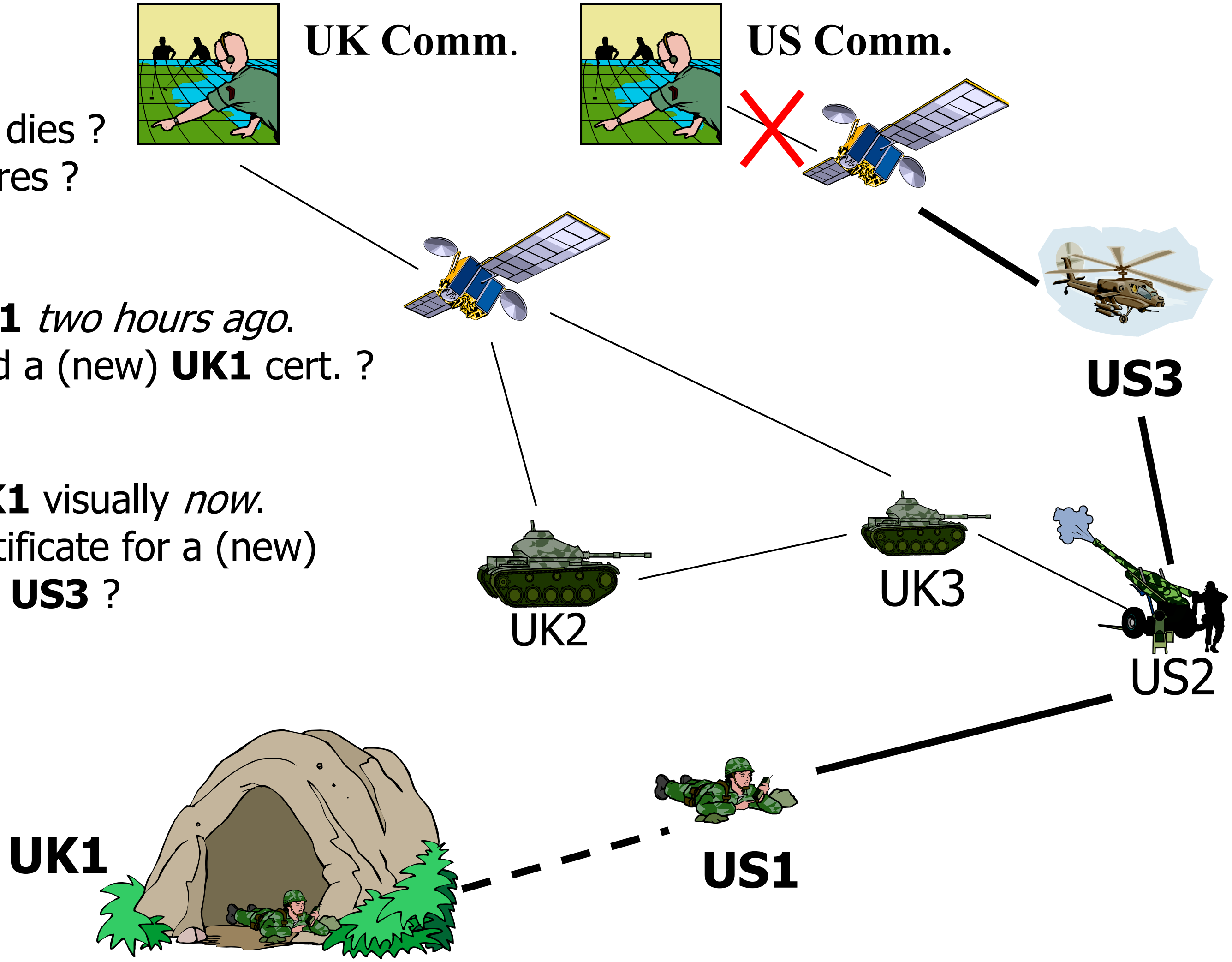
All trust relations (🟥 🟩 and evaluated evidence) are *available* and are used.

… vs. New Focus: MANETs

Scenario 2:
What if **US1**'s satellite link dies ?
Or if **UK1**'s certificate expires ?

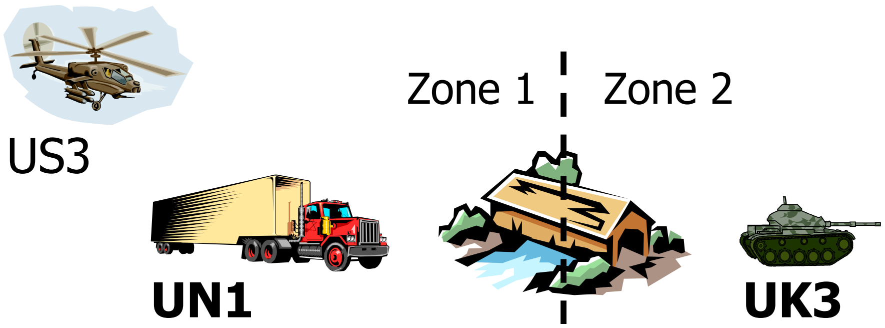
- **Fact 1**: **US3** located **UK1** *two hours ago*.
  - Should **US3** have issued a (new) **UK1** cert. ?

- **Fact 2**: **US1** locates **UK1** visually *now*.
  - Should **US1** issue a certificate for a (new) **UK1**'s key? What about **US3** ?



Need 1: Dynamic, proactive, generation of trust evidence on-line

… MANETs *(cont)*



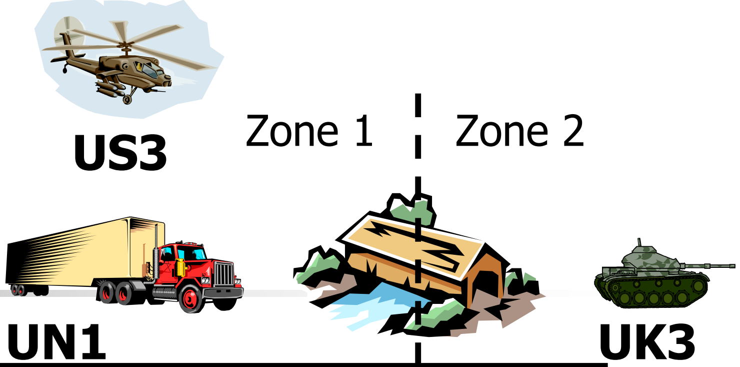
Scenario 3:

- **UN1** needs a “zone report” before entering Zone 2 and sends a request to **UK3**
- **UK3** negotiates with **UN1** the *types* of credentials needed for a “zone report”

UK3’s policy for providing “zone reports”:

(**Role** = UK/US mil.∨ UN convoy) with conf.= high ∧ (**location**={neighbors}) with conf.= medium

… MANETs*(cont.)*



- **UN1's request presents credentials**

Cert(**Role**=UNConvoy)$_{\text{USCA}}$; Cert(**Location**/GPS=zone2)$_{\text{GPS1}}$; Cert(**Location**/Visual=zone2)$_{\text{US3}}$

Fact 3: **UK3**'s trust relations **UKCA** for **Role**; **GPS1**, **UAV1**, and **UK1** for **Location**

Fact 4: Directory Server @ UK Comm. and **UK1** are *out of* **UK3**'s *range*

UK3's *metric* for confidence evaluation of *location evidence*

• Type(source) = GPS	and source trusted	-> conf.= low
= UAV	and source trusted	-> conf.= low
• Type(src1) = UAV		
∧ Type(src2) = GPS	and src1 and src2 trusted	-> conf.= medium
• Type(source) = Visual	and source trusted	-> conf.= high
• Other		-> conf.= null

UK3's *metric* for confidence evaluation of *role evidence*

• Type(source) = CA	and source trusted	-> conf.= high
• Other		-> conf.= null

UK3 must *collect & evaluate evidence* re: **USCA**, **US3** *via net* search

Should UK3 return a "zone report" to UN1 ?

Research Areas

- **Need 1**: Dynamic, proactive, generation of trust evidence
- **Need 2**: Methods for trust-evidence distribution / revocation
  - Characteristics
    - *"Nothing but net": no distribution / rev. infrastructure but the network itself*
      - evidence may be stored anywhere in the network
      - producer may be unreachable at time of evidence use
    - *It is not just a request routing problem ...*
      - A principal may need more than one answer per request
        - Ideally should collect all the evidence that has been generated

          E.g: REQUEST(Alice/Location) should return more than one answer
      - A principal may *not* know what to look for
        - should handle wildcard requests; e.g: REQUEST(Alice/*)

Research Areas (ctnd.)

Need 3: Evaluation metrics for of trust evidence (on-line)

- accept uncertainty
- "weed-out" false evidence

Prior work: limited types of evidence and mostly off-line generated

- R. Yahalom, B. Klein and T. Beth [1993]
- T. Beth, M. Borcherding, and B. Klein [1994]
- Ueli Maurer [1996, 2000]
- M. K. Reiter and S. G. Stubblebine [1997]