14th ICCRTS
C2 and Agility
Washington D.C.
15-17 June 2009

TECHNOLOGY DRIVEN. WARFIGHTER FOCUSED.

Paper No. 191

Towards Trust-based Cognitive Networks: A Survey of Trust Management for Mobile Ad Hoc Networks

Jin-Hee Cho & Ananthram Swami , Army Research Laboratory

Outline

- Background
- Research Motivation
- Multidisciplinary Trust Concept
- Trust, Trustworthiness, and Risk Assessment
- Trust Properties in MANETs
- Survey on Trust Management in MANETs
- Case Study
- Future Research Directions

Background

- **Design Challenges in Mobile Ad Hoc Networks:**
  - **Resource constraints**
    - ✓ energy, bandwidth, memory, computational power
  - **High security vulnerability**
    - ✓ open medium derived from inherent nature of wireless networks
    - ✓ dynamically changing network topology due to node mobility or failure, RF channel conditions
    - ✓ decentralized decision making and cooperation (no centralized authority)
    - ✓ no clear line of defense
- **Trust**: the degree of subjective belief about the behaviors of a particular entity.
- **Trust management**: defined initially by Blaze et al. (1996) as a separate component of security services in networks.

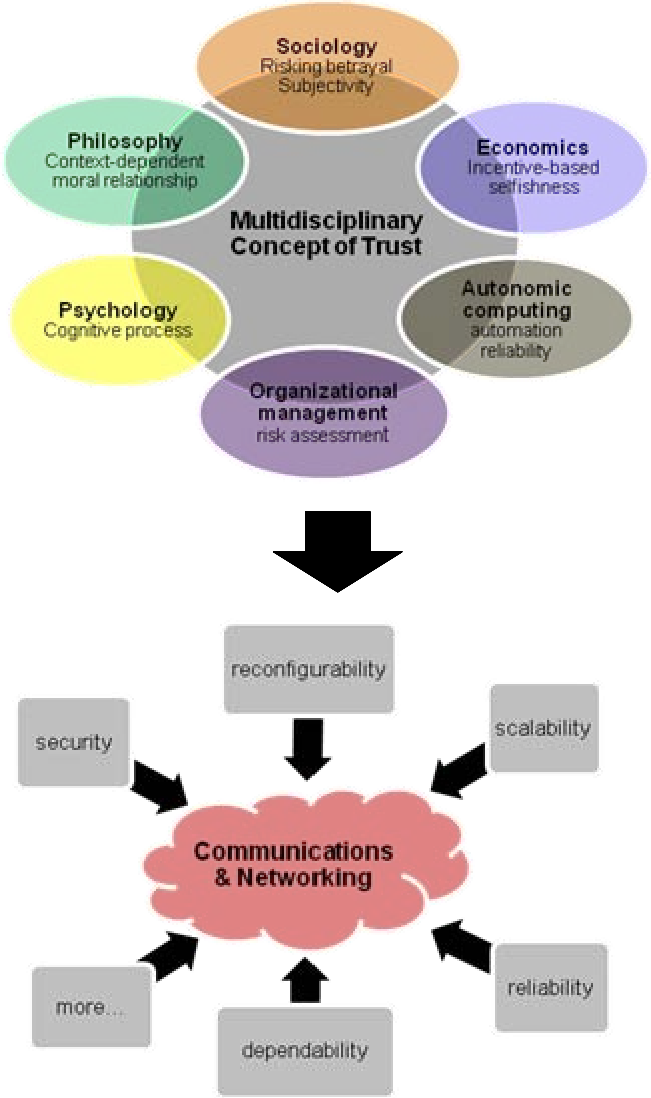
Research Motivation

- Trust management is needed in MANETs with the goal of **establishing a network with an acceptable level of trust relationships among participating nodes**:
  - Network bootstrapping
  - Coalition operation without predefined trust
  - Authentication for certificates generated by the other party when links are down
  - Ensuring safety when entering in a new zone
- **Diverse applicability as a decision making mechanism** for
  - Intrusion detection
  - Key management
  - Access control
  - Authentication
  - Secure routing
  - Others

Multidisciplinary Trust Concept

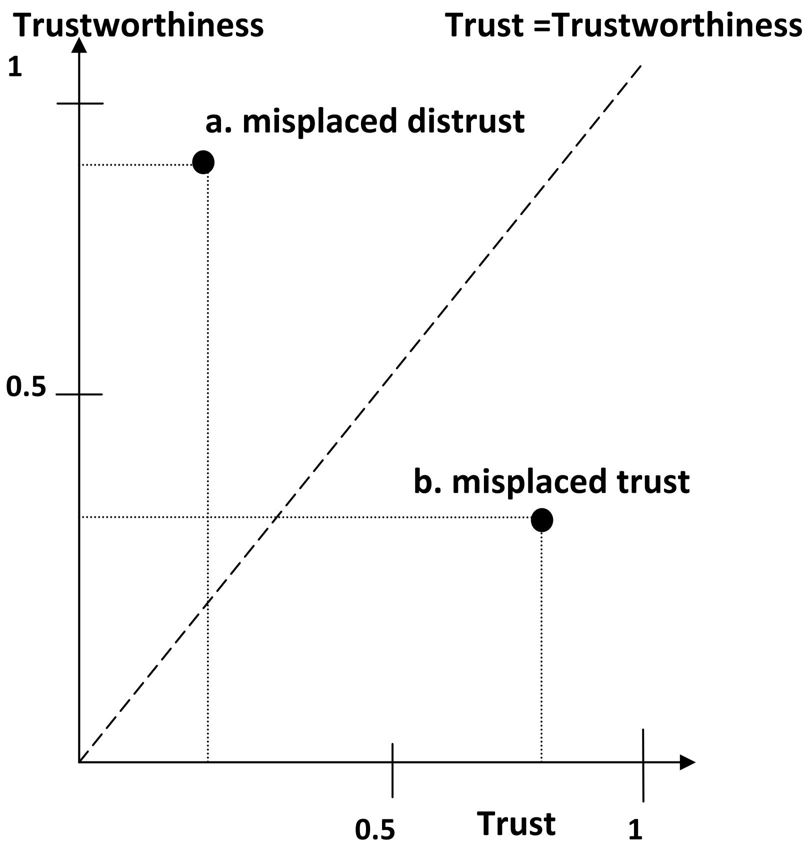
- ***Merriam Webster's Dictionary:*** trust is defined as "assured reliance on the character, ability, strength, or truth of someone or something."
- **Trust in Sociology**
  - Subjectivity, an indicator for future action, and dynamicity based on continuous interactions between two entities.
  - A continuous term and risking betrayal in building trust.
- **Trust in Economics**
  - An expectation that applies to situations in which trustors take risky actions under uncertainty or information incompleteness.
  - Based on the assumption that humans are rational and strict utility maximizers of their own interest or having incentives to themselves.
- **Trust in Philosophy**
  - Important but dangerous
  - Moral relationships: depending on the nature of personal relationships between a trustor and a trustee, trustful actions or betrayal can be taken.
- **Trust in Psychology**
  - Cognitive process that human beings learn trust from their experiences, e.g., relationship between mother and the child

Trust in Communications & Networking



- **Trust in Organizational Management**
  - – The willingness to take a risk or willingness to be vulnerable in the relationship in terms of ability, integrity, and benevolence
- **Trust in Autonomic Computing**
  - – The attitude that an agent will help accomplish an individual's goals in a situation with uncertainty and vulnerability
  - – Automation reliability as the level of trust
- **Trust in Communications & Networking**
  - – A set of relations among entities participating in a protocol based on the evidences generated by the previous interactions of entities
  - – Trust accumulate among entities as their interactional have been faithful to run the protocol
  - – Context-aware trust
- Trust is a well-defined descriptor of security and encryption as a metric to reflect security goals [Golbeck, 2006]

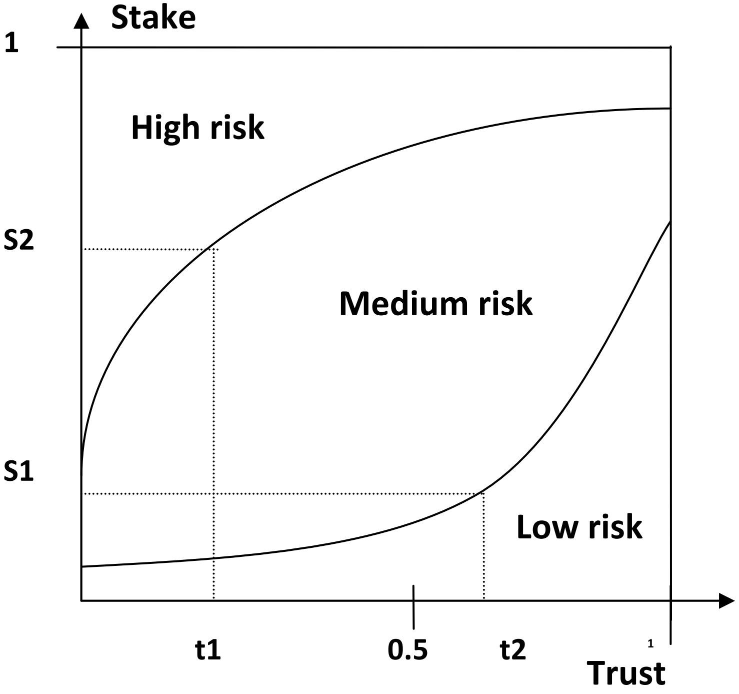
Trust, Trustworthiness, and Risk Assessment



Trust Level [Solhaug et al., 2007]

- **Trustworthiness**: objective trust probability of trust level, *actual trust*
- **Trust**: subjective trust probability of trust level, believed/measured trust
- Risk estimation is closely linked with measuring accurate trust relations
- Real trust may not be applied in real situations
  - Context independent *reliability trust*
  - Context dependent *decision trust*

Trust vs. Risk

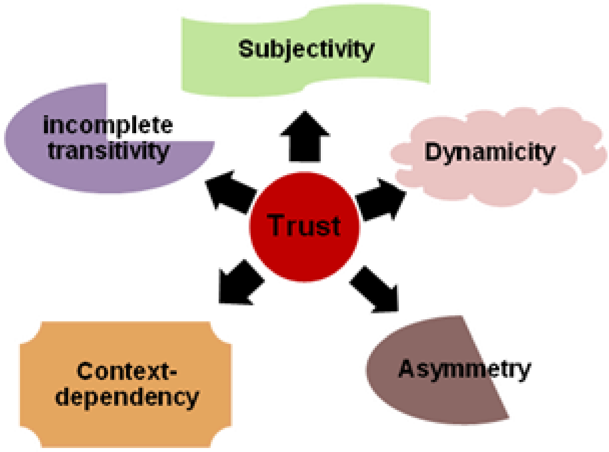


Trust vs. Risk
[Solhaug et al. 2006,
Josang & LoPresti, 2004]

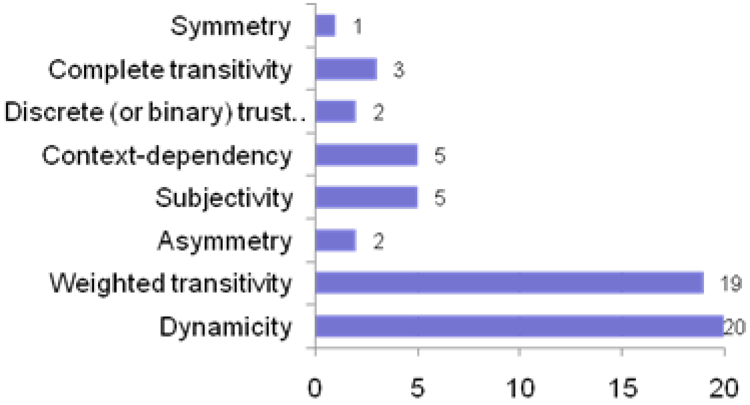
- In general, if trust is high, the risk is low, and vice versa.
- However, notice that even high risk exists when trust is high, trust = 1.
- Opportunity and prospects (positive consequence) are important.
- Trust should be measured considering acceptable risk level in terms of prospects.

Trust is generally neither proportional nor inversely proportional to risk.

Trust Properties in MANETs



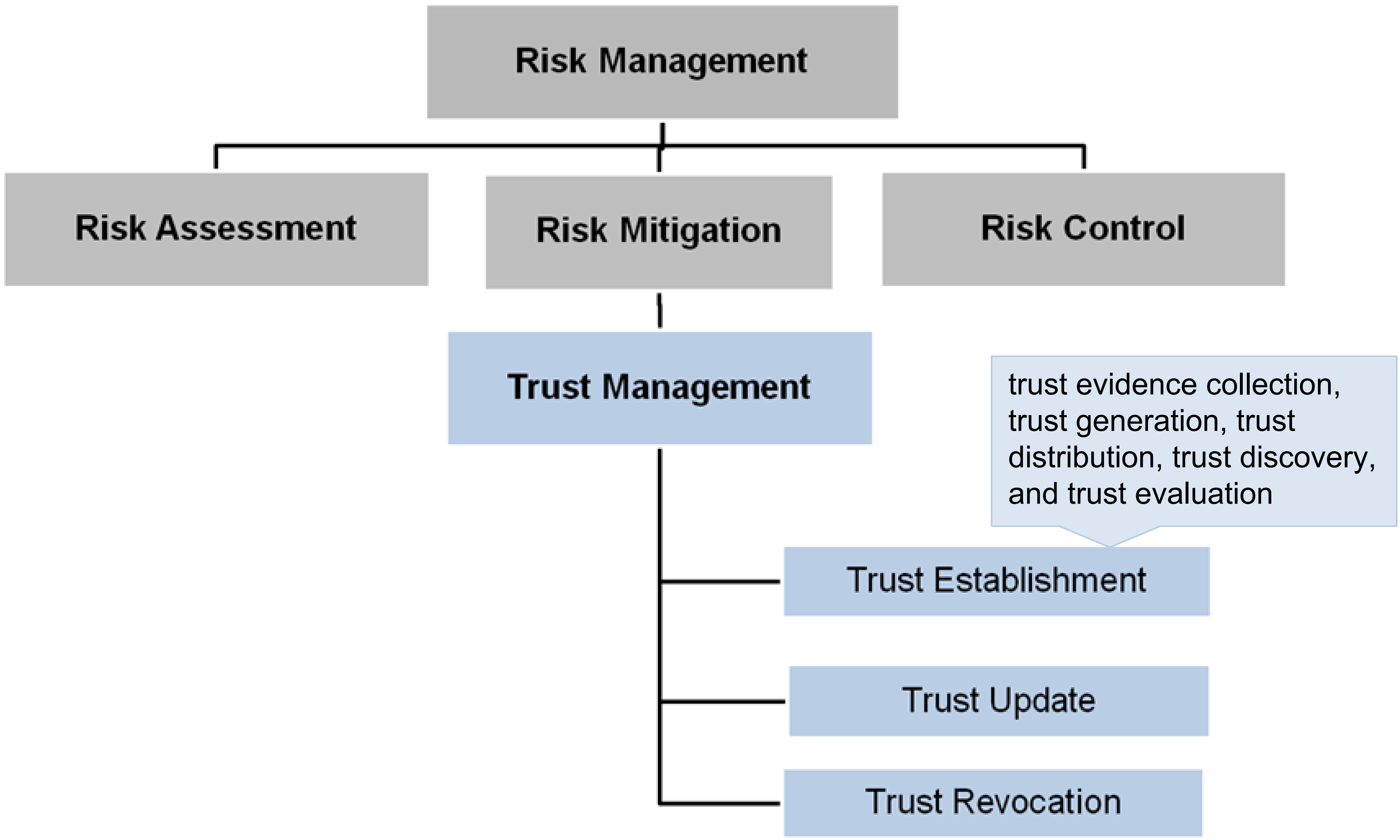
Trust properties in MANETs.



Trust properties in existing trust management in MANETs.

- **Dynamic**, not static
  - Trust in MANETs should be established based on local, short-lived, fast changing over time, online only and incomplete information available due to node mobility or failure, RF channel conditions
  - Expressed as a continuous value ranging from positive and negative degree
- **Subjective**
  - Different experiences derived from dynamically changing network topology
- **Not necessarily transitive**
- **Asymmetric**, not necessarily reciprocal
  - Heterogeneous network
- **Context-dependent**

Classification of Trust Management



Risk Management

Risk Assessment

Risk Mitigation

Risk Control

Trust Management

trust evidence collection, trust generation, trust distribution, trust discovery, and trust evaluation

Trust Establishment

Trust Update

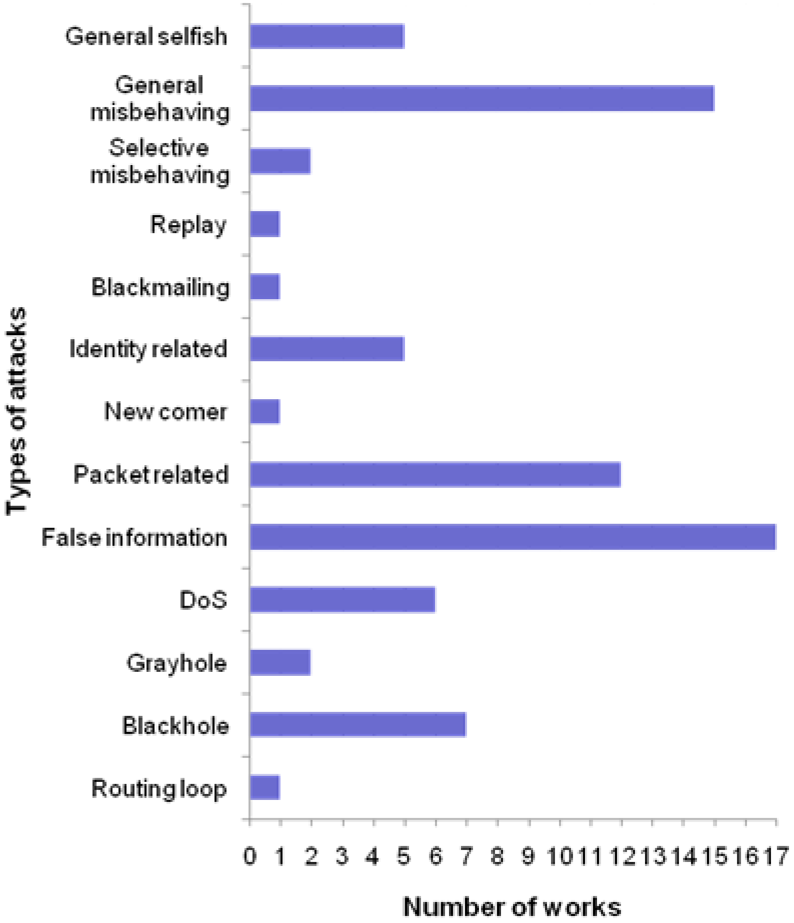
Trust Revocation

[Solhaug et al. 2006]

Classification of Methodologies on Trust Management

- **Reputation-based framework vs. Trust Establishment Framework** [Li et al., 2008]
- **Policy-based trust management vs. Reputation-based Trust Management** [Yonfang, 2007]
- **Evidence-based trust management**: anything that proves the trust relationships among nodes including public key, address, identity, or any evidence that any node can generate for itself or other nodes through the challenge/response process [Li & Singhal, 2007]
- **Monitoring-based trust management**: direct and indirect observations [Li & Singhal, 2007]
- **Trust Establishment Frameworks** [Aivaloglou et al., 2006]**:**
  - Certificate-based framework: using certificates
  - Behavior-based framework: ensured by preloaded authentication mechanism
- **Architectures** [Aivaloglou et al., 2006]:
  - Hierarchical framework: centralized systems
  - Distributed framework: distributed systems such as MANETs

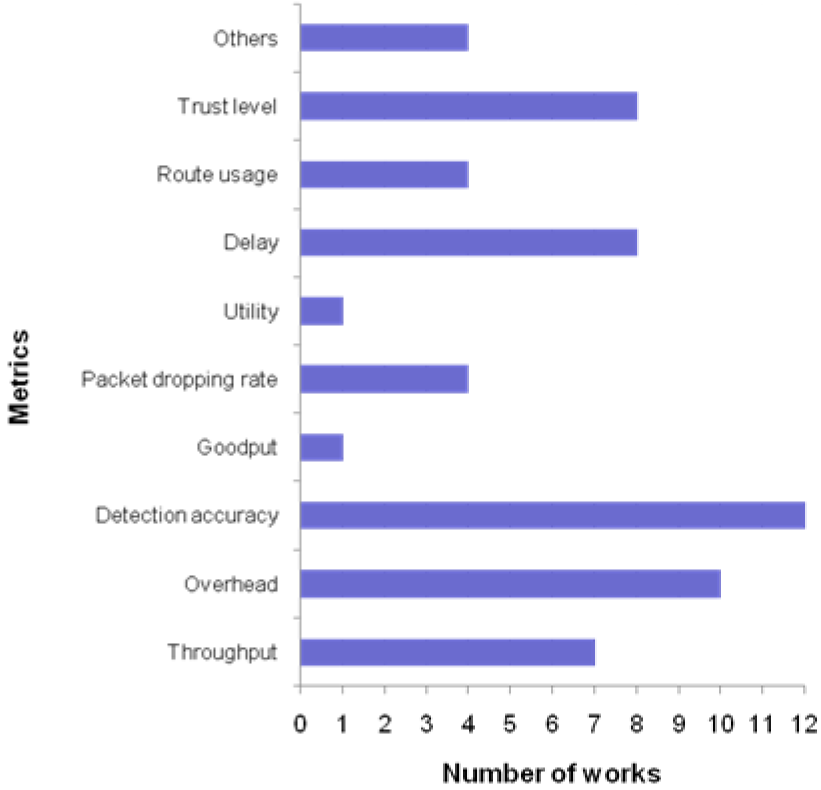
Attacks in MANETs



Attacks considered in existing trust management in MANETs.

- By the nature of attack and the types of attackers [Liu et al., 2004]
  - **Passive Attacks**: when an unauthorized party gains access to an asset but does not modify its content, (e.g., eavesdropping or traffic analysis)
  - **Active Attacks** : masquerading (impersonation attack), replay (retransmitting messages), message modification, DoS (e.g., excessive energy consumption)
- By the legitimacy of attackers [Liu et al., 2004]
  - **Insider attacks**: authorized member
  - **Outsider attacks**: illegal user
- Existing work mostly considered network layer attacks

Metrics for Trust Management in MANETs



Metrics used for evaluating existing trust management in MANETs.

- Trust management schemes has been evaluated by general performance metrics, e.g., throughput, goodput, overhead, delay, utility, packet dropping rate, etc.
- Detection accuracy is most popularly used as a performance metric.
- Recently trust metric (e.g., trust level) has been used to evaluate the proposed trust management schemes.

Composite Trust Metric

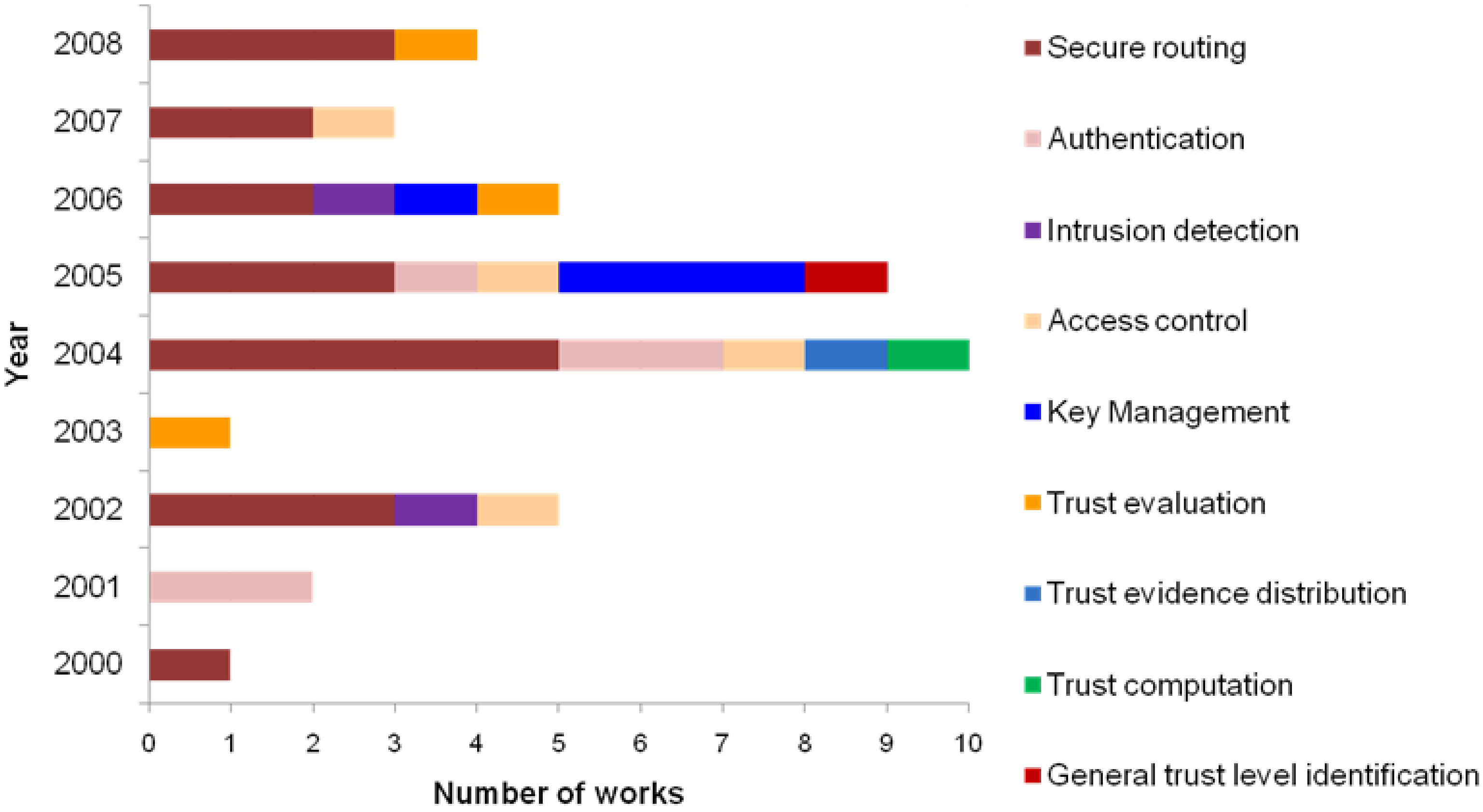
Quality-of-Service (QoS) Trust

- Information on competence, dependability, reliability, successful experience, and reputation or recommendation representing "task" performance
- Examples are the node's energy lifetime or computational power level, completing packet delivery, or evaluations using reputation or recommendation

Social Trust

- Use of the concept of social network [Yu et al., 2008] based on common interests
- Friendship, honesty, privacy, and social reputation or recommendation derived from direct or indirect interactions for "sociable" purpose.

Existing Trust Management in MANETs based on Applicability



Historical summary of existing trust management schemes in MANETs by applicability.

Existing Trust Management in MANETs

Secure Routing

- Isolate misbehaving nodes, either selfish or malicious, encourage collaboration
- Reputation-based trust management
- Extension of the existing routing protocols (e.g., DSR, AODV) using trust concept
- Incentive mechanism
- Redemption mechanism
- Direct and indirect observations
- Various trust models introduced:
  - Bayesian model
  - Entropy-based model
  - Probability model
  - Effort-return-based model

Authentication

- Direct (certificate, observations) plus second hand information (e.g., recommendation)
- Extension of the existing routing protocols (e.g., DSR, ZRP)
- Weighted transitivity
- Trust models
  - Marsh's trust model
  - Pretty good privacy

Key Management

- Trust-based hierarchies for key management
  - Physical logical trust domains
  - Hierarchical trust PKI
- Distributed key management

Existing Trust Management in MANETs (Cont.)

Intrusion Detection

- Trust can be a basis for intrusion detection- Local IDS
- IDS provides audit and monitoring capabilities that offer the local security to a node and help perceive the specific trust level of other nodes.
- Evaluating trust and identifying intrusions may not be a separable process with the same goal to build collaborative network environments

Access Control

- Whether or not access to certain resources or rights is allowed in MANETs
  - Trust-based admission control
  - A localized group trust model based on threshold cryptography

Others

- Trust evaluation
- Trust evidence distribution (directed graph, swarm intelligence)
- Trust computation (random graph theory)

Future Research Directions: Trust-based Cognitive Networks

Propose a set of reliable, reconfigurable, and scalable trust management protocols for mission-driven group communication systems (GCSs) in MANETs for military situations.

- Design challenges in military tactical MANETs in addition to challenges in MANETs
- Use of cognitive networks [Thomas et al., 2005]: having a *cognitive process that is capable of perceiving current network* conditions and then planning, deciding, and acting on those conditions.
- We propose to use this concept of cognitive networks in a MANET to introduce cognitive intelligence into each node to adapt to changing network behaviors, such as attacker behaviors, degree of hostility, node disconnection due to physical environment such as terrain, energy exhaustion on a node, or voluntary disconnection for energy savings.

Case Study: Modeling and Analysis of Trust Management in MANETs

Trust Metric

- The overall trust consists of two components:
  - **QoS trust**: energy level + unselfishness (w.r.t. collaboration)
  - **Social trust**: intimacy (w.r.t. friendliness) + healthiness (w.r.t. honesty)
- Trust decays as length of a trust chain grows
- Trust decays over time as frequency of interactions decreases (location prob.)
- Trust is calculated based on direct observations plus recommendations from others
- Trust values are normalized to lie in the range [-2,2]

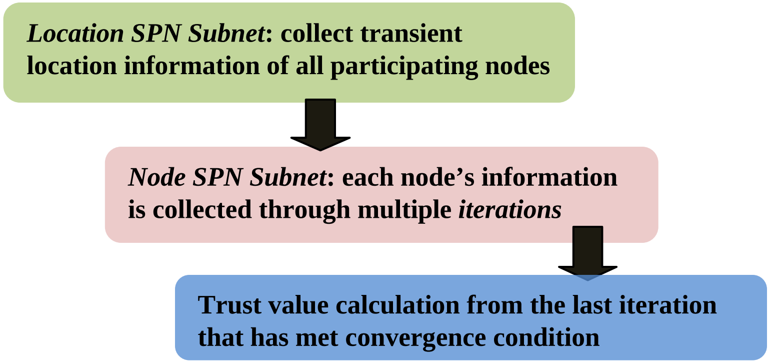
Energy Model

- Energy level of each node is adjusted based on its status such as:
  - Selfish or not
  - Member or not
  - Compromised or not
- Considered energy consumption for transmission and receiving packets

Attack Model

- Prevent outside attackers using intrusion prevention techniques (e.g., authentication or encryption)
- Alleviate inside attackers using IDS
- Attacks performed: fake information dissemination
- Use a distributed rekeying operation as a reaction mechanism of IDS

Case Study: Modeling and Analysis of Trust Management in MANETs (Cont.)

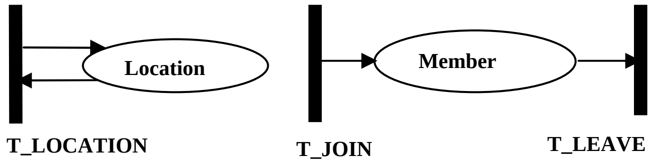


Location SPN Subnet: collect transient location information of all participating nodes

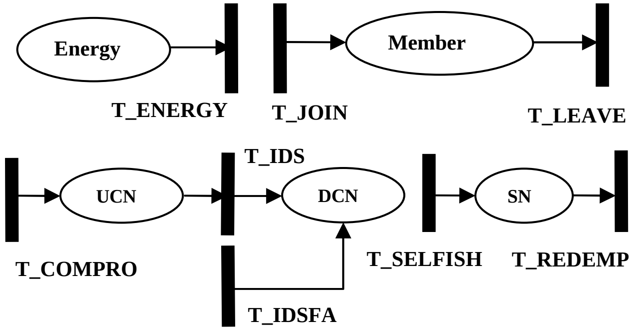
Node SPN Subnet: each node's information is collected through multiple *iterations*

Trust value calculation from the last iteration that has met convergence condition

Hierarchical Modeling Processes using SPNs.

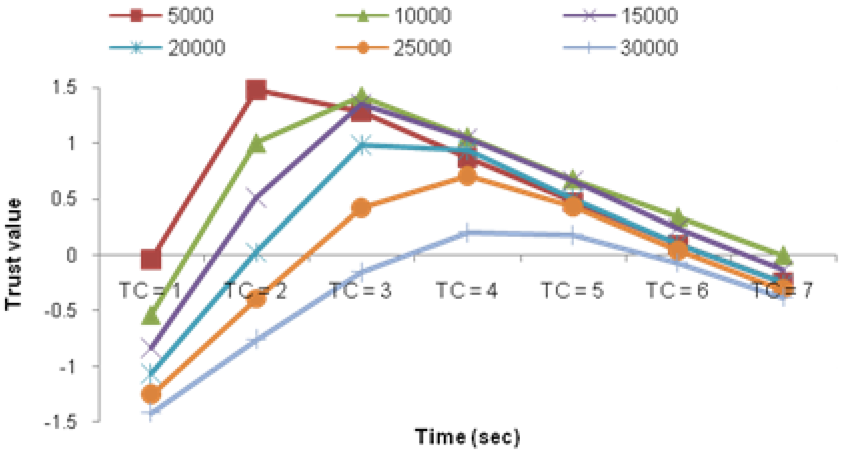


Location SPN Subnet.



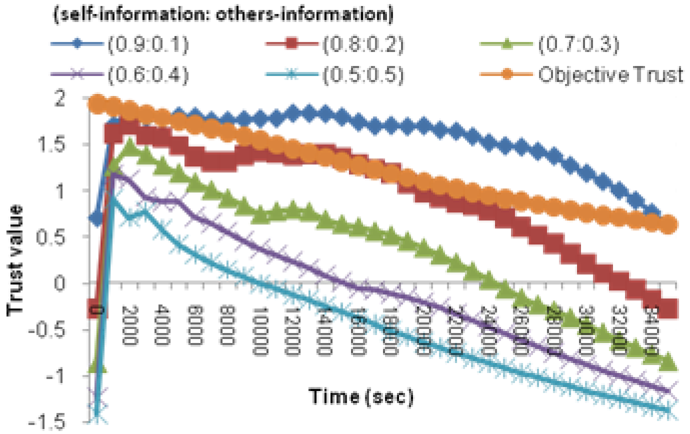
Node SPN Subnet.

- The goal is to identify the optimal length of a trust chain that maximizes trust level over time while meeting trust space requirements (e.g., # of nodes on a trust chain);
- Each node's trust level is maximized by using a different length of a trust chain over time in order to adapt to changing network environment and its own conditions.



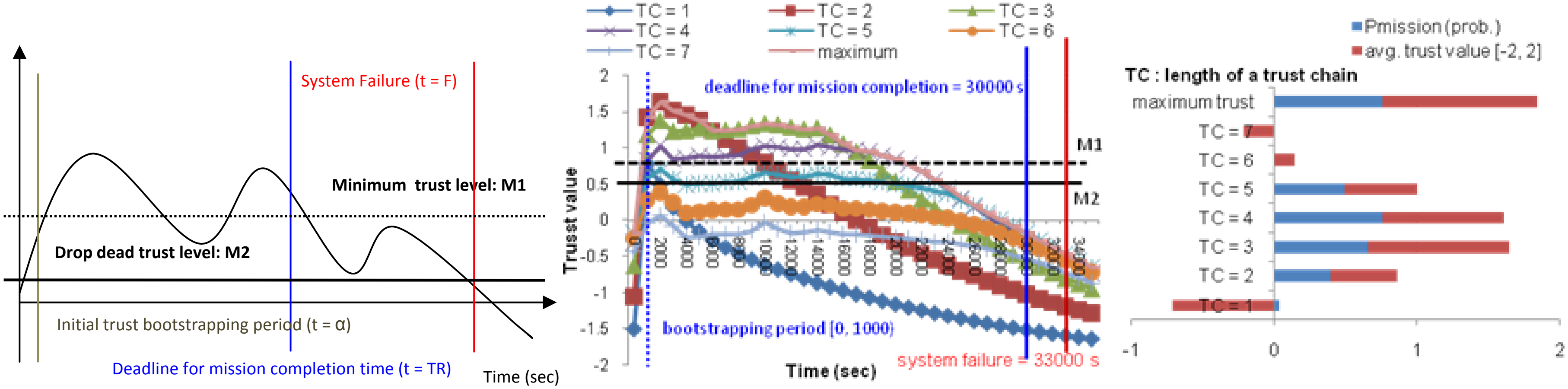
Average trust level versus the length of the trust chain at particular time points-all nodes' evaluation.

Case Study: Modeling and Analysis of Trust Management in MANETs (Cont.)



Average maximum trust level over time with respect to the various ratio of self-information and others-information (β 1: β 2)-all nodes' evaluation.

- High reliance on self-information for evaluating trust on a node may overestimate trust level compared to the predicted objective trust, introducing risk (e.g., a chance of deceit).
- Mission completion with high mission success probability (as a reliability metric) can be achieved by varying the length of a trust chain over time.



Mission success probability based on a required trust level.

Issues for Future Trust Management in MANETs

- Does the trust metric used reflect the unique properties of trust in MANETs ?
- What constituents does the trust metric have? Do the constituents change according to tasks given, changing network environments, or participating nodes’ conditions?
- How does the trust metric contribute to improving scalability, reconfigurability, and reliability of the proposed network?
- Does the proposed network design achieve adaptability to changing network conditions and MANETs environments?
- Does the proposed trust metric provide adequate tradeoffs ?
- Does the proposed network design identify optimal settings under various network and environmental conditions?

Questions?

Contact us at:

Jin-Hee Cho (jinhee.cho@us.army.mil), Army Research Laboratory

Ananthram Swami (aswami@arl.army.mil) , Army Research Laboratory