ICCRTS 2010
22-24 June 2010
Santa Monica, CA

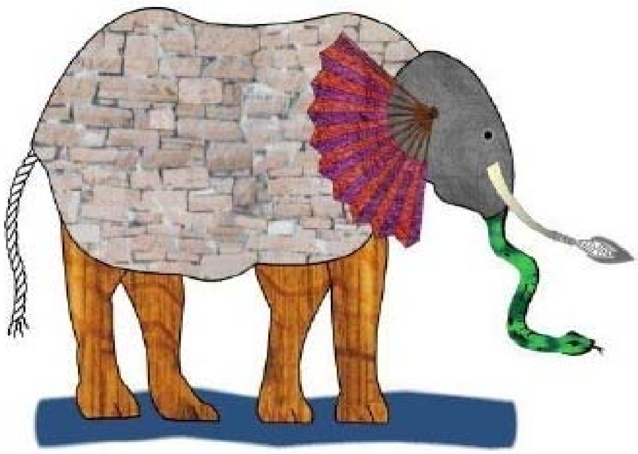
Mission-Dependent Trust Management in Heterogeneous Military Mobile Ad Hoc Networks

Jin-Hee Cho, Ananthram Swami, and Ing-Ray Chen

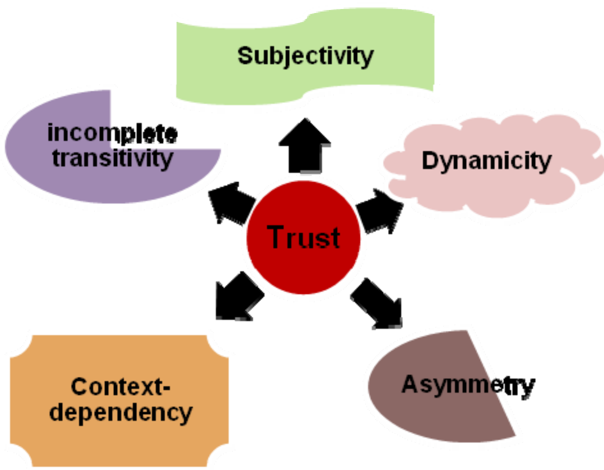
MANET Characteristics

- **Resource constraints**
  - ✓ energy, bandwidth, memory, computational power
- **High security vulnerability**
  - ✓ open medium
  - ✓ decentralized decision making and cooperation
  - ✓ prone to node capture and subversion
  - ✓ no clear line of defense
- **Dynamic:** dynamically changing network topology due to node mobility or failure, RF channel conditions
- **Models:** incomplete models; uncertain data

Trust Properties in MANETs



- **Trust**: the degree of a 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



- **Dynamic**, not static
- **Subjective**
- **Not necessarily transitive**
- **Asymmetric**, not necessarily reciprocal
- **Context-dependent**

Motivation & Goals

- **Motivation**
  - Managing trust in a tactical MANET is crucial for collaboration or cooperation for achieving military missions and system goals.
  - In heterogeneous MANETs, successful mission completion is significantly affected by how trustworthy mission team members are in terms of the required qualifications.
- **Goals**
  - “Can we trust this node to do mission X?”
  - Identify the best qualified team members to maximize the mission success probability given network environmental and operational conditions

Related Work

Context-aware TM

- Incorporate context-aware information for better trust accuracy
  - [Gray, 2002]
  - [Corradi, 2005]
  - [Toivonen, 2006]
  - [Billhardt, 2007]
  - [Uddin, 2008]
  - [Bertocco, 2008]

Resource allocations

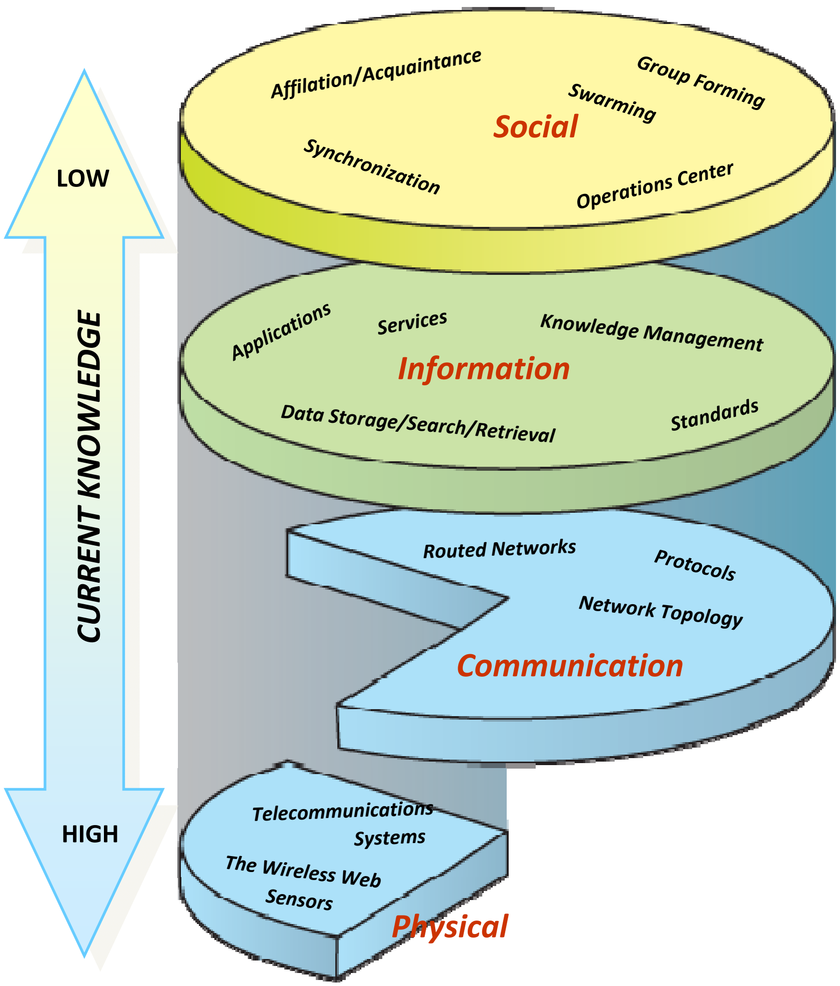
- Matching sensors with missions for resource optimization and successful mission completion
  - [Mainland, 2005]
  - [Wang, 2007]
  - [Preece, 2008]
  - [Rowaihy, 2008]
  - [Namuduri, 2009]

We propose a mission-dependent TM with a composite trust metric that dynamically identifies qualified mission members to meet context-dependent mission requirements for maximizing mission success probability.

Model and Assumptions

- **Assumptions**
  - Trust value is dynamically updated upon node mobility or failure
  - Trust decays as trust chain becomes longer
  - A node's bad behaviors based on both nature and environmental conditions
  - Trust value is dynamically adjusted based on a node's status
- **Parameterization**
  - Trust values between [0, 1]
  - The initial trust values are set to ignorance (can be relaxed)
- **Case Study**
  - Hexagonal network model
  - 4 different node types

Composite Trust Metric



Quality-of-Service (QoS) Trust

- Information on competence, dependability, reliability, successful experience, and reputation or recommendation representing "task" performance
- energy & cooperation

Social Trust

- Friendship, honesty, privacy, and social reputation or recommendation derived from direct or indirect interactions for "sociable" purpose.
- Betweenness, proximity (to a target mission area), and honesty

Computation of Trust Metric

$$T_{i,j}^{n-hop}(t) = P_{i,j}^{n-hop}(t)\left[\begin{array}{c}\beta_1\left(\frac{T_{i,j}^{n-hop,energy}(t) + T_{i,j}^{n-hop,cooperation}(t)}{2}\right) + \\ (1-\beta_1)\left(\frac{T_{i,j}^{n-hop,proximity}(t) + T_{i,j}^{n-hop,honesty}(t) + T_{i,j}^{n-hop,betweenness}(t)}{3}\right)\end{array}\right]$$

$$T_{i,j}^{n-hop,Z}(t) = \alpha T_{i,j}^{(n-1)-hop,Z}(t) + (1-\alpha)T_{i,j}^{n-hop,Z-indirect}(t)$$

- Trust components:
  - QoS trust with a weight β_1 for energy, cooperation
  - Social trust with a weight (1- β_1) for proximity, honesty, betweenness
- Trust information
  - Self-information with a weight α
  - Indirect information (recommendations) with a weight (1- α)
- As the length of a trust chain grows (weighted transitivity) , trust decays but there are more chance to find trust information

Computation of Trust Metric

$$T_{i,j}^{1-hop,Z}(t) = min\left[\frac{T_j^Z(t)}{T_i^Z(t)}, 1\right]$$

Subjectivity of trust concept

Incomplete transitivity of trust concept, trust decay over space

$$T_{i,j}^{1-hop,Z-indirect}(t) = \sum_{k \in K}\left[\left(\frac{T_{i,k}^{1-hop,Z}(t-\Delta)}{\sum_{k \in K} T_{i,k}^{1-hop,Z}(t-\Delta)}\right) T_{k,j}^{1-hop,Z}(t-\Delta)\right]$$

$$T_j^{proximity}(t) = \sum_{i \epsilon L}\left(P_j^{loc=i}(t)\frac{(D_{max}^{target} - D(i, L_{target}))}{D_{max}^{target}}\right)$$

$$T_j^{betweenness}(t) = \frac{\sum_{i \epsilon L} \sum_{h \epsilon M} \sum_{k \epsilon L}\left(P_j^{loc=i}(t) P_h^{loc=k}(t)\frac{(D_{max} - D(i,k))}{D_{max}}\right)}{|M|}$$

Computation of Mission Success Probability-Reliability

$$R(t) = \prod_{v=1}^{m} R_{NT_v}^{k-out-of-n}(t) \;\; where \; k = ceil(\frac{2}{3} * n)$$

$$R_{NT_v}^{k-out-of-n}(t) = \sum_{i=k}^{n} \binom{n}{k} \left(\overline{r_{NT_v}(t)}\right)^k \left(1 - \overline{r_{NT_v}(t)}\right)^{n-k}$$

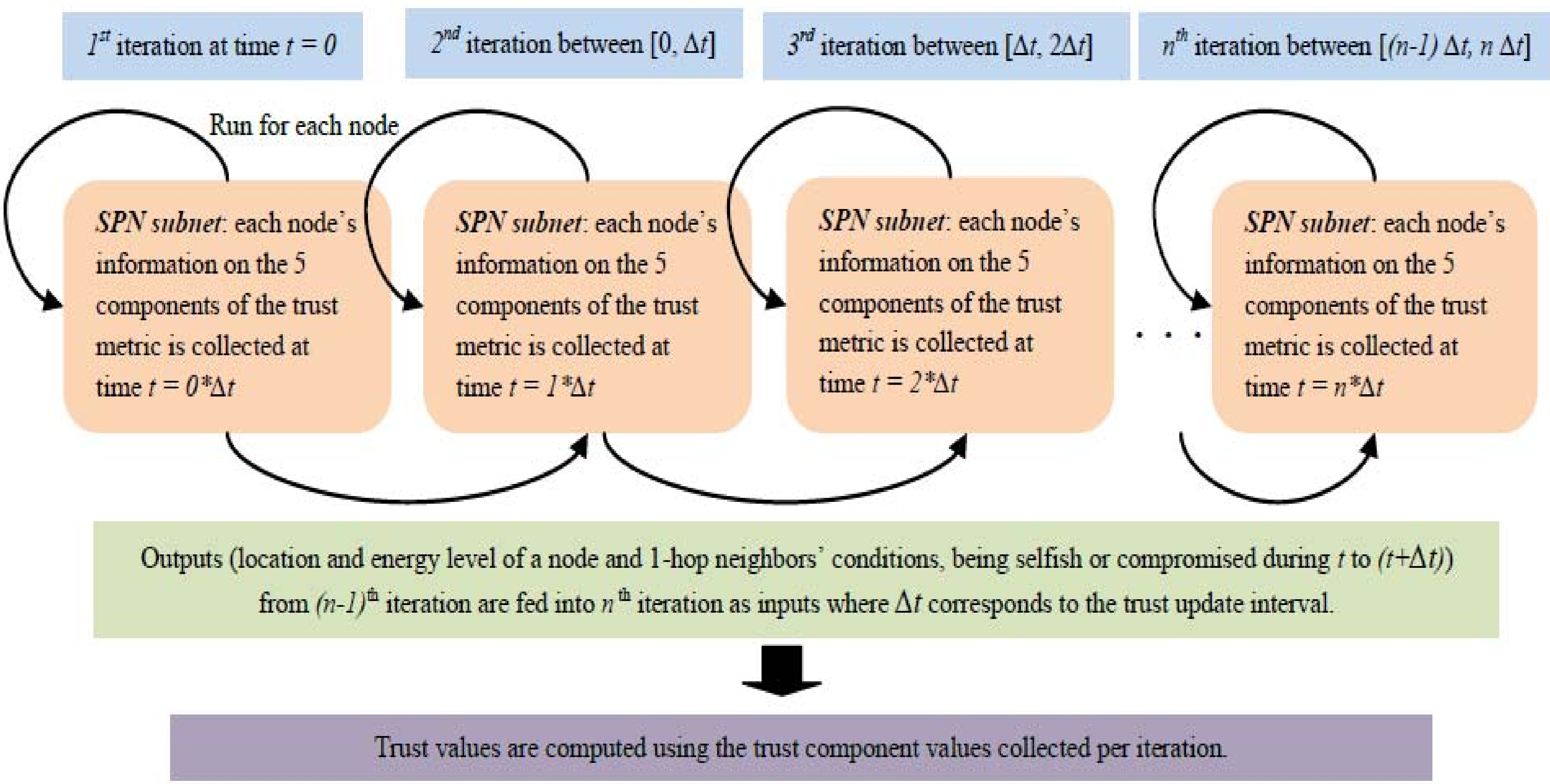
$$\overline{r_{NT_v}(t)} = \frac{\sum_{j \in G} r_{NT_v}^{j}(t)}{|G|}$$

$$r_{NT_v}^{j}(t) = \beta_2 \left(\frac{r_{NT_v}^{j-energy}(t) + r_{NT_v}^{j-cooperation}(t)}{2} \right) + (1-\beta_2)\left(\frac{r_{NT_v}^{j-proximity}(t) + r_{NT_v}^{j-honesty}(t) + r_{NT_v}^{j-betweenness}(t)}{3} \right)$$

$$r_{NT_v}^{j-Z}(t) = \begin{cases} 1 \; if \; T_{NT_v}^{j-Z}(t) \geq D_{NT_v}^{j-Z-1} \\ 0 \; if \; T_{NT_v}^{j-Z}(t) < D_{NT_v}^{j-Z-2} \\ T_{NT_v}^{j-Z}(t) / D_{NT_v}^{j-Z-1} \; if \; D_{NT_v}^{j-Z-2} \leq T_{NT_v}^{j-Z}(t) < D_{NT_v}^{j-Z-1} \end{cases}$$

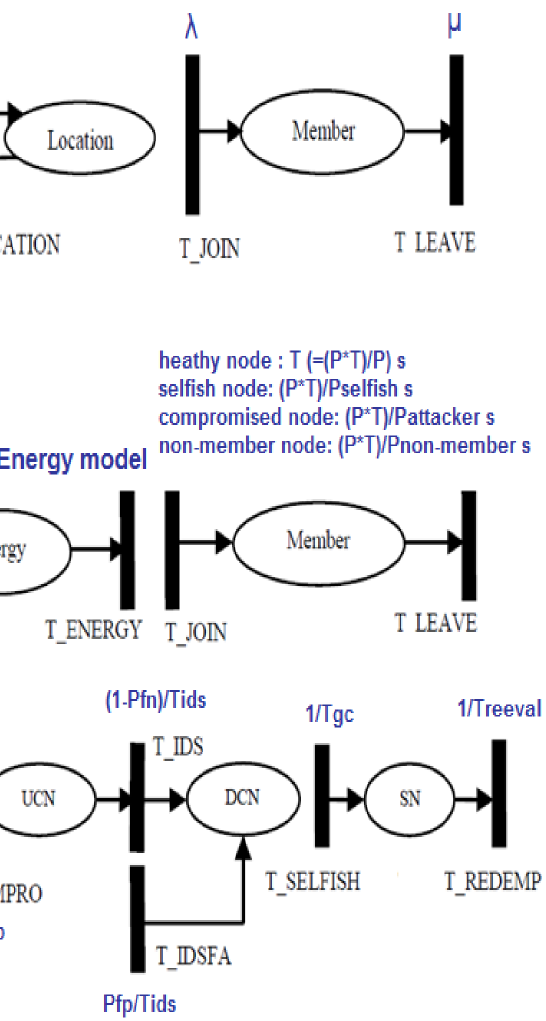
- *k-out-of-n* system meaning the system is functioning as far as k out of n components are operating properly
- Selection of k based on Byzantine Failure condition
- Model like a series system with *n* components
- β_2 is a parameter that represents mission requirements.

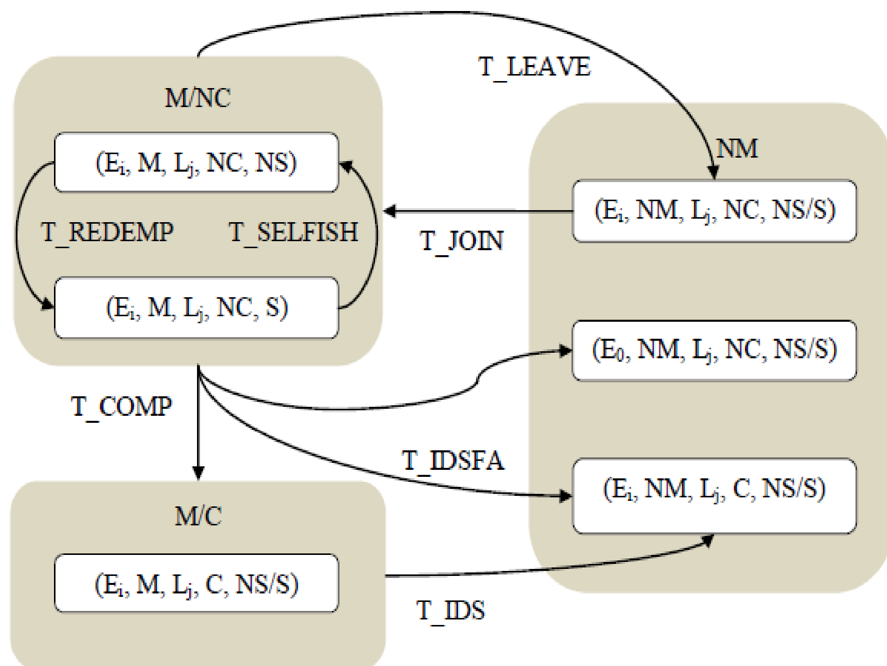
Performance Model



Hierarchical Modeling Processes using SPN Subnets.

Hierarchical SPNs





- E_i: energy level
- M or NM: member or nonmember
- L_j : location
- C or NC: compromised or not
- S or NS: selfish or not

Case Study – QoS trust mission

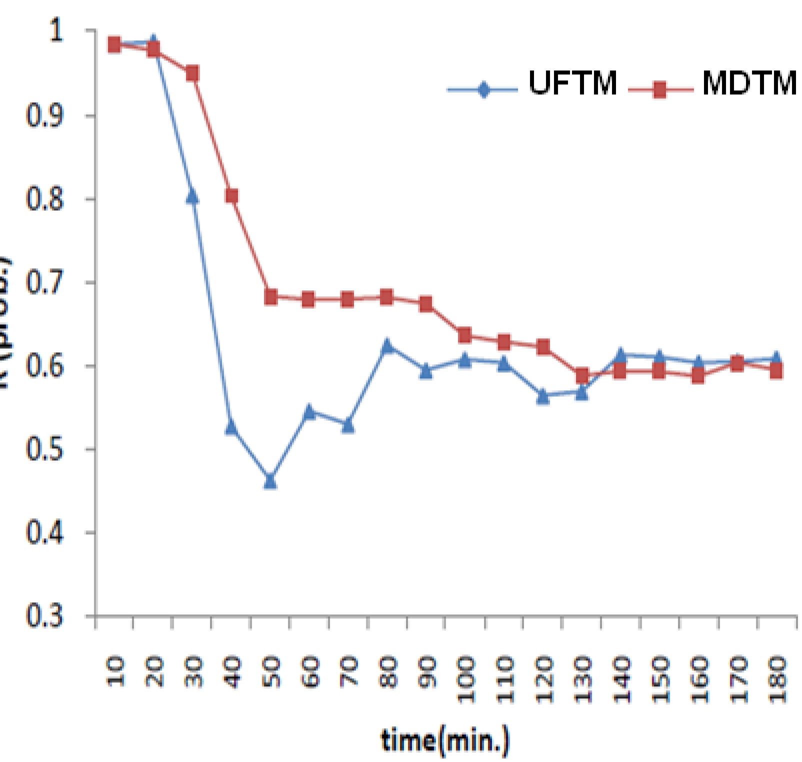
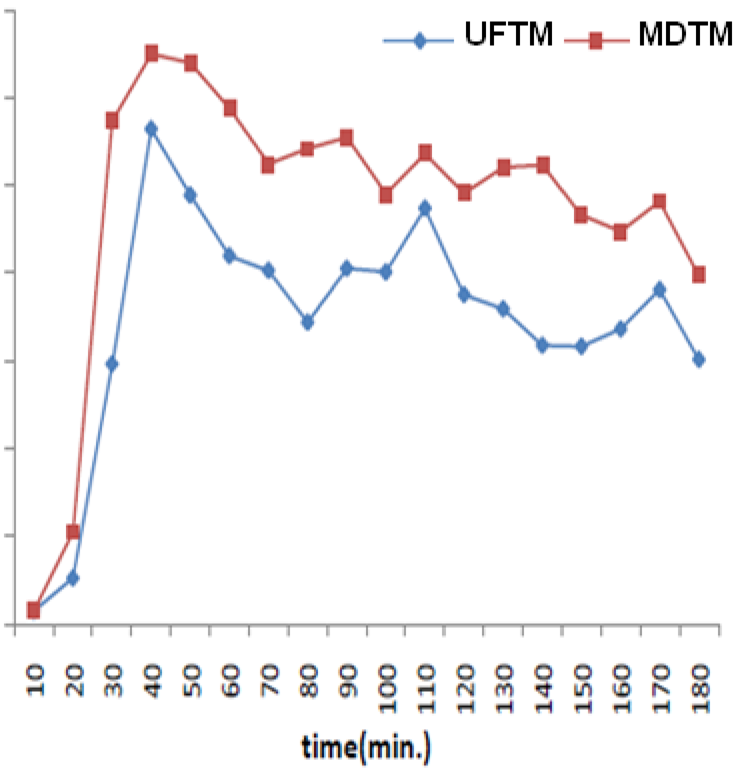


Figure 4: Trust-based Mission Success Probability under QoST mission.

QoS trust mission

- R: trust-based reliability
- UFTM: fixed/mission-independent TM
- MDTM: mission-dependent TM
- Overall: UFTM < MDTM
- t >130 min. : continuous selection of nodes with high QoS features causes lack of high QoS nodes when sufficient time has elapsed.

Case Study – Social trust mission

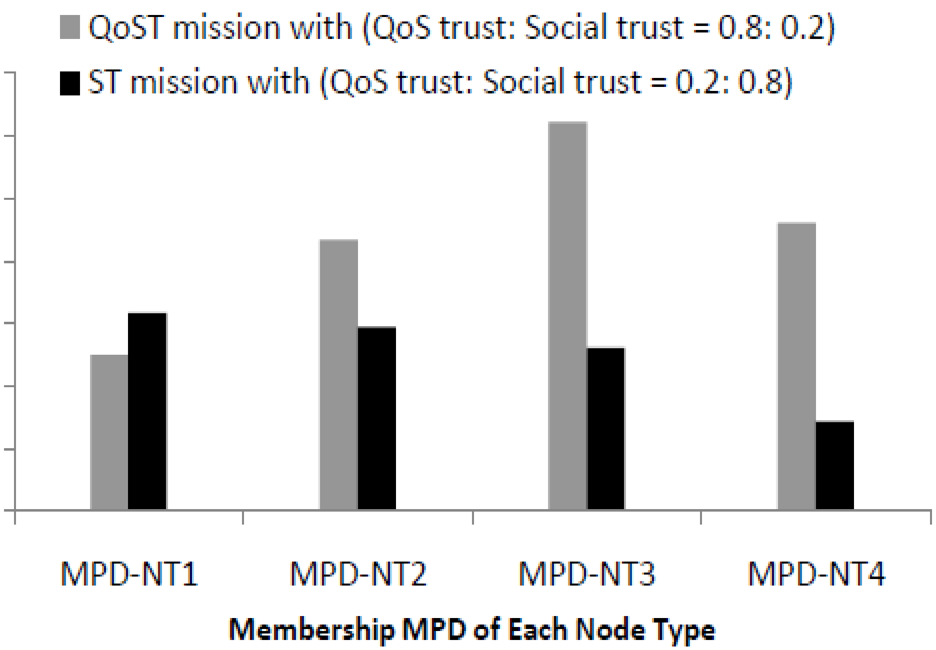


ure 5: Trust-based Mission Success Probability under ST mission.

Social trust mission

- R: trust-based reliability
- UFTM: fixed/mission-independent TM
- MDTM: mission-dependent TM
- Overall: UFTM < MDTM
- Social trust values are less likely to decrease over time compared to QoS trust

Case Study – Dynamic Membership



$$MPD_{membership-NT_v}^{|MD-UF|} = \frac{\sum_{i \in S} \frac{\sum_{k \in G} \left| M_{k,NT_v}^{iR-MD} - M_{k,NT_v}^{iR-UF} \right|}{|G|}}{|S|}$$

MPD based on the membership dynamics of MDTM and UFTM in each node type under QoST mission and ST mission.

More dynamic membership changes in QoST mission than ST mission

Note that a high MPD indicates high membership change.

Conclusion and Future Work

- **Summary**
  - Proposed a composite trust metric considering QoS trust and social trust
  - Developed a mathematical model using hierarchical modeling techniques of SPN to describe trust management for tactical heterogeneous MANETs
  - Mission-dependent TM outperforms unified TM in terms of predicted mission success probability as a reliability metric
- **Future Work**
  - Indentify a set of optimal weights considering operation and mission requirements
  - Model various mission scenarios
  - Consider other types of trust properties

Questions?

Jin-Hee Cho (jinhee.cho@us.army.mil)

Ananthram Swami (ananthram.swami@us.army.mil)

Computational and Information Sciences Directorate

Army Research Laboratory, Adelphi, MD

Ing-Ray Chen (irchen@vt.edu)

Department of Computer Science

Virginia Tech

Modeling of Selfishness and Dishonesty

enabling_T_SELFISH: $if(mark(energy) > 0 \;\&\&\; mark(member) > 0 \;\&\&\; mark(SN) == 0)$

$$\{\, if(N_{rand} \le P_{selfish})\; return\ 1;\;\; else\ return\ 0; \}$$

$$where\ N_{rand} = rand[0,1] * (mark(energy) + 1)/C_{selfish}$$

enabling_T_REDEMP: $if(mark(energy) > 0 \;\&\&\; mark(member) > 0 \;\&\&\; mark(SN) > 0)$

$$\{\, if(N_{rand} \le P_{selfish})\; return\ 0;\;\; else\ return\ 1; \}$$

$$where\ N_{rand} = rand[0,1] * (mark(energy) + 1)/C_{selfish}$$

enabling_T_COMPRO:

$$f(mark(energy) > 0 \;\&\&\; mark(UCN) == 0 \;\&\&\; mark(DCN) == 0 \;\&\&\; mark(member) > 0)$$

$$\{\, if(N_{rand} \le P_{dishonest})\; return\ 1;\;\; else\ return\ 0; \}$$

where $N_{rand} = rand[0,1] * (mark(energy) + 1)/C_{com}$

Considered inherent nature of a node’s behavioral trends as well as dynamic environmental condition such as low energy