Trust management issues for ad hoc and self-organized networks

Vassileios Tsetsos, Giannis F. Marias and Sarantis Paskalis

eSec / P-Comp / CNL Research Groups and Labs
Dept. of Informatics and Telecommunications, University of Athens

2nd IFIP International Workshop on Autonomic Communications WAC2005

4 October 2005
Athens, Greece

Presentation Structure

- **Introduction**
- Ad Hoc Trust Framework (ATF)
- Trust Issues in Autonomic Computing and Communications
- Conclusions

Self-organized networks

- MANETs
- Ad hoc collaborations
- No infrastructure available
- Many threats from selfish, malicious or hacker nodes
- Advanced needs for QoS and security
- Self-optimization principle promotes selfish behavior

Trust management

- A new paradigm for security and QoS solutions in open systems
- Key components:
  - recommendations exchange
  - reputation building/fading
- No central authorities
- Many different trust management schemes have been proposed

Motivation

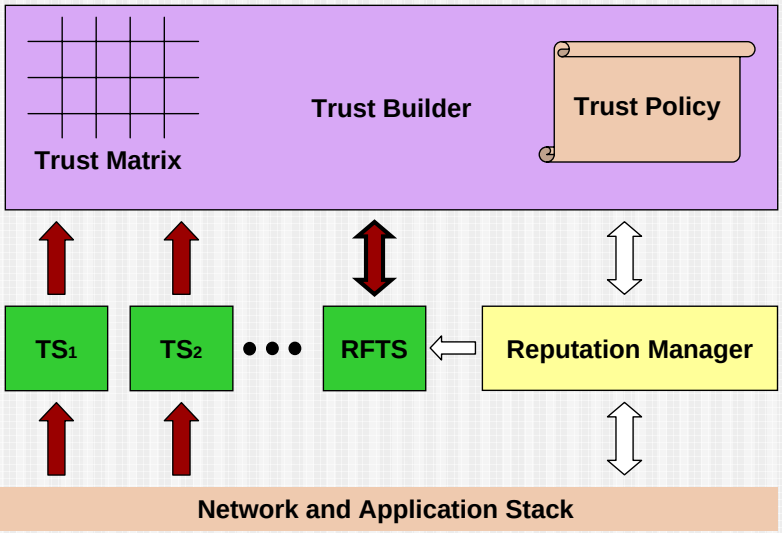
- Trust management schemes seem suitable for ACC
- Existing schemes proposed for MANETs are too specialized
- Those proposed for middleware services are too complex to apply
  - Belief networks, probabilistic methods
- A lightweight flexible framework is needed for assessing the trustworthiness of nodes

  → **ATF (Ad hoc Trust Framework)**

Presentation Structure

- Introduction
- **Ad Hoc Trust Framework (ATF)**
- Trust Issues in Autonomic Computing and Communications
- Conclusions

Overall Architecture



TS: Trust Sensor
RFTS: Recommendation Function TS

Trust Sensors

- Every node provides functions to other nodes
  - Packet forwarding, routing, naming services, ...
- Trust Sensors evaluate the quality of these functions in a node's neighborhood – i.e., capture the ***direct evidence***
  1. Observation of neighbors' behavior
  2. Comparison to reference/ideal behavior
  3. Quantification of the difference to Success/Failure

Reputation Manager

- On-demand recommendations exchange
- The nearest and most trustworthy recommenders are selected
- Recommendations are requested only when there **is no** sufficient direct evidences about a node
- Trusted paths are preferred

Trust Builder

- Main components:
  - Direct evidence (DE)
  - Recommendations (REC)
  - History of interactions
  - Subjective factor (SUB)
- The values for all open parameters are defined in the Trust Policy of each node
- Trust Values are assigned per (node, function) in a Trust Matrix

Trust Computation Model

$$Value_{n,f}(t) = w \cdot NewValue_{n,f} + (1-w)\left[\sum_{i=1}^{H} Value_{n,f}(t-i)\right] / H$$

$$\boxed{TV(n,f,t) \cong (a \cdot DE_{n,f} + b \cdot REC_{n,f}) \cdot SUB_{n,f}(t)}$$

$Value = DE \text{ or } REC$ $NewValue = last\ TS \text{ or } REC\ received$

$TV \in [0,1]$ $DE \in [0,1]$ $REC \in [0,1]$ $SUB \in [0,2]$

w and *H* are defined in Trust Policy so as to decrease the trust fluctuations without losing sensitivity

SUB

- SUB is a time function in the range [0,2]
- It allows for the introduction of subjective criteria in trust assessment
  - SUB=0 → distrust always
  - SUB=1 → use the default ATF trust policy
  - SUB=2 → be enthusiastic
- Ideally used for modeling more complex time-variant behaviors and trust strategies
  - *Example strategy: do not trust the function X of any node until there are W successful interactions*

ATF assessment

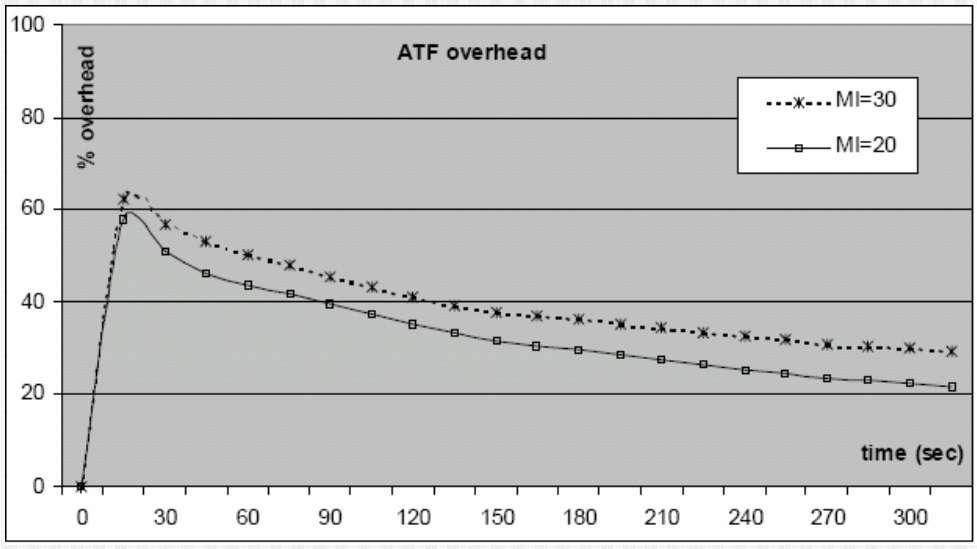
- J-Sim
- MANET / AODV routing
- Target: packet forwarding function (*f*)

Number of nodes	50
Number of selfish nodes	10
Maximum speed	2 m/sec
Pause Time	5sec
Terrain dimensions	300m x 300m
Communication Type	CBR
Source-Destination pairs	20
Data Packet Rate	4 pkts/sec
Radio transmission range	30m

- Communication overhead
- Accuracy
- Convergence rate

Simulations

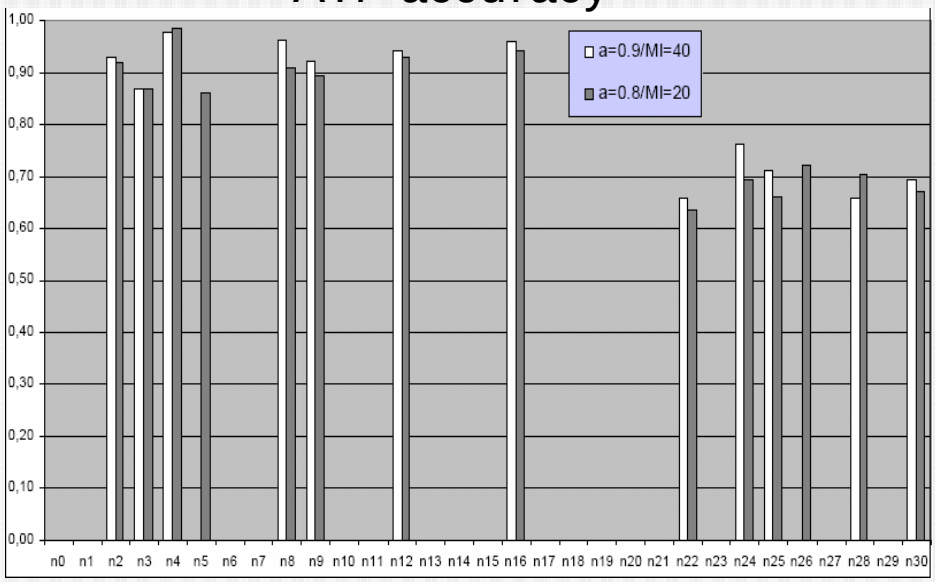
ATF overhead



MI = Minimum Interactions

Simulations

ATF accuracy

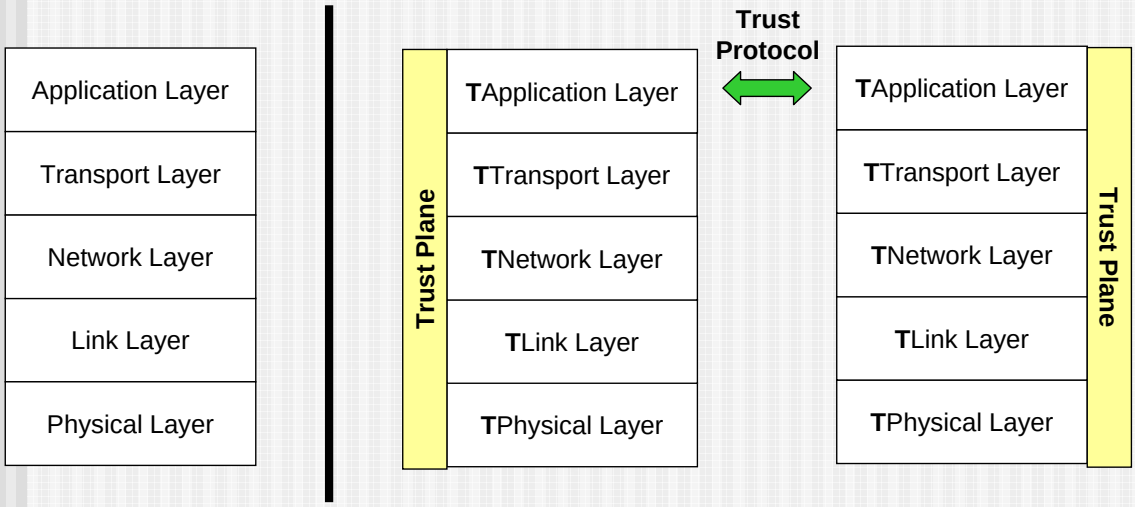


Selfish nodes n21-n30

Presentation Structure

- Introduction
- Ad Hoc Trust Framework (ATF)
- **Trust Issues in Autonomic Computing and Communications**
- Conclusions

Integration Issues (I)



Integration Issues (II)

Trust support in ACC systems requires:

1) Trust Plane
   - trust sensing, trust memory, trust brokering between layers
   - ~ *Knowledge Plane [D. Clark et al.]*
2) Trust Protocol
   - recommendations exchange
   - possibly in the application layer
3) Trust-aware protocols
   - trust-driven protocol **reconfigurability**
   - e.g., Software-defined radio

Interoperability

- Hard-standards
- Protocol-based
- SSL, RSVP,...
- Static protocol semantics
- Easy implementation
- Poor interoperability

- Soft-standards
- Ontology-based
- ???
- Dynamic protocol semantics
- Complex design
- High interoperability

Trust Semantics

- Numeric trust value ranges carry no semantics
  - e.g., $range_A(TV)=[0,1]$, $range_B(TV)=[1,12]$, $range_C(TV)=\{low, high\}$
  - How can systems A, B, C collaborate?
- *Solution: alignment of arbitrary trust ranges to reference trust model*
  - Alignment=assignment of semantics
  - Ontologies are perfect candidates for reference models

Trust Policies

- High-level policies is a key component of autonomic systems
  - distributed policies in hierarchical environments (e.g., grids, ad hoc nets)
- Semantic Web technologies used for rule- and logic-based policies
  - Definition and enforcement of TPs in ACCs
  - Precondition: already established well-defined semantics for trust itself

Conclusions

- ATF seems suitable for ACC
  - Not function-specific
  - Lightweight
  - Involves subjective criteria and policies
- First simulations are encouraging
  - Future work: more simulation scenarios
- Many “trust elements” are still missing
  - Trust semantics, protocol reconfigurability, …
- ACC research *should* explore the applicability of knowledge engineering and Semantic Web solutions

The end

Thank you for your attention!!!

Questions???