Distributed Trust Establishment and Computation in Mobile Ad-Hoc Networks

G. Theodorakopoulos, T. Jiang, P. Ramachandran, J. S. Baras

Motivation

“Lack of trust” in mobile ad-hoc networks
• No trusted centralized authority
• Rapidly changing topology and non-guaranteed connectivity due to mobility
• Vulnerability of links and identities because of wireless communication and open-air environment leads to
• Power-constrained devices with poor protection

Dynamic, distributed, self-organized, fault-resistant trust management model for MANET

Trust Establishment

Bootstrapping
When A makes a direct observation of B, A creates his own trust estimate $T_{ab}$.

Direct observations can be:
• Does User B forward A’s packets? (Watchdog)
• Has A visually identified B? (Mobility helps Security)
• Has A detected any misbehavior on B’s part? (Distributed IDS)

Propagation

• Short time, online distribution
• Proactive or reactive
• Peer-to-peer, self-organized and scalable
• Fast update and revocation

Combination

Along paths – concatenation functions
For path $A \rightarrow B \rightarrow C$, $T_{ac} = T_{ab} \otimes T_{bc}$

Across paths – aggregation function
For paths $A \rightarrow B_1 \rightarrow C$, $A \rightarrow B_2 \rightarrow C$, $T_{ac} = T_{a_1c} \oplus T_{a_2c}$

Trust Model

Physical Topology: graph $G_p = (V, E_p)$

$(i,j) \in E_p \iff i$ and $j$ are within range of each other

Trust Topology: directed graph $G_t = (V, E_t)$

$(i,j) \in E_t \iff i$ has belief on $j$: direct trust or trust by recommendation

Trust Vector: $T_i$

The $j$th component is the trust that node $i$ has for $j$.

Trust value is usually in $[0,1]$.
1 stands for complete trust
0 stands for complete distrust – Negative evidence
For more accurate modelling, trust value may not be scalar.

Example: a pair (Trust, Confidence), where Trust is as before and Confidence corresponds to how certain $i$ is for the Trust value $he$ has assigned.
Trade-off between accuracy and complexity.

Trust combination functions
Efficiently computable
Intuitive results
Difficult to manipulate

Current Work

Trust evidence distribution
Two schemes we have investigated: Freenet-based and swarm-intelligence-based

Trust path exploration
User A sends Trust-Query for destination D to his one hop neighbors. Neighbor $N_i$ picks “best” next hop $N_j$ and appends his trust value $T_{nj}$ to the Trust-Query and forwards it to $N_j$.

Trust routing
Next Trust-hop chosen according to the trust metric (analogous to routing and delay metric)

Distributed trust computation
Computation based on local information
Optimal decision theory:

\[ T_i = \frac{1}{k} \sum_{j=1}^{k} T_{ij} \]

Local and global effect:
Investigating Markov random field, Ising model
Energy function:

\[ E(T) = -\sum_{ij} J_{ij} T_i T_j \]

Dynamic trajectories and convergence behavior
Threshold parameters and phase transition properties

Emergent Patterns
Simple rules based on strictly local information lead to global trust patterns.
Effect of adversaries cannot spread.

Future Work

• Further evaluate different statistical detection and estimation methods
• Relate MRF with statistical estimation methods
• Investigate game theory and Ising model for convergence analysis of distributed inference
• Further mathematical analysis in swarm intelligence scheme in relation to MRF and simulating annealing (SA)
• Specify trust computation policies with respect to logic and formal methods
• Need to incorporate non-monotonic logic along with negative evidence, false evidence

Acknowledgement

This work is sponsored by U.S. Army Research Laboratory under cooperative agreement # DAAD19-01-2-0011