Distributed Trust Establishment and Computation in Mobile Ad-Hoc Networks

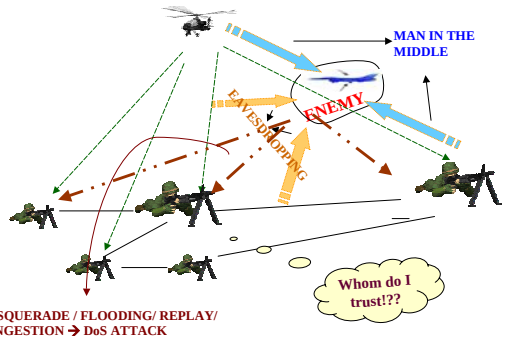
G. Theodorakopoulos, T. Jiang, P. Ramachandran, J. S. Baras

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→B→C, $T_{ac} = T_{ab} \otimes T_{bc}$ (e.g. multiplication, minimum value)

Across paths – aggregation function

For paths A→B1→C, A→B2→C,
$T_{ac} = T_{a1c} \oplus T_{a2c}$ (e.g. maximum value, summation, average, majority votes)

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_1 picks "best" next hop N_2, appends his trust value $T_{N_1 N_2}$ to the Trust-Query and forwards it to N_2.

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:

$\hat{T}_{ij} = E[T_{ij} \mid C_{ij}; R_{n_1 j}, C_{in_1}; \ldots R_{n_k j}, C_{in_k}]$, where T_{ij} is the trust value to be evaluated, C_{kl} is the direct observation of k on l, R_{kl} is the recommendation of l by k

Local and global effect:

Investigating Markov random field, Ising model

Energy function: $C(T) = \sum_{(i,j)} A_{ij} T_i T_j - B \sum_i T_i$

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.

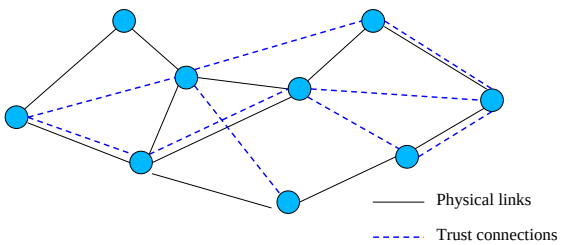
Trust Model

Physical Topology: graph $\boldsymbol{G_P}$=(V,E_P)

(i,j) ∈ E_P ⇔ i and j are within range of each other

Trust Topology: directed graph $\boldsymbol{G_T}$=(V,E_T)

(i,j) ∈ E_T ⇔ i has belief on j: direct trust or trust by recommendation



Trust Vector: $\boldsymbol{T}_i$

The jth 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.

e.g. a pair (Trust, Confidence), where Trust is as before and Confidence corresponds to how certain i is for the Trust value he has assigned.

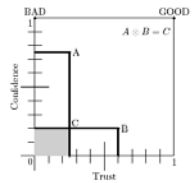
Trade-off between accuracy and complexity.

Trust combination functions

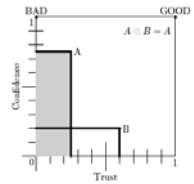
Efficiently computable

Intuitive results

Difficult to manipulate



Concatenation along paths



Aggregation across paths

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