A Trust Evaluation Framework in Distributed Networks

Hu Hao

Mar 31, 2015

NANYANG TECHNOLOGICAL UNIVERSITY

Reference:

1. Sun Y L, Han Z, Yu W, et al. A Trust Evaluation Framework in Distributed Networks: Vulnerability Analysis and Defense Against Attacks INFOCOM. 2006, 2006: 1-13.

NANYANG TECHNOLOGICAL UNIVERSITY

1. Trust Metrics
2. Fundamental axioms of trust
3. Trust models:
    a) entropy-based model
    b) Probability- based model
4. On-Off attack protection

Trust Metrics

Concept of trust:
The most appropriate interpretation of trust in computer networks is **belief**. One entity believes that the other entity will act in a certain way.

Notion of trust:
Trust is established between two parties for a specific action, in particular, one party trusts the other party to perform an action. The first party is referred to as *subject* and the second party as *agent*. We introduce the notation *{subject: agent, action}* to represent a trust relationship.

Trust Metrics

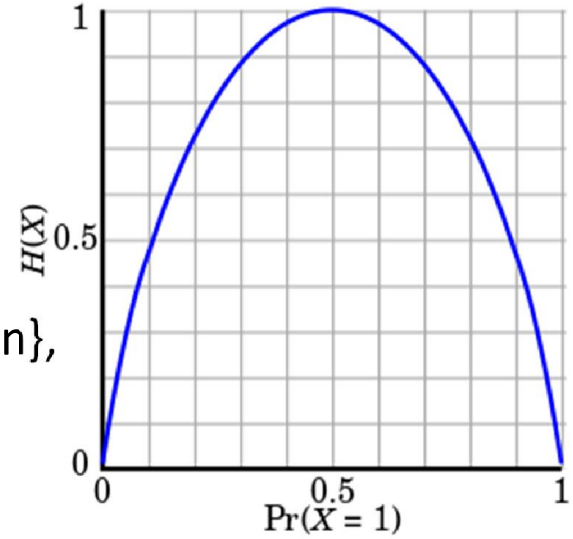
Given that the trust concept in computer networks is belief, how to quantitatively evaluate the level of trust? **Uncertainty in belief** is a measure of trust. Here are three special cases:

1. When the subject believes that the agent will perform the action for sure, the subject fully trusts the agent and there is no uncertainty.
2. When the subject believes that the agent will not perform the action for sure, the subject fully distrusts the agent and there is no uncertainty either.
3. When the subject has no idea about the agent at all, there is the maximum amount of uncertainty and the subject has no trust in the agent

Trust Metrics

How to measure the uncertainty? Information theory states that entropy is the nature measure of uncertainty! We would like to define a trust metric based on entropy. The metric gives trust value 1 in the first special case and -1 to the second special case, and 0 to the third special case.

$$T = \begin{Bmatrix} 1 - H(\mathrm{p}), for 0.5 \le \mathrm{p} \le 1; \\ H(p) - 1, for 0 \le p \le 0.5, \end{Bmatrix}$$



Where T=T{subject: agent, action}, p=P{subject, agent, action},

$$H(p) = -p \log_2(p) - (1-p) \log_2(1-p)$$

Binary entropy function

Necessary Conditions of Trust Propagation

Assume that A and B have established {A: B, $action_r$}, and B and C have established {B: C, *action*}. Then, {A : C, action} can be established if the following two conditions are satisfied:

1. $action_r$ is to make recommendation of other nodes about performing *action.*
2. The trust value of {A: B, $action_r$} is positive.

Fundamental Axioms of trust

Axiom 1: Concatenation propagation of trust does not in crease trust

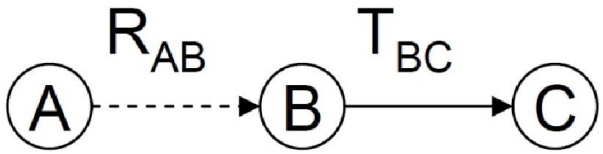


Fig. 3. Trust transit along a chain

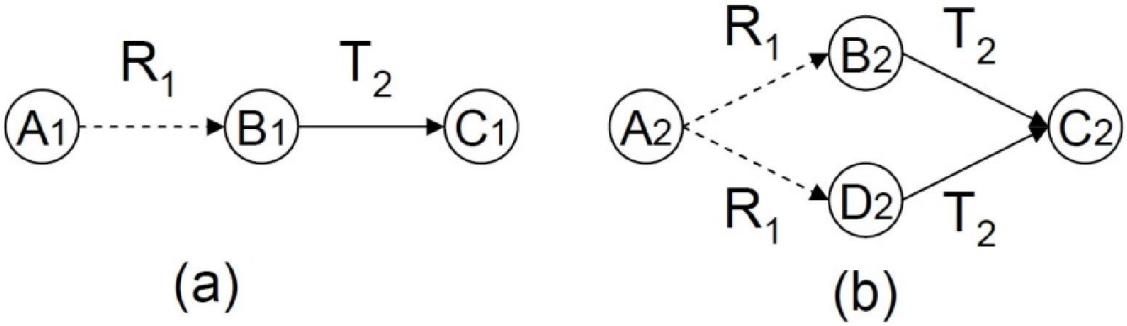
$$|T_{AC}| \leq \min(|R_{AB}|, |T_{BC}|),$$

where T_{AC}=T{A: C, $action$}, R_{AB}=T{A: B, $action_r$} and T_{BC}=T{B: C, $action$}

NANYANG TECHNOLOGICAL UNIVERSITY

Fundamental Axioms of trust

Axiom 2: Multiple propagation of trust does not reduce trust.

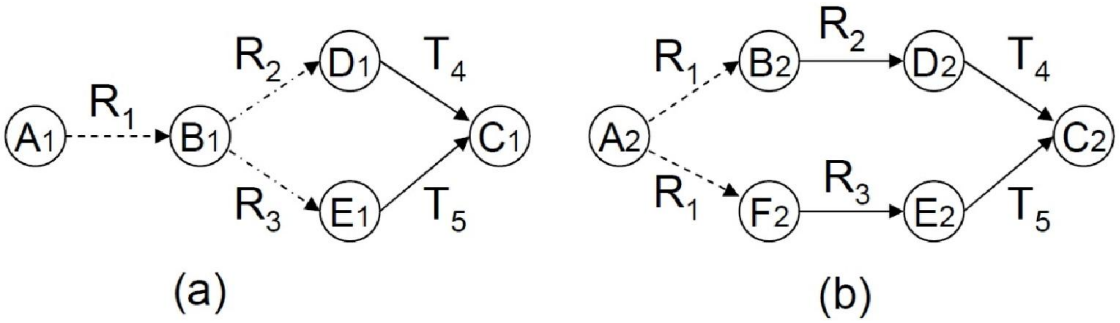


$$T_{A_2C_2} \geq T_{A_1C_1} \geq 0, if\ T_{A_2C_2} \geq 0;$$
$$T_{A_2C_2} \leq T_{A_1C_1} \leq 0, if\ T_{A_2C_2} < 0,$$

NANYANG TECHNOLOGICAL UNIVERSITY

Fundamental Axioms of trust

Axiom 3: Trust based on multiple recommendations from a single source should not be higher than that from independent sources



$$T_{A_2C_2} \geq T_{A_1C_1} \geq 0, if\ T_{A_2C_2} \geq 0;$$
$$T_{A_2C_2} \leq T_{A_1C_1} \leq 0, if\ T_{A_2C_2} < 0,$$

NANYANG TECHNOLOGICAL UNIVERSITY

Trust Models: Entropy-based model

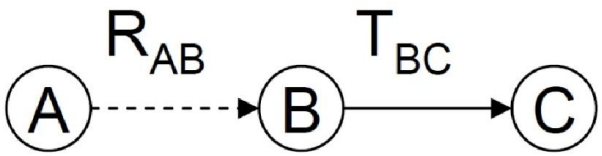


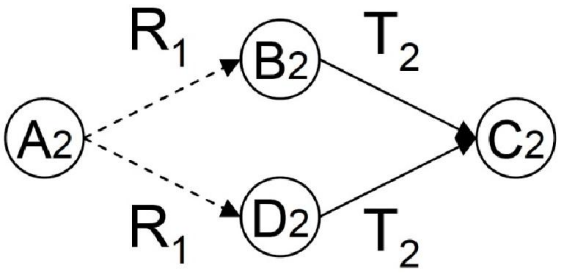
Fig. 3. Trust transit along a chain

We take the entropy function as the input, node B observes the behavior of node C and makes recommendation to node A as T_{BC}={ B: C, *action*}. Node A trust node B with R_{AB}=T{A: B, *making recommendation*}, one way to calculate $T_{ABC} = T\{A: C, action\}$ is

$$T_{ABC} = R_{AB} T_{BC}$$

NANYANG TECHNOLOGICAL UNIVERSITY

Trust Models: Entropy-based model



For multi-path trust propagation, let R_{AB}=T{A: B, *making recommendation*}, $T_{BC} = T\{B : C, action\}$, $R_{AD} = T\{A : D, making\ recommendation\}$, $T_{DC} = T\{D : C, action\}$. Thus A can establish trust to C through two paths: A-B-C and A-D-C. We can combine the trust established through different paths:

$$T\{A : C, action\} = \omega_1(R_{AB}T_{BC}) + \omega_2(R_{AD}T_{DC})$$

where

$$\omega_1 = \frac{R_{AB}}{R_{AB}+R_{AD}}\ ,\ \text{and}\ \ \omega_2 = \frac{R_{AD}}{R_{AB}+R_{AD}}$$

NANYANG TECHNOLOGICAL UNIVERSITY

Trust Models: Probability-based model

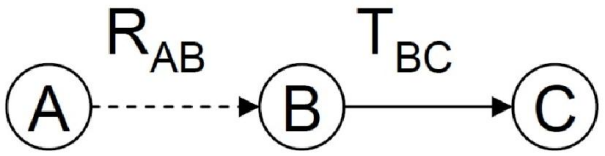


Fig. 3. Trust transit along a chain

Concatenation Propagation Model:

- Random variable P is the probability that C will perform the action. In A's opinion, the trust value T{A: C, action} is determined by E(p).
- Random variable X is binary. X=1 means that B provides honest recommendations. Otherwise, X=0.
- Random variable Θ is the probability that X=1, i.e. $P_r(X = 1|\Theta = \theta) = \theta$. In A's opinion, P{A: B, making recommendation}=$p_{AB} = E(\theta)$

How to calculate E(p)?

NANYANG TECHNOLOGICAL UNIVERSITY

On-Off attack protection

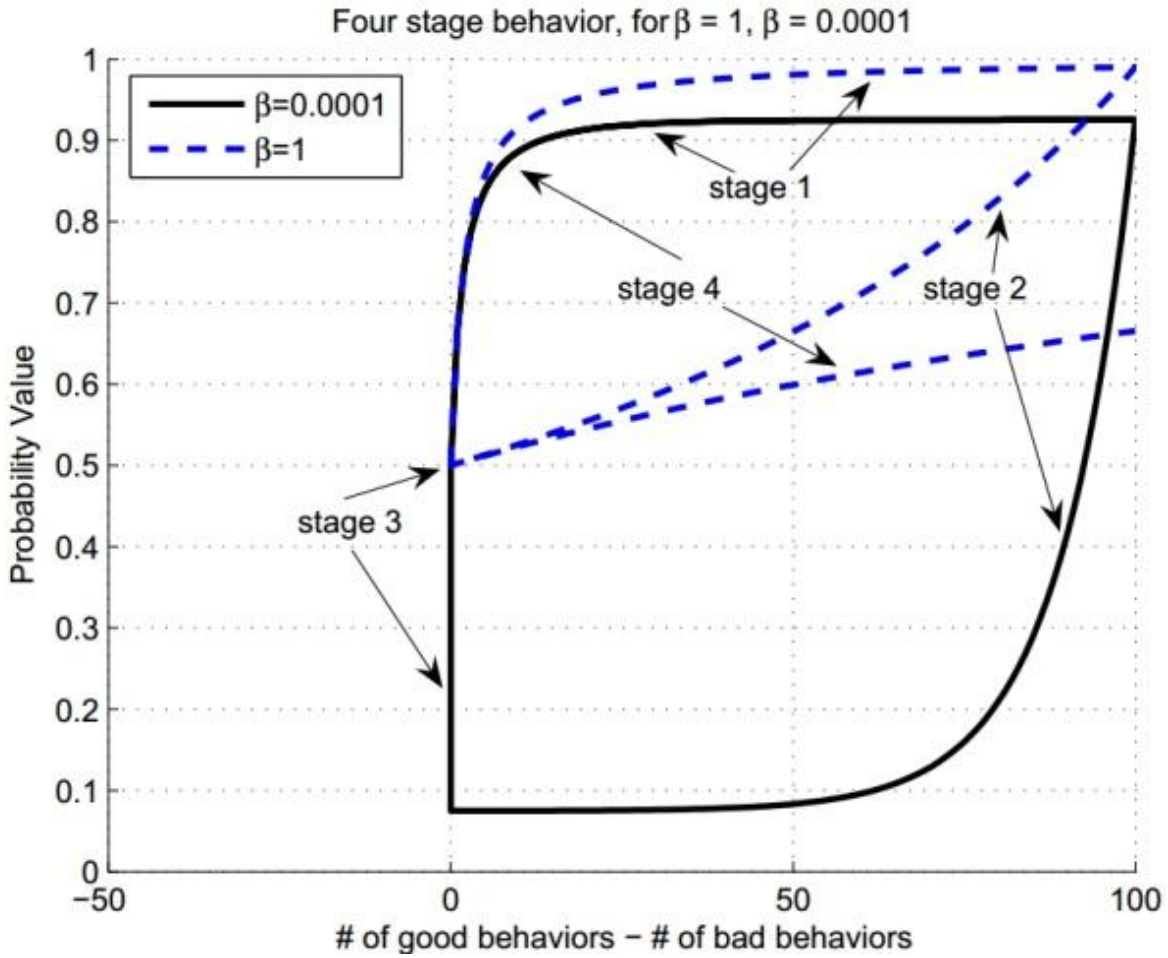
On-off attack means that malicious entities behave well and badly alternatively, hoping that they can remain undetected while causing damage.

Forgetting factor:

Performing K good actions at time t_1 is equivalent to performing $K\beta^{t_2-t_1}$ good actions at time t_2, where β ($0<\beta<1$) is referred to as the forgetting factor

On-Off attack protection

Stage 1: first behaves well for 100 times
Stage 2: then behaves badly for 100 times
Stage 3: then stops doing anything for a while
Stage 4: repeat stage 1.



Probability value:

$$\frac{S+1}{S+F+2}$$

Where S is the number of good behaviors and F is the number of bad behaviors

NANYANG TECHNOLOGICAL UNIVERSITY

On-Off attack protection

To defend against the on-off attack, we propose a scheme that is inspired by a social phenomenon – while it takes long-time interaction and consistent good behaviors to build up a good reputation, only a few bad actions can ruin it.

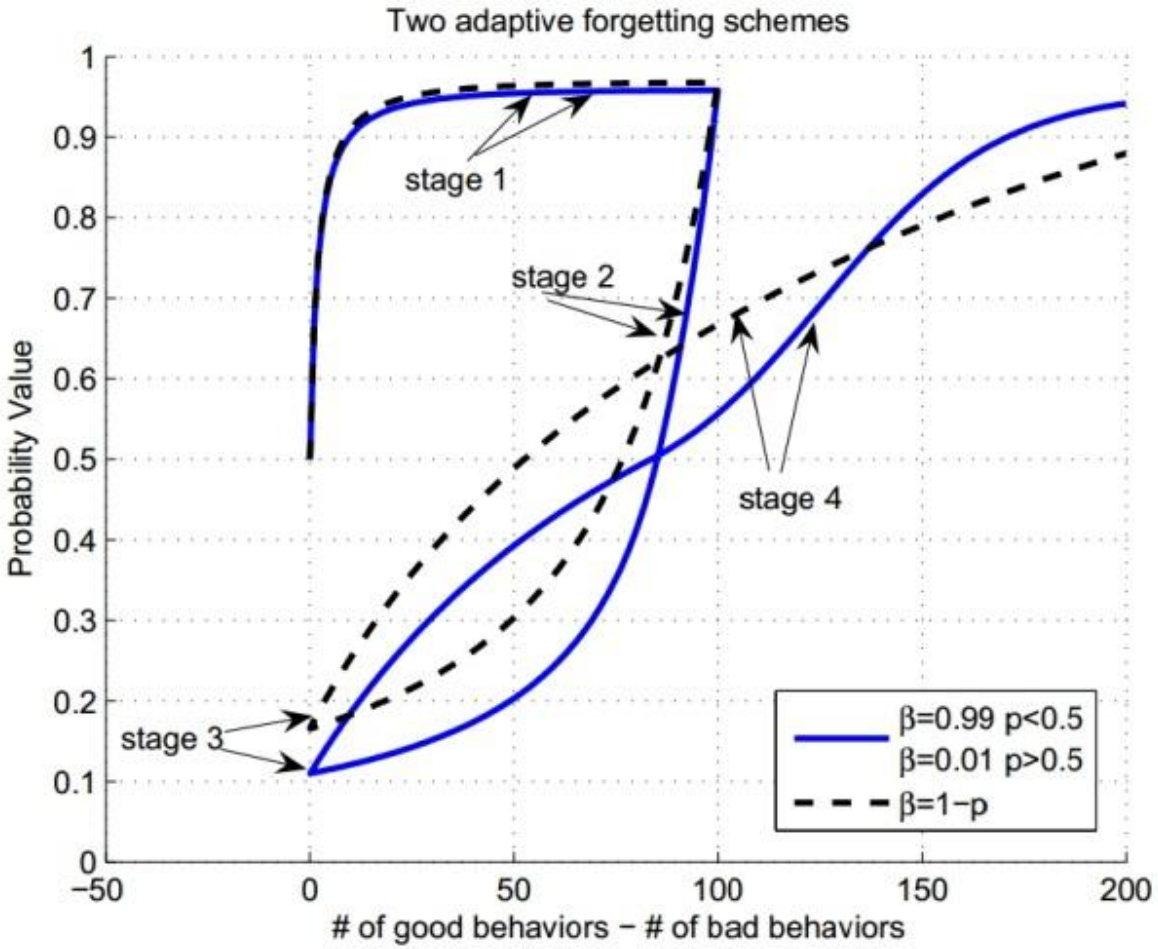
好事不出门，坏事传千里

Adaptive forgetting scheme

On-Off attack protection

We can choose
$\beta = 1 - p$ or,

β=β_1 for $p \geq 0.5$; and β=β_2 for $p < 0.5$ where $0 < \beta_1 \leq \beta_2 \leq 1$.



In this example:

β_1=0.01
β_2=0.99

NANYANG TECHNOLOGICAL UNIVERSITY

Thank you!

NANYANG
TECHNOLOGICAL
UNIVERSITY