Trust-Aware Failure Detector

In Multi-Agent Systems

Xinyu Zhou, David M. Nicol

Introduction

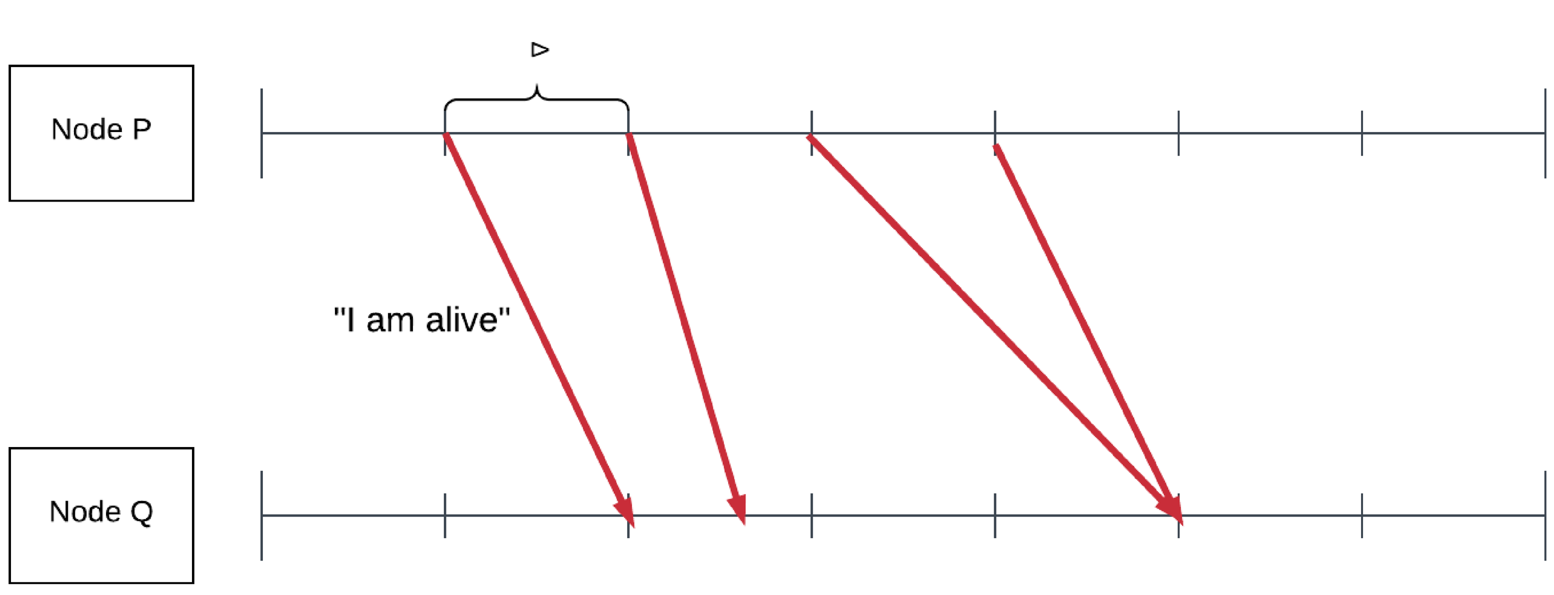
The notion of failure detector(FD) is firstly introduced by Chandra and Toueg to solve the consensus problem. However, most FD implementations consider that all the nodes as equally trustworthy which will limit the performance of the failure detection in dynamic network environment.

With **partial synchronous model** and **crashing failure pattern**, our work proposes a new failure detector implementation incorporated with the trust update model, we interpret the trust as the **belief** that the targeted node has not crashed. The trust value derived can provide more information and allow more flexible strategy in the failure detection.

Heartbeat Strategy

The Node P sends an "I am alive" heartbeat message to other nodes every Δ time.

- If a node Q does not receive the heartbeat signal after the expiration of a time out, it will raise the suspicious by reducing the belief that node P is still alive.
- Meanwhile, node Q can regain the belief after receiving the "I am alive" message.
- Every message is composed of two components: the index of the message i and the time τ_i that the message is transmitted.



Basic Probability Assignment

- Let $\theta = \{c, \neg c\}$ be the frame of discernment, where c represents the event that node P has crashed.
- Basic probability assignment (BPA) m: $2^{\theta} \rightarrow [0,1]$, which measures the belief that is committed exactly to $A \subset \theta$, satisfies:

  1)$m(\emptyset) = 0$ 2)$\Sigma_{A\subset\theta} m(A) = 1$

Assumption: The lifetime of the nodes L follows the exponential distribution with parameter λ.

$$P(L \le t) = 1 - e^{-\lambda t}$$

Then we have:

$$P_{t,\tau_i} = P(Node\ P\ alive\ at\ t | message\ with\ \tau_i\ received) = P(L > t | L > \tau_i) = e^{-\lambda(t-\tau_i)}$$

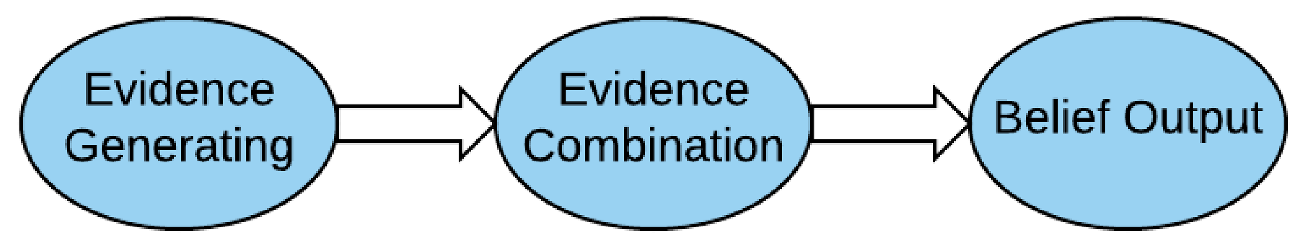
The derivation of the basic probability assignment based on P_{t,τ_i}

$$m(c, \neg c) = H_b(P_{t,\tau_i}) = -P_{t,\tau_i}\log(P_{t,\tau_i}) - (1 - P_{t,\tau_i})\log(1 - P_{t,\tau_i})$$

$$m(c) = (1 - m(c, \neg c))(1 - P_{t,\tau_i}) \qquad m(\neg c) = (1 - m(c, \neg c))P_{t,\tau_i}$$

The value $m(c, \neg c)$ can be interpreted as the uncertainty of node Q because of the lack of evidence.

Evidence Based Trust Update Model

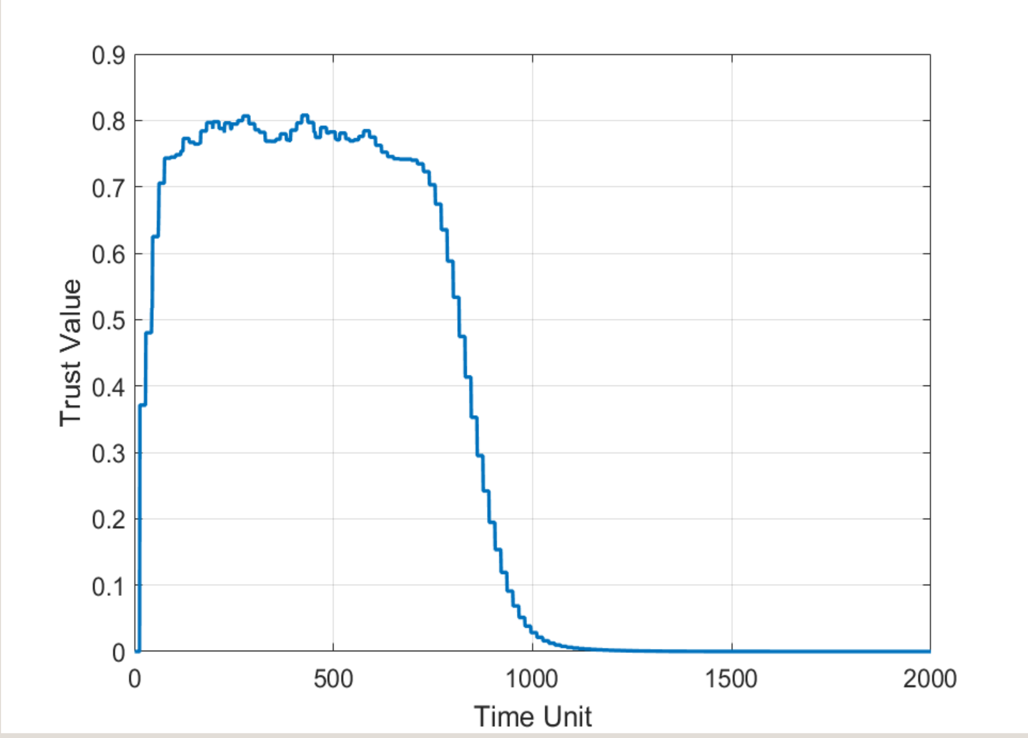


- Node Q generates new evidence in the following two cases
  - One heartbeat message is received by Q
  - Q has waited for over Δ time without receiving any further messages, and the evidence is regenerated every Δ time.
- The evidences are combined by the Yager's modified Dempster's rule
  - $q(A) = \Sigma_{B\cap C=A}\, m(B)m_e(C)$ where m_e represents the BPA of the new coming evidence.
  - $m_u(A) = q(A)$ for $A = c\ or\ \neg c$
  - $m_u(\{c, \neg c\}) = q(\{c, \neg c\}) + q(\emptyset)$ where m_u is the updated BPA for P.
- The belief function that node P is still alive can be characterized as:

$$Bel(\neg c) = \Sigma_{A\subset\{\neg c\}} m(A) = m(\neg c)$$

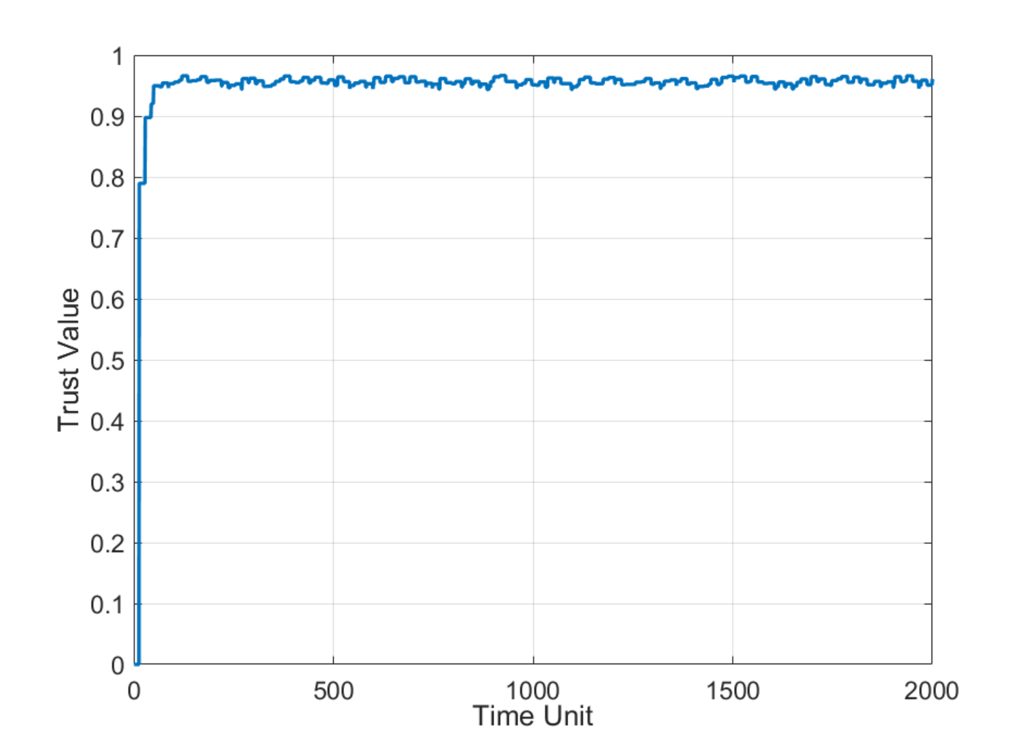
Simulations On the Trust Update Process

Crashed Case:



- $\lambda = 1/200 \quad \Delta = 15$
- Crashed time=552
- Latency∈ [30,50]
- The trust value quickly rises to 0.7 within 150 time units.
- The value starts stepping down at 150 time units after the node crashes.

Uncrashed Case:



- $\lambda = 1/1000 \quad \Delta = 15$
- Latency∈ [30,50]
- The trust value rises to 0.9 within 100 time units.
- The value remains higher than 0.9 as long as the node is alive.

Conclusion and Future Work

Our work incorporates the trust update model into the implementation of the failure detector. The incorporation is realized by the heartbeat strategy as well as the Yager's rule of the evidence combination. We show that the trust-aware detector can achieve great accuracy and is responsive to the failure of the targeted node.

In the future work, we will introduce the cooperation among the nodes to evaluate the targeted nodes' state(alive or crashed). Moreover, we will investigate the trust prorogation scheme in the failure detection algorithm.

SCIENCE OF SECURITY
VIRTUAL ORGANIZATION
Funded by the National Security Agency.

INFORMATION TRUST INSTITUTE