Trust Modeling and Verification using Colored Petri Nets

Amir Jalaly Bidgoly
Behrouz Tork Ladani
Department of Computer Engineering
University of Isfahan

Agenda

- Introduction & Motivation
- A Conceptual Model
- Formalism
- Trust Colored Petri net Model
- Case Study
- Conclusion & Future works

9/6/2011

2

INTRODUCTION & MOTIVATION

3

TRUST

- Trust is a well-known social behavior.
- It occurs between two entities;
  - a trustor who believes that the trustee's expected behavior occurs and is willing to take a risk for that belief.
- Many of modern systems and applications are interested in trust.
  - web applications
  - wireless networks
  - grid computing application
  - …

4

TRUST (CONT.)

- Trust Measurement
  - how to represent the value of trust between two nodes
- Trust Management
  - tries to find a way to make decision based on trust values

9/6/2011

5

TRUST MODELING

- So far, the only known method for modeling and verification of trust is **application specific simulation**.
  - User is forced to develop or have a specific tool for every application type.
  - there is no way to compare different methods.
- If Trust can be modeled by an standard formalism:
  - It may be simulated using standard simulation.
  - It may be checked using standard model checkers.

9/6/2011

6

A Conceptual Model of Trust

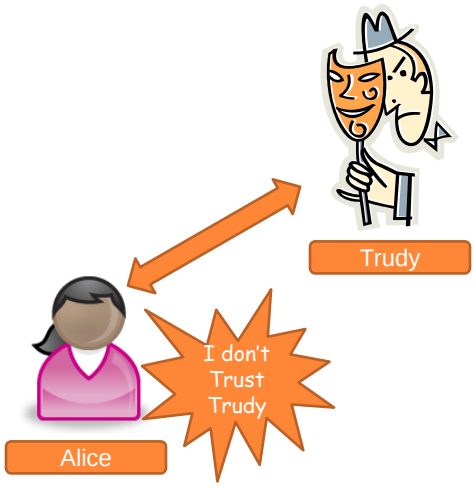
A Scenario

Trudy

Alice

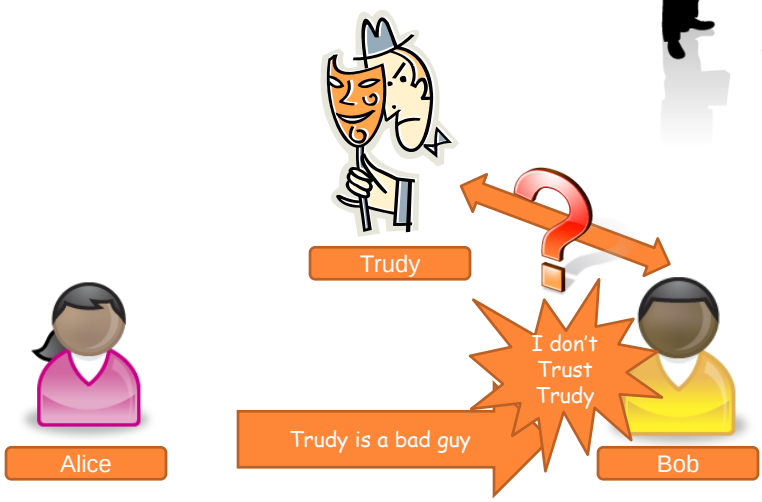
Bob

Direct Experiment



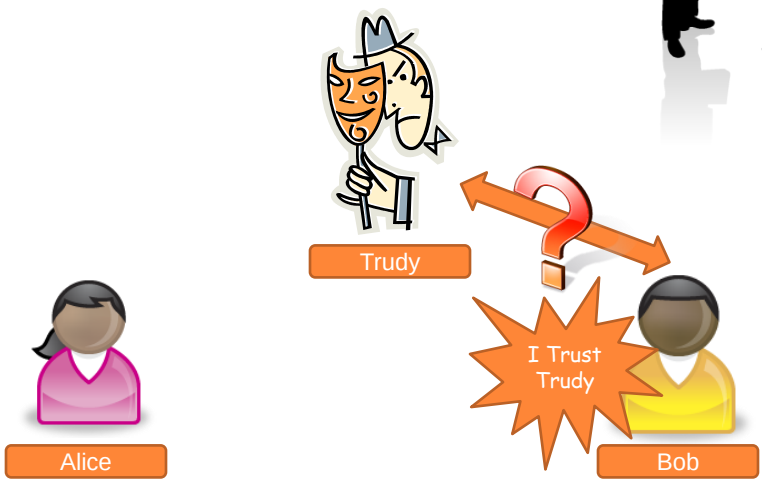
9/6/2011

Indirect Experiment



9/6/2011

Indirect Experiment



Attacks

- Trudy tries to be keeping herself as a trusted node using misleading actions or reputations.
  - She intends to execute her malicious plan whenever she deceives others.
- Every proposed model for trust must be able to model these attacks and also verify system against them.

ATTACKS (CONT.)

- On-Off Attack
- Location-depend Attack
- Bad mouthing Attack
- Selective misbehavior
- Sybil Attack
- Newcomer Attack

13

SOME DEFINITIONS

- "Node":
  - Refers to each entity of the society.
    - A person in the society
    - A sensor in a wireless sensor network.
- "Action"
  - Perform a direct experiment
    - having a social manner
    - passing information over the network
- "Recommendation"
  - Perform an indirect experiment (i.e. reputation)

14

Some Definitions (cont.)

9/6/2011

- The value of trust is just changed over the time as the discrete-event system.
  - The context of the environment is constant.
- Changes are performed by
  - Action Event
    - Trudy has acted something bad which makes Alice to do not trust Trudy anymore.
  - Recommendation Event
    - Alice might recommend to Bob about Trudy.

Action Events

9/6/2011

- can be change the trust state of system.
  - may be bad or good
- In a real world usually there is no absolute good action or bad action.
  - Peoples may have small mistake or a big mistake.
- The model must difference between small and big misbehavior.
- So every action must have a weight which show the rate of its trueness.
  - w = 1: completely true
  - w = 0: completely false
  - w = 0.9: a good action with some mistake (e.g. 18 out of 20)

An example: Do her homework

9/6/2011

Action Events (cont.)

9/6/2011

- In children's story,
  - bad peoples always do bad actions.
  - heroes always do the best.
- In a real environment,
  - No hero, no complete black person.
  - no absolute good node or bad node.
- A real person may have good actions or bad actions.
  - Alice is a good person however she will sometimes naughty.
  - Trudy may sometimes act good to deceive others.

Probability of action event

- **Probability of the action event**: An Action
  - May occur with the probability of ρ
  - may not occur with the probability of $(1-\rho)$.
- Some Cases
  - $\rho = 0$: never occur
  - $\rho = 1$: surely occur
  - $\rho = 0.9$: a person might do the action with the probability of 0.9 and might do not it with probability of 0.1.

Recommendation Event

- A node x says the reputation of node y in its own viewpoint to node z.
- There are two types of nodes:
  - Truthful
    - Say the truth
  - Liar
    - Say lie
- The liar node tries to mislead others using absolute false information.
  - In the real world an absolute liar will be discovered soon.
  - malicious nodes try to hide their lies between truths.

Recommendation Event (cont.)

- Malicious nodes try to hide their lies between truths:
  - Trudy may sometimes say lie and sometimes say right
    - Like on off attack
  - Trudy does not say an absolute lie. She says truth but just change some minor part of it.
    - Trudy changed it a little toward her malicious goals.

9/6/2011

21

Recommendation Event (cont.)

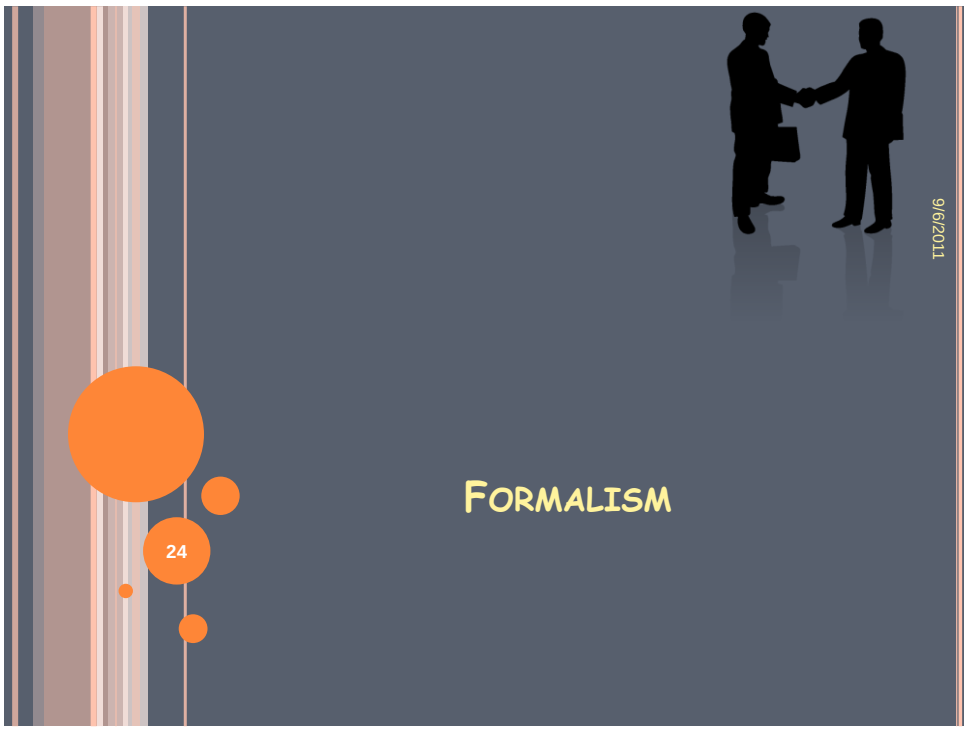
- So every recommendation event has a
  - **Veracity**: level of trueness which shows how false it is.
    - E.g. modeling bad mouthing -like attacks
  - **Probability:** which shows how often it occurs.
    - E.g. Rumor, overstate, understate.

9/6/2011

22

Rumor

23



Formalism

24

Definitions

- **Definition 1**: An action event means one node (e.g. *x*) does something for another node (e.g. *y*) which has a specified value called weight and may be happened with the probability of *p*.
- **Definition 2**: A recommendation event means one node (e.g. *x*) says its opinion about other nodes (e.g. *z*) to third node (e.g. *y*). It may be happened with the probability of *p* and has a veracity level.

9/6/2011

25

Modeling Trust

- Trust values
- Peoples/Nodes
- Recommendation
- Action

9/6/2011

26

Modeling Trust

- The model is independent of how trust is measured and used.
- Each state of the model contains just trust values between each two unique pair of nodes which is named *trust matrix*.
- **Definition 3**: The *trust matrix* (displayed by *Trust*) is a matrix which its rows and columns are nodes identity and its cells contain the corresponding trust values. *trust(x,y)* represents the trust value of node *x* to node *y*.

9/6/2011

27

Formal Definition

- Our trust model consists of:

$$(S, I, \alpha, \rho, T_\alpha, T_\rho)$$

- S is the set of People/Nodes.
- I is an initial trust matrix.
- Alpha is the transition function for Action.
- Rho is the transition function for Recommendation.
- T-alpha update trust considering an action.
- T-rho update trust with regards of a recommendation.

9/6/2011

28

Initial Trust matrix

- Initial Trust shows that how people trust each others in the beginning of simulation/verification.

$$I : S \times S \rightarrow Trust$$

- Initial Trust usually could be filled by:

$$a, b \in S, a \neq b$$

$$I(a,a) = \max trust$$

$$I(a,b) = \min trust$$

29

Action events

- Alpha presents the Action events.
  - X does something for Y.

$$\alpha : S \times S \rightarrow 2^{Weight \times P}$$

$$x, y \in S, \alpha(x, y) = \{(w_1, p_1), (w_2, p_2), \ldots (w_n, p_n)\}$$

- It is allowed to have more than one action event between two nodes

30

Recommendation Events

- Rho represents the recommendation transition function.
  - X recommends to Y

$$\rho : S \times S \rightarrow 2^{Veracity \times P}$$

$$x, y \in S, \rho(x, y) = \{(v_1, p_1), (v_2, p_2), \ldots (v_n, p_n)\}$$

- It is allowed to have more than one recommendation event between two nodes

31

T-Alpha

- T-Alpha is a function which is used after any action to update trusts.

$$T_\alpha : Trust \times Weight \rightarrow Trust$$

- It's a part of Trust Measurement system that should be evaluated.
- The simpler mode:

$$T_\alpha : trust(x, y) \times Weight \rightarrow trust(x, y)$$

32

T-RHO

- T-Rho is a function which is used after any recommendation to update trusts.

$$T_\rho : Trust \times Veracity \rightarrow Trust$$

- It's a of part Trust Measurement system that should be evaluated.
- The simpler mode:

$$T_\rho : trust(y,z) \times trust(y,x) \times$$

$$trust(x,z) \times Veracity \rightarrow trust(y,z)$$

9/6/2011

33

TRUST CPN MODEL OR TCPN

9/6/2011

34

CPN Model

- Each CPN Model Consists of:
  - ∑: Color set
  - **P**: Place
  - **T**: Transitions
  - **A**: Arcs
  - **C**: Color Function
  - **G**: Guard Functions
  - **E**: Arc Inscription
  - **I**: Initialization Function

35

Limits of CPN

- CPN does not allow to have color set of real number.
- All value must be Integer.

$$Trust, Weight, Veracity \in \mathrm{I}$$

$$\min trust = 0, \max trust = 100, \min trust \le Trust \le \max trust$$

$$0 \le Weight \le 100$$

$$0 \le Veracity \le 100$$

- Weight = 100 Best Action, Weight = 0 Worst Action
- Veracity = 0 Absolute lie, Veracity = 100 Truth

36

SIMPLICITY

9/6/2011

- all action and recommendation events have the same probability to occur.
  - *p* which is definition is not necessary.
- this change is not required
  - CPN has a well implementation of stochastic event
  - For simplicity
- One may ignore this and continue for modeling without any lose.

$$\alpha : S \times S \rightarrow 2^{Weight}$$

$$\rho : S \times S \rightarrow 2^{Veracity}$$

TYPES: COLOR SET

9/6/2011

- Trust : int with 0..100;
- Weight : int with 0..100;
- Veracity : int with 0..100;
- TrustToken : list trust with |S|..|S|;
  - **Definition 4**: A *trust vector* is a row of trust matrix that keeps only trust values of a specific node to other ones.
- Σ={Trust, Weight, Veracity, TrustToken}

PLACES

- Any People/Node is modeled by a colored place.
- P=S

39

COLOR FUNCTION

- Define the type of each place:

$$\forall p \in P, C(p) = TrustToken$$

40

Initialization Function

- Initial Marking of Place p:

$$\forall p \in P, s \in S \perp s \equiv p \Rightarrow I(p) = \bigcup_{x \in S} I(s, x)$$

41

Transitions

- There are two types of event
  - Action transition.
  - Recommendation transition.

42

TRANSITIONS - ACTIONS

9/6/2011

- Alpha function: For each w in $\alpha(x,y)$ we add a transition between Place X and Y:
  - Transition is always enabled.
  - Transition does not change the marking of X.
  - The TrustToken of Y is replaced with a new marking with the regards of action w.

$$Tr'_{yx} = T_{\alpha}(Tr_{yx}, w) \wedge Same(Tr / Tr_{yx})$$

TRANSITIONS - ACTIONS

9/6/2011

- Rho function: for each v in $\rho(x,y)$ we add a transition between Place X and Y:
  - Transition is always enabled.
  - Transition does change the marking of X.
  - The TrustToken of Y is replaced with a new marking with the regards of V.

$$\bigcup_{z \in S, z \neq x, z \neq y} Tr'_{yz} = T_{\rho}(Tr_{yz}, Tr_{yx}, Tr_{xz}, v)$$
$$\wedge same(Tr_{yx}) \wedge same(Tr_{yy})$$

Case Study

45

A simple Story

Shangool

Mangool

Wolf

46

Our Trust Model

- S={shangool, mangool, wolf}

I	Shangool	Mangool	Wolf
Shangool	100	30	0
Mangool	50	100	0
Wolf	0	0	100
α	Shangool	Mangool	Wolf
Shangool		50..80	30..60
Mangool	40..70		40..70
Wolf	100	100	
ρ	Shangool	Mangool	Wolf
Shangool		80..90	40..70
Mangool	50..80		50..80
Wolf	20..50	20..50	

9/6/2011

47

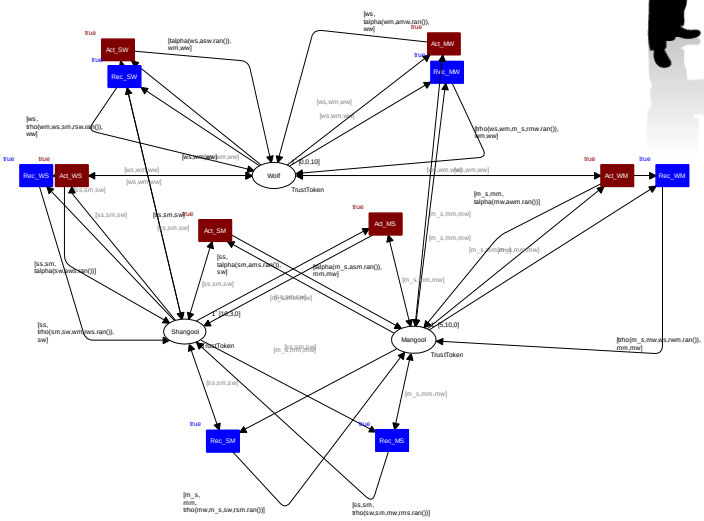
Our Trust Model: Simple Trust Measurement

- T-Alpha:
  - [trust*4+weight]/5
- T-Rho
  - [ta*(100-tb)+tc*tb*v]/100

9/6/2011

48

Our CPN Model



9/6/2011

49

Results

Trust	Shangool	Mangool	Wolf
Shangool		48	90
Mangool	51		91
Wolf	45	55	

9/6/2011

50

Making Legend

I	Shangool	Mangool	Wolf
Shangool	100	30	0
Mangool	50	100	0
Wolf	0	0	100
α	Shangool	Mangool	Wolf
Shangool		50..80	
Mangool	40..70		
Wolf			
ρ	Shangool	Mangool	Wolf
Shangool		80..90	
Mangool	0..100		
Wolf			

9/6/2011

51

Results

Trust	Shangool	Mangool	Wolf
Shangool		54	21
Mangool	60		17
Wolf			

9/6/2011

52

Conclusion & Future Works

Summary

- In this paper, we have proposed a model for evaluation of Trust based on Colored Petri Nets.
- In the proposed model, each node do an action with a weight as its degree of trueness.
- Also each node could recommend each other again by a factor of veracity called v.
- Model is capable of either simulation or model checking.

Future Work

- Proposed method is unable to model some attacks;
  - On-off attacks
    - Need to include time [easy in Petri nets]
  - Absolute Badmouthing Attack:
    - Always say false, In our model a node may lie but the lie is not always false.
    - T-Alpha and T-Rho should be changed to
      - PxP->Trust

9/6/2011

55

Selected Refrences

- S. Ruohomaa and L. Kutvonen, "Trust Management Survey," Lecture Notes in Computer Science (LNCS), vol. 3477, Springer-Verlag, 2005, pp. 77-92.
- Z. Malik and A. Bouguettaya, "Reputation Bootstrap-ping for Trust Establishment among Web Services," IEEE Internet Computing, vol. 13, no. 1, 2009, pp. 40–47.
- T. Eymann, S. Konig, and R. Matros, "A Framework for Trust and Reputation in Grid Environments," J. Grid Computing, vol. 6, no. 3, 2008, pp. 225–237.
- L. Rasmusson and S. Janson, "Simulated social control for secure Internet commerce," In New Security Paradigms '96, ACM Press, Sept 1996.
- A. Abdul-Rahman and S. Hailes, "A Distributed Trust Model," in Proceedings of the ACM New Security Paradigms Workshop, 1997, pp 47-60.

9/6/2011

56

SELECTED REFRENCES

- A. Josang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," Journal of Decision Support Systems, vol. 43, no. 2, 2007, pp. 618-644.
- M. Reith, J. Niu, and W.H. Winsborough, "Apply model checking to security analysis in trust management," in Data Engineering Workshop, 2007 IEEE 23rd International Conference on, 2007, pp. 734-743.
- H. Wu, C. Shi, H. Chen and C. Gao, "A Trust Management Model for P2P File Sharing System," International Conference on Multimedia and Ubiquitous Engineering (mue 2008), 2008, pp.41-44.
- J. Huang, and D. Nicol, "A Formal-Semantics-Based Calculus of Trust," IEEE Internet Computing, vol. 14, no. 5, 2010, pp. 38-46.

9/6/2011

57

Thanks
Any Question?

9/6/2011

58