Formalizing Trust in Mobile Wireless Networks

Yan Sun

Department of Electrical and Computer Engineering
University of Rhode Island

Trust in Computer Networks

- **Trust**
  - A well studied concept in sociology and psychology.
  - known as the driving force for collaboration in social communities.
- **Distributed computer networks**

  for example, ad hoc networks, sensor networks, and the future Internet
  - Rely on collaboration among network participants.
- **Trust in distributed computer networks**
  - When network participants do not know how to trust each other, network operations suffer.
  - Participants that naively trust will be victimized.
  - Mistrustful participants will ignore opportunities and their resources will be wasted because of inefficiency.

The Role of Trust (I)

Prediction and Diagnosis

When a network entity establishes trust in other network entities, it can *predict* others' future behaviors and *diagnose* their security properties.

- Assistance in decision-making to improve security and robustness.
- Adaptation to risk, leading to flexible security solutions.
- Misbehavior detection.
- Quantitative assessment on system-level security properties.

The Role of Trust (II)

Simplification and Abstraction

- The design of many network protocols and applications must consider the possibility that some participants will not follow the protocols honestly.
- **Currently**, this issue is considered by individual protocols or applications
  - repetitive monitoring and high complexity
- **Ideally**, trust information is provided by an infrastructure managed by the network
  - network protocols/applications can simply integrate trust values into their design.
  - the bar for integrating security concerns into regular protocols will be greatly lowered.

The Role of Trust (III)

Integrating Social Needs into System Design

"The most vexing security problems today are not just failures of technology, but result from the interaction between human behavior and technology" – GENI Reports

- Stimulate cooperation -- there is an incentive for users to build high reputation/trust values.
- Improve end-user security -- human users can make better decisions to protect themselves against potential risks.
- advance the understanding in human users' acceptance of new service or systems.

Trust-based Solutions do not …

- replace traditional security services, such as data integrity, confidentiality, authentication, etc.

Outline

- Trust Evaluation Foundation

What is Trust?

How to quantitatively evaluate trustworthiness?

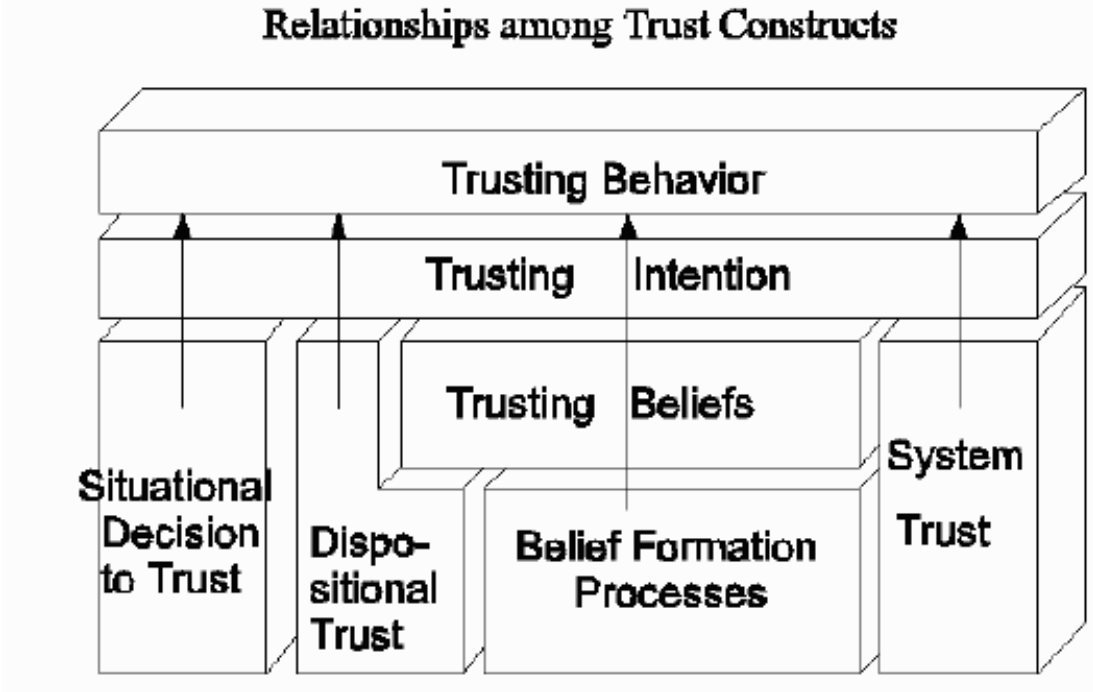
Is trust evaluation vulnerable to attacks?

- Trust Concept
- Trust Metrics
  - Quantitative
  - Physical meaning
- Trust Models
  - Fundamental rules for trust propagation
- Attacks and Protection

- Trust management system and its applications in Mobile Ad hoc networks.

- Trust Concept
- Trust Metric
- Trust Models
- Attack and Protection
- Trust evaluation system

Trust Concept in Social Networks



After examining trust definition in **60** research articles and books, Dr. McKnight and Dr. Chervany identified six representative trust constructs.

UNIVERSITY OF Rhode Island

Trust Concept in Computer Networks

Our understanding of trust in computer networks:

- *The most appropriate interpretation of trust in computer networks is* **belief**.

  One entity believes that the other entity will act in a certain way, or believes that the network will operate in a certain way.

Notation of Trust relationship:

{subject : agent, action}

The subject trusts the agent to perform an action.

Trust Metrics

In the literature

Trust Metrics	
Linguistic Description	PGP
	PolicyMaker trust Management system (Blaze, et al., 1996)
	Distributed trust model (Abdual-Rahman and Hailes 1998)
	Trust policy language (Herzberg et al., 2000)
	SPKI/SDSI public-key infrastructure (Clarke et al., 2001)
	……
Numerical Description	A continuous trust value between 0 and 1 (Maurer 96)
	Trust value & confidence value (Theodorakopoulos 04)
	Triplet: belief, disbelief and uncertainty (Jøsang 99)
	Discrete integer numbers (Abdul-Rahman and Hailes, 97)
	……

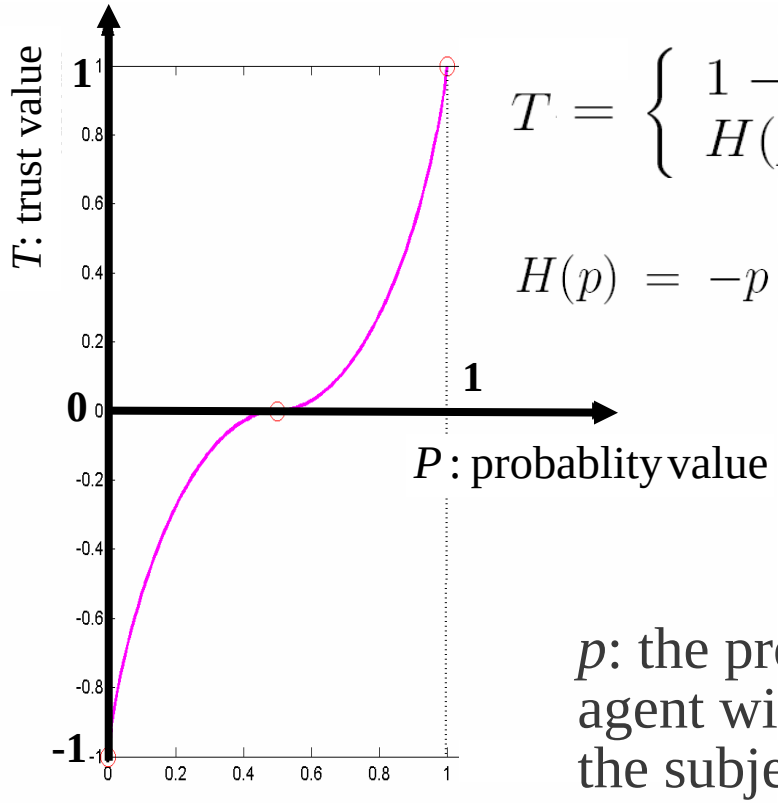
What is the physical meaning of these trust values?

Uncertainty ↔ Trustworthiness

- We argue that *uncertainty in belief* is a measure of trust.
  - Case 1: If the subject believes that the agent will perform the action for sure, subject "trust" the agent to perform the action. no uncertainty;
  - Case 2: If the subject believes that the agent will not perform the action for sure, subject "trust" the agent not to perform the action. no uncertainty;
  - Case 3: If the subject has no idea of whether the agent will perform the action or not, subject does not have trust in the agent. Highest uncertainty.

Entropy-based Trust Metric

- Trust value (*T*) measures uncertainty and is a function of entropy.



$$T = \begin{cases} 1 - H(p), & \text{for } 0.5 \le p \le 1 \\ H(p) - 1, & \text{for } 0 \le p < 0.5 \end{cases}$$

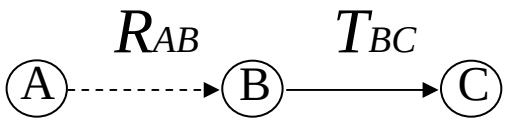
$$H(p) = -p\log_2(p) - (1-p)\log_2(1-p)$$

p: the probability with which the agent will perform the action in the subject's point of view

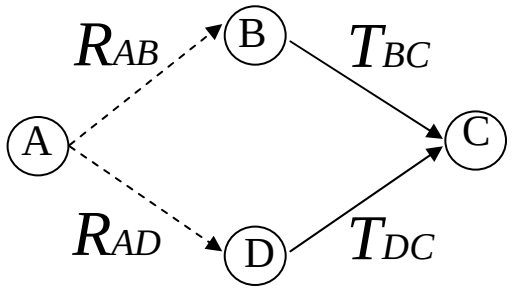
p ↔ T: one-to-one mapping

Trust Models

- Estimate trust value based on direct observation
- Estimate trust value based on recommendations (third parties' opinion) – *Trust propagation*.
- Concatenation trust propagation



- Multipath trust propagation



- Trust model: calculate trust via trust propagation

UNIVERSITY OF Rhode Island

UNIVERSITY OF Rhode Island

Rules for Trust Propagation

- Rule 1: Concatenation propagation does not increase trust.
- Rule 2: Multipath propagation does not reduce trust.
- Rule 3: Trust based on multiple recommendations from a single source should not be higher than that from independent sources.

Trust models should satisfy rules.

Trust models are not unique.

UNIVERSITY OF Rhode Island

Attacks and Protection

- Trust evaluation is an attractive target for attackers.
- Attackers' goals
  - Damage the network, e.g. reduce performance
  - Keep their own trust value above a certain threshold.
  - Cause inaccurate trust records.
    - *good nodes have low trust value*
    - *bad nodes have high trust value*
  - Discourage cooperation

Bad Mouthing Attack

- Malicious nodes providing dishonest recommendations.
  - Frame up good entities
  - Boost trust values of malicious peers

- Defense: ***Recommendation Trust***
  - The action trust and recommendation trust records are maintained separately.

    {A: C, performing action} – action trust

    {A: C, making honest recommendation} – recommendation trust

    To gain high recommendation trust, a node must provide good recommendations.

- *Bad Mouthing*
- On-off attack
- Conflicting behavior
- Sybil
- Newcomer

Usage of Recommendation Trust

– Trust models

Design rules: the subject assign low weight to the recommendations from the nodes with low recommendation trust.

– Recommendation trust is used in malicious node detection.

On-off Attack

Time-domain inconsistence attack

Dynamic Property of Trust:

- The observation made long time ago should not carry the same weight as those made recently.
- Forgetting Factor β $(0 < \beta \leq 1)$

$$K \text{ good actions at time } t_1$$

$$\Leftrightarrow K\beta^{t_2 - t_1} \text{ good actions at time } t_2$$

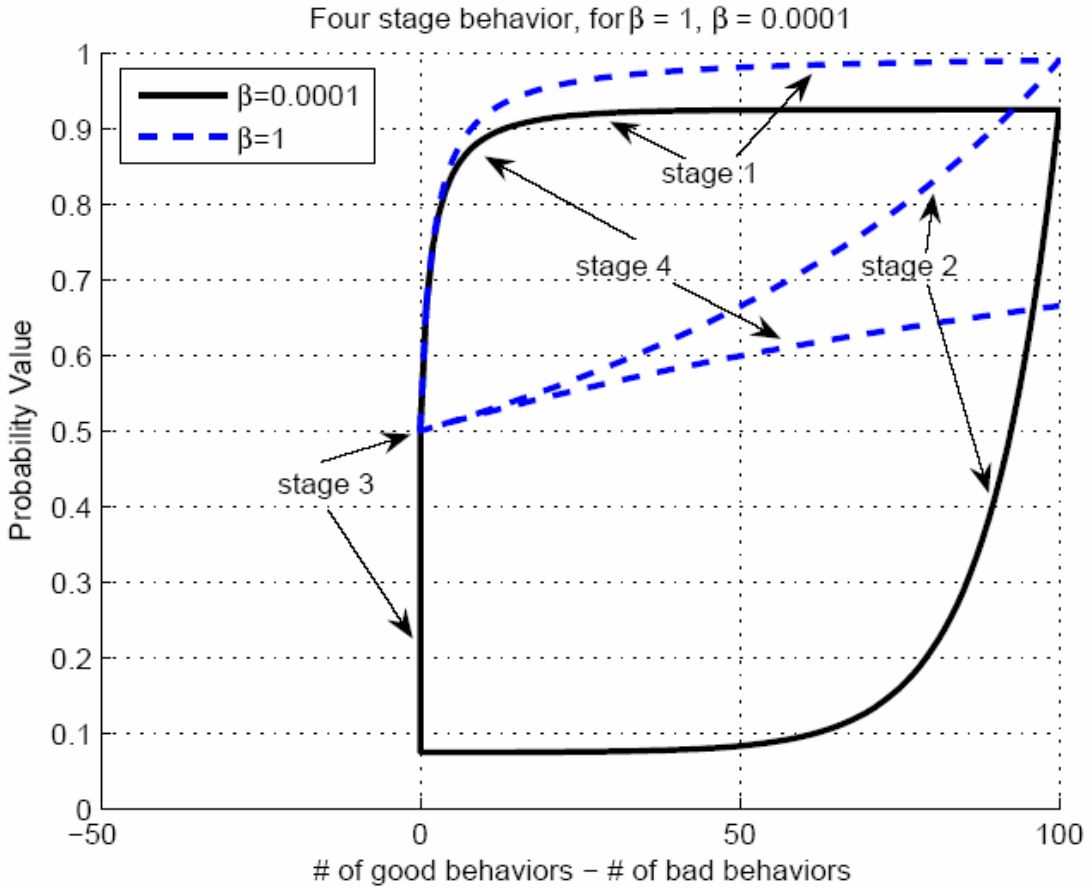
UNIVERSITY OF Rhode Island

On-off Attack

- Two representative cases:
  - Case 1: Don't forget ($\beta \approx 1$)
  - Case 2: Forget quickly ($\beta << 1$)

- A simple scenario:
  - Stage 1: Behave well for 100 times
  - Stage 2: Behave badly for 100 times,
  - Stage 3: Stop doing anything for sometime
  - Stage 4: Behave well again.

On-off Attack



- Large β : trust value cannot keep up with users' current status;
- Small β :Attackers can recover trust values by waiting.

UNIVERSITY OF Rhode Island

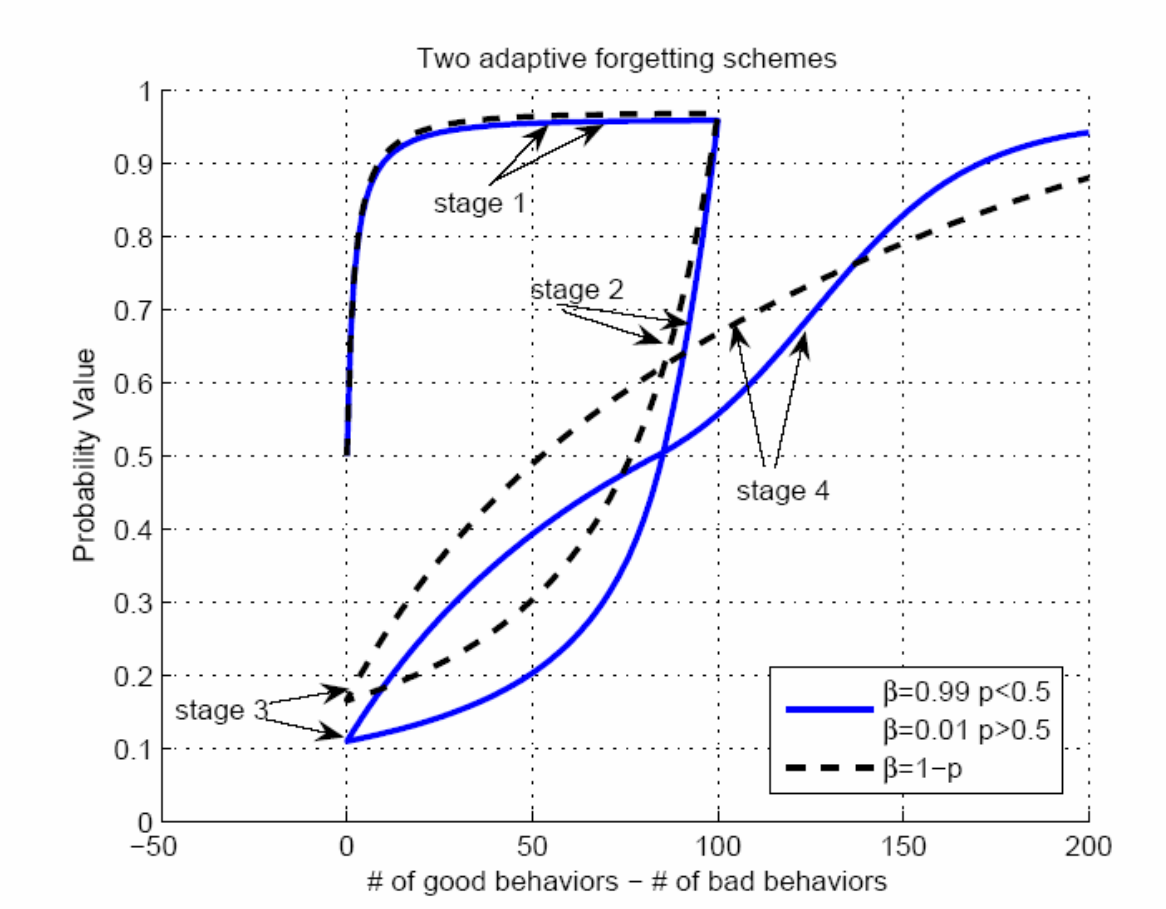
On-off Attack -- Defense

- A social phenomenon
  - It takes long-time interaction and consistent good behaviors to build up a good reputation, but only a few bad actions can ruin it.
- The solution: dynamic forgetting
  - When trust value is high, forget faster.
  - When trust value is low, forget slower.
  - β is a function of the current trust value.

$$\beta = 1 - p, \text{ where } p = P\{subject : agent, action\} \quad (1)$$

$$\text{or, } \beta = \beta_1 \text{ for } p \geq 0.5; \text{ and } \beta = \beta_2 \text{ for } p < 0.5, \quad (2)$$

On-off Attack -- Defense



- Trust value can keep up with the entity's current status after the entity turns bad.
- An entity can recover its trust value after some bad behaviors, but this recovery requires many good actions.

Conflicting Behavior Attack

- User-domain inconsistence.
- The attackers behave well to one group of users and behave badly to another group of users.
- These two groups develop conflicting opinions about the malicious users.

  T{A : X, action} = T1 (high)

  T{B: X, action} = T2 (low)

  -- B provides recommendation about X to A

  -- A compares B's recommendation and A's own experience

  -- A will assign low recommendation trust to B.

- As a consequence, two groups will not trust the recommendations from each others.

Sybil Attack

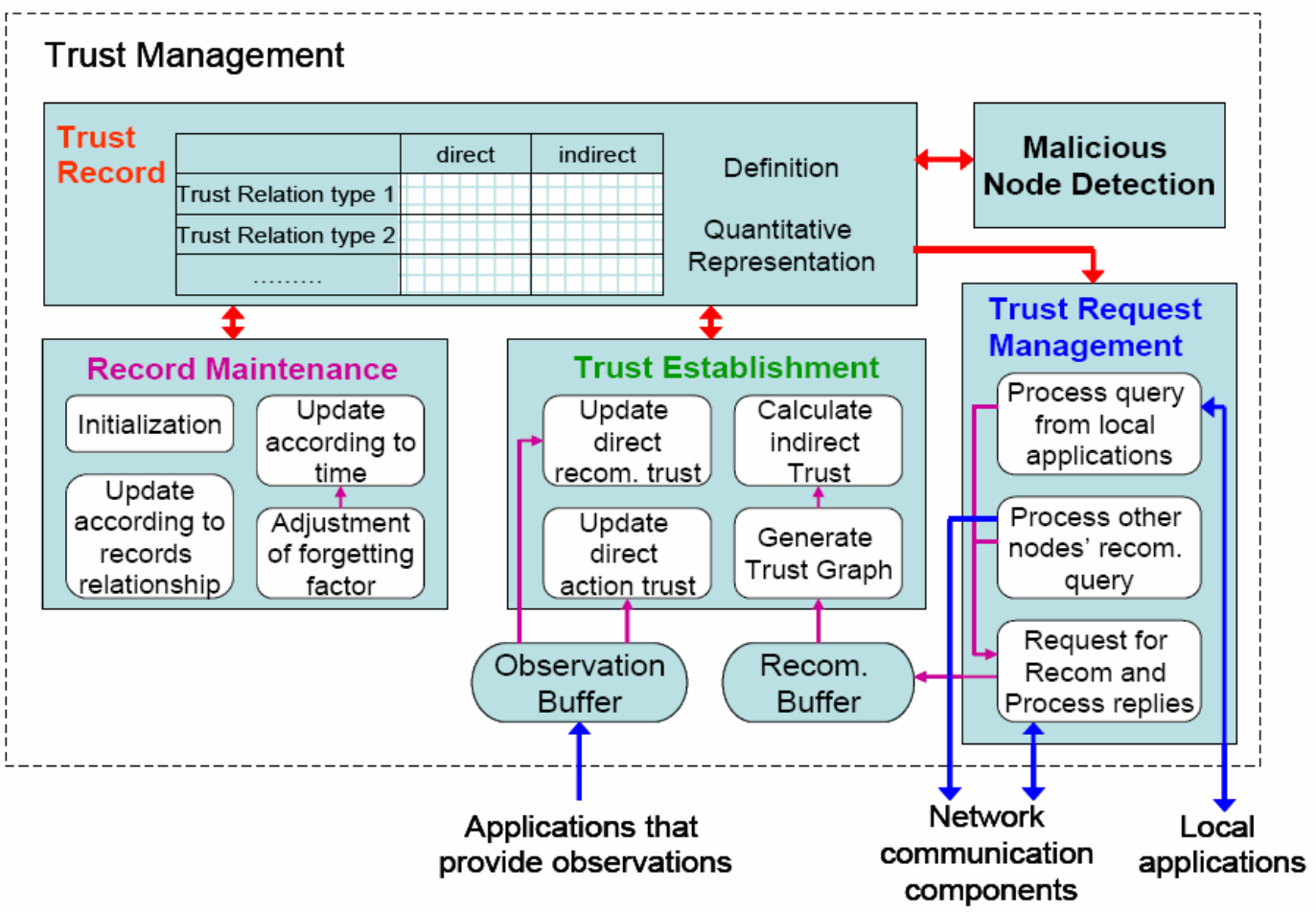
- Sybil Attack:
  - If a malicious node can create several faked IDs, then faked IDs can share or even take the blame, which should be given the malicious node.
- Defense: Authentication

Newcomer Attack

- If a malicious node can easily register as a new user, the trust management suffers the newcomer attack.
- Malicious nodes can easily remove their bad history and significantly reduce the effectiveness of trust management.
- Defense: access control policy and authentication

- Foundation
- Attack and Protection
- **Trust Evaluation System**

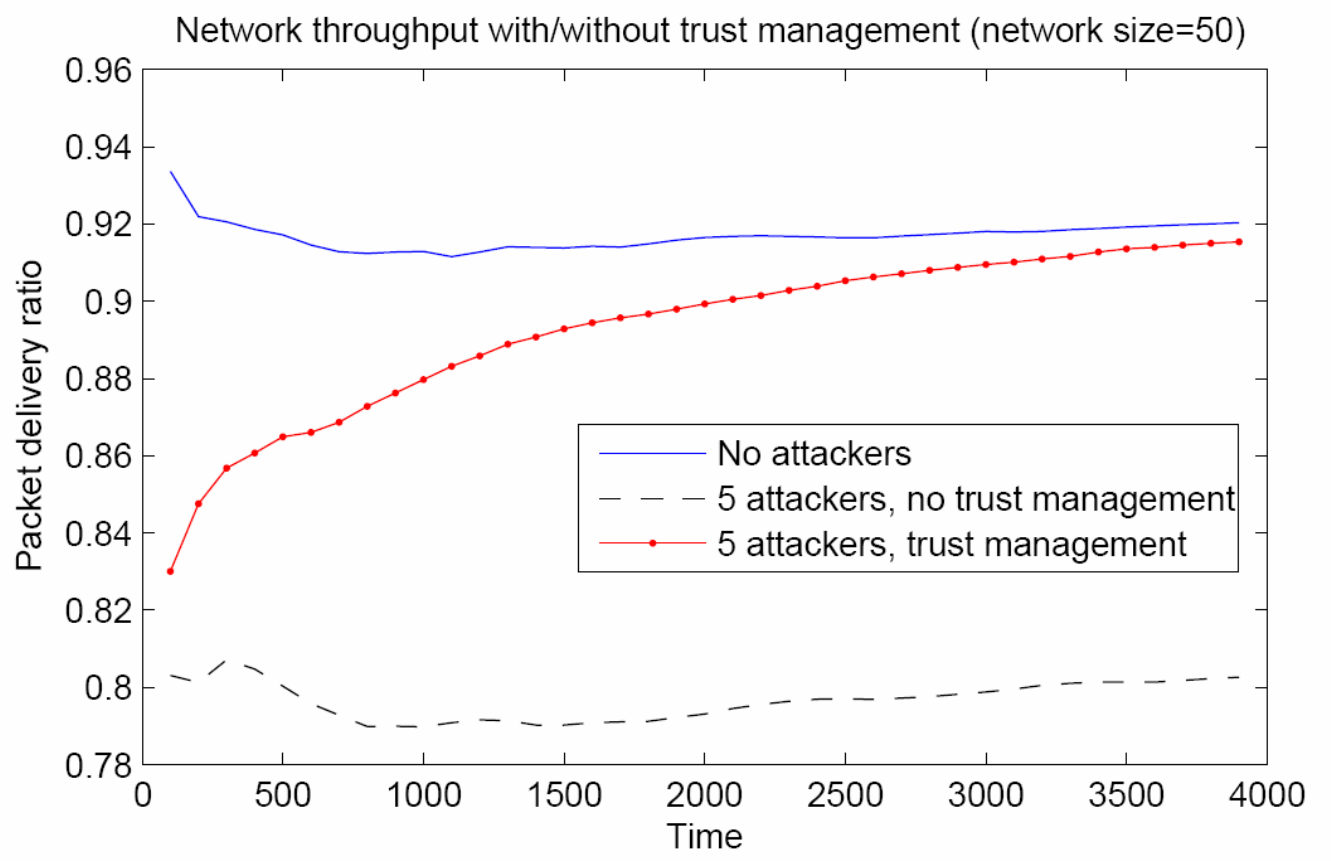
Trust Management System



Simulation System Setup

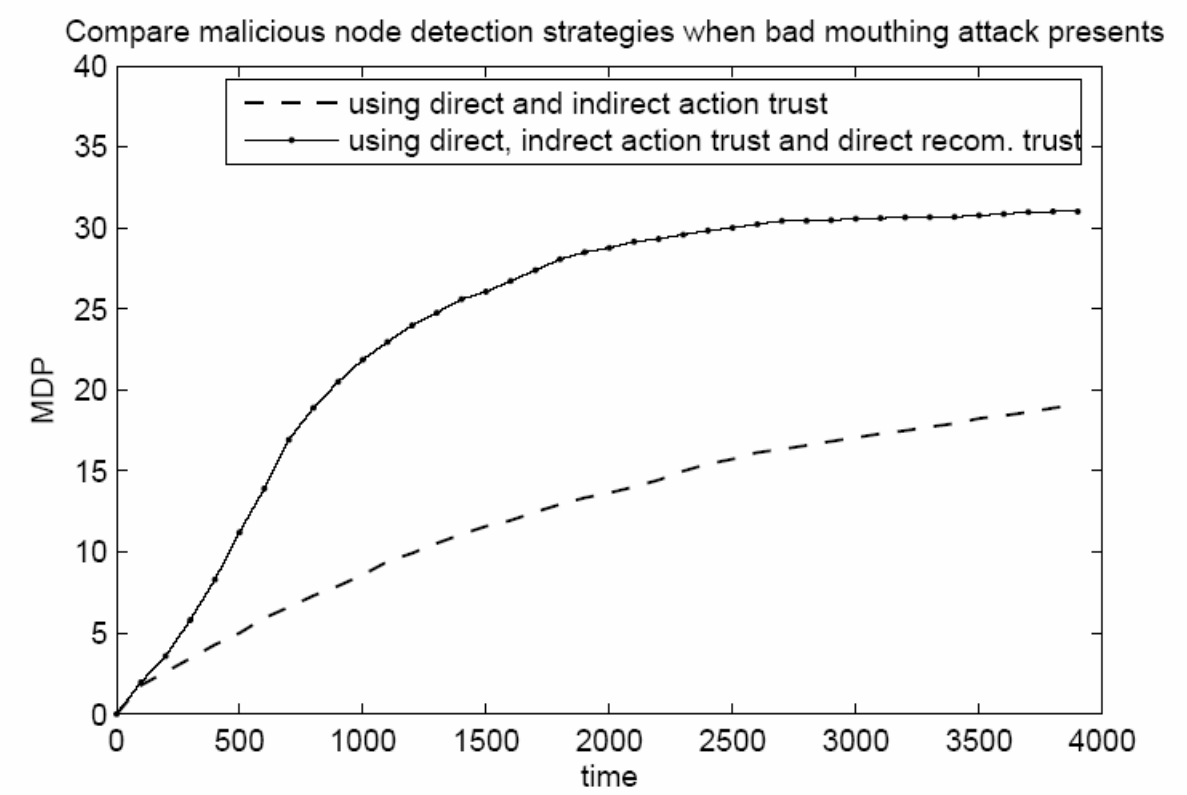
- Applications in Ad-hoc network
  - Malicious node detection
  - Route selection
- Attack model
  - Gray-hole attack
  - Attacks on trust evaluation
- Practical Issues
  - System structure
  - Obtaining trust recommendations
  - Privacy of trust recommendation

Effects of Trust Management



- Trust evaluation can improve network throughput because the malicious node has less chance to be on the route, and can be detected.

Bad Mouthing Attack

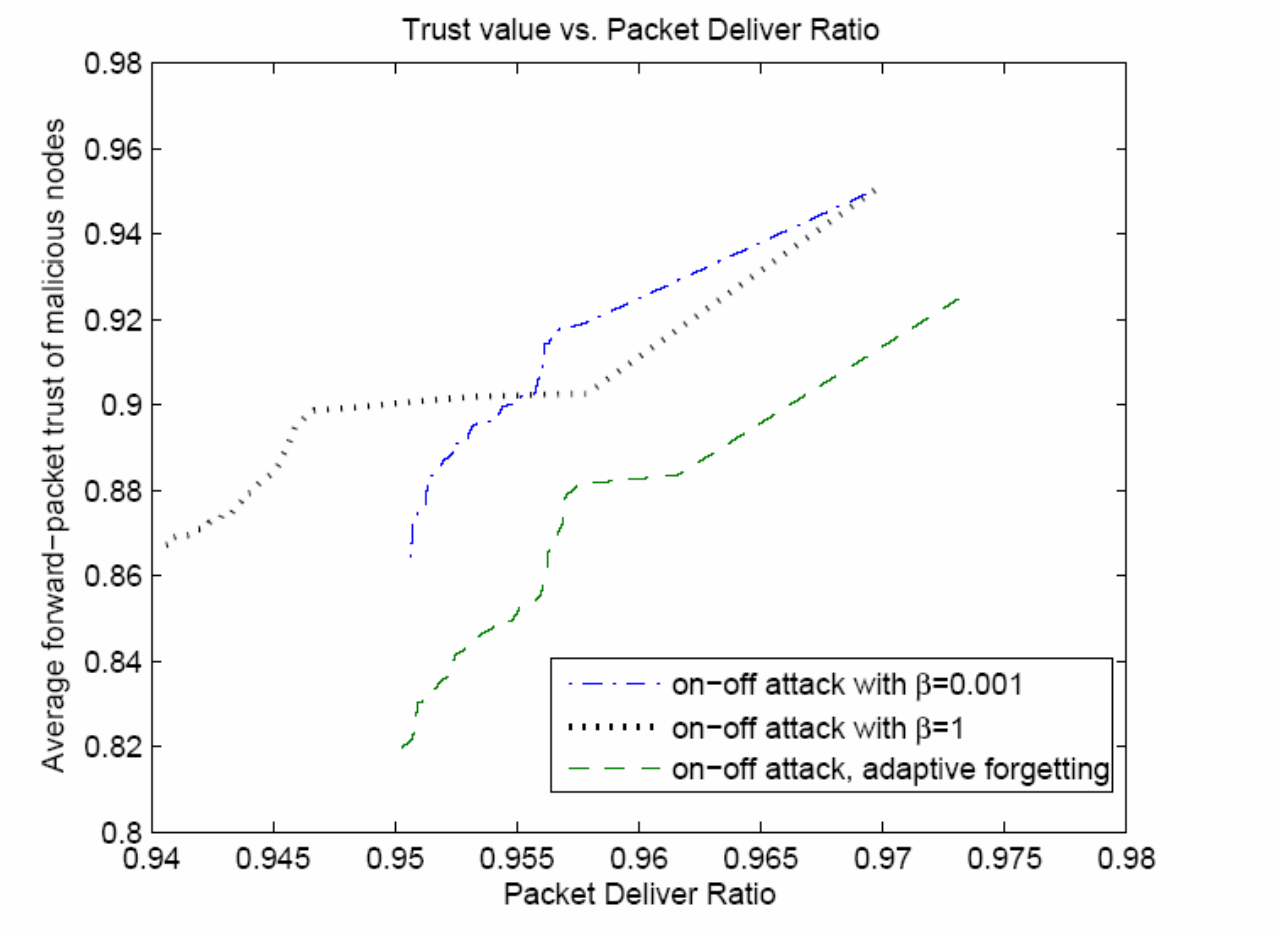


MDP = x means for each malicious node, there are about x good nodes have detected it as malicious.

- Using recommendation trust in malicious node detection significantly improves detection rate.

UNIVERSITY OF Rhode Island

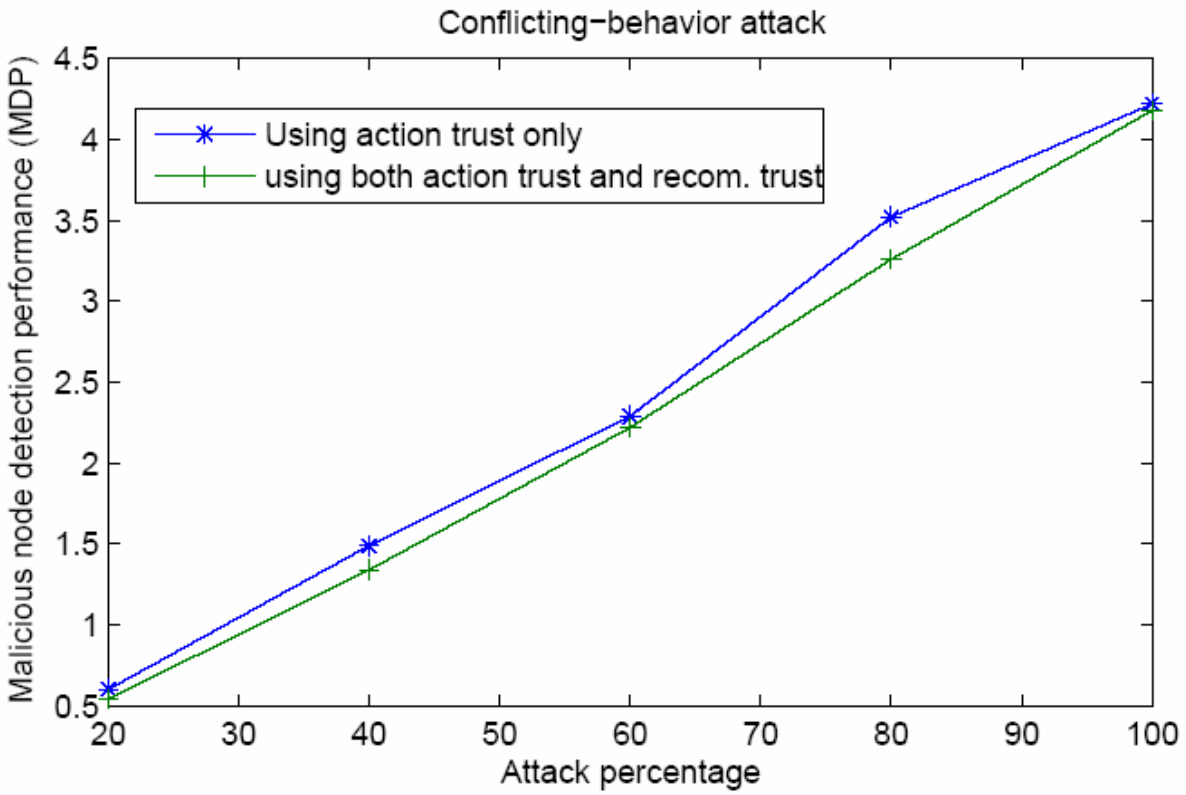
On-off Attack



- When the same packet deliver ratio is achieved, the adaptive forgetting scheme results in the lowest trust value of malicious users.

UNIVERSITY OF Rhode Island

Conflicting-behavior attack



- When confliction behavior attack presents, using recommendation trust for malicious node detection can reduce detection rate.

UNIVERSITY OF Rhode Island

Summary

- To defeat bad-mouthing attack, both action trust and recommendation trust should be used in malicious node detection.
- To defeat on-off attack, adaptive forgetting scheme should be used.
- When conflicting-behavior attack is launched, using recommendation trust in malicious node detection can reduce the detection rate.

Future work: New attacks and jointly investigate various attacks.