Reputation Systems for Mobile Ad hoc Networks

2004.04.15

林佑青

Outline

- Introduction
- Reputation systems
  - CORE
  - CONFIDANT
  - Nuglets
  - Sprite
- Discussion and conclusion

Introduction

- Cooperation is crucial in mobile ad hoc networks.
- Non-cooperation nodes:
  - Malicious nodes – Damage the network
  - Selfish nodes – Save energy, maximum welfare
- The reputation system is used to stimulate cooperation in ad hoc networks.

CORE (Collaborative Reputation) (1/3

- Each node keeps reputation values of other nodes in a reputation table
- Positive reputation values indicate trusted nodes
- Negative reputation values indicate misbehaving nodes
- Misbehaving nodes are denied the network service

CORE (2/3)

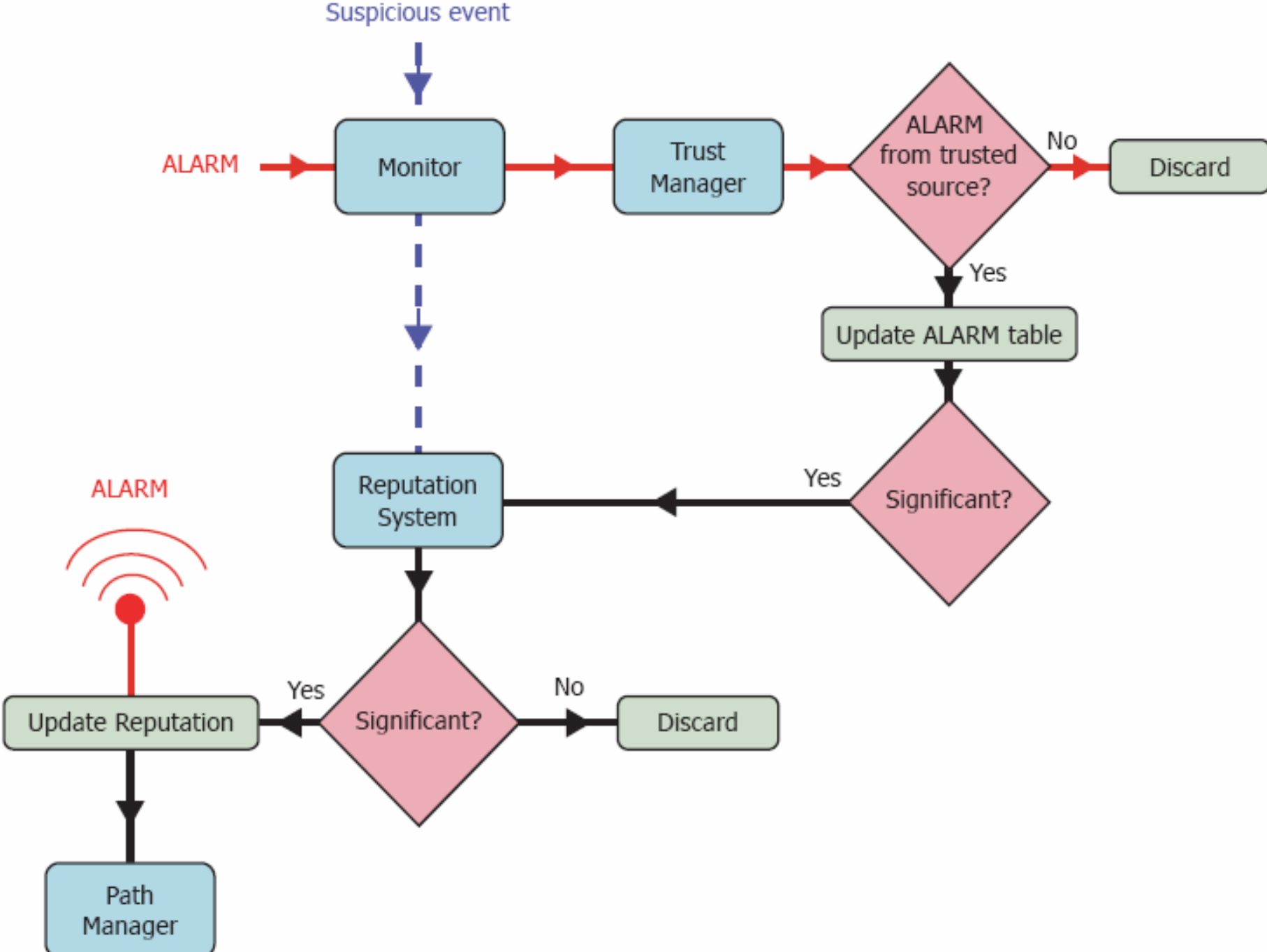
- CORE defines three types of reputation
  - Subjective reputation
  - Indirect reputation
  - Functional reputation
- Reputation values in CORE are based on observations.
  - From -1 (bad) to 1 (good)

CORE (3/3)

- Each node maintains a reputation table which consists of the reputations of other nodes.
  - A requests a service from B, but B refuses
  - There is no interaction with the observed node
  - A refuses B who has a bad reputation
    - A sends a message to all neighbor nodes
    - Neighbor nodes checking agree with A or not

CONFIDANT

- Cooperation Of Nodes: Fairness In Dynamic Ad-hoc NeTworks
- Detecting and isolating misbehaving nodes
- Consists of some components:
  - Monitor
  - Reputation System
  - Trust Manager
  - Path Manager


Suspicious event
ALARM
Monitor
Trust Manager
ALARM from trusted source?
No
Discard
Yes
Update ALARM table
Significant?
Yes
Reputation System
ALARM
Significant?
Yes
No
Discard
Update Reputation
Path Manager

Drawbacks

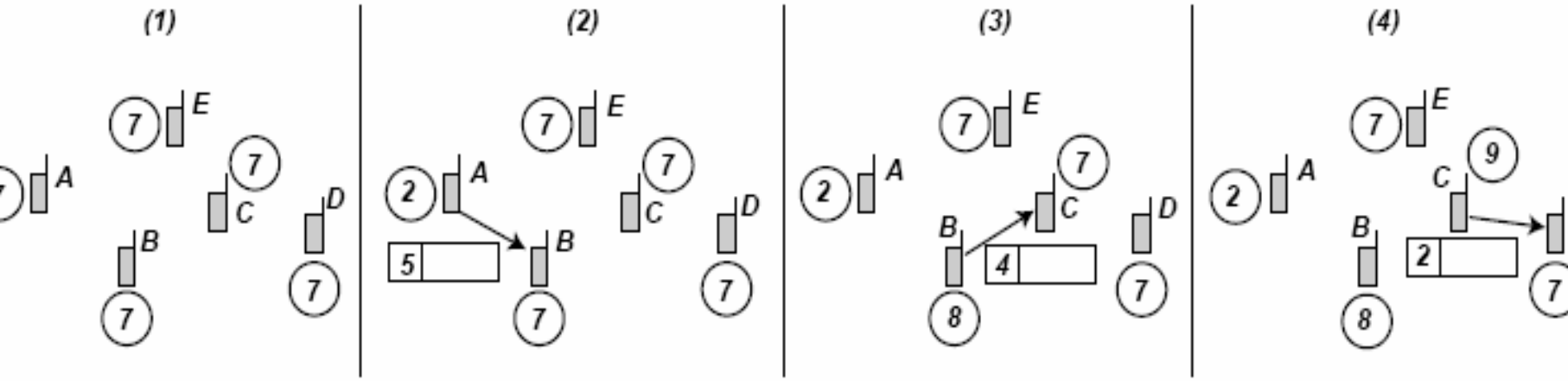
- There is no formal specification and analysis of incentive provided by such systems.
- The systems have not considered that the selfish nodes may collude with each other.
- The monitoring scheme may not always be possible when nodes use power control.

Nuglets

- A virtual currency to stimulate cooperation in self-organized mobile ad hoc networks.
  - Packet Purse Model (PPM)
  - Packet Trade Model (PTM)
- Using virtual currency (credit) to stimulate cooperation.
- If a node wants to use a service, then it has to pay for it in nuggets.

Packet Purse Model

- The originator of the packet pays for the forwarding service.
- Each forwarding node takes out nuggets for its forwarding service.

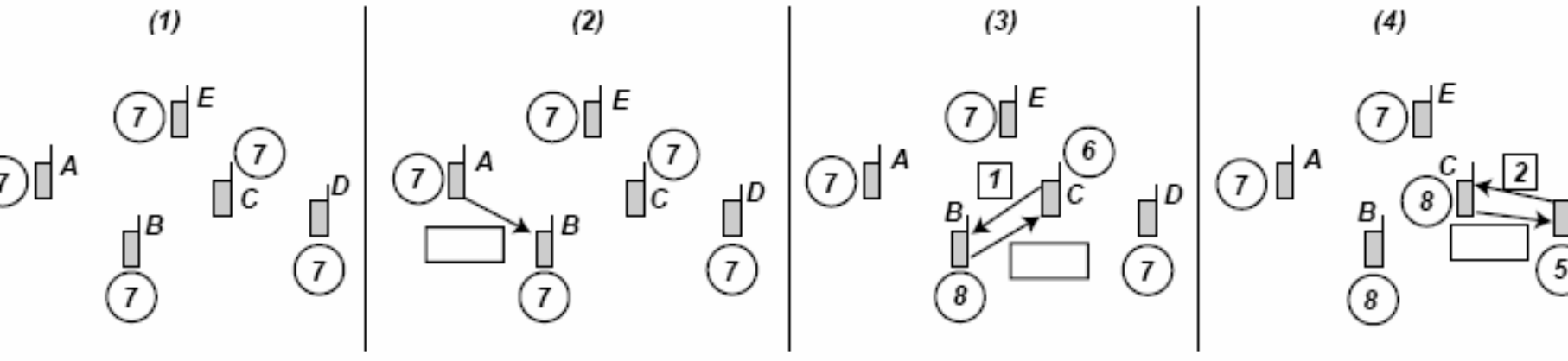


Pros and Cons

- Pros
  - Discourage users from sending useless data and overloading the networks.
- Cons
  - Source node needs to know exactly how many nuggets to include in the packet

Packet Trade Model

- Each intermediary node buys the packet from the previous node, and sells it to the next node for more nuggets.
- The total cost of forwarding the packet is covered by the destination node.



Pros and Cons

- Pros
  - The source node does not need to know how many nuggets to load into the packet.
- Cons
  - Since no charge for packet generation, malicious users might try to flood the network.

Tamper resistant security module

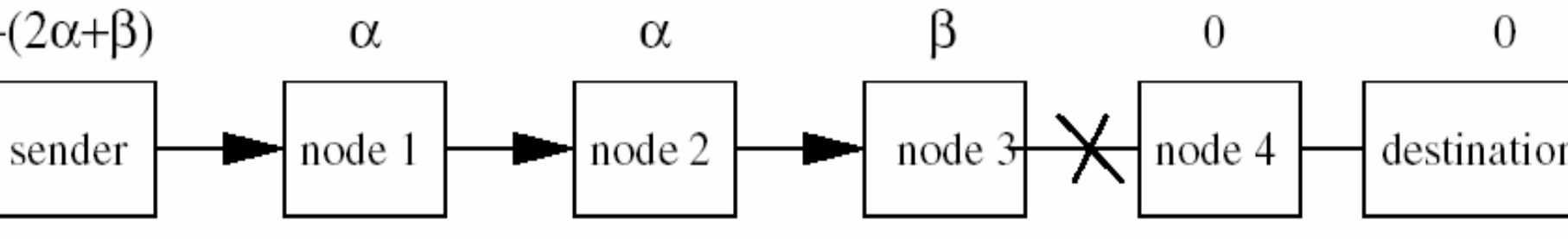
- Assume that each node has a tamper resistant module
  - Special chip
  - Smart card
- The security module is used for the management of nuggets.
- The module's behavior can not be modified.

Sprite

- A simple, cheat-proof, credit-based system for mobile ad-hoc networks
- Determines charge and credit from a game-theoretic perspective, and motivates each node to report its actions honestly.
- The system does not require any tamper-proof hardware at any node.
- Requires a centralized server
  - Credit clearance system (CCS)

Payment scheme

- CCS should give more credit to a node who forwards a message than to a node who does not forward a message.
- The CCS determines the last node on the path that has ever received the message.



Computing payments

The CCS charges C from node n_0 , and pays P_i to node n_i ,

$$C = (d-1)\alpha + \beta - (d-e)\gamma\beta$$

$$P_i = \begin{cases} \alpha & \text{if } i < e = d \\ \beta & \text{if } i = e = d \\ \gamma\alpha & \text{if } i < e < d \\ \gamma\beta & \text{if } i = e < d. \end{cases}$$

$P = (n_0, n_1, \ldots, n_e, \ldots, n_d)$

N_e is the last node on path P that submits a valid receipt

Analysis of the receipt-submission game

- Theorem 1: In the receipt-submission game, truth-telling is an optimal strategy for every node.
- Theorem 2: The receipt-submission game is collusion-resistant.
- Theorem 3: The receipt-submission game is cheat-proof.

Discussion

Comparison	Cons
CORE	No incentive provided Monitoring scheme
CONFIDANT	No incentive provided Monitoring scheme
Nuglets	Tamper-proof hardware required
Sprite	Centralized server required

Conclusion

- Reputation systems are used to establish trust and encourage trustworthy behavior.
- In the reputation system for mobile ad hoc networks, there are several defeats can be improved in the future.

Reference

- [1] S. Marti, T. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks,” in *Proceedings of The Sixth International Conference on Mobile Computing and Networking 2000*, Aug. 2000.
- [2] P. Michiardi and R. Molva, “CORE: A Cooperative reputation mechanism to enforce node cooperation in mobile ad hoc network,” in Communications and Multimedia Security Conference (CMS) 2002.
- [3] S. Buchegger and J.-Y. L. Boudec, “Performance analysis of the CONFIDANT protocol: Cooperation of nodes - fairness in dynamic ad-hoc networks,” in *Proceedings of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC)*. IEEE, June 2002.
- [4] L. Buttyan and J. P. Hubaux, “Nuglets: A Virtual Currency to Stimulate Cooperation in Self-Organized Mobile Ad-Hoc Networks”. Technical Report DSC/2001/001, Swiss Federal Institute of Technology, January 2001.
- [5] S. Zhong, Y.R. Yang, and J. Chen, “Sprite, A Simple, Cheat-Proof, Credit-based System for Mobile Ad-Hoc Networks,” in Proceeding of IEEE INFOCOM ’03, Apr. 2003.
- [6] Y. Liu and Y. R. Yang, “Reputation propagation and agreement in mobile ad-hoc networks,” in *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC)*, March 2003.