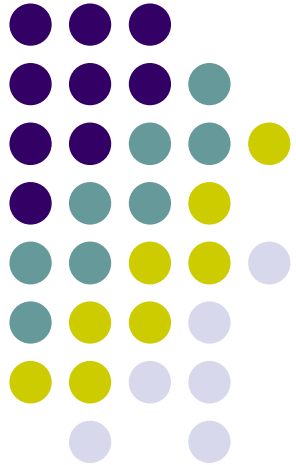
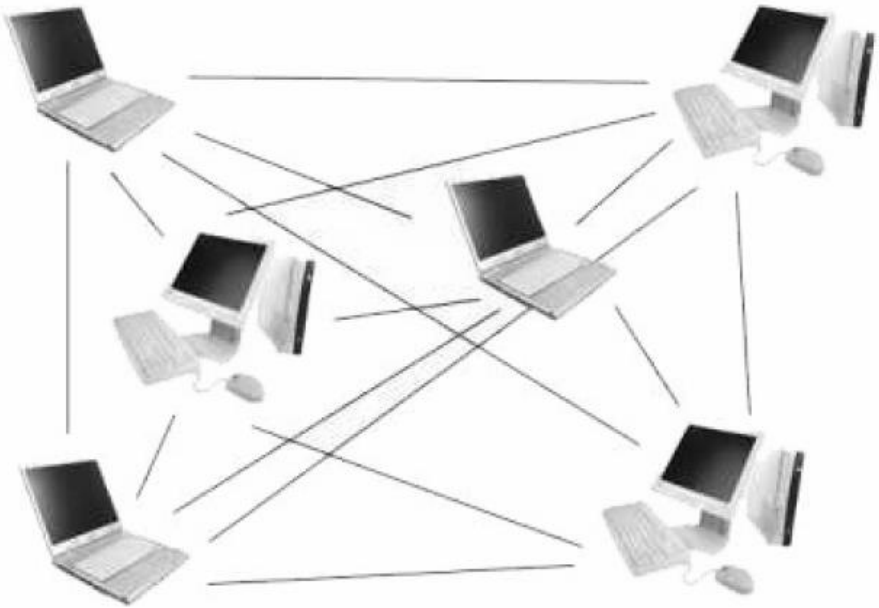
Cooperation in Mobile Ad hoc Networks



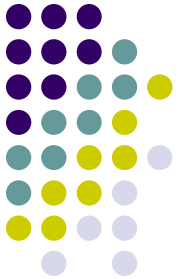
Introduction

Mobile Ad hoc Network (MANET)



A MANET.

Introduction



Characteristics of MANETs:

- Wireless
- Mobile
- Lack of structure
- Energy-constrained
- Heterogeneous
- Prone to abuse

Introduction

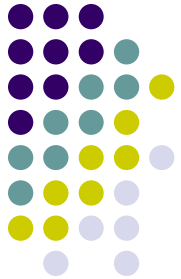
MANET support applications:

- No infrastructure available
- Flexible application
- Collaborative Computing

Examples of MANET applications:

- Business environment
- Crisis management
- Military Applications

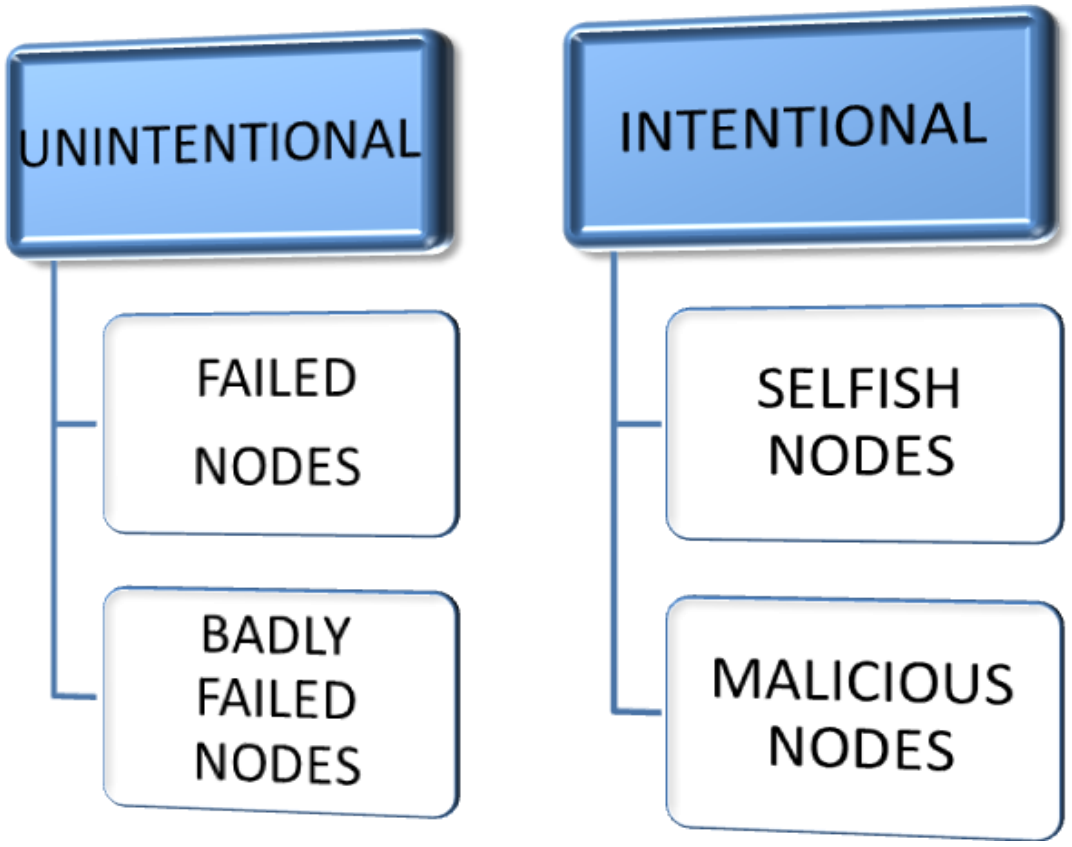
Introduction



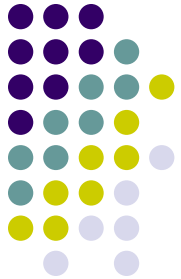
Selfish nodes may gain distinct advantages:

- Exploit the service of cooperating nodes;
- Exploit incentive measures to gain monetary benefits;
- Preserve resource and power;
- Prevent other nodes from getting proper service.

Types of Node Behavior

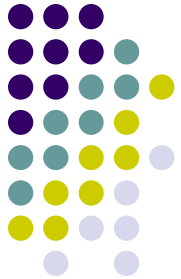


Misbehaved nodes



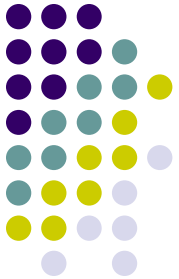
- ***Failed nodes*** are simply those unable to perform an operation; this could be because of power failure and environmental events.
- ***Badly failed nodes*** exhibit features of failed nodes but they can also send false routing messages which are a threat to the integrity of the network.
- ***Selfish nodes*** are typified by their unwillingness to cooperate, as the protocol requires whenever there is a personal cost involved. Packet dropping is the main attack by selfish nodes.
- ***Malicious nodes*** aim to deliberately disrupt the correct operation of the routing protocol, denying network service if possible.

Dealing with Misbehaviors



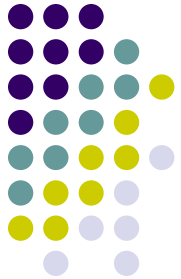
- Work of Marti et al. published in MobiCom (2000).
- Misbehaving nodes: Nodes which agree to cooperate, but do not.
- Intelligently identify misbehaving nodes and avoid relaying through those nodes.
- Two components:
  - Watchdog: Runs on every node to keep track of the behavior of the other nodes.
  - Pathrater: Uses the Watchdog information to find out the reliable routes.

Incentives for Cooperating



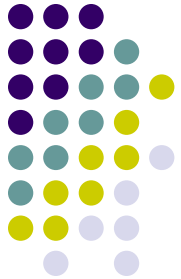
- Works by Buttyan and Hubaux (2000-2001), published in MobiHoc (2000) and IEEE Communications Magazine (2001).
- Provide incentives for cooperating without overloading the network.
- Reward/penalty model:
  - Charge the nodes receiving a service.
  - Remunerate the nodes providing a service.
  - Accept/reject a relay request based on this model.
- Drawback: Large overhead in a resource constrained ad hoc/sensor network.

Countering Misbehavior



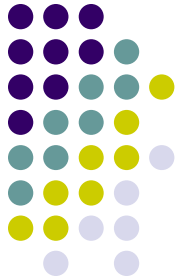
- Virtual Currency Systems (Payment Systems)
  - Nuglets
  - Sprite
- Reputation Systems
  - CONFIDENT
  - CORE
  - OCEAN

Virtual Currency Systems



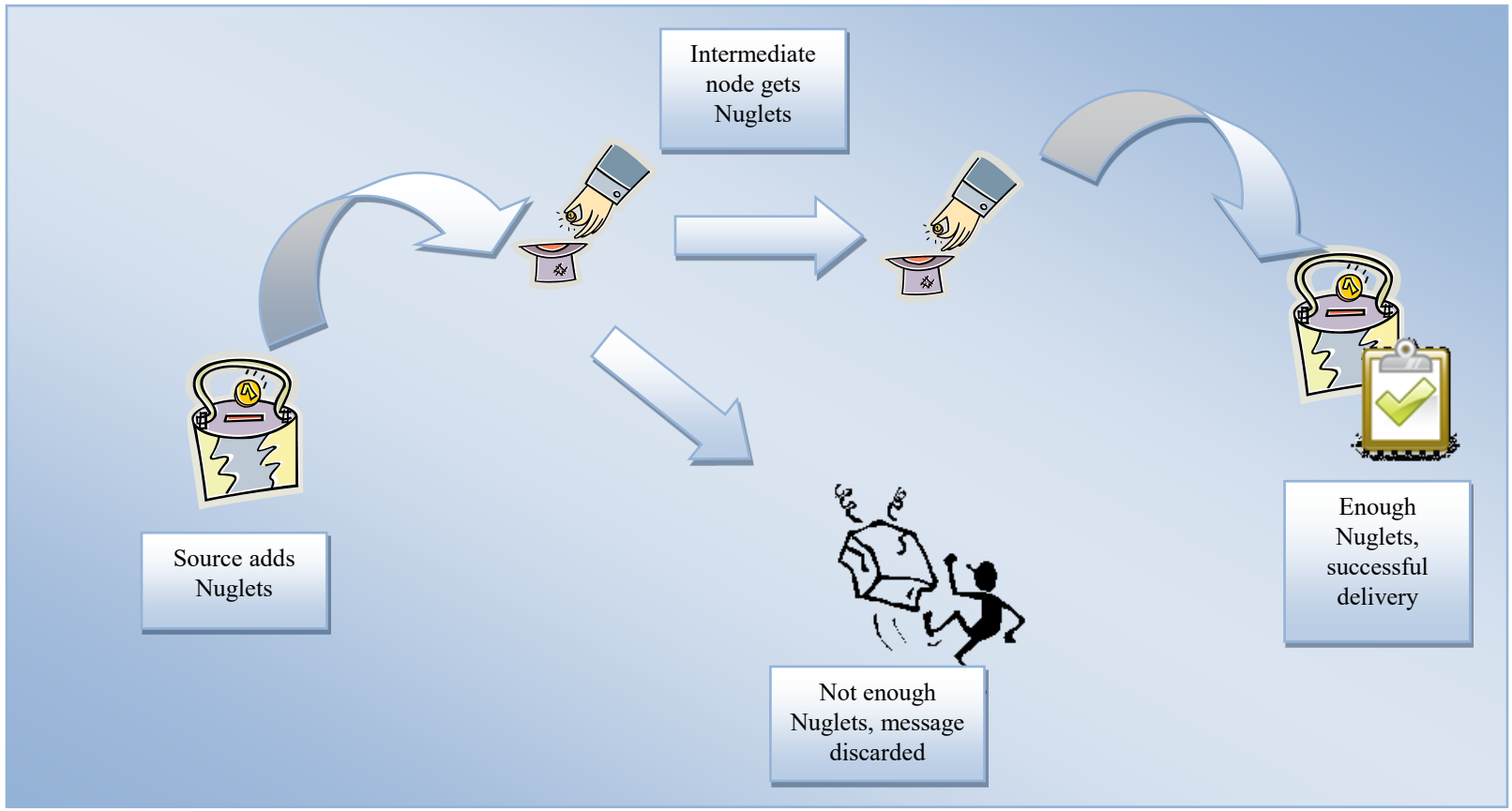
- Use some forms of incentive to compensate for the service of a node.
- A node receives a virtual payment for serving the network.
- A node uses the incentives to gain service from the network.
- Examples:
  - Nuglets
  - Sprite

Payment Systems: Nuglets

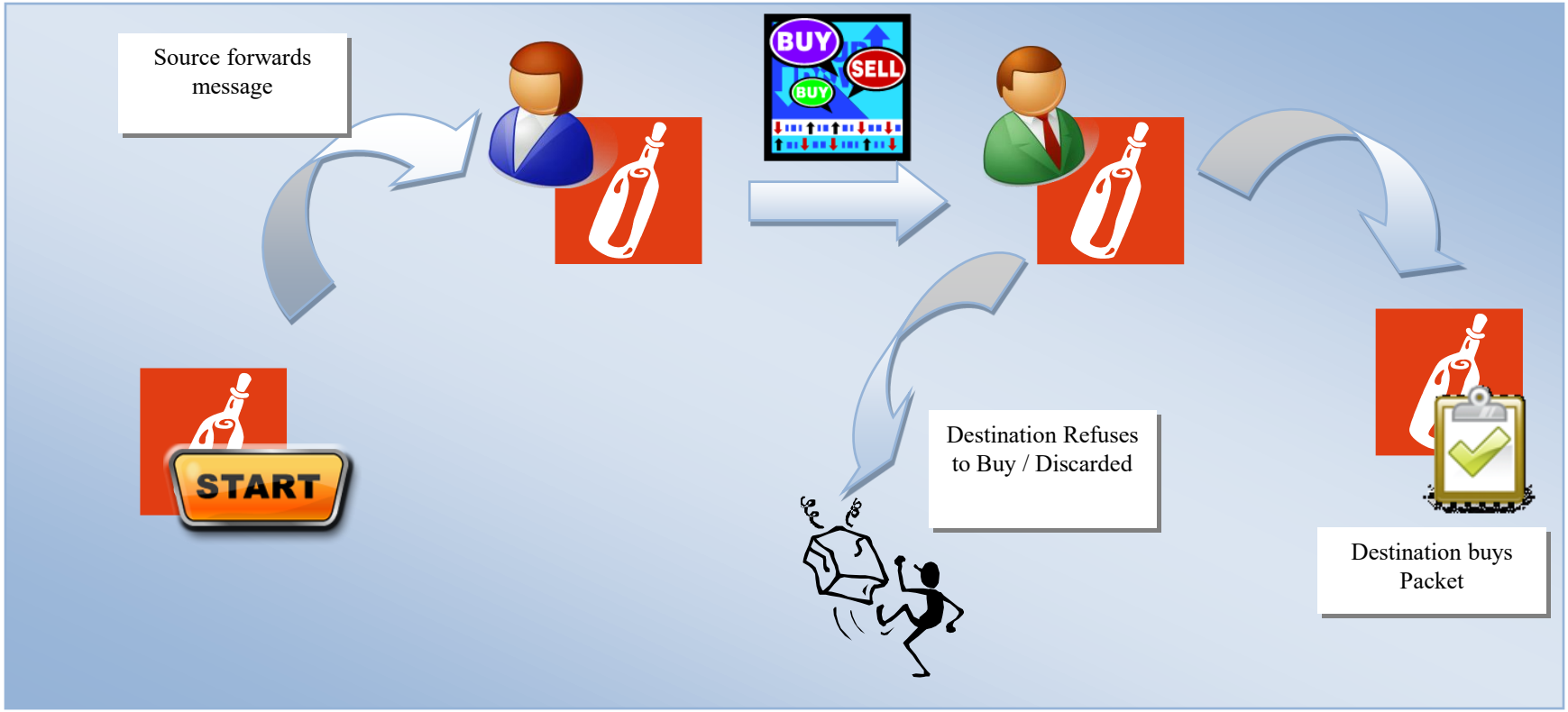


- Virtual currency mechanism for charging (rewarding) server usage (provision).
- Nodes that use a service must pay for it (in nuglets) to nodes that provide the service.
- A typical service is packet forwarding which is provided by intermediate nodes to the source and the destination of the packet.
- Therefore either the source or the destination should pay for it.
- Models for charging for the packet forwarding :
  - Packet Purse Model
  - Packet Trade Model

Packet Purse Model



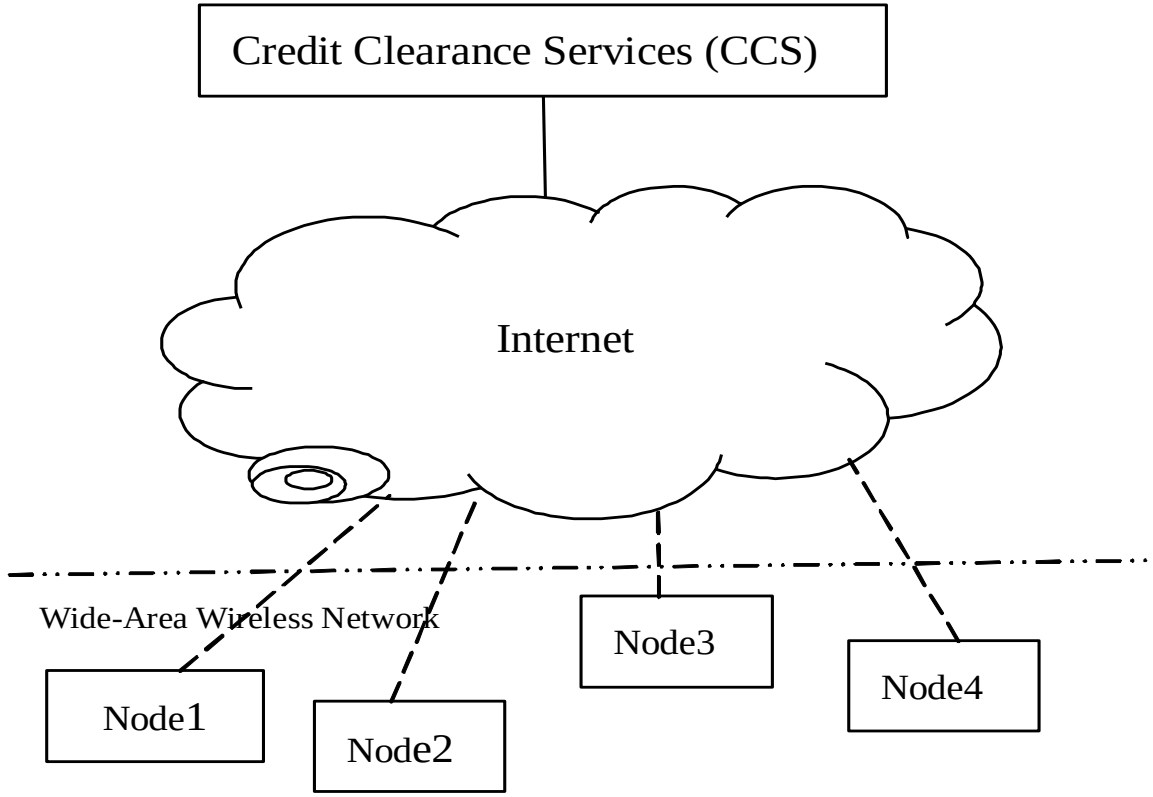
Packet Trade Model



Nuglets

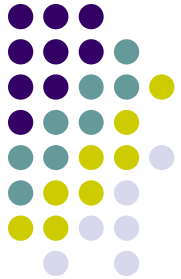
	Advantage	Disadvantage
Packet purse model	deters nodes from sending useless data and overloading the network	difficult to estimate the number of nuglets that are required
Packet trade mode	source does not have to know in advance the number of nuglets required	May not prevent nodes from overloading the network

Sprite (S. Zhong, J. Chen & Y. R. Yang, 2003)



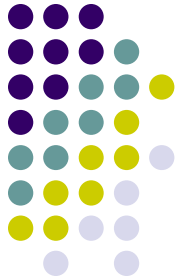
Architecture of Sprite.

Sprite (S. Zhong, J. Chen & Y. R. Yang, 2003)



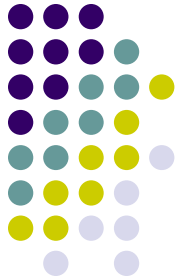
- A credit based system.
- Uses *credit* to provide incentives to selfish nodes.
- Nodes keep *receipt* to get payments from the Credit Clearance Service (CCS).
- The credit a node gets depends on whether the service is successful or not.

Virtual Currency Systems



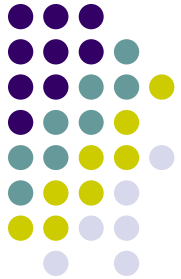
- Nuglets requires tamper-proof hardware to control the number of nuglets that are charged.
- Sprite requires a central server to determine the charge and credit to each node.
- Both systems suffer from the *location privilege problem:*
  - Nodes in certain locations of the network have a better chance for earning credits, which may not be fair for all nodes.

Reputation Systems



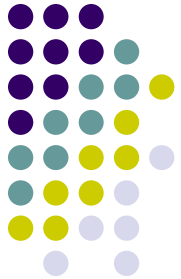
- Useful way to reduce the risk entailed in interactions among total strangers in electronic marketplace
- Different types
  - Centralized reputation systems (e.g., eBay)
  - Decentralized reputations (e.g., in MANETs)
    - Each node keeps the ratings about other node
    - Updates the ratings by direct observation of the behaviors of neighboring nodes or second hand information from other trusted nodes.
- The three goals for reputation systems are:
  - To provide information to distinguish between a trust-worthy principal and untrustworthy principals.
  - To encourage principals to act in a trustworthy manner.
  - To discourage untrustworthy principals from participating in the service the reputation mechanism is present to protect.

Reputation Systems: Examples



- CONFIDANT
- CORE
- OCEAN

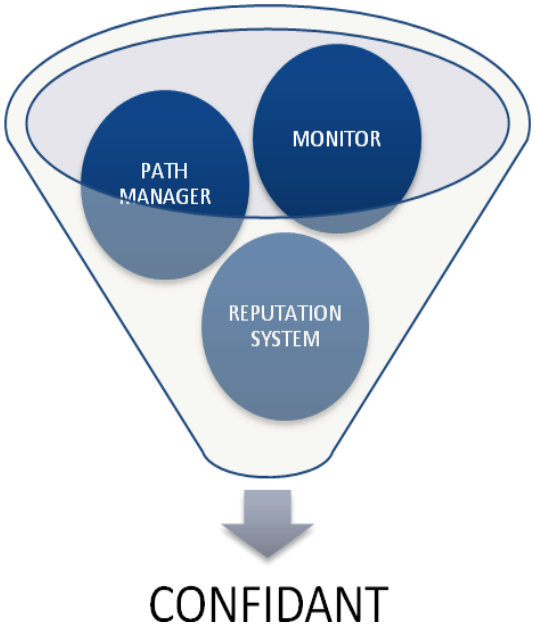
Types of Reputation Systems



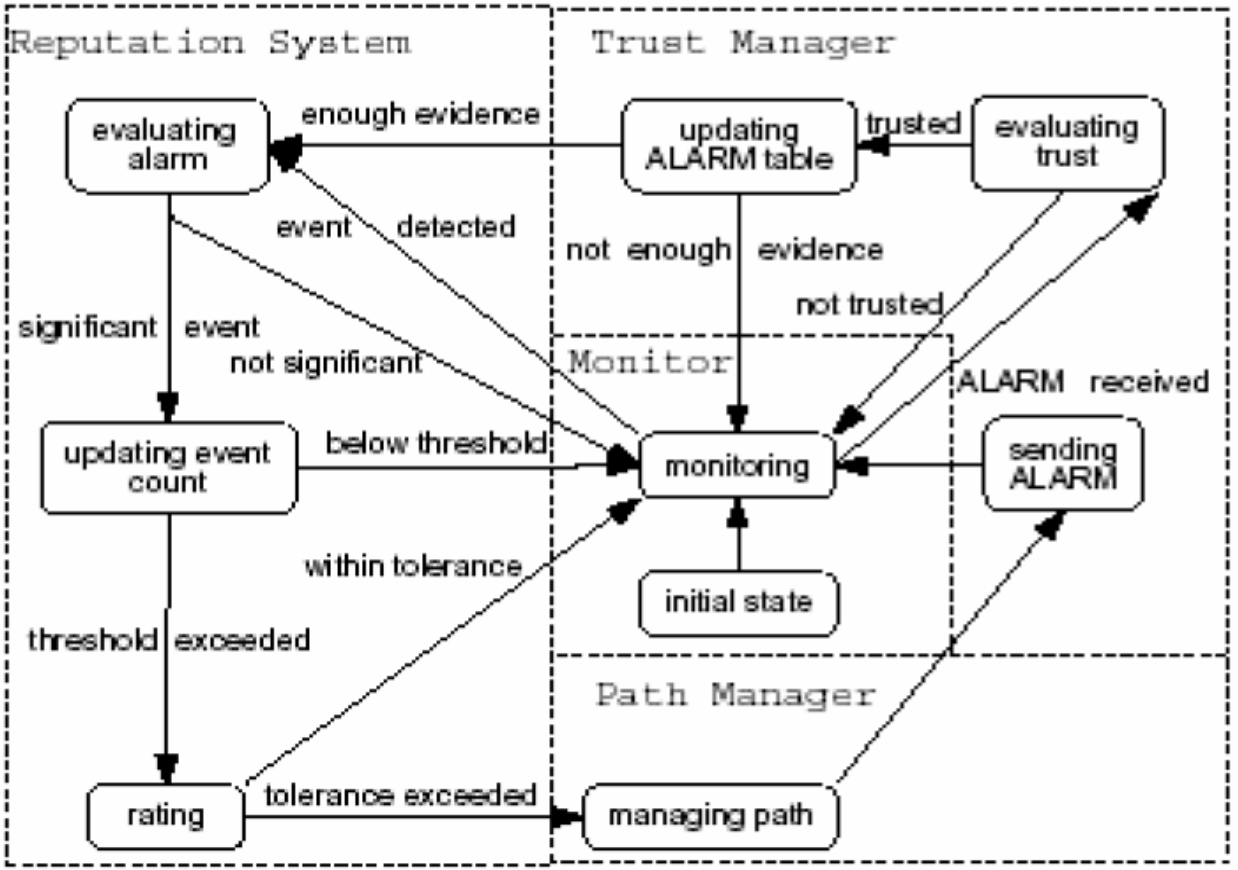
- **Global reputation system**:
  - Each node knows the reputation value of every other node in the network.
  - Achieved by exchange indirect reputation message among the network.
  - Examples: CONFIDANT and CORE.
  - Disadvantages:
    - Each node maintains reputation values of every other node, which costs a lot of storage.
    - Disseminate reputation information greatly increases the volume of network traffic.
    - The decision and incorporating second hand information consumes addition computation.
    - The reputation information could be modified, replayed or accidentally lost during transmission.
- **Local reputation system**:
  - Each node only keeps the reputation value of its neighboring nodes.
  - Instead of distributing reputation value or information periodically, the local reputation systems usually update reputation value based on its own observation.

CONFIDANT: Cooperation of Nodes – Fairness in Dynamic Ad-hoc Network

- Detect the misbehaved nodes and isolate them from communication by not using them for routing and forwarding and by not allowing the misbehaved nodes to use itself to forward packets.

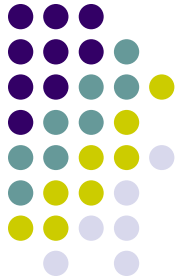


CONFIDANT (Buchegger & Boudec, 2002)



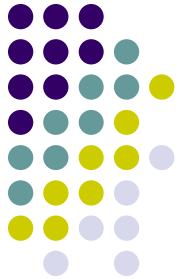
The interaction of the components in CONFIDANT.

CORE (Michiardi & Molva, 2002)



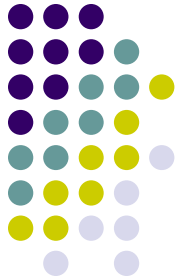
- CORE: COllaborative REputation
- Similar to CONFIDANT.
- Three types of reputations are used in the CORE.
  - ***Subjective reputation*** of a target node is the reputation calculated directly from a subject's observation of the target node's behavior.
  - ***Indirect reputation*** is evaluated only considering the direct interaction between a subject and its neighbors.
  - ***Function reputation*** is the subjective and indirect reputation calculated with respect to different functions such as forwarding a data packet, reply route request.
- CORE consists of two basic components:
  - Reputation Table (RT): a data structure stored in each network entity, keeping the reputation data pertaining to the nodes in the network.
  - Watchdog mechanism (WD): used to detect misbehaved nodes.

OCEAN (S. Bansal and M. Baker, 2003)



- OCEAN stands for Observation-based Cooperation Enforcement in Ad hoc
- Disallows second-hand reputation exchange.
- Makes routing decisions based on direct observations of its neighboring nodes interaction.
- Five components reside in each node:
  - *NeighborWatch*
  - *RouteRanker*
  - *Rank-Based Routing*
  - *Malicious Traffic Rejection*
  - *Second Chance Mechanism*

Reputation Systems



- Without a priori “trust” relationship or a trusted management mechanism, these systems may be destabilized by false rating, either false accusation or false praise.
- Nodes have to keep, update and share reputation information; this causes more overhead both for individual node and for the network.