Performance Analysis of the CONFIDANT Protocol

CONFIDANT- Cooperation Of Nodes: Fairness In Dynamic Ad-hoc NeTworks

Introduction

- CONFIDANT aims at making misbehavior in mobile ad hoc networks unattractive.It is based on selective altruism and utilitarianism.
- Trust relationships and routing decisions are based on experienced,observed or reported routing and forwarding behavior of other nodes.
- Here DSR is taken to be the base protocol.

Introduction

- A performance analysis of DSR with CONFIDANT is presented with a comparison to regular DSR.
- This analysis shows that a network with CONFIDANT and up to 60% of misbehaving nodes behaves almost as well as a benign network, in contrast to a defenseless one.

The DSR Protocol

- Dynamic Source Routing is a protocol developed for routing in mobile ad hoc networks.
- Nodes send out a ROUTE REQUEST message, all nodes that receive this message put themselves into the source route and forward it to their neighbors.
- If a receiving node is the destination, or has a route to the destination, it sends a REPLY message containing the full source route.

The DSR Protocol

- After receiving routes, the source node selects the best, stores it and sends messages along that path.
- A link failure is detected by a node that cannot forward the packet to the next node in the source route. It then sends a ROUTE ERROR message to the source.
- Packets are then forwarded along an alternate route that does not contain the bad link.

Attacks against Routing

- Mobile ad-hoc networks lack an infrastructure and organizational environment that makes them easily vulnerable to attacks.
- CONFIDANT aims to protect against the following attacks.
  - No forwarding.
  - Traffic Deviation.
  - Route salvaging.
  - Lack of error messages.
  - Unusually frequent route updates.
  - Silent route change.

Related Work

- Anderson & Stajano- device imprinting
- Zhou & Haas – asynchronous threshold security and share refreshing for key management.
- Smith,Murthy & Garcia-Luna-Aceves – routing security of distance vector protocols
- Buttyan & Hubaux- incentives for cooperation through nuglets.
- Marti, Giuli, Lai & Baker- Watchdog & Pathrater.
- SAR by Yi, Naldburg & Kravets.
- Ariadne,etc.

Approach

- The method proposed is based on detection of misbehavior, followed by a reaction of other nodes that results in a disadvantage for the malicious node.
- Packets of malicious nodes should, upon detection, not be forwarded by normal nodes.

Approach

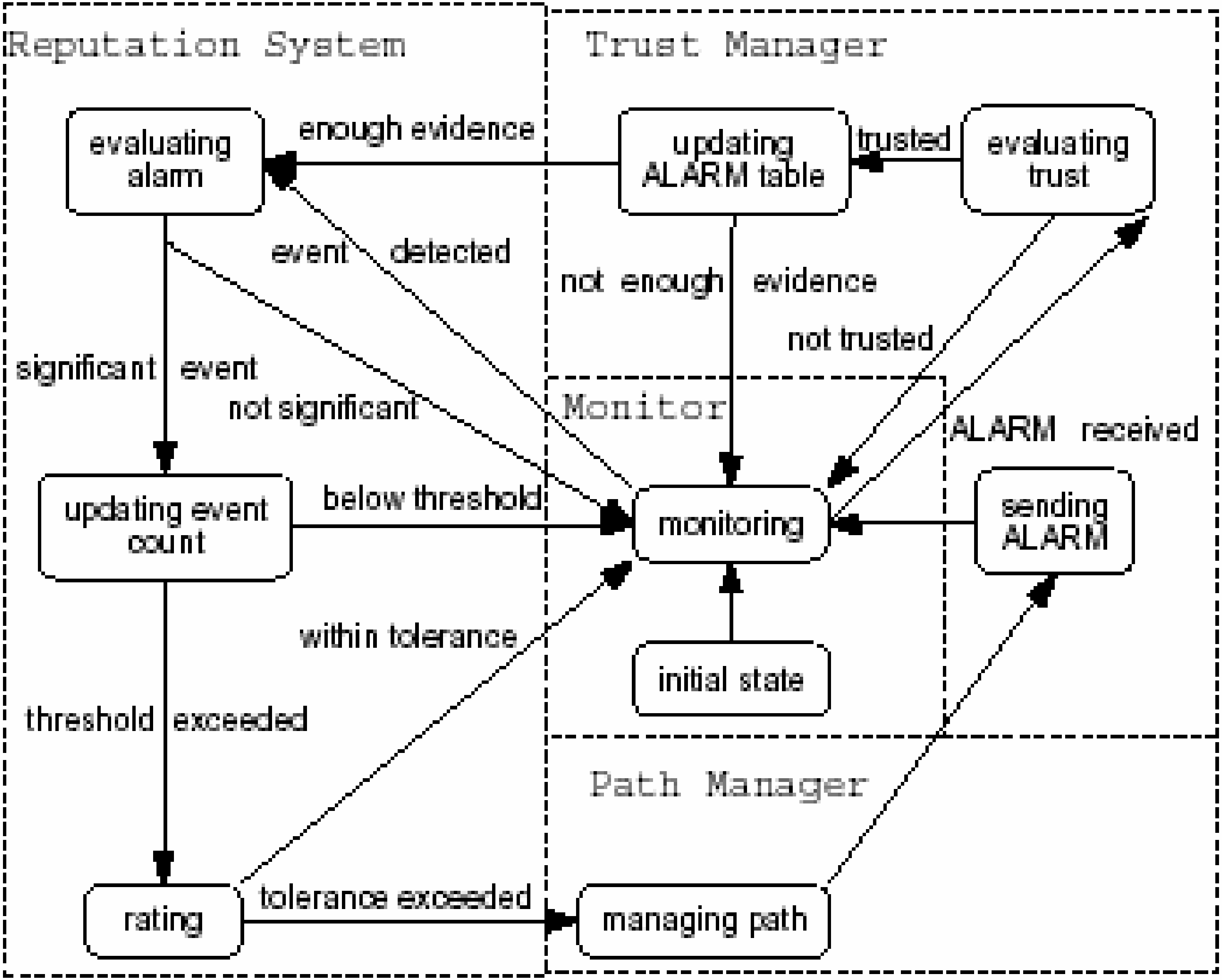
- It is based on an ecological analogy that is about reciprocal altruism, where you start with helping everyone, but then bear a grudge against those who do not return the favor and subsequently no longer help them. This ensures your survival over time.
- This is applied to nodes in an ad-hoc network where nodes forward on behalf of each other.

Approach

- The following ideas are incorporated in CONFIDANT to speed up triumph of grudger nodes:
  - Learn from observed behavior: employ ‘neighborhood watch’.
  - Learn from reported behavior: share information of experienced malicious behavior with friends and also learn from them.

Components

- CONFIDANT consists of the following components in each node:
  - The Monitor
  - The Reputation System
  - The Path Manager
  - The Trust Manager


Reputation System
Trust Manager
Monitor
Path Manager
evaluating alarm
enough evidence
updating ALARM table
trusted
evaluating trust
event detected
not enough evidence
not trusted
significant event
not significant
ALARM received
updating event count
below threshold
monitoring
sending ALARM
within tolerance
initial state
threshold exceeded
rating
tolerance exceeded
managing path

The Monitor

- The nodes most likely to detect misbehavior in a wireless network are the ones in the vicinity of the offender and in some cases the source and the destination.
- Here, nodes locally look for deviating nodes- *neighborhood watch*.
- Nodes of the neighborhood watch can detect deviations by the next node on the source route

The Monitor

- by using Passive Acknowledgement scheme or by observing route protocol behavior.
- The monitor within each node registers these deviations from normal behavior. When a given bad behavior occurs, the reputation system is called.

The Trust Manager

- This component deals with incoming and outgoing ALARM messages.
- ALARM messages are sent by the trust manager to warn other nodes of malicious nodes.
- Outgoing alarms are sent by a node to its friends after having experienced, observed or received a report of malicious behavior.

The Trust Manager

- Incoming alarms originate from either outside friends or other nodes, so the source of an alarm has to be checked for trustworthiness before triggering a reaction.
- A mechanism similar to the trust management in PGP is used here for determining if there is enough trusted evidence for the misbehavior of a node.

The Trust Manager

- The Trust Manager consists of the following components:
    - An alarm table containing information about received alarms.
    - A trust table managing trust levels for nodes to determine the trustworthiness of an alarm.
    - A friends list containing all friends a node potentially sends alarms to.

The Reputation System

- The reputation system manages a table of entries for nodes and their rating. The rating is changed only when there is enough evidence of malicious behavior that is significant for a node and that has occurred a no. of times exceeding a threshold to rule out coincidences.

Reputation System

- The rating is then changed as per a rate function that assigns different weights to the type of behavior detection, namely the greatest weight for own experience, a smaller weight for observations in the neighborhood and an even smaller weight for reported behavior.

Reputation System

- When the rating for a node has deteriorated so much as to fall out of a tolerable range, the Path Manager is called for action.
- The Reputation System is built on negative experience rather than positive impressions.

The Path Manager

- The Path Manager performs the following:
  - Path re-ranking according to security metric, such as reputation of nodes in the path.
  - Deletion of paths containing malicious nodes.
  - Action on receiving a request for a route from a malicious node such as deny.
  - Action on receiving a request for a route containing a malicious node in the source route.

Protocol Description

Each node monitors the behavior of its next hop neighbors. If a suspicious event is detected, the information is given to the reputation system. If the event is significant for the node, it is checked whether it has occurred more often than a predefined threshold. If so, the reputation system updates the rating of the node that caused the event. If the rating turns out to be intolerable, the information is relayed to the Path Manager. The node continues to monitor the neighborhood and an ALARM message is sent.

Protocol Description

- The ALARM message is sent by the trust manager. It contains the type of protocol violation, the no. of occurrences observed, if the message was self-originated, address of reporting node, the address of observed node and the destination address. In the simulation, the alarm is sent to the source.
- When the monitor component of a node receives such an alarm, it passes it to the Trust Manager where the source of the message is evaluated. If

Protocol Description

- the source is at least partially trusted, the ALARM table is updated. If there is sufficient evidence that the node reported is malicious, the reputation system is called.
- Here it is again evaluated for significance and accumulated reputation of the node. Sufficient evidence means either that the source of the ALARM is fully trusted or that several partially trusted nodes have reported the same and the respective trust adds up.

Performance Analysis

- Objective is to determine the impact of the CONFIDANT routing protocol extensions on metrics where part of the population acts maliciously.
- The Metrics used are Goodput, Overhead and Utility.
  - Goodput(G) = Total packets received/ Total packets originated

- Overhead(O) = Total Alarms $_{tx}$ / Total RREQ $_{tx.}$ + Total RREP $_{tx}$ + Error $_{tx.}$
- Utility (ui) = b_r total packets $_{Received}$ + b_s total packets $_{Sentsuccessfully}$ - c_f total packets $_{transmitted}$

Simulation Setup:

The first network analyzed is the regular DSR network that is used as reference. Then compromised nodes are introduced and then DSR fortified with CONFIDANT is used. Forwarding defection is studied. The simulation is implemented in GloMoSim. The mobility model used is the Random Waypoint Model.

The factors varied are the total no. of nodes in the network, the percentage of malicious nodes, the pause time and no. of applications.

Simulation Results

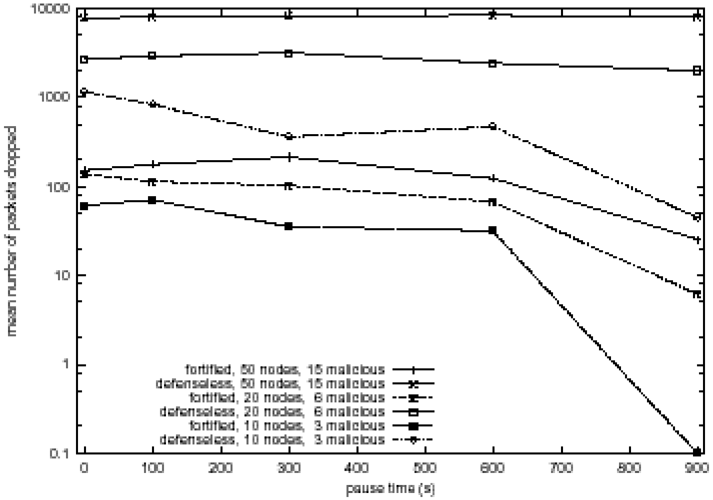


Figure 2: Mean number of packets dropped versus pause time.

- It is shown that the performance difference increases with the total no. of nodes in the network when considering the no. of packets dropped w.r.t network size . The fortified network keeps the no. of dropped packets fairly constant irrespective of network size whereas the defenseless one deteriorates with increase in size.
- The no. of applications is then increased and the percentage of malicious nodes varied and the same effect was observed.

Future Work

- How to win friends dynamically?
- The threshold value used to change a node’s rating.
- Methods to efficiently distribute reputation information to avoid malicious nodes as early as possible.
- CONFIDANT assumes that nodes are authenticated and that no node can pretend to be another. If a node is compromised then it could send ALARMs about a benign node to its neighbors and propagate this by pretending to be another node.

Conclusions

- New ways of distributing trust can be implemented by introducing the notion of friends and making cooperation payoff, which is what CONFIDANT does.
- This paper recognizes the requirements of mobile ad-hoc networks in terms of cooperation, robustness and fairness, and analyzes the performance of a scheme to cope by retaliating for malicious behavior and warning affiliated nodes to avoid bad experiences.