Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks

IEEE INFOCOM 2003

2003.3.13 林佑青
Outline

♦ Introduction
♦ Approach overview
♦ Message-forwarding protocol
♦ Routing discovery and multicast
♦ Evaluations
♦ Conclusion
Introduction

♦ In order to make an ad hoc network functional, the nodes are assumed to follow a self-organizing protocol. As a result, cooperation among the nodes must be considered.

♦ A selfish node is an economically rational node whose objective is to maximize its own welfare. Since forwarding a message will incur a cost to a node, a selfish node will need incentive in order to forward others’ messages.
The system uses credit to provide incentive to selfish nodes.

Determines charge and credit from a game-theoretic perspective, and motivates each node to report its actions honestly.

Model the system as a game and prove the correctness of the system under this model.
System architecture

Credit Clearance Service (CCS)

Internet

Wide-Area Wireless Network

Node 1

Node 2

Node 3

Node 4

Node 5
When a node sends its own messages, the node will lose credit to the network because other nodes incur a cost to forward the messages.

A node needs to report to the CCS which messages it has helped to forward.
Who pays whom?

♦ Charging only the sender will be a more robust and general approach.
♦ Any node who has ever tried to forward a message should be compensated, no matter successful or not.
♦ CCS believes that a node has forwarded a message if and only if there is a successor of that node on the path reporting a valid receipt of the message.
Objectives of the payment scheme

♦ Prevent cheating actions and to provide incentive for the nodes to cooperate.
♦ In order to prevent one type of cheating actions, CCS charges the sender more than it gives to the other nodes.
Cheating actions in the receipt-submission game

♦ After receiving a message, the node saves a receipt but does not forward the message.
♦ The node has received a message but does not report the receipt.
♦ The node does not receive a message but falsely claims that it has received the message.
Motivating nodes to forward messages

♦ 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.
Motivating nodes to report receipts

♦ The last node can collude with the sender, if the last node does not report its receipt, the sender saves $\alpha$ while the last node loses $\beta$.

♦ In order to prevent this cheating action, the CCS charges the sender an extra amount of credit if the destination does not report the receipt of a message.
Preventing false receipts

♦ To prevent such attack depends on the destination.
♦ Greatly reducing the amount of credit given to the intermediate nodes, if the message is not reported to be received by the destination.
Message-forwarding protocol

- Send \((m, p, seq_0(0,d), s)\) to the next node
- \(n_i\) receives \((m, p, seq, s)\), and checks three conditions:
  1. \(n_i\) is on the path
  2. the message has a sequence number greater than \(seq_i(0,d)\)
  3. the signature is valid

\[p = (n_0, n_1, \ldots, n_e, \ldots, n_d)\]
\(n_e\) is the last node
**Computing payments**

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

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

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

When the destination submits its receipt, the node will get its full credit of $\alpha$. 
A formal model and analysis

Players: \( n_0, n_1, \ldots, n_e, \ldots, n_d \)

Players’ information: 
\[
T_i = \begin{cases} 
\text{TRUE} & \text{if } 0 < i \leq e' \\
\text{FALSE} & \text{if } e' < i \leq d 
\end{cases}
\]

Actions: \( A_i = \text{True or False} \)

Cost of Actions: 
\[
U_i = \begin{cases} 
\delta & \text{if } T_i = \text{FALSE} \text{ and } A_i = \text{TRUE} \\
0 & \text{otherwise.}
\end{cases}
\]

Payment: 
\[
P_i = \begin{cases} 
\alpha & \text{if } i < e = d \\
\beta & \text{if } i = e = d \\
\gamma \alpha & \text{if } i < e < d \\
\gamma \beta & \text{if } i = e < d.
\end{cases}
\]

Welfare: 
\[
W_i = P_i - U_i
\]
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.
Analysis of performance

- An intermediate node can expect a net gain of:
  \[ p_2 \alpha + (p_1 - p_2) \gamma \alpha + (1 - p_1) \gamma \beta - \gamma \beta \]
  \[ \equiv p_2 (1 - \gamma) \alpha + p_1 \gamma (\alpha - \beta) > 0 \]

\( p_1 \) is the probability that the message arrives at the next node,
\( p_2 \) is the probability that the message arrives at the destination.
Route discovery and multicast

- CCS builds a tree based on the accepted ROUTE REQUEST messages.
Evaluations

Effects of battery on message transmission

Message success rate

B

simulation: number of nodes=70
simulation: number of nodes=200
analysis: L=3
Evaluations (cont.)

Message transmission dynamics

Message success rate

#generated packets

B=100
B=500
Conclusion

- Sprite, a system to provide incentive to mobile nodes to cooperate.
- Simulations and analysis showed that the nodes can cooperate and forward each other’s messages, unless the resource of the nodes is extremely low.