MobileAds: Advertisement on Mobile Devices

Wenbo He
Department of Computer Science
University of Illinois at Urbana Champaign

Klara Nahrstedt
Department of Computer Science
University of Illinois at Urbana Champaign

Abstract

We study the requirements and challenges that arise in the mobile advertisement applications, which are more and more anticipated and will bring great societal and economic impact in the future. The goal of advertisement is to reach largest possible target population. Hence, we propose a reliable and robust message propagation protocol in this paper.

1 Introduction

Due to the proliferation of mobile devices, such as PDAs, GPS devices, cell phones, and laptops, there is a growing demand for reliable message propagation protocols for imminent commercial purposes. For example, in *Mobile Advertising* applications, department stores/service providers/sellers desire to advertise goods/immediate sales across customers who carry mobile devices. There are lots of potential benefits from mobile ads, especially in the quick service oriented industry. Image the scenario that on your wife's/husband's birthday, you need to get a birthday cake, a gift, and a dozen of roses before you go home and celebrate the birthday. Wouldn't it be great if on you way home from the office, a mobile device shows you the nearest and/or cheapest bakery and floral shops, and direct you to pick up the right things you need. Mobile ads technology is expected to change the way we do business, interact with each other, and navigate through our daily lives. With mobile ads platform, advertisers can conveniently delivery electronic coupons to potential customers, can easily track the percentage of consumers that actually took advantage of a particular offer. On the other hand, customers are able to acquire commercial product or service information through mobile devices. In mobile ads platform, there is close integration between Internet and mobile devices, tight coupling between communication and computing, and urgent demand of security and reliability. However, in this essay, we focus on the problem of mobile advertisement propagation.

The ad hoc mobile advertising propagation has the following major requirements:

- First, the relevant messages must be distributed in an inexpensive and efficient manner. That means we need optimized transmission of advertisement content throughout mobile devices.
- Second, security of commercial advertisement messages is a big concern. The mobile ads platform should be able to detect and/or prevent various attacks, such as DoS attacks and impersonation attacks. In the former, attackers propagating dummy/fake advertisements through out the network; in the latter, an attacker pretends to be one or more legitimate users by fabricating or stealing identities.
- Third, some mobile device users can be selfish and they may refuse to propagate advertisements to other users. Hence, the mobile advertisement message propagation should be reliable and tolerate a portion of selfish nodes. Further more, we may need proper incentives to encourage advertisement message propagation.

2 Proposed Solution for Mobile Ads Propagation

Figure 1 depicts the system architecture for mobile advertisement propagation. In this architecture, we use *mobility assisted message propagation* component to achieve efficiency, reliability and robustness of advertisement message propagation. *Authentication* is an important component in the architecture to verify identity of message senders and forwarders, therefore it helps acquiring statistics about mobile devices, and further helps keeping track of behaviors of mobile users and reinforcing security. *Advertisement Propagation Management* component controls the parameters of mobility assisted message propagation, and optimizes the ads propagation with minimum transmission overhead.

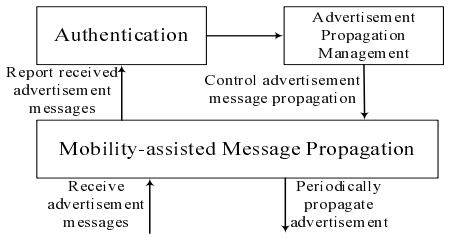


Figure 1. System architecture of Mobile Ads message propagation

Due to the page limit, we focus on *mobility-assisted message propagation* in this section. The goal of mobile ad-

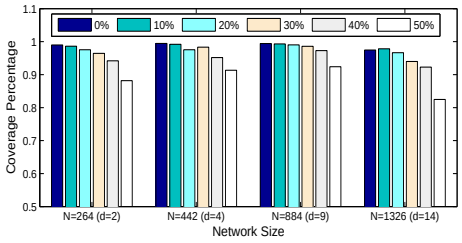
vertisement is to reach largest potential customers through mobile ad hoc networks (MANETs) or vehicular ad hoc networks (VANETs). Our solution is inspired by the wide spread of dandelion seeds. When a puff ball bursts, dozens of floating seed-bearing parachutes fly with wind across its neighborhood, and may travel a long distance before landing. In this way, dandelion flowers proliferate everywhere. We borrow this idea to achieve efficient message propagation at the cost of the acceptable delivery latency. In our mobility-assisted message propagation protocol, messages are carried by mobile nodes, which mimics that dandelion seeds are carried by floating parachutes. When the parachutes travel a certain distance, the dandelion seeds are brought to a new neighborhood. As dandelion seeds landed on ground, they grow and further propagate later on. Similarly, due to the node mobility, mobile nodes bring the messages to a new neighborhood within a certain period of time. When new neighbors hear the message, they will further propagate the message. Our proposed message propagation protocol relies on periodically retransmission of messages by mobile nodes. The key design issue is when to terminate the propagation of a message, so that the message is able to reach all the network nodes without consuming extra bandwidth. We adopt a parameter *times-to-send (TTS)* to control the termination of message propagation. A *times-to-send (TTS)* field is included in the header of a message. In each step, when a mobile node retransmits a message, *TTS* value is reduced by one. When *TTS* reaches zero, nodes stop forwarding the message. Hence, the message propagation procedure is terminated. We want to design the initial *TTS* value properly, so that a message can be disseminated to almost all network nodes with a high probability, but any smaller *TTS* value cannot attain such high coverage of message delivery.

3 Preliminary Simulation Results

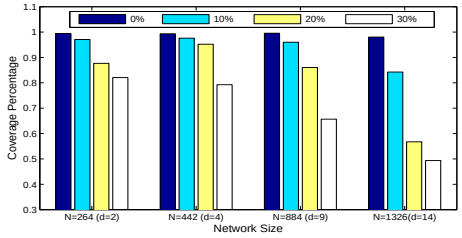
3.1 Against Selfish Nodes

If a portion of selfish nodes suppress the transmission of an advertisement message, other message carriers still actively forward the message until its *TTS* reaches zero. When a single message carrier forwards a message, all the nodes in its neighborhood can receive the message. Hence, our proposed protocol is able to tolerate non-trivial portion of selfish nodes. We use small-scaled simulations to verify this property of the protocol. In our simulation scenario, we assume that advertisers are trying to disseminate ads in a square area with edge length $L = 500meter$ ($|\mathcal{A}| = L \times L$). We use variant transmission range r and the network size $\mathcal{N}$ to simulate different network diameters and different node densities in the network. We randomly select a node to initiate the message to be propagated. The node density of a network is represented by the average degree d. Both malicious nodes and legitimate nodes follow *Random WayPoint*, and moving speed of a node is from $0.5\ mps$ to $5\ mps$.

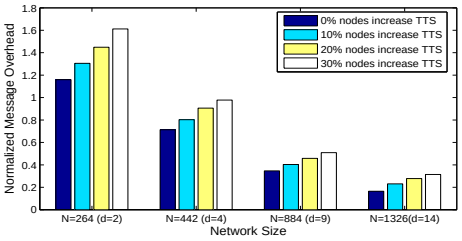
Figure 2(a) illustrates the percentage of nodes received the advertisement message under different portion of the selfish nodes.



(a) Against selfish nodes



(b) Against malicious nodes which decrease the TTS



(c) Normalized message overhead under attacks where a portion of malicious nodes increase TTS values

Figure 2. Robustness of the protocol

3.2 Against Malicious Nodes

Next, we consider attacks where malicious nodes attempt to modify *TTS* values during ads propagation.

Figure 2(b) depicts the average coverage of advertisement messages (percentage of nodes which receive the advertisement), when a certain percent of nodes maliciously replace TTS value with zero in order to prevent message propagation. Figure 2(c) demonstrates *normalized message overhead*[1] under the TTS manipulating attack, where a portion of malicious nodes double TTS value to trigger extra unnecessary transmissions. From the simulation result, we conclude that the increment of message overhead under such malicious attack is moderate. Judging from Figure 2(b) and 2(c), we can conclude that the protocol is robust to malicious attacks which try to manipulate TTS values.

4 Discussions and Future Work

There need much more efforts to develop a complete platform of mobile ads systems, where efficiency, security and reliability are big concerns. We expect much work in the near future to address these concerns.

[1] *normalized message overhead*$= \frac{\#\ of\ transmissions}{\#\ of\ nodes\ which\ received\ the\ ads\ message}$.