Ad Hoc Networks 26 (2015) 69–87

Contents lists available at ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

Protecting data flow anonymity in mobile ad hoc networks that employ cooperative caching

Noor Abbani, Hassan Artail *

Department of Electrical and Computer Engineering, American University of Beirut, P.O. Box 11-0236, Riad El-Solh, Beirut 1107 2020, Lebanon

ARTICLE INFO

Article history:
Received 25 February 2014
Received in revised form 29 August 2014
Accepted 29 October 2014
Available online 4 November 2014

Keywords:
Data caching
Privacy
Anonymity
Data communications
MANETs

ABSTRACT

Caching systems have been proposed for mobile ad hoc networks (MANETs) to increase data availability and reduce data access delays. However, such caching systems can expose the identities of the participants and have their interests profiled. In this work, we propose a privacy preserving system for caching systems in MANETs, and consider as a test case a caching architecture that was proposed earlier by one of the authors. The system protects the privacy of the nodes that request data and those that provide it by offering source and destination anonymity, thus hiding their identities from other nodes in the caching paradigm and from the service provider. Our system was implemented using ns-2 and was found to achieve high values of anonymity with mitigated delays and overhead traffic.

1. Introduction

Mobile ad-hoc networks (MANETs) require the cooperation of nodes in forwarding and routing each other's packets to achieve application functionalities. In caching applications, specifically, nodes cooperate to cache data items, answer queries, or send them to the data server. This cooperation exposes the data and the nodes to other nodes, leading to privacy breaches. It is well recognized that data caching is essential in MANETs as it improves overall system performance [10,32]. Typically, several mobile devices cache data that other devices frequently access or query. Essentially, all proposed caching architectures for MANETs suffer from privacy violations that enable attackers to profile users. We elaborate on this point in the following section, and use an illustrating scenario to prove the need for privacy protection in MANET environments that offer data caching services.

According to [5], privacy means that one can control when, where, and how information is used and by whom. However, it does not mean that one must hide personal information from all others, but rather, he or she needs to show the right information to the right people. For example, a patient must share his sensitive information with his doctor. This scenario, similar to many others, shows how privacy is applied, as a party reveals its identity and data to other parties on a need to know basis. Wireless mobile networks provide unique challenges to privacy as compared to wired networks. Two privacy goals are sought in such networks: communication privacy and location privacy. The first is related to controlling access to the actual message content and information that describe the source, destination, and flows. Considerable research on this issue has been done, but the proposed approaches mainly resort to data encryption to protect the message content. Location privacy, on the other hand, relates to protecting the privacy of the participating nodes in the network, since revealing their locations might lead attackers to learn information about their movements.

In the same context, communication privacy preserving systems, such as those described in [8,9,22], seek to ensure

* Corresponding author.
E-mail addresses: nma51@aub.edu.lb (N. Abbani), hartail@aub.edu.lb (H. Artail).

http://dx.doi.org/10.1016/j.adhoc.2014.10.018

many objectives, including anonymity, untraceability, and unlinkability. Anonymity, such as sender anonymity and destination anonymity, is about hiding the user that performed a certain action among nodes that performed similar actions, whereas untraceability is about making the adversary unable to identify a set of actions as having been performed by the same node. On the other hand, unlinkability is the inability to link a sender and a receiver as communicating with each other [5]. In this work, we seek to achieve the above objectives through realizing communication privacy for caching applications in mobile ad hoc networks.

From a different perspective, The work in this paper serves to complete a line of research that began with [2] which introduced the base cooperative caching system (COACS), and then extended it with semantic caching in [26] and with replication in [15]. We also added consistency provisions to it using a server-based approach in [25] and also using a client-based scheme in [16]. In [14] we surveyed and analyzed a number of caching frameworks for MANETs and concluded the need for a privacy preservation scheme to prevent profiling users' interests. That work proposed a simple system with basic experimental evaluation, but was followed by the work in [1] that expanded on [14] by adding further privacy capabilities that aimed at removing the association between being a caching node for a data item, and having requested that particular item in the past. This paper describes a more complete system that is comprehensively analyzed and evaluated. More specifically, it offers the following contributions relative to our earlier work in [1]:

1. It proves the need for ad hoc networking, and effectively justifies the need for anonymous communication for caching systems in MANET environments, in general, and for the COACS framework in particular.
2. It experimentally demonstrates the vulnerability of COACS to anonymity attacks through ns2 simulations.
3. It presents the system model in a simpler but yet more effective way.
4. The threat model in [1] did not consider receiver anonymity explicitly, while the work presented in this paper does. This was discussed throughout the paper, and described in the middle paragraph of Section 4.6. Moreover, it provides a better definition of the threat model, by outlining the considered anonymity attacks, the employed mechanisms to mitigate them, and the anonymity types they fall under.
5. It adds request hopping to the proposed system which serves to enhance its anonymity protection feature.
6. It adds the capability of handling node disconnections due to mobility, which improves the robustness of the system.
7. Several of the concepts in [1] were expanded and clarified in this work (e.g., the threat model depicted in Fig. 4, and the encryption levels in the packets, shown in Fig. 5).
8. The experimental results in this paper were obtained from a new set of simulation experiments based on the truncated Levy walks (TLW) mobility model, in contrast to the old random way point (RWP) mobility model used in [1]. Moreover, the plotted results are now more presentable and informative.
9. An important aspect of the system is scalability, which was analyzed in this paper, but was not discussed in [1].

On the other hand, the novelty of our proposed work is can be summarized by the following:

- It integrates a collection of privacy and anonymity schemes into a coherent solution, adapted to provide anonymity services to a caching framework [2] that was proposed earlier by one of the authors and has become well cited in the literature. The system in [2] has a given architecture composed of caching nodes and directory nodes that communicate among each other according to a particular protocol, and hence, adapting the devised solution to this distributed system can be regarded as a contribution. As a matter of fact, a similar strategy has been followed in the literature, as we describe in Section 3: mixes were applied to offer anonymous MANET routing, like in [9,22,33]; to authenticate MANET users wanting to access the Internet, as in [3]; and to protect specific applications from privacy attacks, like in [17,18,34].
- It proposes a more comprehensive protection framework than the majority of schemes in the literature by (1) providing both sender and receiver anonymity services; (2) considering local, global, and colluding attackers (Sections 4.2 and 3) extending mixes techniques with "auxiliary functions", like request hopping (Section 4.3), piggybacking (Section 4.4), encryption and hop modification (Section 4.5), and fake messages by the recipient (Section 4.6).
- It offers a comprehensive analytical anonymity and delay analysis using a proposed anonymity metric, in addition to the experimental evaluation.

2. Background and motivation

Mobile ad-hoc networks (MANETs) are suited for use in situations where an infrastructure is unavailable, or to deploy one is not cost effective. They are also appropriate in places where the need for collaborative computing is important, such as in a business meeting outside the office, or essential, like in disaster areas or combat scenarios. A MANET can be setup to provide crisis management services, like disaster recovery, where major parts or the entire communication infrastructure is destroyed, and restoring communication quickly is crucial. Another classical example is combat scenarios where military operations are often spontaneous and require quick network establishment, accurate positioning (e.g., using triangulation), and where network security is essential especially when the ground troops are deployed in or near residential areas. In such cases, a system like the one we propose in this