Computer Communications 48 (2014) 111–120

Contents lists available at ScienceDirect

Computer Communications

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

Resilience and opportunistic forwarding: Beyond average value analysis

Fredrik Bjurefors [a,*], Merkourios Karaliopoulos [b], Christian Rohner [a], Paul Smith [c], George Theodoropoulos [b], Per Gunningberg [a]

[a] Uppsala University, Department of Information Technology, Box 337, 75105 Uppsala, Sweden
[b] Center for Research and Technology Hellas, 38334 Volos, Greece
[c] AIT Austrian Institute of Technology, 2444 Seibersdorf, Austria

ARTICLE INFO

Article history:
Available online 16 April 2014

Keywords:
Opportunistic networking
Forwarding
Routing
Simulations

ABSTRACT

Opportunistic networks are systems with highly distributed operation, relying on the altruistic cooperation of highly heterogeneous, and not always software and hardware-compatible, user nodes. Moreover, the absence of central coordination and control makes them vulnerable to malicious attacks. In this paper, we study the resilience of popular forwarding protocols to a representative set of challenges to their normal operation. These include *jamming* locally disturbing message transfer between nodes, *hardware/software failures* and incompatibility among nodes rendering contact opportunities useless, and *free-riding* phenomena. We first formulate and promote the *metric envelope* concept as a tool for assessing the resilience of opportunistic forwarding schemes. Metric envelopes depart from the standard practice of average value analysis and explicitly account for the differentiated challenge impact due to node heterogeneity (device capabilities, mobility) and attackers' intelligence. We then propose heuristics to generate worst- and best-case challenge realization scenarios and approximate the lower and upper bounds of the metric envelopes. Finally, we demonstrate the methodology in assessing the resilience of three popular forwarding protocols in the presence of the three challenges, and under a comprehensive range of mobility patterns. The metric envelope approach provides better insights into the level of protection path diversity and message replication provide against different challenges, and enables more informed choices in opportunistic forwarding when network resilience becomes important.

1. Introduction

In opportunistic networks, nodes store, carry, and forward messages when they encounter other nodes using short-range wireless communication. This store-carry-forward (SCF) transport service enables the data flow in the network despite the absence of simultaneous end-to-end connectivity. Yet, the network is a system with highly distributed operation, relying on the good will and cooperation of highly heterogeneous, and not always software and hardware-compatible, user nodes. Moreover, the absence of central coordination and control makes it an easier target for malicious attacks.

Inherent resilience against these challenges to the network operation is provided by data replication. Ideally, data travel in the network over diverse space–time paths, involving disjoint physical spaces and different network nodes. In practice, however, the actual data transfer diversity is highly dependent on the mobility patterns of nodes and the rules of the particular forwarding protocol. In general, forwarding protocols prioritize different performance characteristics such as message delivery ratio or buffer usage, and assign different importance to individual nodes during the data transfer. This, in turn, may render them more vulnerable to a particular type of challenge and more resilient to another.

In general, the performance degradation of opportunistic forwarding in the presence of challenges has been dealt with in literature both analytically [1–3] and with simulations [4–6]. Common to all these works is that the opportunistic forwarding performance in the presence of a challenge is assessed through averages values of the performance metrics, usually computed over several simulation runs.

On the contrary, in this paper, we compute and plot *metric envelopes*, whose upper and lower bounds reflect the best- and worst-case response of a metric, *e.g.*, message delivery ratio, to different realizations of a challenge. The motivating remark is that a simple challenge, such as "*K* selfish nodes" or "*M* jamming devices" can have a widely different impact on the performance of the opportunistic forwarding, depending on *which K* nodes behave selfishly or

* Corresponding author.
E-mail addresses: fredrik.bjurefors@it.uu.se (F. Bjurefors), mkaraliopoulos@iti.gr (M. Karaliopoulos), christian.rohner@it.uu.se (C. Rohner), paul.smith@ait.ac.at (P. Smith), per.gunningberg@it.uu.se (P. Gunningberg).

http://dx.doi.org/10.1016/j.comcom.2014.04.004
0140-3664/

where the M jammers will be physically placed. The metric envelopes implicitly account for the heterogeneity of the opportunistic network nodes in terms of device capabilities and mobility patterns, as well as the varying intelligence of attackers. At the same time, they provide insights that single average values do not. The breadth of the envelope is an indication of how predictably a protocol will perform in the presence of a given challenge; or, equivalently, how much risk is involved in using the protocol in this case. Hence, a protocol with tight metric envelopes may be occasionally preferable to another with better average scores but higher spread of values.

Drawing on earlier work in [7] we use metric envelopes to assess the resilience of three popular forwarding protocols to three representative types of challenges: occasional *software/hardware failures*, *e.g.*, due to incompatibility of the software/hardware the encountered devices may use; intentional *jamming*, a typical example of malicious behavior; and *free-riding*, is a classical instance of non-cooperative behavior emerging in networked settings lacking central coordination and control functionality. The *exact* computation of the metric envelope values for these challenges would require enumerating *all* possible challenge realizations, *e.g.*, combinations of K selfish nodes or placements of the M jammer nodes in the physical space. Clearly such an enumeration becomes computationally intractable already for moderate and even small values of K and M. Therefore, we propose heuristics (cues) for *inferring* "best"- and "worst"-case scenarios for each challenge and *approximating* the respective metric envelopes. The derivation of best- and worst-case partitioning of nodes into software/hardware compatible groups are formulated as instances of the community detection and weighted coloring problems, respectively; jammers are placed in the areas that rank highest (resp. lowest) with respect to the density of encounters; and free riders are let coincide with the most (least) central nodes with respect to message delivery.

We demonstrate the use of envelope metrics and the additional information they can deliver through simulation scenarios with various synthetic and experimental mobility traces. The envelopes can provide arguments in favor of one protocol over the other when they are indistinguishable with respect to average performance values. Their width provides an indication of how much performance differentiation is possible in the presence of a given challenge and given node mobility patterns and how well random simulation runs may fail in predicting the impact of a challenge.

In summary, the contributions of this paper are highly methodological and include: (i) the formulation and promotion of the metric envelope concept as a tool for assessing the resilience of opportunistic forwarding schemes in a way that explicitly accounts for the node heterogeneity (device capabilities, mobility), and when relevant, attacker's intelligence (Section 2); (ii) the proposal of heuristics for approximating the worst- and best-case scenarios for representative challenges (Section 3); and (iii) the demonstration of the methodology in the assessment of three popular forwarding protocols under different challenges and mobility patterns (Section 4). We position this work within the broader literature on opportunistic network resilience in 5 and discuss research directions out of it in Section 6.

2. Assessing resilience: envelopes instead of average values

To assess the performance of forwarding protocols, we consider two standard performance metrics, the message delivery ratio and delay. The message delivery ratio equals the fraction of messages that reach their destinations out of those generated at their sources (ignoring replicas). For every delivered message, message delay equals the time elapsed between the message generation epoch and its arrival at the destination node.

However, and contrary to earlier studies in literature, we are interested in the full range of values a metric can obtain in the presence of a challenge. For example, the impact of K free-rider nodes may vary considerably depending on the importance of the specific K nodes that exhibit this behavior for the forwarding process. Likewise, there are many different ways to place K jammer nodes with jamming radius r_{jam} in the physical space, each placement affecting differently the forwarding operation.

To introduce some terminology that is necessary for the rest of the paper, jamming is a *challenge instance*, which is parameterizable by certain variables such as the number of jamming nodes and their jamming radius. We use the term *challenge realization* to denote a specific implementation of a challenge; for example, a jamming realization describes where exactly the K jamming nodes with jamming radius r_{jam} are placed. On the other hand, *challenge parametrization* denotes the full set of all possible challenge realizations for given values of the challenge parameters. Therefore, "K jammers of radius r_{jam}" is a challenge parameterization, *i.e.*, a shortcut term for all possible challenge realizations involving K jammers of r_{jam} jamming radius.

An example metric envelop diagram is shown in Fig. 1 for a single-parameter challenge. It plots the best- and worst-case values of a metric as the challenge parametrization varies, whereby performance is assumed to be monotonically increasing with the metric value. Each single point at the x-axis corresponds to a certain parametrization and the respective best- and worst-case values enclose (hence, the term envelope) the outcomes of all its realizations. The intermediate curve, between the best- and worst-case, corresponds to the outcome of a random realization or the average of more than one random challenge realizations.

The motivation for promoting envelop diagrams over single average-value curves roots back to longtime practices in engineering different entities, ranging from a single link [8] to a whole system [9]. In all cases, the requirement is to secure an availability of some nines (*e.g.*, three nines corresponds to an availability of 99.9%). Hence, it is much more important for an engineer/designer to know how often performance degrades below some threshold and plan for countermeasures that can make up for this degradation. In the case of opportunistic networks, envelop diagrams explicitly account for the heterogeneity of network nodes with respect to their mobility and hardware/software capabilities and add another dimension to the comparison of the opportunistic forwarding protocols. Since the spread of the envelope is also a measure of the uncertainty/risk related to a certain challenge parametrization, it is possible that one forwarding protocol be preferable to another with higher average performance but broader envelope.

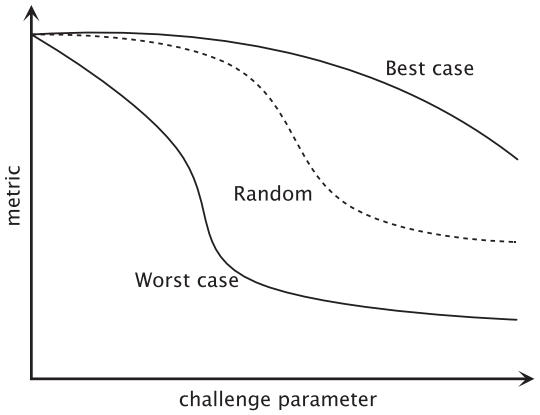

Fig. 1. Metric envelope.