Chapter 19
Reducing Blocking Risks of Atomic Transactions in MANETs Using a Backup Coordinator

Joos-Hendrik Böse
International Computer Science Institute Berkeley, USA

Jürgen Broß
Freie Universität Berlin, Germany

ABSTRACT
In this paper, the authors present a probabilistic model to evaluate the reliability of the atomic commit for distributed transactions in mobile ad-hoc networks (MANETs). This model covers arbitrary MANET scenarios as well as strict and semantic transaction models. The authors evaluate the approach to integrate a backup coordinator to reduce blocking risks. For the purpose of showing an example of a MANET scenario, the authors illustrate how the considered blocking probability is very low.

1. INTRODUCTION
To provide for robustness and reliability of applications deployed to volatile environments such as MANETs, transaction processing is a key concept. Atomic transactions guarantee consistency of data and system states. Our belief is that MANETs are a fundamental building block of ambient computing environments. Several types of applications in ambient computing environments demand for atomicity guarantees, e.g., trading applications require money and goods atomicity when virtual goods, for example a music file, are exchanged for virtual money with persons nearby. Guaranteeing atomicity of such a distributed transaction requires agreement among transaction participants on the outcome of the transaction. This is typically achieved by an atomic commit protocol (ACP). It is generally known that in the presence of node or communication failures such protocols cannot avoid blocking (Skeen & Stonebraker, 1983). While in fixed networks such situations are rare

DOI: 10.4018/978-1-4666-0038-6.ch019
Reducing Blocking Risks of Atomic Transactions in MANETs Using a Backup Coordinator

due to low probabilities of site and communication failures, ambient computing scenarios are a more challenging environment.

Generally, a blocking situation arises when participants can no longer terminate their transaction branch independently, but are forced to wait until they can learn about the global transaction decision. Compared to ACPs tailored to MANETs like (Böse et al., 2005; Gruenwald & Banik, 2001), the use of a backup coordinator (BC) (Reddy & Kitsuregawa, 1998) is a more lightweight strategy to compensate for blocking. However, it is unclear whether the use of a BC is generally beneficial in a MANET scenario, as it introduces an additional source of failure. In this article we provide an in-depth analysis of the BC scheme for MANETs. We present a calculation model to answer the question whether blocking is a relevant problem in a specific MANET and transaction scenario and thus may require use of a BC. Additionally, the model then allows predicting to which degree blocking is reduced.

The remainder of this article is structured as follows: Section 2 introduces our system and failure model as well as the strict and semantic transaction model used within later sections. For both transaction models the integration of a backup coordinator is described. Section 3 presents an example MANET scenario and derives node and communication failure probabilities for this scenario. In Section 4 we describe a calculation model to estimate the risk of blocking situation caused by a node failure of the transaction coordinator and enhance the model to estimate the reduction of this risk if a backup coordinator is used in strict and semantic transaction models. Finally, Section 5 summarizes and concludes the article.

2. SYSTEM AND TRANSACTION MODEL

2.1 System and Failure Model

A MANET $A$ is established between nodes located in a specific area. Due to node and communication failures, we do not assume that $A$ is fully connected. For each node a chance exists to completely leave the area and thus to disconnect from $A$. We describe the probability for this event to happen until time $t$ by the cumulative distribution function (cdf) $FL(t)$. We assume that a multi-hop routing protocol, such as AODV or DSDV, is used. Although message delays in $A$ depend on the hop count of communication paths, for sake of simplicity, we assume an average message delay $\delta_m$ for all messages.

Communication characteristics of $A$ are captured by the cdf $Fc(t)$, describing the probability that a communication path breaks until time $t$. In the following we refer to this time as path duration. The according probability density function (pdf) is denoted by $fc(t)$. Note that in this article we do not consider the case that a link may recover. In addition to communication failures, a node may suffer from exhausted energy resources or general technical failures. For these events we assume cdfs $FE(t)$ and $FT(t)$. Given the assumptions above, the proposed probabilistic failure model covers the following two types of failures:

**Node Failures** denote all events that cause a node to disconnect from $A$. Hence, $FN(t)$, the cdf of a node failure until time $t$, is given by the probability that a node leaves $A$, exhibits exhausted energy resources or suffers from a technical failure until $t$. $FN(t)$ is calculated by considering complementary probabilities:

$$FN(t) = 1 - (1 - FL(t))(1 - FE(t))(1 - FT(t)).$$

**Communication Failures** cause the break of a communication path that was functional before. The failure of the link is induced by mobility or by node failures of relaying nodes. The cdf for a communication failure is denoted by $Fc(t)$. We