Byzantine-Tolerant, Information Propagation in Untrustworthy and Unreliable Networks

Kai Han[1], Binoy Ravindran[1], and E. Douglas Jensen[2]

[1] ECE Dept., Virginia Tech, Blacksburg, VA, USA
{khan05,binoy}@vt.edu
[2] The MITRE Corporation, Bedford, MA, USA
jensen@mitre.org

Abstract. In a decentralized network system, an authenticated node is referred to as a Byzantine node, if it is fully controlled by a traitor or an adversary, and can perform destructive behavior to disrupt the system. Typically, Byzantine nodes together or individually attack point-to-point information propagation by denying or faking messages. In this paper, we assume that Byzantine nodes can protect themselves from being identified by authentication mechanisms. We present an authentication-free, gossip-based application-level propagation mechanism called LASIRC, in which "healthy" nodes utilize Byzantine features to defend against Byzantine attacks. We show that LASIRC is robust against message-denying and message-faking attacks. Our experimental studies verify LASIRC's effectiveness.

1 Introduction

In a decentralized, network-based information system, nodes communicate with each other through point-to-point information propagation (i.e., directly sending messages to destination nodes without receiving help from a server). The propagation may suffer attacks from malicious nodes hiding in the system. Attacks where a traitor or an adversary has full control of an authenticated device, and can perform destructive behaviors to disrupt the system are referred to as Byzantine attacks [1]. A node showing Byzantine behaviors is called a Byzantine node. Byzantine nodes are more difficult to deal with than other attackers [2].

We consider network systems where authentication mechanisms (including any kind of encryption) are unable to defend against Byzantine attacks [3]. Since Byzantine nodes are authenticated, in any authentication process, they act just like other nodes. Therefore, a "healthy" node cannot trust its peers — it does not know whether another node is a friend, a traitor, or an adversary. Further, we assume that Byzantine nodes are intelligent—i.e., if a Byzantine node cannot protect itself from being identified by others, it will not attack. For instance, it is less possible for an attacker to fake a reply message during a request message propagation process, because such an attack will finally be identified by the real reply node (we discuss this attack scenario in Section 2.2). In the rest of the paper, we use the terms "Byzantine nodes" and "Byzantine attackers", interchangeably.

T. Enokido, L. Barolli, and M. Takizawa (Eds.): NBiS 2007, LNCS 4658, pp. 207–216, 2007.

We focus on application-level Byzantine attacks in *request-reply* message propagation. A node initiates such a process by sending REQUEST (REQ) messages to others, trying to get a "YES"/"NO" answer from them (e.g., requesting a service that it cannot provide [4]). A knowing receiver responds by sending back REPLY (REP) messages, indicating its answer to the sender. Byzantine nodes may attack both processes by denying or faking messages (e.g., faking requested service ID in a REQ message, faking "NO" for an "YES" answer in a REP message, or directly faking REP messages). Furthermore, we consider information systems that use *unreliable networks* (e.g., those without a fixed network infrastructure, including mobile, ad hoc and wireless networks) with dynamically uncertain properties. These uncertain properties, which are application- and network-induced, include arbitrary node failures, transient and permanent network failures, and varying packet drop behaviors. Example such systems that motivate our work include US DoD's Network-Centric Warfare system [5].

In this paper, we present LASIRC, a Byzantine-tolerant, gossip-based, point-to-point application-level information propagation model/mechanism. Gossip mechanisms are well-known for their robustness to propagation uncertainties in unreliable networks [2,6]. A node initiates a gossip process by starting a series of synchronous gossip rounds. During each round, nodes holding REQ messages randomly select a set of neighbors and send REQ messages to them. The number of gossip rounds (or R), and the number of selected neighbors (i.e., the "fan-out" number, or F) are determined by the original sender. If a receiver knows the answer, it gossips REP messages back. Message losses and node failures may happen during a gossip process. However, gossip "fights" non-determinism (i.e., unpredictable message losses and node failures) with non-determinism (i.e., randomly selecting sending targets) — duplicated REQ and REP messages guarantee the normal information propagation. Our gossip-based LASIRC model/mechanism also features this same robustness, and makes LASIRC robust against Byzantine message-denying attacks, as these attacks can be regarded as message losses/node failures (Byzantine attackers receive, but do not forward messages). In addition to message-denying attacks, LASIRC also provides a set of mechanisms to detect and defend Byzantine message-faking attacks.

The rest of the paper is organized as follows: In Section 2, we discuss possible Byzantine attacks in the LASIRC model. We then present our Byzantine attacker detectors in Section 3. Sections 4 describe and analyze the LASIRC model and mechanism, respectively. In Section 5, we report on our experimental (simulation) studies. We conclude the paper in Section 6.

2 Byzantine Attacks

We describe the REQ and REP message structures, discuss Byzantine attack types (denying and faking messages), and possible Byzantine attacks in REQ and REP message propagation under gossip protocols.

Message Structures. A REQ message contains the original sender's (the request node) IP, the intermediate node's (message-transferring node in gossip