Protecting Internet Public Information Integrity during Transmission

Jyh-haw Yeh

Dept. of Computer Science, Boise State University

Chung-wei Lee

Dept. of Computer Science & Software Engineering, Auburn University

Wen-chen Hu

Dept. of Computer Science, University of North Dakota

INTRODUCTION

Phenomenons:

1. **A popular site may incur a large volume of requests**

2. **Transmitted information may need to be protected**

   Authentication, privacy, integrity, ...

Objectives:

1. **Design a Fault Tolerant Public Site:**

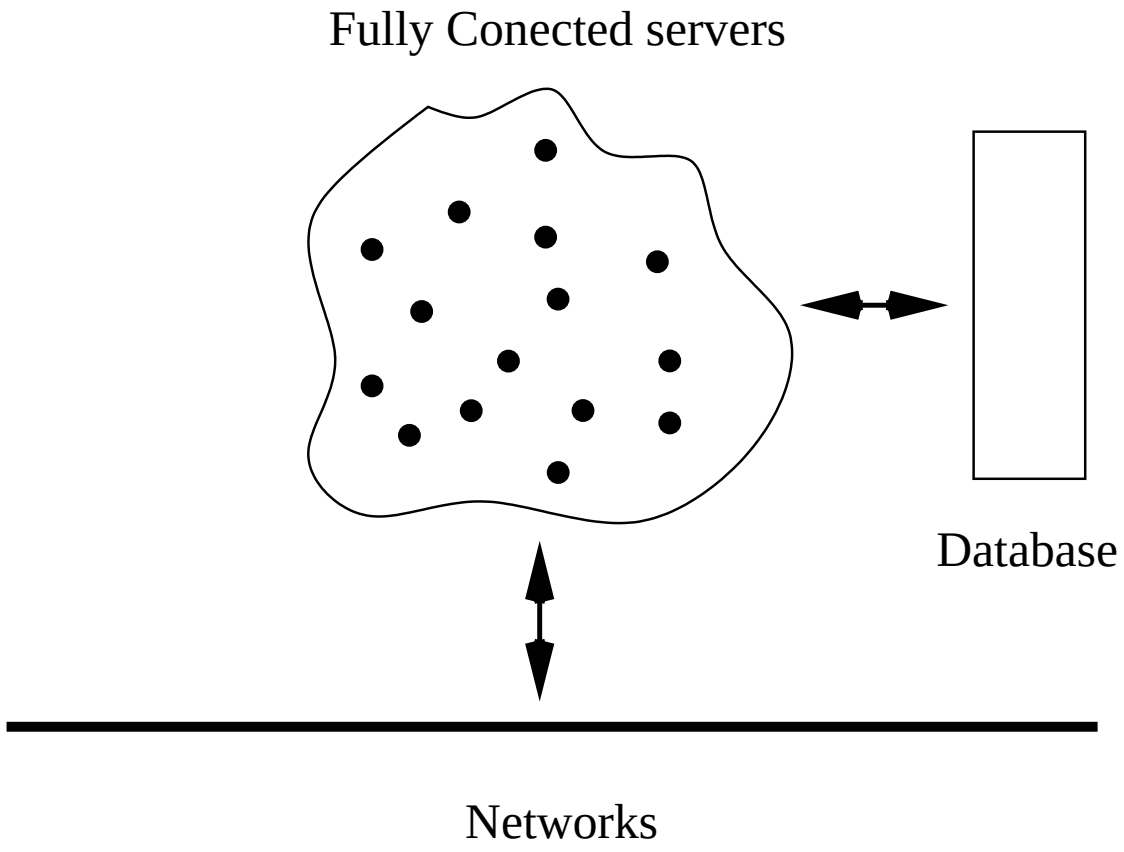
   Use Multiple servers

2. **Protect Public Information Integrity During Transmission:**

   Use Undetachable Signature

SITE ARCHITECTURE

The Architecture with Multiple Servers



SITE ARCHITECTURE

1. One master and many slaves at any given time.

2. Master evenly distributes requests to slaves.

3. In case a master is failed, one and only one slave will take over.

4. The take over procedure is quick and smooth because of

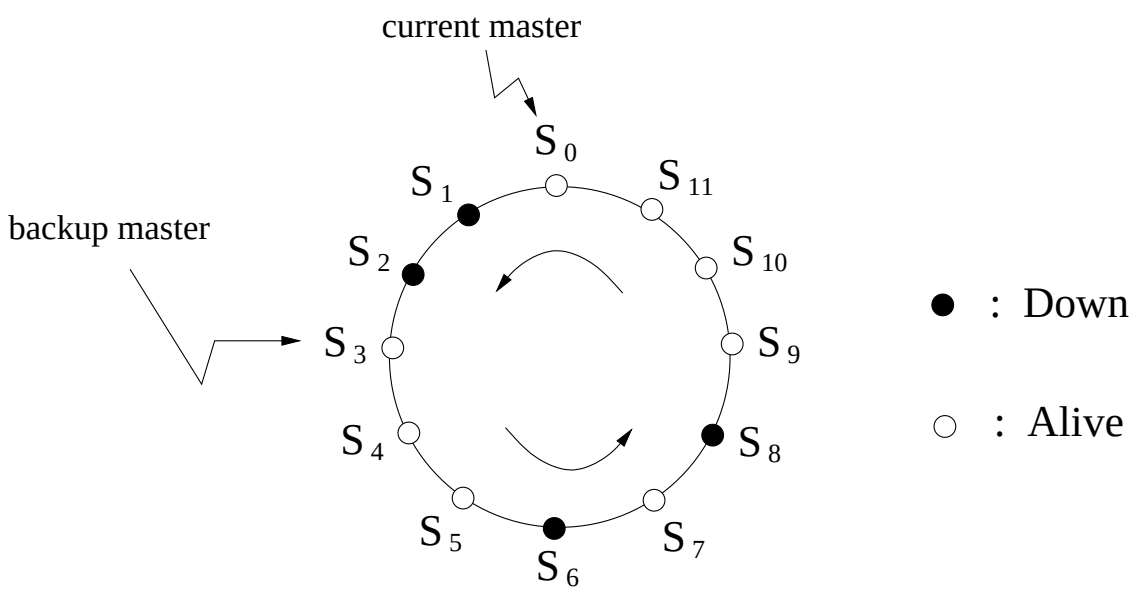
Numbering scheme

Keep-alive message scheme

Key management scheme

SITE ARCHITECTURE

Numbering Scheme



1. The closest slave to the current master (in counter clockwise) is the backup master.

2. All servers need to be aware of the master's number and the backup master's number.

SITE ARCHITECTURE

Keep-alive Message Scheme

1. The master periodically sends a keep-alive message to all slaves.

2. Any slave periodically sends a keep-alive message to those slaves who have a lower priority to take over than itself.

3. With the numbering scheme, all servers could reach consensus of who is the backup server.

SITE ARCHITECTURE

Key Management Scheme

1. Public cryptosystem is used for protecting data integrity.

2. For fast take over, each server has an RSA key pair, but only the master's key pair is active.

3. The master assigns (off line) a pair of delegated keys to each slave. The delegated key pair is derived from the RSA key pair.

4. A slave could use its delegated key pair to sign a message on behalf of the master for integrity protection.

UNDETACHABLE SIGNATURE

1. Let $(e, n), (d, n)$ be the RSA public and private keys of the master.

2. Let $(h, n), (k, n)$ be the delegated public and private keys of a slave, where

$$k = h^d \bmod n.$$

3. Slave generates an undetachable signature for a message M by computing

$$k^M \bmod n = (h^d)^M \bmod n = (h^M)^d \bmod n.$$

UNDETACHABLE SIGNATURE

4. User verifies the signature by computing

$$h^M \bmod n \quad \text{and} \quad (k^M \bmod n)^e \bmod n$$

The signature is correct if they are the same. Since

$$\begin{aligned}
&(k^M \bmod n)^e \bmod n \\
&= ((h^d)^M \bmod n)^e \bmod n \\
&= ((h^M)^d \bmod n)^e \bmod n \\
&= (h^M)^{de} \bmod n \\
&= h^M \bmod n
\end{aligned}$$

5. Use two public key certificates to get the public keys $(e, n), (h, n)$.