TECHNOLOGY

INNOVATE CALGARY

CONTACT: ipm@innovatecalgary.com• 403.284.6400

Secure Relaying Protocol with Partial Trust for QKD-Secured Networks

TECH ID #: 730.1

Background

Public key cryptography forms the security layer which enables e-commerce, online banking, and a host of other sensitive activities. Present-day public key cryptosystems, such as RSA, are secure only so long as an attacker's computing resources are limited. The security of these systems diminishes with time as the available computing power grows exponentially and advances are made in cryptanalysis. Quantum computers are expected to present a particularly serious threat to conventional ("computationally-secure") cryptosystems within ten to fifteen years. This future threat is a concern today since an attacker can conceivably intercept and record a present-day transmission to be decrypted in the future.

Cryptosystems are being developed which provide a fixed level of security regardless of the computing power used to attack them. One such informationtheoretic secure technology which is already commercially available is quantum key distribution (QKD). It uses optical fiber to securely transmit information between two parties who share a small secret key for authentication. QKD through optical fiber is currently limited to a maximum span length on the order of 100 km, so a network of relays must be employed to transmit QKD-secured information over longer distances. Conventional relay protocols require perfect trust ($t = 1$) of all relay nodes in the network. Consequently the secret information can be intercepted if a single relay node is compromised.

Researchers at the University of Calgary have developed a novel relay protocol which allows QKD-secured information to be transmitted over a network that may include relay nodes which are only partially trusted. This allows the implementation of information-theoretic secure networks which span large geographic distances and do not rely on unrealistic assumptions of perfectly trustworthy nodes. Security can be maintained for an arbitrary level of relay node trust ($0 < t \leq 1$) with only a modest increase in resources required as the level of trust declines.

Areas of Application

- Financial networks
- Electronic commerce
- Communication of private information (such as health records)
- Military communication networks
- National security organizations

Competitive Advantages

- Relay nodes in a QKD network need not be fully-trusted
- The use of partially-trusted nodes facilitates the practical implementation of geographically large-scale QKD networks
- Security of information is independent of the computing power and cryptanalysis techniques available to an attacker
- Information is protected now and for the future

Stage of Development

The technique has been successfully implemented in software and successfully simulated in hardware form.

Intellectual Property Status

- US Patent Issued: US 8,050,410
- Europe Patent Pending: EP2095561