Solving the Identity Theft Problem Using Quantum Memories

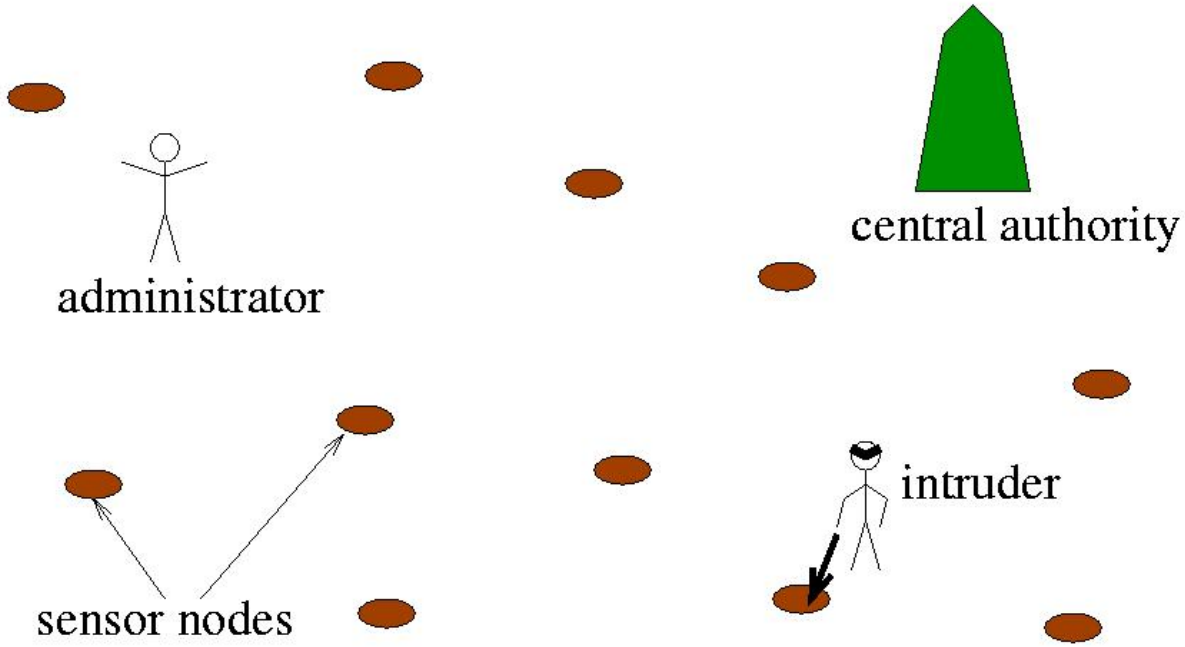
Naya Nagy, Marius Nagy and Selim G. Akl

School of Computing
Queen's University
Canada

SUM ERGO COMPUTO

Main Result

- Quantum memories can solve the pervasive problem of identity theft in sensor networks.
- The identity of a sensor node as a communication partner is viscerally the same as its cryptographic identity.
- The scheme presented here is complete: a secret key is generated between two parties such that the identity of the partner is ensured and the key cannot be broken.

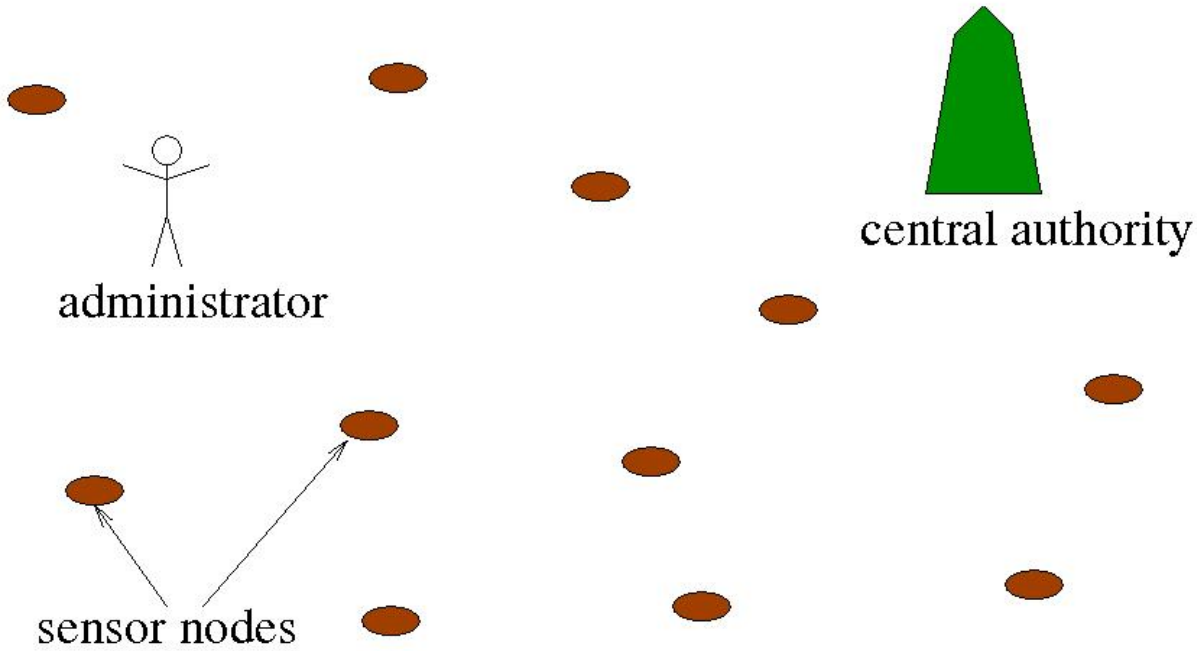


- Administrator - Walks in the field, listens and sends messages in the sensor network. Takes decision concerning movement, queries.
- Central Authority - Provides security.
- Sensor Nodes - Measure parameters in their environment. Send and receive messages.
- Intruder - Picks up nodes and reads and writes into their memory.

Task: Determine whether a node has been touched by the intruder. If the node is trustworthy, generate a secret key shared by the administrator and the node.

Overview

Sensor Networks



- Sensor nodes are deployed at random. Restricted by their transmission range, they self organize in a network.
- The administrator is moving in the field.
- The central authority (CA) can communicate with the administrator.

Security in Sensor Networks

Security in sensor networks has been studied less extensively than the reliability of sensor networks.
The problem of security in sensor networks arises from the type of application the sensor network is used for.
The type of application also defines the type of possible attacks on the network.

1. External Attacks
   - Listening to the environment for messages passed in the network.
   - Inserting a fake node.
2. Internal Attacks
   - Physically capturing a node and then using the compromised node to send virus-type messages.

Previous Work

1. External Attacks
   - Various secret key management schemes
     - Encrypt every packet.
     - Authenticate every sensor node.
   - Our previous work in quantum sensor networks offers a solution with quantum generated secret keys.
2. Internal Attacks
   - Eliminate nodes that have a high probability of being compromised or of becoming compromised in the future.

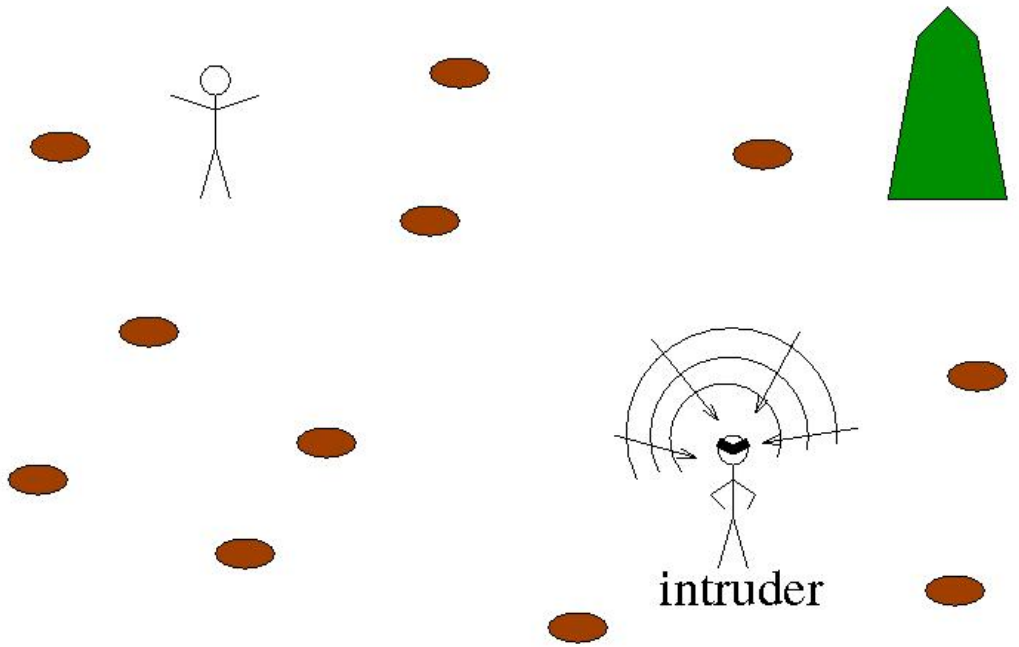
Scheme against External Attacks

- Protects the environment against listening.
- Encrypts packets with quantum generated secret keys.
- Uses the advantages of quantum cryptography.
- It is a *simple* secret key management system.
- The secret key is generated only when needed and is used exactly once. Therefore, an intruder has practically no chance to discover the secret key. The intruder has to know *in advance* both the time and the place in the network, where the key will be generated.

Scheme against Internal Attacks

- Sensor nodes are equipped with quantum memories.
- The node's identity signature is written in its memory.
- The signature is an array of quantum bits.
- The signature cannot be copied due to the *non-clonability theorem*.
- The identity of a node is destroyed when an intruder accesses its memory.

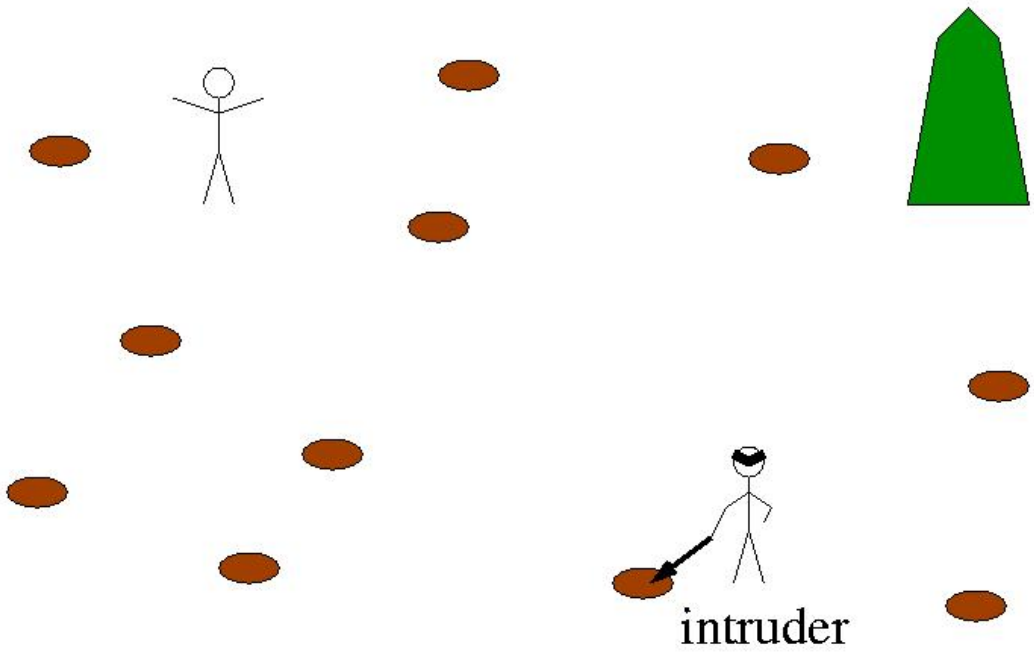
External Security Problem



The intruder listens to the environment to gather information about the location of events, the nature of the events, the parameters of the events, and so on.

Problem: Encrypt the messages broadcast in the environment such that they will not be intelligible to the intruder.

Internal Security Problem

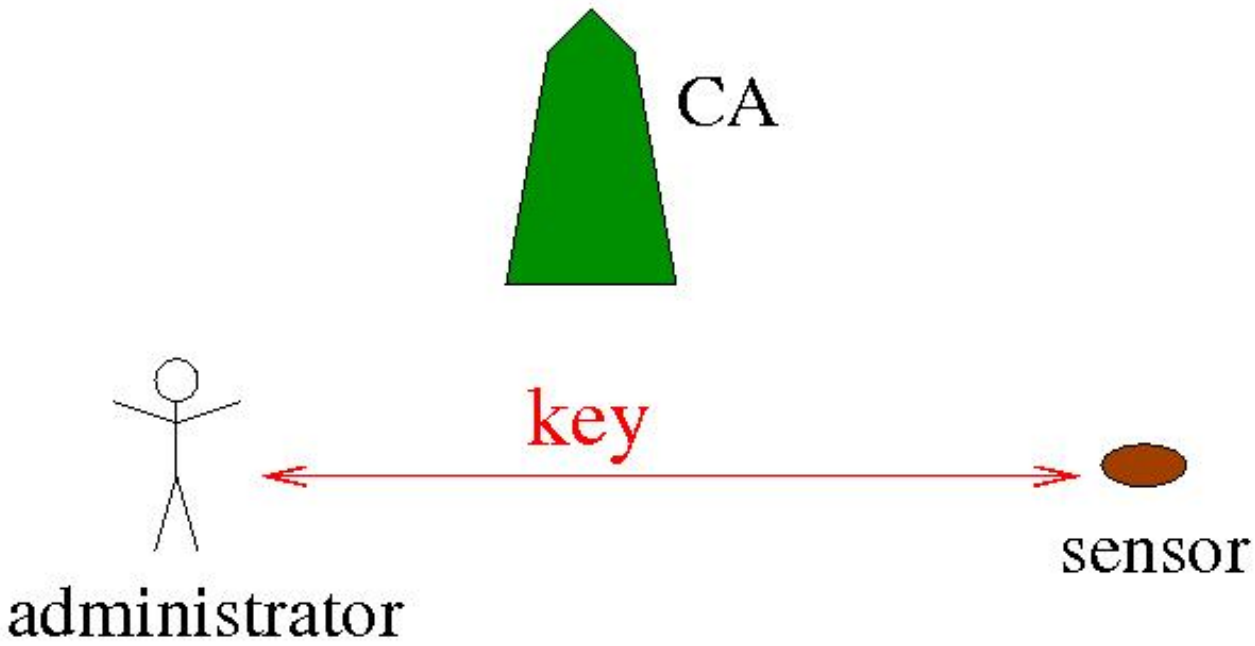


The intruder picks up a node and reads its memory and then may write a modified version of the node's program.

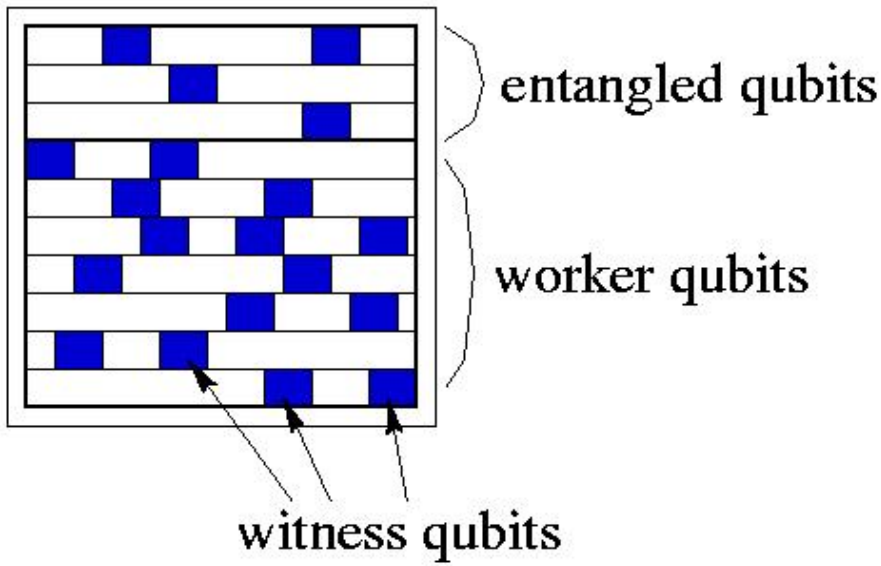
Problem: Detect the intrusion even if the intruder just reads memory locations.

Role of the Central Authority

Construct a k-bit key to be used by the administrator and sensor node for secure communication.
This is done through entanglement swapping.



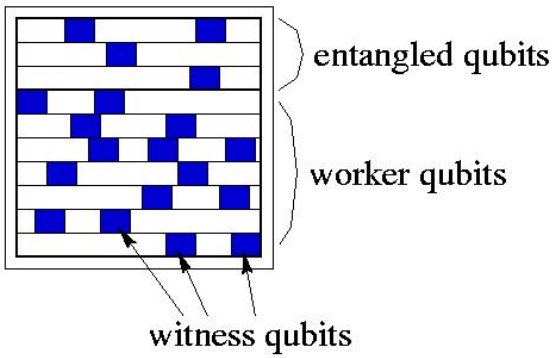
The Sensor Node's Quantum Signature



The **sensor node's memory** consists of:

1. **Entangled qubits.** These qubits are entangled to the CA. They will be used to establish the secret key.
2. **Worker qubits.** These qubits are used for regular programs and data.
3. **Witness qubits.** These qubits encode the node's signature.

The Sensor Node's Quantum Signature - continued

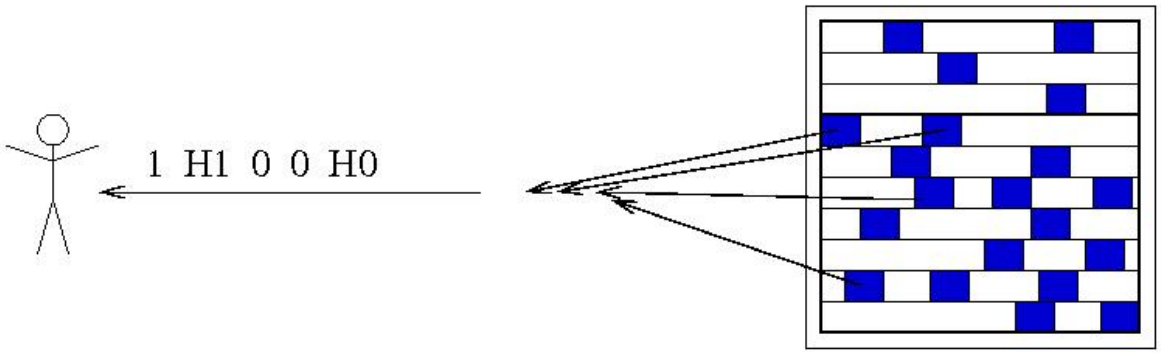


Example of a signature: 1 H1 0 0 H0.

Properties:

1. Can be read only by a person (administrator) who knows which qubits are Hadamard rotated.
2. Cannot be meaningfully read by an intruder.
3. Cannot be copied - no-cloning theorem.

Quantum Signature Checking



1. The sensor node sends the qubits representing its signature to the administrator.
2. The administrator reads the qubits according to their Hadamard / no Hadamard encoding:
   direct Hadamard direct direct Hadamard
3. The administrator compares the reading with the expected signature value.

Secret Key Distribution

1. **Communication Request:** The administrator requests from the CA to communicate with node i. The identifier i does not reveal the location (x, y) of the node.
2. **Entanglement Swapping:** The CA performs an entanglement swapping.
3. **Entanglement Verification:** The administrator verifies the entanglement directly with the node.
4. **Secret Key Measurement:** The administrator and the node measure the remaining entangled qubits. This is the secret key.
5. **Identity Checking:** This is optional. The administrator checks the node's quantum signature.

Security Properties

- The intruder can listen to the environment and understand *all* unencrypted messages.
- The intruder cannot get the position of the location (x, y) of interest.
- The intruder cannot get any information about the value of the secret key. No information in the field or on the authenticated classical channel reveals anything about the value of the secret key.
- The intruder cannot decrypt the communication messages between the administrator and the node. These messages would reveal the nature and parameters of the event.
- Further, it is only the (x, y) sensor node that can encrypt and decrypt messages for the administrator. Thus, if the intruder corrupts a random node, that node won't yield any information about the (x, y) sensor.

Security Properties - continued

- The intruder cannot read and cannot copy the node's signature.
- The intruder cannot get any information about the value of the signature.
- When an intruder reads a node, it kills its identity, its quantum signature.
- The intruder cannot touch a node without leaving an unmistakable mark on it.

Conclusion

1. Security of sensor networks can benefit from quantum cryptography.
2. Encryption / decryption can be done with (quantum generated) classical secret keys.
3. Secret key generation is based on entanglement and entanglement swapping.
4. Quantum generated secret keys are effectively unbreakable.
5. A node's identity is unequivocally linked to its cryptographic identity.

Open Problems

1. Messages are still classical. It is not clear how a sensor network might benefit from quantum messages.
2. The secret key is quantum generated but is a classical binary value. Again, it is not clear how the sensor network would benefit from quantum secret keys. A quantum key would be a string of qubits.