Quantum Wireless Sensor Networks

Naya Nagy, Marius Nagy and Selim G. Akl

School of Computing
Queen's University
Canada

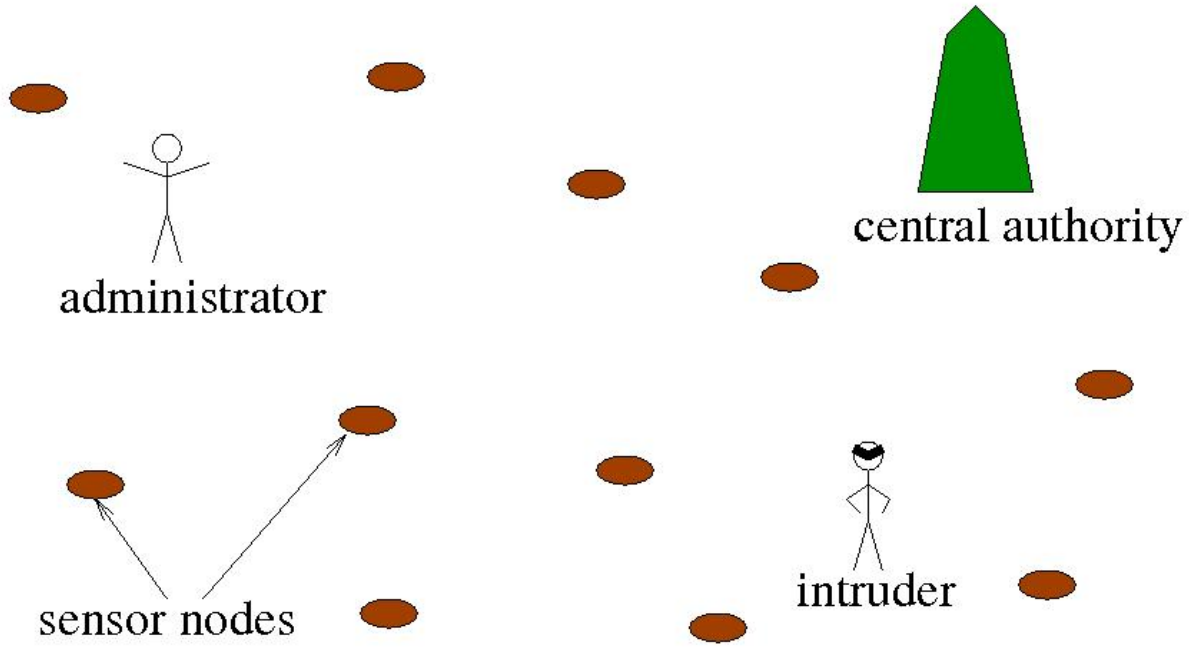
Seventh International Conference on Unconventional Computation
Vienna, August 2008

Main Result

Quantum cryptography can solve the problem of security in sensor networks.

The security scheme presented in the following slides uses secret keys to encrypt messages.
The secret keys are developed in a quantum setting and thus have the advantage of quantum cryptography:

The secret keys are effectively unbreakable.

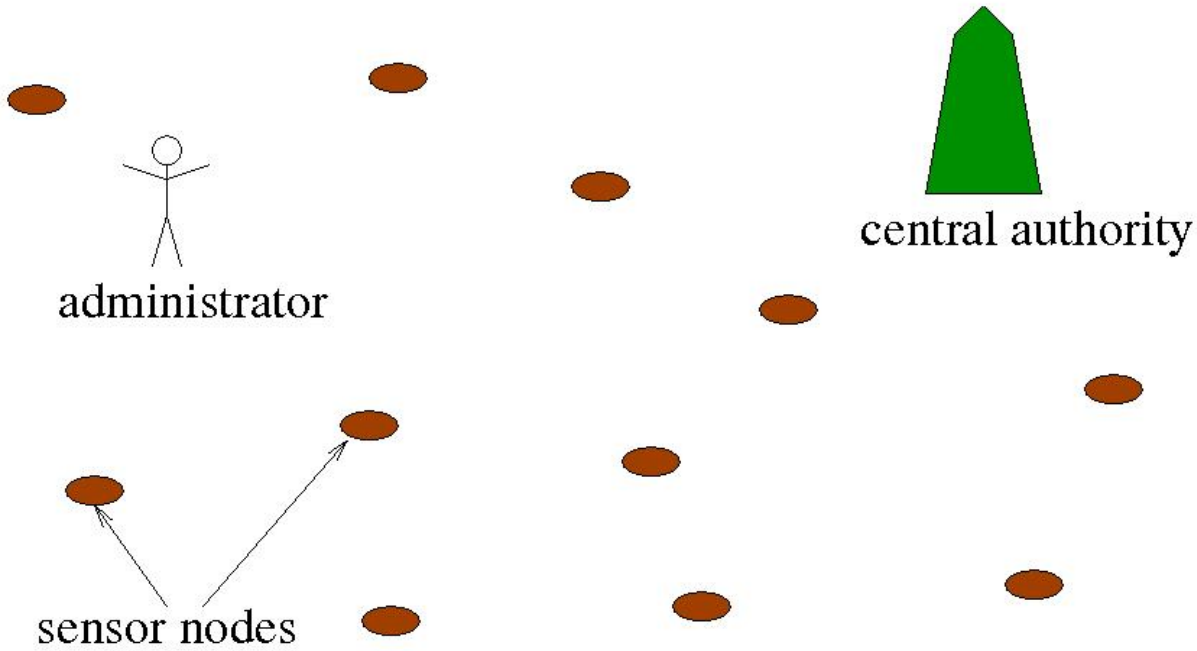


- Administrator - Walks in the field, listens and sends messages in the sensor network. Takes decision concerning movement, queries.
- Central Authority - Provides security.
- Sensor Nodes - Measure parameters in their environment. Send and receive messages.
- Intruder - Listens to the environment to gather information.

Task: Protect the environment from the intruder.

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

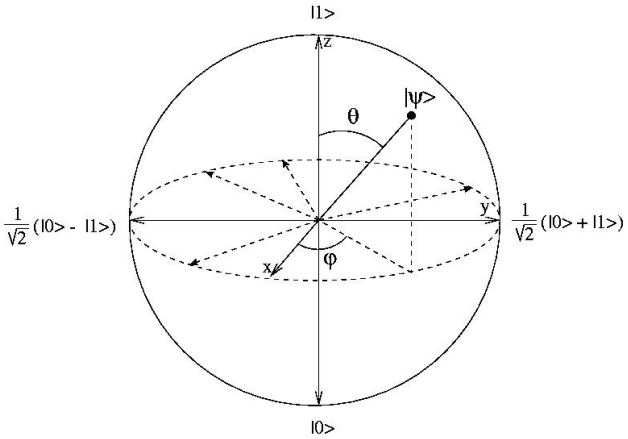
1. External Attacks
   - Various secret key management schemes
     - Encrypt every packet.
     - Authenticate every sensor node.
2. Internal Attacks
   - Eliminate nodes that have a high probability of being compromised or of becoming compromised in the future.

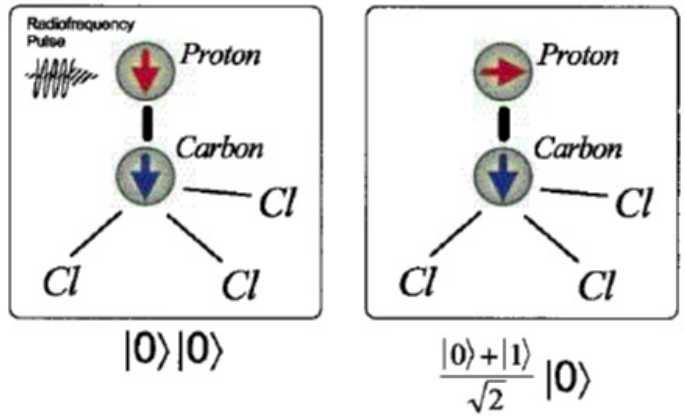
New Approach: Using a Quantum Setting

- Addresses external attacks.
- Uses the advantages of quantum cryptography.
- It is a *simple* secret key management system.
- The secret keys are quantum generated.
- 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.

Qubits

A classical bit has two states: 0 and 1.
A qubit is a vector on a unitary sphere.

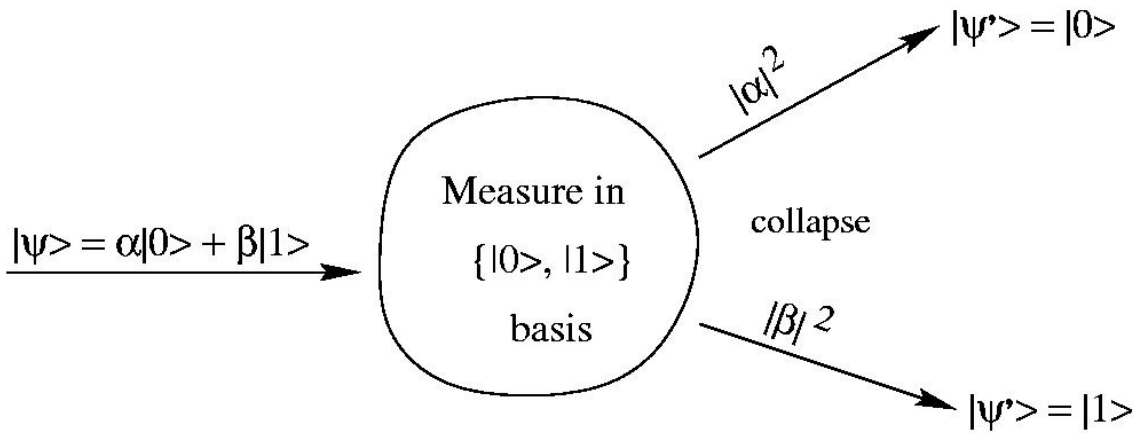




The position of the vector on the sphere yields the binary value. If the vector is

- Up. The qubit has the value 1.
- Down. The qubit has the value 0.
- On the equator. The qubit has an equal probability (50%) of being 0 or 1.
- In any other position. The qubit is in some superposition of 0 and 1.

Measuring the Value of a Qubit



In general, a qubit $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is a superposition of 0 and 1.
When $|\Psi\rangle$ is measured, the result will be a classical 0 or 1.
The probability to measure a 0 is $|\alpha|^2$ and
the probability to measure a 1 is $|\beta|^2$.

Entangled Qubits

An ensemble of two qubits is represented as the tensor product of its component vectors. For example:

$$|\Psi\rangle = (\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle) \otimes (\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle) = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle).$$

Now, there exist states describing an ensemble of two (or more) qubits that cannot be decomposed into a tensor product of two *distinct* qubits. For example: $\nexists\ \alpha, \beta, \gamma, \delta$ such that

$$(\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle) =$$

$$= \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

An ensemble of (two) qubits that cannot be written as a tensor product is called entangled. The states of the two qubits are not independent.

Entangled Qubits - Continued

The most common entangled states are the Bell states:

$$q_A q_B = |\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

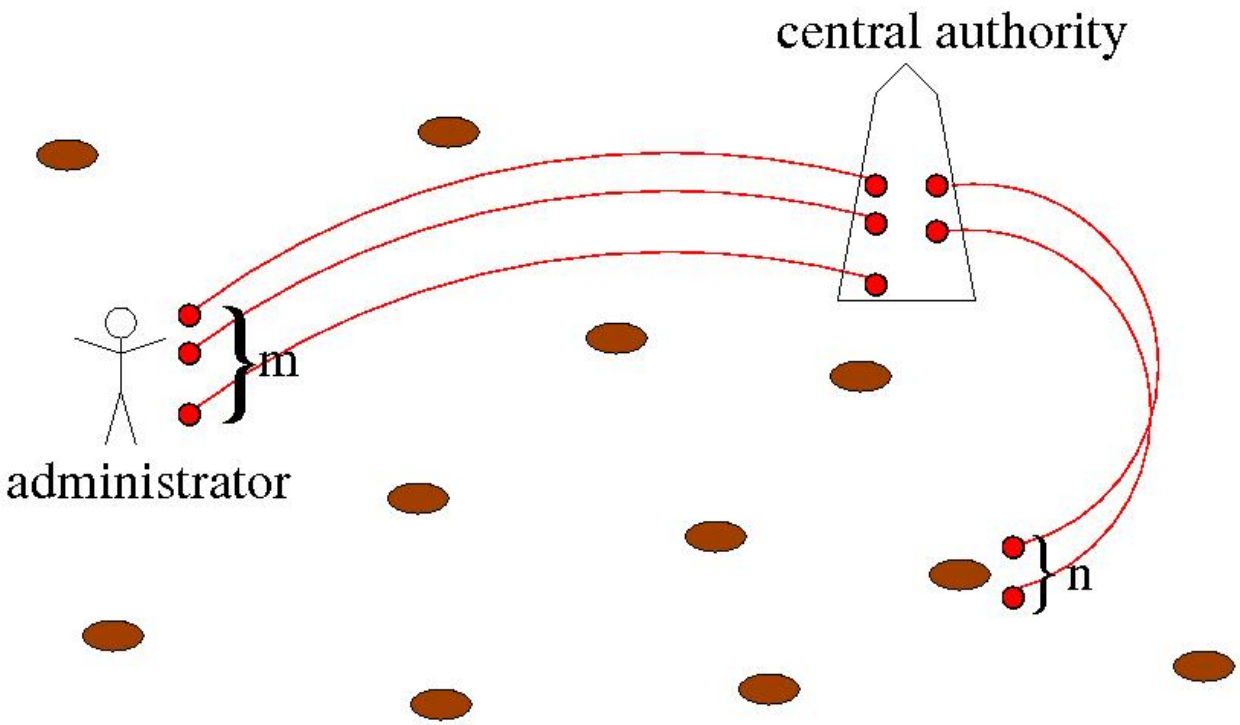
$$q_A q_B = |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$q_A q_B = |\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$q_A q_B = |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

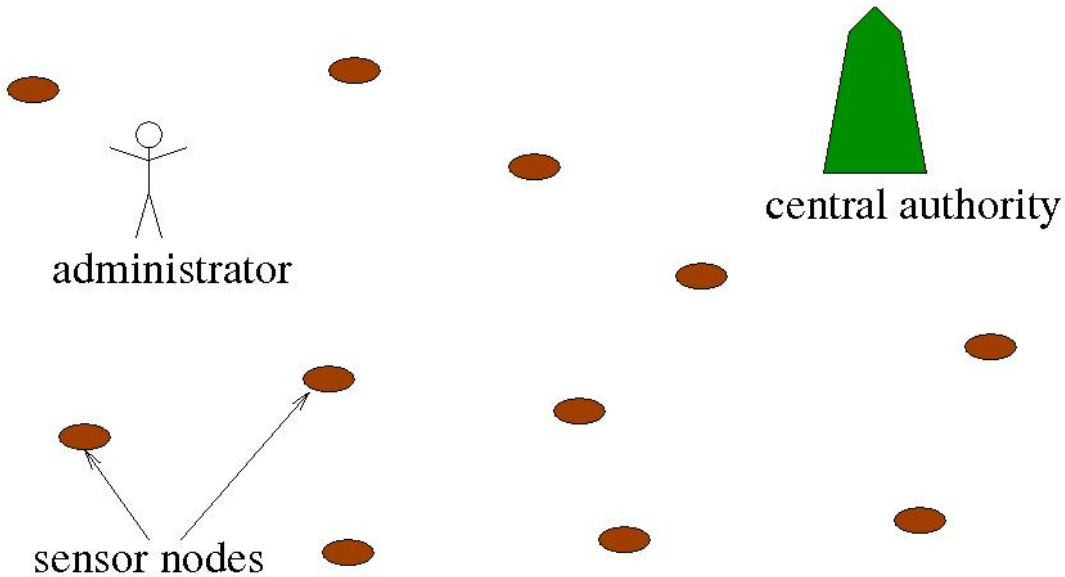
For each Bell state, measuring one qubit, collapses the other qubit to a classical state. For $|\Phi^+\rangle$, the following two scenarios are possible:
$q_A = 0 --> q_B = 0$
$q_A = 1 --> q_B = 1$

Quantum Sensor Networks



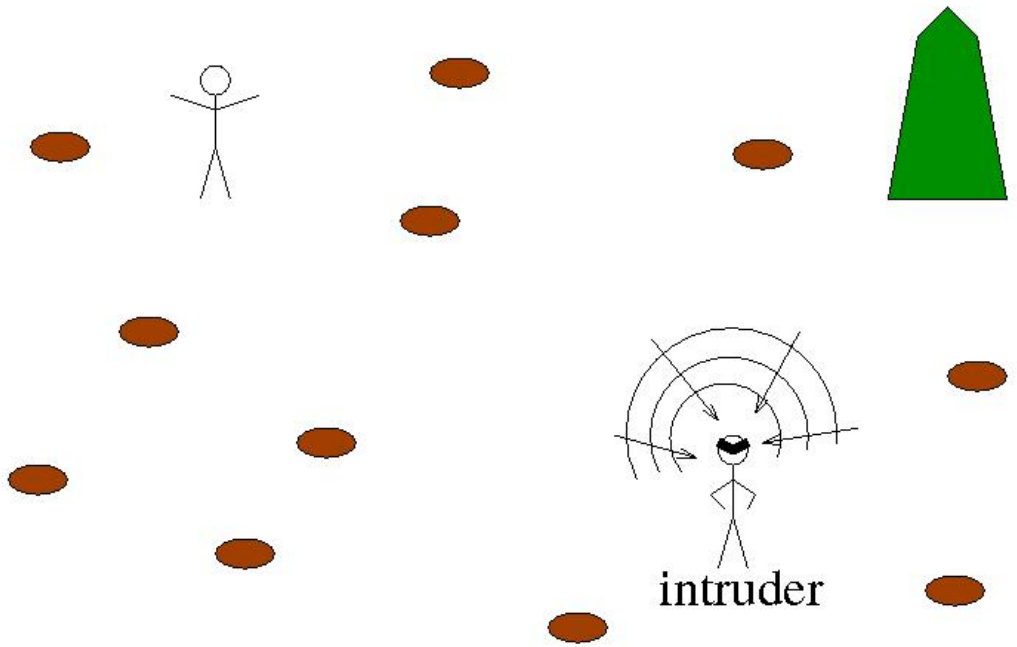
- Each sensor node has some n qubits.
- The administrator has m qubits, with $m > n$.
- Each of these qubits is entangled with a second qubit stored at the central authority.

Security Setting



- The central authority (CA) is trusted.
- The administrator is trusted.
- The sensor nodes are trusted. This is a strong assumption.
- The environment carrying the messages is not trusted.

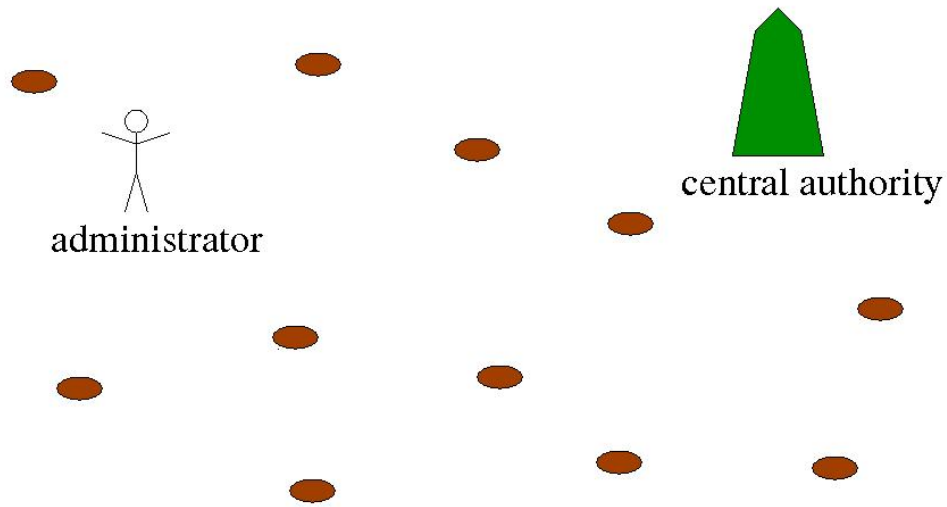
Security Problem



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.

Security Protocols



The paper discusses two possible scenarios

1. The administrator wants to obtain information from a selected sensor at location (x, y).
2. A sensor node detects some event at its location (x, y) and wants to inform the administrator.

It is advantageous if sensor nodes have unique identifiers, beside their physical location. In this case, all messages addressed to a sensor node contain the identifier, rather than the location, thus hiding (x, y) from the intruder.

First Security Protocol - The Administrator's Query

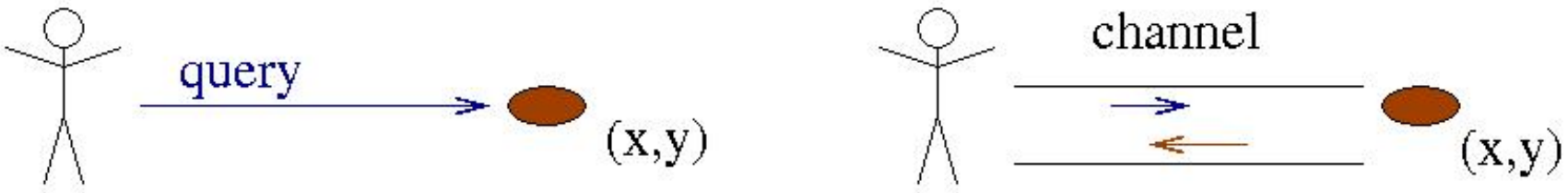
The administrator wants to obtain information from a selected sensor at location (x, y).

1. The administrator broadcasts a query into the field.

First Security Protocol - The Administrator's Query

The administrator wants to obtain information from a selected sensor at location (x, y).

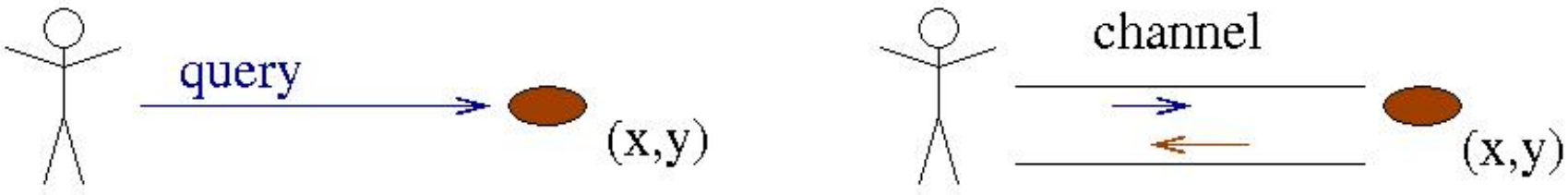
1. The administrator broadcasts a query into the field.
2. The selected sensor node answers the query. Messages can be further exchanged.



First Security Protocol - The Administrator's Query

The administrator wants to obtain information from a selected sensor at location (x, y).

1. The administrator broadcasts a query into the field.
2. The selected sensor node answers the query. Messages can be further exchanged.



- The intruder will not be able to gather information about the nature or the parameters of the events at (x, y), but is able to know that there was a query for (x, y). [Think of (x, y) as the node identifier, not its coordinates.]

Second Security Protocol - The Sensor Node's Request

A sensor node detects some event and wants to inform the administrator.

1. The sensor node broadcasts a request in the network, presenting itself as (x, y).

Second Security Protocol - The Sensor Node's Request

A sensor node detects some event and wants to inform the administrator.

1. The sensor node broadcasts a request in the network, presenting itself as (x, y).
2. The administrator broadcasts a query into the field.

Second Security Protocol - The Sensor Node's Request

A sensor node detects some event and wants to inform the administrator.

1. The sensor node broadcasts a request in the network, presenting itself as (x, y).
2. The administrator broadcasts a query into the field.
3. The selected sensor node answers the query. Messages can be further exchanged.

Second Security Protocol - The Sensor Node's Request

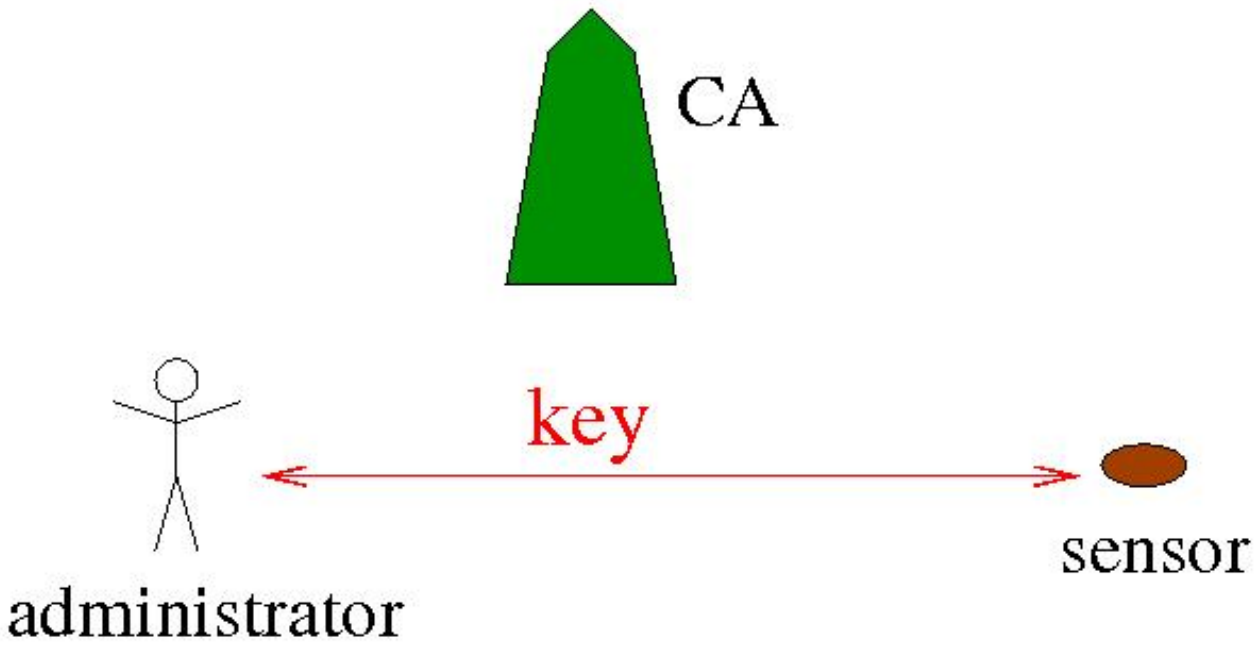
A sensor node detects some event and wants to inform the administrator.

1. The sensor node broadcasts a request in the network, presenting itself as (x, y).
2. The administrator broadcasts a query into the field.
3. The selected sensor node answers the query. Messages can be further exchanged.

- The intruder can detect the initiative of the sensor node, but gathers no information about the nature and parameters of the event.

Role of the Central Authority

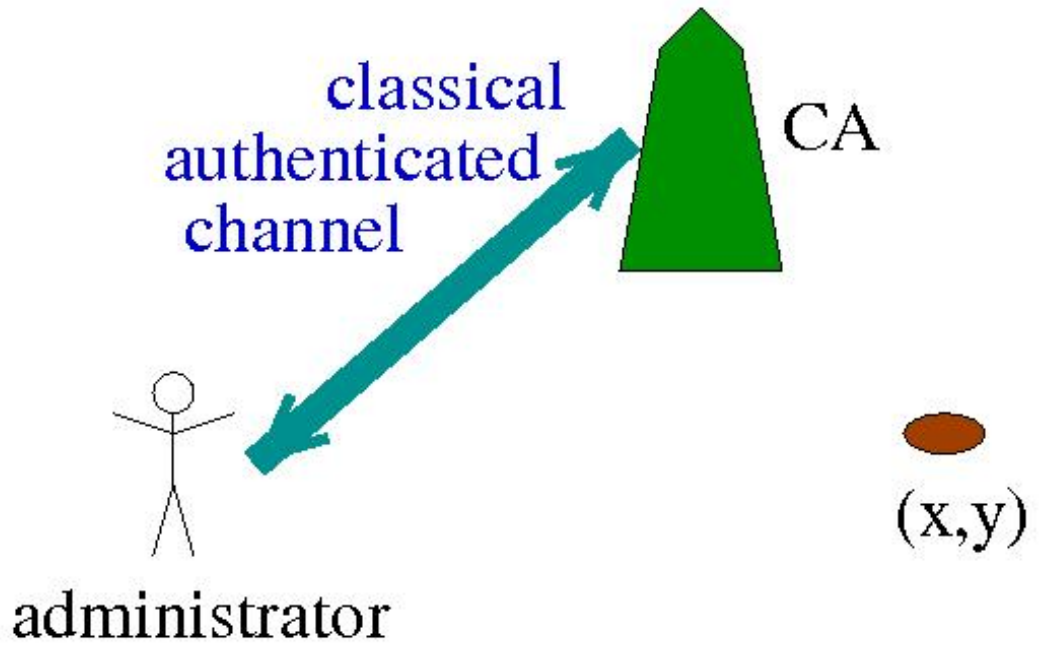
Construct a k-bit key to be used by the administrator and sensor node for secure communication.
This is done through entanglement swapping.



Entanglement Swapping

The following steps involve the CA when performing entanglement swapping.

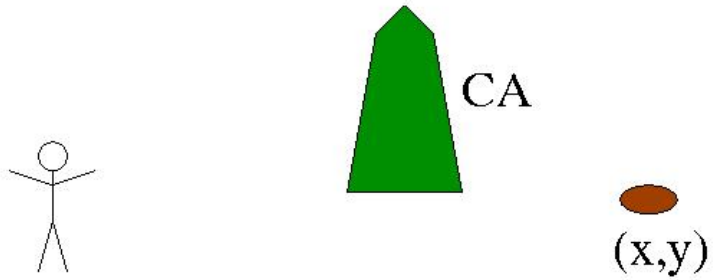
1. The administrator informs the CA of the intention to query a sensor at the approximate location (x, y).



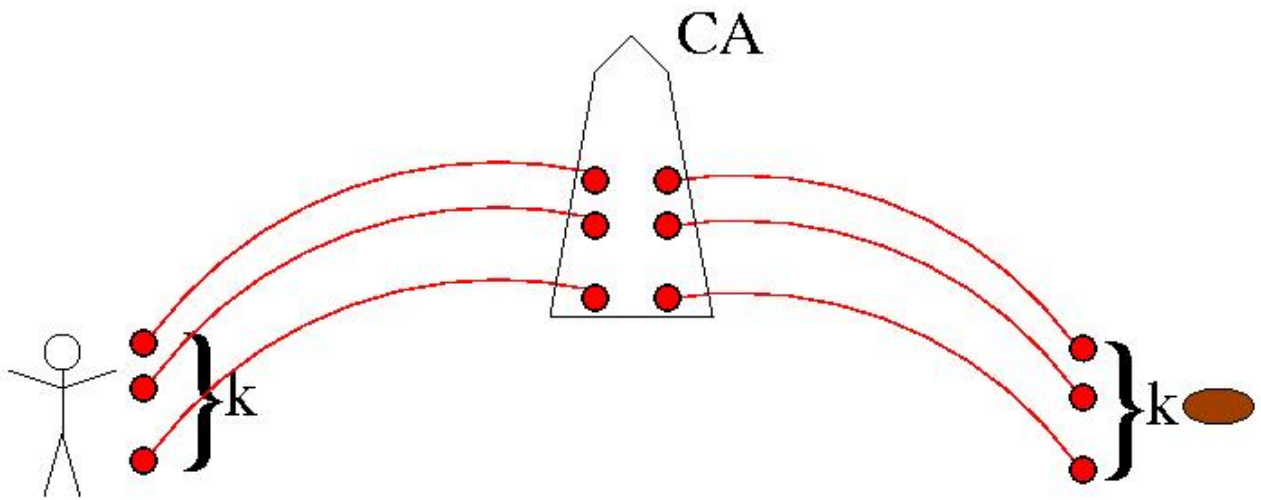
The classical channel uses classical binary bits (non-quantum) and can be authenticated using private keys or public keys for digital signature.

Entanglement Swapping - Continued

2. The CA selects a sensor node in the vicinity location (x, y).

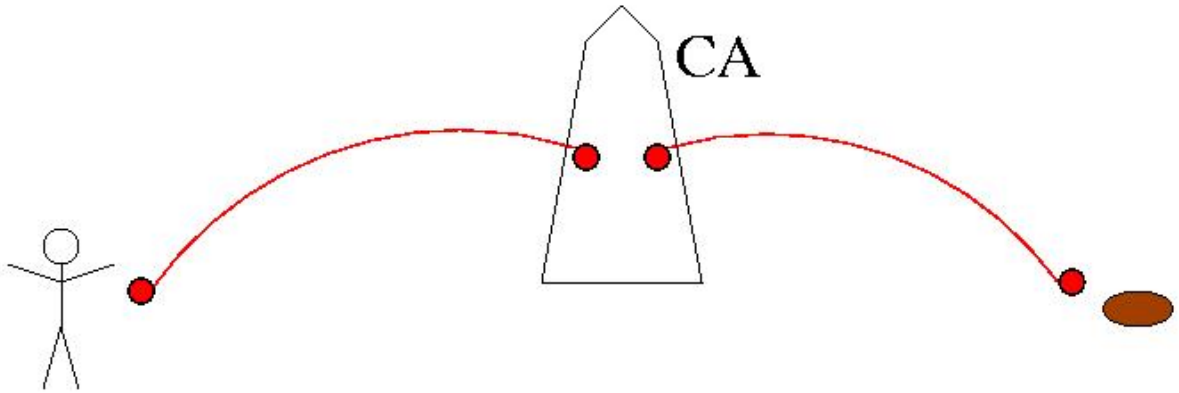


3. The CA selects k of its qubits entangled with the qubits of the sensor at (x, y) and k qubits entangled with qubits of the administrator.

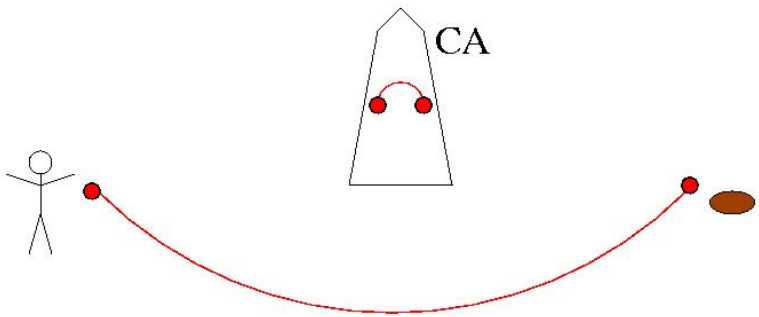


Entanglement Swapping - Continued

4. Consider two such entangled pairs

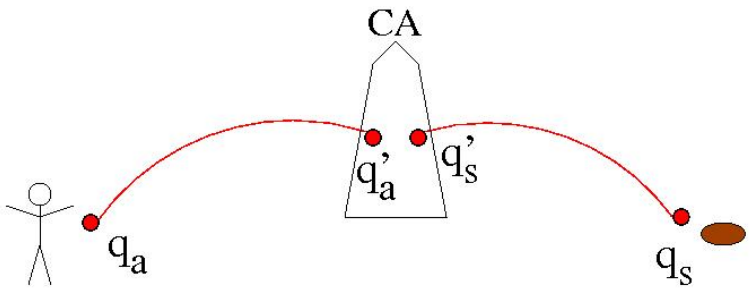


The CA performs an entanglement swap.



This is done for all k pairs.

How Entanglement Swapping Is Performed

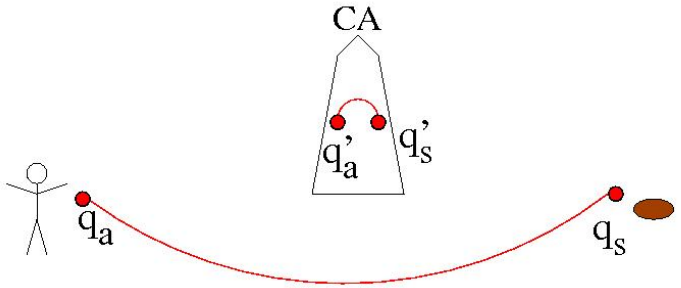


The CA performs a measurement on q'_a and q'_s in the Bell Basis.

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \qquad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Now the administrator and the sensor node have entangled qubits.



Entanglement Swapping - Ensemble of the Four Qubits before Measurement

$$ensemble = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

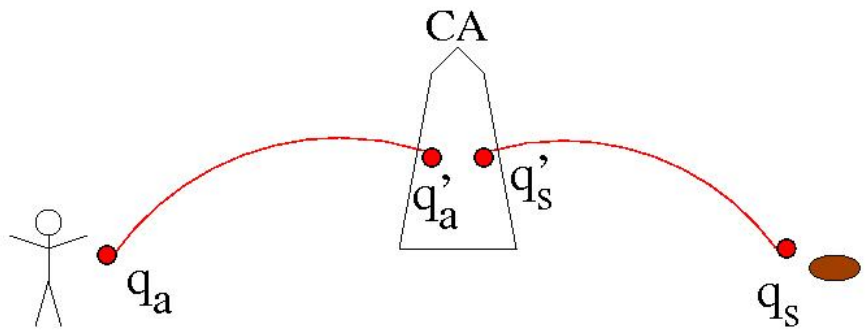
$$= \frac{1}{2}(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle)$$

$$= \frac{1}{2\sqrt{2}}(|0\rangle \otimes |\Phi^+\rangle \otimes |0\rangle + |1\rangle \otimes |\Phi^+\rangle \otimes |1\rangle +$$

$$|0\rangle \otimes |\Phi^-\rangle \otimes |0\rangle - |1\rangle \otimes |\Phi^-\rangle \otimes |1\rangle +$$

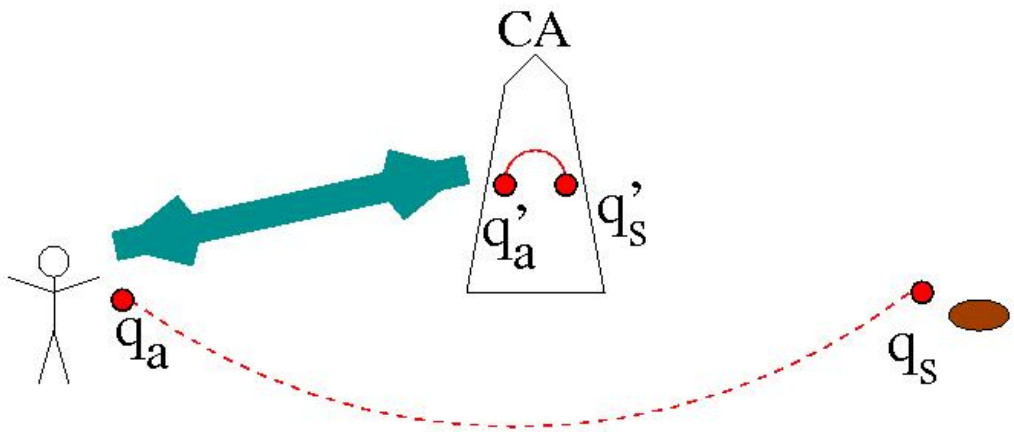
$$|0\rangle \otimes |\Psi^+\rangle \otimes |1\rangle + |1\rangle \otimes |\Psi^+\rangle \otimes |0\rangle +$$

$$|0\rangle \otimes |\Psi^-\rangle \otimes |1\rangle - |1\rangle \otimes |\Psi^-\rangle \otimes |0\rangle).$$



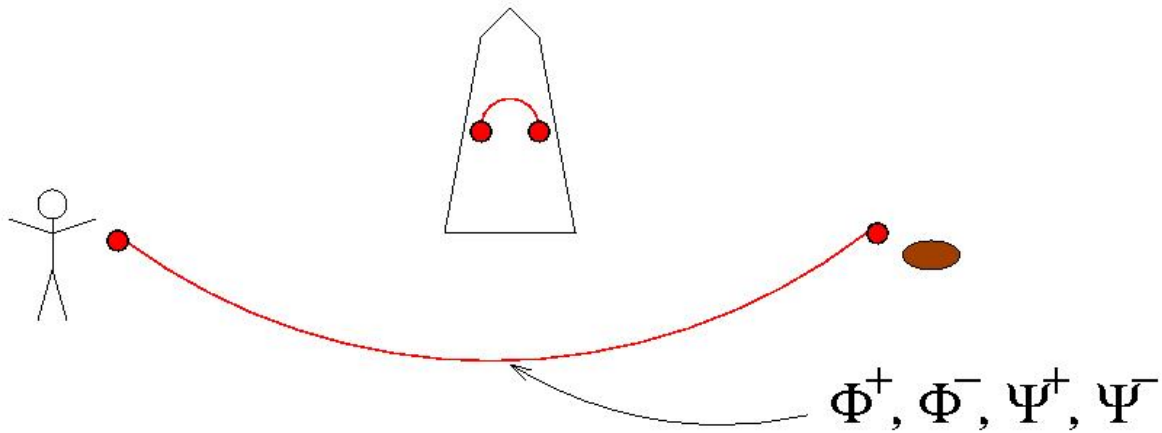
How Entanglement Swapping Is Performed - Continued

1. The CA performs a partial measurement in the Bell basis. The outcome of the measurement is one of the values Φ^+, Φ^-, Ψ^+, or Ψ^-.
2. The CA informs the administrator of the outcome of the measurement. The communication is done via the classical authenticated channel.



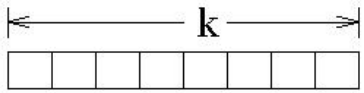
How Entanglement Swapping Is Performed - Continued

1. The administrator knows now the type of the entanglement of its qubit with the sensor node.

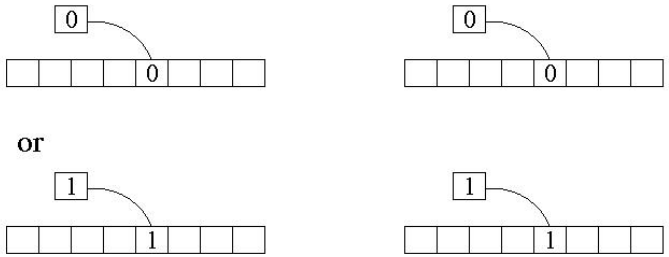


Forming the Secret Key

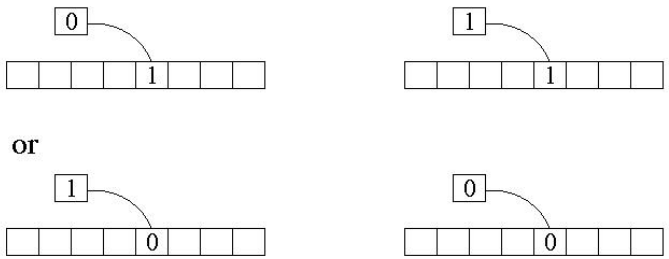
The administrator and the sensor node, each measure their qubits to obtain one (classical) bit of the (k-bit) secret key.



1. If the entanglement was of type $|\Phi^+\rangle$ or $|\Phi^-\rangle$ that bit would be the same for both the administrator and the sensor node.

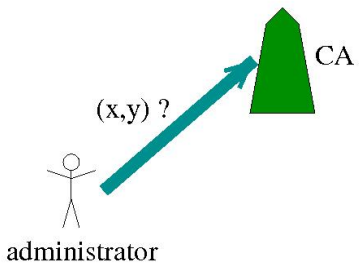


2. If the entanglement was of type $|\Psi^+\rangle$ or $|\Psi^-\rangle$, the administrator and the sensor node will have complementary bits. Consequently, the administrator's bit gets flipped.

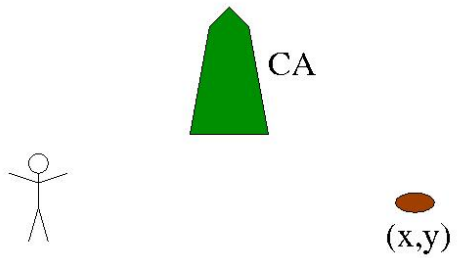


First Protocol - The Administrator Gathers Information from the Field

1. The administrator sends the location of interest (x, y) to the central authority.

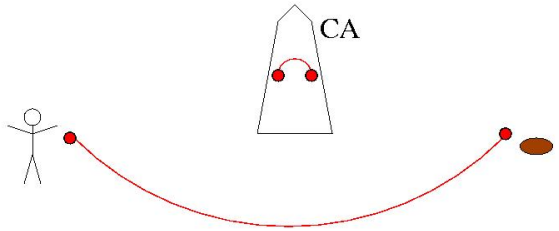


2. The central authority locates a sensor node s close to (x, y).

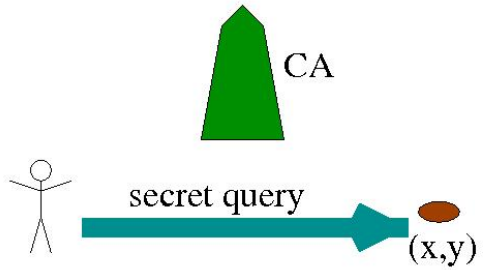


First Protocol - Continued

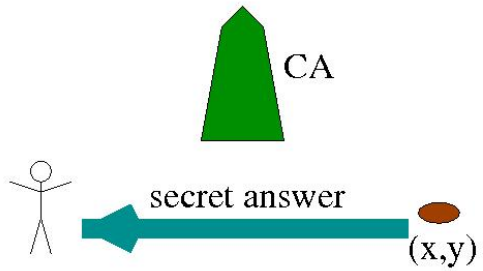
3. The administrator and the sensor establish a secret key using entanglement swapping.



4. The administrator sends an encrypted query to the node s.

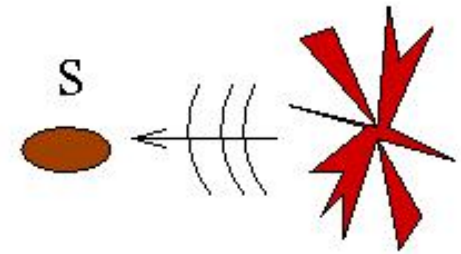


5. The node s sends the answer back, using the same encryption key.

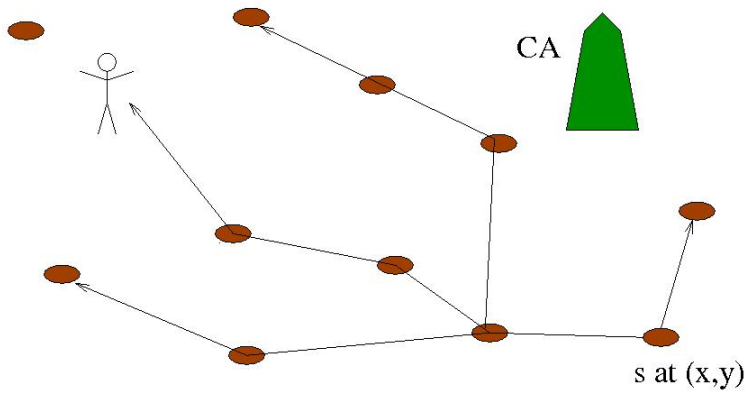


Second Protocol - Some Node s Detects an Event

1. The sensor s detects an event.



2. s broadcasts an unencrypted message saying that it wants to communicate with the administrator from its own location (x, y).



3. From here on, the protocol follows the steps of the first protocol.

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.

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.

Open Problems

1. We have shown a scheme to protect the environment.
   The sensor nodes are considered trusted and this is a strong assumption. The problem of sensor node corruption has not yet been addressed using quantum cryptographic means. Our protocol, however, as it is, offers already some limited protection in node corruption attacks. Any node, except the node of interest (x, y) does not know the quantum generated key. Thus, corrupting a node and reading the information inside it, does not reveal any additional information to listening to the environment.
2. Specific quantum cryptographic methods apply to unusual settings. We believe that the applicability of quantum cryptography is much larger than presently exploited.