Technical Report No. 2008-544
Quantum Wireless Sensor Networks*

Naya Nagy, Marius Nagy and Selim G. Akl

School of Computing

Queen's University

Kingston, Ontario K7L 3N6

Canada

Email: {nagy,marius,akl}@cs.queensu.ca

Abstract

Security in sensor networks, though an important issue for widely available wireless networks, has been studied less extensively than other properties of these networks, such as, for example, their reliability. The few security schemes proposed so far are based on classical cryptography. In contrast, the present paper develops a totally new security solution, based on quantum cryptography. The scheme developed here comes with the advantages quantum cryptography has over classical cryptography, namely, effectively unbreakable keys and therefore unbreakable messages. Our security system ensures privacy of the measured data field in the presence of an intruder listening to messages broadcasted in the field.

Keywords: wireless sensor networks, quantum cryptography, quantum teleportation, entanglement swapping.

1 Introduction

Wireless sensor networks are becoming increasingly more feasible in monitoring or evaluating various data fields. Their domain of applicability is steadily increasing, ranging from civil objective surveillance to strategic surveillance, from environmental forest condition monitoring to urban information gathering. Given the large variety of working environments, the question of protect-

*This research was supported by the Natural Sciences and Engineering Research Council of Canada.

ing the privacy of the gathered data is almost overdue and will be addressed here.

In general, a sensor network is a collection of sensor nodes arbitrarily spread over a geographic field [14]. The purpose of the network is to collect or monitor data from the field. From an abstract point of view, each point of the field is defined by a small set of significant parameters. Each node in its turn is able to measure (sense) the field parameters of its geographical location.

Sensor nodes can communicate with each other via radio signals, which means that they are not hardwired to one another. Each node has a certain transmission power, and it can send messages to any of the nodes within its transmission range. Also a sensor node can receive messages sent by another node. Note that, the energy consumed to receive a message is independent of the distance between the source and the destination and thus, a node can receive a message from arbitrarily large distances (provided that it falls within the transmission range of the sender). As the nodes are deployed at random across the field, they self organize themselves in a network, restricted only by their transmission range.

Each sensor node has a local limited computational capacity and is therefore able to perform modest sized computations locally.

1.1 Protecting the Sensor Network

The reliability of sensor networks [1] has been studied extensively and refers to the correct functioning of the network in the face of adverse events and failure of some of the nodes. Indeed, sensor nodes function in more challenging and unpredictable circumstances than regular computers and therefore can fail for multiple reasons. For example, sensor nodes are battery operated and battery failure implicitly causes the failure of the node. Again, sensor nodes are deployed in real natural environments, where natural events may destroy the node. Thus, the network as a whole needs to be operational, even though a fraction of the nodes are not operational. Algorithms to deal with node failure are basic to sensor network management and ensure that sensor networks work reliably.

Note that all the challenges of the network considered up to now are natural, read *unintentional*. In this paper, by contrast, we explore some aspects of a *malevolent* intervention in the network. We note here, that the issue of *security* in a sensor network has been studied decidedly very little compared to, for example, the reliability of such networks. Security treats the situation where an intruder purposefully inserts itself in the sensor network. The intruder may intend to perform one or more of the following actions:

1. Listen to the environment for messages transmitted among sensor nodes,
2. Tamper with the content of messages,
3. Insert false messages in the network,
4. Insert itself on a privileged communication line and then drop a message.

Perrig et al. [9] designed a subsystem to provide security of communication in a wireless sensor network. Their messages are encrypted with secret keys. The whole subsystem was implemented in a small network at Berkeley, consisting of nodes communicating with a base station. Messages are either destined for the base station or originate at the base station.

Our paper describes a totally new approach to protecting the privacy of the data field. The method relies on quantum means to obtain security. We envision sensor nodes that have both a classical work memory and a set of quantum bits. Quantum cryptography methods will be used to establish effectively unbreakable secret keys.

Experiments with quantum bits are very impressive. Although mostly in the experimental stage, the age of commercially used quantum devices may be nearer than we expect. Already, practical implementations of the BB84 [3] protocol are commercially available.

Our security scheme has a requirement that is not yet practically feasible. Quantum bits, as used in our protocol, have to be *entangled*. Entanglement will be defined in the next section and has been obtained experimentally in several settings. Additionally, our quantum bits have to persist in time. That is, these quantum bits have to retain their state for a reasonable amount of time and be able to be moved and deployed with the deployment of the sensor nodes. Trapping and transporting entangled quantum bits has not yet been done. Nevertheless, once entangled quantum bits can be stored and transported, applications of the kind described in this paper become very attractive indeed.

The rest of the paper is organized as follows. Entangled qubits are introduced in section 2. Section 3 defines the sensor network with quantum properties. Section 4 describes quantum teleportation which is the essential means in our security scheme. The algorithm that allows secret message exchange in the network is given in section 5. The paper concludes with section 6.

2 Entangled Qubits in Quantum Cryptography

It is well known that quantum cryptography offers improved security for communication over classical cryptography. Two parties, Alice and Bob intend to communicate secretly. They go through a quantum key distribution protocol and establish a binary secret key. The key value is now known to both Alice and Bob. This secret key will be used afterwards to encrypt / decrypt classical messages. The secret key that is obtained from a quantum key distribution protocol has several desirable and important properties:

1. The secret key is unbreakable [10]. This means that the protocol that establishes the key, does not reveal any information about the value of the key. There is no advantage for an intruder, Eve, to listen to the quantum key distribution protocol. Any particular bit in the secret key still has a 50% chance of being either 0 or 1.

2. Intrusion detection is possible [10]. If Eve tampers with the messages and the quantum bits during the protocol, her presence is detected.

3. Information exchanged during the protocol is public [7]. There is no need for classical authentication, which would have typically required a small secret key known to Alice and Bob prior to the protocol.

Many quantum key distribution algorithms rely on entangled qubits [5, 4, 11]. Two qubits that are entangled share their quantum state. Consider an entangled qubit pair: Alice holds the first qubit and Bob holds the second qubit. If one party, say Alice, measures her qubit, Bob's qubit will collapse to the state compatible with Alice's measurement.

The vast majority of key distribution protocols based on entanglement, rely on Bell entangled qubits [8]. The qubit pair is in one of the four Bell states:

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

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

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

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

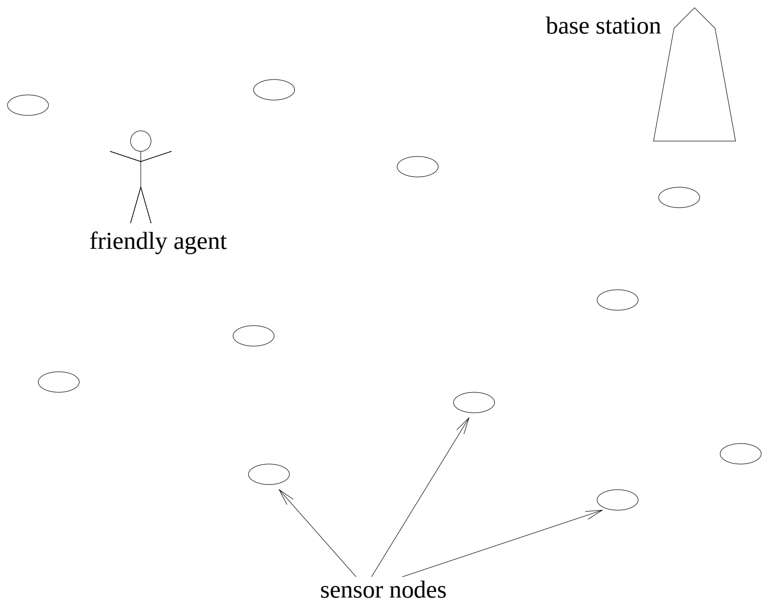

Figure 1: A network of sensor nodes with a friendly agent walking in the field.

Suppose Alice and Bob share a pair of entangled qubits described by the first Bell state:

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

Alice has the first qubit and Bob has the second. If Alice measures her qubit and sees a 0, then Bob's qubit has collapsed to $|0\rangle$ as well. Bob will measure a 0 with certainty, that is, with probability 1. Again, if Alice measures a 1, Bob will measure a 1 as well, with probability 1. The same scenario happens if Bob is the first to measure his qubit.

Note that any measurement on one qubit of this entanglement collapses the other qubit to a *classical* state. This property is specific to all four Bell states and is then exploited by key distribution protocols: If Alice measures her qubit, she *knows* what value Bob will measure.

3 The Definition of a Quantum Sensor Network

The goal of our sensor network is to monitor a geographic data field to the benefit of a mobile agent (or person) walking *in* the field (see fig. 1). The agent should be able to take decisions based on the information gathered from the field. Consider the following toy example. The agent is a fox hunting rabbits. The sensor nodes are able to detect the presence of a rabbit and also the size of the rabbit. The fox wants to be able to *know* where the rabbits are, without walking through the whole field, indeed it wants to get this information without moving from its present location. Once the fox knows about the position and sizes of the rabbits, it will decide to go catch the largest rabbit. The security question translates for our game to the following scenario. Besides the fox, there is also a large cat walking in the field. Formally, we will call the cat the intruder, or adversary. The cat also wants to catch rabbits. The problem of the entire network is to prevent the cat from gathering any knowledge about the rabbits in the field. The cat is able to listen to the environment and record the messages transmitted among the sensor nodes. The protocol presented below will make the messages unintelligible to the cat.

Sensor nodes are deployed at random in the field. We assume that the nodes know their geographic location. Each node has a small work memory to prepare and transmit messages. Also, an arbitrary node s has a set of n quantum bits $q_{s1}, q_{s2}, q_{s3}, ..., q_{sn}$. The only operation that the node needs to be able to perform on the qubits is to measure them.

The (legitimate) agent a has greater computational power, and a larger memory than a sensor node. It also owns a larger set of m quantum bits $q_{a1}, q_{a2}, q_{a3}, ..., q_{am}$, where $m > n$. The operations the agent is able to perform on its bits are: measuring and simple transformations. In fact, only two transformations are necessary: phase rotation (Z operator) and negation (NOT operator).

The agent wishes to be able to query the field. These queries give the agent information about the field. The collected information will then affect its decision and movement in the field. The adversary or intruder, on the other hand, is interested in gathering the same information as the legitimate agent but harbors malevolent plans. The sensor network should be able to answer the queries of the agent, while protecting its measured data from the adversary.

Wireless communication is not secure. The adversary can listen to the environment for broadcasted messages. Therefore, our security scheme will provide the means to encrypt the messages. The intruder will have no benefit from intercepting the messages.

To be able to effectively use the quantum bits, we will require the existence of a base station (see fig. 1). The base station is situated anywhere outside the field. It does not need to be in the communication range of any sensor node. It can be far from the sensor field, and is not directly connected to the sensor nodes. The agent is able to communicate with the base station on

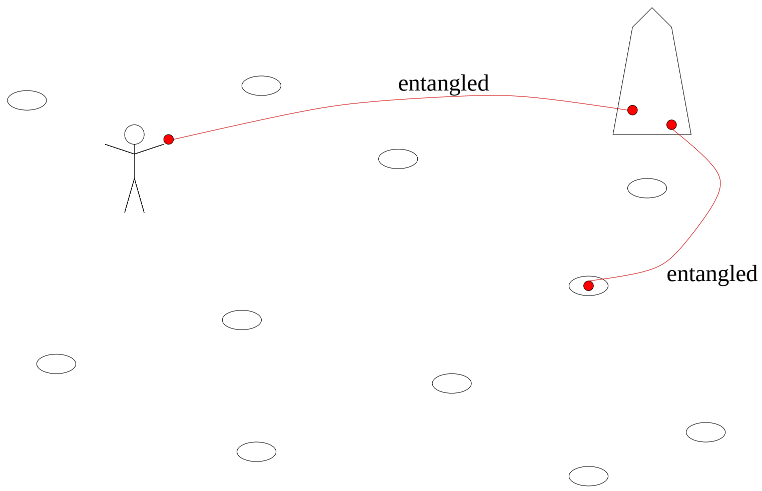

Figure 2: For every sensor node and for the agent, the base station manages the entangled pair of several qubits. The figure shows only one pair for the agent and one pair for an arbitrary sensor node.

an authenticated telephone line. This telephone line can be made available prior to any interaction between the agent and the field.

The reason for the base station is that it makes the connection between the agent and the sensor nodes in terms of quantum bits. Every quantum bit of the sensor nodes is entangled with a quantum pair physically situated at the base station. As such, the qubits of node s are pairwise entangled with a set of qubits at the base station $q^{'}_{s1}, q^{'}_{s2}, q^{'}_{s3}, ..., q^{'}_{sn}$. The base station manages these quantum bits and knows the connection between the quantum bits at the station and the geographic sensor nodes in the field. The entanglement is of the type Φ^+ as described in the previous section.

Additionally, the base station also owns a larger set of quantum bits entangled with the quantum bits of the agent $q^{'}_{a1}, q^{'}_{a2}, q^{'}_{a3}, ..., q^{'}_{am}$. This entanglement is also of the type Φ^+.

In short, both the sensor nodes and the agent are entangled via multiple quantum bits with the base station and the main purpose of the base station is to manage these quantum bits (see fig. 2). Following a quantum teleportation protocol, described in the next section, the base station will be able to entangle qubits of the agent with qubits of some chosen sensor node. The result is that the agent now is directly entangled with a sensor node of its choice and can establish a secure secret key.

It is important now to mention that in this security scheme, several objects are trusted, namely:

1. The base station is trusted. This is a reasonable assumption, as the

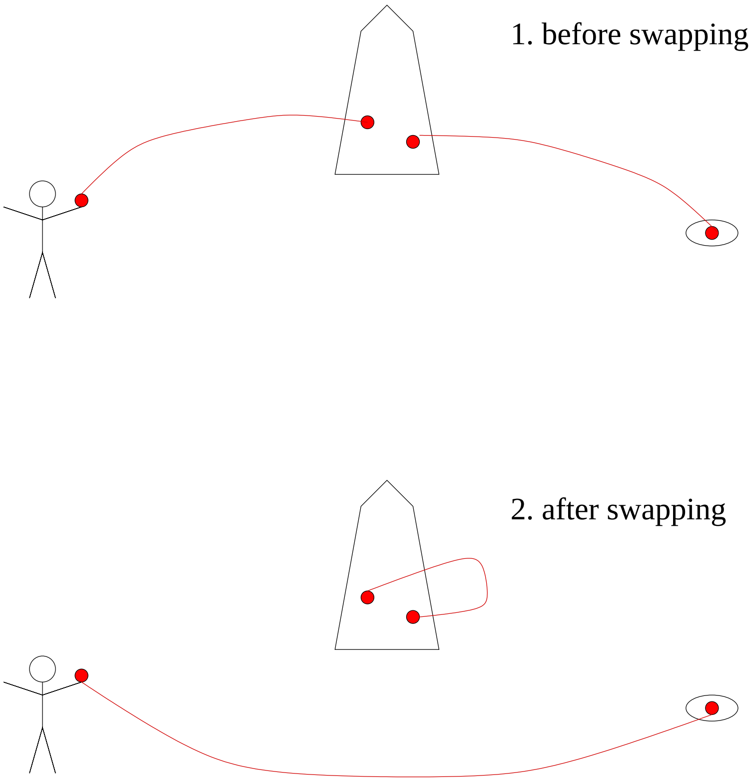

Figure 3: The entanglement is transferred to the two qubits belonging to the agent and the sensor node respectively.

base station is not part of the field and can be located in a secure place.

2. The agent is trusted. The agent is the basic decision making component and thus is given authority and trust.

3. The sensor nodes are trusted.

On the other hand, the environment is not trusted. Messages among sensor nodes can be freely intercepted. Also the telephone line between the agent and the base station is not secure, though authenticated. The adversary can listen to the telephone conversations.

4 Quantum Teleportation and Entanglement Swapping

Quantum teleportation was defined in [2, 12]. It refers to the transfer of an *unknown* quantum state from one geographical source location to another destination location. This state transfer does not involve any transfer of matter from the source to the destination. It needs an entangled qubit pair, with the first qubit located at the source and the second qubit located at the destination. The second qubit will receive the desired unknown state. In transferring the state to the destination, it disappears from the source, thus preserving the "no cloning" theorem [13].

To obtain the desired teleported state at the destination, two bits of classical information need to be sent from the source to the destination. Depending on this information, the destination qubit needs to be transformed by a simple gate. This property complies with the principle that information cannot be transmitted at a speed larger than the speed of light.

A variant of quantum teleportation is entanglement swapping (see fig. 3). Note that, in teleportation, the quantum state of the source qubit q_{source} disappears from the source location and reappears in the destination qubit $q_{destination}$ as exactly the same state. If the original state q_{source} was entangled with some other qubit q_{pair}, this entanglement will be transferred to the destination qubit $q_{destination}$, causing the latter to be entangled with q_{pair}. This scenario is called entanglement swapping and has been demonstrated in practice [6].

Quantum swapping will be described in detail below in the particular setting of our sensor network. Quantum swapping is the basic step towards private communication between the agent and some sensor node.

Consider some qubit of the agent q_{ai} entangled with its base station companion qubit $q_{ai}^{'}$. The agent intends to communicate secretly with node s. The node's qubit offered for this entanglement swapping may be q_{sj} entangled with the base station's qubit $q_{sj}^{'}$. These four qubits form an ensemble

$$ensemble = q_{ai}q_{ai}^{'}q_{sj}^{'}q_{sj}.$$

Note that, the first qubit of the ensemble belongs to the agent. The second and third qubits belong to the base station and the fourth qubit belongs to the sensor node. This order has been chosen so that the transformations applied by the base station and the agent are easier to see. As both the agent's qubit pair and the sensor node's qubit pair are entangled in the Φ^{+} Bell state, the ensemble can be rewritten as

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

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

The following formula rewrites the base station's two qubits highlighting the Bell basis

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

$$+|0\rangle \otimes \frac{1}{\sqrt{2}}(|\Psi^+\rangle + |\Psi^-\rangle) \otimes |1\rangle +$$

$$+|1\rangle \otimes \frac{1}{\sqrt{2}}(|\Psi^+\rangle - |\Psi^-\rangle) \otimes |0\rangle +$$

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

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

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

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

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

The base station now measures qubits two and three, located at the station. The qubits are measured in the Bell basis (Φ^+, Φ^-, Ψ^+, Ψ^-).

It is interesting to see what happens to the state of the other two qubits after this measurement. The base station will have to communicate the result of the measurement to the agent. This is done via the insecure classical channel. If the station's measurement was:

1. Φ^+. The remaining qubits have collapsed to

   $$ensemble_{1,4} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

   This is a Bell Φ^+ entanglement, the desired one. The agent and the field node are now entangled.

2. Φ^-. The remaining qubits have collapsed to

$$ensemble_{1,4} = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

This is not quite a Φ^+ entanglement, but can be easily transformed into it. The agent has to change the phase of his qubit and can do so by applying the gate defined by the Pauli matrix [8]:

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

3. Ψ^+. The remaining qubits have collapsed to

$$ensemble_{1,4} = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

In this case the agent has a qubit in which the bit values ($|0\rangle$ and $|1\rangle$) compared to the field node are reversed. The agent has to apply the gate for the Pauli matrix that performs a NOT:

$$NOT = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

4. Ψ^-. The remaining qubits have collapsed to

$$ensemble_{1,4} = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Now the agent's qubit has both the bit values reversed and the phase is also rotated. Thus, the agent will apply a gate defined by the product:

$$Z \cdot NOT = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

The agent has to communicate with the base station in order to know what transformation, if any, to apply on his qubit to obtain the final Φ^+ entanglement with the field node. This is why they need a telephone line. The base station communicates to the agent the outcome of its measurement. As there are four possible measurement outcomes, two classical bits suffice to discriminate among the measurements.

After this step, the agent and the field node have Φ^+ entangled qubits, without having ever met.

5 Security Protocols

The following two scenarios will be discussed

1. **Agent query**. The agent has a map of the field and wishes to obtain information from a selected location (x, y) regarding a possible event e. The location (x, y) to be queried will be visible by the intruder. Yet, the nature of the event and the parameters of the event will be private.

2. **Sensor node event signaling**. A sensor node located at (x, y) detects an event of importance. It sends a signal to the agent. The agent then queries the node as to the nature and parameters of the event. Again, the intruder will know the location of the event but will not have any information about the nature of the event and its parameters.

We are ready now to describe an algorithm that allows the agent to query the field in some specific location. For simplicity, let us consider that the secret key that will encrypt the messages is just three bits long, $k = k_1k_2k_3$. This is of course a short key for practical purposes. The agent query algorithm follows the steps below:

1. The agent a sends the location (x, y) of the query to the base station.

2. The base station locates a sensor node s that is closest the (x, y) and performs an entanglement swapping for three qubit pairs.

3. The agent and the node s establish a secret key k of three bits.

4. The agent uses this secret key to encrypt a message containing the nature of the event of interest. Then it broadcasts the message in the network. The message will be unintelligible to all nodes except s which shared the secret key k.

5. When s receives the encrypted message, it reads the parameters of the requested event. These parameters are then encrypted using the same key k. The new message is broadcasted in the field again and the agent eventually receives the desired information.

Most steps are straightforward and need no further explanation. We will insist on step 3, establishing the secret key. The agent and the node share three entangled quantum bit pairs. Remember that we trust both the agent and the node. A simple measurement performed in the computational basis will yield the same three classical bits for both the agent and the node. These three classical bits are the key k.

In the second scenario, in which the sensor node is signaling the event, the procedure is very similar to the previous one. One step is performed ahead of the previous algorithm.

1. The sensor node that has detected an event broadcasts its location on the network. The agent will read this message with the position of the sensor node and start a query procedure with this location.

The important feature of both algorithms is that the wireless environment does not reveal the measured parameters, nor the nature of the event. The only information which is not encrypted in the network is the location of the event or query.

Note that, in the process that establishes the value of the secret key, no information concerning this value is ever visible in the environment. The key is therefore unbreakable by the intruder listening to the environment.

6 Conclusion

We have shown that sensor networks can benefit from quantum cryptography. In particular, the issue of security in sensor networks can find basic solutions in the already well established field of quantum cryptography.

We described a security scheme for sensor networks using entangled qubits. The scheme protects the measured data of the field in the insecure wireless environment.

The intruder is considered to be able to listen to the environment, but is considered unable to inject data in the data field or corrupt a sensor node. The issue of the intruder behaving as a sensor node in the field and injecting false messages will be treated in a future work.

In the definition of the sensor network we considered all sensor nodes to be trusted. This is a strong assumption. It might be expected, that an intruder may try to insert itself in the network or corrupt an existing sensor node and then send spurious messages. Work is in progress to adress these issues in future schemes.

Acknowledgement

The authors wish to thank Waleed Al Salih for his important comments on this paper.

References

[1] H.M.F. AboElFotoh, E.S. ElMallah, and H.S. Hassanein. On the reliability of wireless sensor networks. In *IEEE International Conference on Communications (ICC)*, pages 3455–3460, June 2006.

[2] C.H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W.K. Wootters. Teleporting an unknown quantum state via dual classical Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70:1895–1899, 1993.

[3] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, IEEE, New York, 1984. Bangalore, India, December 1984.

[4] Charles H. Bennett, Gilles Brassard, and David N. Mermin. Quantum cryptography without Bell's theorem. *Physical Review Letters*, 68(5):557–559, February 1992.

[5] Artur Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67:661–663, 1991.

[6] Matthus Halder, Alexios Beveratos, Nicolas Gisin, Valerio Scarani, Christoph Simon, and Hugo Zbinden. Entangling independent photons by time measurement. *Nature Physics*, 3:659–692, 2007.

[7] Naya Nagy, Marius Nagy, and Selim G. Akl. Key distribution versus key enhancement in quantum cryptography. Technical Report 2007-542, School of Computing, Queen's University, Kingston, Ontario, 2007.

[8] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[9] Adrian Perrig, Robert Szewczyk, Victor Wen, David E. Culler, and J. D. Tygar. SPINS: security protocols for sensor netowrks. In *Mobile Computing and Networking*, pages 189–199, 2001.

[10] Jr. Samuel J. Lomonaco. A Talk on Quantum Cryptography or How Alice Outwits Eve. In *Proceedings of Symposia in Applied Mathematics*, volume 58, pages 237–264, Washington, DC, January 2002.

[11] Bao-Sen Shi, Jian Li, Jin-Ming Liu, Xiao-Feng Fan, and Guang-Can Guo. Quantum key distribution and quantum authentication based on entangled states. *Physics Letters A*, 281(2-3):83–87, 2001.

[12] Lev Vaidman. Teleportation of quantum states. *Phys. Rev. A*, 49(2):1473–1476, Feb 1994.

[13] William K. Wootters and Wojceich H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, October 1982.

[14] Feng Zhao and Leonidas Guibas. *Wireless Sensor Networks - An Information Processing Approach.* Elsevier, 2004.