Low cost solutions to pairing issues in IEEE 802.15.4 networks.

Authors: M. Meli, M. Gysel, M. Würms

Marcel Meli
Email: Marcel.Meli@zhwin.ch
Tel: +41 (0)52 267 72 47
Fax: +41 (0)52 268 72 47

Abstract
The last years have seen an important increase in the development and proliferation of wireless technologies. This success, mostly related to mobility and the relative ease with which wireless devices can be linked (no wires needed between parties), has affected consumer as well as industrial applications. There are however many areas that are still closed to the introduction of wireless systems. Among the factors that affect wireless acceptance, one can name security and the complexity often involved in setting up networks. Unlike wired systems, the extra confidence afforded by "seen wires" is not available in wireless systems, making it difficult for the users to know if communication occurs between legitimate parties. This places wireless technology before the need to introduce simple methods to improve the set up and authentication processes. These aspects are addressed by binding methods.
It is our purpose in this document to present such solutions, and especially how they can be used in 802.15.4 based networks. We will mainly focus on solutions involving optical or RFID techniques. We will also suggest some improvements where needed.

1. Introduction.

One of the great advantages wireless systems confer is mobility. Devices of reasonable size can be easily moved, and made to interact with each other. Several devices can be joined in

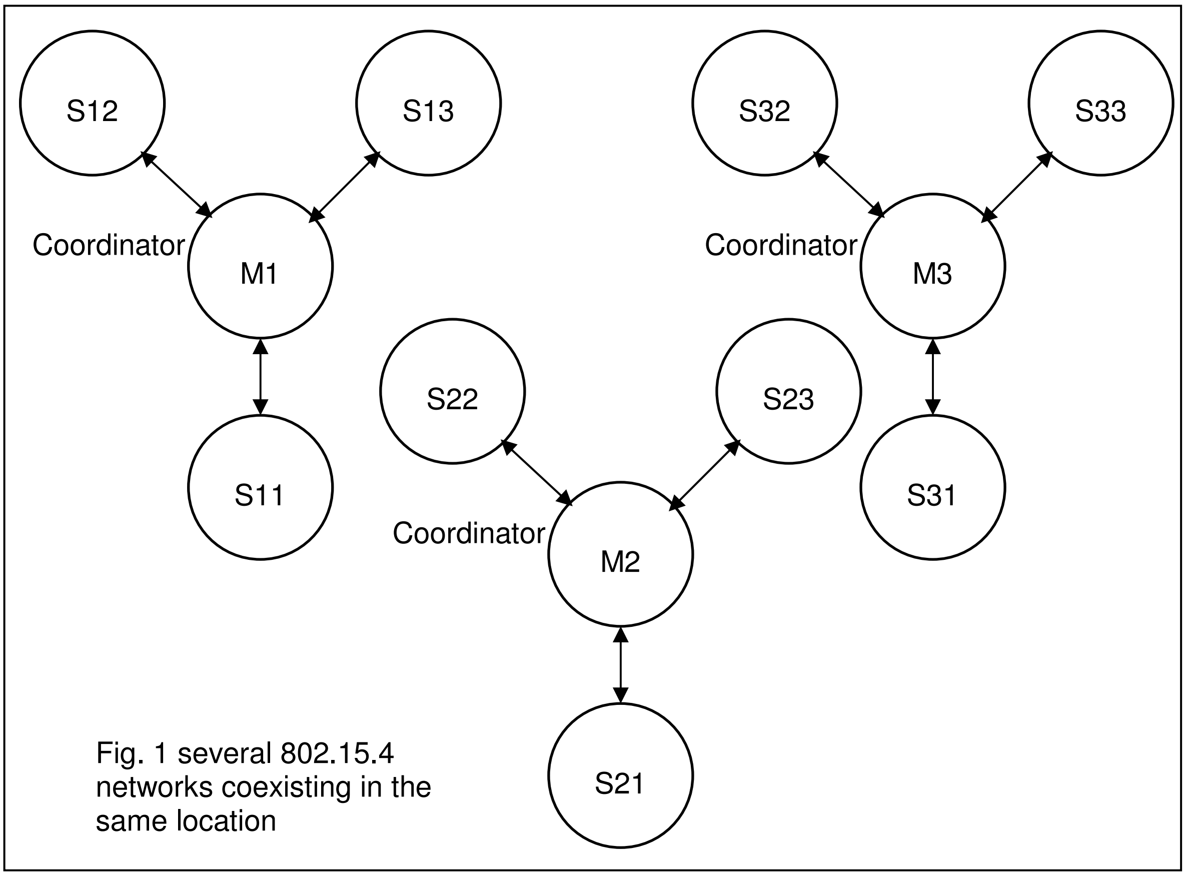


Fig. 1 several 802.15.4 networks coexisting in the same location a network for a limited amount of time, then disassociate and join other networks. This greatly improves the ability of sharing resources, but comes with its challenges. The difficulties of Bluetooth pairing scheme have been well documented [19]. For example, wireless monitoring devices in a hospital environment sending their data to the wrong monitors could lead to mistakes. The problem is even more acute if it is desired in the pairing process to minimize interference with other networks.

Let us illustrate all this with Fig. 1
The description is based on 2.4 GHz star networks of 802.15.4.
3 networks that are physically near one another are formed around network coordinators M1, M2, M3. A different frequency band is used for each network. Communication between devices in a network goes through the coordinator
For network N1 we have devices M1, S11, S12, S13 ,
For network N2 we have devices M2,S21,S2 ,S23
For network N3 we have devices M3,S31,S32,S33.

In N1, M1 is attached to a PC used for reporting the data of patient Meier. Devices S11 and S12 are attached to medical instruments used for the consultation. S13 is attached to a small printer.
Network N2 is identical to N1, but is used for patient Mueller.
Network N3 is used for patient Schweizer, with a data been sent to a monitor instead of a printer.

At one point, it might be decided to move the medical device S21 from Network N2 to network N3, and to add the printer S13 to N3. The printer should only print data from S21.
The measurement now done for patient Schweizer dare not appear in the logs for patient Mueller, and vice versa. Measurements in progress should not be affected by the new set up.

To be able to move devices from network to network as the need occurs, a reliable and simple way to quickly bind device to device or device to network is needed. The frequency of these changes depends on the application for which the wireless systems are been used. It is desired to operate the changes in an easy and reliable way. Ideally, communication in the networks should not be disrupted (at least not to the point of loosing valuable data). The communicating parties should also be clearly identified to avoid data be sent to the wrong device.

2. Definition.

We use binding here to refer to 2 things:

- A transfer of information that allows a device to join a network with minimal disruption of other communications. We will refer to this as pairing a device and a network (or associating a coordinator an a device, but with minimal disruption to the ongoing communications).
- A transfer of information that allows devices within an established network to transfer their information exactly to the proper partners. We will refer to this as pairing a device to a device.

3. Requirements.

To accomplish pairing, extra information must be shared between the parties that want to communicate.
There is some diversity in the kind of information that should be shared. It can be the identities of the parties that want to communicate, for example the addresses of the end points that should communicate. It can also be information about the network that should be used for communication, for example the channel number in 802.25.4. It can also be a secret to help establish a secure link, or any other information needed by the application. This extra information could be provided by the parties themselves or a by a third party. For

example a user can enter the identity of the communicating parties, a password, etc. The information could also be automatically generated. For example the random generation of a shared key that will then be passed on to the parties that want to communicate. The quantity of the information to be shared is generally small, but can influence the way this sharing should occur. For example, a system where a user is frequently required to manually enter 20 bytes of information will be slow and prone to many failures.

The channel used for sharing the information can in some cases be the main communication network (for example a dedicated channel of 802.15.4). Generally, an out-of-band link, that is another type of link, is used. For instance, a keypad can be used by the user to enter the information for the parties that should establish a communication. The way the information is shared will affect the security of the system, and its costs. It will also impact the speed at which this sharing can occur and thus its acceptance by users.

3.1. Factors to consider when choosing a pairing method.

3.1.1. Purpose of pairing in the application.

One must be clear as to the goals of pairing in the application, and how much information is to be shared.

3.1.2. Size of the groups to pair

How large are the groups to pair? For example is one lamp to be paired to just one switch or with several switches.

3.1.3. Proximity of the elements to pair

How mobile are the parties that will need pairing? Are they too large to be displaced? Are they easily accessible?

For example lamps on a ceiling that is 3 m high are less accessible than a switch near the door.

3.1.4. Frequency of pairing

How often is pairing likely to occur? It could be several times a day and once a year, or even once in the life time of a product.

3.1.5. Who should do the pairing

Is paring to be done at the production’s site or/and at the user’s site?

Is pairing to be done only by qualified personnel or by less trained end customer?

In the case of qualified personnel, the use of more expensive and sophisticated pairing tools is well acceptable.

3.1.6. Interface for pairing

How should pairing be done? Simply by pushing a few buttons or by entering a complicate code sequence. How should one verify that the pairing process was successful?

If the user has a large part in entering the pairing information, then an appropriate user interface should be provided.

3.1.7. Environment of use

Are the pairing methods acceptable in the environment of use?

For instance use of a light channel in an environment where strong light sources are present could present additional challenges.

What will be the effect of pairing on other networks (if they exist)? Sending Association request on each channel of 802.15.4 could increase the number of retries (or fail deliveries) for communications that are in progress in the vicinity.

3.1.8. Extra costs

Pairing will often come with extra costs. This could be in hardware (switches, tags, etc), in software (extra memory needed), development time, certification process, training of service personnel, …etc.

It will however also bring important advantages such as increasing the acceptance of a product, and even lead to the reduction of servicing costs.

The extra cost should be taken into account, but also the benefits.

4. Pairing methods.

We will briefly present some pairing methods that can be used for 802.15.4

Basically, each device can be equipped with extra hardware for the out-of-band link. This can be seen as some kind of shared memory. It will allow the retrieving and writing of pairing information by means of another link. The data written contain information to allow and easy set up of the wireless communication (frequency band, security ,…). Many papers listed in the reference section describe such methods.

4.1. Use physical links or devices with sophisticated user interfaces

Some methods such as electrical contact [14] , use of sound [9],[15], ultrasound[6], use of shaking [5] have been successfully used for pairing. Electrical pairing is easy to implement and relatively low cost. It requires appropriate mechanical contacts and memory. Data exchange is initiated by bringing devices in contact at the appropriate points. Cambridge Consultants has also developed a software pairing method based on RSSI [20]. Those methods will not be discussed in this paper.

We will also leave out the use of PCs or tools with very sophisticated user interface that allow the manipulation of tables for hundreds of devices, and the automation of the binding process using the main wireless channel. For easy systems and for many normal consumers, this might prove a difficult and slow method. In some applications, it could even be unacceptable to have a complicated user interface.

4.2. Use of switches.

Switches have been used for years in order to bind wireless devices [1,2].Basically, devices are fitted with switches that will be pressed by the user to start the binding process. This method can often be found in wireless mice and keyboards that need to be paired with a computer. The mouse, keyboard and a device linked by wire to the computer are all equipped with a button. Once the button is pressed, the device sends a pairing message for a certain time on a wireless channel. Pressing the button on the mouse or keyboard will cause it to scan the channels, searching for the channel where the pairing message is been sent, and in this way agree with the computer on a communication channel. A timeout is used to create a time window in which the binding is possible.

For 802.15.4 the method will work well between coordinator and a slave that is joining the network. Network disassociation can be made to occur by depressing the button for a longer time. In order to pair 2 devices that have already joined the network, it might be necessary to add an extra button for that purpose.

4.2.1. Advantages

The method is cheap (requires very few components or software) and very easy to implement.

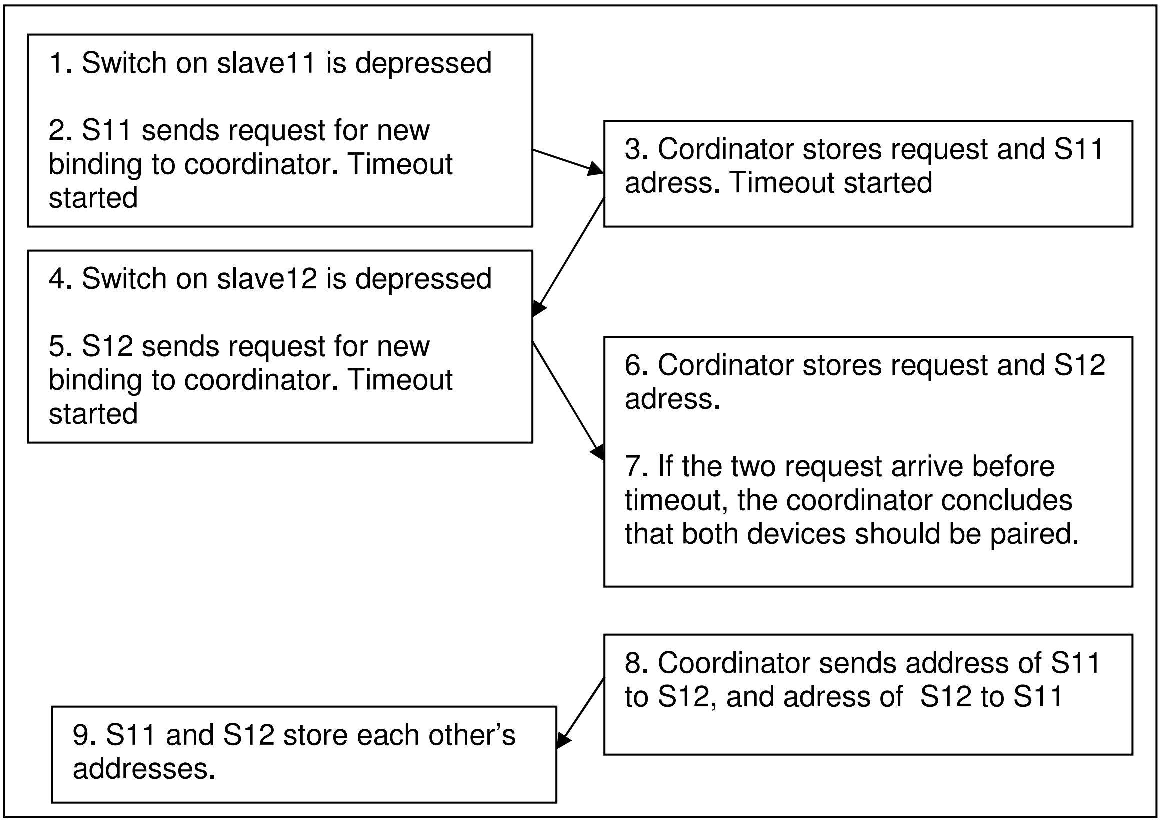
4.2.2. Disadvantages

The method is limited.

Basically, only a bit can be shared. In order to have diversity in the information that can be shared, many switches need to be combined or one must play with different depressing time. The limited robustness and the placement of the switch (if mechanical) might also be a disadvantage.

Switches have also been replaced by Hall Effect devices [2] to automatically start the binding process when the devices are near one another.

The following steps show how 2 slaves in the same network can be paired.



1. Switch on slave11 is depressed

2. S11 sends request for new binding to coordinator. Timeout started

3. Cordinator stores request and S11 adress. Timeout started

4. Switch on slave12 is depressed

5. S12 sends request for new binding to coordinator. Timeout started

6. Cordinator stores request and S12 adress.

7. If the two request arrive before timeout, the coordinator concludes that both devices should be paired.

8. Coordinator sends address of S11 to S12, and adress of S12 to S11

9. S11 and S12 store each other's addresses.

4.3. Use of IrDA (transceiver and stack) (Fig. 2)

Binding methods that use IR or visible light [8, 18] have been proposed
One is to fit the devices that are to be paired with IrDA communication (Transceivers and Stack). To pair devices, they have to be brought near one another by the user, so as to allow communication over the optical link. The exchange of data can be triggered by the user (using a switch) or started automatically as soon as the devices are near enough.
A dedicated IrDA device can be used, or the IrDA stack can be integrated in the software of the device's processor. Also, it is not necessary to support the whole stack. A procedure can be implemented on the application level to restrict the access to pairing data to authorised parties. Thanks to the wide use of IrDA, the HW cost of implementing IrDA has gone down. But it could still prove much for price sensitive devices.
For the user, use of light (line of sight) to communicate will imply the need to properly align the devices. This might be seen as an advantage (pairing muss really be wanted) or a disadvantage.

4.3.1. Advantages

The main advantage of this solution is that the interface for pairing is standard.
Lots of data could be transferred between the pairing parties without much intervention from the user.

4.3.2. Disadvantages

Near the need to for designers to deal with yet another technology, the solution is too expensive for some applications. If an own stack is used, certification will also be an issue. The devices should be so designed as to allow light to get to the IR sensors, and the light transceiver must be kept clean and unobstructed. The issues about primary and secondary devices muss be well though of when working with IrDA. Pairing more than 2 devices at once is difficult and unpractical.

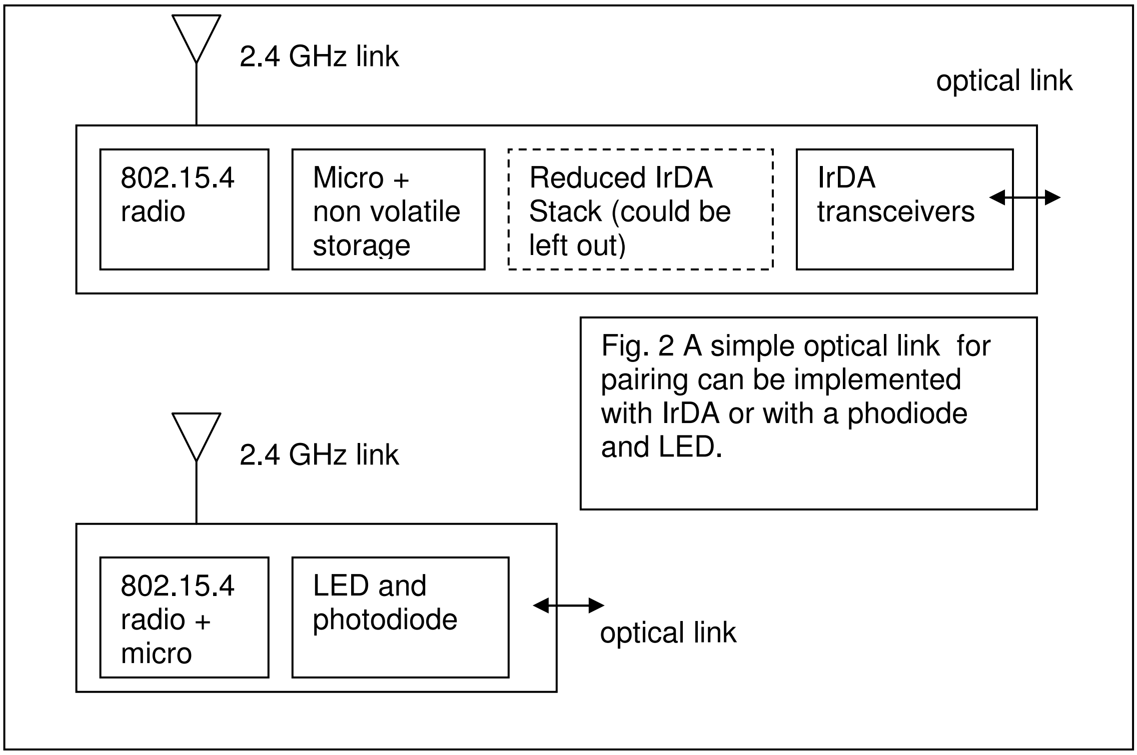


Fig. 2 A simple optical link for pairing can be implemented with IrDA or with a phodiode and LED.

Some of the disadvantages mentioned above can be reduced in the following way.

- Use of IrDA transceivers, no IrDA stack

To reduce the cost and the complexity of using an IrDA stack (even a light version), one could just use the infrared transducers and develop an own firmware to deal with the transfer of the needed data.

- Another way to reduce costs is to fit devices with a proprietary light link made up of a LED and a photodiode working in the visible spectrum. Appropriate software will then be used to enable communication. Proper modulation can reduce interference from other light sources and ensure that an acceptable data rate for transmission is possible on very short distances. In principle, the amount of data needed for pairing in this kind of application will be in tens or hundreds of bytes, making the data rate nearly irrelevant. This solution has the extra advantage of making it possible to use the LED also for other functions.

- Since it is possible to use an LED in reverse mode as a photodiode, one could also build a communication scheme based on one LED. This LED could be used for normal device functions, or when needed for pairing activities. A good description of such a system can be found in [13], [17]. This is certainly a very low cost method. Our own experience has shown that great care is needed in selecting the LEDs that are used for this type of application, and to adjust them to the microcontroller. The data rate achieved is low, but this is no major disadvantage.

4.4. Use of RFID methods

RFID technology has also been used for the pairing of wireless devices [3].

A tag or a transponder is needed in each device that requires binding. Information is written in the tags by an RFID writer/reader. This information is then read by the device at the needed time, and used as binding parameter (Fig. 3). Tags need to be accessible both by the external reader/writer, and the local microprocessor. This method can be implemented by using some standard RFID components or modules. A certain understanding of RFID technology is however needed to make the right choices of components and implement the system integration.
Pairing could be made to start as soon as the devices are near one another, or dependant on a users input. Line of sight is not necessary. However, the system might be susceptible to the orientation and size of the antenna, and the strength of the magnetic field.

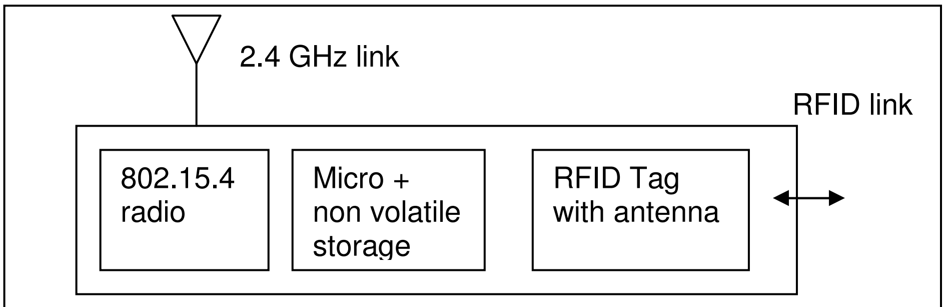


Fig. 3 An RFID tag on the device to be paired, can be used to write and store the necessary information.

NFC (near field Communication) is a standard based on 13.56 MHz RFID that enables applications such as pairing [16]. It is foreseen to enable automatic associations for some wireless standards.

4.4.1. Advantages

NFC is a standard. Line of sight not needed. Lots of information can be stored. Proximity is needed for pairing, meaning that the operator has a certain control over the operation.

4.4.2. Disadvantages

Near the need for engineers to be trained in RFID technology, the implementation of pairing in 802.15.4 systems is still expensive. Certification issues may also need to be addressed.

Since it is foreseen to equip mobile phones and PDAs with NFC, the cost of the technology will go down. This could become a very interesting solution for the pairing 802.15.4 systems With the help of an extra device that is equipped with an NFC reader.
NFC readers can also read and write tags. The 802.15.4 devices will only need to be equipped with an appropriate tag that can also be read by the local processor. The binding reader will then be used to read and program the proper information in all the parties that need to be paired.

As in the case of IrDA, proprietary solutions are also possible. Only so much hardware and software as necessary can be used, in order to keep prices and complexity down.

- A minimal system will simply store the MAC address of the 802.15.4 in a tag. That address can then be read every time the device is brought near a coordinator equipped with a reader.
- Each device may also be equipped with a reader/writer, but this will add to the cost of the devices. Although it is possible to do this for simple RFID system, it seems best to

equip one device (the network coordinator for example) with the ability to read and write tags.

4.5. Pairing for systems with difficult accessibility.

One feature of the methods considered so far is that the devices to pair can be easily accessed, or brought together. Or at least, one could easily take a special binding device to them to initiate the pairing. This proximity itself is an important factor is communicating a shared secret. In some applications, proximity is not guaranteed
For devices that are physically too distant to allow pairing by proximity, other methods have been suggested. Use of ultrasound as out of band channel or the use of a laser pointer device to communicate the shared secret [4,7,8,11]
We will only discuss the second method here.

A device is equipped with a visible pointing laser, whose light is modulated in function of the message to send. A message generator insures that a different shared secret message is communicated for each pairing session. The devices to be paired are equipped with the appropriate light sensors to receive the message from the pointing laser. binding is achieved by sending the message to parties that need to be associated. They can then find one another over the RF link using the shared secret and the appropriate algorithms.
At the minimum, the laser light can be compared to a long finger used to activate a switch. It could also be seen as a write only device that can send a complex message. In some cases, the pointing device could be equipped with an RF channel that will allow a bidirectional communication in order to give some feedback and improve the pairing process.

One important advantage of the pointing device is its ability to work with close and far targets. It could be designed for simplicity and low cost, and use for pairing activities as an IR remote control device will be used. Another advantage is the possibility of the user to actively and easily select the devices that he wants to pair. The visible laser light provides an important element for selection and for confidence. The area where the laser beam should be pointed must be so marked that the user will see it from distance and easily target it.
Among the drawbacks to consider when implementing such a system are:

- The possibility of jamming the receiving device by shining a signal on the target
- The possibility (because of light reflections) to send the message to an unintended party on which the light is reflected. It is also relatively easy for a third party who has access to the premises to listen to the shared secret.

5. <u>Conclusion.</u>

Designers of IEEE 801.15.4 based wireless systems can benefit from the experience made with other wireless standards in order to incorporate fitting pairing techniques in their products. This calls however for careful choices in order to deliver appropriate products and competitive prices. In order to further the interoperability issues, it might be worth considering the use of an appropriate subset of the NFC standard. For the pairing of devices that are inaccessible but visible, laser pointing is an acceptable alternative.

6. References

[1] http://www.howstuffworks.com/mouse.htm/printable

[2] patent 20070070035: Method for pairing 1-way devices without buttons

[3] http://www.logitech.com/pub/pdf/bluetooth/secure_connect_whitepaper.pdf
Logitec secureconnect mouse: A major leap in the cordless desktop experience.

[4] A Human-Verifiable Authentication Protocol Using Visible Laser Light. Rene Mayrhofer and Martyn Welch Computing Department, Lancaster University
Improved laser pointer for identification.

[5] R. Mayrhofer and H. Gellersen. Shake well before use: Authentication based on accelerometer data. In Proc. Pervasive 2007: 5th International Conference on Pervasive Computing. Springer, May 2007. to appear.

[6] R. Mayrhofer, H. Gellersen, and M. Hazas. An authentication protocol using ultrasonic ranging. Technical Report COMP-002-2006, Lancaster University, October 2006.

[7] S. N. Patel and G. D. Abowd. A 2-way laser-assisted selection scheme for handhelds in a physical environment. In Proc. UbiComp 2003: 5th Int. Conf., pages 200–207. Springer, October 2003.

[8] M. Ringwald. Spontaneous interaction with everyday devices using a PDA. In Proc. Workshop on Supporting Spontaneous Interaction in Ubiquitous Computing Settings, September 2002.

[9] [4] M. T. Goodrich, M. Sirivianos, J. Solis, G. Tsudik, and E. Uzun. Loud and clear: Human verifiable authentication based on audio. In Proc. ICDCS 2006: 26th Conf. on Distributed Computing Systems, page 10. IEEE, July 2006.

[10] J.-H. Hoepman. The emphemeral pairing problem. In Proc. 8th Int. Conf. Financial Cryptography, pages 212– 226. Springer, February 2004.

[11] T. Kindberg and K. Zhang. Secure spontaneous devices association.
In Proc. UbiComp 2003: 5th Int. Conf., pages 124–131. Springer, October 2003.

[12] Brian Brooker. Wireless binding methodologies.
AN6066, Cypress Semiconductor Corporation

[13] P. Dietz , W. Yerazunis, W.Leigh. Very low-cost sensing and communication using bidirectional LEDs. In Proc. UbiComp 2003: 5th Int. Conf., pages 124–131. Springer, October 2003.

[14] F. Stajano and R. J. Anderson. The resurrecting duckling: Security issues for ad-hoc wireless networks. In 7th Security Protocols Workshop, volume 1796 of Lecture Notes in Computer Science, pages 172–194, Cambridge, United Kingdom, 1999. Springer-Verlag, Berlin Germany.

[15] Claudio Soriente, Gene Tsudik, Ersin Uzun, "HAPADEP: Human Assisted Pure Audio Device Pairing". Cryptology ePrint Archive 2007.

[16] www.nfc.com
http://www.nfc-forum.org/resources/white_papers/nfc_forum_marketing_white_paper.pdf

[17] patent US2004208632 : Communication using bi-directional LEDs

[18] Balfanz, D., Smetters, D., Stewart, P., Wong, H.C.: Talking to Strangers: Authentication in ad-hoc wireless networks. In: Proceedings of the Symposium on Network and Distributed Systems Security (NDSS 2002), San Diego, CA, Internet Society (February 2002)

[19] Y. Shaked and A. Wool. Cracking the Bluetooth PIN.
In Proc. 3rd USENIX/ACM Conf. Mobile Systems, Applications, and Services (MobiSys), pages 39-50, Seattle, WA, June 2005.

[20]
http://www.cambridgeconsultants.com/Downloads/Case_Studies/ZigBee_click_and_pair.pdf