A Security Application of the Warwick Optical Antenna in Wireless Local and Personal Area Networks

I. Pavlosoglou, R. Ramirez-Iniguez, M. S. Leeson and R. J. Green ‡

‡ Communications & Signal Processing Group, School of Engineering, University of Warwick.

Abstract: The objective of this paper is to propose an implementation utilising the Warwick optical antenna for securing wireless communications in a combined radio and infrared environment. By treating the infrared channel as a protected medium for exchanging information, security can be maintained in any radio communication taking place in the local or personal area network, provided the correct methods are used.

1 Introduction.

One of the advantages of using infrared (IR) radiation as part of the physical medium for indoor wireless communications lies in the fact that infrared light, sharing many of the features of visible light, does not have the ability to propagate through opaque barriers, leaving the signal confined within the room from which it originated [1].

Thus, provided that our selection of the configuration for the wireless optical link is a line-of-sight (LOS), requiring an unhindered path between the two ends and either involving a directed transmitter, with a narrow beam radiation pattern (figure 1a), or a non-directed transmitter with a broad-beam radiation pattern (figure 1b) [2], any data exchange taking place can be targeted to, if not a single device, a limited number of devices closely located to each other.

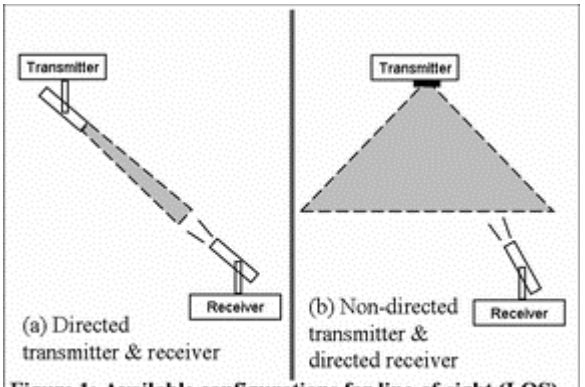

Figure 1: Available configurations for line-of-sight (LOS) optical links.

From a security perspective, having the ability to target the data flow on the network to particular users and devices, straight from the physical layer, provides us with a great advantage towards any form of passive or active eavesdropping.

A malicious user, wanting to listen in to the information exchange between any two devices on the network (passive eavesdropping) or even try and modify the data being sent (active eavesdropping) would have to satisfy either of the following two requirements:

- Be physically present within the line-of-sight (LOS) of the transmitter and receiver.
- Have the ability to fool the receiving party towards the origin of the received data.

Both these requirements take the burden of security in networks from the protocol and application layer to the concept of physical security. Information is no longer sent in a broadcast manner, leaving it to encryption and authentication procedures for securing any data exchange. Instead, the user is responsible for what data travels to what device, by means of pointing the transmitter towards the required receiving party.

Today, infrared wireless links are used to bypass the encryption and authentication stages necessary for securing Radio Frequency (RF) communications [3], thus taking a huge weight of the network (in terms of traffic) and the device (in terms of processing power), allowing the secure data exchange in broadband channels without any further requirements other than a LOS between the sender and receiver.

For Local Area Networks (LANs) and Personal Area Networks (PANs), combining the security advantages of infrared, with the broadcast nature and connectivity of RF could provide a way of securing diverse communications (such as ad-hoc networking), taking place in a dynamic environment, where the number of devices and links may vary in time.

2. Utilising the Warwick optical antenna.

One of the most important parts in a wireless infrared receiver is the optical front end. By carefully designing and using an optical concentrator it is possible to increase the effective collection area of the receiver. Doing so enables us to improve on power, which in turn allows for an increase of the distance between the transmitter and receiver or a decrease in the receiver capacitance, thus allowing the use of smaller photo-detectors [4].

The Warwick optical antenna represents such a front end to an optical receiver. By using a rotationally-symmetric, dielectric totally internally reflecting concentrator (DTIRC) it is feasible to achieve concentrations close to the theoretical maximum limit. This is done by combining front surface refraction with total internal reflection from the sidewall. The idea originates from solar concentration [5], but it has been proven that DTIRCs work effectively in optical wireless receivers [6] as well.

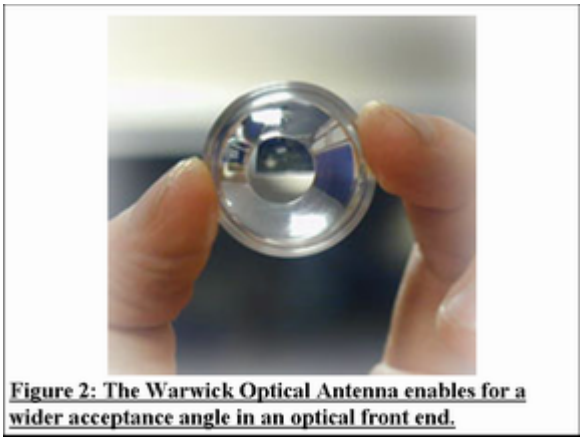

Figure 2: The Warwick Optical Antenna enables for a wider acceptance angle in an optical front end.

The key advantage in using an optical receiver with a wider acceptance angle for securing wireless communications lies in the wider field-of-view (FOV) of the optical front end.

Positioned as shown in figure 3, typically at the physical entrance(s) of the area where the wireless LAN or PAN is operating, the infrared link can act as an alternative secure channel for data exchange prior to initialising an RF link with the network.

Hence, in a typical scenario, consider an office environment having wireless RF capabilities similar to those described in the IEEE 802.11x wireless LAN standard and a user with a portable device, such as a Personal Digital Assistant (PDA) or 3G mobile phone, having both wireless RF and infrared capabilities[1]. Since the devices in such an environment, are not fixed, securing any data exchanged or providing means for authenticating users poses as a very difficult task; if we are to use RF all information is out in the open. As a result any attempt to exchange a secure key, that would enable us to use encryption algorithms for securing the data sent, can be easily eavesdropped.

By utilising an infrared link, located at the physical entrance of the wireless network, any user, as they enter the area, can exchange any number of keys using a secure channel, which can later on be used for authentication and encryption purposes.

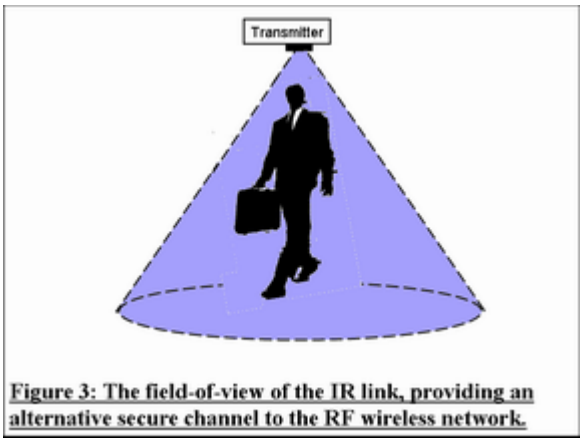

Figure 3: The field-of-view of the IR link, providing an alternative secure channel to the RF wireless network.

The advantages of using an optical receiver with a wider acceptance angle lie mostly in an aspect security implementations tend to lag on; that of human computer interaction. Using a simple LOS infrared link, would work just as well, but it would mean that users would have to probably queue for obtaining their secret key. Furthermore, depending on the position of the transmitter, which in turn defines the radius of the FOV, users can continue to move within the specified radius without affecting the handshake and data exchange between the transmitting and receiving end.

---

[1] Such a scenario is not far from today's standards: Most mobile phones come equipped with IR links and RF connectivity is a matter of purchasing the appropriate expansion device. As for the network, a number of wireless LAN products based on the 802.11x standard, are available and in already widely in use.

3. Security overview.

Having briefly defined the requirements and motivation behind a physical layer implementation involving both IR and RF, it is time to question the security objectives behind such a system. In all communications, whether wired or wireless, data security can be seen as the superset of three attributes, all of which must be maintained [7]:

- **Integrity**
  Broadly speaking, integrity is compromised when unauthorised users are capable of modifying data. *"Has somebody improperly changed the data?"*
- **Secrecy**
  Of all three terms, secrecy is perhaps the easiest to understand. We all have secrets and can easily understand the effect of a leak. *"Has the data been improperly disclosed?"*
- **Availability**
  Data is only as good as your ability to use it. Denial-of-Service[2] (DOS) attacks are the most common threat to availability. *"Can I read my data when I want to?"*

In an RF network, all three of the above attributes are compromised. Since any message is transmitted throughout a general area, users have the ability to jeopardise both the integrity (by claiming a different origin) and secrecy (by listening to all messages sent) of the system. Availability is still a major issue, but very little extra weight is added to it from the fact that our communications are taking place using RF. Furthermore, if we can insure the first two attributes to be maintained, it becomes much harder for a DOS attack to be launched against the network.

By introducing a secure IR channel and deploying a strong encryption algorithm, devices which have never previously existed on the network (ad-hoc networking represents a typical case), now have the ability to communicate securely over radio, provided a valid key exchange previously takes place. Thus the aspect of secrecy can be maintained.

Having the ability to exchange a key securely also indirectly implies the ability to distinguish different users and devices between them. For this, a number of methods and algorithms exist [9].

Moreover, since portable devices have limited memory and processing power, but also have rapid growth for both, standardising security requirements can be seen as a drawback especially when this is done in hardware. With the above described system, all security considerations fall under the application layer, thus allowing for adjustments within the specification, without any alterations in the physical and Media Access Control (MAC) layer.

Finally, in designing such a network architecture there are two pitfalls that should be avoided. Firstly, a system is only as secure as its weakest link. When deciding on the protocol structure on which the encryption algorithm is going to be based on, it must be made certain that new flaws do not emerge. Issues involving key length, key re-usage and key generation must be clearly defined so that not to leave any security flaws. This was the case with the Wired Equivalent Privacy (WEP) security standard for the IEEE 802.11 Wireless LAN specification [10]. Despite the fact that a secure algorithm was deployed, misinterpretation of some cryptographic primitives led to an insecure standard.

Secondly, more closely related to the physical layer, is the issue of reflected rays from the contact surface. When an infrared beam comes in contact with any surface, some of the radiation will be absorbed from it and some reflected towards the surrounding environment. The reflected index of any material specifies the amount of radiation capable of escaping from absorption and refraction. Thus, as a final requirement, for added security, materials with a low reflected index [11] should be placed in the final contact surface within the field of view of the optical antenna.

---

[2] A Distributed DOS attack can be seen as an attack where a number of compromised systems attack a single target, therefore causing a Denial Of Service for users on the targeted system. The flood of incoming packets to the targeted system causes it not to be able to handle legitimate users, resulting in data inaccessibility. A paper by Bennett Todd providing more details can be found in [8].

4. Conclusions.

Due to the nature of wireless radio communications, it is very difficult to maintain a secure network structure. Issues such as data integrity and user authentication contradict the dynamic characteristics of the network, thus providing connectivity to any user in a number of different locations. Furthermore, having the ability to exchange information between two parties in a secure fashion comes in direct contrast with the broadcast behaviour of RF.

For this purpose, deploying an infrared link at the physical entrance(s) to the location of the network enables the user to exchange a key using a secure line-of-sight channel, which they can in turn use for RF connectivity. By utilising the Warwick optical antenna, such a key exchange can take place in a wider field-of-view, allowing the user to freely move within the pre-specified range.

Provided that a well-designed secure protocol for RF is used and also that any reflections of the optical signal can be minimised through the use of absorbent material, such a system can guarantee the secure exchange of information between different devices on the network, as well as provide methods of authenticating users.

Such a scenario does not only have applicability in an office environment, but can also be extended to a number of other circumstances where network security plays a vital role. From smart homes, to wireless campuses, anyone wishing to secure their radio communications only has to go through the process of exchanging a key by means of a contained infrared channel.

References.

[1] J. R. Barry, *"Wireless Infrared Communications"*, Kluwer Academic Publishers, 1994, pp 6-7.

[2] J. M. Kahn & J. R. Barry, *"Wireless Infrared Communications"*, Proceedings of the IEEE, Vol. 85, No. 2, pp. 265-298, Feb. 1997.

[3] D. A. Kahn, *"Security Aspects of Infrared Wireless Links"*, Plaintree Systems Inc., http://www.plaintree.com/whitepaper3p.htm, 2000.

[4] R. Ramirez-Iniguez, *"Dielectric Totally Internally Reflecting Concentrators (DTIRCs) for Optical Wireless Receivers"*, PREP2002 Conference, 17-19 April 2002, Communications Track – 4.

[5] X. Ning, R. Winston & J. O'Gallagher, *"Dielectric totally internally reflecting concentrators"*, Applied Optics, Vol. 26, No. 2, Jan 1987, pp. 300-305.

[6] R. Ramirez-Iniguez & R. J. Green, *"Totally internally reflecting optical antennas for wireless IR communication"*, IEEE Wireless Design Conference, May 2002, pp. 129-132.

[7] M. Gast, *"802.11 Wireless Networks: The Definitive Guide"*, O'Reilly, 2002, pp 267-269.

[8] B. Todd, *"Distributed Denial of Service Attacks"*, OVEN Digital, http://www.opensourcefirewall.com/ddos_whitepaper_copy.html, 2000.

[9] B. Schneier, *"Applied Cryptography: Protocols, algorithms and source code in C"*, 2nd ed. – Chichester: Wiley, 1996, pp 65-68.

[10] N. Borisov, I.Goldberg, D. Wagner, *"Security of the WEP algorithm"*, University of Berkeley, Department of Computer Science, http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html, 2001.

[11] F. R. Gfeller, H. R. Muller & P. Vettiger, "Infrared communications for in-house applications", IEEE COMPCON'78, Washington DC, p. 134, Sep 1978.