Security in Bluetooth, RFID and Wireless Sensor Networks

Saroj Kumar Panigrahy, Sanjay Kumar Jena, and Ashok Kumar Turuk
Department of Computer Science and Engineering
National Instiute of Technology Rourkela
Rourkela, Odisha, India
{panigrahys,skjena,akturuk}@nitrkl.ac.in

ABSTRACT

Recently, new families of wireless ad hoc networks have emerged for specialized applications— personal area networks. Wireless personal area networks (WPAN) is rapidly gaining popularity. A wide variety of traditional computing devices and embedded Internet appliances are networked around us. However, due to the broadcast nature of these networks and the heterogeneity of devices on these networks, new security problems will arise, because the different types of devices have different capabilities and security requirements. In this paper, an overview of security issues like attacks and its countermeasures for wireless personal area networks such as Bluetooth, RFID and wireless sensor networks has been provided.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General—*Security and protection.*

General Terms

Theory.

Keywords

WPAN, Bluetooth, RFID, WSN.

1. INTRODUCTION

In the past few years, wireless keyboards, mice, headsets, broadband networking, and even hi-fi speakers have been used widely. New wireless technologies range from those that provide simple identifying information (such as radio frequency identification-RFID) to those that provide the wide-area broadband service Wi-Max, with Wi-Fi, Bluetooth, wireless USB (WUSB), wireless personal area network (WPAN), etc. [2].

A personal area network (PAN) is a computer network used for communication among computer devices, including telephones and personal digital assistants, in proximity to an individual's body. The reach of a PAN is typically a few meters. PANs can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet (an uplink). PANs may be wired with computer buses such as USB and FireWire or can also be made wireless with the use of network technologies such as IrDA, Bluetooth, UWB, Z-Wave and ZigBee.

WPAN is a network for interconnecting devices centered around an individual person's workspace, in which the connections are wireless. Typically, a WPAN uses some technologies that permits communication within a very short range, i.e., about 10 meters. One such technology is Bluetooth, which was used as the basis for a new standard, IEEE 802.15.

A WPAN could serve to interconnect all the ordinary computing and communicating devices that many people have on their desk or carry with them today, or it could serve a more specialized purpose such as allowing the surgeon and other team members to communicate during an operation. A key concept in WPAN technology is known as "plugging in". In the ideal scenario, when any two WPAN-equipped devices come into close proximity (within several meters of each other) or within a few kilometers of a central server, they can communicate as if connected by a cable. Another important feature is the ability of each device to lock out other devices selectively, preventing needless interference or unauthorized access to information.

The technology for WPANs is in its infancy and is undergoing rapid development. Proposed operating frequencies are around 2.4 GHz in digital modes. The objective is to facilitate seamless operation among home or business devices and systems. Every device in a WPAN will be able to plug in to any other device in the same WPAN, provided they are within physical range of one another. In addition, WPANs worldwide will be interconnected. Thus, for example, an archaeologist on site in Greece might use a PDA to directly access databases at the University of Minnesota in Minneapolis, and to transmit findings to that database.

A Bluetooth PAN is also called a "piconet", and is composed of up to 8 active devices in a master-slave relationship (a very large number of devices can be connected in "parked" mode). The first Bluetooth device in the piconet is the master, and all other devices are slaves that communicate with the master. A piconet typically has a range of 10 meters, although ranges of up to 100 meters can be reached under ideal circumstances.

ICCCS'11 February 12-14, 2011, Rourkela, Odisha, India

WPANs are intended to provide advanced capabilities such as cable replacement, interconnection of various electronic devices, monitoring of physical parameters on the human body, and the like, all within a person's workspace. Different application areas for WPANs have widely differing requirements in terms of data rate, power consumption, and quality of service, such networks are typically classified into the following three classes [22]:

- High data rate WPANs are needed for real-time and multimedia applications. Such applications are supported through the IEEE 802.15.3 standard (IEEE 2003a), with the maximum data rate of 55 Mbps (megabits per second).
- Medium data rate networks for cable replacement and consumer devices. This was the original use of WPANs, as envisioned in the IEEE 802.15.1 (Bluetooth) communications standard, with raw data rates of 1 Mbps up to 3 Mbps. The original Bluetooth specification (Bluetooth SIG 2003; IEEE 2002) allowed raw data rates of up to 1 Mbps, but recent improvements allow data rates of up to 3 Mbps (Bluetooth SIG 2004; IEEE 2005).
- Finally, low data rate WPANs are intended for use in wireless sensor networks and other similar application scenarios. A typical example of a LR-WPAN is the 802.15.4 standard (IEEE 2003b, 2006), which allows data rates of up to 250 kbps (kilobits per second).

1.1 Bluetooth Network

Bluetooth [1] is a standard for wireless communications based on a radio system designed for short-range cheap communication devices suitable to substitute for cables for printers, faxes, joysticks, mice, keyboards, and so on. The devices can also be used for communications between portable computers, act as bridges between other networks, or serve as nodes of ad hoc networks [9]. Bluetooth is a low-cost, low-power technology that provides a mechanism for creating small wireless networks on an ad hoc basis, known as piconets. A piconet is composed of two or more Bluetooth devices in close physical proximity that operate on the same channel using the same frequency hopping sequence. Bluetooth piconets are often established on a temporary and changing basis, which offers communication flexibility and scalability between mobile devices. Devices can be members in several piconets and in that case they are called as being part of a scatternet as shown in Figure 1. Not all Bluetooth devices have the same signal strength nor can cover the same distance. Most of the devices have a freedom in selecting their output power level. The Bluetooth specification sorts devices based on their power class which is summarized in Table 1. Some key benefits of Bluetooth technology are: cable replacement, ease of file sharing, wireless synchronization, and Internet connectivity [25].

Table 1: Bluetooth Classification

Class	Output Power	Distance Covered
Class 1	1 mW – 100 mW	up to 100 meters
Class 2	0.25 mW – 2.5 mW	up to 10 meters
Class 3	1 mW – 1mW	up to 1 meter

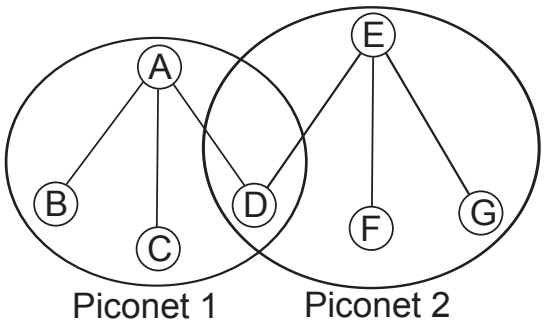

Figure 1: A scatternet consisting of two piconets

1.2 RFID Systems

In a broad context, radio transmissions containing some type of identifying information are considered RFID. RFID is about devices and technology that use radio signals to exchange identifying data [28], i.e., a small tag or label that identifies a specific object. The action receives a radio signal, interprets it, and then returns a number or other identifying information. Alternatively, it can be as complex as a series of cryptographically encoded challenges and responses, which are then interpreted through a database, sent to a global satellite communications system, and ultimately influence a backend payment system. Some of the current uses of RFID technology include: Point of Sale (POS), Automated Vehicle Identification (AVI) systems, restrict access to buildings or rooms within buildings, livestock identification, asset tracking, pet ownership identification, warehouse management and logistics, product tracking in a supply chain, product security, raw material tracking/parts movement within factories, library books check-in/check-out, railroad car tracking, luggage tracking at airports, and telemedicine [30].

1.3 Wireless Sensor Networks

A sensor network is an infrastructure comprises sensing (measuring), computing, and communication elements that gives an administrator the ability to instrument, observe, and react to events and phenomena in a specified environment [26]. Typical applications include, but are not limited to, data collection, monitoring, surveillance, and medical telemetry. There are four basic components in a sensor network: (a) an assembly of distributed or localized sensors; (b) an interconnecting network (usually, but not always, wireless-based); (c) a central point of information clustering; and (d) a set of computing resources at the central point (or beyond) to handle data correlation, event trending, status querying, and data mining. For researchers, Wireless Sensor Network (WSN) is becoming an exciting emerging domain of deeply networked systems of low-power wireless motes with a tiny amount of CPU and memory, and large federated networks for high-resolution sensing of the environment. The field is now advancing under the *push* of recent technological advances and the *pull* of a myriad of potential applications [26].

The rest of the report is organized as follows. The risks involved in Bluetooth, RFID and WSN are explained in Section 2. Section 3 states the objective of the work. Reported literature are summarized in Section **??**. Section 6 provides the concluding remarks.

2. RISKS IN BLUETOOTH, RFID & WSN

Risks are inherent to any wireless technology. And the most significant risk in the wireless technology is that the underlying communication medium is open to everybody, including authentic users as well as the intruders. Also, radio frequency-based products' move toward the consumer space has greatly reduced the equipments' price, and this, in turn, has caused a movement towards manufacture of new consumer- and enterprise-oriented products that use wireless technology [2]. This, however, creates the potential for security and privacy problems.

Bluetooth is emerging as a pervasive technology that can support wireless communication in various contexts in everyday life. For this reason, it's important to understand the potential risks linked with various wireless devices and communication protocols [3]. In its decade of public use, hackers and researchers have discovered several security risks to Bluetooth-enabled devices [8]. Bluetooth uses short-range radio which is very vulnerable. For instance, if the intruders had the frequency to connect to your PC, they can use their own Bluetooth technology monitor and mouse to get access. So they can have all information in your PC. And if the attackers' headsets connected to your mobile phone by hacking the frequency, you will never know somebody bugged your phone and everything will be unsafe. Therefore we need to put extra efforts in security section to make sure the technology is safe for the users.

RFID tags are used routinely these days. Examples include proximity cards, automated toll-payment transponders, and payment tokens. The ignition keys of many millions of automobiles, moreover, include RFID tags as a theft-deterrent [15]. In a world where everyday objects carried RFID tags, remarkable things would be possible. RFID security and privacy are also stimulating research topics because the simplest RFID tags—soon to be the most numerous [18].

WSNs are limited in their energy, computation, and communication capabilities. In contrast to traditional networks, sensor nodes are often deployed in accessible areas, presenting a risk of physical attacks. Sensor networks interact closely with their physical environment and with people, posing additional security problems. Because of these reasons current security mechanisms are inadequate for WSN. These new constraints pose new research challenges on key establishment, secrecy and authentication, privacy, robustness to denial-of-service attacks, secure routing, and node capture. To achieve a secure system, security must be integrated into every component, since components designed without security can become a point of attack [27]. They all have great things to offer consumers and businesses alike. All, however, have some security or privacy concerns because the designers didn't pay attention to these issues in the design or implementation stages (as current and past analyses show) or because of how the technology can be used.

3. BLUETOOTH SECURITY

Let us start with a brief review of the strengths and weaknesses of the security mechanisms defined in Bluetooth. In particular, we discuss how existing weaknesses can be exploited to attack communicating Bluetooth devices. Also various security and privacy issues are discussed. The weaknesses can be prone to various kinds of threats.

3.1 Threats

Classification of threats can assist in finding threat severity, precautions, and its countermeasures. A Bluetooth Threat Taxonomy (Aboott) provides a framework for satisfying all threats. Abott consists of nine distinct classes [8]. The threats can ne classified as shown in Table 2. Each attack appears in only one classification, based on its predominant characteristic, although a single attack can fall under several classifications.

Table 2: Bluetooth Threats

Classification	Threats
Surveillance	Blueprinting, bt_audit, redfang, Warnibbling, Bluefish, sdptool, Bluescanner, BTScanner
Range extension	BlueSniping, bluetooone, Vera-NG
Obfuscation	Bdaddr, hciconfig, Spooftooph
Fuzzer	BluePass, Bluetooth Stack Smasher, BlueSmack, Tanya, BlueStab
Sniffing	FTS4BT, Merlin, BlueSniff, HCIDump, Wireshark, kismet
Denial of service	Battery exhaustion, signal jamming, BlueSYN, Blueper, BlueJacking, vCardBlaster
Malware	BlueBag, Caribe, CommWarrior
Unauthorized direct data access	Bloover, BlueBug, BlueSnarf, BlueSnarf++, BTCrack, Car Whisperer, HeloMoto, btpincrack
Man in the middle	BT-SSP-Printer-MITM, BlueSpooof, bthidproxy

3.2 Attacks

These so-called Bluetooth cavities have generated a pleasing vocabulary of new words and phrases to name and describe them [20].

- ***Bluejacking***— temporarily hijacking another person's cellphone by sending it an anonymus text message using Bluetooth wireless networking system.
- ***Bluespamming***— sending unsolicited commercial messages.
- ***Warchalking***— using chalk to place a special symbol on a sidewalk or other surface that indicates a nearby wireless network, especially one that offers Internet access.
- ***Bluestumbling***— randomly searching for hackable Bluetooth devices.
- ***Bluesnarfing***— exploiting the object exchange (OBEX) protocol for pairing of two Bluetooth devices and copying e-mail messages, calendars, etc. by the crackers.
- ***Bluebugging***— reading data on a Bluetooth enabled cellphone, eavesdropping on conversations and even sending executable commands to the phone to initiate phone calls, sending text messages, connecting to the Internet, and more.
- ***Bluetracking***— tracking peopleŠs locations by following the signal of their Bluetooth devices.

- ***Bluesnipping***— scanning with a Bluetooth scanning device that looks like a sniper rifle with an antenna instead of a barrel.

- ***Man-in-the-Middle Attack***— is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker [11, 12, 13].

3.3 Security Services

The following are the three basic security services specified in the Bluetooth standard [25]:

- ***Confidentiality***— preventing information compromise caused by eavesdropping by ensuring that only authorized devices can access and view data.

- ***Authentication***— verifying the identity of communicating devices. User authentication is not provided natively by Bluetooth.

- ***Authorization***— allowing the control of resources by ensuring that a device is authorized to use a service before permitting it to do so.

4. RFID SECURITY & PRIVACY ISSUES

Despite of their myriad uses, RFID chips scare many people due to various tpes of attacks. Tags that optimize supply chains can also violate a personŠs privacy by tracking the tagged itemŠs owner. Muggers with RFID readers could scan crowds for high-value bank notes. Terrorists could scan digital passports to target specific nationalities. And police could abuse a convenient new method of cradle-to-grave surveillance. As futuristic as these threats sound, they have precedent. The draft recommendation on RFID privacy and security published by the European Commission in February 2008 states that RFID applications need to operate in a secure manner and that research needs to be carried out into high-performance and low-cost security solutions for RFID devices.

4.1 Attacks

As RFID is adopted for more applications, vandalism and other attacks against RFID will likely occur, stemming from temptation, dishonesty, civil disobedience, and a perverse sense of humor. But despite these differences, modern RFID security and privacy threats can still be grouped into familiar categories [24]. Understanding attack sequences is useful when deploying countermeasures because it helps us identify the types of attacks to which an RFID system is vulnerable. Also A taxonomy of system attacker behavior reveals security vulnerabilities in RFID authorization and monitoring systems [21]. The following are some of the attacks existing in literatures.

- ***Sniffing***— RFID tags are indiscriminate— they are designed to be readable by any compliant reader. Unfortunately, this lets unauthorized readers scan tagged items without the knowledge of the bearer, often from great distances [24].

- ***Tracking***— misuse of RFID technology for hidden monitoring of individuals' locations and actions [5].

- ***Spoofing***— Attackers can mimic authentic RFID tags by writing appropriately formatted data on blank RFID tags, also known as *Cloning* [19].

- ***Replay Attacks***— Relay devices can intercept and retransmit RFID queries, which offenders can use to abuse various RFID applications [17, 14, 10].

- ***Denial of Service***— RFID systems only work when RFID tags and back-end databases are available. Thieves can exploit this to steal RFID-tagged items by removing tags from the items completely or by putting them in a foillined booster bag (that is, a Faraday cage) that blocks RFID readersŠ query signals and temporarily deactivates the items [16].

4.2 Security and Privacy Solutions

Modern RFID poses special problems and constraints that will require academic and industry researchers to show the same ingenuity as their predecessors. RFID imposes physical limitations for on-tag security mechanisms. Fifteen microAmps of power and 5,000 gates are typical for a 0.35-micrometer complementary metal-oxide semiconductor process [24].

- ***Cryptography***— To cope with these limitations, researchers have devised ultra lightweight cryptographic and procedural solutions.

- ***Detection and evasion***— Consumers able to detect unauthorized RFID activity can also take their own evasive maneuvers. Other devices, such as the RFID Guardian (www.rfidguardian.org), will interpret RFID scans and log their meaning. Customers can also perform more active RFID evasion by RFID blocking in either a distributed or centralized fashion.

- ***Temporary Deactivation***— Consumers can sometimes deactivate their RFID tags to avoid most modern-day threats. One temporary tag-deactivation method is using a Faraday cage, such as the RFdeflecting metallic sleeves that will be issued with digital passports. Researchers have also created on-tag mechanisms for tag deactivation. EPCglobal tags come with a password-protected kill function that permanently deactivates tags, and some more expensive tags might offer a password-protected sleep/wake function, which temporarily deactivates and then reactivates RFID tags.

- ***Authentication***— Digital signatures are an important tool for data and device authentication. There are low cost digital signature architecture available [23].

- ***Other Techniques***— Numerous other techniques protect RFID devices from attacks. Periodically modifying RFID tag identifiersŠ appearance and data can prevent unauthorized tag access. RFID tagsŠ pseudonyms consist of names that are periodically refreshed, either by trusted RFID readers or an on-tag pseudorandom number generator. A mixnet of RFID readers can also periodically reencrypt tag data.

5. WSN SECURITY

Providing security in sensor networks is not an easy task. Compared to conventional desktop computers, severe constraints exist since sensor nodes have limited processing capability, storage, and energy, and wireless links have limited bandwidth. Despite the aforementioned challenges, security is important and even critical for many applications of sensor networks, such as military and homeland security applications [7]. Here are some of the literatures related with attacks, security challenges and goals.

5.1 Attacks

The small sensor nodes in a WSN are susceptible to many kinds of attacks. Various classification of these attacks are [29, 4, 7, 6]:

A. Based on the network environment:

- *External* or *Outside*— the attacker node is not an authorized participant of the sensor network. An outside attacker has no access to most cryptographic materials in sensor networks. These are further divided into two categories:
  - *Active*— disrupts network functionality by introducing some denial-of-service (DoS) attacks, such as jamming, power exhaustion.
  - *Passive*— involves unauthorized 'listening' to the routing packets.
- *Internal* or *Inside*— An inside attacker may have partial key materials and the trust of other sensor nodes (node compromising). Inside attacks are much harder to detect and defend against.

B. Based on different network layers:

- *Physical*— jamming, tampering.
- *Link (medium access control)*— collision, exhaustion.
- *Network*— manipulating routing information, selective forwarding attack, sybil attack, sinkhole (blackhole), wormhole, hello flood.
- *Transport*— Flooding.
- *Application*— Cloning.

C. Based on the capability of the attacker:

- *Sensor-level*— less harmful as smaller computational and limited battery power
- *Laptop-level*— more harmful as larger computational and more battery power

5.2 Security Challenges

Security challenges in sensor networks can be summarized as follows [6]:

- Minimizing resource consumption and maximizing security performance.
- Sensor network deployment renders more link attacks ranging from passive eavesdropping to active interfering.
- In-network processing involves intermediate nodes in end-to-end information transfer.
- Wireless communication characteristics render traditional wired-based security sche-mes unsuitable.
- Large scale and node mobility make the affair more complex.
- Node adding and failure make the network topology dynamic.

5.3 Security Goals

When dealing with security in WSNs, we mainly focus on the problem of achieving some of all of the following security contributes or services [6]:

- ***Confidentiality***: Confidentiality or secrecy has to do with making information inaccessible to unauthorized users.
- ***Availability***: Availability ensures the survivability of network services to authorized parties when needed despite denial-of-service attacks.
- ***Integrity***: Integrity measures ensure that the received data is not altered in transit by an adversary.
- ***Authentication***: Authentication enables a node to ensure the identity of the peer node with which it is communicating.
- ***Non-repudiation***: Non-repudiation denotes that a node cannot deny sending a message it has previously sent.
- ***Authorization***: Authorization ensures that only authorized nodes can be accessed to network services or resources.
- ***Freshness***: This could mean data freshness and key freshness. Since all sensor networks provide some forms of time varying measurements, we must ensure each message is fresh. Data freshness implies that each data is recent, and it ensures that no adversary replayed old messages.

6. CONCLUSION

Security is becoming a major concern for Bluetooth, RFID and WSN protocol designers because of the wide security-critical applications. The goals for Bluetooth security is to model new man-in-the middle attacks and its countermeasures using cryptographic primitives. Also to model other possible attacks and their counter security services, i.e., confidentiality, authentication and authorization. The draft recommendation on RFID privacy and security published by the European Commission in February 2008 states that RFID applications need to operate in a secure manner and that research needs to be carried out into high-performance and low-cost security solutions for RFID devices. So our objective to model various possible attack models and their countermeasures to improve the security issues. The ultimate security objective in WSN is to provide confidentiality, integrity, authenticity, and availability of all messages in the presence of resourceful adversaries. Key management is an essential cryptographic primitive upon which other security primitives are built. Most security requirements, such as privacy, authenticity, and integrity, can be addressed by building on a solid key management framework.

Acknowledgment

The authors are indebted to Information Security Education and Awareness (ISEA) Project, MCIT, Department of Information Technology, Govt. of India, for sponsoring this research and development activity.

7. REFERENCES

[1] I. S. 802.15.1. Information Technology Ů Telecommunications and Information Exchange between Systems Ů Local and Metropolitan Area Networks Ů Specific Requirements Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs), 2005.

[2] W. Arbaugh. Guest Editor's Introduction: Wired on Wireless. *IEEE Security & Privacy*, 2(3):26–27, May-Jun. 2004.

[3] L. Carettoni, C. Merloni, and S. Zanero. Studying Bluetooth Malware Propagation: The BlueBag Project. *IEEE Security & Privacy*, 5(2):17–25, Mar-Apr. 2007.

[4] H. Chan and A. Perrig. Security and Privacy in Sensor Networks. *IEEE Computer*, 36(10):103–105, Oct. 2003.

[5] J.-C. Chang and H.-L. Wu. A Hybrid RFID Protocol against Tracking Attacks. Cryptology ePrint Archive, 2009.

[6] X. Chen, K. Makki, K. Yen, and N. Pissinou. Sensor Network Security: A Survey. *IEEE Communications Surveys & Tutorials*, 11(2):52–73, Second Quarter 2009.

[7] X. Du and H.-H. Chen. Security in Wireless Sensor Networks. *IEEE Wireless Communications*, 15(4):60–66, Aug. 2008.

[8] J. Dunning. Taming the Blue Beast: A Survey of Bluetooth Based Threats. *IEEE Security & Privacy*, 8(2):20–27, Mar-Apr. 2010.

[9] E. Ferro and F. Potorti. Bluetooth and Wi-Fi Wireless Protocols: A Survey and A Comparison. *IEEE Wireless Communications*, 12(1):12–26, Feb. 2005.

[10] L. Francis, G. Hancke, K. Mayes, and K. Markantonakis. Practical NFC Peer-to-Peer Relay Attack using Mobile Phones. In *Workshop on RFID Security, RFIDSec'10*, Istanbul, Turkey, Jun. 2010.

[11] K. Haataja and K. Hypponen. Man-In-The-Middle attacks on Bluetooth: A Comparative Analysis, A Novel Attack, and Countermeasures. In *3rd International Symposium on Communications, Control and Signal Processing, ISCCSP'08*, pages 1096–1102, Mar. 2008.

[12] K. Haataja and P. Toivanen. Practical Man-in-the-Middle Attacks Against Bluetooth Secure Simple Pairing. In *4th International Conference on Wireless Communications, Networking and Mobile Computing, WiCOM'08*, pages 1–5, Oct. 2008.

[13] K. Haataja and P. Toivanen. Two Practical Man-in-the-Middle Attacks on Bluetooth Secure Simple Pairing and Countermeasures. *IEEE Transactions on Wireless Communications*, 9(1):384–392, Jan. 2010.

[14] G. Hancke. Practical Attacks on Proximity Identification Systems. In *IEEE Symposium on Security and Privacy*, Oakland, California, USA, May 2006.

[15] A. Juels. RFID Security and Privacy: A Research Survey. *IEEE Journal on Selected Areas in Communications*, 24(2):381–394, Feb. 2006.

[16] J. Kang and D. Nyang. RFID Authentication Protocol with Strong Resistance against Traceability and Denial of Service Attacks. In R. Molva, G. Tsudik, and D. Westhoff, editors, *European Workshop on Security and Privacy in Ad hoc and Sensor Networks, ESAS'05, Lecture Notes in Computer Science, Springer Berlin/Heidelberg*, volume 3813, pages 164–175, Visegrad, Hungary, Jul. 2005.

[17] Z. Kfir and A. Wool. Picking Virtual Pockets Using Relay Attacks on Contactless Smartcard Systems. In *In IEEE Conference on Security and Privacy for Emerging Areas in Communication Networks, SecureComm'05*, pages 47–58, Athens, Greece, Sep. 2005.

[18] T. Kohno. An Interview with RFID Security Expert Ari Juels. *IEEE Pervasive Computing*, 7(1):10–11, Jan-Mar. 2008.

[19] M. Lehtonen, F. Michahelles, and E. Fleisch. How to Detect Cloned Tags in a Reliable Way from Incomplete RFID Traces. In *IEEE International Conference on RFID, RFID'09*, pages 257–264, Orlando, Florida, USA, Apr. 2009.

[20] P. McFedries. Bluetooth Cavities. *IEEE Spectrum*, 42(6):88, Jun. 2005.

[21] L. Mirowski, J. Hartnett, and R. Williams. An RFID Attacker Behavior Taxonomy. *IEEE Pervasive Computing*, 8(4):79–84, Oct-Dec. 2009.

[22] J. Misic and V. B. Misic. *Wireless Personal Area Networks: Performance, Interconnections And Security With IEEE 802.15.4*. John Wiley & Sons, Mar. 2008.

[23] M. O'Neill and M. Robshaw. Low-Cost Digital Signature Architecture Suitable for Radio Frequency Identification Tags. *IET Computers Digital Techniques*, 4(1):14–26, Jan. 2010.

[24] M. Rieback, B. Crispo, and A. Tanenbaum. The Evolution of RFID Eecurity. *IEEE Pervasive Computing*, 5(1):62–69, Jan-Mar. 2006.

[25] K. Scarfone and J. Padgette. Guide to Bluetooth Security. NIST Special Publication 800-121, Sep 2005.

[26] K. Sohraby, D. Minoli, and T. Znati. *Wireless Sensor Networks: Technology, Protocols, and Applications*. Wiley-Interscience, Apr. 2007.

[27] J. A. Stankovic. Research Challenges for Wireless Sensor Networks. *ACM SIGBED Review*, 1(2):9–12, Jul. 2004.

[28] F. Thornton, B. Haines, A. M. Das, H. Bhargava, A. Campbell, and J. Kleinschmidt. *RFID Security*. Syngress Publishing Inc., 2006.

[29] A. Wood and J. Stankovic. Denial of Service in Sensor Networks. *IEEE Computer*, 35(10):54–62, Oct. 2002.

[30] Y. Xiao, X. Shen, B. Sun, and L. Cai. Security and Privacy in RFID and Applications in Telemedicine. *IEEE Communications Magazine*, 44(4):64–72, Apr. 2006.