Paper

New Threats and Innovative Protection Methods in Wireless Transmission Systems

Tomasz Bilski

Institute of Control and Information Engineering, Poznan University of Technology, Poznan, Poland

Abstract—Many improvements in the field of wireless communication can be observed nowadays. Some developments are gradual, others are revolutionary. It is obvious that each innovation in the area may lead to new security threats and vulnerabilities. Such technologies and transmission methods as: Near Field Communication (NFC), Visible Light Communication (VLC), handover, mesh networks, 5G cellular network, mobile IPv6, beamforming, cooperative beamforming, Multiple Input Multiple Output (MIMO), Orthogonal Frequency Division Multiple Access (OFDMA), transmission in Extra High Frequency (EHF) band are very important from the security point of view. In order to preserve high level of security one needs to identify, analyse and classify distinctive sets of threats and vulnerabilities as well as some emerging data protection opportunities related to innovative wireless transmission methods and technologies. This identification, analysis and classification is a main purpose of the paper. It will focus on cryptography in wireless systems, security vs. energy tradeoffs, physical layer security. For example, common problems related to cryptography may be solved with a use of physical layer security. Data confidentiality may be fulfilled with a use of beamforming and jamming, authentication may be performed with a use of out-of-band authentication model.

Keywords—authentication, confidentiality, cryptography, threats, vulnerabilities, wireless transmission.

1. Introduction

1.1. Advances in Wireless Transmission

Wireless, mobile communication systems are commonly used. Number of applications as well as number of technologies are growing. An evolutionary improvements may be observed in such exemplary communication systems as: cell networks, wireless Local Area Networks (LANs), wireless Metropolitan Area Networks (MANs). Some new (often revolutionary) forms/modes of transmission crop up from time to time. The technology progress is a result of greater demand for rich media services and rapid growth of subscriber base.

From the user point of view transmission system should be effective, reliable and secure. Unfortunately, the main drawback of wireless transmission is fundamental lack of data security. There are many intentional as well as non-intentional threats and many vulnerabilities that should be evaluated in wireless environment. Numerous security problems should be solved today, nevertheless pioneering wireless technologies materialize together with new threats and vulnerabilities.

The advances in wireless transmission may be described with a use of three factors:

- universal trends in development,
- constant, evolutionary enhancements in well-established and commonly used systems,
- new forms, modes, techniques (some of them are revolutionary) of transmission.

1.2. Universal Trends

There are some trends observable in the development of different transmission systems. Obviously, the systems progress in time: transmission parameters (throughput, delay, bit error rate, jitter) are improving. Better, wireless communication channel parameters are achieved with advances in many areas, such as:

- silicon technology,
- keying (modulation) techniques,
- spread spectrum techniques,
- signal processing,
- radio bandwidth expansion,
- adaptive arrays and other types of smart antenna,
- multiple access techniques,
- network topology.

Spectral efficiency is growing. Nevertheless it is slowly reaching theoretical limits. Furthermore, hardware (user devices as well as infrastructure equipment) costs are constantly decreasing – this is a result of pushing down the cost of components and leaving the manufacturing to Asian companies, which are good at making products at high volumes and low costs.

1.3. Network Convergence

Next important trend is convergence – different networks and services are merging into single network. Wireless networks management systems are more often based on cloud computing. User mobility becomes a service which is supported by upper layers of protocol stacks (e.g. mobility features in IPv6). It must be noted that all given above progress trends have significant impact on data security.
For example, decreasing cost of hardware is a double-edged sword. Users get cheaper devices. At the same time cost of attacks also decreases and new attack methods materialize. Nowadays, frequently used (and cheap) method of Internet attack (called phishing) is based on false servers connected to Internet and used to attract Web users in order to get their passwords to bank accounts and other confidential data. Decreasing cost of telecommunication infrastructure means that it becomes relatively easy to build and attract users not only to false computer imitating bank server but also to false communication infrastructure, e.g. false LTE femtocells. The fake femtocells delivered by impostor may be used for eavesdropping, denial of service as well as for spoofing purposes.
Another set of security issues is related to convergence. For example, incorporating IP protocol in LTE systems means introducing all security threats and vulnerabilities of Internet to cell phone networks. In the past, voice-dominated, phone networks have been built on proprietary interfaces and protocols (e.g. SS7 signalling protocol) also cell phone networks have been relatively difficult to penetrate, malicious attacks were infrequent in comparison to Internet. Radio Access Network (RAN) and backhaul had complex deployment configurations, specific to operator, location and equipment vendor. Attacks on them required sophisticated preparation and on-site access.
Today, cell phone networks are primarily data networks based on IP with more open architecture and protocols (e.g. diameter open signalling protocol). As a consequence new threats emerge. An example is signalling flood problem, which may be caused either by malicious activity directed at the cell phone network, or accidentally as an indirect effect of upgrades[1].
In such converged network single, modern attack on a mobile device may have impact on [1]:

– cell phone subscriber (owner of the device),

– corporate subscriber network,

– mobile core network,

– Internet.

Today, we are living in transitional phase of Internet. Two versions of Internet Protocol are used side by side: IPv4 and IPv6. IPv4 is old, unprotected, inefficient protocol with some additional drawbacks as limited address space and Network Address Translation (NAT) obstacles. IPv6 is newer, integrated with security tools, more efficient protocol, without address complications, with mobility enhancements. Nevertheless, it must be added that IPv6 is not a matured technology. There are many issues related to IPv6 availability, performance and security. Furthermore, there are some problems related to coexistence of the protocols and to transformation from IPv4 to IPv6 period [2], [3].

1.4. New Transmission Forms, Modes, Techniques

In the last years many innovative technologies utilized in wireless systems are appeared. First of all new and diverse bands of electromagnetic waves are incorporated into transmission, e.g.: NFC (13.5 MHz), EHF (30–300 GHz), VLC (428–750 THz).
Electromagnetic waves are main but not only communication medium. Transmission systems based on acoustic energy are also developed[2].
Another area of progress is related to space radio coverage. A lot of research and implementation work is done in such issues as:

– mesh networking,

– cooperative relaying,

– beamforming and cooperative beamforming,

– IP mobility,

– handover processes.

1.5. Inherent Lack of Security in Wireless Networks

Computer system security is frequently defined (e.g. in ISO standards) with a use of three general factors: confidentiality, integrity and availability (called sometimes CIA). These requirements incorporate such elementary security controls as: authentication, authorization, accounting, replay protection, Man in the Middle (MiTM) protection, non-repudiation. The requirements are independent of technology. They should be fulfilled in wired as well as in wireless transmission systems. Nevertheless, wireless networks distinctive features make it is much harder to satisfy the CIA requirements.
First of all, data confidentiality may be threaten by eavesdropping. In ordinary radio communication system eavesdropping is much easier since wireless communications systems have usually broadcast nature – radio signal is available for everyone in the range of the transmitter. Data integrity is a function of transmission correctness. Transmission systems based on wireless medium have much

[1] In January 2012, NTT DoCoMo in Japan experienced a signalling flood that disrupted network access, caused by a VoIP OTT application running on Android phones [http://www.reuters.com/article/2012/01/27/us-docomo-idUSTRE80Q1YU20120127].

[2] For example, Microsoft is working on Dhwani Project, which uses acoustic waves for short range communication (http://research.microsoft.com/apps/pubs/default.aspx?id=192134).

higher (up to 10^7 times greater) nominal bit error rates than transmission systems based on copper wire or optical fibre (Table 1).

Table 1
Bit Error Rates

Technology	BER (absolute)	BER (relative)
Wire		
Gigabit Ethernet	10^{-12}	1
Fibre Channel		
Wireless		
Satellite (GEO)	10^{-8}	10^4
Satellite (LEO)	10^{-6}	10^6
Point-to-point	10^{-5}	10^7
IEEE 802.11	10^{-6}	10^6
IrDA	10^{-8}	10^4

An attack on availability of communication services is called Denial of Service (DoS). There are many methods used to perform DoS or distributed DoS in computer networks. Exemplary attacks use some features of communication protocols from higher layers of TCP/IP stack, such as: Address Resolution Protocol (ARP), Transmission Control Protocol (TCP) or Domain Name Services (DNS). Such attacks may be executed in all networks without regard to transmission medium. In addition to mentioned above attacks based on higher layers, DoS in wireless network may be performed at physical layer by jamming radio channel [4].
Intentionally generating jamming signal is relatively simple and inexpensive. Furthermore, jamming may also result from non-intentional reasons. Radio bandwidth (especially unlicensed part of it) is limited resource. Growing number of systems using the same unlicensed radio band (especially 2.4–2.5 GHz) leads to increasing interference risk. Unlicensed ISM (Industry Science Medicine) band is utilized by such systems and applications as:

– IEEE 802.11 (Wi-Fi),

– IEEE 802.15.1 (HR WPAN),

– IEEE 802.15.3 (Bluetooth),

– IEEE 802.15.4. (ZigBee),

– HomeRF,

– RFID,

– microwave ovens.

A lot of work is done in search of new, higher and uncrowded EHF (30–300 GHz) frequency bands (e.g. IEEE 802.11ad already uses 60 GHz). But, it must be noted that wave propagation at these frequencies is related to entirely different set of difficulties, e.g. increased free space path loss. Channel models developed for systems using the 1–3 GHz microwave bands are inadequate to characterize wireless systems with 10 or even 100 times greater carrier frequencies. Interference problem is additionally difficult to solve since signal bandwidth of a single channel is also much wider than before (see Tables 2 and 3).

Table 2
Signal bandwidth growth in WLAN with IEEE 802.11

IEEE 802.11 version	Single channel bandwidth
802.11a	20 MHz
802.11b	22 MHz
802.11n	40 MHz
802.11ac	80 MHz
802.11ac (option)	160 MHz
802.11ad	2 GHz

Table 3
Signal bandwidth growth in cellular phone systems

Cell phone system	Single channel bandwidth
Tetra, NMT	25 kHz
GSM	200 kHz
UMTS	5 MHz
LTE	20 MHz
LTE advanced	100 MHz

1.6. Common Security Controls

Some security tools and methods for wireless networks are used for years. The main of them are:

– hidden channels in Frequency Hopping Spread Spectrum (FHSS),

– communication range control methods as sector antenna, transmit power restrictions, different forms of Faraday cages, e.g. shielding paints,

– Medium Access Control (MAC) address filtering,

– data encryption,

– Wireless Intrusion Prevention System (WIPS) and Network Admission Control (NAC).

2. Cryptography in Wireless Networks

Data encryption is very powerful and widely utilized protection against eavesdropping. There are many encryption techniques and protocols used in higher layers of TCP/IP stack: IPSec, Secure Socket Layer/Transport Layer Security (SSL/TLS), Secure Multipurpose Internet Mail Extensions

(SMIME), Pretty Good Privacy (PGP) and so on. Nevertheless, the emergence of large-scale, dynamic and decentralized wireless networks imposes many new challenges on classical cryptography.
In wireless environment there are some inherent impediments related to cryptography applications. Data encryption/decryption is restricted in mobile devices with low processor performance and energy limitations. Furthermore, key management is complex and delicate matter especially in heterogeneous environment with many different protocols and networks, i.e. IEEE 802.11, IEEE 802.16, UMTS, LTE. Cryptography has a negative impact on network throughput. Some protocols devised for wireless networks, e.g., Wired Equivalent Privacy (WEP) proved to be very vulnerable to cryptanalysis.
An example, of decentralized wireless network is a mesh. Some specific challenges related to security are visible here [9]:

– secure multi-hop routing,

– detection of corrupted nodes,

– denial of service attacks,

– fairness factor of the distribution of network resources.

From the cryptography point of view, an important impediment is links heterogeneity and devices organized into a mesh. The protection of the communication between non-neighboring nodes is more complex. It requires the use of integrity and/or encryption on a higher protocol layer than the MAC. Furthermore, different wireless technologies such as IEEE 802.11, IEEE 802.16 used in a mesh may support different algorithms with different cryptography strength [10].
Even when message confidentiality is provided by standards with higher level of security like WPA (Wi-Fi Protected Access) or WPA2, usually only the frame payload is protected and MAC address in the header of the frame is transmitted in unencrypted form. So, traffic analysis by frame sniffing may be used to monitor and track users in the network.

Table 4
Exemplary sizes of data fields in IP packets

Application	Data field size [bytes]
Internet games	40–110
VoIP with LP codec (e.g. G.728)	50–80
Ping	56
World of Worldcraft	74
Skype	84
VoIP with PCM codec (e.g. G.711)	180–260
BitTorrent	377
eMule	1180

Furthermore, complex traffic analysis based on entire frame size may give some hints on application that is used by a given user. The frame size is related to data field, which contains IP packet – different network applications send packets with different number of bytes in data fields (Table 4) [5]–[8]. It has been demonstrated that traffic analysis based on IP packet sizes may be used to infer some information, e.g., the source of a Web page retrieved by a given user or applications run by the user [11].

3. Physical Layer Security

As an alternative to data encryption in higher TCP/IP layers the physical layer characteristics of the wireless channel such as fading or noise may be used to protect confidentiality. Beyond securing wireless transmissions of confidential information, physical layer security solutions have been also exploited to provide or enhance the authentication and privacy of legitimate wireless users [12]. There is a lot of research work in the area of physical layer security. The main research topics are:

– code design for physical layer security,

– advanced signal processing and space-time secure transmission techniques, e.g. secure OFDMA subcarrier allocation [13],

– secure relaying and cooperative transmission techniques,

– advanced physical layer security attacks, e.g., smart eavesdropping or jamming, and their countermeasures,

– physical layer authentication.

It must be noted that the use of physical layer for data protection originates from Shannon's notion of communication channel information capacity and perfect secrecy.

4. Energy vs. Security

4.1. Energy Gap

Energy available in mobile devices is a limited resource. Device performance and its internal complexity are rising. Smartphones, tablets and other mobile devices are equipped with more and more functions demanding energy. On the other hand capacity of batteries produced for the devices is growing but the improvements are very slow. As a result power gap between energy consumption and battery lifetime is not decreasing.
The energy gap between energy demands and availability is widening. The gap has negative impact on data security. First of all the security tools such as encryption/decryption, key management, firewall, antivirus working in mobile devices utilize a lot of energy. Switching on the security tools

may double the energy used by a given device. Authentication, Authorization, Accounting (AAA) processes consume energy, especially in device that changes location and has to make frequent disassociations and associations with many access points (APs) or base stations (BS) [14]. Secondly, device energy may be a resource that is intentionally attacked.
Here we have some examples of an old dilemma – functionality vs. security. Higher security level equals to shorter battery lifetime.

4.2. Energy Usage by Security Tools

It has been proved that there is no big difference between wireless protocols in terms of energy consumption per crypto operation. The energy consumption related to cryptography is dependent mainly on key length (independently on the selected algorithm) [15]. Longer battery lifetime (more functionality) means short cryptographic key, short cryptographic key means low level of security.
Additional problem is related to user behavior. In order to increase battery life of the device one has to switch off some or all security tools – for a second time, functionality increases while security decreases.

4.3. Intentional Threats Related to Energy

From energy point of view two forms of intentional threats and malware may be distinguished:

- common malware utilizing available energy as side effect,
- dedicated malware for mobile device energy resources in order to exhaust it.

Each common form of attack and malware (e.g. simple port scanning or ping flooding) utilizes energy of the device that has been attacked. The device is forced by an attacker to perform additional tasks like executing code inserted by intruder or sending data to some unexpected by an owner of device destinations. If an attack is persistent for a long time the energy of the device is slowly vanishing. The experiments [14] demonstrated that port scanning attacks or ping flooding attacks may double the power consumption of an exemplary Android based smartphone.
One of the critical categories of attacks is DoS. As a result of such attack user is unable to use his device, resources or services. There are many methods for DoS attacks – they are routinely performed in Internet. The attacks utilize and drain some resources of attacked system, e.g., memory for communication buffers, processing power, throughput. In the case of wireless, mobile device DoS attack may be completed by quickly exhausting the energy of a device. This may be done by:

- creating unsolicited network traffic,
- forcing erratic and CPU consuming behavior,
- utilizing power consuming services, especially GPS or Bluetooth communication [1].

4.4. New Protection Tools and Methods

Common methods for malware detection and for intrusion detection systems are: signature based scanning and heuristic scanning. In the wireless and mobile environment a new technique for malware and attack detection is possible. Anti malware system may use detailed data on current energy usage in the device to detect malware or attack. Normal energy usage profile may be identified, stored and compared with recent usage. Deviations from this typical profile may indicate an infection or an attack.
Another important research area is related to energy savings. In order to save the device energy consumed by security tools some changes are necessary. The following solutions are considered:

- security controls offloading,
- some modifications to existing malware detection methods, e.g. based on virtual machines,
- security tools with decreased energy usage.

4.5. Offloaded Security

In order to preserve mobile device energy some tasks of the device may be moved from the device to another component of IT system. The security tasks may be offloaded to server or cloud [16]. The scenario of malware or attack detection process may look as follows:

- operation (function call, signal) is logged in user mobile device,
- system log is transmitted from the device to server,
- server performs the same operation in simulated user terminal environment and checks security points,
- result of the checking is transmitted from the server to the device.

Offloading security controls has some drawbacks. Energy for data processing (related to security check) in the device is saved but at the same time extra energy is utilized for device-server and server-device transmissions. Furthermore, malware detection in server has to be done with a use of signature-based method, which is vulnerable to some sophisticated malware attacks using stealth techniques, polymorphism or encrypted code. In order to detect such attacks signature-based method should be supported by heuristic detection implemented directly in the device and obviously draining some energy of the device.

4.6. Energy Limited Security Tools

Another important research area is designing security tools with decreased energy usage. This may be done by decreased number of control points for malware detection, or decreased frequency of control checks.
It must be noted that some research teams are working on more general solutions to energy problem. For example, researchers from Worcester Polytechnic Institute are working on analytic 3-dimensional model of relations between data security and energy consumption. The model takes into account a given attack countermeasure and the level of security-reliability it can provide and relationship between the energy spent in carrying out a countermeasure and the energy level that is potentially lost if a given attack is successful [15].

5. Handover vs. Security

Handover is a process for switching wireless network while mobile device is moving from the range of one access point (or base station) to the range of another access point (or base station). Signaling processes may be executed in many layers. MAC signaling is performed with such protocols as IEEE 802.11i or IEEE 802.11r. IP signaling utilizes mobile IPv6 options.
Handover processes may be performed while the device is moving between two access points utilizing the same protocol and the same radio band or while the device is changing access network e.g. from IEEE 802.11 to UMTS. The processes are supported by IEEE 802.21 Media-Independent Handover Services.
Handover processes perform some functions related to security, like: authentication, key management. For real-time services handover delays should be kept minimal (at the level of several tens of milliseconds). Unfortunately, delays are usually much greater, in some cases up to several seconds.
Solutions to handover delay problems are based on predictions of awaiting handover and performing some processes related to handover in earlier times. Furthermore, time may be saved by eliminating unnecessary IP handovers (e.g., when user is roaming among base stations connected to the same access router) and by combining the mechanisms in the MAC layer with that of the IP layer [17].
An example is Handover Keying (HOKEY) proposed by Internet Engineering Task Force (IETF) Working Group [18]. It is based on modified Extensible Authentication Protocol (EAP), with decreased number of messages sent between parties. Keys from previous sessions are used in order to re-authenticate device with next access point. The process is initiated, while the device is still in the range of former access point antenna.
Modified Kerberos authentication for handover is proposed by Ohba *et al*. [19] for secure key distribution. Mobile node obtains master session keys without communicating with a set of authenticators before handover. Signalling related to key distribution is based on re-keying. The process is separated from EAP re-authentication and AAA signalling similar to initial network access authentication.

6. Secrecy Capacity

6.1. Quantitative Security Measure

Security (confidentiality) level of wireless network may be measured not only qualitatively but also quantitatively. Secrecy capacity is a measure for confidentiality level based on communication channel information capacity. Channel information capacity defined as the tightest upper bound on the rate of information that can be reliably transmitted over a given communication channel.
Secrecy capacity is defined as difference between the channel capacity of the link between sender and legitimate receiver and the channel capacity of the link between the same sender and eavesdropper. Value of the parameter is related to Signal to Noise Ratio (SNR) difference between the legitimate receiver and eavesdropper. It must be noted that some theoretical foundations of wireless security were presented many years ago, e.g. [20].
So, in order to increase confidentiality level this SNR level of the communication link between the sender and eavesdropper should be decreased. In systems with MIMO and antenna arrays this may be accomplished by:

- beamforming,
- transmit antenna selection [21],
- sending the jamming signal in the direction of the eavesdropper.

6.2. Beamforming Solutions

Common beamforming may be used to improve secrecy capacity. SNR difference between the legitimate receiver and the illegitimate receiver may be increased in order to minimize eavesdropping risk. Beamforming for security may be used in some different modes with assumption that the location of the eavesdropper is known, or without such assumption, e.g. [22]–[24].
Common beamforming system uses antenna array integrated with a single node. Cooperative beamforming [25] is a transmission mode in which in randomly distributed nodes antenna array is created with antennas from many nodes. The main purpose of such a system is data transmission on long distances in energy-efficient way.
Cooperative beamforming may be used to increase secrecy capacity. The protection is based on a subset of intermediate nodes which adopt distributed beamforming for sending information to legitimate receiver. At the same time other nodes send jamming signal to eavesdropper. Both tasks are accomplished with preserving individual power constraints of the nodes [26].

6.3. An Intelligent Jamming

Intelligent jamming is a security strategy aimed at the potential eavesdroppers locations. If the locations of eavesdropper and legitimate receiver are different then jamming signal may be directed. Jamming signal is sent (by sector antenna or by antenna array with beamforming) in the direction of the area of eavesdropper. At the same time legitimate receiver is not receiving this jamming signal. The method can effectively raise the noise floor at eavesdropper position, which makes for him difficult to distinguish between wireless signals and normal background noise on the wireless medium.

7. Out-of-Band Authentication

Standard electromagnetic waves communication channel may not be considered as trusted or authentic. Electromagnetic waves may be send from long distances, from different places which may be hidden. In general, user receiving such signals is not able to determine their source and may not be assured that a given signal is transmitted by certain sender. So, reliable procedure for sender authentication becomes a challenge. Unsecured authentication may lead to eavesdropping or spoofing.

The authentication problem (also cryptographic key for symmetric algorithms exchange problem) is usually solved with a use of asymmetric cryptography, e.g. Public Key Infrastructure and certificates. Nevertheless, there are some problems related to cryptography, e.g. the complexity of key management problem, especially in wireless and heterogeneous environment. So, another authentication method becomes crucial.

Out-of-band authentication is an authentication mode that uses additional communication channel/method for authentication processes. It is assumed that the system utilizes common unsecured radio channel (with high bitrate) for normal data transmission and the second out-of-band channel with relatively low bitrate, e.g. acoustic channel or visual channel like IEEE 802.15.7), for authentication purposes only.

The second channel should be authentic: receiver is guaranteed that a message he receives actually was send by a given sender. It is important that human (not the electronic device) is able to verify the authenticity of the sender device. The requirement may be satisfied in some different ways:

- electric contact,
- NFC,
- relative location check with a use of ultrasound impulses for measurement,
- visual markers photographed with camera smartphones, e.g. Seeing is Believing (SiB) method,
- common motion of two devices and accelerometer data analysis,
- acoustic, e.g. Loud&Clear (L&C) method.

Experiments with the given above methods are carried on. An exemplary protocol for creating an out-of-band channel for authentication with visible laser light has been proposed in [27]. The authors assume the laser transmission is not confidential. An attacker is able to either violate the confidentiality of data transmitted by VLC or to violate its authenticity. Proposed protocol, based on off the shelf components (so relatively cheap), establishes a secret, authenticated shared key between the personal trusted device and a remote device.

VLC channel is used also in the method proposed by Mayrhofer *et al*. [27]. The devices are equipped with visible barcodes that encode hashes or public keys. The data from the barcode of the first device are read by taking photo by the second device. User is aware what is photographed by the first device. The same data are transmitted by radio channel. Two sets of data received with a use of two different channels are compared in order to authenticate the second device.

Acoustic channel may be used in a similar way. Authentication data are played by one device and heard by the other device.

8. Conclusion

The author have presented several issues related to latest innovations in wireless communications systems. Each innovation is related to new threats and new vulnerabilities. At the same time the innovations may be used as new opportunities for data protection.

There are many protection methods and tools used widely in wired networks. Many of them are used also in wireless environment. Nevertheless, one has to be careful transferring security controls between different networks with different devices (including mobile ones). The features like limited energy, limited processing power and mobile device memory of wireless networks and mobile devices are unlike wired networks and immobile devices. So, security controls should be cautiously chosen and adjusted according to the features of this different environment.

An important and open, scientific research area is related to physical layer security in wireless networks. Upper layers security controls that are hard to use in mobile environment (e.g. cryptography) may be replaced by or used together with physical layer controls, for example: beamforming, dedicated subcarrier allocation in OFDMA, transmit antenna selection, jamming the eavesdropper, authentication with a use of out-of-band communication channel (e.g. VLC, NFC, SiB, L&C).

A lot of work is to be done in the area related to energy-security trade-offs. Such issues as models and standards for these relations, power management methods, off-loading security mechanisms from mobile devices are the exemplary

topics. Research on new security tools and methods with reduced power consumption is necessary.

References

[1] J. E. Bicford, "Rootkits on smart phones: Attacks, implications and energy-aware defense techniques", Graduate School – New Brunswick Rutgers, The State University of New Jersey, 2012.

[2] T. Bilski, "From IPv4 to IPv6 – Data Security in the Transition Phase", in *Proc. 7th Int. Conf. Netw. Serv. ICNS 2011*, Venice/Mestre, Italy, 2011, pp. 66–72.

[3] T. Bilski, "Network performance issues in IP transition phase", in *Proc. 6th Int. Conf. Netw. Comput. Adv. Inform. Manag. NCM 2010*, Seoul, Korea, 2010, pp. 39–44, 2010.

[4] K. Bauer, D. McCoy, B. Greenstein, D. Grunwald, and D. Sicker, "Physical layer attacks on unlinkability in wireless LANs", in *Privacy Enhancing Technologies*, I. Goldberg and M. Atallah, Eds. LNCS, vol. 5672. Berlin Heidelberg: Springer, 2009, pp. 108–127.

[5] T. Bilski, "Traffic analysis based on IP packet size", *Studia Informatica*, vol. 32, no. 3A(98), Silesian University of Technology Press, Gliwice, Poland, pp. 167–176, 2011.

[6] S. Joyce, "Traffic on the Internet – Report", 2000 [Online]. Available: http://wand.cs.waikato.ac.nz/old/wand/publications/sarah-420.pdf

[7] J. Postel, "Internet Control Message Protocol", IETF, RFC 792, 1981.

[8] L. Ying-Dar *et al.*, "Application classification using packet size distribution and port association", *J. Netw. and Comp. Appl.*, vol. 32, no. 5, pp. 1023–1030, 2009.

[9] B. Salem and J. P. Hubaux, "Securing wireless mesh networks", *Wirel. Commun.*, vol. 13, no. 2, pp. 50–55, 2006.

[10] A. Egners and U. Meyer, "Wireless mesh network security: State of affairs", in *Proc. 5th IEEE Conf. Local Comp. Netw. LCN 2010*, Denver, USA, 2010.

[11] M. Liberatore and B. N. Levine, "Inferring the source of encrypted HTTP connections", in *Proc. 13th ACM Conf. Comp. Commun. Secur. CCS 2006*, New York, USA, 2006.

[12] *Physical Layer Security in Wireless Communications*. X. Zhou, L. Song, Y. Zhang, Eds. Boca Raton: CRC Press, 2014.

[13] X. Wang, M. Tao, J. Mo, and Y. Xu, "Physical-layer security in OFDMA-based broadband wireless networks", in *Proc. IEEE Int. Conf. Commun. ICC 2011*, Kioto, Japan, 2011, pp. 1–5.

[14] L. Caviglione and A. Merlo, "The energy impact of security mechanisms in modern mobile devices", *Netw. Secur.*, Feb. 2012 [Online]. Available: http://www.ai-lab.it/merlo/publications/NS-2012.pdf

[15] F. C. Colon Osorio, E. Agu, and K. McKay, "Tradeoffs between energy and security in wireless networks", Worcester Polytechnic Institute, 2005 [Online]. Available: http://digitalcommons.wpi.edu/computerscience-pubs/67

[16] G. Portokalidisi, P. Homburg, K. Anagnostakis, and H. Bos, "Paranoid Android: Versatile protection for smartphones", in *Proc. 26th Ann. Comp. Secur. Appl. Conf.*, Austin, TX, USA, 2010, pp. 347–356.

[17] C. Chung-Kuo and H. Chin-Tser, "Fast and secure mobility for IEEE 802.16e broadband wireless networks", in *Proc. Int. Conf. Parallel Process.Workshops ICPPW 2007*, Xi-An, China, 2007.

[18] Q. Wu, T. Taylor, Y. Nir, K. Hoeper, and S. Decugis, "Handover Keying (HOKEY) Architecture Design", IETF, RFC 6697, 2012.

[19] Y. Ohba, S. Das, and D. Ashutosh, "Kerberized handover keying: A media-independent handover key management architecture", in *Proc. 2nd ACM Int. Worksh. Mobil. Evolv. Internet Archit. MobiArch 2007*, Kyoto, Japan, 2007.

[20] I. Csiszar and J. Korner, "Broadcast channels with confidential messages", *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[21] N. Yang, P. Lep Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels", *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, 2013.

[22] J. Mo, M. Tao, Y. Liu, B. Xia, and X. Ma, "Secure Beamforming for MIMO Two-Way Transmission with an Untrusted Relay", in *Proc. IEEE Wirel. Commun. Netw. Conf. WCNC 2013*, Shanghai, China, 2013, pp. 3279–3284.

[23] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI", *IEEE Trans. Sig. Proces.*, vol. 59, no. 1, pp. 351–361, 2011.

[24] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Physical layer security of MIMO frequency selective channels by beamforming and noise generation", in *Proc. 19th Eur. Sig. Proces. Conf. EUSIPCO 2011*, Barcelona, Spain, 2011, pp. 829–833.

[25] H. Ochiai, P. Mitran, H. V. Poor, and V. Tarokh, "Collaborative beamforming for distributed wireless ad hoc sensor networks", *IEEE Trans. Sig. Proces.*, vol. 53, no. 11, pp. 4110–4124, 2005.

[26] H. Wang, M. Luo, X. Xia, and Q. Yin, "Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdropper's CSI", *IEEE Sig. Proces. Lett.*, vol. 20, no. 1, pp. 39–42, 2013.

[27] R. Mayrhofer and M. Welch, "A human-verifiable authentication protocol using visible laser light", in *Proc. 2nd Int. Conf. Availab., Reliab. Secur. ARES 2007*, Vienna, Austria, 2007.

Tomasz Bilski received M.Sc. (1985) and Ph.D. (1995) degrees in Computer Science from Poznan University of Technology. He is working as an academic teacher in Division of Information Systems Security, which is a part of Institute of Control and Information Engineering Poznań University of Technology. He is regularly giving lectures also on Adam Mickiewicz University in Poznań. His main research areas include: computer networks, data security and data storage. He is also involved in some projects related to time synchronization in telecommunication networks for Orange Poland – the results of the work are widely utilized by Polish telecommunication operators. He is an author and co-author of 7 books and about 70 papers, published in scientific journals and presented at national and international conferences. He has been invited to give lectures in foreign universities in Germany, Greece, Portugal and Spain.

Institute of Control and Information Engineering
E-mail: tomasz.bilski@put.poznan.pl
Poznan University of Technology
Pl. Sklodowskiej-Curie 5
60-965 Poznan, Poland