12-4-2007

Increasing security in the physical layer of wireless communication

Luke Golygowski
Edith Cowan University

DOI: 10.4225/75/57b52d39b8753
5th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, December 4th 2007

COPYRIGHT

Increasing security in the physical layer of wireless communication

Luke Golygowski
School of Computer and Information Science
Edith Cowan University
lgolygow@student.ecu.edu.au

Abstract

This paper introduces a concept of increasing securing in the Physical layer (PHY) of wireless communication. It gives a short description of current status of wireless standards and their security. Despite the existence of advanced security protocols such as IEEE 802.11i or WLAN VPNs, wireless networks still remain vulnerable to denial-of-service (DoS) attacks aiming at PHY and Data Link Layers. The new solution challenges the problems with the currently defined PHY and Data Link layers. The concept introduced here, holds a promise of descending with some of the security measures to the lower layers of the TCP/IP and in this way not only increases security but also efficiency and performance. In addition this model would reduce management overhead and security architecture complexity. The proposed solution is dealing with: encryption implemented as part of modulation techniques as well as authentication procedures partially deployed within the first two layers of Open System Interconnection (OSI) protocol stack. The introduced model attempts to solve problems related to DoS that is focused on Data Link Layer, eavesdropping and man-in-the-middle (MITM) attacks. Additionally, there are presented some ideas for future research in the area of protection from malicious activity aimed at the PHY Layer – e.g., jamming attacks, as well as other security issues such as eavesdropping prevention by use of physics laws and tunnelling as another layer of protection to ensure privacy and signal robustness. The potential deployment of this technology embraces Wireless Local Area Networks (WLANs) as well as the emerging IEEE 802.16e (mobile WiMAX) standard. In this paper there are considered and analysed practical needs, defined necessary steps and set priorities. In the final part, there are presented challenges concerning the research and there is established a background for the consecutive papers.

Keywords

Modulation, cryptography, TCP/IP, OSI Layers, PKI, Wireless DoS attacks.

INTRODUCTION

In its core design, the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol stack was not meant to be secure. It was supposed to remain operational in case of geographically dispersed disaster (Ciampa et al 2005). It was developed in times of political unrest and cold war. TCP/IP goal was to assure communication even after nuclear attack (Thomas et al 2004). However, since it was an extraordinary invention capable of completely changing the world, it was quickly released to the public. The academic circles were the first that could experiment with the new technology (Boswell et al 2003). Soon after that, it became a germ of the Internet. The potential of TCP/IP was impressive. There was created a great number of new services taking advantage of the new protocol stack (Boswell et al 2003). Despite its great functionality TCP/IP was soon proved to be missing security measures. Apart from ordinary users Internet begun to host a new black hat community of crackers (Pipkin et al 2002). Since then, members of this group keep exploiting flaws in the design of the TCP/IP protocol stack. Due to a great number of new malicious code, exploits, etc, in order to keep functionality of Internet services secure, scientists and organizations were forced to conduct intensive work in the area of security.
After release of IEEE 802.11i, there was introduced a new term in wireless communication - Robust Security

Network (RSN) (Akin et al 2003). This technology implements mutual authentication by use of digital certificates and Certification Authorities (CA). There is deployed Authentication Server (AS) - typically Remote Authentication Dial-In User Service (RADIUS) with Extensible Authentication Protocol-Transport Layer Security (EAP-TLS). This method incorporates symmetric Advanced Encryption Standard (AES) and asymmetric Rivest Shamir Adleman (RSA). Such implementation has only one weak point - CA. In addition to the RSN there is another way to secure wireless networks - it is by use of wireless Virtual Private Networks (VPNs) (Thomas et al 2004). Recently there were introduced many technologies whose vendors claim, they support mobile roaming. This indicates that enterprise implementation of WiFi Protected Access 2 (WPA2) is not the only way to support roaming users. Wireless networks configured consistent to RSN or wireless VPNs maintain integrity, protect confidentiality and ensure availability (CIA triad) (Ciampa et al 2006). Security in wireless communication is slowly reaching a point where there is not much left to invent. The similar phenomenon has affected modems, where a technology limitation was the issue. Although difficult to manage and configure it is possible to set up a reasonably secure wireless network, apart from the built-in vulnerability of wireless communication in layers one and two of Open System Interconnection (OSI) model (Ciampa et al 2006). The inherited insecurity is resulting from the open medium characteristics and deployed association mechanisms (Thurwachter et al 2002). They make this technology sensitive to PHY and Data Link layer based DoS attacks - e.g., jamming, de-authentication, flooding with incorrect frames.

Due to the enormous number of tasks often required to be accomplished by administrators, the issue is not to find the right solution but to implement it in a proper way (Boswell et al 2003). The knowledge of how to secure a wireless network is easily accessible - for instance with Google. Despite of the availability of information related to RSNs and wireless VPNs unsecured Wireless Local Area Networks (WLANs) are relatively easy to encounter (AusCERT et al 2006, CSI/FBI et al 2006, RSA et al 2007 and AirDefense et al 2007). Surprisingly this is also relevant to large corporations. This is mainly because of the ignorance of IT staff or insufficient resources. The network systems are weak either because they do not introduce the recommended solutions or they do, but in a faulty way.

Properly configured networks introduce security in depth concept. They are equipped with firewalls of many kinds: application layer, stateful packet inspecting (SPI), etc, anti-virus software (AV), proxies, intrusion detection (IDS) and prevention (IPS) systems, tunnelling protocols such as IPSec or SSH, key management protocols, authentication, authorization mechanisms, auditing tools, sophisticated cryptography tools like AES, honeypots, security policies and procedures, security policy enforcement tools like software, law. Almost every layer of the communication is fitted with security measures (Whitman and Mattord et al 2005). Current security architectures are intensively patched and often use encapsulation mechanisms around actual data stream. In this way they resemble more Frankenstein than modern technology. Security mechanisms increasingly demand and consume more of the available resources like bandwidth and processing power – e.g., various encapsulation protocols such as EAP-TLS. Together with procedures, they are driving the technology to a point where the bandwidth or other resources would be more appropriate for security than for data itself. With this tendency, future security systems would take precedence over data in the bandwidth and other resources allocation process. The continuous need for deployment of new devices and new software, arising new areas of studies, and new job positions create a “black hole” consuming budget, time and other assets. Although it may be hard to release the burden of responsibility for security from the application layer, with a slight change in the point of reference, it may be possible to increase efficiency of wireless systems without jeopardizing security. This may be possible by decrementing the layer of implementation of security measures in wireless networks to the Network Access Layer. However, this may only be the case for systems that are fully wireless and do not communicate with any network nodes over the wired infrastructure other than transmission lines between server room and Access Points (APs). In other words, there are no points of access to the network over LAN sockets. This is mainly because the security measures like encryption, would be deployed in the PHY layer which is dependent on the medium. Thus, once packets leave secured wireless medium and enter wired infrastructure there is no protection. For this reason implementation of the proposed model may be represented by wireless Wide Area Networks (WANs) and wireless Metropolitan Area Networks (MANs) like IEEE802.16e combined with WLANs and Bluetooth technologies. Wireless standards' limitations are obvious and difficult to resolve. The solution may however be closer and easier than it appears. In dynamic environments such as these present in wireless security measures development, simple solutions can be easily overlooked.

THE MEDIUM CONSIDERATIONS

Years 1980 and 1985 were breakthrough in wireless communication (Muller et al 2005). In 1980 the restrictions of use of the spread spectrum modulations to the military only, were released. In 1985 the Federal Communications Commission (FCC) defined an unlicensed operation in three frequency bands: industrial, medical and scientific (ISM). This boosted the development of commercial wireless technologies. Anyone can operate at these bands. Users are only restricted with the power levels, which had to be limited due to the

interference at these frequencies. The FCC part 15 regulates the power levels for antennas:

- Omni-directional in the 900MHz and 2,4GHz
  - Max transmitter output - 1W
  - Max Equivalent Isotropically Radiated Power (EIRP) 4W, for every additional dB of antenna gain over 6dBi, the transmitter output must be decreased by 1dBm
- Directional in 2,4 GHz
  - For every 3 additional dB of antenna gain over 6dBi, the transmitter output must be decreased by 1dBm

Current wireless LANs operate at two frequency ranges of ISM spectrum: 2,4-2,48GHz with 83,5MHz of bandwidth and 5,7-5,85GHz with 125MHz bandwidth (Henty et al 2001). The wavelength of the signal at the 2,4GHz band is approximately 12,5cm. WiMAX standard operates at UHF, SHF and EHF frequencies: below 11GHz and 10-66 GHz with channels of 25/28 MHz bandwidth (IEEE et al 2005). There are undertaken steps to utilize the 3,5GHz band worldwide as a standard frequency band for the purpose of global roaming by use of WiMAX (Maravedis et al 2005). In addition, the exclusive rights of the cellular service providers, for the lower frequency bands - e.g., 450MHz and 700MHz are being released to allow utilization of this spectrum by other technologies. The use of these bands would allow to ensure true mobility for standards such as WiMAX.

Wireless technologies transmit signals by use of electromagnetic waves. Digital signal sourcing from transmission device is used as modulating signal and may take many forms. As a carrier there is usually used a sine wave $e(t) = E_c(t)\sin(\omega_c t + \varphi)$ of much greater frequency than the baseband signal (Blake et al 2001). Modulating signal varies the carrier, according to specified modulation scheme. As a result there is emitted a modulated signal. The amount of information that can be sent is strictly related to two factors: bandwidth and modulation technique applied. The relationship is defined by the Hartley Law:

$$I = kBt, \qquad \text{where } k \text{ is a constant that depends on the SNR and modulation} \qquad (1)$$

Since WLANs face significant bandwidth and power-level restrictions, the main tool for the purpose of increasing the data rate of the signal is the appropriate modulation technique. The choice must be dictated by the allowable signal power and bandwidth.
The sine wave equation implies that carrier can be varied by changing three of its attributes: amplitude, frequency and phase. The most effective modulation schemes combine the change of more than one component simultaneously and by this achieve higher bit-rates and become more robust, for example Quadrature Amplitude Modulation (QAM) varies amplitude and phase. The modulated signal becomes a complex wave that occupies more than one frequency. These frequencies grouped together form a bandwidth. In some cases the modulated signal occupies the infinite bandwidth. The modulating signal is usually a well behaved waveform that when expanded with the Fourier series, exists in the infinite bandwidth:

$$F(t) = \tfrac{A_0}{2} + A_1\cos\omega t + B_1\sin\omega t + A_2\cos 2\omega t + B_2\sin 2\omega t + \ldots \qquad (2)$$

Apparently, for many systems, to achieve desired Quality of Service (QoS) only a small part of this spectrum is required (Blake, 2001). For example the square wave can be well represented by 10 components. In these cases, the amplitude of the frequencies drops very quickly and so does their power, thus they can be neglected. Usually the amplitude of less than 1% of the total signal voltage can be ignored. The interference imposed by these frequencies is not significant.

Instead of modulating signals in a continuous way, digital signals do it discretely (Thurwachter et al 2002). Receiver analyses a modulated signal at specified times. At these times there is identified a state of the signal, which is called a symbol. Symbols may represent a number of bits-states. This makes the transmission more bandwidth efficient. The amount of data that can be sent within a bandwidth is limited by the Shannon limit: $C = B\log_2(1 + \frac{S}{N})$, which is related to inter-symbol interference. This equation implies that the maximum number of represented bits is limited only by the Signal-to-Noise-Ratio (SNR).

Communication signals degrade due to the introduced by the operating environment noise (Mark and Zhuang et al 2003). For the purpose of effective communication the SNR is monitored and kept to a certain level. Thermal noise is always present in wireless communication. It results from the random motion of the molecules stimulated by any temperature above the absolute zero. Unfortunately the noise power is directly proportional to the bandwidth occupied by the signal. It can be defined by the following equation:

$$P_N = kTB, \quad \text{where } k \text{ is the constant Boltzmann constant} \tag{3}$$

The SNR figure indicates that it can be increased by either incrementing the signal power, or decreasing the noise level. However, increasing the power level component may be sometimes impossible, this is the case for the unlicensed spectrum (Gast et al 2002). It is either due to the regulations and law or because of the efficiency requirements. The second is especially adequate when there are introduced battery powered devices. Due to the above, the focus is made on reducing the noise. It can be done either by decreasing the noise temperature of the system or by decreasing its bandwidth. For this reason adoption of appropriate modulation technique is critical. The noise temperature must not be misunderstood with the operating environment temperature. The noise temperature is resulting from the superposition of noises introduced by each communicating device. To measure the noise temperature, there must be calculated Noise figure:

$$NF_T + NF_1 + \frac{NF_2 - 1}{A_1} + \frac{NF_3 - 1}{A_1 A_2} + \ldots \tag{4}$$

The total noise is usually specified in dB:

$$NF(dB) = 10 \log NF \tag{5}$$

Finally the noise temperature:

$$T_{eq} = 290(NF - 1) \tag{6}$$

To find the total system noise temperature there must be added several sources of the noise - for example antenna or transmission lines.

MODULATION ASPECTS

It would be a good approach to modulate the carrier without varying its amplitude, this would make the signal more robust and noise immune, allowing the receiver to neglect the envelope issues. In this way the devices would be able to implement nonlinear amplifiers. This is because the amplitude linearity is irrelevant. Although Frequency Shift Keying (FSK) introduces a good behaviour in presence of interference and is robust, it is not a good solution for modern data communication systems which require very efficient use of bandwidth (Blake et al 2001). The FSK uses only two states per symbol: Mark and Space. Frequency modulation is used for low data-rate applications - e.g., pagers and high frequency radio systems for teletype transmission (Miceli et al 2003). This spectrum is very noisy and imposes rich phase shifts to the signal. This is due to the travel through ionosphere, thus the schemes referencing to phase measurements are undesirable.

The recommended modulation scheme for systems requiring high data bit-rates within narrowband channels is QAM. The number of states a symbol can embrace is limited by the influence on the distinguishing of symbols due to the noise and distortion which is the difference between the adjacent states (Thurwachter et al 2002). Each symbol represents an amplitude/phase change made to the carrier. The 64QAM varies phase and amplitude in order to increase the error distance from each constellation point. To limit the errors due to the amplitude modification there can be used a limited number of amplitude states. In addition, introducing second component allows the system to be more efficient. This is due to the fact that the hexagonal system is more tolerant to noise than Phase Shift Keying (PSK) alone and allows to reduce the amplitude levels within the decision regions. Unfortunately this method is not free from drawbacks. The QAM modulation is more susceptible to noise then other systems (Blake et al 2001). In addition signals vary in amplitude, what results with the need of linear amplifiers.

Employing narrowband modulation would result in more robust signals. The thermal noise is equally distributed over the frequency domain, what results in relatively less noise applied to the system (Thurwachter et al 2002). More robust signal gives more precision and allows to carry more sensitive to damage data which may be crucial for tracking slight changes, reducing or eliminating false positives and passing important management

parameters which often are dependent on a single bit. This may be used to detect an attempt of tempering the signal. It may be possible to achieve this by implementation of self extracting components that take as a parameter time counter. Narrowband signals would allow to create a tunnel. Sending three signals carefully designed would appear to be like a high bandwidth signal on the frequency domain graph, hiding the information within. It may be useful to attempt to combine a spread spectrum with narrow band signals. The spread spectrum will provide protection from jamming. It also provides protection from Rayleigh fading (Blake et al 2001), which completely destroys narrowband signals. In addition the frequency hopping scheme may be designed to support, in the most effective way, a desired number of users. Within a particular bandwidth, it would also allow to send data over multiple channels. Either doing it simultaneously or using a hopping scheme. This would increase performance and better utilization of the medium, as well as increase security to a certain level.

ESTABLISHING SECURITY

The proposed model incorporates a subscribing process that assembles authentication mechanisms present in the upper layers of the TCP/IP protocol stack. To increase the overall performance, the system will use the Public Key Infrastructure (PKI), which may have already been adopted in the upper layers. The Network Interface Card (NIC) of the Subscriber Station (SS) will be issued with the encoded private-public key pair and initial modulation array. This will be done during the manufacturing process. Since the certificate exchange takes place via management frames (Ciampa et al 2005), it is possible to descend with the authentication process to the PHY layer. The Base Station (BS) will not establish connection association with the subscriber unless they are verified against AS - e.g., RADIUS. This will protect other SSs from being de-authenticated by malicious persons.

The BS will exchange with its clients certificates. In this way there will be exchanged public keys. At this stage there is no association, neither there are any frames sent to the Data Link layer. The keys are transmitted conforming to the constant scheme programmed during the manufacturing process. This burned in carrier modulation pattern exposes the public key. The hardware component decodes and extracts the public key and next passes it to the upper layers. Both communication parties perform authentication - e.g., RADIUS, and decide whether to proceed to the next step. In this way no client can exchange any management frames with the BS. Communication, network entry and initialization processes are protected against disassociation attacks.

Basing on the initial public key exchange, there will be created an *8x8* dynamic array of mappings - symbol-bit sequence. It results from the algorithm, which has to be asymmetrical in order to support PKI. It takes as an input the key and the array of symbols. The same array will be created on the peer station, for example after receiving a peer's digital certificate. Unfortunately the only existing system that would allow creating similar arrays, but in a symmetrical form is Random Number Generator (RNG) (Pfleeger and Pfleeger et al 2003). There must be developed a new algorithm, preferably basing on the existing ones, that have been tested against real life as well as widely adopted like Rivest Shamir Adleman (RSA) algorithm. Since the possible number of combinations is very low, there must be introduced some measures to increase the security, taking advantage of the key length and complexity. It is recommended to implement a chaining mechanism that would create pseudo random sequence of changes in interpretation of each symbol. The sequence must appear to the outside world as unpredictable. This complex array must be evaluated prior to transmission, instead of developed on the fly on a per packet basis. In this way there will be increased efficiency and operational speed. In addition there must be introduced a large enough counter, that would keep track of the repeated bit-sequence. It will be used as a reference to the mapping array.

Example: *Bit-symbol representation*

First iteration: 10101010 → S_1

Second iteration: 10101010 → S_2 (next symbol according to the pseudo random sequence)

This sequence must be large enough to prevent repetitions in a danger time interval zone, what was the case with Wired Equivalent Privacy (WEP) Initialization Vector (IV) length (Ciampa et al 2006). This process will divide data in blocks which are differently interpreted. The unpredictable hopping pattern will ensure privacy and complexity. In order to reduce overhead resulting from complex operations, this array generation should be implemented in hardware.

The presented above procedures were the first phase of the subscribing process, which established a secure tunnel for the shared secret evaluation. In the next step there will be established a shared secret among communicating parties. This will be achieved by use of the Diffie-Hellman algorithm [see section Diffie-Hellman algorithm on page 6]. As a result there will be created a new mapping array that will be used for modulating data transmissions. It will be evaluated using symmetric key, in the same way at both sites of communication. It must be periodically changed in order to increase protection. This section of the subscribing

process will be preferably implemented in hardware as well. After connection to the BS is established, there will be performed actions related to other layers of the TCP/IP protocol.

DIFFIE-HELLMAN ALGORITHM

Diffie-Hellman is a key exchange mechanism design to operate in a secure manner over an unsecured channel (White and Fisch and Pooch et al 1996). It is adopted by many security protocols such as SSH, IPSec or Pretty Good Privacy (PGP) (Ciampa et al 2005). The shared secret can be established by two parties without exchanging any sensitive data. The strength of the protocol relies on the fact that it is secure against eavesdropping. Even if the public number of each site has been retrieved and the encapsulating cryptographic algorithm broken by finding the public key of the communication devices, having the Y_j the attacker would have to evaluate:

$$K_{ij} = a^{X_i \log_a Y_j} \bmod q \tag{7}$$

This calculation is very CPU intensive. This is because it is extremely difficult to calculate *log mod q* in comparison to multiplication by *mod q*. If *q* was chosen to be slightly less than 2^{200}, it would take 2^{100} operations to derive this key (White and Fisch and Pooch et al 1996). Currently such calculations are considered infeasible.

The initial assumptions of the algorithm state that *q* must be defined as a prime integer. Additionally, there must be introduced a large integer *a*, such that $a < q$. Next each of the communicating parties randomly choose a number from a set of integers: *{1, 2, … q-1}*. These numbers are kept secret and denoted by each site as X_i and X_j respectively (Pfleeger and Pfleeger et al 2003). Next both devices compute their public numbers as follows:

$$Y_i = a^{X_i} \bmod q \qquad \text{and} \qquad Y_j = a^{X_j} \bmod q \tag{8}$$

After these public numbers are exchanged there can be calculated shared secret:

$$K_{ij} = Y_i^{X_j} \bmod q = (a^{X_i} \bmod q)^{X_j} \bmod q = a^{X_j X_i} \bmod q \tag{9}$$

Among the drawbacks of this algorithm one may distinguish as the most significant one, lack of the authentication mechanisms. This makes the Diffie-Hellman exchange vulnerable to the MiTM attacks (Ciampa et al 2005). In cases of systems that additionally incorporate digital certificates and provide mutual authentication, this does not affect the overall security.

SPECIAL CONSIDERATIONS AND CHALLENGES

Protection against attacks aiming at Data Link layer such as the de-authentication DoS, requires in-depth analysis of currently deployed network entry and initialization processes as well as comprehensive understanding of management frames. This must result in designing a new set of management packets as well as new mechanisms for ranging, network entry and initialization that are free from previous security flaws. In addition the new authentication mechanism must support roaming clients and cannot impose significant overhead. There must be determined how does the incorporation of PKI into the modulation and interpretation of received signals influence the total system efficiency. This also relates to the generation and management of the mapping arrays. It cannot introduce greater delays than those already present in current technologies. Depending on the results it may be necessary to search for alternative solution. Mapping arrays also introduce another concern related to cryptography. For this purpose there must be found an appropriate algorithm. Since any variations or adjustments made to the cryptographic scheme may result in compromising the algorithm (Pfleeger and Pfleeger et al 2003), the system must be designed accordingly to the algorithm, not inversely. In case no such algorithm can be found, there must be considered the feasibility of designing a new encryption algorithm for the needs of this particular system. All of the deployed handshakes must be well defined and tested in terms of security. Apart from the above concerns there must be considered modulation aspects of the proposed model. The implemented modulation must either implement the existing schemes or be compatible to

them.
In case the adoption of cryptography to the modulation mechanisms is proved to be successful, there will arise new issues with modulation regarding the signal-jamming attacks (Ciampa et al 2006). It will be necessary to modify current techniques or design a new one. It may be even desired to redefine the communication channels. There will be conducted a detail analysis of hopping schemes and their possible combination with narrowband signals. In addition there must be evaluated the required level of signal robustness. To further increase security it may be possible to introduce tunnelling mechanisms for data signal. In this way the modulated signal would be isolated from the surrounding environment.

The open character of the medium, brings benefits in the form of computer network accessibility, but also provides great potential for attackers. Rogue clients may experience anonymity caused by lack of any physical points of access. For this reason, wireless systems require technology that would allow to discover, locate and forensically identify malicious activity. At later stage of this research, there will be conducted work towards finding a forensically sound method for solving these issues.

One of the most important aspects of this research is establishing backward compatibility with existing wireless standards. This is important due to the transformation processes and the related costs. Many innovative technologies were not successfully deployed because of these issues. For many organizations a complete redesigning and rebuilding of their Information Technology (IT) architecture may be not feasible. This is especially the case when an organization has recently updated their systems. For this reason the new model deployment must support seamless transformation. It may be possible to achieve backward compatibility by introducing a modular design. Ideally the system would be independent on the implemented modulation scheme as it would reside in an separate module. In this way the new technology would also be independent from the allocated frequency band. Such design would support future industry efforts toward global roaming - e.g., 3,5GHz (Maravedis et al 2005).
Finally the developed model must be analysed in the context of introduced flaws and weaknesses (IEEE et al 2005). This embraces but is not limited to the analysis of the following:

- Certification Authorities and Digital Certificates reliability and authenticity
- Timing attacks
- Key generation and validity period
- Timer settings and re-association
- Search for opportunities for DoS attacks due to the ability to disable the station because of the performance issues or supported security protocols

When designing the new Physical layer of wireless communication it may be desired to attempt to establish a pseudo-full-duplex communication. One way of approaching this problem may be based on adoption of Multiple-Input-Multiple-Output (MiMO) smart antennas together with appropriate design of a modulation scheme. This issue may be a subject to this research in its later stage.

CONCLUSION

Security in the Physical Layer of wireless communication systems is usually referred to as a myth. The open character of the medium and its propagation together with the broadcast nature, impose threats by its nature. The factor of the risk is significant and thus the subject of securing the medium tends to be dropped. There were several attempts to increase security at this level performed by the military. One of the most well recognized method was adoption of the Frequency Hopping Spread Spectrum (FHSS) with the secret hopping scheme, known only to the communicating parties. All other projects are kept secret and the real state is unknown.
Wireless transmission is the future for communication. Looking into forward, it is hard to imagine different scenario. There will be finally developed a model that will ultimately secure this unruly medium. It will not impose unnecessary overhead and will not take precedence over data exchange. It will be simple and effective.
This paper is an introductory paper to the concept of securing the PHY layer of wireless networks' architecture. In the first stage of this research, it will be verified whether the Field Programmable Gate Arrays (FPGAs) are appropriate for adoption in this model. Tests will be performed on the current IEEE 802.11b wireless NICs. FPGAs are very powerful hardware widely adopted in current standards. They provide impressive performance and great capabilities, allowing for various implementations. The 802.11b network cards work on the similar basis as their younger equivalents. They have been chosen due to the price and accessibility. This choice of equipment forecasts the best chances of the research to be successful. However, FPGAs must be verified whether they can be programmed to perform the functions that will produce the array of mappings between symbols and sequence of bits. This embraces exchange of the digital certificates, Diffie-Hellman based handshake and cryptography support. In this way if successful, this research could be implemented in the

existing hardware. This would greatly reduce the deployment and transformation costs. If the first attempt is unsuccessful it might be necessary to develop a new wireless Network Interface Card (NIC).

ACKNOWLEDGEMENTS

The author would like to thank Dr. Andrew Woodward for his help in editing this paper as well as for sharing his knowledge and Sandra Lukasinska for her support and patience.

REFERENCES

White, G., B, Fisch, E., A, & Pooch, U., W. (1996). Computer System and Network Security: CRC Press.

Ciampa, M. (2006). CWSP Guide to Wireless Security: Thomson Course Technology.

Pfleeger, C. P. and Pfleeger, S. L. (2003). Security in Computing: Prentice Hall PTR.

Thomas, T. (2004). Network security first-step: Cisco Press

howstuffworks. (2007). from http://www.howstuffworks.com/wireless-network2.htm.

NASA. (2007). from http://science.hq.nasa.gov.

rfzone. (2007). from http://www.rfzone.org/free-rf-ebooks/.

Anttalainen, T. (2003). Introduction to Telecommunications Network Engineering: Artech House

Blake, R. (2001). Wireless Communication Technology: Delmar Thomson Learning.

Chen, Z. (2004). EMC Antenna Fundamentals.

Clancy, T. (2007). "Handover Key Management and Re-authentication Problem Statement draft-ietf-hokey-reauth-ps-01." from http://www.ietf.org/internet-drafts/draft-ietf-hokey-reauthps-01.txt.

DallasSemiconductors (2000). QPSK Modulation Demystified.

DeLucca, M. (2003). QPSK Modulation and Error Correcting Codes.

Dobbelsteijn, E. (2002). What about 802.1X? An overview of possibilities for safe access to fixed and wireless networks.

Ciampa, M. (2005). Security + Guide to network security fundamentals: Thomson Course Technology.

Gast, M. S. (2002). 802.11 Wireless Networks: O'REILLY.

Gibilisco, S. (2001). The ilustrated dictionary of Electronics: McGraw-Hill.

Henty, B. E. (2001). "A Brief Tutorial on the PHY and MAC layers of the IEEE 802.11b Standard."

IEEE. (2003). "IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines." from http://www.rfc-archive.org/getrfc.php?rfc=3580.

IEEE (2005). IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands.

Intel (2004). Adaptive Modulation (QPSK, QAM).

Limehouse Book Sprint Team (2006). "Wireless Networking in the Developing World."

Maravedis. (2005). "The WiMAX Spectrum Picture." From http://www.wimax.com/commentary/spotlight/wimaxspotlight2005_04_25.

Mark, J., W. and W. Zhuang (2003). Wireless Communications and Networking: Prentice Hall.

Miceli, A. (2003). Wireless Technician's Handbook: Artech House.

Morinaga, N., R. Kohno, et al. (2002). WIRELESS COMMUNICATION TECHNOLOGIES: NEW MULTIMEDIA SYSTEMS: Springer

Muller, N. J. (2005). Wireless A to Z: McGrw-Hill Professional.

Akin, D. (2003). CWSP. Certified Wireless Security Professional. Official Study Guide: McGrwa-Hill Professional.

RFC3748. (2004). "Extensible Authentication Protocol (EAP)." from

http://www.apps.ietf.org/rfc/rfc3748.html.

Simon, D., B. Adoba, et al. (2007). "The EAP TLS Authentication Protocol." from

http://www.ietf.org/internet-drafts/draft-simon-emu-rfc2716bis-08.txt.

Thurwachter Jr, C., N (2002). Wireless Networking: Prentice Hall.

Vorst, A. V., A. Rosen, et al. (2006). RF/Microwave Interaction with Biological Tissues. Chapter One: Fundamentals of Electromagnetics: Wiley-IEEE.

Wang, Y., M. Chow, et al. (2004). "QPSK Modulation and Demodulation."

Boswell, S. (2003). Security + Guide to network security fundamentals: Thomson Course Technology.

Pipkin, D. (2002). Halting the hacker: Prentice Hall PTR.

RSA. The Security Division of EMC. (2007). The Wireless Security Survey of London. 6th Edition. Retrieved from http://www.rsa.com/solutions/wireless/survey/wireless_security_survey_london_2007.pdf

CSI/FBI. (2006). Computer Crime and Security Survey.

Whitman, M. E. Mattord, H. J. (2005). Principles of Information Security: Thomson Course Technology.

AusCERT. (2006). 2007 retail shopping wireless security survey.

AirDefense. (2007). Australian Computer Crime and Security Survey.

COPYRIGHT