International Journal For Technological Research In Engineering
Volume 2, Issue 7, March-2015 *ISSN (Online): 2347 - 4718*

SURVEY ON PHY-LAYER KEY EXCHANGE FOR WIRELESS COMMUNICATION USING NEURAL NETWORKS

Shashikala B Roogi[1], Manjunath R Kounte[2]
Reva Institute of Technology and Management
Bangalore, India

Abstract: ***The multipath-rich wireless environment associated with typical wireless usage scenarios is characterized by a fading channel response that is time-varying, location-sensitive, and uniquely shared by a given transmitter-receiver pair.We review the PHY- layer security algorithms whose function is based on neural networks. Specifically, we studied a full key exchange scheme which includes channel sampling and thresholding and neural network based error reconciliation.***

Index Terms: Physical layer security, Information-theoretic security, wiretap channel, secrecy.

I. INTRODUCTION

Wireless communication is the fastest growing segment of communication industry. The first wireless networks were developed in pre-industrial age. These systems transmitted information through line-of sight distances. Wireless communication applications are numerous such as video transfer, military applications, voice, internet access, web browser, short messages etc. Wireless channel have time varying and multipath propagation properties. Communicate over a medium significantly less reliable than wired physical layer. Are unprotected from outside signals and interceptions. Multiuser interference (MUI) is a significant problem in wireless communications. Has neither absolute nor readily observable boundaries outside of which stations are known to be unable to receive network frames. Many technical challenges must be addressed to enable the wireless applications of the future. These challenges extend across all aspects of system design. In this paper, we analyzed a PHY-Layer key exchange protocol for a wireless link between two transceivers. Thereby, the principle of reciprocity is utilized so that the transceivers extract two highly correlated channel magnitude envelopes [6]. Furthermore, a novel thresholding process is studied, where the channel magnitude envelope is sampled by the transceivers over a pre-determined time duration, and a least square curve is calculated by using a number of these samples as a dataset. Each transceiver generates a bit string by comparing each sample of the magnitude envelope with the value of the least square curve at the corresponding position. Thus, the transceivers generate two similar bit strings that provide the basis for the cryptographic key. Due to the existence of noise and various sources of interference, there will generally be discrepancies between these two bit strings. However, symmetric key cryptography requires that both transceivers possess identical cryptographic keys. To this end, we propose an error reconciliation method, whose function is based on at wo-layer neural network. The produced key is known only t othe legitimate transceivers and is secure against eavesdropper activity [19]. The rest of the paper is organized as follows. In Section II, literature survey is given. And in Section III overview of the PHY-layer key exchange, and new channel thresholding method is reviewed. In Section IV, we describe the training process and the operation of the neural network. Simulation results are presented in Section V, andsome conclusions are drawn in Section VI.

II. LITERATURE SURVEY

A. Information Theoretically Secret Key Generation For Fading Wireless Channels

Suhasmathuret.all has presented a scheme based on level crossings of the fading process, which is well suited for the Rayleigh and Racian fading models associated with scattering environment. The complexity associated with the short term fading process is hard to predict and best modeled stochastically. The channel is used for transmission for building practical secret key generation protocols between two entities. Also motivated by observations on quantizing jointly Gaussian processes. The reliable secret key establishment can be accomplished at rates on the order of 10bitspersecond.

B. Principles of Physical Layer Security in Multiuser Wireless Networks

The paper provides a comprehensive review on the domain of physical layer security in multiuser network. The essential premise of physical layer security is to enable the exchange of confidential message over wireless channel in the presence of eavesdroppers, without relying on higher layer encryption. They proposed the pioneering work of Shannon and wyner or information-theoretical security.Also described the evolution of secure transmission strategies from point-to-point channels to multiple antenna systems. Secret key generation and establishment based on physical layer mechanism are subsequently covered.

C. Securing OFDM over Wireless Time-Varying Channels Using Subcarrier Overloading With Joint Signal Constellation

The method of overloading is based on reverse piloting, superposition modulation, and jointly decoding. It uses channel randomness, reciprocity, and fast decorrelation in space to secure OFDM with low overheads on encryption, decryption and key distribution. A necessary condition for achieving information theoretic security in accordance with

channel and system parameters is derived.

D. Key Generation in Wireless Sensor Networks Based on Frequency-Selective Channels Design Implementation and Analysis

Matthaiswihelm proposed the key generation concept in wireless sensor networks based on frequency selective channels. Key management in wireless sensor network faces several challenges such as scale, resource limitations, and new threats such as node capture.The main contributions of this paper are:

- Design of a robust key generation protocol with an error-correcting property against channel deviations.
- Implementation of the protocol on static MICAz sensormotes and analysis of the protocol's robustness and the secrecy of derived keys, especially with respect to dependencies between wireless channels .
- Derivation of a stochastic model describing the secrecy of the protocol, its validation using experimental data, and guidelines on increasing the number of generated secret bits.

E. Generation of Secret Key for Physical Layer to Evaluate Channel Characteristics in Wireless Communications

This paper aims to describe the process for encryption techniques for multimedia encryption. In this the multimedia image input is considered for encryption and decryption process. Traditional security schemes rely on public key infrastructures and cryptographic algorithms to manage secret keys. Recently, many physical-layer (PHY) based methods have been proposed as alternative solutions for key generation in wireless networks. These methods exploit the inherent randomness of the wireless fading channel to generate secret keys while providing information-theoretical security without intensive cryptographic computations.

F. A Physical Layer Key Negotiation Mechanism to Secure Wireless Networks

A physical layer key negotiation mechanism is proposed to quickly exchange and establish cryptographic keys from the legitimate channel's characteristics of uniqueness, reciprocity and unpredictability. In a system with time division duplex (TDD), the forward and the reverse channels are identical by the propagation reciprocity, while the channel to eavesdropper is independent to that of the legitimate users due to multipath or attenuation. The transmitted bits are scrambled using a shared secret key based on the channel between two nodes to secure the wireless link without key management.

III. OVERVIEW OF PHY-LAYER KEY EXCHANGE

The simplest network where problems of secrecy and confidentiality arise is a three-terminal system comprising a transmitter, the intended (legitimate) receiver, and an unauthorized receiver, wherein the transmitter wishes to communicate private message to the receiver. In the sequel, the unauthorized receiver is referred to interchangeably as an eavesdropper or wiretapped. The vast majority of physical layer security research reviewed in this survey contains the premise that the eavesdropper is passive, i.e., does not transmit in order to conceal its presence.

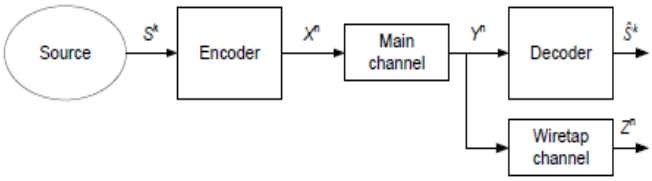

Fig .1 Communication wiretap channel

Encryption of messages via a secret key known only to the transmitter and intended receiver has been the traditional route to ensuring confidentiality. In the early 20th century, the design of cryptographic methods was based on the notion of computational security, without a solid mathematical basis for secrecy.

A. Key Exchange

A cryptographic key exchange scheme for a wireless communication setting has to adhere to some basic principles. In that the two transceiver nodes are communicating over a wiretapped channel. That being said, the key exchange scheme should (a) produce information-theoretically secure keys and (b) perform error reconciliation between the private keys generated by the transmitter and receiver, such that they become identical. It is assumed that the transceivers communicate over an additive white Gaussian noise (AWGN) channel with slow Rayleigh fading, Our approach utilizes the reciprocity principle in a wireless channel as in [2], where two transmitters operating in the same frequency band would experience the same channel characteristics at the same time. Also, we assume that the eavesdropper is at such a distance from both communicating nodes, that the envelope of the signal received by the eavesdropper is uncorrelated with the signal received by the legitimate receivers. This statement is true in most practical implementations. Specifically, an eavesdropper who is more than half a wavelength away from both legitimate transceivers will experience two independent fading channels to the two transceivers.

B. Thresholding

A thresholding method was studied, where thethreshold of the sampled sequences is determined by an automatic gain control (AGC) mechanism, so that it is independentof the transmit power and the link attenuation. Here, we present an alternative thresholding method which is more efficient even in environments where deep fades do not occur, e.g. in line-of-sight (LoS) situations. Let g_A and g_B be the sampled sequences of length L thatboth transceivers - A and B - generate by sampling the channel magnitude envelope. Each sample is represented by (i, g_K [i]),where i is the position of the sample in the sequence andg_K[i], K € {A,B}, denotes its value. Transceivers A and B form the sets S_A and S_B, respectively, which contain all local maxima and minima of

g_A and g_B. We define the sets S_K^{max} and S_K^{min}, which contain the localmaxima and minima of g_K, respectively, multiplied by ascaling factor, $u \leq 1$. These sets are formally defined as

S_K^{max}= {(i, $ug_K[i]$) $Ig_K[i-l]<g_K[i]$ ^ $g_K[i+l]<g_K[i]$,
i = 2,⋯ ,L - I} (1)

S_K^{min} = {(i,$ug_K[i]$) $Ig_K[i-l]>g_K[i]$ ^$g_K[i+l]>g_K[i]$,
i =2,⋯,L-1} (2)

Thus, the set S_K is

$S_K^{max} \cup S_K^{min}$ (3)

Then, each transceiver calculates a least-square polynomialcurve [20] by using the elements of S_K as data points. Thedegree of the polynomial can be selected depending on thelength of the sampling time frame and the maximum Dopplershift. Afterwards a sequence of length L, S_K, is formed byboth transceivers by sampling their respective least-squarecurves at the points 1,2,⋯ , L. Each transceiver generatesa bit string ρ_K of length L by comparing each element of S_K with its respective element of g_K. For each i € [0, L], if thevalue of $S_K[i]$ is greater than that of $g_K[i]$, the correspondingelement $\rho_K[i]$ of the bit string ρ_K is set equal to 0. Otherwise,it is set equal to 1. Thus, the bit strings ρ_A and ρ_B are

$\rho_K[i]$= {1, $g_K[i] \leq S_K[i]$ } .
$\rho_K[I]$ = {0, $g_K[i] \leq S_K[i]$ } i= 1,2,…..L (4)

Before the sampling process, a low-pass filter should be usedin order to smoothen the sequence g_K and eliminate highfrequencycomponents that can potentially harm the effectiveness of this method.

IV. ALGORITHM GIVEN BY DIMITRIOS et.all

Error Reconciliation Algorithm Reimplementation

An efficient neural network based error reconciliation method is presented. Let the transceivers A and B have generated bit strings ρ_A and ρ_B, respectively, of length L. The eavesdropper is oblivious to the fading characteristics of the communication channel between the two legitimate nodes, and thus cannot deduce the values of ρ_A and ρ_B. The correlation between the channels perceived by A and B will always be less than 1. However, if ρ_A and ρ_B are not identical, they cannot be used as cryptographic keys. The method presented in this uses these two similar bit strings in order to generate a cryptographic key of arbitrary length, which will be known to both transceivers.

A. Neural Network Description and Operation

Let L be the length of ρ_A and ρ_B, ρ the cryptographic key, and Lt the length of ρ, which is selected arbitrarily based on the desired key length. The neural network uses binary inputs and outputs and consists of an input layer of L nodes, a hidden layer of N nodes, and an output layer of Lt nodes. The value of N is selected taking into account that higher values increase the complexity, but also the error reconciliation capability of the key exchange scheme. A graphical representation of this neural network can be seen in Fig.2, where the hidden layer neurons are denoted by Hj and the output layer neurons by Zj'

An overview of this scheme is described as follows.

- Transceiver A creates a binary neural network with the parameters as noted above and randomly initializes its synaptic weights.
- Transceiver A randomly generates the cryptographic key ρ of length Lt·
- The neural network is trained by using a training set that consists of inputs similar to ρ_A.
- The synaptic weights of the neural network are transmitted to transceiver B.
- Transceiver B applies ρ_B as an input to the neural network with the received synaptic weights. The neural network should output ρ.

In Step 2, the cryptographic key is randomly generated. It should be noted in order to maximize the security of the key, each bit of ρ, which is denoted by

ρ[i] ,i = 1,2,⋯ Lt, .

Also, in Step 4, to ensure the correct transmission of the required information, the use of an error correction scheme is recommended.

B TRAINING OF NEURAL NETWORK

We define the training set that is used for the training process of the neural network.

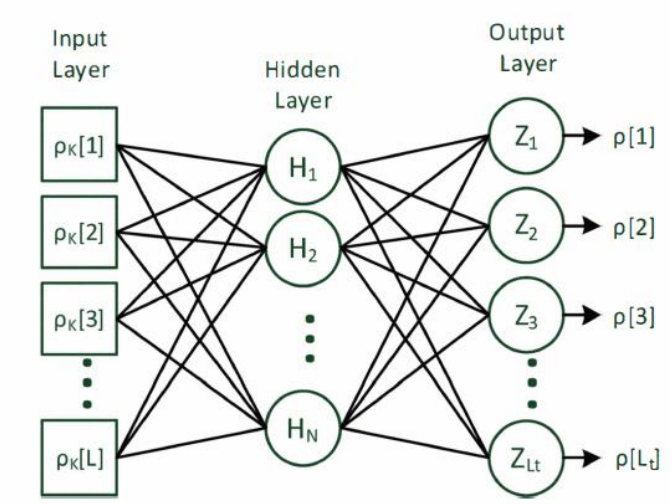

Fig. 2 the neural network

ρ_K - which has previously been defined in (4) is redefined as

ρ_K= {(i_l^k ,j_l^k)|l = 1,…t}, (5)

where t denotes the number of fades detected by the thresholding process. Let

$h_l(s, k)$ = {s , k = l}
$h_l(s,k)$ = {0 , k ≠ l},l, s, k € Z (6)

Given the bit string $\rho_A$and using the notation described above, we define the strings $T_1^{s,k}$and $T_2^{s,k}$ as

$T_1^{s,k}$ = { (i_l^A+ h_l (s,k),J_l^A) | (i_l^A, j_l^A) € ρ_A}, (7)
$T_2^{s,k}$ = { (i_l^A,j_l^A+ h_l (s,k)) | (i_l^A, j_l^A) € ρ_A}, (8)

Thus, we define the set of bit strings T, for the Neural Network's Training set is,

T = {$Tj^{s,k}$| s € [-M, M], k € [1,t], j € {1,2}} (9)

Where M is a parameter that denotes the maximum shift that is applied to a fade's beginning or end.

In order to describe the neural network'straining algorithm, we consider a layer with N_1 inputs andN_2 nodes - and subsequently N_2 outputs. This can refer toeither the hidden or

the outer layer. The synaptic weight forthe j-th input of the i-th neuron on this layer is denoted byw_{ij} All weights w_{ij} are initialized randomly to be either -1or 1, so that $P(w_{ij} = -1) = P(w_{ij} = 1)$. If Xij denotes thej-th input of the i-th neuron.
For the neural network's training, a Hebbian learning rule is used, so that the alteration in the value of $w_{ij}$is definedas

$$\Delta w_{ij} = c e_i x_{ij}, \quad (10)$$

Where $c \in R^+$ denotes a training parameter that can be selected arbitrarily. The altered value of w_{ij} is given as

$$w_{ij}^{|} = w_{ij} + \Delta w_{ij} \quad (11)$$

The bit string $\rho_A[i]$ of the neural network's training process is performed by transceiver A consists of the following steps:

- The cryptographic key ρ is generated and the neural network's synaptic weights are initialized.
- The output layer of the neural network is trained by using ρ_A as an input m times. The synaptic weights of the output layer are updated accordingly, while the synaptic weights of the hidden layer remain unchanged.
- The output of the hidden layer, denoted by ρ_h, is calculated with ρ_A as input.
- The training set T is formed and the neurons of both hidden and output layers are trained by using ρ_h and ρ as target outputs, respectively. Each element of T is used m times. m is a parameter that can be selected based on the time available for the neural network's training.

V. TEST RESULTS

In this section we discuss the example test results on Neural Network tool box in MATLAB.

A. Classification of a 4-class problem with a multilayer perceptron.

In this example a 4 clusters of data (A,B,C,D) are defined in a 2-dimensional input space. The task is to define a neural network for classification of arbitrary point in the 2 dimensional space into one of the classes (A,B,C,D).Firstly we define 4 clusters of input data, And define the output coding for all 4 clusters. Plot the clusters of data has shown in fig 1. Prepare the input & output for training a multilayer perceptron neural network, by combining the input data and defining output target.

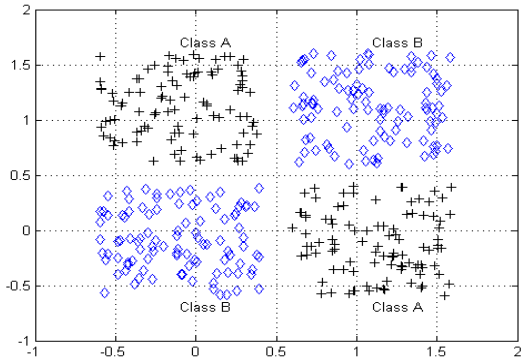

Fig 3: Plot of 4 clusters of data

Create and train a multilayer perceptron, after training, plot targets and network response to see how good the network learns the data shown in fig2.

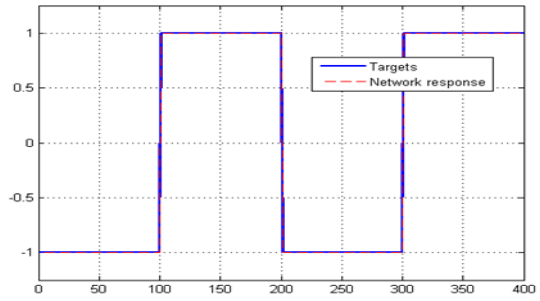

Fig 4: plot of targets and network response

plot classification result for the complete input space as shown in fig 3.

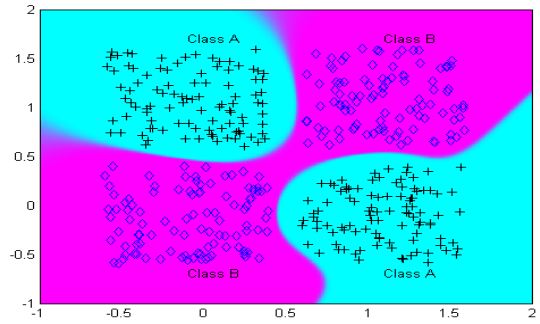

Fig 5: Plot of classification result for the complete input space

B. Prediction of chaotic time series with Non Linear auto regressive neural network.

Design a neural network for the recursive prediction of chaotic Mackay-Glass time series, try various network architectures and experiment with various delays. Generate the data using Mackay-Glass time series equation. And prepare the validation and training data and plot shown in fig1.

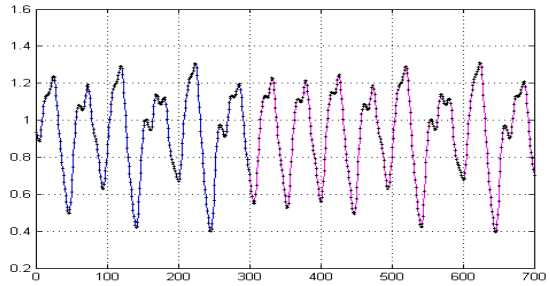

Fig 6: plot of validation & training data

Define the non linear auto regressive neural network and Prepare input and target time series data for network training. Train the network and predict recursive on validation data and plot shown in fig 2

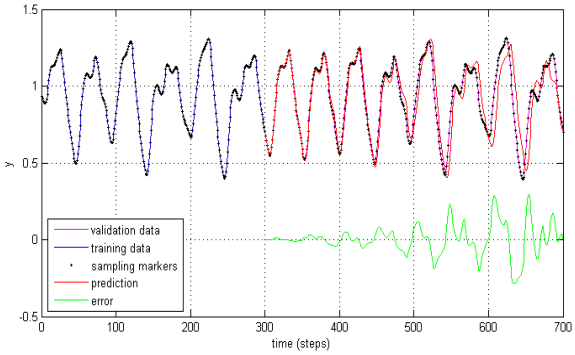

Fig 7: plot of predicted Recursive on validation data

VI. CONCLUSION AND FUTURE WORK

PHY-layer key exchange algorithm for wireless communications and analyzed its performance and security level. We are going to implement a least-square based channel thresholding method in order to extract a bit string from the channel's fading characteristics. the concept behind neural network based error reconciliation was applied, and its specific characteristics, as well as studied training process, were implemented and also error rate is reduced in future.

REFERENCES

[1] W. Diffie and M. E. Hellman, "New directions in cryptography," IEEETrans. Inf. Theory, vol. 22, no. 6, pp. 644--654, November 1976.

[2] J. Hershey, A. Hassan, and R. Yarlagadda, "Unconventional cryptographickeying variable management," IEEE Trans. Commun., vol. 43,no. 1, pp. 3 --6, Jan. 1995.

[3] Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust keygeneration from signal envelopes in wireless networks." in ACM Conf.on Comput. andCommun. Security'07, 2007, pp. 401--410.

[4] S. Mathur, N. M, C. Ye, and A. Reznik, "Radio-telepathy: extracting asecret key from an unauthenticated wireless channel," in MobiCom 08,2008, pp. 128-139.

[5] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Using thephysical layer for wireless authentication in time-variant channels," IEEETrans. Wireless Commun., vol. 7, no. 7, pp. 2571-2579, 2008.

[6] P. Yu, 1. Baras, and B. Sadler, "Physical-layer authentication," IEEETrans. Inf. Forensics Security, vol. 3, no. 1, pp. 38-51, 2008.

[7] N. Patwari, 1. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelatedbit extraction for shared secret key generation from channel measurements,"IEEE Trans. Mob. Comput., vol. 9, no. 1, pp. 17-30, 2010.

[8] 1. Croft, N. Patwari, and S. K. Kasera, "Robust uncorrelated bit extractionmethodologies for wireless sensors," in Proc. of the 9th ACMflEEEInternational Conf. on Inf. Process. in Sensor Netw., ser. IPSN '10. NewYork, NY, USA: ACM, 2010, pp. 70-81.

[9] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, "Exploiting multipleantennadiversity for shared secret key generation in wireless networks,"in Proc. of the 29th Conf. on Inf. Commun., ser. INFOCOM'10.Piscataway, NJ, USA: IEEE Press, 2010, pp. 1837-1845.

[10] G. R. Tsouri and D. Wulich, "Securing OFDM over wireless timevaryingchannels using subcarrier overloading with joint signal constellations,"EURASIP 1. Wirel. Commun. Netw., vol. 2009, pp. 6:1--6:18,March 2009.

[11] M. Wilhelm, I. Martinovic, and 1. B. Schmitt, "Key generation inwireless sensor networks based on frequency-selective channels - design,implementation, and analysis," CoRR, vol. abs/1005.0712, 2010.

[12] M. Wilhelm, I. Martinovic, and 1. B. Schmitt, "On key agreement inwireless sensor networks based on radio transmission properties," in 5thIEEE Workshop on Secure Netw. Protocols, 2009. NPSec2009.,oct.2009, pp. 37--42.

[13] M. Forman and D. Young, "The generation of shared cryptographic keysthrough half duplex channel impulse response estimation at 60GHz,"in 2010 International Conference on Electromagnetics in AdvancedApplications (ICEAA), 2010, pp. 627--630.

[14] M. Di Renzo and M. Debbah, "Wireless physical-layer security: Thechallenges ahead," in International Conf. on Advanced Technologies forCommun., 2009. AT C '09, 2009, pp. 313 -316.

[15] S. Mathur, A. Reznik, C. Ye, R. Mukherjee, A. Rahman, Y. Shah, W. Trappe, and N. Mandayam, "Exploiting the physical layer forenhanced security [security and privacy in emerging wireless networks),"IEEE Wireless Commun., vol. 17, no. 5, pp. 63 -70, 2010.

[16] M. Zafer, D. Agrawal, and M. Srivatsa, "A note on information-theoreticsecret key exchange over wireless channels," in 47th Annual AllertonConf. on Commun., Contr., and Comput., 2009. Allerton 2009, 30 2009.

[17] Martinovic, P. Pichota, and J. B. Schmitt, "Jamming for good: a freshapproach to authentic communication in WSNs," New York, NY, USA,pp. 161-168, 2009.

[18] R. Liu and W. Trappe, Securing Wireless Communications at thePhysical Layer, 1 st ed. Springer Publishing Company, Incorporated,2009.

[19] S. Haykin, Neural Networks: A Comprehensive Foundation. PrenticeHall, 1999.

[20] Dimirios S. Karas, George K. karagiannidis, and Robert Schober, “Neural network based PHY-layer key exchange for wireless communication”, Dept. of Electrical and computer engineering, IEEE Indoor and Mobile Radio Communication, 2011.

