Secret Keys Based on Multipath Directivity in Wireless Channels

Dimitar G. Valchev

***Abstract* – This paper proposes a new method for determining the secret key for encrypting the information exchanged through the multipath channel between two wireless communicating nodes. Based on the multipath structure of the wireless environment, this method is site-specific, making it stable against various kinds of systematic attacks.**

***Keywords* – Cryptography, multipath channels.**

I. INTRODUCTION

The shared medium of the wireless channel poses a challenge in implementing secure communications. The problem is addressed mainly by various cryptographic methods usually performed at the application layer of wireless networking. The so implemented cryptographic algorithms are vulnerable to attacks similarly to every kind of encrypting algorithm. A usual way to achieve resistance to attacks is to regularly change the algorithm according to some predetermined sequence. Another way is to exploit the physical and geometrical parameters of the multipath wireless channel to determine the secret key shared between the communicating nodes [1, 2]. This can be used especially in multiple-input multiple-output (MIMO) communications where the transmission parameters of the distinct propagation paths may be used to determine the secret keys used for the encrypted signal through them.

To ensure unique symmetric secret key through a given propagation path, the channel has to be reciprocal, meaning that the propagation path between two wireless link ends is one and the same in both directions of transmission. The reciprocal multipath wireless channel having *directivity* at both link ends is characterized by a set of spatial parameters [4] that can be used to determine the parameters of the encryption algorithm. Those spatial parameters are derived from the bidirectional joint angular power density (APD) function showing how much multipath power is exchanged at a particular azimuth pair at both wireless link ends. The joint APD depends on the scattering in the wireless channel. Thus, the encryption would be based on a particular placement of the scattering objects within the environment of the wireless networks. The spatial parameters determining the secret key can be properly quantized to map a particular secret key to a quantization level for the spatial parameter.

Dimitar G. Valchev is with the Department of Computer Systems and Technologies, Asen Zlatarov University, Burgas 8010, Bulgaria, E-mail: dvalchev@ece.neu.edu

This work is supported by Asen Zlatarov University, Faculty of Technical Sciences, project # 213/2010.

This approach may be used in both infrastructure-based and ad hoc wireless networks. In the infrastructure-based wireless networks a reciprocal channel is formed between the access point and each wireless user to which the corresponding channel is assigned. In ad hoc wireless networks there is a reciprocal channel between each pair of communicating nodes. In both cases the spatial parameters of the multipath channel may determine the secret key used to encrypt the information between the two communicating devices.

II. JOINT MULTIPATH SHAPE FACTORS

In [4] the concept of spatial parameters termed joint multipath shape factors has been developed for modeling wireless channels characterized by multipath at both link ends. Those spatial parameters are extensions to the multipath shape factors developed in an earlier work for a single wireless node [3]. The joint multipath shape factors are derived in terms of the double Fourier coefficients of the joint multipath APD at both the communicating nodes. A particular interest is paid to the following joint multipath shape factors:

Positive joint angular constriction between link ends a and b:

$$\Gamma_{+} = \frac{2\left|F_{1,-1} - F_{1,0}F_{0,-1}\right|}{2F_{0,0}^2 - F_{1,0}^2 - F_{0,1}^2} \tag{1}$$

Negative joint angular constriction between link ends a and b:

$$\Gamma_{+} = \frac{2\left|F_{1,1} - F_{1,0}F_{0,1}\right|}{2F_{0,0}^2 - F_{1,0}^2 - F_{0,1}^2} \tag{2}$$

with $F_{m,n}$ being the m^{th} order, n^{th} order double Fourier coefficient of the joint APD $p(\theta_a, \theta_b)$ given by

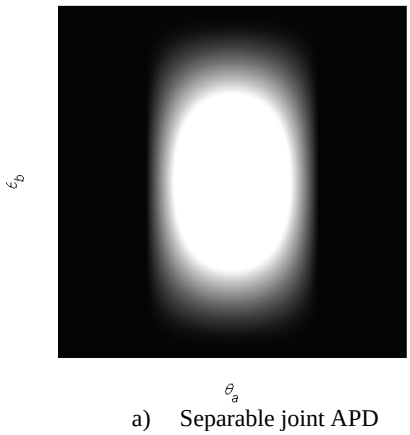
$$F_{m,n} = \int_0^{2\pi}\int_0^{2\pi} p(\theta_a, \theta_b) e^{j(m\theta_a + n\theta_b)} d\theta_a d\theta_b \,. \tag{3}$$

with θ_a and θ_b being the azimuths at link ends *a* and *b*, respectively. The joint APD function may be estimated by channel sounding techniques between the *a* and *b* link ends before the actual communication process begins. Then the corresponding spatial parameters in (1)–(2) are derived for determining the secret key.

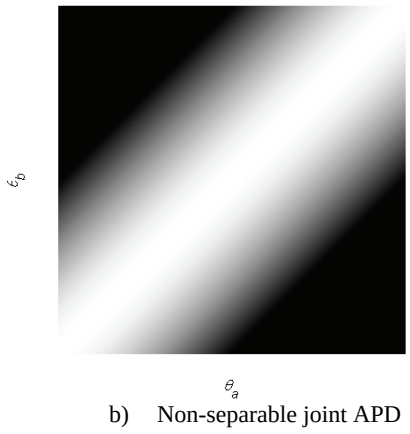
The positive and negative joint angular constrictions between the *a* and *b* link ends, Γ_+ and Γ_-, both range from 0 to 1 and are measures of the angular separability of the joint APD. Indeed, if the joint APD is separable, that is, $p(\theta_a,\theta_b)=p(\theta_a)p(\theta_b)$, then after substitution in (3) it can be easily shown that both (1) and (2) become zero. Note that the terms positive and negative a relative, depending on the chosen orientation at each link end. For $\Gamma_+=\Gamma_-=0$, the joint APD is separable in the azimuth angles at the two link ends,

or $p(\theta_a,\theta_b) = p(\theta_a)p(\theta_b)$. The positive joint angular constriction Γ_+ is equal to one when the joint APD is non-zero only on the line $\theta_a - \theta_b = \theta_0^+$ for some $0 \le \theta_0^+ \le 2\pi$. The negative joint angular constriction Γ_- is equal to one when the joint APD is non-zero only on the line $\theta_a - \theta_b = \theta_0^-$ for some $0 \le \theta_0^- \le 2\pi$.

The so defined joint multipath shape factors have certain significance in expressing the second-order fading statistics in mobile-to-mobile wireless channels [4]. Here, these multipath



a) Separable joint APD



b) Non-separable joint APD

Fig. 2. Joint APD between link ends *a* and *b*

shape factors are used only to determine the secret keys for the encryption algorithm.

Two possible joint APDs are shown in Fig. 1 with the darker regions corresponding to lower power and the brighter regions corresponding to higher power at a given angular pair θ_a, θ_b. Fig.1a shows a separable joint APD and Fig.1b shows a non-separable joint APD. The separable joint APD determines zero joint angular constrictions while the non-separable joint APD determines non-zero joint angular constrictions. Thus, the joint APD with its spatial parameters given by (1) and (2) determines the secret key to be used for encryption.

III. Secret Key Determination

The joint multipath shape factors are suitable for determining a symmetric secret key generation because they are directly associated with the reciprocity of the channel. The single node multipath shape factors are characteristic only to the node for which they are derived and therefore are not appropriate for determining a symmetric secret key to be used to transmit information to the other node.

It is possible to derive the secret key using the multipath shape factors at a single node only [3] but then the secret key would no longer be symmetric, since the multipath structure at the one node is generally different than the multipath structure at the other node. However, such an approach would allow for a larger variety of methods for determining the secret key since more spatial parameters would be used either alone or in a combination. In an infrastructure-based wireless network the information about the multipath structure at each node could be sent from the node to the access point so the controller at the access point determines the secret key to be used for that wireless node. In an ad hoc wireless network the information about the multipath structure at each node is exchanged between the communicating devices during a handshaking phase of the communication initialization process. Taking this idea further, the secret keys can be based on the three-dimensional multipath shape factors at each link end [5] which would give more possibilities for combining the increased number of spatial parameters and hence for making the encrypting algorithms less vulnerable to various attacks.

IV. Conclusion and Future Work

This paper proposes a new method for generating secret keys for encrypting the information transmitted between two communicating nodes. The method is based on the joint multipath directivity characterizing the wireless channel between the two devices. There are two joint spatial parameters, termed joint angular constrictions, which characterize the joint multipath directivity. This gives freedom to choose various approaches for determining the corresponding secret key for communication between the two nodes. If the placement of the communicating nodes or the scattering objects within the wireless environment changes, the secret key would also be changed through the new spatial parameters. This further stabilizes the method against attacks. Future work will be focused on designing non-symmetric secret keys based on the single multipath shape factors at each wireless communicating node.

References

[1] A. Sayeed and A. Perrig, “Secure wireless communications: secret keys through multipath”, ICASSP 2008, 2008.

[2] T.-H. Chou, A. Sayeed and S. Draper, “Impact of channel sparsity and correlated eavesdropping on secret key generation from multipath channel randomness”, ISIT 2010, 2010.

[3] G. D. Durgin and T. S. Rappaport, “Theory of multipath shape factors for small-scale fading wireless channels”, *IEEE Trans. Antennas Propag.*, vol. 48(5), pp. 682–693, 2000.

[4] D. G. Valchev, "Spatial modeling of three-dimensional multipath wireless channels", PhD dissertation, Boston, 2008.

[5] D. G. Valchev and D. Brady, "Three-dimensional multipath shape factors for spatial modeling of wireless channels", *IEEE Trans. Wireless Commun.*, vol. 8(11), pp. 5542–5551, 2009.