Contribution Estimation of Dominant Partial Waves into Phase of Multipath Signal Used for Encryption Key Generation

Amir I. Sulimov, *Member, IEEE,* Oleg N. Sherstyukov, Arkadiy V. Karpov, *Member, IEEE*
Department of radio physics, Institute of physics
Kazan Federal University
420008, 18th Kremlyovskaya Str., Kazan, Russian Federation
asulimo@gmail.com, lada-sher@mail.ru, arkadi.karpov@kpfu.ru

***Abstract* — Randomness of fast fading multipath channels has been used for encryption keys generation for a long time. It is believed that until an adversary is able to intercept all partial waves detected by legal users, generated keys are secure. In many cases, however, only one or two dominant waves may define the channel fading and generated key. In this work, we examine a possibility of creating a partial key highly-related to the legal key using information about only a few dominant partial waves. Based on simulation of multipath radio propagation, correlation of partial phase formed only by dominant waves and total phase of multipath signal is assessed for various contributions of the dominating component. A key interception probability is estimated for Multipath Key Generation systems exploiting randomness of carrier phase. An influence of the line-of-sight component and number of multipaths on the correlation of partial and total phases is considered. It is shown that a serious threat to security of the generated key exists only if the dominating component holds at least a 95%-share of the signal power, which is unlikely in practice.**

Key words — multipath radio propagation; encryption key; carrier phase; partial waves; partial phase; partial key; correlation.

I. INTRODUCTION

The Multipath Key Generation (MKG) exploits randomness of fast fading multipath channel to create identical copies of a shared encryption key at two nodes *A* and *B* [1]. Both nodes should exchange a series of probing signals. While propagating through a multipath environment, the signals are randomly modulated by the fast fading. By further demodulation of the received signal, the nodes generate two random bit strings key_A and key_B. These strings are identical ($key_A = key_B$) due to the channel reciprocity and not known to anyone, except for the nodes *A* and *B*, which allows their use as a secret encryption key. Such scenario is natural for urban environment, which allows its implementation in cellular communications for secure distribution of secret keys between base transceiver stations and user mobile phones.

Various signal parameters are used for the key generation purposes. However, one of the most secure are phase methods [2][3]. Being both periodical and ambiguous, carrier phase cannot be intercepted reliably at distances greater than $\lambda/2$ from a legal node. Thus, security of the generated key relies on a rapid spatial decorrelation of the carrier phase. From a physical point of view, it means that an adversary is unable to eavesdrop to all partial waves detected by user. When analyzing wireless communications in urban environment, it is common to refer to the Rayleigh channel model that assumes equal power of all partial waves. A more general model based on the Nakagami-m distribution permits a presence of a few dominant waves in the received signal [4]. Such waves may define almost completely dynamics of the channel fading along with the generated key. Therefore, if the adversary focused his efforts on intercepting the dominant waves (or simply D-waves, for shortness), it would be a serious threat to security of the key.

Another malicious threat is the external modulation attack that completely compromises all amplitude-based MKG-systems [5][6]. In this attack, a set of high-power transmitters is arranged around the legal nodes to imitate a natural channel fading by modulated radio emissions. In essence, each malicious transmitter creates its own D-wave. Due to use of modulated phase samples, legal nodes create an unsecure key that follows the modulation law defined by the adversary.

The purpose of this work is to examine a possibility of creating a partial key highly-related to the legal key using information about only a few D-waves. We perform numerical estimates of correlation of partial phase formed only by a few D-waves and total phase formed by all multipaths for various contributions of the dominating component. By binary quantization of samples of total and partial phases, the legal and partial keys are created to assess a key interception probability. The estimates are done both for LOS and NLOS scenarios with typical (12-tap) and low (3-tap) number of multipaths.

The paper is structured as follows. Section II presents scenario model. Channel simulation is described in Section III. Correlation estimates of partial and total phases are given in Section IV. Section V gives estimates of the key interception probability. Conclusion summarizes our principal results.

II. SCENARIO MODEL

In this section, we present a mathematical model of the multipath signal containing two D-waves and describe scenarios of both passive and active attack on the system.

This work was performed according to the Russian Government Program of Competitive Growth of Kazan Federal University.