Zheng WAN, Mengyao YAN, Kaizhi HUANG, Zhou ZHONG, Xiaoming XU, Yajun CHEN, Fan WU, 2023. Pattern-reconfigurable antenna-assisted secret key generation from multipath fading channels. *Frontiers of Information Technology & Electronic Engineering*, 24(12):1803-1814. https://doi.org/10.1631/FITEE.2300126

Pattern-reconfigurable antenna-assisted secret key generation from multipath fading channels

Key words: Physical layer security; Secret key generation; Reconfigurable reflecting surface; Multipath fading; Pattern-reconfigurable antenna

Corresponding author: Kaizhi HUANG
E-mail: huangkaizhi@tsinghua.org.cn
ORCID: https://orcid.org/0000-0002-7084-3826

Motivation

1. Compared with traditional cryptography techniques with high computational complexity and high delays, physical layer key generation (PKG) provides an alternative idea to establish symmetric keys between legitimate parties.
2. Multipath fading at the receiver may degrade the correlation between legitimate uplink and downlink channels, resulting in a low key generation rate (KGR).
3. By effectively and rapidly changing the radiation pattern in a software-programmable manner, pattern-reconfigurable antenna (PRA) has the ability to combat fast fading and thus improves the receiving performance.

Method

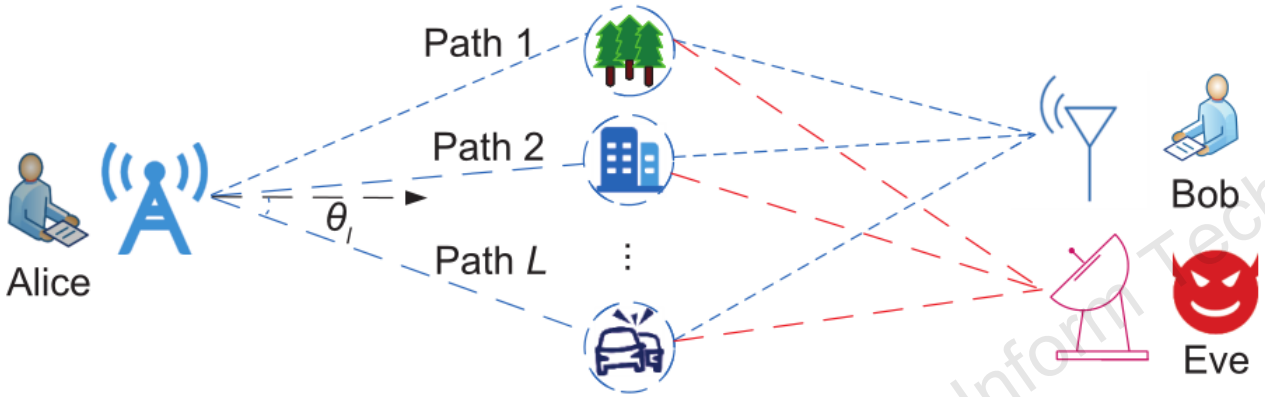


Fig. 1 System and channel model

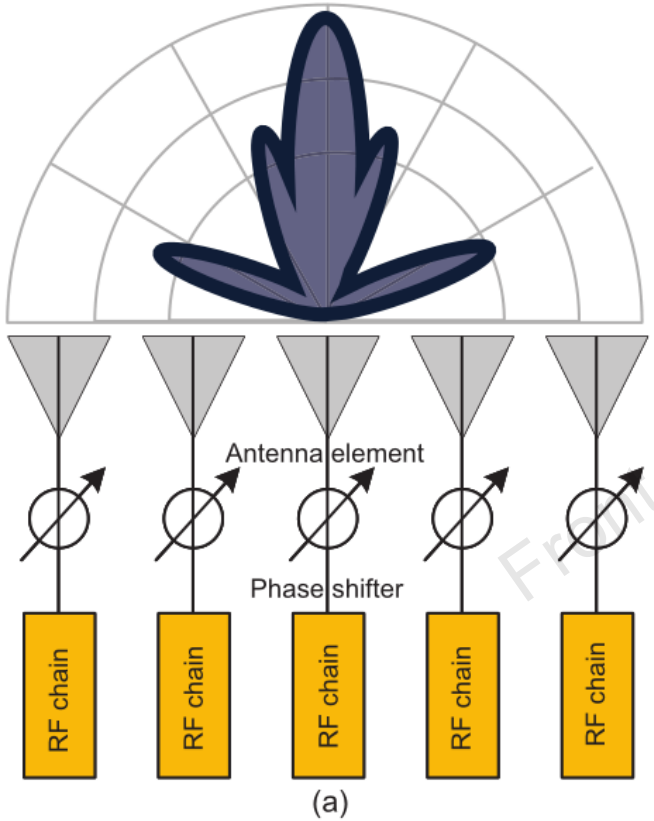
We consider a narrowband time-division duplexing (TDD) communication system, wherein a base station (BS) Alice and a user Bob aim to extract consistent keys from the wireless channel.

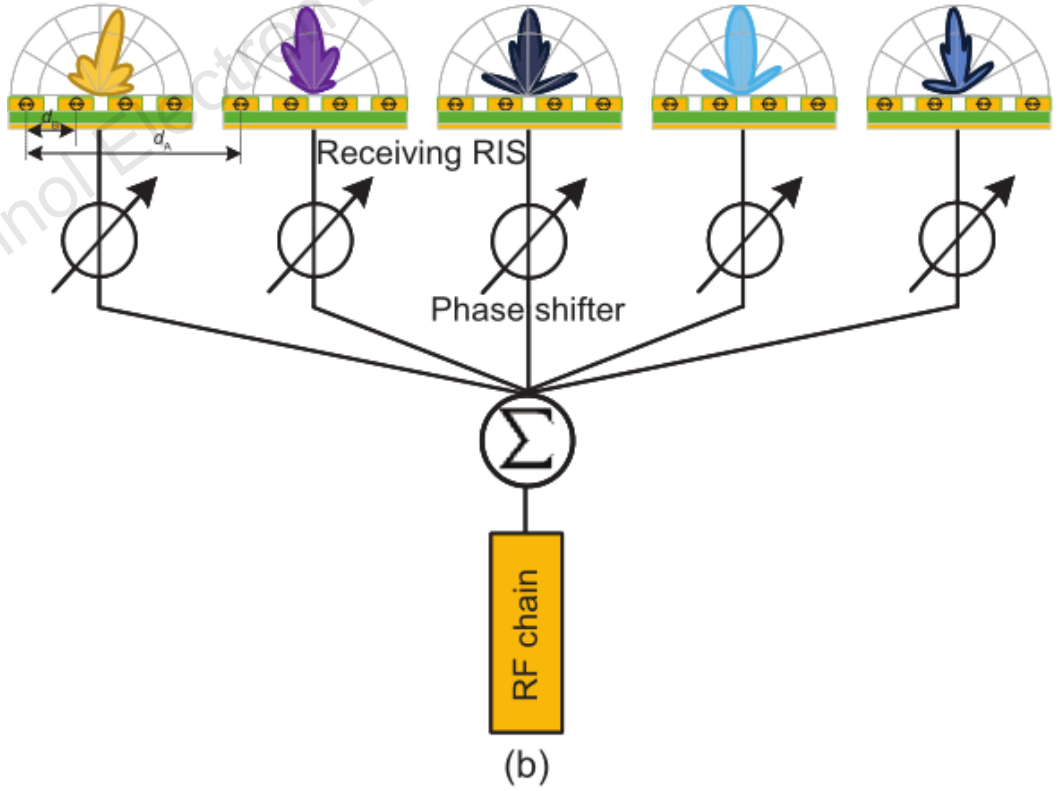
Alice is equipped with a PRA, and Bob is a single-antenna user. Meanwhile, a passive eavesdropper Eve is several wavelengths away from Bob.

The wireless channel between Alice and Bob is modeled as the typical Saleh–Valenzuela channel model, in which the signal travels through L resolvable paths to reach the receiver.

Method

Unlike existing arrays that maintain a fixed structure, PRA is a single-channel antenna, in which the PRA elements control patterns in terms of shape, direction, or gain.





(a) a conventional phased array architecture;

(b) the proposed pattern-reconfigurable antenna architecture;

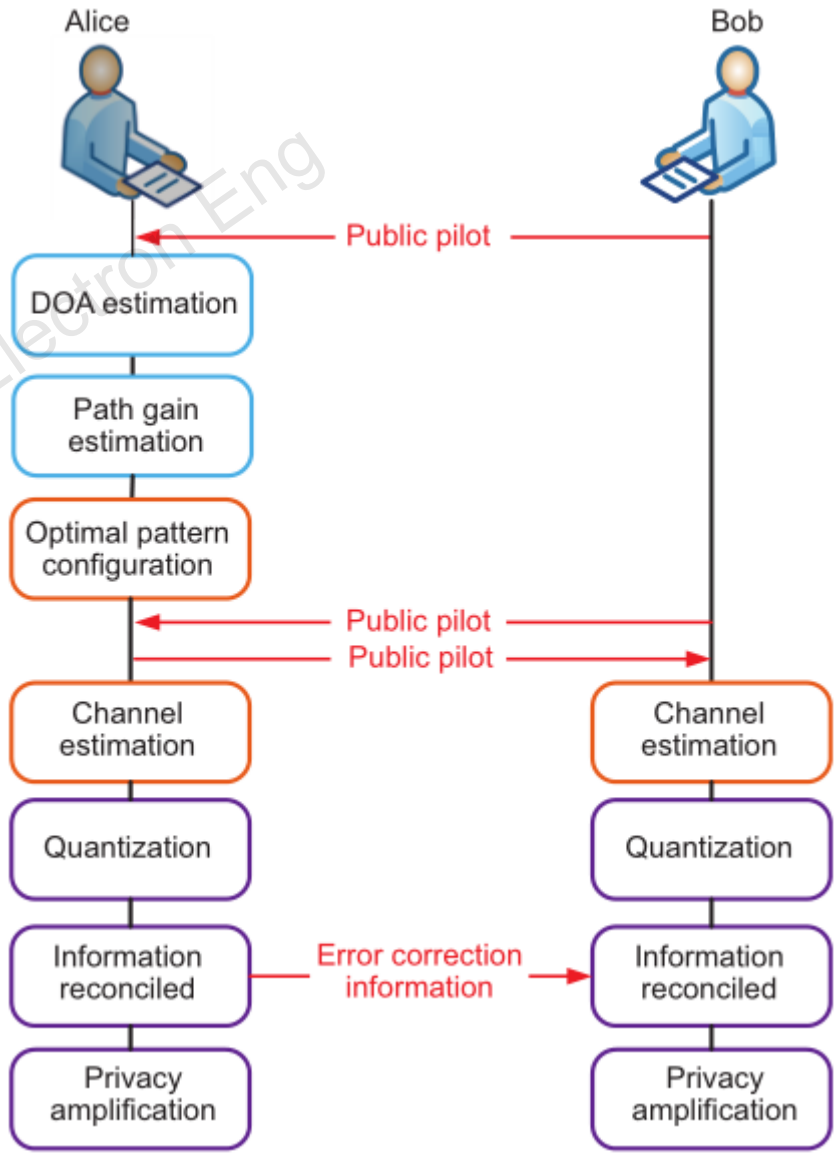
Method

The proposed PRA-based PKG scheme includes three main steps:

(1) the BS estimates the multipath channel parameters;

(2) the BS configures the optimal pattern to maximize the receiving SNR;

(3) the BS and the user generate secret keys from channel measurements.



Method

To address the discrete non-convex constraint effectively, we propose an improved BPSO algorithm to optimize $\boldsymbol{\Psi}$.

$$\begin{aligned}\boldsymbol{v}_i^{k+1} =& w\boldsymbol{v}_i^k + c_1 \cdot \mathrm{rand}_1^k \cdot \left(\mathbf{pBest}_i^k - \boldsymbol{x}_i^k\right) \\ &+ c_2 \cdot \mathrm{rand}_2^k \cdot \left(\mathbf{gBest}_i^k - \boldsymbol{x}_i^k\right),\end{aligned}$$

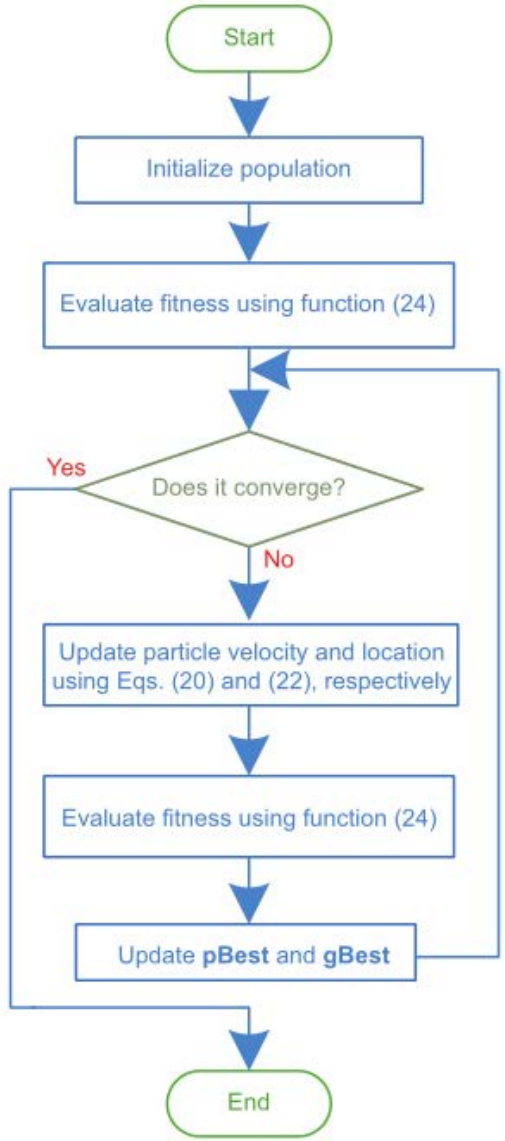
$$\mathrm{Sigmoid}\left(v_i(j)\right) = \frac{1}{1+\mathrm{e}^{-v_i(j)}}.$$

$$x_i^{k+1}(j) = \begin{cases} 1, & \mathrm{rand} < \mathrm{Sigmoid}\left(v_i^{k+1}(j)\right), \\ 0, & \mathrm{rand} \geq \mathrm{Sigmoid}\left(v_i^{k+1}(j)\right), \end{cases}$$

$$\bar{\boldsymbol{x}}_i^{k+1}(m) = \boldsymbol{x}_i^{k+1}(m:b\cdot m)\cdot\left[\pi/2^0, \pi/2, \cdots, \pi/2^{b-1}\right]^{\mathrm{T}},$$

$$\mathrm{fitness}\left(\bar{\boldsymbol{x}}_i^{k+1}\right) = \left|\mathrm{e}^{\mathrm{j}\bar{\boldsymbol{x}}_i^{k+1}} \boldsymbol{C}_n(\hat{\boldsymbol{\theta}})\hat{\boldsymbol{g}}\right|.$$

Through multiple iterations and evaluation of the fitness, the optimal patterns with the desired receiving performance can be conveniently and quickly obtained for b-bit coding elements.



Flowchart of the proposed improved binary particle swarm optimization algorithm

Conclusions

1. We proposed a novel RIS-based PRA architecture. PRA can optimize the antenna pattern in real time according to the multipath signal to change the way of the multipath superposition.
2. We proposed a novel PRA-based PKG protocol.
3. Simulation results showed that the proposed method can resist multipath fading and achieve a low key disagreement ratio (KDR).

Zheng WAN received his BS degree in communication engineering from Huazhong University of Science and Technology, Wuhan, China, in 2018. Currently, he is pursuing his Ph.D. degree at PLA Strategic Support Force Information Engineering University. His research interests include wireless communication security and smart and reconfigurable environment.

Kaizhi HUANG received her B.E. degree in digital communication and M.S. degree in communication and information system from PLA Strategic Support Force Information Engineering University, and Ph.D. degrees in communication and information system from Tsinghua University, Beijing, China, in 1995, 1998 and 2003 respectively. She has been a faculty member of NDSC since 1998, where she is currently a professor and director of Laboratory of Mobile Communication Networks. Her research interests include wireless network security and signal processing.