Secure wireless key distribution verified within a real outdoor environment

November 2 2015

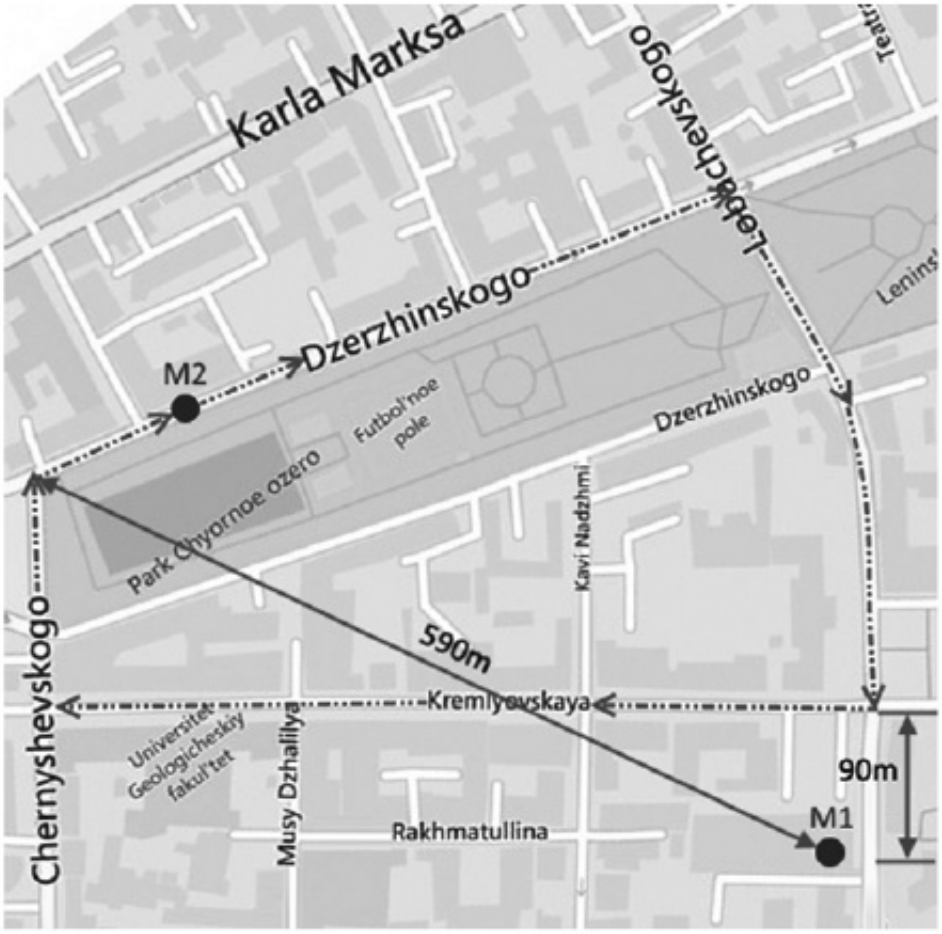

Figure 1: Moving route of mobile user.

A pair of identical transceiving test devices (M1 and M2) has been designed to implement the experimental verification. The M1 test device was placed at the 14th floor of our research facility at approximately 45 meters abovethe mean

roof height to serve as a base station. The M2 test device was placed into a car to be moved on the closed route within the surrounding urban environment.

As the most popular type of wireless systems, cellular communications carry high demand for confidentiality of traffic data of mobile subscribers. Wireless key distribution is one of the most promising and fast-growing areas in modern applied cryptography.

It covers various techniques of secure secret key distribution between two legitimate users who share a common radio channel with unpredictable signal fading in a multipath environment.

The experiments conducted by researchers of the Kazan Federal University Department of Radio Physics are the first experimental verification of secure wireless key distribution by observation of random variations of the carrier phase fluctuations of the received signal between two legitimate nodes with a common multipath channel placed into moving cars within a real outdoor environment.

According to the researchers, the measurements of signal carrier phase could be more appropriate for cryptographic applications because the approach has at least three valuable benefits:

Firstly, the probability distribution of carrier phase is usually closer to uniform as opposed to the distribution of the received signal strength indication (RSSI). Secondly, the RSSI-based method is mainly limited to a fixed link length communication scenario. Finally, the phase measurements have ambiguity, making key interception more complicated in practice.

To perform the experiment, researchers used wireless Internet

transmission of concurrent service data to maintain a required level of synchronization of one stationary and one mobile legal node. During the data collecting procedure, the nodes continued transmitting the sounding signals at the carrier frequency f = 963 MHz in a time-division duplex mode.

"The key generation rate about RK ~ 0.1 bits per second (bps) has been achieved at satisfactory statistical properties of the generated key, which sequence also satisfies the criteria of randomness. Despite the humble key generation rates achieved in practice, we believe in the great potential of the method for secure wireless key distribution between the base station and mobile subscriber in a cellular communications scenario.

"We succeeded in our goal, but a further wireless synchronization enhancement is required to achieve better system performance," says Prof. Arkadiy Karpov.

Provided by Kazan Federal University

Citation: Secure wireless key distribution verified within a real outdoor environment (2015, November 2) retrieved 18 May 2024 from https://phys.org/news/2015-11-wireless-key-real-outdoor-environment.html