ФИЗИЧЕСКИЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ТЕХНОЛОГИИ МОБИЛЬНОЙ СВЯЗИ 5G

Сальников Д.С.
Научный руководитель - д.т.н., проф. Цопа А.И.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки,14, каф. Радиотехнологий информационно-коммуникационных систем, тел.(057)7021444)
e-mail: dmytro.salnykov@nure.ua тел. 0999775180

The possible requirements and ways to build 5G. Attacks are considered the physical layer for unauthorized access to the mobile networks. The methods and techniques to address the availability of a new generation of mobile networks for vulnerabilities in complex with new security technologies.

С момента появления и до сегодняшнего дня сети мобильной связи прошли большой путь развития: появились новые способы передачи информации и более сложные пользовательские устройства -- смартфоны. Возможности, которые открывают мобильные технологии сегодня, уже давно вышли за рамки голосовых услуг, создавая новые способы общения, обмена данными и внедрение технологии «интернета вещей» (IoT).

Сети пятого поколения будут одновременно и похожи на любое предыдущее поколение мобильных сетей, и в тоже время заметно отличается от них, так как 5G строятся на базе основных 8 требований:

– скорость передачи данных до 10 Гб/с, что значительно превосходит скорости сетей 4G и 4.5G в 10-100 раз;
– задержки сигнала на уровне 1 миллисекунды;
– в 1000 раз больше пропускной способности на единицу площади;
– до 100 раз больше подключенных устройств на единицу площади;
– доступность сервиса 99.999%;
– покрытие 100%;
– снижение энергопотребления сетевых устройств на 90%;
– до 10 лет работы от батареи для устройств IoT;

Использование в высокоскоростных мобильных сетях нового поколения текущие беспроводные технологии (3G, 4G, WiFi, Bluetooth, Zigbee и т.д.) в связке с новыми технологиями и стандартами приведет к увеличению угроз информационной безопасности, как для обычных пользователей, так и для государственных и частных учреждений, ведь для злоумышленников откроются еще больше технических возможностей и путей для несанкционированного получения информации.

Перейдем непосредственно к рассмотрению информационной безопасности на физическом уровне (PHY) в текущих средствах связи с учетом внедрения новых технологий и рассмотрим возможные средства для их преодоления в концепции развития 5G.

Типы атак на физическом уровне делятся на два вида (рисунок 1):

1) активные: помехи; интерференция.
2) пассивные: прослушивание; анализ трафика.

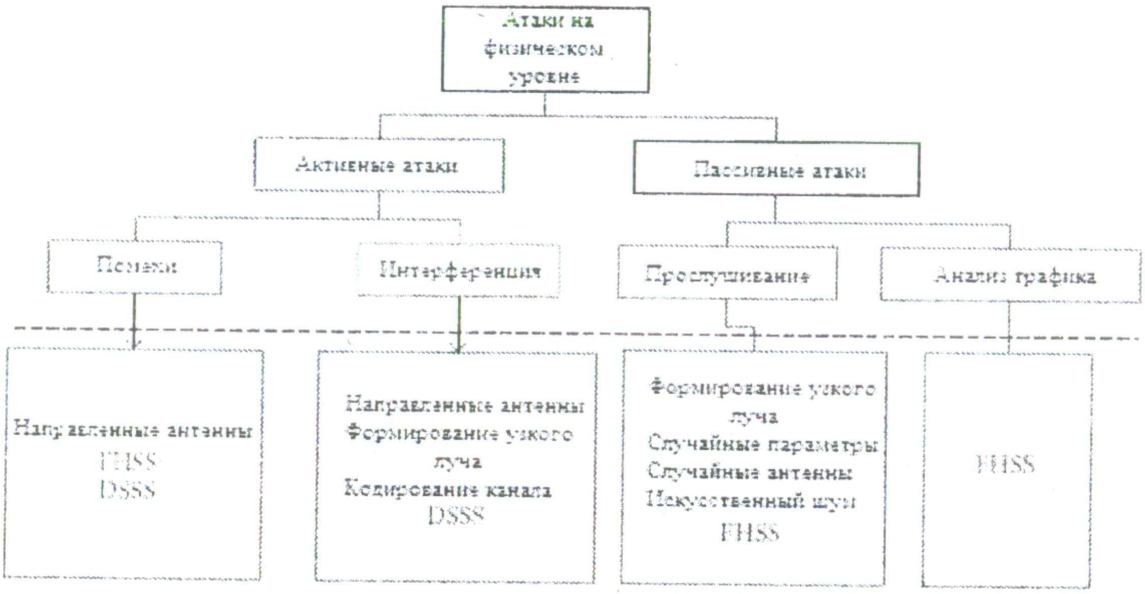

Рисунок 1 – Основные типы атак и средства защиты на PHY уровне

В докладе рассмотрены общие методы и средства для защиты от атак на физическом уровне:

– направленные антенны (Direction antenna) – это специальные антенны для обеспечения надежной связи в миллиметровом диапазоне волн;

– формирование узкого луча (Beamforming) – это технология обработки и формирования сигнала, которая позволяет поддерживать достаточно высокую скорость передачи изащиту от перехвата;

– псевдослучайное изменение рабочей частоты (FHSS) – согласно методу FHSS данные передаются только по одному каналу, но сам канал с частотой не более 20 мс изменяется псевдослучайным образом;

– расширение спектра методом прямой последовательности (DSSS) – один из основных методов модуляции сигнала, используемый в беспроводных локальных сетях;

– кодирование канала (Channel coding) помехоустойчивое кодирование/декодирование передаваемого сигнала;

– случайные параметры (Random Parameters), случайные антенны (Random Antennas) основаны на использовании весовых коэффициентов, которые скрывают истинные параметры канала и несущей частоты;

– искусственный шум (Artificial Noise) – этот метод опирается на добавление искусственного шума в общий канал передачи информации.

Применение рассмотренных выше методов может существенно повысить информационную безопасность беспроводных сетей 5G.

Список литературы

1. Weidong Fang, Fengrong Li, Yanzan Sun, Lianhai Shan, Shanji Chen, Chao Chen, and Meiju Li, «Information Security of PHY Layer in Wireless Networks». – Journal of Sensors, 2016, 10 p.