ОЦЕНКА ВОЗМОЖНОСТИ ПЕРЕХВАТА ИНФОРМАЦИИ В СИСТЕМАХ СВЯЗИ МИЛЛИМЕТРОВОГО ДИАПАЗОНА ВОЛН

Д.С. САЛЬНИКОВ, А.И. ЦОПА, д-р. техн. наук
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Науки,14, каф. Радиотехнологий информационно-коммуникационных систем, тел.(057)7021444
E-mail: dmytro.salnykov@nure.ua

Next generation wireless networks utilizing millimeter waves (mm-waves) achieve extremely high data rates using narrow signal beams. Featuring a high directivity and being susceptible to blockage by objects, mm-waves are often assumed to be hard to intercept. In this report, we practically demonstrate the vast impact that inconspicuous objects might have on mm-wave security.

Беспроводные системы связи следующего поколения *5G*, использующие миллиметровые волны (ММ ДВ), обеспечивают чрезвычайно высокие скорости передачи информации с использованием узких сигнальных лучей. Обладая высокой направленностью и будучи восприимчивыми к блокировке объектами окружающей среды, каналы ММ ДВ часто считаются трудными для перехвата нарушителем [1].

Однако мелкомасштабные объекты внутри основного луча канала распространения вызывают отражения, что позволяет устройствам перехвата получать сигнал вне основного луча. В работе [2] экспериментально показано, что даже небольшие по площади отражатели позволяют принимать сигналы ММ ДВ нарушителем. Современные коммуникационные устройства с металлическими поверхностями, такие как мобильные телефоны или ноутбуки, могут также вызывать достаточное отражение сигнала, что может создавать угрозу для перехвата информации.

Для прогнозирования защищенности беспроводных систем передачи информации на физическом уровне в настоящее время широко используется концепция отводного канала (ОК).

Цель работы: оценка возможности перехват информации в системах связи миллиметрового диапазона.

При разработке критериев оценки угроз для беспроводных систем передачи информации на физическом уровне модели *OSI* необходимо учитывать особенности распространения радиоволн и эффектов, возникающих в реальных условиях работы канала связи.

К числу главных преимуществ применения ММ ДВ в системах связи следует отнести прежде всего такие факторы как увеличение объема и скорости передачи информации, высокое усиление антенн при малой их апертуре и повышенная помехозащищенность канала связи, возможность организации локальных широкополосных систем передачи данных, применение остронаправленных антенн и особенность распространения волн ММ-диапазона.

Характерной чертой любого радиосигнала является уменьшение уровня сигнала при распространении за счет ослабления в свободном пространстве, потерь в газах атмосферы и некоторых других видов дополнительных потерь. Особенность использования ММ ДВ для радиосвязи (наземной, спутниковой) состоит в том, что при их распространении радиоизлучение затухает в атмосферных газах и гидрометеорах .

Сигналы ММ ДВ имеет довольно большое затухание в свободном пространстве и для обеспечения эффективной работы системы связи необходимо использовать высоконаправленные антенные системы, обладающие большим усилением и узкой диаграммой направленности. Например, рупорные антенны могут иметь ширину основного луча в пределах (5-15)◦. Стандарт связи *IEEE 802.11ad* описывает алгоритм формирования луча с антенными решетками для достижения ширины луча 3◦.

Системная модель беспроводной системы связи ММ ДВ, представленная на рис.1, включает в себя канал передачи информации от передатчика Алисы до получателя информации приемника Боба, который называется основным, или легитимным каналом связи *(main channel)*. Алиса передает сигналы Бобу и для повышения защищенности канала использует узкую диаграмму направленности. Мы предполагаем, что обе антенны Алисы и Боба идеально выровнены и передают сигналы в оптимальном направлении.

Нарушитель Ева нацелена на перехват сигналов, которые Алиса посылает Бобу, не мешая ей. Она действует пассивно и только слушает сигналы и пытается принять отраженные сигналы от объектов расположенных в сигнальном луче. Для удобства анализа мы предполагаем, что Ева использует те же аппаратные средства, что и Алиса и Боб. Канал отвода от передатчика легитимного канала к приемнику незаконного потребителя (нарушителя) является отводным каналом ОК *(wiretap channel)*.

Исходя из системной модели, можно выделить три возможных варианта поведения нарушителя при атаке на канал связи:

– перемещение манипулятора объекта и помещение различных объектов в сигнальный луч, чтобы вызвать отражение сигнала к фиксированной позиции перехвата;

– перемещение самого нарушителя и использование отражения от существующих объектов в среде распространения, которую он не может изменить;

– стационарное положение нарушителя, который не может ни двигаться, ни манипулировать объектами окружающей среды и только попытается перехватить сигнал.

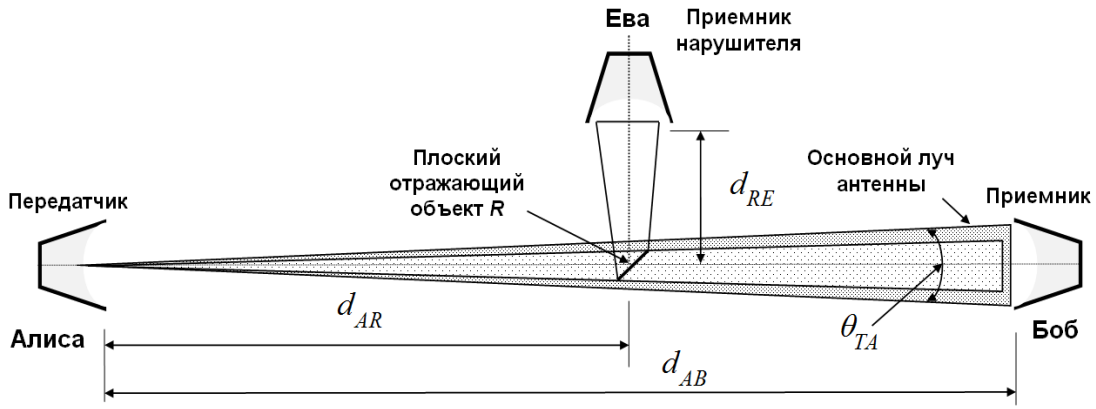

Рис. 1. Системная модель угроз канала связи ММ ДВ

Манипулирование объектом. Эта модель атаки предполагает, что нарушитель Ева находится в фиксированном положении вне основного сигнального луча и непосредственно оттуда невозможно принять сигнал. Однако Ева помещает произвольные объекты в окружающей среде, чтобы вызвать отклонение сигнала в нужную ей сторону. Она может управлять своей антенной по направлению к этому объекту, чтобы оптимально получать сигналы передаваемого сигнала и стремится получить достаточное качество сигнала для декодирования информации. В то же время Ева пытается оставаться невидимой для Алисы и Боба, вызывая лишь незначительную блокировку прямой передачи сигнала.

Одной из метрик оценки защищенности канала связи на физическом уровне является секретная производительность C_S изображенная на рис.2, которая определяется как максимальная разность между скоростью передачи информации в легитимном C_{AB} и отводном C_{AE}, ее можно записать соответствующие выражения для производительности основного канала C_{AB}, отводного канала C_{AE} и секретной производительности C_S :

$$C_S = C_{AB} - C_{AE} = W \log_2 \left\{ \frac{\left[1 + \frac{P_{TA} \cdot G_{TA} \cdot G_{RB}}{W \cdot k \cdot T} \left(\frac{\lambda}{4\pi} \right)^2 \cdot \left(\frac{1}{d_{AB}} \right)^n \right]}{\left[1 + \frac{P_{TA} \cdot G_{TA} \cdot G_{RE}}{W \cdot k \cdot T} \left(\frac{\lambda}{4\pi} \right)^2 \cdot \left(\frac{1}{d_{AE}} \right)^n \right]} \right\}$$

где: G_{RB} – коэффициент усиления приемной антенны Боба; d_{AB} – расстояние между передающей антенной Алисы и приемной антенной Боба, *м*; G_{RE} – коэффициент усиления приемной антенны Евы; d_{AE} – расстояние между передающей антенной Алисы и приемной антенной Евы, *м*.

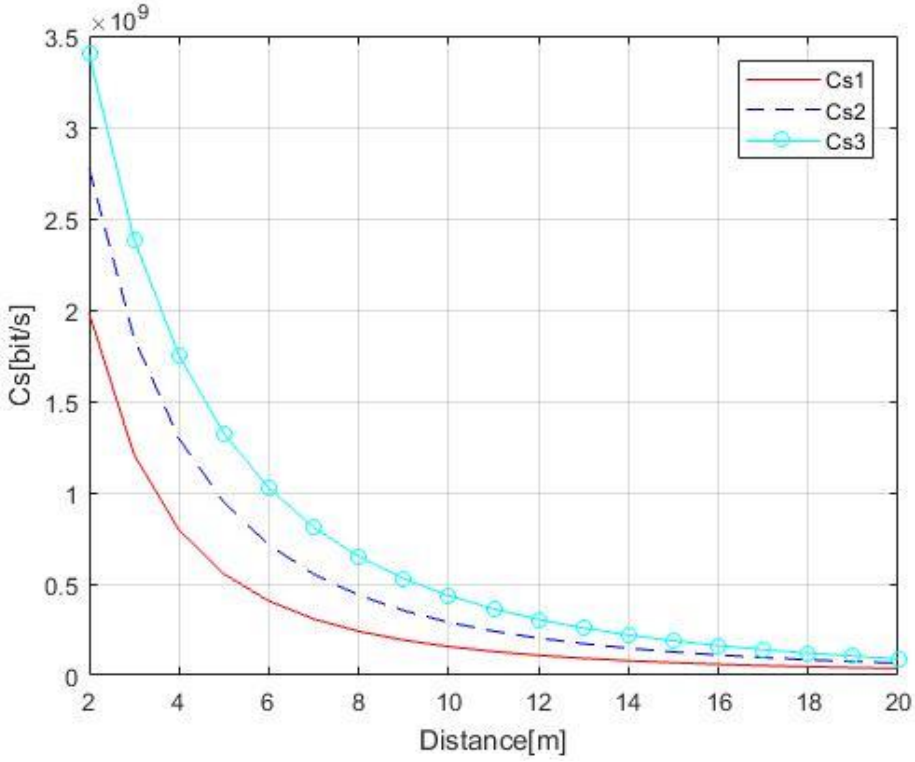

Рис.2.Зависимость секретной производительности C_S от расстояния

На данном рисунке показана зависимость секретной производительности C_S от расстояния, при изменяющихся параметрах: P_A (мощность передатчика Алисы) – 30,*60,100*; *mBm*; G_{RE} (коэффициент усиления приемной антенны Евы) – 24.8, 27, 29 дБ; d_{AB} – расстояние между антеннами Алисы и Боба, в пределах от 2 до 20,м и фиксированным расстоянием до Евы 100м.

В работе рассмотрен один из методов для оценки параметров защищенности систем передачи информации на физическом уровне модели взаимодействия систем связи *OSI*.

Список литературы

1. *Nitsche T., Cordeiro C., Flores A. B., Knightly E. W., Perahia E. and Widmer J. C.* IEEE 802.11ad: directional 60 GHz communication for multi-Gigabit-per-second Wi-Fi. // IEEE Communications Magazine. – 2014. – vol. 52, № 12, – pp. 132–141.

2. *Liu R. and Trappe W.* Securing Wireless Communications at the Physical Layer. // New York: Springer, 2010.