МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ульяновский государственный технический университет»

Защита беспилотных летательных аппаратов от спуфинг атак

Студент бакалавриата, направления - «Инфокоммуникационные технологии и системы связи»
Прокопьев Т.В.

Кафедра «Телекоммуникации»

Научный руководитель - профессор Гладких А.А.

Ульяновск – 2018

Сирия. Январь 2018.Атака БПЛА

Рисунок 1

Цель работы: Проведение анализа существующих методов захвата беспилотных летательных аппаратов с помощью спуфинг атак.

Задачи исследования:

1. Рассмотреть стратегии откровенного и скрытого спуфинга, отличающиеся попытками спуфера, избежания обнаружения целевого GPS-приемника и целевой навигационной системы оценщика.

2. Выявить необходимые условия для захвата БПЛА с помощью спуфинга.

3. Проанализировать взаимосвязанную динамику БПЛА и спуфера, и имитации для изучения практических сценариев контроля после захвата.

4. Внедрение метода перестановочного декодирования в систему управления БПЛА.

Общее описание спуфинг атаки

Спуфинг (от англ. spoofing — подмена, мистификация) – это атака, которая пытается обмануть GPS-приемник, широковещательно передавая немного более мощный сигнал, чем полученный от спутников GPS, такой, чтобы быть похожим на ряд нормальных сигналов GPS.

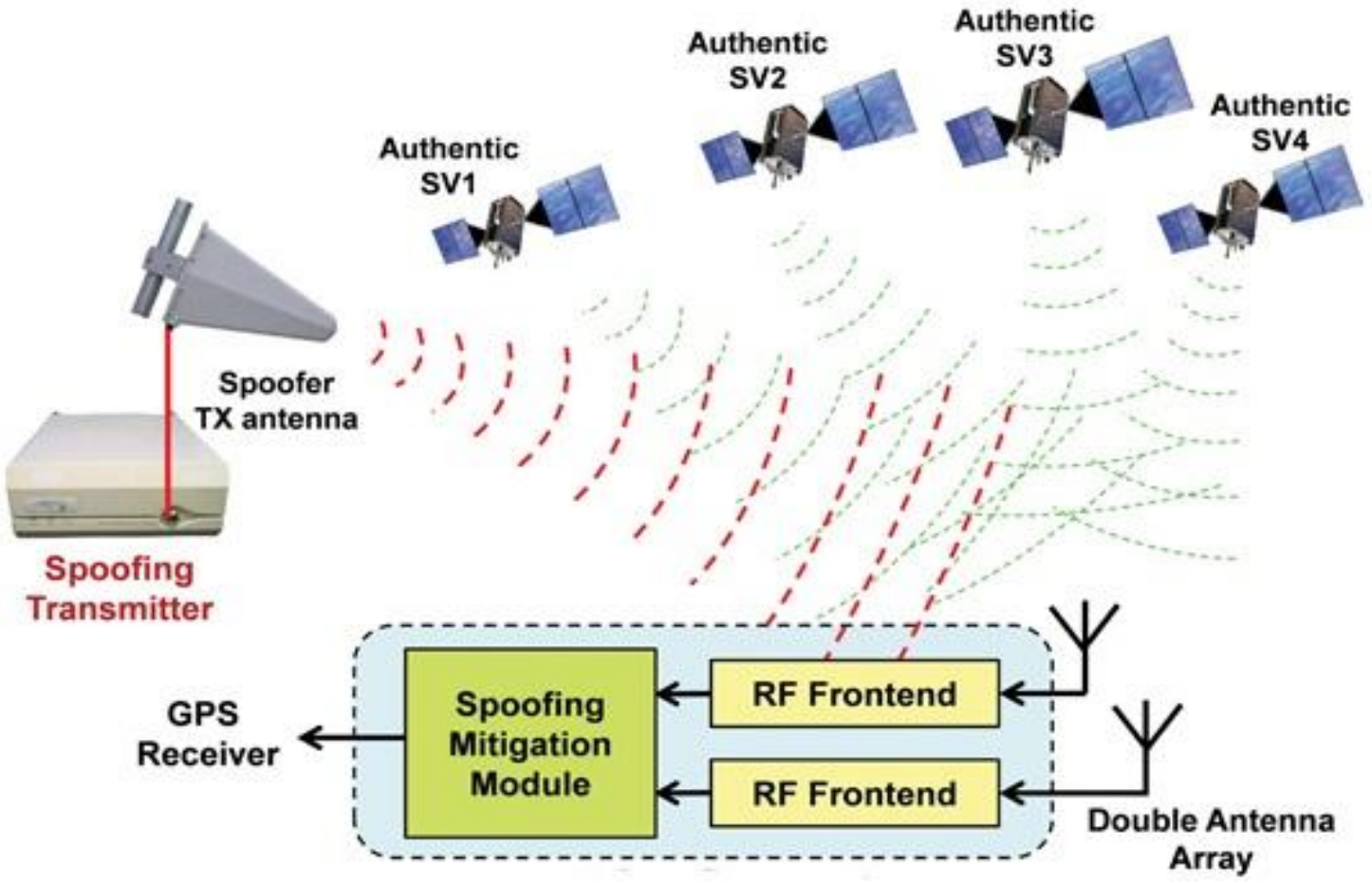


Рисунок 2

Процесс захвата БПЛА

Красные точки – точки отслеживания, которые пытаются удерживать себя центрированными на этом пике.

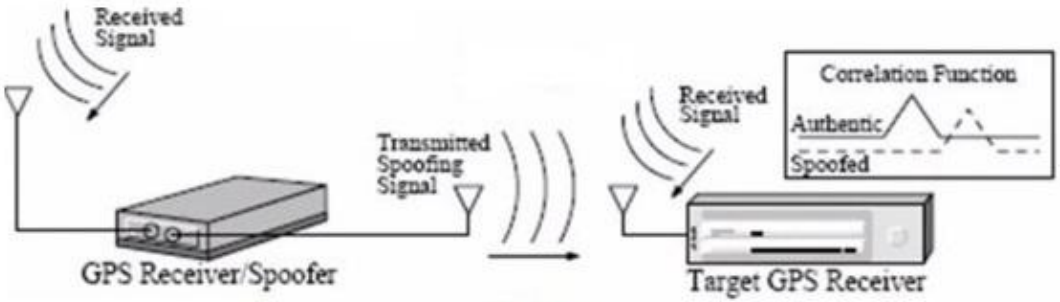
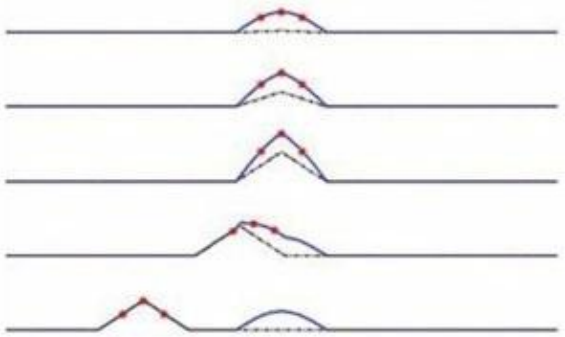


Рисунок 3



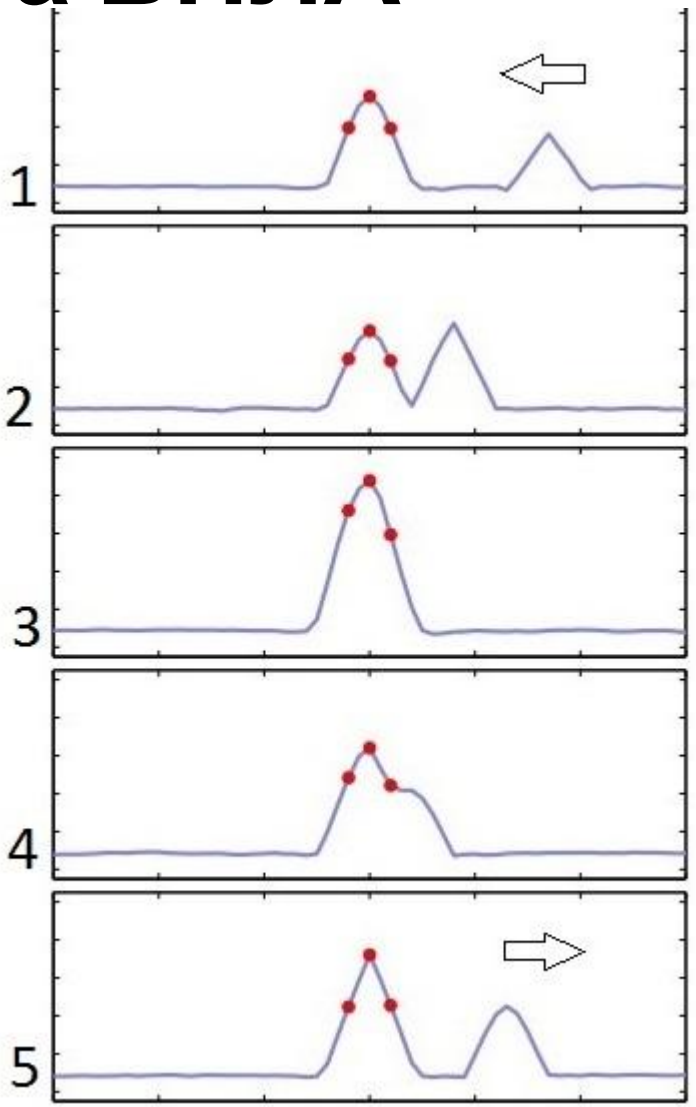
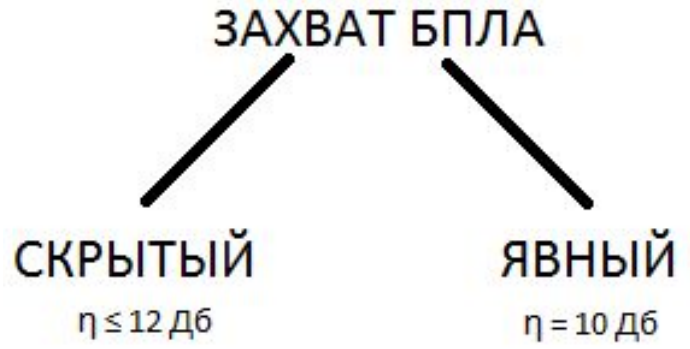


Рисунок 4

Классификация захватов

- Захват навигационной системы подразумевает, что spoofer получил контроль над достаточным количество целевых GPS-приемников активных кодов и отслеживает БПЛА.

- Основным «оружием» спуфера стал имитатор GPS-сигналов и усилители

- 

$$\eta = \frac{Пс}{Па}$$

Пс - мощность спуфинг сигнала

Па - мощность подлинного сигнала

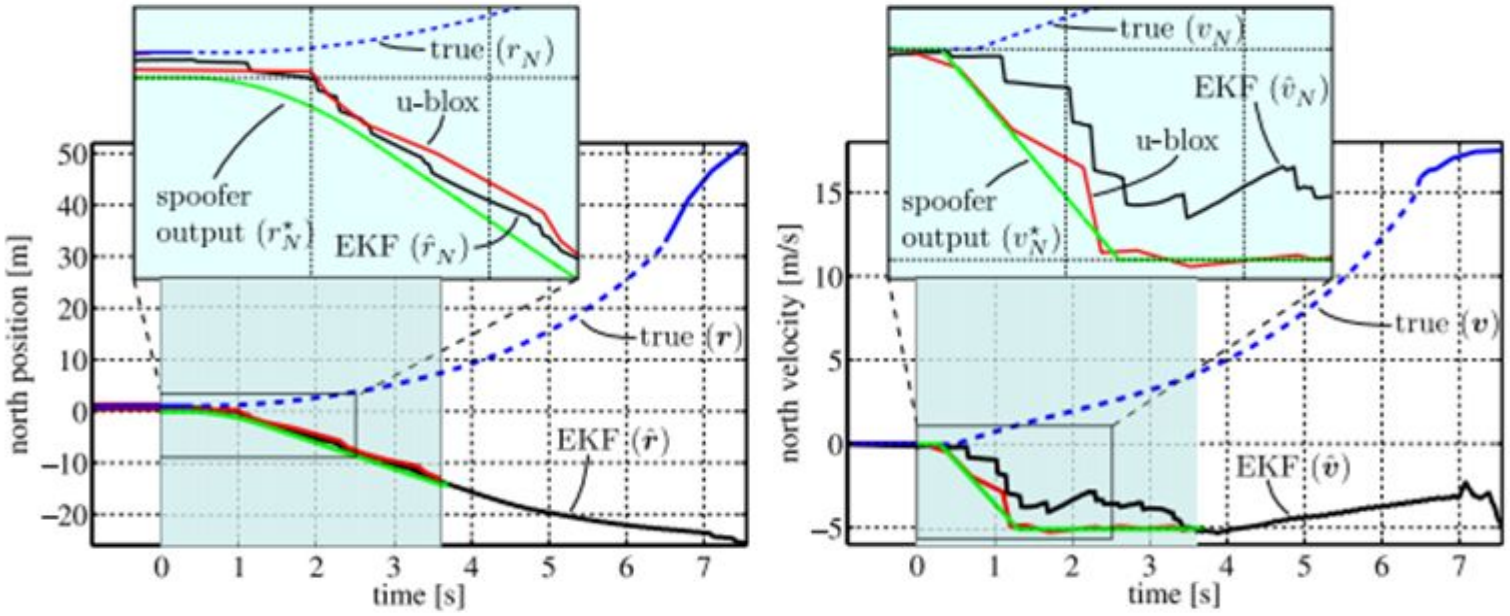
Захват оценщика навигационного состояния

η (dB)	Maximum velocity offset [m/s]		
	Javad Delta	Trimble Juno SB	ublox Lea-6N
1	10	10	10
2	10	10	15
3	15	10	15

Результаты тестов спуфинг атак против различных коммерческих GPS-приемников(скорость смещения 10 м/с соответствует смещению Доплера 53 Гц и смещение 15 м/с соответствует 79 Гц)

Управление после захвата БПЛА

- Цель управления спуфера - заставить БПЛА отслеживать некоторые исходные положения, скорость и траекторию перемещения.



Оператор немедленно приказывает БПЛА ускориться на юг. Однако, он не имеет достаточного контроля, чтобы остановить последствиями спуфинг атаки.

Проблемы возникающие при захвате

1. Тенезация антенны
2. Расположение антенны

Рисунок 6

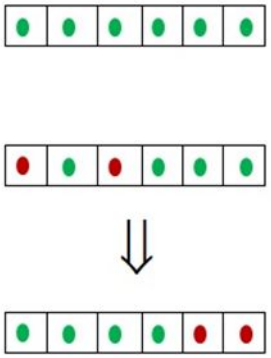
Алгебраическая основа формирования эквивалентных кодов

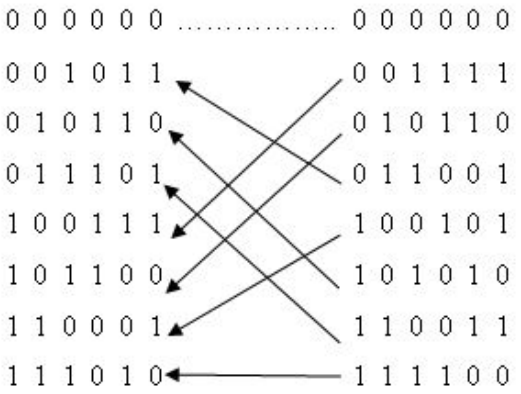
В теории групп под перестановкой произвольного множества подразумевается биекция этого множества на себя. Пусть $S_{k\times k}$ - невырожденная матрица , а векторы V_i и V_j длины k. В этом случае $V_iS \oplus V_jS = (V_i \oplus V_j)S$ - вектор кода. Если $(V_i \oplus V_j)S = 0$, при условии $(V_i \oplus V_j) \neq 0$.

Если $V_i \neq V_j$, то $V_iS \neq V_jS$, тогда все строчки матрица M^TS - различны

$M_{k\times(q^k-1)}$ - матрица модулярного представления кода $M^TS = RM^T$, где R - матрица перестановок

Пример:





Весовой спектр двоичных кодов одинаков

Питерсон У., Уэлдон Э. Коды, исправляющие ошибки, пер. с англ.; под ред. Р. Л. Добрушина и С. Н. Самойленко. – М. : Мир, 1976. – 594 с.
Морелос-Сарогосса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение.– М.: Техносфера, 2005.– 320 с.

Теорема 1. *Л*юбая циклическая перестановка столбцов порождающей матрицы исходного кода $G_{исх}$ при оценке произвольной матрицы $Q_{k\times k}$, образованной случайным образом из столбцов матрицы $G_{исх}$ приводит к $\Delta \neq 0$ и тождеству $G_s^{'} \equiv G$.

Доказательство. Поскольку столбцы матрицы $G_{исх}$ линейно независимы, то любой их циклический сдвиг обеспечивает невырожденность матрицы $Q_{k\times k}$ и приведение переставленной матрицы $G^{'}$ в несистематической форме к матрице $G_s^{'} \equiv G$.

$$G_{исх} \Longrightarrow G_{пер} \Longrightarrow G_{пер}^{сис}$$

$$G_{исх} = \begin{Vmatrix} \alpha^0 & 0 & 0 & \alpha^4 & \alpha^0 & \alpha^4 & \alpha^5 \\ 0 & \alpha^0 & 0 & \alpha^2 & \alpha^0 & \alpha^6 & \alpha^6 \\ 0 & 0 & \alpha^0 & \alpha^3 & \alpha^0 & \alpha^1 & \alpha^3 \end{Vmatrix}$$

$$G_{\substack{пер \\ 4567123}} = \begin{Vmatrix} \alpha^4 & \alpha^0 & \alpha^4 & \alpha^5 & \alpha^0 & 0 & 0 \\ \alpha^2 & \alpha^0 & \alpha^6 & \alpha^6 & 0 & \alpha^0 & 0 \\ \alpha^3 & \alpha^0 & \alpha^1 & \alpha^3 & 0 & 0 & \alpha^0 \end{Vmatrix} \Longrightarrow G_{\substack{сис \\ 4567123}} = \begin{Vmatrix} \alpha^0 & 0 & 0 & \alpha^4 & \alpha^0 & \alpha^4 & \alpha^5 \\ 0 & \alpha^0 & 0 & \alpha^2 & \alpha^0 & \alpha^6 & \alpha^6 \\ 0 & 0 & \alpha^0 & \alpha^3 & \alpha^0 & \alpha^1 & \alpha^3 \end{Vmatrix}$$

$$Q_{k\times k} = \begin{Vmatrix} \alpha^4 & \alpha^0 & \alpha^4 \\ \alpha^2 & \alpha^0 & \alpha^6 \\ \alpha^3 & \alpha^0 & \alpha^1 \end{Vmatrix} \qquad \Delta Q = \alpha^5 \qquad Q_{норм} = \begin{Vmatrix} \alpha^5 & \alpha^5 & \alpha^5 \\ \alpha^2 & \alpha^4 & \alpha^6 \\ \alpha^3 & \alpha^4 & \alpha^1 \end{Vmatrix} = Q^* \qquad \left(Q_{норм}\right)^T = \begin{Vmatrix} \alpha^5 & \alpha^2 & \alpha^3 \\ \alpha^5 & \alpha^4 & \alpha^4 \\ \alpha^5 & \alpha^6 & \alpha^1 \end{Vmatrix} = \left(Q^*\right)^T$$

$$Q^{-1} = \frac{1}{\Delta Q} * \left(\left(Q_{норм}\right)^T\right) = \begin{Vmatrix} \alpha^0 & \alpha^4 & \alpha^5 \\ \alpha^0 & \alpha^6 & \alpha^6 \\ \alpha^0 & \alpha^1 & \alpha^3 \end{Vmatrix} \qquad Q \cdot Q^{-1} = E$$

$$Q^{-1} \cdot G_{\substack{пер \\ 4567123}} = G_{сис} \qquad \begin{Vmatrix} \alpha^0 & \alpha^4 & \alpha^5 \\ \alpha^0 & \alpha^6 & \alpha^6 \\ \alpha^0 & \alpha^1 & \alpha^3 \end{Vmatrix} \times \begin{Vmatrix} \alpha^4 & \alpha^0 & \alpha^4 & \alpha^5 & \alpha^0 & 0 & 0 \\ \alpha^2 & \alpha^0 & \alpha^6 & \alpha^6 & 0 & \alpha^0 & 0 \\ \alpha^3 & \alpha^0 & \alpha^1 & \alpha^3 & 0 & 0 & \alpha^0 \end{Vmatrix} = G_{\substack{сис \\ 4567123}} = \begin{Vmatrix} \alpha^0 & 0 & 0 & \alpha^4 & \alpha^0 & \alpha^4 & \alpha^5 \\ 0 & \alpha^0 & 0 & \alpha^2 & \alpha^0 & \alpha^6 & \alpha^6 \\ 0 & 0 & \alpha^0 & \alpha^3 & \alpha^0 & \alpha^1 & \alpha^3 \end{Vmatrix}$$

Гладких А.А., Ал Тамими Т.Ф.Х. Структура быстрых матричных преобразований в процедуре формирования эквивалентных избыточных кодов // Радиотехника. – 2017. – № 6 С.41—44.

Шахтанов С.В. Перестановочное декодирование недвоичных избыточных кодов // Вестник НГИЭИ. – 2017. – № 8()75. – С. 7 – 14.

Выводы

1. Развитие беспроводных сенсорных сетей требует предвидения спуфинг атак и разработку методов противодействия таким акциям.
2. В качестве методов борьбы с акциями спуфинга следует рассматривать системы криптографии, которые экономически невыгодны на таких устройствах.
3. Применение средств помехоустойчивости кодирования с использованием управляемых перестановок, позволяющих на коротком отрезке времени осуществлять маскировку истинной структуры сигнала.

СПАСИБО ЗА ВНИМАНИЕ!