

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.

Сирия. Январь 2018. Атака БПЛА



Рисунок 1

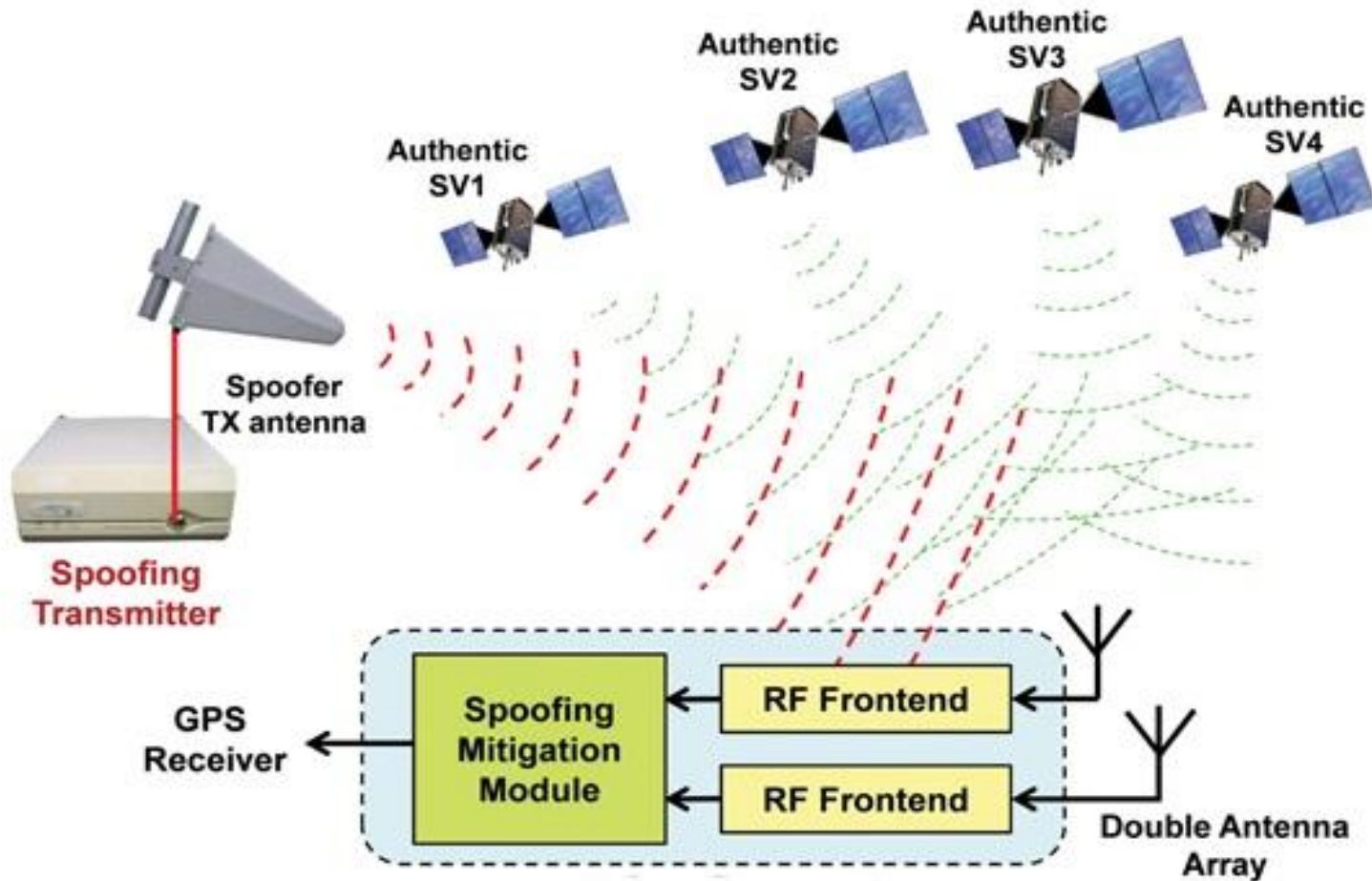
Цель работы: Проведение анализа существующих методов захвата беспилотных летательных аппаратов с помощью спуфинг атак.

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

Процесс захвата БПЛА

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

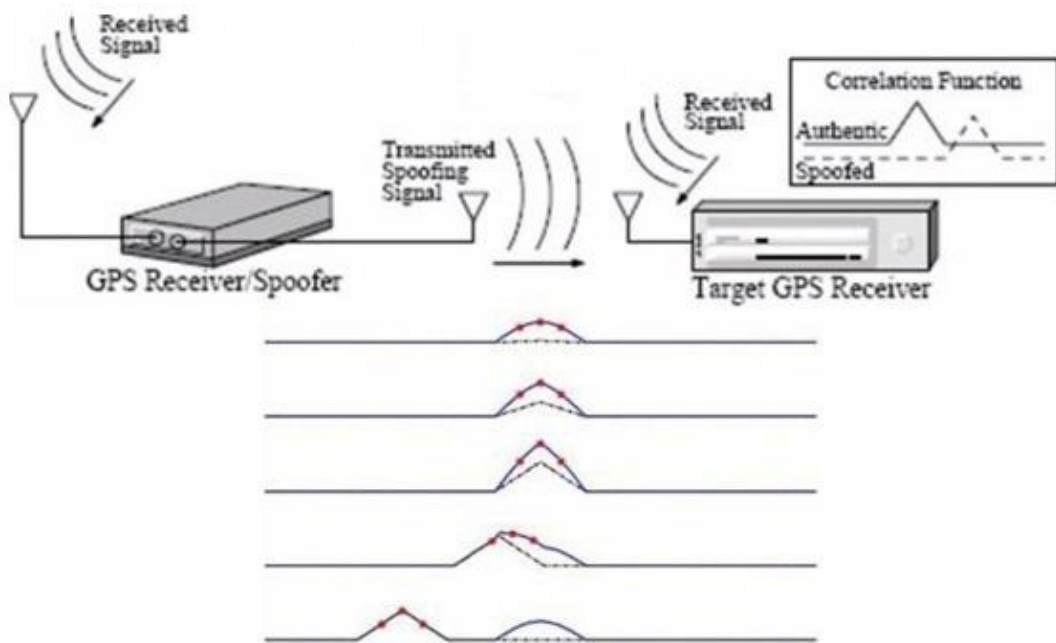


Рисунок 3

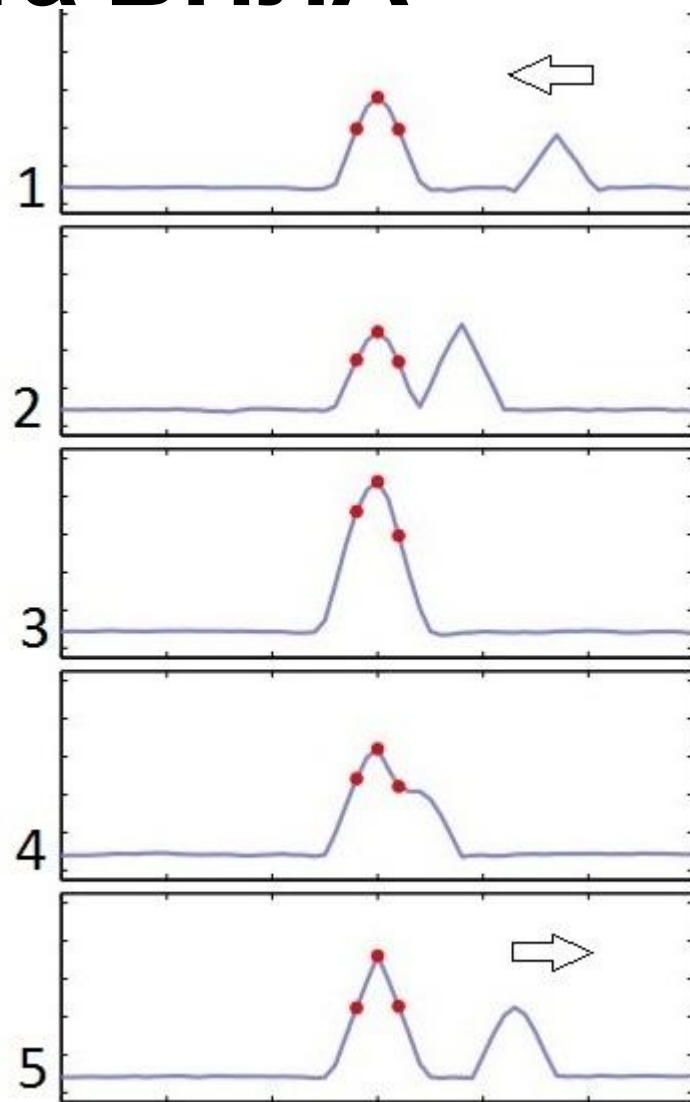


Рисунок 4

Классификация захватов

- Захват навигационной системы подразумевает, что spoofer получил контроль над достаточным количеством целевых GPS-приемников активных кодов и отслеживает БПЛА.
- Основным «оружием» спуфера стал имитатор GPS-сигналов и усилители



$$\eta = \frac{P_c}{P_a}$$

P_c - мощность спуфинг сигнала

P_a - 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.

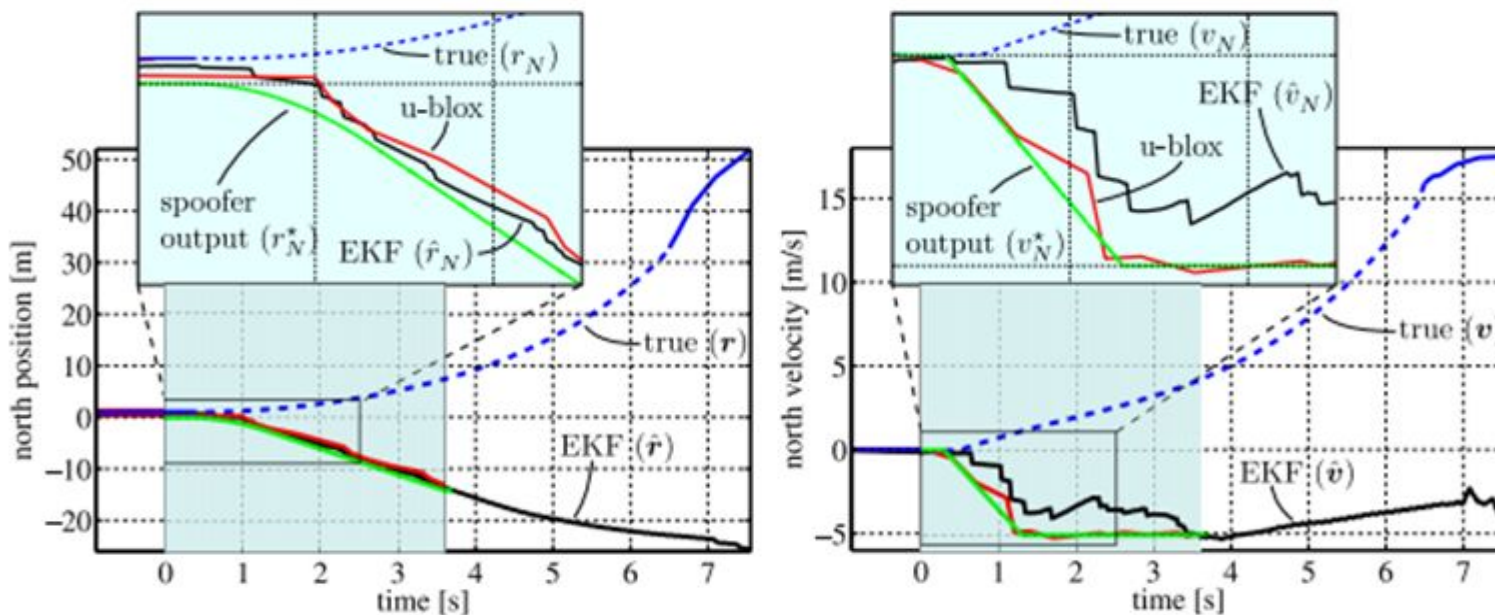


Рисунок 3

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

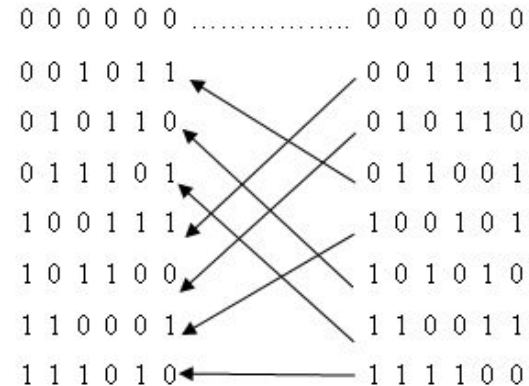
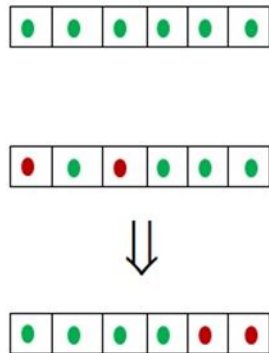
Алгебраическая основа формирования эквивалентных кодов

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 $V_i S \oplus V_j S = (V_i \oplus V_j) S$ - 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 $V_i S \neq V_j S$, тогда все строки матрица $M^T S$ - различны

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

Пример:



Весовой спектр двоичных кодов одинаков

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

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

$$\begin{aligned}
 & G_{ucx} \implies G_{nep} \implies G_{nep}^{cuc} \\
 & G_{ucx} = \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_{nep} = \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} \implies G_{nep}^{cuc} = \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} \quad \Delta Q = \alpha^5 \quad Q_{norm} = \begin{vmatrix} \alpha^5 & \alpha^5 & \alpha^5 \\ \alpha^2 & \alpha^4 & \alpha^6 \\ \alpha^3 & \alpha^4 & \alpha^1 \end{vmatrix} = Q^* \quad (Q_{norm})^T = \begin{vmatrix} \alpha^5 & \alpha^2 & \alpha^3 \\ \alpha^5 & \alpha^4 & \alpha^4 \\ \alpha^5 & \alpha^6 & \alpha^1 \end{vmatrix} = (Q^*)^T \\
 & Q^{-1} = \frac{1}{\Delta Q} * ((Q_{norm})^T) = \begin{vmatrix} \alpha^0 & \alpha^4 & \alpha^5 \\ \alpha^0 & \alpha^6 & \alpha^6 \\ \alpha^0 & \alpha^1 & \alpha^3 \end{vmatrix} \quad Q \cdot Q^{-1} = E \\
 & Q^{-1} \cdot G_{nep} = G_{nep}^{cuc} \quad \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_{nep}^{cuc} = \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}
 \end{aligned}$$

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!