показатель успеха деанонимизации: чем выше F1, тем лучше нарушитель восстанавливает структуру CPP. Проверки выполнены для сценариев: «без анонимизации» (F1=1,0), ротация адресов (F1=0,23), метод CoinJoin (F1=0,22), stealth-выходы (F1=0,21). Разработанный метод достигает значения F1=0,17 благодаря сочетанию криптографической несвязываемости выходов и снижению мультивходовости через UTXO shaping, ослабляющему эвристику общего входа. При этом средний размер транзакции (369 байт) ниже, чем у stealth-выходов за счет уменьшения числа входов.

Исследование выполнено за счет гранта Российского научного фонда №24-11-20005, https://rscf.ru/project/24-11-20005/, гранта Санкт-Петербургского научного фонда (договор №24-11-20005 о предоставлении регионального гранта).

Список использованных источников

1.Stütz R. Adoption and actual privacy of decentralized coinjoin implementations in bitcoin // Proceedings of the 4th ACM Conference on Advances in Financial Technologies. – 2022. – P. 254-267.

2.Ruffing T., Moreno-Sanchez P., Kate A. Coinshuffle: Practical decentralized coin mixing for bitcoin //European symposium on research in computer security. – Springer, 2014. – P. 345-364.

3.Sasson E.B. Zerocash: Decentralized anonymous payments from bitcoin //IEEE symposium on security and privacy. – 2014. – P. 459-474.

4.Van Saberhagen N. CryptoNote v.2.0. – 2013.

5.Herskind L., Katsikouli P., Dragoni N. Privacy and cryptocurrencies. A systematic literature review // IEEE Access. – 2020. – Т. 8. – P. 54044-54059.

6. Nguyen-Dinh T. A hierarchical deterministic wallet using Ed25519 digital signature scheme // International Conference on Future Data and Security Engineering. – 2022. – P. 240-257.

Охлопков Никита Михайлович, студ., техник Высшей школы кибербезопасности ИКНК, СПбПУ, ohlopkov_nm@spbstu.ru.
Калинин Максим Олегович, д.т.н., профессор Высшей школы кибербезопасности ИКНК, СПбПУ, max@ibks.spbstu.ru.

УДК 004.056 ; 621.391

ОЦЕНКА НАРУШЕНИЯ СЕКРЕТНОСТИ ПЕРЕДАЧИ ДАННЫХ В РЭЛЕЕВСКОМ КАНАЛЕ

А.А. Тарасенко[1], Е.В. Прокопенко[2]
[1]филиал КузГТУ, г. Новокузнецк,
[2]Кузбасский государственный технический университет имени Т.Ф. Горбачева,г.Кемерово

Ключевые слова: передача данных; пассивный перехват; рэлеевское замирание; вероятность нарушения секретности; нейронная сеть.

Введение

В беспроводных каналах сигнал замирает. Канал может слушать пассивный перехватчик. Поэтому одной криптографии иногда недостаточно. Помогает защита на физическом уровне. Она использует разницу условий распространения к приемнику и к перехватчику. Системе нужна быстрая оценка риска. Она помогает выбирать скорость, кодирование и мощность [1-3].

Рассмотрим канал с пассивным перехватом. Передатчик A посылает сигнал x. Его принимает легитимный приемник B. Его же наблюдает перехватчик E. Коэффициенты канала - h_b и h_e. Шум - n_b и n_e. Тогда:

$$y_b = \sqrt{P}\, h_b\, x + n_b;\;\; y_e = \sqrt{P}\, h_e\, x + n_e$$

Сигнал x считают комплексным. Выполняют нормировку $E\{|x|^2\}=1$. Шумы n_b и n_e моделируются как комплексные гауссовы с дисперсией N_0 на комплексный отсчет. Введем отношение сигнал/шум (ОСШ) на B и E. При мощности передачи P получаем:

$$\gamma_b = (P\cdot|h_b|^2)/N_0,\;\; \gamma_e = (P\cdot|h_e|^2)/N_0$$

Пусть замирание — рэлеевское. Тогда коэффициенты h_b и h_e — комплексные гауссовы с нулевым средним. Величины $|h_b|^2$ и $|h_e|^2$ имеют экспоненциальное распределение. Следовательно, γ_b и γ_e также экспоненциальны. Их средние значения обозначим $\bar{\gamma}_b$ и $\bar{\gamma}_e$.

Емкости каналов для B и E:

$$C_b = \log_2(1+\gamma_b),\;\; C_e = \log_2(1+\gamma_e)$$

Секретная пропускная способность:

$$C_s = [C_b - C_e]+ = \max\{\, \log_2(1+\gamma_b) - \log_2(1+\gamma_e),\, 0\,\}$$

Зададим целевую секретную скорость R_s. Тогда риск - это вероятность нарушения секретности:

$$P_{out}(R_s) = \Pr\{\, C_s < R_s \,\}$$

$P_{out}(R_s)$ можно посчитать двумя способами.

Первый - интегрирование по распределению ОСШ перехватчика. Второй - оценка методом Монте-Карло. Для N реализаций:

$$P_{out}(R_s) = \int_0^\infty F_{\gamma_b}(2R_s(1+\gamma_e)-1)\, f_{\gamma_e}(\gamma_e)\, d\gamma_e =$$
$$= 1 - (\bar{\gamma}_b/(\,\bar{\gamma}_b + 2R_s\bar{\gamma}_e\,))\, \exp(-(2R_s-1)/\bar{\gamma}_b) \approx$$
$$\approx (1/N)\sum_{i=1}^{N} I\{\, C_s(i) < R_s \,\}$$

Интегрирование и Монте-Карло работают медленно, когда запросов много. Замкнутая формула существует для независимых рэлеевских каналов. Однако при усложнении модели (корреляция, помехи, неоднородность) она исчезает. Поэтому используют замещающую модель на нейронной сети. Сначала готовят выборку. Она связывает ($\bar{\gamma}_b$, $\bar{\gamma}_e$, R_s) и P_{out}. Значения P_{out} получают моделированием. Потом, в реальном времени,

сеть быстро оценивает P_{out} по этим параметрам. Так система быстрее выбирает режим передачи.

Для адаптации удобно использовать дискретный набор режимов модуляции и кодирования. Каждый режим задаем спектральной эффективностью R_k и порогом ОСШ. Пример - в таблице 1. Значения приведены для примера.

Таблица 1 - Пример набора режимов модуляции и кодирования

k	Модуляция/код	R_k, бит/с/Гц	ОСШ_req,k, дБ
1	QPSK 1/2	1,0	0
2	QPSK 3/4	1,5	3
3	16QAM 1/2	2,0	6
4	16QAM 3/4	3,0	9
5	64QAM 2/3	4,0	12
6	64QAM 3/4	4,5	14

Нейросеть работает как быстрый модуль оценки риска. Для каждого режима считаем $P_{out}(R_s)$. Если $P_{out}(R_s) > \delta$, режим не берем. Из оставшихся выбираем режим с максимальной полезной скоростью. Так мы снижаем вычислительную нагрузку и укладываемся в задержку.

Заключение

Сформулировали модель беспроводного канала с пассивным перехватом при рэлеевском замирании. Для оценки риска выбрали показатель: $P_{out}(R_s) = \Pr\{ C_s < R_s \}$

Описали расчет этого показателя двумя способами. Первый — численное интегрирование. Второй — метод Монте-Карло. Эти процедуры используем для генерации обучающих данных. Предложили замещающую нейросетевую модель: $P_{out} \approx f\theta(\bar{\gamma_b}, \bar{\gamma_e}, R_s)$

Она быстро оценивает вероятность нарушения секретности. Параметры канала и целевую скорость можно менять. Показали применение аппроксимации в контуре адаптации модуляции и кодирования. Задали ограничение: $P_{out}(R_k) \le \delta$

По нему выбираем режим с максимальной спектральной эффективностью. Результаты подходят системам связи. Там риск нужен в реальном времени. И вычислительный ресурс ограничен.

Список использованных источников

1.Wyner A. D. The wire-tap channel // Bell System Technical Journal. 1975. Vol. 54, No. 8. P. 1355-1387.

2.Bloch M., Barros J. Physical-Layer Security: From Information Theory to Security Engineering. Cambridge: Cambridge University Press, 2011. 406 p.

3.Mukherjee A. et al. Principles of physical layer security in multiuser wireless networks: A survey // IEEE Communications Surveys & Tutorials. 2014. Vol. 16, No. 3. P. 1550-1573.

Тарасенко Артем Алексеевич, студент, gamenk987@gmail.com.