

АЛГОРИТМ ВИБОРУ ДОПОМІЖНИХ ВУЗЛІВ ДЛЯ БЕЗПРОВОДОВОЇ КООПЕРАТИВНОЇ РЕТРАНСЛЯЦІЇ З ПЕРЕХОПЛЮВАЧЕМ

Афанасьєва Л. О.

*Інститут телекомунікаційних систем КПІ ім.Ігоря Сікорського, Україна
E-mail: liana.afanasyeva@gmail.com*

Selection algorithm of helper nodes in wireless cooperative relaying with eavesdropper

Due to broadcasting nature of wireless channel, information privacy is exposed to be undesirable overheard. Therefore, wireless network implementation feature requires a specific approach to ensuring the security. This paper provides an overview of the cooperative relaying with eavesdropper scheme. This paper provides an overview jamming technique that produce an artificial interference at the eavesdropper node in order to reduce the capacity of the link.

Конфіденційності інформації в безпроводових мережах приділяється значна увага через ширококомунікаційну природу безпроводового середовища, що дозволяє всім користувачам в зоні покриття передачі підслухувати вихідне повідомлення [1]-[3]. Традиційно, захист інформації в безпроводових мережах реалізовується в основному на вищих рівнях з використанням криптографічних методів [4]-[5]. Однак, такі методи забезпечення секретності стають предметом збільшення потенційних атак, тому впровадження нових підходів, що реалізують безпеку каналів на фізичному рівні (РНУ) є актуальною задачею. В роботах [1] показано, що коли канал вузла, що підслухує є погіршеною версією основного каналу, джерело і цільовий приймач можуть обмінюватися повідомленнями з безпечною ненульовою швидкістю, зберігаючи при цьому данні передачі від вузла, що підслухує. Максимальна швидкість такої передачі від джерела до його цільового приймача називається безпечною швидкістю (secure rate), при якій ймовірність помилки декодування цільового приймача прагне до нуля, а ймовірність помилки для вузла, що підслухує прагне до одиниці.

Розглядається системна модель кооперативної мережі джерело S -цільовий приймач D з одним перехоплювачем E (eavesdropper) і набором проміжних терміналів-ретрансляторів $S_R = \{1, 2, \dots, N\}$ з N вузлами (рис 1).

Проміжні вузли працюють в напівдуплексному режимі, отже, процес зв'язку здійснюється в два етапи по двом ортогональним каналах. Під час першої фази джерело S передає дані на цільовий приймач D , і за рахунок ширококомунікаційного характеру передачі проміжні вузли ретрансляції R і перехоплювач E прослуховують передану інформацію.

Вузли генерації перешкод (jammer) J_1, J_2 працюють в «режимі перешкод», отже, не декодують вихідний сигнал, а застосовуються для генерації навмисних перешкод, щоб погіршити якість лінії зв'язку перехоплювача.

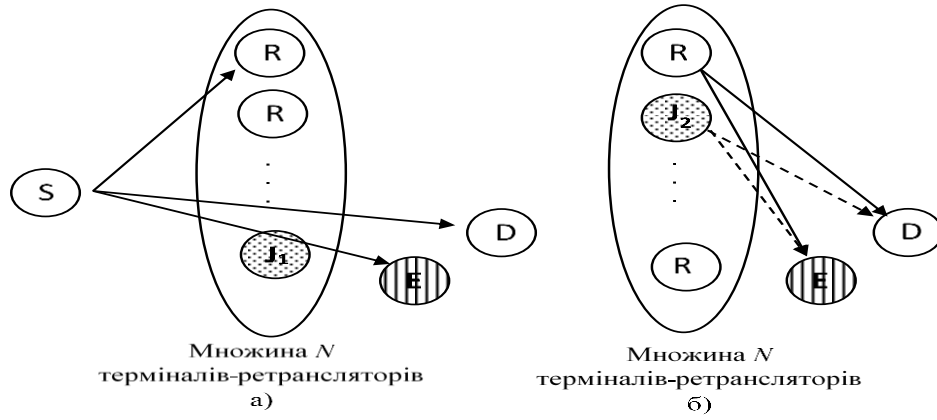


Рис.1. Схема кооперативної ретрансляції з перехоплювачем:
а) фаза ширококомовлення, б) фаза кооперації.

Під час кооперативної фази, відповідно до схем безпеки вибирається проміжний вузол R , який успішно декодував вихідний сигнал з підмножини $C_d \in S_R$, для роботи в якості терміналу-ретранслятора та пересилає вихідне повідомлення на цільовий приймач D .

Алгоритм оптимальної схеми вибору R і J передбачає наявність набору значень певних параметрів для всіх ліній зв'язку, критерієм оптимальності є максимальне значення миттєвої пропускної здатності для набору декодування C_d .

Пропускна здатність при кооперативній ретрансляції з перехоплювачем може бути виражена в наступному вигляді:

$$C_S^{|C_d|}(R, J_1, J_2) = \left[\frac{1}{2} \log_2 \left(1 + \frac{\gamma_{S,D}}{1 + \gamma_{J_1,D}} + \frac{\gamma_{R,D}}{1 + \gamma_{J_2,D}} \right) - \frac{1}{2} \log_2 \left(1 + \frac{\gamma_{S,E}}{1 + \gamma_{J_1,E}} + \frac{\gamma_{R,E}}{1 + \gamma_{J_2,E}} \right) \right], \quad (1)$$

для $|C_d| > 0$,

де $R \in C_d, J_1 \in S_R, J_2 \in \{S_R - R^*\}, \gamma_{a,b}$ - миттєве відношення сигнал/шум (SNR) для лінії зв'язку $a \rightarrow b$, R^* - обраний термінал-ретранслятор. Вибір вузлів для передачі даних, які дозволяють мінімізувати ймовірність збою зв'язку визначаються за наступними критеріями

$$(R^*, J_1^*, J_2^*) = \arg \max_{R \in C_d, J_1 \in S_R, J_2 \in \{S_R - R^*\}} \left\{ \frac{\gamma_{S,D} + \gamma_{R,D}}{\frac{\gamma_{J_1,D} + \gamma_{J_2,D}}{\gamma_{S,E} + \gamma_{R,E}} + \gamma_{J_1,E} + \gamma_{J_2,E}} \right\} \quad (2)$$

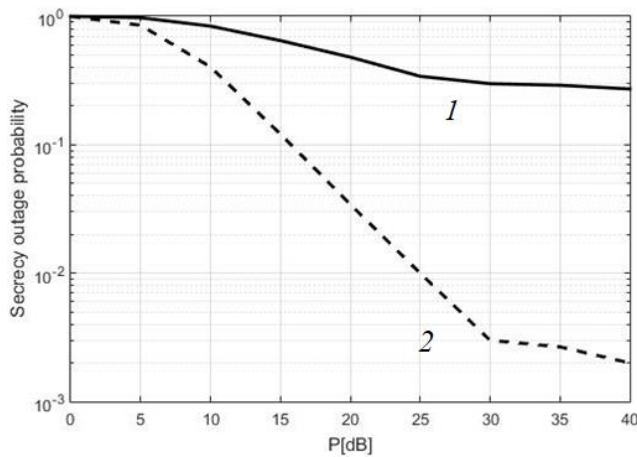
З рівняння (2) отримуємо

$$J_1^* = \arg \max_{J_1 \in S_R} \left\{ \frac{\gamma_{J_1,E}}{\gamma_{J_1,D}} \right\}, \quad (3)$$

$$R^* = \arg \max_{R \in C_d} \left\{ \frac{\gamma_{R,D}}{\gamma_{R,E}} \right\} \quad (4)$$

$$J_2^* = \arg \max_{J_2 \in \{S_R - R^*\}} \left\{ \frac{\gamma_{J_2,E}}{\gamma_{J_2,D}} \right\} \quad (5)$$

Розглянутий алгоритм передбачає вибір R по критерію максимального відношення $\gamma_{n,D}, \gamma_{n,E}$, в той час як для вузлів генерації перешкод J вибір ґрунтується на мінімальному значенні відношення $\gamma_{J,E}$ до $\gamma_{J,D}$. Отже, критерій вибору не залежить від порядку вибору і завжди будуть вибиратися різні термінали-ретрансляції.



1 - перехоплювач E знаходиться ближче до джерела S ,
2 - перехоплювач розташований ближче до цільового приймача D .

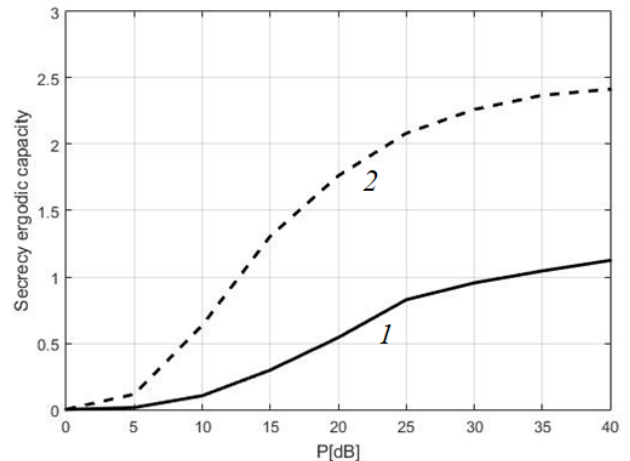


Рис. 2. Залежність вірогідності збою на лінії зв'язку від переданої потужності.

Рис. 3. Залежність пропускної здатності від переданої потужності.

Як можна бачити з графіків на рис.2 та рис.3, при розташуванні перехоплювача ближче джерела методи безперервного глушіння менш ефективні, а саме генерація перешкод забезпечує меншу ймовірність збою зв'язку та забезпечується краща продуктивність системи зв'язку при наявності шумів для випадку розташування J біля D .

Література

1. Silva E. D., Santos A. L. D., Albin L. C. P., Lima M. Identity based key management in mobile ad hoc networks: techniques and applications// IEEE Wireless Commun. . –2008. –vol. 15. – pp. 46-52 (DOI: <https://doi.org/10.1109/MWC.2008.4653131>).
2. S. Kravchuk, L.Afanasieva Wireless cooperative relaying without maintaining a direct connection between the source and target receiver terminals// Information and Telecommunication Sciences. – No 2, pp. 5-11, 2019 (DOI: <https://doi.org/10.20535/2411-2976.22019.5-11>)
3. Афанасьєва Л.О., Кравчук С.О. Протокол адаптивної ретрансляції для кооперативних мереж// Матер. 13-ї міжнар. наук.-техн. конф. “Перспективи телекомунікацій”, 15-19 квітня 2019 р. – К.: КПІ ім. Ігоря Сікорського, 2019. – С. 192–195.
4. Zou Y, Zhu J, Wang X, Leung VCM Improving physical-layer security in wireless communications using diversity techniques//IEEE Netw. –2015. . – No. 29(1) . – 42–48.
5. Li J., Petropulu A.P., Weber S. On cooperative relaying schemes for wireless physical layer security// IEEE Trans. Signal Process. –2011. –No. 59(10) . – pp. 4985–4997 (DOI: <https://doi.org/10.1109/TSP.2011.2159598>).