УДК 004.056.5

Чевардін В. Є. (ВІТІ НТУУ „КПІ”)
Романюк В. А. (ВІТІ НТУУ „КПІ”)
Шевченко В. С. (ВІТІ НТУУ „КПІ”)

МОДЕЛЬ ЗАГРОЗ БЕЗПЕКИ ІНФОРМАЦІЇ В СУЧАСНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ З ДИНАМІЧНОЮ ТОПОЛОГІЄЮ

З використанням певних обмежень наведені аналітичні вирази для оцінки імовірності реалізації загроз безпеки інформації в мережах з динамічною топологією. Визначені ризики реалізації існуючих загроз безпеки маршрутної інформації в ad hoc мережі. Визначені критерії забезпечення безпечної маршрутизації в мережі ad hoc та їх зв'язок з показниками стійкості механізмів захисту інформації.

Чевардін В. Є., Романюк В. А., Шевченко В. С. Модель угроз безопасности информации в современных телекоммуникационных сетях с динамической топологией. *С использованием определенных ограничесний представлены аналитические выражения для оценки вероятности реализации угроз безопасности информации в сетях с динамической топологией. Определены риски реализации существующих угроз безопасности маршрутной информации в ad hoc сети. Определены критерии обеспечения безопасной маршрутизации в сети ad hoc и их связь с показателями стойкости механизмов защиты информации.*

Chevardin V.E., Romanyk V. A., Shevchenko V. S. The model of information security in modern network with dinamic topology. *We presented formulas for the probability estimates of the used information security threats in network with dynamic topology. We determined risks of the use information security threats for the route information in ad hoc network. We determine criterions of secure routing in ad hoc network and their link with security parameters in the protection information mechanisms.*

Ключеві слова: *атака на ad hoc мережу, загроза безпеці інформації, безпека інформації, захист мереж.*

Вступ

Одним з перспективних напрямків розвитку сучасних інформаційно-телекомунікаційних мереж критичного застосування є створення мобільних радіомереж, до складу яких входять мережі з динамічною топологією. Прикладом таких мереж є ad hoc мережі, MANET та інші [1, 2]. Особливістю таких мереж є легкість побудови мережі, відносно низька вартість обладнання, швидкість розгортання мережі в будь-яких умовах. Однак головною проблемою впровадження мобільних радіомереж з динамічною топологією є ускладнення процесів забезпечення захисту від сучасних загроз безпеки інформації [3 – 5]. Сучасні способи реалізації загроз безпеки інформації в мережах з динамічною топологією іноді можуть привести від порушення вимог щодо ефективності, надійності та безпеки функціонування телекомунікаційних мереж до катастрофічних наслідків [8 – 10]. Для аналізу сучасних загроз безпеки інформації скористуємось наступними визначеннями.

Загроза безпеки системи (мережі) – потенційно можлива подія, що може завдати шкоди інформації та її властивостям (конфіденційності, цілісності, доступності) у системі.

Вразливість системи (мережі) – будь-яка характеристика системи (мережі), що створює основу для виникнення загрози безпеки інформації.

Атака порушника (мережна) – дія або сукупність дій порушника, яка використовує вразливості системи (мережі) для реалізації певних загроз безпеки інформації.

Ризик порушення безпеки системи (мережі) – ймовірний збиток, що залежить від захищеності системи. Як правило, ризик вимірюється у коштах, але далі пропонується використовувати якісну оцінку ризику порушення безпеки інформації – r_i.

Сучасні загрози безпеки інформації в ad hoc мережах можуть реалізовуватись як у вигляді атак на апаратні ресурси мережі (DoS-атак, Syn-атак, жадібність), атак на інформаційні ресурси мережі (модифікація повідомлень, видалення повідомлень, додавання надлишкових повідомлень), атак на основі клонування вузлів, комбінованих атак. Враховуючи призначення та особливості сучасних мереж з динамічною топологією, вразливим місцем таких мереж є процеси маршрутизації, які відбуваються на кожному вузлі мережі. Загрози безпеки інформації, яка обробляється на кожному вузлі, створюють додаткові ризики порушення безпеки мережі в цілому (порушення працездатності мережі,

порушення зв’язаності вузлів мережі).

Найбільш небезпечними атаками на процеси маршрутизації є: Grayhole – атака, Wormhole – атака, Sybil – атака, DoS – атака [6 - 10]. Сьогодні існує немало часткових рішень, які дозволяють забезпечити захист від однієї або декількох з цих атак. Однак ці рішення мають певні недоліки та обмеження, які не дозволяють забезпечити вимоги щодо захисту інформації в радіомережах від усіх існуючих загроз безпеки інформації в мережі.

Таким чином, поширення впливу загроз безпеки інформації окремого вузла на безпеку мережі створює додаткові умови для здійснення потужних атак на мережу, які не враховують сучасні підходи до захисту ad hoc мереж. Це робить дослідження сучасних загроз безпеки інформації в мережах з динамічною топологією актуальними.

Метою роботи є розробка моделі загроз безпеки мережі з динамічною топологією, яка дозволяє оцінити імовірність реалізації певних ризиків порушення безпеки інформації з урахуванням показників стійкості криптографічних механізмів забезпечення безпеки інформації.

1. Ризики порушення безпеки інформації в мережі з динамічною топологією

Процес маршрутизації в мережах з динамічною топологією є однією з важливих задач функціонування мережі [1]. Як правило, особливості кожного з протоколів маршрутизації потенційно є основою для реалізації сучасних атак на мережу. Більшість сучасних атак на ad hoc мережі основані на зміні маршрутної інформації: маршрутних метрик, числові послідовності часу створення маршрутів, ідентифікатори вузлів та інших маршрутних параметрів [3, 4]. В зв’язку з чим, забезпечення безпечної маршрутизації вже неможливе без використання криптографічних механізмів забезпечення захисту інформації [5, 6].

Одним з розповсюджених механізмів забезпечення безпеки маршрутної інформації є механізм побудови ланцюгів ґеш-дерев Меркля, який реалізований у найбільш відомих протоколах безпечної маршрутизації SEAD, DSDV та інших [6, 10, 13]. Головним показником надійності (з точки зору стійкості до зламу ланцюгів ґеш-дерев Меркля) протоколу механізму побудови ланцюгів ґеш-дерев Меркля є стійкість односпрямованої функції (геш-функції), яка використовується в ньому. Зв’язок показників криптографічної стійкості механізмів захисту з кількісними характеристиками мережі дозволить отримати новий погляд на побудову моделі загроз безпеки мережі з динамічною топологією.

Для проведення аналізу надійності протоколів та оцінки загроз безпеки інформації в мережі ad hoc зафіксуємо наступні параметри мережі:

- N – число вузлів мережі;
- статуси вузлів мережі (нбв – небезпечний вузол, б – безпечний вузол);
- δ – граничне число небезпечних вузлів, при якому мережа вважається непрацездатною або повністю підконтрольною порушнику;
- r_1 – порушення нормального функціонування одного вузла (компрометація одного вузла);
- r_2 – порушення нормального функціонування g вузлів (компрометація g вузлів);
- r_3 – порушення нормального функціонування мережі в цілому (порушення зв’язаності мережі, якщо $g = \delta$);
- $i = 1, ..., I$ – номер вузла відправника пакетів;
- $j = 1, ..., J$ – номер вузла отримувача пакетів;
- d_{ij} – метрика маршруту (число кроків передачі) між вузлами i та j;
- s_{ij} – значення числової послідовності, яка вказує на строк створення маршруту до j-го вузла, яка відома i-му вузлу;
- ID_i – ідентифікатор i-го вузла;
- V_{ij} - інтенсивність надходження пакетів від i-го вузла до j-го вузла;
- P_i^k – імовірність реалізації k-ої атаки проти вузла i, $k = 1, ..., \mathrm{K}$;

– P_{r_t} – імовірність реалізації *t*-го ризику, $t = 1, 2, 3$.

Ймовірність реалізації ризику r_1 (успішної реалізації будь-якої атаки з k можливих), проти *i*-го вузла дорівнює:

$$P_{r_1} = P_i^K = \max_k P_i^k, k = 1, ..., K. \quad (1)$$

Ймовірність успішної реалізації *k*-ої атаки проти g вузлів дорівнює:

$$P_g^k = \prod_{i=1}^{g} P_i^k. \quad (2)$$

З урахуванням виразу (2) імовірність реалізації ризику r_2, або ризику r_3 (якщо $g = \delta$) дорівнює:

$$P_{r_3} = P_{r_2} = \max_k P_g^k = \max_k \prod_{i=1}^{g} P_i^k, k = (1, ..., K). \quad (3)$$

Приклад. Припустимо що успішність *k*-ої атаки на будь-який вузол мережі є рівноймовірною подією. Нехай P_i^1 – ймовірність успішної Grayhole-атаки на *i*-ий легальний вузол мережі, P_i^2 – ймовірність успішної Wormhole-атаки на *i*-ий легальний вузол мережі, P_i^3 – ймовірність успішної Sybil-атаки на *i*-ий легальний вузол мережі, P_i^4 – ймовірність успішної DoS-атаки на *i*-ий легальний вузол. У такому випадку, ймовірність реалізації ризиків r_2, r_3 дорівнює:

$$P_{r_3}(g = \delta) = P_{r_2} = \max_k \prod_{i=1}^{g} P_i^k = \max\left\{\prod_{i=1}^{g} P_i^1, \prod_{i=1}^{g} P_i^2, \prod_{i=1}^{g} P_i^3, \prod_{i=1}^{g} P_i^4\right\}, \quad (4)$$

де $k = (1, ..., 4)$, g – число вузлів групи, δ – число вузлів, успішне атакування яких може привести до порушення нормальної роботи мережі (наприклад до порушення зв’язаності).

Таким чином, значення P_{r_3} дозволяє оцінити імовірність порушення нормальної роботи мережі в залежності від числа вузлів мережі та ймовірностей реалізації кожної з атак. Отримана модель також може бути використана для випадку з більш детальним розподілом ризиків порушення працездатності в мережі.

Наприклад, ризик втрати частини пропускної спроможності вузла, ризик втрати частини заряду батареї вузла та інші. Для отримання ймовірностей реалізації кожної з атак необхідно визначити критерії забезпечення безпеки маршрутної інформації та інших параметрів в мережі, порушення яких дозволяє реалізувати певну атаку.

2. Критерії забезпечення безпечної маршрутизації

Для визначення критеріїв забезпечення безпеки інформації в мережі з динамічною топологією представимо фрагмент мережі (рис. 1).

Усі критерії розділимо на дві категорії: забезпечення захисту від атак на основі зміни маршрутної інформації (d_{ij}, s_{ij} або ID_i), на основі виснаження програмно-апаратних ресурсів вузлів мережі (пропускна спроможність вузлів, час роботи батареї).

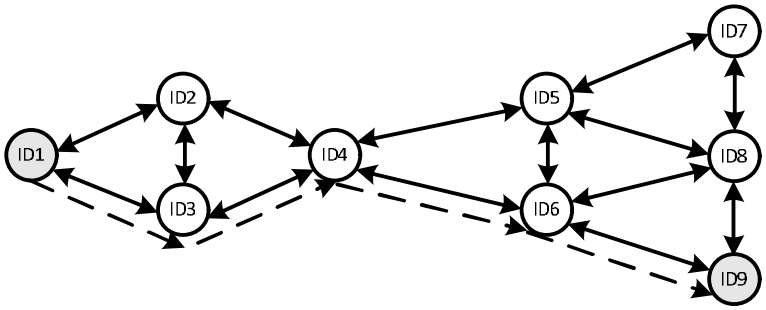

Рис. 1. Фрагмент мережі з динамічною топологією

Критерій забезпечення захисту від атак на основі зміни маршрутної метрики

Для будь-якого вузла в мережі при побудові маршрутів від вузла з ID1 до вузла з ID9 існує загроза хибного зменшення маршрутної метрики одним з вузлів мережі (порушником) з метою ретрансляції пакетів через себе. Згідно з протоколом маршрутизації в мережі кожен з вузлів, в нашому випадку вузол з ID1, будує маршрут до вузла призначення – вузла ID9.

Визначимо одним з маршрутів від вузла з ID1 до вузла з ID9 $M_{ID1ID9}^{1}: \{ID1, ID3, ID4, ID6\}$. Для забезпечення справжності маршруту M_{ID1ID9}^{1} необхідно, щоб маршрутна метрика (відстань у кроках до вузла призначення), яка відома кожному наступному вузлу маршрута M_{ID1ID9}^{1} (при проходженні зліва направо, тобто від вузла з $ID1$ до вузла з $ID6$) зменшувалась, $d_{ID1ID9} > d_{ID3ID9} > d_{ID4ID9} > d_{ID6ID9}$.

Критерій – для забезпечення справжності маршруту від вузла i до вузла j $M_{ij}^{1}: \{i, j-1\}$ необхідно щоб для кожного наступного вузла $i+1$ маршруту M_{ij}^{1} при наближенні до вузла призначення (вузла j) метрика (відстань у кроках) зменшувалась:

$$d_{ij} > d_{i+1j}, \tag{5}$$

де d_{ij} – маршрутна метрика (число кроків передачі до вузла j), яка відома i-му вузлу маршруту M_{ij}.

Критерій забезпечення захисту від атак на основі зміни значення актуальності маршруту

Для будь-якого маршруту від вузла з ID1 до вузла з ID9 $M_{ID1ID9}^{1}: \{ID1, ID3, ID4, ID6\}$ однією з потужних атак є атаки на основі несанкціонованої зміни значень актуальності маршрутів (часу існування маршруту).

Критерій – для фіксованого маршруту від вузла з ID1 до вузла з ID9 $M_{ID1ID9}^{1}: \{ID1, ID3, ID4, ID6\}$ необхідно щоб для кожного наступного вузла $i+1$ маршруту M_{ij}^{1} при наближенні до вузла призначення (вузла j) значення s_{ij} (актуальність маршруту) не зменшувалась:

$$s_{ij} \le s_{i+1j}, \tag{6}$$

де s_{ij} – ц е числова послідовність (час створення маршруту до j-го вузла), що відома вузлу i.

Критерій забезпечення захисту від виснаження програмно-апаратних ресурсів вузла

Нехай V_{ij} – інтенсивність надходження пакетів від i-го вузла до j-го вузла, тобто число прийнятих або відправлених пакетів за одиницю часу i-им вузлом.

Тоді сумарний потік повідомлень, які надходять до вузла *j* складе:

$$V_j^{\Sigma} = \sum_{i=1}^{n} V_{ij} \ . \tag{7}$$

де *n* – число однокрокових сусідів вузла *j*.

Одним зі способів захисту від подібних атак вважається обмеження інтенсивності надходження пакетів до вузла в мережі, шляхом розрахунку відносного значення границі інтенсивності надходження пакетів. Для цього використовується критерій забезпечення захисту від DoS-атак.

Критерій – для легального *j*-го вузла мережі інтенсивність вхідного та вихідного потоку маршрутних (службових) пакетів не повинно перебільшувати поріг:

$$V_j^{\Sigma} < V_{Lim} . \tag{8}$$

Критерій забезпечення захисту від клонування вузлів мережі

Нехай P_i^{coll} – колізія ідентифікаторів, яка визначає випадок існування двох вузлів з однаковими ідентифікаторами в двох різних точках мережі одночасно. Для захисту від загрози клонування використовують автентифікацію при поверненні до мережі знову. Внаслідок чого, випадок співпадіння ідентифікаторів різних вузлів може виникнути лише при зламу порушником механізму автентифікації або завдяки протоколу маршрутизації (але для військових мереж імовірністю клонування вузла через відхилення у роботі протоколу маршрутизації можна знехтувати).

Критерій – імовірність P_i^{coll} для кожного вузла мережі не повинна перебільшувати максимуму ймовірностей зламу механізму автентифікації вузлів в мережі або відхиленнями протоколу маршрутизації від нормальної роботи:

$$P_i^{coll} \le \max\{P_i^{Aut}, P_i^{Abnorm}\} , \tag{9}$$

де P_i^{Abnorm} – імовірність відхилення протоколу маршрутизації від нормальної роботи;

P_i^{Aut} – імовірність зламу механізму автентифікації вузлів в мережі.

Нехай для захисту в мережі використовують відомий механізм побудови ґеш-дерев Меркля [13]. Порушення критеріїв захисту від атак на основі зміни маршрутної метрики та основі на основі зміни значення актуальності маршруту вважається можливим лише у випадку зміни кореневого ґеш-значення (10) або при зміні значення геш-функції, тобто знаходження колізії для геш-алгоритму.

$$h_{0,s} = PRF(K, s) , \tag{10}$$

де *K* – секретний ключ вузла, який створює ґеш-ланцюг;

s_i – числова послідовність;

PRF – псевдовипадкова функція.

Складність реалізації атак через зміну маршрутної інформації буде еквівалентною відтворенню закону формування *PRF* або знаходженню алгоритму H^{-1}. Ймовірність успішної реалізації атаки на *i*-ий вузол (порушення одного з критеріїв) дорівнює:

$$P_i = \max\{P_i^{PRF^{-1}}, P_i^{H^{-1}}, P_i^{DoS}, P_i^{Aut}, P_i^{Abnorm}\} . \tag{11}$$

Таким чином, якщо безпечність маршрутних процесів у мережі (рис. 1) забезпечується з використанням механізму побудови ґеш-дерев Меркля, ймовірність реалізації атаки на *i*-ий вузол мережі визначається виразом (11). Якщо припустити, що протокол мережі виключає можливість здійснення DoS-атак, тоді ймовірність реалізації атаки на *i*-ий вузол мережі та, як наслідок, імовірність реалізації ризиків $r_1 – r_3$ залежить від стійкості алгоритмів H та PRF.

Висновки

В ході аналізу існуючих загроз безпеки інформації в мережах з динамічною топологією були отримані аналітичні вирази для оцінки ймовірності реалізації ризиків порушення нормального функціонування мережі. Визначено, що поширення впливу загроз безпеки інформації окремого вузла на безпеку мережі ad hoc викликає появу додаткових загроз безпеки мережі. Визначені критерії забезпечення безпечної маршрутизації в мережі з динамічною топологією. З використанням отриманої моделі загроз безпеки в мережі ad hoc стало можливим визначати сучасні вимоги до протоколів безпечної маршрутизації та перспективні шляхи щодо їх вдосконалення.

ЛІТЕРАТУРА

1. Миночкин А.И. Маршрутизация в мобильных радиосетях – проблема и пути решения / Миночкин А.И., Романюк В.А. // Зв’язок. – 2006. – № 7. – С. 49 – 55.

2. Akyildiz I. F. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks / I. F. Akyildiz, W. Su, Y. // IEEE Communications Magazine, 40(8):102 – 114. – 2002.

3. Міночкін А. І. Виявлення атак у мобільних радіомережах / Міночкін А.І., Романюк В.А., Шаціло П.В. // Збірник наукових праць ВІТІ НТУУ “КПІ”. – 2005. – № 1. – С. 102 – 111.

4. Xu Li. On Secure Mobile Ad hoc Routing / Xu Li, Amiya Nayak, Isabelle Ryl, David Simplot // Old City Publishing, Inc. Ottawa, Canada. 2007.

5. Anjum F. Security for Wireless Ad hoc Networks / F. Anjum, P. Mouchtaris // John Wiley & Sons, Inc., Hoboken, New Jersey, 2007.

6. Karlsson J. Routing Security in Ad-hoc Networks / J. Karlsson, L.S. Dooley, G. Pulkkis // Issues in Informing Science and Information Technology. Vol. 9. – 2012. P. 369 – 383.

7. J. Newsome, E. Shi, D. Song, and A. Perrig. The Sybil attack in sensor networks: Analysis and defenses. In Third International Symposium on Information Processing in Sensor Networks, IPSN 2004, pp. 259 – 268, Monterey, CA, United States. – 2004.

8. Yin J. Sybil attack detection in a hierarchical sensor network / J. Yin and S. K. Madria // In Third International Conference on Security and Privacy in Communications Networks and the Workshops (SecureComm 2007), pp. 494 – 503. – 2007.

9. Yun J.-H. WODEM: Wormhole Attack Defense Mechanism in Wireless Sensor Networks / J.-H. Yun, I.-H. Kim, J.-H. Lim, and S.-W. Seo. // In Ubiquitous Convergence Technology (ICUCT 2006), pp. 200 – 209. LNCS 4412. – 2007.

10. Venkatraman L. Strategies for enhancing routing security in protocols for mobile ad hoc networks / Lakshmi Venkatraman, Dharma P. Agrawal // Jornal of Parallel and Distributed Computing, 63 (2003). P. 214 – 227.

11. Xinxin F. Key Revocation Based on Dirichlet Multinomial Model for Mobile Ad Hoc Networks / Xinxin F., and Guang G. // Security and Privacy for Emerging Areas in Communication Networks (SecureComm 08), 2008.

12. Hoeper K. Monitoring-Based Key Revocation Schemes for Mobile Ad Hoc Networks: Design and Security Analysis / Katrin Hoeper, Guang Gong // Security and Privacy for Emerging Areas in Communication Networks. Waterloo, ON, N2L 3G1, Canada 2009.

Hu Y.C. SEAD: secure efficient distance vector routing for mobile wireless ad hoc net-works / Hu Y.C., Johnson D.B., Perrig A. // Proceedings of the 4th IEEE Work-shop on Mobile Computing Systems & Ap-plications (WMCSA 2002). – 2002. – Calicoon(NY, USA). – PP. 3 – 13.