23. Богданович В.Ю. Рекомендації щодо інтеграції зусиль суб'єктів системи забезпечення національної безпеки для нейтралізації виявлених загроз без застосування силових методів / І.С.Романченко, В.Ю.Богданович, І.Ю.Свида, А.Л.Висідалко // Харьків: Зб.наук. праць ХУПС, №1, 2012, с.29-33.

24. Бодрук О.С. Структури воєнної безпеки: національний та міжнародний аспекти: Монографія. / О.С. Бодрук. – К.: НІПМБ, 2001. — 300 с.

25. Арзуманян Р. Кромка Хаоса. Сложное мышление и сеть: парадигма нелинейности и среда безопасности XXI века: монография / Р. Арзуманян.- М.: Издательский Дом «Регнум», 2012. 600 с.

26. Сищук Олексій Збройним Силам прописали реформи// Віче, №13, 2012.

27. Воєнна доктрина України. - Затверджена Указом Президента України від 15 червня 2004 року №648 (в редакції Указу Президента України від 8 червня 2012 року №390/2012)

28. Бегма В. М., Литвиненко О.В. Військово-технічне співробітництво в умовах глобалізації: український вимір: зб. мат-лів «круглого столу» / – К. : НІСД, 2011. – 80 с.

29. Дмитренко Г., Гошко А. Підвищення ефективності державної служби в Україні: методологічний підхід // Вісник державної служби України, 2000, №3.

30. *Їжак О.І.* Питання забезпечення розвідувальної діяльності в умовах фінансових обмежень: використання досвіду провідних країн для України. Аналітична записка. [Електронний ресур

Надійшла: 12.10.2013р. Рецензент: д.т.н., проф. Олійник В.Ф.

УДК 004.415.056.5(075)

**Павлов І.М.**

## АНАЛІЗ ШЛЯХІВ МАРШРУТИЗАЦІЇ ЗАГРОЗ В СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

У статті проводиться аналіз шляхів маршрутизації загроз в системах захисту інформації на основі протоколів маршрутизації інформаційних системтехнологій мобільного доступу.

**Ключові слова:** загрози, маршрутизація, механізми захисту інформації, протоколи, системи захисту інформації.

### Вступ

У наступний час у світі виконується повномасштабна модернізація інформаційних систем управління і зв'язку різного призначення, яка передбачає наряду з внесенням змін у конструкцію, так і зміну протоколів маршрутизації і топології, які дозволять, у майбутньому, створити автономні, мобільні і адаптивні інформаційні системи. Ключове місце займають технології мобільного доступу до розподілених інформаційних ресурсів.

Тому важливим питанням, вцих системах, є питання захисту інформації, так як аналіз шляхів доступу загроз до критично небезпечних ресурсів показує проблему боротьби зі шляхами впливу загроз, які використовують автоматичну маршрутизацію інформаційних систем. Як висказуються у [1-3], необхідно проаналізувати ці шляхи і показати всю небезпечність і актуальність цих питань, чому і призначена ця робота.

### Основна частина

У цілому при маршрутизації у мобільних інформаційних мережах використовуються наступні протоколи, які дозволяють застосовувати автоматичну маршрутизацію в інтересах ворожих впливів загроз (рис. 1):

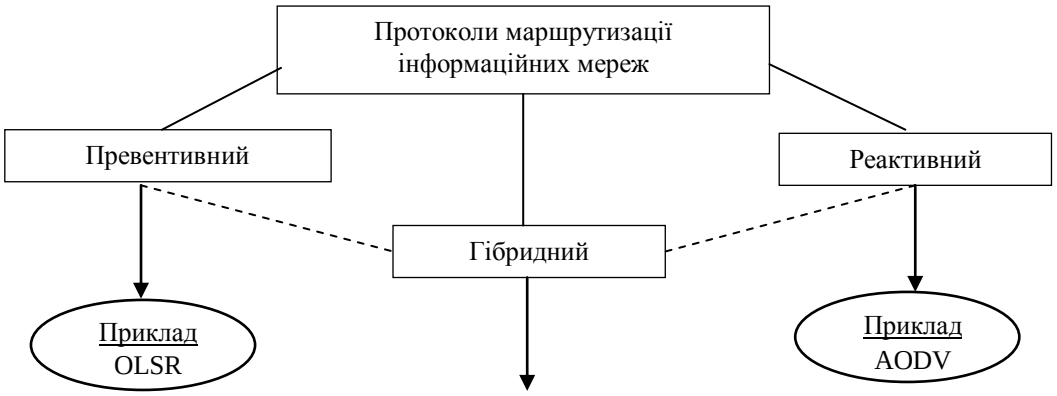



Рис. 1. Приклади протоколів маршрутизації мобільної
інформаційної мережі

При цьому реактивні протоколи повинні знаходити маршрут у тому випадку, коли необхідно передати пакет і для нього нема відомого шляху, а також змінюють шлях, якщо пройшла помилка маршруту. Превентивні протоколи знаходять маршрут завчасно для усіх пар джерело-приймач і періодично оновлюють інформацію про маршрутизацію підтримки шляхів. Гібридні протоколи повинні мати усі ці переваги. У наступний час проводиться робота по впровадженню 4-х основних протоколів маршрутизації:

спеціалізований протокол вектора відстані по запиту (AODV);

протокол динамічної маршрутизації джерела (DSR);

протокол оптимізованої маршрутизації стану з'єднань (OLSR);

протокол топологічного оповіщення, який базується на зворотному проходженні даних (TBRPF).

Звертаючись до моделі системи захисту інформації з повним перекриттям загроз [4,5] розкриємо порядок впливу загроз на механізми захисту використовуючи перспективну систему маршрутизації інформаційної системи [1,2]. Для чого визначимо взаємозв'язки між елементами області загроз та механізмів захисту, як надано на рис. 2а.,де $t_1$ – загроза з області загроз, $u_1, u_2$ – уразливості механізмів захисту, $b_1, b_2, b_3$ – бар'єри у складі механізмів захисту (фільтри), $v_1$ – область захисту інформаційної системи, або самої системи захисту інформації.

У подальшому, для аналізу, ці області тільки пронумеруємо, як надано на рис. 2б.

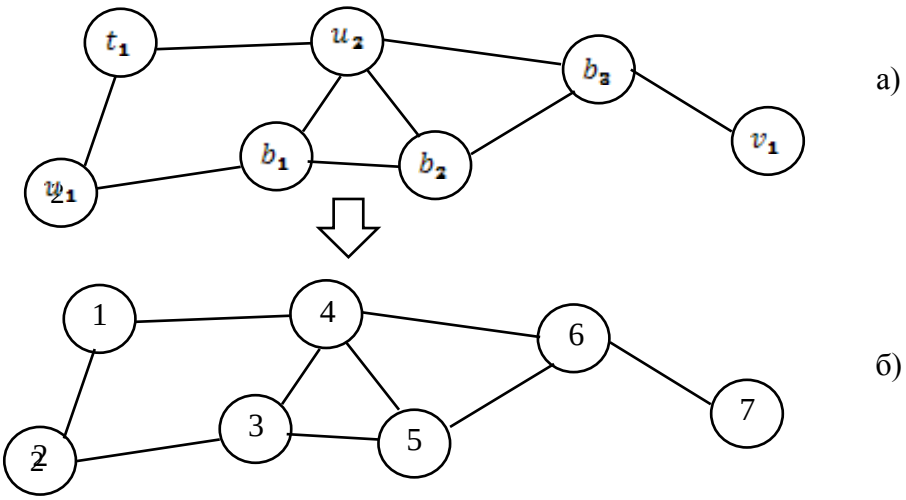



Рис. 2. а) граф взаємовідносин загроз та механізмів захисту.
б) граф маршрутизації

Кожен вузол *N* (рис. 2б) має набір сусідніх вузлів у якості "багатоточкового реле" MPR(*N*), яке передає керуючі сигнали (ворожу, або корисну інформацію) від *N*. MPR(*N*) вибирається таким чином, щоб усі двомаршрутні сусіді*N* перекривалися одномаршрутними сусідами MPR(*N*). В приведеному випадку оптимальним набором для маршруту вузла 3 буде: MPR(4) = { 3, 6 }. Це пов'язано зі зв'язністьюграфу.

Розкриємо інший оптимальний шлях MPR(3).Багатоточковий набір релейного сектору для вузла *N* (MS(*N*)), це набір вузлів, які включили вузол *N* до своїх релейних наборів. В керуючих повідомленнях будуть представлені тільки з'єднання *N*-*M* для усіх *M*, так щоб *N*∈MS(*M*). Необхідно знайти MS(3) = {…, 4, …}, MS(6) = {…, 4, …}, як представлено на рис. 3.

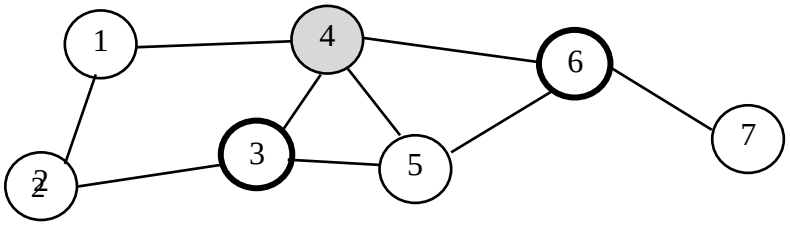



Рис. 3. Граф дослідження оптимальних шляхів маршрутизації для MS(3) = {…, 4, …}, MS(6) = {…, 4, …}

При цьому припускається наявність двонаправлених з'єднань.

Кожен вузол між собою використовує повідомлення (типу HELLO)для формування свого набору MPR. Усі вузли періодично відправляють своїм одномаршрутнимсусідам повідомлення (з'єднання двонаправленні). Наприклад: $HELLO{:}NBR(4) = \{1,3,5,6\}$. (рис. 4).

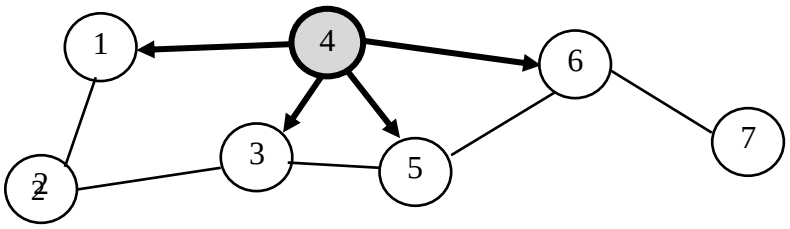



Рис. 4. Граф дослідження оптимальних шляхів маршрутизації для $HELLO{:}NBR(4) = \{1,3,5,6\}$

Використовуючи список сусідів з повідомленьHELLO, які прийняті, вузли можуть встановлювати (ідентифікувати) своїх сусідів і визначати оптимальний (або близький до оптимального) набір MPR. Цьому набору присвоюється номер. При цьому номер інкримінується будь-який раз, коли обчислюється новий набір. Наприклад, на рис 5 представлений наступний набір в вузлі 4:

$$NBR\ (1) = \{2\}, NBR\ (3) = \{2,5\}, NBR\ (5) = \{3,6\}, NBR\ (6) = \{5,7\},$$

при цьому $MPR\ (4) = \{3,6\}$.

Послідовні повідомлення HELLO вказують на сусідів, які знаходяться у наборі MPR цього вузла. Набір MPR прораховується повторно, якщо виникає зміна одно або двомаршрутних сусідів.

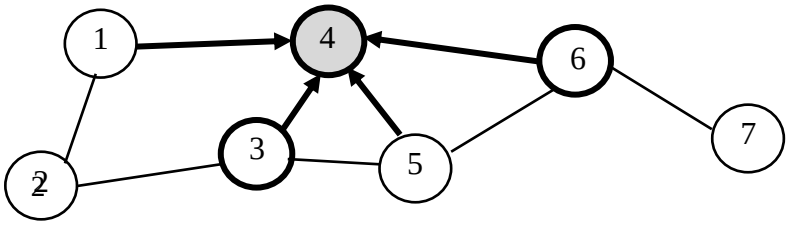



Рис. 5. Граф дослідження оптимальних шляхів маршрутизації для $MPR\ (4) = \{3,6\}$

Вузли відправляють інформацію (рис. 6) про топологію в керуючих повідомленнях (ТС), у яких визначаються:

список оповіщених сусідів;

послідовний номер (інформація про з'єднання).

Вузли генерують повідомлення тільки для тих сусідів, які знаходяться в їх наборі MS, при цьому:

тільки вузли MPR генерують керуючі повідомлення;

не усі вузли оповіщаються.

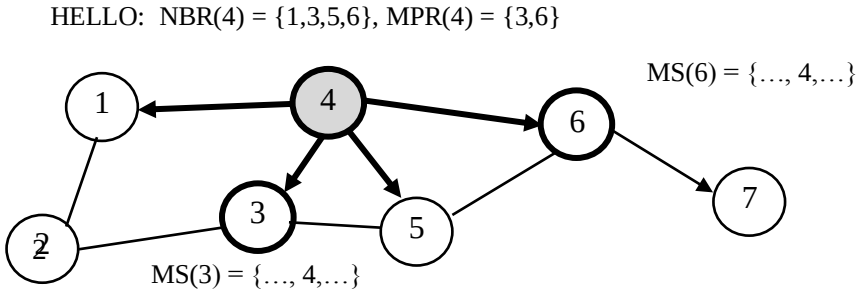



Рис. 6. Граф повторного дослідження оптимальних шляхів маршрутизації наборуMPR

Вузли обробляють усі повідомлення, які приймаються, але перенаправляють їх тільки у тому випадку, коли відправник знаходиться у їх наборі MS, при цьому тільки вузли MPR розповсюджують керуючі повідомлення. Наприклад (рис. 2б): MPR(1) = {4}, MPR(2) = {3}, MPR(3) = {4}, MPR(4) = {3, 6}, MPR(5) = {3, 4, 6}, MPR(6) = {4}, MPR(7) = {6}. MS(1) = { }, MS(2) = { }, MS(3) = {2, 4, 5}, MS(4) = {1, 3, 5, 6}, MS(5) = { }, MS(6) = {4, 5, 7}, MS(7) = { }.

Вузол 3 (рис. 7) генерує керуюче повідомлення, оповіщаючи вузли з MS(3) = {2, 4, 5}.

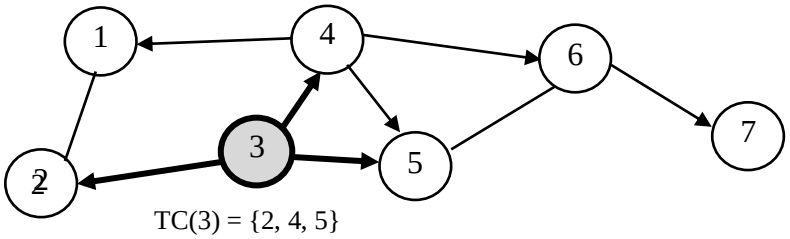



Рис. 7. Граф оповіщення сусідніх вузлів MS(3) = {2, 4, 5}

Вузол 4 пересилає керуюче повідомлення вузла 3, оскільки вузол 3∈ MS(4) = {1, 3, 5, 6}. Вузол 6 пересилає керуюче повідомлення вузла 3, оскільки вузол 4∈ MS(6). У подальшому (рис. 8) вузол 4 генерує керуюче повідомлення(ТС), оповіщаючи вузли з MS(4) = {1, 3, 5, 6}, а вузли 3 і 6 пересилають ТС(4), оскільки вузол 4∈MS(3) і вузол 4∈ MS(6).

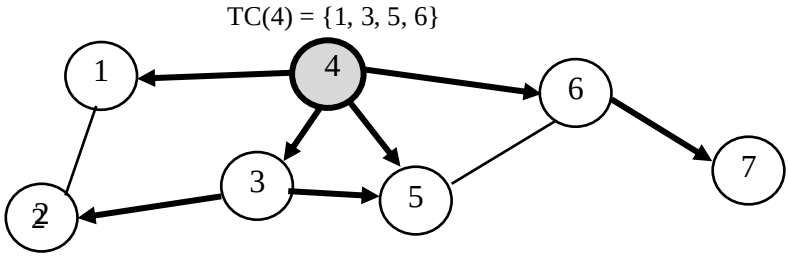



Рис. 8. Граф генерації керуючих повідомлень TC(4) = {1, 3,5, 6}

У подальшому робота маршрутизації проходить наступним чином (рис. 9): вузол6 генерує повідомлення ТС, оповіщаючи вузли з MS(6) = {4, 5, 7}, при цьому вузол 3 пересилає ТС(5) від вузла 5, а вузол 4 пересилає ТС(5) від вузла 4.

Після того, як вузли 3, 4 і 6 згенерували повідомлення ТС, у всіх вузлів буде інформація про стан з'єднання для будь-якого маршруту.

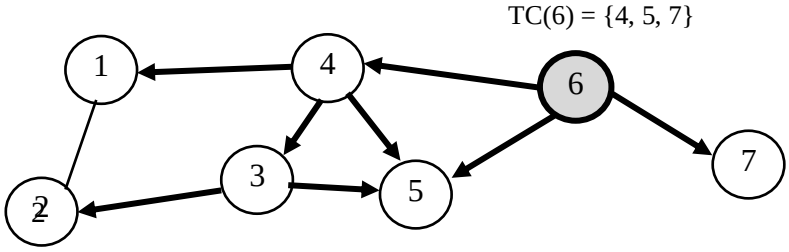
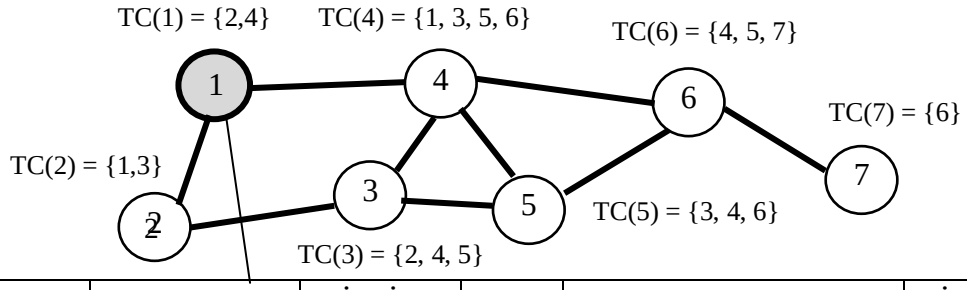



Рис. 9. Граф генерації керуючих повідомлень TC(6) = {4, 5,7}

Маючи інформацію ТС (рис. 10), кожен вузол формує таблицю топології та маршрутизації. Маршрутизація розраховується з топології.




| **Вузол** | **топологія** | **кількість опт. маршрутів (вузли)** | **Вузол** | **топологія** | **кількість опт. маршрутів (вузли)** |
|---|---|---|---|---|---|
| 2 | (1,2); (1,4,3,2). | 1 (1,2) | 5 | (1,4,5); (1,2,3,5); (1,2,3,4,5); (1,4,3,5); (1,4,6,5). | 1 (1,4,5) |
| 3 | (1,2,3); (1,4,3). | 2 (1,2,3); (1,4,3). | 6 | (1,4,6); (1,2,3,5,6); (1,4,5,6), (1,2,3,4,5,6); (1,4,3,5,6). | 1 (1,4,6) |
| 4 | (1,4); (1,2,3,4). | 1 (1,4) | 7 | (1,4,6,7); (1,2,3,5,6,7); (1,4,5,6,7); (1,4,3,5,6,7); і т.п. | 1 (1,4,6,7) |

Рис. 10. Граф топології та маршрутів для TC(1) = {2, 4}

Відповідно розраховуються маршрути для інших вузлів.

Таким чином, інформація про взаємозв'язки між вузлами (фільтрами) є відомою для вузла 1, який є областю загроз для інформації нашої моделі(рис. 2).

У подальшому необхідно побудувати оптимальний маршрут впливу загроз (вузол 1) на області, які захищаються (вузол 7) системою захисту у вигляді механізмів захисту (у нашому випадку це вузли 3,5,6 зі своїми областями уразливості – вузли 2,4).

Область загроз аналізує наступну інформацію:

усі фільтри використовують протокол маршрутизації виключно по запиту;

усі фільтри системи захисту не виконують пошуку маршрутизації або його підтримку до тих пір поки йому буде необхідним маршрут до іншого фільтру (вузла) або поки він не запропонує свої послуги у якості проміжного вузла;

у цій схемі маршрутизації використовується механізм оповіщення пошуку маршруту, який проходить від проміння (ветві) маршруту до іншого промені.

Для визначення наявності місцевих з'єднань використовуються локальні повідомлення HELLO, при цьому:

зменшується час відклику на запити маршруту;

ініціюється оновлення по мірі необхідності.

Між вузлами запит маршруту ініціюється у тому випадку, коли вузол хоче з'єднаєтися, але не знає маршруту. Вузол-джерело посилає широкомовний пакет з запитом (RREQ) своїм сусідам (табл. 1).

Таблиця 1

Широкомовний пакет з запитом (RREQ)

| **type** | **flags** | **resvd** | **hopcnt** |
|---|---|---|---|
| broadcast_id | | | |
| dest_addr | | | |
| dest_sequence_# | | | |
| source_addr | | | |
| source_sequence_# | | | |

Запит маршруту протоколу AODV проводиться за послідовними номерами, при цьому послідовний номер джерела показує "ступінь свіжості" зворотнього маршруту до джерела. Кожен сусідній вузол приймає RREQ або повертає інформацію з відповіддю маршруту (RREP), або пересилає RREQ своїм сусіднім вузлам.

Поля (source_addr, broadcast_id – табл. 1) унікально ідентифікують RREQ, broadcast_id інкремінтується для кожного пакетуRREQ, який посилається а приймачі розпізнають і знищують дублюючі пакети RREQ.

Якщо вузол не може відповісти на RREQ, то вузол інкримінує зчитувач променів маршруту і зберігає інформацію, яка необхідна для підтримки зворотнього маршруту (AODV припускає наявність симетричних з'єднань), у яких мається:

ідентифікатор сусіднього вузла, який присилає пакетRREQ;

IP адрес місця призначення;

IP адрес джерела;

широкомовний ID;

послідовний номер вузла джерела;

час закінчення запису для зворотнього маршруту.

Розглянемо приклад встановлення маршруту від джерела загроз, який наданий на рис. 11.

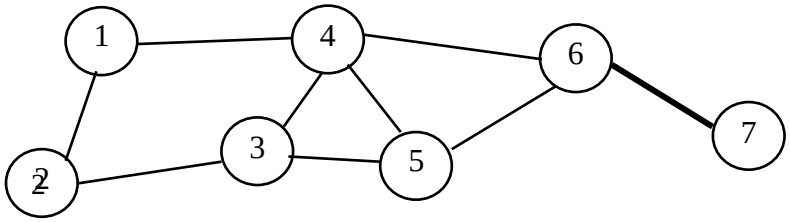



Рис. 11. Граф встановлення маршруту від джерела

Вузол 1 хоче послати пакет вузлу 7. Припустимо, що вузол 6 знає маршрут до вузла 7, а також, що в мережі більше не існує будь якої інформації про маршрутизацію, яка відноситься до вузла 7.

Вузол 1 посилає пакет RREQ своїм сусіднім вузлам (рис. 12) у якому:

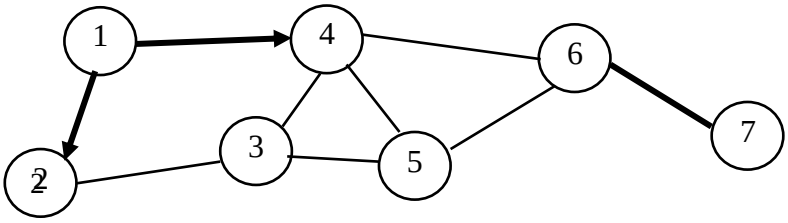



Рис. 12. Граф посилки пакету RREQ від вузла 1

source_addr = 1;
dest_addr = 7;
broadcast_id = broadcast_id + 1;
source_sequence_# = source_sequence_# + 1;
dest_sequence_# = lastdest_sequence_# forNode 7.

Вузли 2 і 4 перевіряють (рис. 13), що це новий RREQ і що source_sequence_# не застарів відносно зворотнього маршруту до вузла 1. У подальшому вузли 2 і 4 пересилають RREQ, оновлюють source_sequence_# для вузла 1 і інкрементуютьhop_cnt у пакеті RREQ.

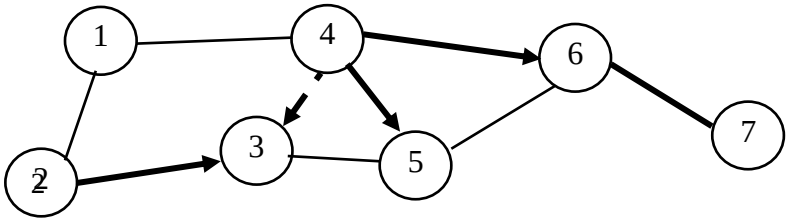



Рис. 13. Граф перевірки нового пакету RREQ від вузлів 2, 3

RREQ приходить на вузол 6, якому відомий маршрут до вузла 7. Вузол 6 повинен перевірити, щоб послідовний номер приймача був менше або дорівнював послідовному номеру приймача, який він зберіг для вузла 7. А вузли 3 і 5 будуть ретранслювати пакет RREQ, однак приймачі будуть рахувати його дублікатом (рис. 14).

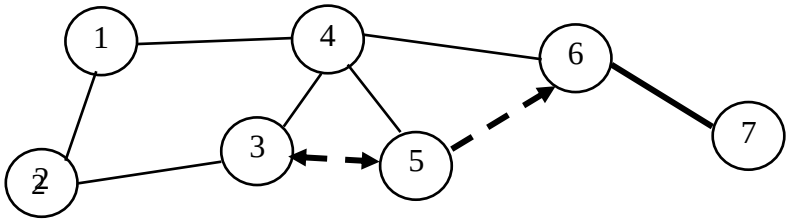



Рис. 14. Граф передачі RREQ від вузла 5

Якщо вузол приймає пакет RREQ і у нього є існуючий маршрут до місця призначення, то він відправляє однонаправлений пакет з відповіддю маршруту (RREP) тому сусідньому вузлу, від якого він прийняв пакет RREP (таблиця 2). Проміжні вузли будуть ретранслювати перший RREP на напрямку до джерела, використовуючи керовані записи зворотнього маршруту. Інші пакети RREP відкидаються до тих пір, поки (табл. 2): номер dest_sequence_# більше попереднього, або destination_sequence_# такий же, але hop_cnt менше (тобто, це кращий шлях) – RREP.

Таблиця 2

Однонаправлений пакет з відповіддю(RREP)

| **type** | **flags** | **rsvd** | **prsz** | **hopcnt** |
|---|---|---|---|---|
| dest_addr | | | | |
| dest_sequence_# | | | | |
| source_addr | | | | |
| lifetime | | | | |

Наприкінці RREP досягає джерела, який може використовувати сусідній вузол, який прислав RREP у якості наступного проміння для пересилки інформації до місця призначення.

Кешовані зворотні маршрути будуть відходити по часу у тих вузлах, які не бачать пакету RREP.

Розглянемо це на прикладі рис.15.

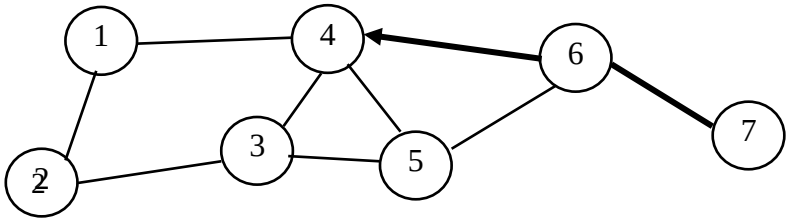



Рис. 15. Граф передачі кешованого пакету RREP від вузла 6

Вузол 6 знає маршрут до вузла 7 і відправляє RREP до вузла 4 у складі:
source_addr = 1;
dest_addr = 7;
dest_sequence_# = max (особистий послідовний номер, dest_sequence_# з RREQ);
hop_cnt = 1.

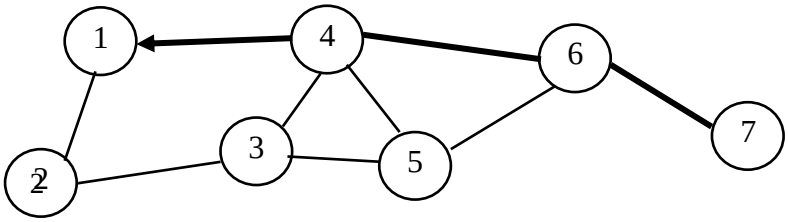



Рис. 16. Граф передачі кешованого пакету RREP від вузла 4

Вузол 4 перевіряє, що це нова відповідь про маршрут (випадок, який наданий на рис. 16) або відповідь, яка має найменшу кількість промінів, і, якщо це так, пересилає пакет RREP до вузла 1 і інкримінує hop_cnt в пакетіRREP. Вузол 1 знає маршрут з 3-х променів до вузла 7 (рис. 17)і може використовувати його для відправки загрозливих повідомлень.

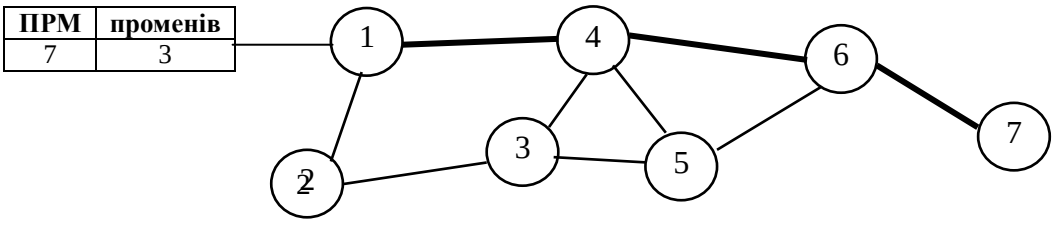



Рис. 17. Граф визначення оптимального маршруту від вузла 1

При цьому перший пакет даних буде затриманий до тих пір, поки не повернеться перший RREP.

Якщо необхідно проконтролювати зміну маршруту з вузла 1, то зміну маршруту можна бути виявити при:

пропажі періодичних повідомлень HELLO;

аварії на рівні зв'язності вузлів;

помилці передачі пакету до наступного променя (помилка може бути виявлена за допомогою прослуховування ретрансляції, якщо це кінцева точка призначення).

Вищестоящий (по напрямку до джерела) вузол, який виявив помилку, передає пакет помилкового маршруту (RERR) з новим послідовним номером місця призначення і кількістю променів. Джерело (або інший вузол маршруту) може знову побудувати шлях, передав пакет RREQ.

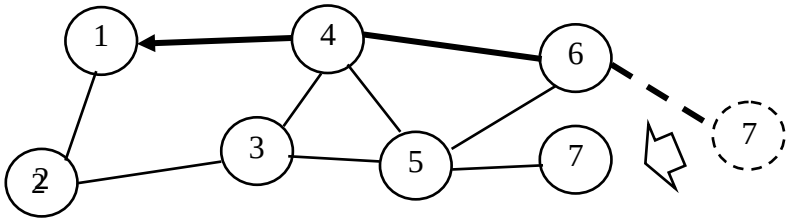



Рис. 18. Граф пошуку нового оптимального маршруту при отриманні вузлом 1 пакету RERR

Наприклад, як показано на рис. 18, припустимо, що вузол 7 змінив своє місце, і зв'язок вузлів 6-7 розірвався. Тоді вузол 6 посилає пакет RERR з вказівками зруйнованого маршруту. RERR розповсюджується у зворотному напрямку до вузла 1, який після цього повідомлення починає пошук нового маршруту.

**Висновки**

Запропоновані протоколи впроваджуються в мобільні мережі, які є, на сьогоднішній час, перспективними і призначені для надання інформаційних послуг в інтересах мобільних користувачів. Але питання захисту інформації базуються тільки на ідентифікації користувачів, вузлів, що є недоліком таких систем. Як видно з рисунків, які пояснюють дії протоколів, загрози, під виглядом відомого вузла спроможні, використовуючи протоколи автоматичної маршрутизації та пошуку оптимального маршруту, вільно просуватися до необхідного вузла, причому така маршрутизація сама допомагає загрозам виконати руйнівні дії всередині інформаційної системи.

Для запобігання таким діям необхідно запропонувати математичну модель взаємовідносин загроз та механізмів захисту системи захисту інформації з подальшою розробкою заходів по блокуванню загрозливим діям.

## ЛІТЕРАТУРА

1. C. Adjih, etal. "OptimizedLinkStateRoutingProtocol"IETF Internet Draft, draft-ietf-manet-olsr-08.txt, March 3, 2003.

2. P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot, "OptimizedLinkStateRoutingProtocolforAdHocNetworks," Proceedings IEEE INMIC, 2001, pp. 62-68.

3. Хамула С.М. Формалізація процесів захисту інформації в інформаційно-обчислювальних системах / С.М. Хамула, В.С. Ковбаса, Ю.Р. Кулинич. – Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – К.: 2003. – Вип. 7. – С. 113 – 117.

4. Лівінцев С.П. Математична модельзахисту інформації в автоматизованих мережах спеціального призначення / С.П. Лівінцев, І.М. Павлов, О.І. Романов. – Збірник наукових праць ВІТІ НТУУ "КПІ". – К.: 2004. – № 5. – С. 23 – 31.

5. Павлов І.М. Проектування комплексних систем захисту інформації / І.М. Павлов, В.О. Хорошко. – К.: 2011. – 245 с.

Надійшла: 18.11.2013р Рецензент: д.т.н., професор Олійник В.Ф