УДК 621.391

АТАКА «ЧОРНА ДІРА» В МЕРЕЖАХ MANET

Вовк А.В.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: anastasiavitaliivna@ukr.net

Black-Hole Attack in Mobile Ad-hoc Network

Were discussed the black hole attack problem in the mobile ad-hoc network. There are various techniques which have been proposed by the researcher for dealing with the black hole attacks and these techniques have been classified into various categories according to their basic operation.

В останні роки активно впроваджуються бездротові децентралізовані мережі з самоорганізацією, що складаються з мобільних пристроїв MANET (Mobile Ad-hoc Network). Кожен пристрій такої мережі може незалежно пересуватися в будь-яких напрямках, і, як наслідок, часто розривати та встановлювати зв'язок з сусідами.

Мережі MANET мають наступні переваги над бездротовими мережами традиційної архітектури:

- можливість передачі даних на великі відстані без збільшення потужності передавача;
- стійкість до змін в інфраструктурі мережі;
- можливість швидкої реконфігурації в умовах несприятливого середовища з завадами;
- простота і висока швидкість розгортання мережі.

Однак мобільність вузлів веде до додаткового підвищення динамічності топології мережі і, отже, до можливості обриву зв'язку через перешкоди або включення/виключення вузла додається ймовірність його переміщення. Окрім цього, існує загроза атак на систему, найбільш відома з них атака «чорна діра».

Black-Hole Attack відома, як атака нападу на систему, що серйозно погіршує продуктивність мережі. У цьому типі атаки у мережі може бути один легітимний вузол або кілька таких вузлів. Коли існує два або більше легітимних вузлів, які співпрацюють один з одним, щоб порушити зв'язок, вони називаються кооперативними атаками «чорної діри». Напад, започаткований справжнім вузлом, називається візантійськими атаками [1]. У звичайному протоколі AODV, коли джерелу потрібно зв'язатися з місцем призначенням, воно передає пакет запитів, якщо не має шляху до місця призначення. Вузол призначення відправляє назад пакет відповіді на отримання запиту маршруту від проміжного вузла. Але атаці «чорна діра», «чорний» вузол на отримання маршрутного запиту пакета посилає у відповідь пакет з неправдивою

інформацією, що має мінімальну кількість переходів у напрямку до місця призначення з дуже високим порядковим номером. Високий номер послідовності вказує на свіжість шляху. При отриманні пакета відповідей з шкідливого вузла, вихідний вузол починає передавати пакети даних з шляху, який містить шкідливий вузол, а потім цей зловмисний вузол починає скидати пакет даних. В мережі маршрут встановлюється на базі двох основних параметрів відповідних пакетів, які є порядковим номером вузла призначення та кількістю переходів. Вузли можуть поводитися по-різному, як представлено в таблиці 1, де 1 означає справжню інформацію, а 0 означає фальшиву інформацію [4].

Таблиця 1. Поведінка вузла при наявності атаки і без неї

Номер призначення	*Кількість переходів*	*«Падіння» пакету*	*Атака*	*Тип атаки*
1	1	Ні	Ні	Відсутня атака
0	0	Так	Так	Black-Hole
0	1	Так	Так	Black-Hole
1	0	Так	Так	Black-Hole
1	1	Так	Так	Gray-Hole

Існують різні методики, які були запропоновані багатьма дослідниками для боротьби з атакою Black-Hole в MANET. Ці методики були класифіковані у десять основних категорій:

- *Криптографічна схема*. Вона включає в себе всі ті рішення, в яких криптографічні технології, такі як симетрична ключова криптографія, цифровий підпис або хешування, використовуються для цілей шифрування, перевірки цілісності для забезпечення захисту мережі від можливих атак.

- *Підслуховуюча схема*. Вона складається з усіх рішень, в яких звичайні мобільні вузли можуть підслухати передачу свого сусіда, щоб перевірити його чесність. Якщо виявиться, що його сусідній вузол виконує деяку несподівану подію, вона буде розглядатися, як шкідливий вузол, а потім інформація поширюється в мережі.

- *Послідовна кількість порогової схеми*. У цій категорії вихідний вузол обчислює порогове значення вартості, використовуючи параметр номера послідовності вузла призначення відповідного пакета і скидає відповідний пакет, якщо він містить номер послідовності, що перевищує порогове значення. Пороговим значенням може бути статичний тип або динамічний тип.

- *Підтвердження на основі схеми*. У цій категорії відправляється пакет вузлу, що має підтвердити про вдалий прийом пакетів.

- *Кластеризована схема*. У цій схемі мережа розділена на кластер, в яких «головний» виявляє атаку чорної діри та повідомляє про це в мережі.

- *Крос-шарова схема співпраці*. У цьому розділі вона охоплює всі ті рішення, в яких більш, ніж два шари співпрацюють один з одним для виявлення шкідливої активність у мережі.

- *Схеми на основі перехресної перевірки*. У цій схемі перехресну перевірку виконує вихідний вузол з іншим вузлом так, щоб природу проміжного вузла можна виявити. Потрібно використовувати перехресну перевірку без даних таблиці DRI (даних маршрутизації) .

- *Схеми, засновані на довірі*. Він включає в себе рішення, які обчислюють довіру до вузла цінності на основі сусідньої передачі, яка допомагає у виявленні природи вузла, чи злочинець чи нормальний. Якщо довірче значення будь-якого вузла менше, ніж порогове, він вважається шкідливим, інакше - нормальним вузлом.

- *Схеми, основані на IDS*. Ця схема базується на спеціальних вузлах, які називаються IDS вузли, які мають можливість виявити зловмисну діяльність, підслуховуючи її біля передачі і коли виявлено будь-яку аномалію, вона передає повідомлення в мережі - ізолювати її.

- *Інші схеми*. У цій секції є багато рішень, які не підпадають під зазначені вище категорії. Крім цього деякі рішення базуються на механізмі кешування відповідей, повторюється наступний перехід на базі тощо[3].

Як правило, основним не правильним припущенням, яке відноситься до MANET, є те, що кожен вузол є довіреним вузлом. В реальному сценарії існують деякі ненадійні вузли, які виконують атаку «чорна діра», в якій неправильні вузли притягують весь трафік до себе, надаючи неправдиву інформацію про те, що він має мінімальний шлях до пункту призначення з дуже високим порядковим номером призначення та знижує всі пакети даних. Висвітлено різні категорії технік для пом'якшення впливу атаки Black-Hole, які необхідно розглянути під час розробки ефективного протоколу.

Література

1. A. R. Sangi, J. Liu, and L. Zou, “A performance analysis of AODV routing protocol under combined byzantine attacks in MANETs,” International Conference on Computational Intelligence and Software Engineering, pp. 1–5, 2009.
2. Метелёв А.П., Чистяков А.В., Жолобов А.Н. Протоколы муршрутизации в беспроводных самоорганизующихня сетях [Електронний ресурс] / Метельов А.П., Чистяков А.В. та інші. Режим доступу: https://cyberleninka.ru/article/v/protokoly-marshrutizatsii-v-besprovodnyh-samoorganizuyuschihsya-setyah.
3. Shashi Gurung, Siddhartha Chauhan A review of black-hole attack mitigation techniques and its drawbacks in Mobile Ad-hoc Network [Електронний ресурс] / Shashi Gurung, Siddhartha Chauhan Режим доступу: ieeexplore.ieee.org/document/8300186.
4. S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, “Prevention of cooperative black hole attack in wireless ad hoc net-works,” [Електронний ресурс] / S. Ramaswamy, H. Fu, M. Sreekantaradhya та інші Режим доступу: https://pdfs.semanticscholar.org/eff7/532e9de97faa4d746b0f37997baf67f68879.pdf.