УДК 621.396:004.056.5

к.т.н. Чевардін В.Є. (ВІТІ НТУУ „КПІ”)
Романюк А.В. (НТУУ „КПІ”)
Діянчук І.М. (ВІТІ НТУУ „КПІ”)

АНАЛІЗ ЗАГРОЗ БЕЗПЕКИ ІНФОРМАЦІЇ В МЕРЕЖАХ MANET

Забезпечення безпеки інформації в сучасних мережах MANET є актуальною науково-технічною проблемою. Способом її рішення є проведення постійного аналізу загроз безпеки MANET, а також розробка й вдосконалення механізмів забезпечення безпеки інформації в мережі. Проведено аналіз сучасних атак на мережі MANET та відповідних ним загроз безпеки інформації. Розглянуті недоліки та переваги протоколів безпечної маршрутизації. В результаті цього визначені перспективні напрямки вдосконалення та подальшого розвитку систем безпеки та протоколів безпечної маршрутизації в мережах MANET.

***Чевардин В.Е., Романюк А.В., Диянчук И.Н. Анализ угроз безопасности информации в сетях MANET.** Обеспечение безопасности информации в современных сетях MANET является актуальной научно-технической проблемой. Способом ее решения является проведение постоянного анализа угроз безопасности MANET, а также разработка и усовершенствование механизмов обеспечения безопасности информации в сети. Проведен анализ современных атак на сети MANET и соответствующих им угроз безопасности информации. Рассмотрены недостатки и преимущества протоколов безопасной маршрутизации. В результате этого определены перспективные направления усовершенствования и дальнейшего развития систем безопасности и протоколов безопасной маршрутизации в сетях MANET.*

***V. Chevardin, A. Romanyk, I. Dyanchuk Analysis of information security threats in MANET.** Ensuring information security in today's networks MANET is an urgent scientific and technological challenge. The way to solve it is to conduct a continuous review of security threats MANET, as well as the development and improvement of information security mechanisms in the network. The analysis of the attacks and their respective information security threats has been done. The shortcomings and advantages of secure routing protocols were done. As a result, identified promising areas of improvement and further development of security systems and secure routing protocols in networks MANET.*

***Ключові слова:** MANET, ad hoc мережа, механізми забезпечення безпеки в MANET, захист від атак на MANET, протоколи безпечної маршрутизації.*

1. Формулювання задачі

Сучасна військово-політична ситуація в світі, досвід останніх конфліктів показують, що вирішальним фактором у сучасній війні є інформаційна перевага. Для ефективного управління військами в сучасному військовому конфлікті необхідна мобільна, надійна та живуча інформаційно-телекомунікаційна мережа. Забезпечити зростаючі вимоги мереж військового призначення неможливо без використання децентралізованих радіомереж. Прикладом таких мереж є ad hoc мережі або мережі MANET [4, 5, 11 – 13]. Їх особливістю є використання однотипних засобів зв’язку (низьких за вартістю, низьких за енергоживленням, невеликих в розмірі та автономних), які забезпечують прийом, передачу інформаційних пакетів та їх ретрансляцію. Такі мережі позбавлені центрів управління мережею, авторизованих центрів генерації криптографічних ключів та видачі сертифікатів відкритих ключів.

Це, з однієї сторони, забезпечує гнучкість, життєвість телекомунікаційної мережі, а з іншої ускладнює маршрутизацію та забезпечення безпеки інформації в мережі. У зв’язку з цим, актуальним науковим завданням є розробка теоретичних основ щодо підвищення безпеки інформації в сучасних ad hoc мережах.

Питанням забезпечення безпеки інформації в ad hoc мережах присвячено багато робіт [2 – 5, 10, 11 – 19]. Багато підходів лягло в основу протоколів безпечної маршрутизації: *SAODV*, *TAODV*, *ARAN*, *SAR*, *SRP*, *SEAD*, *SLSP*, *CONFIDANT* та інші, які мають як переваги так і певні недоліки [3 – 5]. Є також ряд робіт, що містять пропозиції щодо вдосконалення та забезпечення безпеки алгоритмів маршрутизації повідомлень [21 – 24]. Однак відсутність сьогодні нормативної бази з побудови системи захисту інформації в сучасних ad hoc мережах створює ряд проблем в подальшому розвитку мереж MANET в нашої державі.

Метою роботи є аналіз існуючих загроз безпеки ad hoc мереж та виявлення проблеми її забезпечення, а також визначення перспектив подальшого розвитку методів забезпечення безпеки інформації в ad hoc мережах.

2. Аналіз існуючих робіт з підходами щодо захисту інформації в ad hoc мережах

Перед розглядом сучасних загроз безпеки інформації в ad hoc мережах представимо термінологію згідно чинного законодавства [6] (рис. 1).

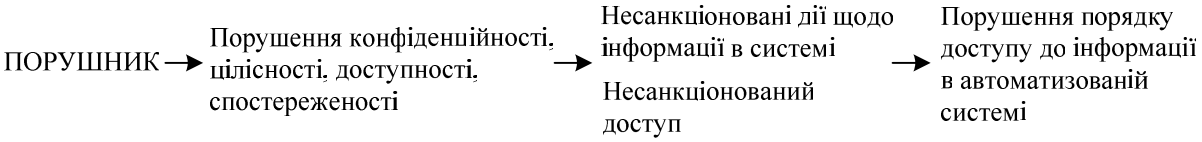

Рис. 1. Термінологічна структура досліджень

Загрозами безпеки інформації в сучасній автоматизованій системі вважаються несанкціоновані дії щодо інформації в системі та несанкціонований доступ до інформації. Для запобігання існуючих загроз розробляється модель порушника та модель загроз безпеки інформації, на основі яких визначаються основні вимоги (функціональні критерії) щодо захисту інформації та правил доступу до неї в системі, після чого визначаються механізми забезпечення безпеки інформації.

Несанкціоновані дії щодо інформації в системі – дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства.

Порядок доступу до інформації в системі – умови отримання користувачем можливості обробляти інформацію (виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів) в системі та правила обробки цієї інформації.

Несанкціонований доступ – доступ до інформації, що здійснюється з порушенням встановлених в АС правил розмежування доступу (одна з загроз безпеки інформації). Несанкціонований доступ до інформації може привести до витоку інформації, втрати інформації, підробки інформації, блокування інформації або порушення роботи автоматизованої системи.

В якості *порушника безпеки інформації* [9] вважається особа, яка може одержати доступ до роботи з засобами, включеними до складу комп’ютеризованої системи. Для аналізу використовують порушника четвертого рівня (фахівець вищої кваліфікації, який має повну інформацію про комп’ютерну систему і комплекс засобів захисту інформації).

Захист інформації в системі – діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі. Іншими словами, захист інформації спрямовано на забезпечення безпеки оброблюваної інформації і АС в цілому, тобто такого стану, який забезпечує збереження заданих властивостей інформації і АС, що її обробляє.

Згідно з постановою [7] будь-який план захисту інформації в системі включає до себе визначення моделі загроз для інформації в системі та визначення основних вимог (функціональних критеріїв) щодо захисту інформації та правил доступу до неї в системі.

Згідно з [8] функціональні критерії захищеності інформації розбиті на чотири групи, кожна з яких описує вимоги до послуг, що забезпечують захист від загроз одного із чотирьох основних типів (рис. 2) відповідно до певного виду інформації.

Усі існуючі атаки на ad hoc мережі реалізують одну або декілька наведених на рис.2 загроз. Наприклад атака людина по середині реалізується з порушенням конфіденційності та спостереженості.

Таким чином, враховуючи еквівалентність телекомунікаційних послуг, які надаються сучасними ad hoc мережами, послугам сучасних автоматизованих систем, доцільно оцінити існуючі загрози безпеки інформації в ad hoc мережах військового призначення в умовах динамічної зміни їх топології.

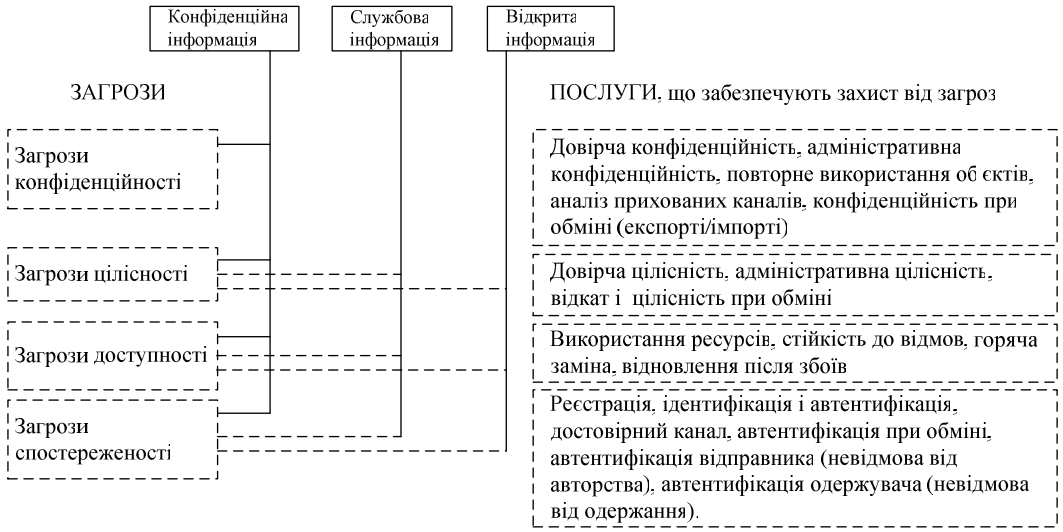

Рис. 2. Загрози безпеки інформації та відповідні послуги забезпечення захисту від них

Розглянемо ряд робіт, що присвячені забезпеченню безпеки інформації в сучасних ad hoc мережах. Так, сертифікати авторства та пов’язані з ними процедури детально розглянуті в роботах – [1, 11 – 13], ідентифікація в мережі на основі криптосистем та цифрових підписів у [1], ідентифікація в мережі на основі обміну ключами [14], схеми відкликання криптографічних ключів розглянуті у [15 – 19], протоколи безпечної маршрутизації проаналізовані у роботах [3, 21 – 24]. В цих роботах запропоновані аналітичні вирази для розрахунку імовірності проведення звичайних *Sybil*-атак та атак *l*-крокових вузлів у зговорі на мережу, які є сьогодні найбільш небезпечними атаками в мережах MANET. Враховуючи особливості динаміки змін топології мережі при проведенні сучасних військових операцій, імовірність атак *l*-крокових вузлів у зговорі на мережу зростає зі збільшенням кількості вузлів мережі та темпами проведення операцій. Це, в свою чергу, викликає необхідність якісної оцінки потенційних загроз мережі в усіх можливих умовах зміни її топології. Проведемо огляд сучасних загроз безпеки інформації в мережах MANET та існуючих протоколів безпечної маршрутизації.

3. Загрози безпеки інформації в мережах MANET

Характерною рисою ad hoc мереж військового призначення, в порівнянні зі звичайними телекомунікаційними мережами, є відсутність інфраструктури та довірчої третьої сторони (TTPs – Trusted third parties), що викликало необхідність реалізації послуг центрів генерації криптографічних ключів (KGC – key generation center) на кожному вузлі мережі. KGC забезпечує початкову безпеку вузла, автентифікацію та зміну криптографічних ключів вузла, відкликання існуючого ключа та генерацію нового ключа у випадку компрометації особистого ключа вузла мережі або проведення атак на ресурси мережі. Це вплинуло на збільшення в мережі процедур пов’язаних з генерацією та розповсюдженням криптографічних ключів, а також на необхідність використання додаткових процедур ідентифікації та автентифікації вузлів з метою запобігання атак на легальні вузли мережі. В таких умовах, існуючі підходи не завжди дозволяють забезпечити безпеку інформації в мережі з задовільною якістю обслуговування. Розглянемо особливості сучасних атак на мережі MANET та загрози безпеки інформації, які вони створюють.

За основною класифікацією протоколи маршрутизації розділяються на зондові протоколи та таблично-орієнтовані протоколи. Зондові протоколи працюють на основі розсилки зондів-запитів та отримання зондів-відповідей, тобто маршрутні таблиці змінюються тільки у випадку потреби. Це викликає затримки при передачі пакетів по мережі та іноді перевантаження вузлів [4, 5]. Таблично-орієнтовані протоколи працюють на основі коригування маршрутних таблиць, що відтворюється періодично або за графіком, на основі широкомовних маршрутних повідомлень, що викликає іноді перевантаження мережі

службовим трафіком [4, 5]. В деяких протоколах передбачено шифрування маршрутних пакетів для більш потужного захисту процедур маршрутизації в мережі.

Аналіз протоколів [4, 5] показав, що більш популярними протоколами є зондові протоколи: DSR, AODV, DSDV, OLSR. Однак недоліки цих проколів в умовах забезпечення безпеки інформації можуть викликати погіршення характеристик мережі в декілька разів. Однією з важливих характеристик протоколів маршрутизації є метрика (параметр) за якою працює протокол. Наприклад, метрики обрання маршруту, метрики збору інформації про мережу, метрики кількості маршрутів та інші. Кожна така метрики крім основного свого призначення потенційно створює основу для проведення певної атаки на мережу або її ресурси. Наприклад, метрики обрання маршрутів для найбільш розповсюджених протоколів наведені в табл. 1.

Таблиця 1

Метрика	Сутність метрики	Протоколи звичайної та безпечної маршрутизації
$\min(N_{hop})$	Обрання маршрутів з мінімальним числом кроків передачі пакетів, N_{hop}.	AODV, DSDV, OLSR, ZRP, DSR та інші
$\max(S_{ch})$	Обрання маршрутів з найбільшим значенням стабільності каналу зв’язку, S_{ch}.	SSR, MAP та інші
$\min(E)$	Обрання вузлів маршруту з найменшим значенням енергії випромінювання вузлів, E.	SPAN, FAR та інші
$\max(E_s)$	Обрання вузлів маршруту з найбільшим значенням енергії сигналу на вході приймача, E_s.	SSA, SSOD та інші
$N_o{}^j < N_o{}^{req}$, $tr_j > tr^{req}$	Обрання маршрутних вузлів з числа вузлів кількість обвинувачень в небезпечної поведінки вузла j, N_o^j менше припустимої границі та інші критерії безпеки.	SAODV, SAR, TAODV, SEAD, SRP, SLSP, ARAN, Ariadne SQoS Route Discovery, QoS Route Discovery, Confidant та інші

Кожна з метрик потенційно створює умови для проведення різноманітних атак. Найбільш популярні протоколи маршрутизації: AODV, DSDV, OLSR, ZRP, DSR, базуються на обранні маршрутів з мінімальною метрикою (мінімум кроків передачі пакетів в мережі). В зв’язку з чим, існує багато робіт присвячених аналізу вразливостей таких протоколів за рахунок створення хибних маршрутів зі зменшеною метрикою: чорна діра, сіра діра, біла діра [28 – 32]. Для аналізу загроз безпеки сучасним ad hoc мережам звернемо увагу на процеси передачі інформації в ad hoc мережі та процеси маршрутизації, що забезпечують її роботу (рис. 3).

Рис. 3. Потенційно небезпечні процеси в ad hoc мережі

Таким чином, на рис.3 наведені найбільш небезпечні процеси, що відбуваються в ad hoc мережах. Окреме забезпечення безпеки (конфіденційності – К, цілісності – Ц та доступності – Д) повідомлень в мережі не є великою проблемою, якщо використовувати сучасні криптографічні методи шифрування, забезпечення цілісності та автентичності

інформації. Однак, в умовах обмежень в часі передачі повідомлень, необхідності гарантувати доставку повідомлень адресатам, динамічності топології мережі та наявності активних та пасивних атакуючих вузлів забезпечення безпеки повідомлень становиться складною науково-технічною проблемою. Для визначення шляхів вирішення цієї проблеми проведемо аналіз існуючих атак проти ресурсів та процесів маршрутизації в мережі.

Усі атаки на ad hoc мережі можна розділити на пасивні та активні атаки (табл. 2). Перший тип реалізується на основі прослуховування трафіка мережі з метою виявлення потрібної інформації (у відкритому вигляді: конфіденційна інформація або будь-яка службова інформація), другий тип атак є результатом впливу на мережу („маскарад”, „повторення”, „введення повідомлення” – як частина атаки „чорної діри’, „модифікація повідомлення” або „фабрикування” – „людина по середині”, „видалення повідомлення”, „спуфінг”, „відмова в обслуговуванні”). Втрати від цих атак, або їх комбінацій можуть бути збільшені, якщо декілька вузлів вступають у зговір – так звані *Sybil*-атаки.

Таблиця 2

Атаки на ad hoc мережу		**Загроза безпеки**
Активні атаки		
Чорна діра / сіра діра (*blackhole-attack* / *grayhole-attack*)	Створення хибного маршрутного повідомлення зі зменшеною метрикою для введення в оману одного або групи легальних вузлів мережі. Зміна метрики для усіх маршрутів – чорна діра, для частини маршрутів – сіра діра. *Необхідні умови*: порушник має доступ до ідентифікаторів легальних вузлів та можливість створювати маршрутні повідомлення відповіді зі зменшеною метрикою, які приймає вузол-жертва.	Порушення процесів маршрутизації / порушення Ц, С
Біла діра (*wormhole attack*).	Створення маршруту (тунелю) для передачі повідомлень між двома вузлами різних сегментів мережі за рахунок зменшення метрик у маршрутних повідомленнях. При цьому вузли вважають себе сусідами. *Необхідні умови*: порушник має доступ до ідентифікаторів легальних вузлів та можливість створювати маршрутні повідомлення запити та відповіді зі зменшеною метрикою, які приймає пара вузлів-жертв.	Порушення процесів маршрутизації / порушення Ц, С
Людина по середині (*men-in-the-middle*)	Підробка ідентифікаторів легальних вузлів для введення в оману пари легальних вузлів мережі з метою отримання трафіка, який циркулює між цією парою вузлів. *Необхідні умови*: порушник має доступ до ідентифікаторів легальних вузлів та можливість передавати та приймати повідомлення між два віддаленими легальними вузлами.	Порушення процесів маршрутизації / порушення С, К
Ривок (*rushing attack*)	Підробка маршрутного повідомлення-відповіді та передача його легальному вузлу раніше ніж він отримує дійсне повідомлення-відповідь, що приводе до порушення процедури дослідження маршрутів. *Необхідні умови*: порушник має доступ до ідентифікаторів легальних вузлів та можливість створювати маршрутні повідомлення відповіді зі зменшеною метрикою, та передавати їх швидше за інших вузлів.	Порушення процесів маршрутизації / Ц, С
Фабрикація	Створюються нові маршрути до неіснуючих вузлів, за рахунок чого переповнюються маршрутні таблиці маршрутизації вузлів. *Необхідні умови*: порушник має доступ до ідентифікаторів легальних вузлів та можливість передавати довірчі маршрутні повідомлення одному з легальних вузлів.	Порушення процесів маршрутизації / С, Д
Спуфінг	Підробка ідентифікаторів з метою отримання прав існуючого легального користувача. Може привести до порушення доступності легального вузла мережі. *Необхідні умови*: порушник має можливість обробки ідентифікаторів легальних вузлів та можливість передавати довірчі маршрутні повідомлення від імені різних вузлів мережі одному певному легальному вузлу.	Порушення конфіденційності / Ц, Д
Атака на енергоресурс батареї вузла	Використовуються з великою частотою послуги певного вузла мережі з метою виснаження запасів його батареї. *Необхідні умови*: порушник не має обмежень на передачу повідомлень одним і тим маршрутом через певний вузол мережі, а також обмежень на кількість переданих повідомлень.	Порушення Д

*Продовження табл.*2

Атаки на ad hoc мережу		**Загроза безпеки**
Створення перешкод	Створення у каналі сторонніх шумоподібних сигналів. *Необхідні умови*: порушник має доступ до ідентифікаторів легальних вузлів та можливість передавати маршрутні повідомлення легальним вузлам.	Порушення Д
Впровадження повідомлень	Може використовуватись як частина *blackhole*-атаки. *Необхідні умови*: порушник має доступ до ідентифікаторів легальних вузлів та можливість аналізувати трафік між двома легальними вузлами мережі й створювати нові повідомлення від імені одного з них, додавати їх до складу дійсних пакетів адресованих іншому легальному вузлу.	Порушення процесів маршрутизації / Ц, Д
Модифікація повідомлень	Модифікація повідомлень. Може використовуватись як частина *MITM*-атак (*men-in-the-middle*) або *Sybil*-атак. *Необхідні умови*: порушник має доступ до ідентифікаторів легальних вузлів та можливість змінювати повідомлення, що передаються легальним вузлами.	Порушення процесів маршрутизації / Ц
Видалення повідомлень	Може використовуватись як частина атаки чорна діра, шляхом видалення повідомлень на певному маршруті або тих, що призначені певному адресату. *Необхідні умови*: порушник має доступ до ідентифікаторів легальних вузлів та можливість знищувати повідомлення між двома легальними вузлами.	Порушення процесів маршрутизації / Ц, Д
Dos-атака	Перевантаження вузлів маршрутними повідомленнями, що викликає використання більшої частини пропускної спроможності вузлів. *Необхідні умови*: порушник має доступ до ідентифікаторів легальних вузлів та можливість створювати потік запитів на отримання маршрутів до певних легальних вузлів. Не має обмежень на кількість повідомлень-запитів, що передаються від одного або групи вузлів.	Порушення процесів маршрутизації / Д
Пасивні атаки		
Визначення топології мережі	Аналіз широкомовних повідомлень з метою виявлення ланцюгів вузлів, якими передаються повідомлення. *Необхідні умови*: порушник має доступ до ідентифікаторів легальних вузлів та можливість аналізувати трафік між будь-якими легальними вузлами мережі.	Порушення К (якщо топологія прихована)
Жадібність	Використання не за призначенням пропускної спроможності мережі, що може привести до розряджання батареї певних вузлів мережі. *Необхідні умови*: порушник має можливість користуватись визначеними маршрутами без обмежень.	Порушення процесів маршрутизації / Д
Егоїстичність (*selfish behavior*)	Відмова в маршрутизації повідомлень з метою зберігання власних ресурсів батареї. *Необхідні умови*: порушник має можливість не представляти послуги маршрутизації та передачі повідомлень легальним вузлам мережі.	Порушення процесів маршрутизації / Д

В табл. 2 виділені жирним шрифтом атаки на мережу, які є базовими атаками для побудови більш складних та потужних атак на ad hoc мережі. Враховуючи необхідні умови для проведення відомих атак [2] можна виділити основні послуги, на яких повинні базуватись відомі протоколи безпечної маршрутизації та інші протоколи безпеки інформації в ad hoc мережах: послуга ідентифікації вузлів мережі, послуга автентифікації вузлів мережі, послуга конфіденційності, цілісності та доступності повідомлень, послуга доступності вузлів мережі, послуга спостереженості. Враховуючі особливості забезпечення кожної з цих послуг, створення універсального протоколу безпечної маршрутизації є досить складним завданням.

4. Протоколи безпечної маршрутизації

Сучасні протоколи безпечної маршрутизації в ad hoc мережах розділяються на три типи:

1) протоколи, що використовують криптографічні перетворення;
2) протоколи на основі моделі довіри;
3) гібридні протоколи захисту інформаційних ресурсів ad hoc мережі.

Якщо виділити найбільш розповсюджені протоколи маршрутизації: AODV, DSR, DSDV та ZRP, то недоліки існуючих протоколів безпечної маршрутизації можна представити таблицею 3.

У таблиці 3 усі найбільш розповсюджені протоколи забезпечення безпеки в ad hoc мережі згруповані за принципом побудови протоколу безпечної маршрутизації або на основі

криптографічних функцій або на основі моделі довіри та для кожного протоколу визначені переваги та недоліки з точки зору забезпечення безпеки інформації в мережі.

Таблиця 3

Протокол маршрут.	**Протокол безпечної маршрутизації**	**Основа протоколу**
AODV (Ad Hoc On-demand Distance Vector).	**SAODV –** криптографічне розширення протоколу AODV, на основі цифрових підписів для автентифікації RREQ та RREP, геш-ланцюги для автентифікації поля лічильника кроків передачі. *Захист* від атак: модифікація, спуфінг, фабрикування, біла діра. *Недоліки:* не виявляє егоїстичність.	криптографічні функції
	TAODV – розширення AODV на основі моделі довіри. Використовує аналіз свого оточення кожним вузлом. *Захист* від атак: модифікація, фабрикування, егоїстичність. *Недоліки:* не виявляє спуфінг та червоточину.	модель довіри
	SAR (security aware ad hoc routing). На відміну від AODV будуються маршрути на основі довіри до вузлів мережі. *Захист* від атак: модифікація, спуфінг, фабрикування. *Недоліки:* не виявляє егоїстичність та червоточину, крім того, кожен вузол на шляху прямування пакету повинен виконувати розшифрування та за шифрування пакету, що викликає затримки у передачі пакетів через мережу.	криптографічні функції
	ARAN (authenticated routing for ad hoc network) **–** є додатком протоколу AODV, що використовує автентифікацію маршрутних повідомлень на основі сертифікатів відкритих ключів. *Захист* від атак: модифікація, порушення цілісності, фабрикування. *Недоліки:* не виявляє егоїстичність та червоточину.	криптографічні функції
DSR (Dynamic Source Routing)	**SQoS Route Discovery –** використовує симетричні криптоперетворення для забезпечення безпеки процедур дослідження маршрутів, криптографічно захищена версія QoS Route Discovery. *Захист* від атак: модифікація, порушення цілісності, фабрикування, порушення конфіденційності. *Недоліки:* кожен вузол на шляху прямування використовує процедури розшифрування та зашифрування, що накладає додаткові обчислювальні витрати на вузли мережі та зменшує ресурси батареї вузла.	криптографічні функції
	Ariadne – використовує автентифікацію за протоколом TESLA – автентифікація на основі MAC-алгоритмів. *Захист* від атак: модифікація, спуфінг, фабрикування, біла діра. *Недоліки:* не виявляє егоїстичність.	криптографічні функції
	Confidant – використовує аналіз свого оточення кожним вузлом з показником $(R_s - R_f)/(R_s + R_f)$, де R_s, R_f – вдалі та невдалі події виявленні при спостереженні сусідів. $(R_s - R_f)/(R_s + R_f) = 1$ – повна довіра, $(R_s - R_f)/(R_s + R_f) = -1$ – повна недовіра. *Захист* від атак: егоїстичність. *Недоліки:* не виявляє модифікація, спуфінг, фабрикування, біла діра.	модель довіри
	QoS Route Discovery – використовує дерева довіри для дослідження маршрутів. *Захист* від атак: модифікація, порушення цілісності, фабрикування. *Недоліки:* не забезпечує конфіденційність процедур дослідження маршрутів мережі.	модель довіри
OLSR (Optimized Link State Routing)	**SLSP** (secure link state routing protocol). Протокол містить три рівня: розповсюдження відкритих ключів, дослідження сусідів, оновлення стану зв’язків. *Захист* від атак: модифікація, спуфінг, фабрикування. *Недоліки:* не виявляє червоточину та егоїстичність.	криптографічні функції

Продовження табл. 3

Протокол маршрут.	**Протокол безпечної маршрутизації**	**Основа протоколу**
ZRP (Zone Routing Protocol)	**SRP** (secure routing protocol for MANETs). Використовується захищене з’єднання між відправником i та отримувачем j на основі роздільного ключа $k_{i,j}$. Використовується заголовок QSEC|QID|MAC, де MAC забезпечує стійкість ідентифікації та автентифікації маршрутних повідомлень. *Захист* від атак: модифікація, спуфінг, фабрикування. *Недоліки:* не виявляє червоточину та егоїстичність.	криптографічні функції

З отриманих результатів порівняльної оцінки протоколів захисту інформації можна помітити, що будь-який протокол в умовах суттєвих обмежень роботи ad hoc мереж не дозволяє забезпечити безпеку інформації в мережі від усіх потенційних загроз. Існуючі протоколи безпечної маршрутизації не задовольняють підвищеним вимогам щодо швидкості обробки інформації та енерговитрат вузлів в сучасних мережах. Можливості протоколів безпечної маршрутизації не в змозі забезпечити захист від існуючих загроз безпеки інформації в MANET, якщо порушник не обмежений потужністю обчислювальних систем, а також може створювати групи вузлів у зговорі та здійснювати різні комбінації відомих атак.

Аналіз можливостей сучасних протоколів безпечної маршрутизації показав, що перспективний протокол безпечної маршрутизації повинен базуватись на моделі довіри та основі потужних криптографічних функцій. Для забезпечення конфіденційності, цілісності та доступності інформації в мережах MANET необхідно використовувати єдині бібліотеки криптографічних функцій, що дозволить знизити обчислювальні витрати вузлів на криптоперетворення. Прикладом існуючих бібліотек криптографічних функцій на еліптичних кривих, що використовуються в схемах генерації та розповсюдження криптографічних ключів для ad hoc мереж є TinyECC, NanoECC, TinyPBS [25 – 27].

Висновки

Таким чином, в результаті проведеного огляду протоколів безпечної маршрутизації, можна виділити протокол Ariadne, який не забезпечує захист тільки від атак егоїстичних вузлів, протокол SAODV, який не забезпечує захист від атак егоїстичних вузлів та атаки біла діра. Вдосконалити протокол SAODV можливо з використанням вдосконаленої техніки виявлення егоїстичних вузлів та атакуючих вузлів у зговорі. Забезпечити захист від розглянутих загроз можливо з використанням нових методів генерації та розповсюдження криптографічних ключів на основі криптоперетворень в групі точок еліптичної кривої. Ці перетворення є досить складними, що в умовах зростання трафіка може викликати суттєві затримки передачі повідомлень в мережі, тому їх реалізація потребує використання більш швидких алгоритмів аналізу оточення вузлів й алгоритмів генерації та відкликання криптографічних ключів.

Проведений огляд загроз безпеки інформації в ad hoc мережі дозволив виділити основні напрямки забезпечення безпеки – це захист від атак біла діра, людина по середині, фабрикація, спуфінг, модифікація повідомлень, егоїстичність. Забезпечити таких захист можливо з використанням системі криптографічних механізмів захисту від існуючих атак на мережу, яка включає:

– підсистему генерації, розповсюдження та відкликання криптографічних ключів;

– підсистему генерації та верифікації кодів автентифікації повідомлень;

– підсистему шифрування даних;

– підсистему дослідження та аналізу свого оточення;

– підсистему ідентифікації та автентифікації користувачів та вузлів мережі;

– підсистему виявлення атак на основі зговору сусідів.

Подальші дослідження будуть присвячені новим методам аналізу оточення вузла, процедурам забезпечення конфіденційності та причетності до побудови та замовлення маршрутів в ad hoc мережі, а також генерації та розповсюдженню криптографічних ключів на основі ізоморфних трансформацій точок еліптичних кривих [33, 34]. Розробка

теоретичних засад щодо створення протоколів на основі моделі довіри, стійкість яких еквівалентна рішенню теоретико-складних задач математики дозволить забезпечити безпеку інформації в ad hoc мережі с теоретично-доведеною стійкістю методів забезпечення безпеки інформації в MANET.

ЛІТЕРАТУРА

1. *Shamir A.* Identity Based Cryptosystems and Signature Schemes / A. Shamir // Proceedings of Advances in Cryptology – CRYPTO 1984, ser. LNCS 196, pp. 47 – 53, 1984.

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

3. *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.

4. *Миночкин А.И.* Многопутевая маршрутизация в мобильных радиосетях / Миночкин А.И., Романюк В.А. // Зв’язок. – 2004. – № 6. – С. 65 – 69.

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

6. *Закон України* «Про захист інформації в інформаційно-телекомунікаційних системах.

7. *Постанова* від 29 березня 2006 р. – №373. – Київ. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.

8. *НД ТЗІ 2.5-004-99.* Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу. Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, від “28” квітня 1999 р. – № 22. – Київ, 1999.

9. *НД ТЗІ 1.1-002-99.* Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу. Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, від “28” квітня 1999 р. – № 22. – Київ, 1999.

10. *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.

11. *Yi S.* MOCA: Mobile Certificate Authority for Wireless Ad Hoc Networks / S. Yi, and R. Kravets // Proceedings of the 2nd Annual PKI Research Workshop (PKI’03), pp. 65 – 79, 2003.

12. *Zhang Y.* Securing Mobile Ad Hoc Networks with Certificateless Public Keys / Y. Zhang, W. Liu, W. Lou, Y. Fang // IEEE Transactions on Dependable and Secure Computing, vol.3, no. 4, pp. 386 – 399, OCTOBERDECEMBER 2006.

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

14. *Hoeper K.* Identity-Based Key Exchange Protocols for Ad Hoc Networks / K. Hoeper, G. Gong // Proceedings of the Canadian Workshop on Information Theory (CWIT’05), pp. 127 – 130, 2005.

15. *Hoeper K.* Key Revocation for Identity-Based Schemes in Mobile Ad Hoc Networks / K. Hoeper, and G. Gong // Proceedings of the 5th International Conference on Ad-Hoc, Mobile, and Wireless Networks - ADHOC-NOW 2006, ser. LNCS 4104, pp. 224 – 237, 2006.

16. *Hoeper K.* Bootstrapping Security in Mobile Ad Hoc Networks Using Identity-Based Schemes with Key Revocation / Katrin Hoeper, Guang Gong // Security and Privacy for Emerging Areas in Communication Networks (SecureComm 06), 2006.

17. *Arboit G.* A Localized Certificate Revocation Scheme for Mobile Ad Hoc Networks / G. Arboit, C. Cr.epeau, C. R. Davis, and M. Maheswaran // Ad Hoc Network, vol.6, no.1, pp. 17 – 31, 2008.

18. *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.

19. *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.

20. *IEEE P 1609.2 Version 1* – Sitana for Wireless in Vehicelar Environment 2006. (Tomas Kung).

21. *Hu Y.C.* SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks / 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). – p. 3 – 13.

22. *Papadimitratos P.* Secure routing for mobile ad hoc networks / Papadimitratos P., Haas Z.J. // SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002) – San Antonio(TX, USA). – 2002.

23. *Venkatraman L.* Strategies for enhancing routing security in protocols for mobile ad hoc networks / Venkatraman L., Agrawal D.P. // Journal of Parallel and Distributed Computting. – 2003. – Vol.63. – №2. – pp. 214–227.

24. *Кулаков Ю.А.* Алгоритмы безопасной маршрутизации для мобильных компьютерных сетей / Кулаков Ю.А., Деревянчук А.О. // Проблеми інформатизації та управління, 3(27). – Київ – 2009.

25. *Malan D. J.* A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography / D. J. Malan, M. Welsh, and M. D. Smith // In First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks (IEEE SECON 2004), pp. 71 – 80. – 2004.

26. *Liu A.* TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks / A. Liu and P. Ning // In International Conference on Information Processing in Sensor Networks (IPSN ’08), pp. 245 – 256. – 2008.

27. *Szczechowiak P.* NanoECC: Testing the Limits of Elliptic Curve Cryptography in Sensor Networks / P. Szczechowiak, L. Oliveira, M. Scott, M. Collier, and R. Dahab // In Wireless sensor networks, pages 305 – 320. LNCS 4913. – 2008.

28. *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.

29. *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.

30. *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.

31. *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.

32. *Anderson R.* Key Infection: Smart Trust for Smart Dust / R. Anderson, H. Chan, and A. Perrig // In Proceedings of the 12th IEEE International Conference on Network Protocols (ICNP’04), pp. 206 – 215. – 2004.

33. *Chevardin V.* A pseudorandom bit generator based on elliptic curve transformations / V. Chevardin // Науково-технічний журнал “Радіоелектронні і комп’ютерні системи” № 5(57). Харків “ХАІ”. – 2012 р. – С. 48 – 50.

34. *Chevardin V.* Deterministic random bit generator on elliptic curve transformations / V. Chevardin // Modern problems of radio engineering, telecommunications and computer science: proceedings of the XIth international conference TCSET’2012. – Lviv-Slavske, Ukrain. – 2012. – p. 468.