5. Веплинг Л. Томсон. Л. Разработка Web-приложений с помощью PHP и MySQL, 2-е издание. – Издательский дом «Вильямс», 2003 – 800с.
6. Ноблес Р., Греди К., Эффективный Web-сайт: Учебное пособие – М: Издательство ТРИУМФ, 2004 – 560с.

Надійшла: 9.11.2012 р.

Рецензент: д.т.н., професор Юдін О.К.

УДК 621.396:004.056.523

Чевардін В.Є., Ізофатов Д.О.

АНАЛІЗ МЕХАНІЗМІВ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ТА АВТЕНТИЧНОСТІ ПОВІДОМЛЕНЬ В МЕРЕЖАХ MANET

Забезпечення цілісності та автентичності повідомлень в сучасних мережах MANET є актуальною науково-технічною проблемою. Способом її вирішення є проведення постійного аналізу загроз безпеки MANET, а також розробка й вдосконалення механізмів забезпечення цілісності та автентичності інформації в мережі. Проведено аналіз сучасних атак на мережі MANET та відповідних ним загроз цілісності та автентичності 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.

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 MANET або ad hoc мережі [1–5]. 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. Одними з найбільших загроз мереж MANET є загрози цілісності та спостереженості як відкритої так і службової інформації [6]. Характерною рисою таких мереж є відсутність центрів управління мережею, авторизованих центрів генерації криптографічних ключів та видачі сертифікатів відкритих ключів, які в свою чергу необхідні для механізмів забезпечення цілісності та спостереженості в сучасних автоматизованих системах. Механізмами забезпечення цілісності та спостереженості, що використовуються сьогодні в ad hoc мережах є алгоритми генерації та верифікації MAC-кодів (Message Authentication Code), безключові геш-функції SHA-256, SHA-384, SHA-512, RIPEMD-160, MDx, алгоритми автентифікації користувачів на основі рукопотискання, алгоритми автентифікації на основі електронного цифрового підпису DSA, ECDSA. Стійкість та надійність механізмів цілісності та спостереженості залежить від наступних показників: стійкість алгоритмів гешування до колізій та інших атак на геш-алгоритми, стійкість до зламу алгоритмів електронного цифрового підпису, стійкість алгоритмів рукопотискання, стійкість алгоритмів генерації та розповсюдження криптографічних ключів.

Питанням забезпечення безпеки інформації в ad hoc мережах присвячено багато робіт [1–5, 7–15]. 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 [1, 2, 8]. Слід зауважити, що в умовах розвитку сучасних інформаційно-телекомунікаційних технологій неможливо забезпечити безпеку мереж MANET без використання потужних алгоритмів автентифікації, генерації та розповсюдження криптографічних ключів. Відсутність сьогодні нормативної бази з побудови системи захисту інформації в сучасних ad hoc мережах створює ряд проблем в подальшому розвитку мереж MANET в нашій державі.

Метою роботи є аналіз існуючих загроз безпеки ad hoc мереж та механізмів забезпечення цілісності й спостереженості в ad hoc мережах з визначенням напрямків підвищення стійкості механізмів забезпечення цілісності та спостереженості для мереж MANET.

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

Перед розглядом сучасних загроз безпеки інформації в ad hoc мережах використаємо термінологію згідно чинного законодавства [16] (рис. 1).

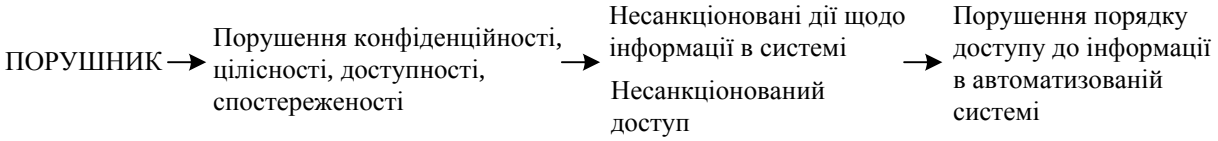

Рис. 1. Термінологічна структура досліджень

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.

Згідно з [6, 17] функціональні критерії, що використовують механізми автентифікації повідомлень, є цілісність та спостереженість. Ці критерії описують вимоги до послуг, що забезпечують захист від загроз цілісності та спостереженості (рис. 2) певному виду інформації. Послуги забезпечення цілісності при обміні реалізуються механізмами безключового гешування як корисних так і маршрутних повідомлень. Послуги забезпечення автентичності повідомлень при обміні реалізуються механізмами генерації та верифікації MAC-кодів.

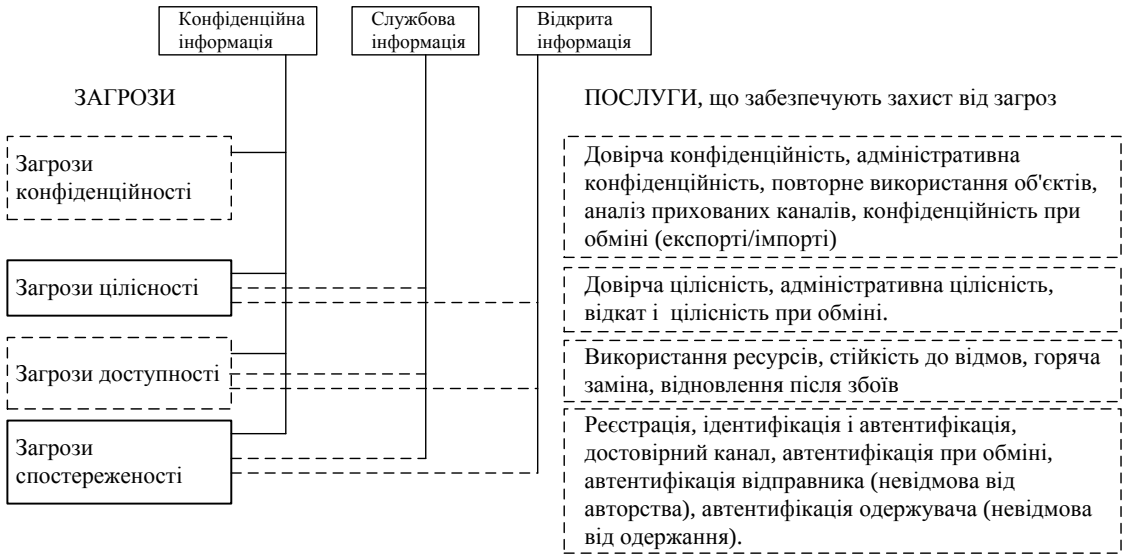

Рис. 2. Загрози безпеки інформації та відповідні послуги забезпечення захисту від них

Усі існуючі атаки на ad hoc мережі реалізують одну або декілька наведених на рис. 2 загроз. Наприклад атака людина посередині або Sybil-атака базується на основі підробки модифікації повідомлень, що є порушенням цілісності та спостереженості (рис. 2). Таким чином, враховуючі еквівалентність телекомунікаційних послуг, які надаються сучасними ad hoc мережами, послугам сучасних автоматизованих систем, доцільно оцінити існуючі загрози цілісності та спостереженості в мережах MANET.

Останні результати дослідження загроз та розробки нових підходів щодо забезпечення безпеки інформації в сучасних ad hoc мережах можна представити наступними роботами.

Так, сертифікати авторства та пов'язані з ними процедури детально розглянуті в роботах [3–5, 18], ідентифікація в мережі на основі криптосистем та цифрових підписів у [18], ідентифікація в мережі на основі обміну ключами [10], схеми відкликання криптографічних ключів розглянуті у [11–15], протоколи безпечної маршрутизації проаналізовані у роботах [8, 19–22], питання анонімності та автентифікації в мережі розглянуті в роботах [9, 23, 24], моделі безпеки Канетті та Кравчика розглянуті в [25], моделі Ламача [26]. З використанням існуючих результатів щодо розробки нових підходів до атак на ad hoc мережі проведемо огляд сучасних загроз безпеки інформації в мережах MANET.

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 [1, 2]. Таблично-орієнтовані протоколи працюють на основі коригування маршрутних таблиць, що відтворюються періодично або за графіком на основі широкомовних маршрутних повідомлень, що викликає, іноді, перевантаження мережі службовим трафіком [1, 2]. Кожне з таких повідомлень підписується на основі MAC-алгоритму, як правило це алгоритм UMAC, в зв'язку з чим стійкість автентифікації повідомлень визначена стійкістю алгоритму UMAC та алгоритмом генерації та розповсюдження криптографічних ключів. В деяких протоколах передбачено шифрування маршрутних пакетів для більш потужного захисту процедур маршрутизації в мережі.

Аналіз протоколів [1, 2] показав, що більш популярними протоколами є зондові протоколи: DSR, AODV, DSDV, OLSR кожний з яких використовує для підпису повідомлень алгоритм ключового гешування (MAC-алгоритм). Однак недоліки цих проколів в умовах забезпечення безпеки інформації можуть викликати погіршення характеристик мережі в декілька разів, що пов'язано з процедурою генерації та верифікації MAC-кодів.

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 [27–31]. 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).

Таким чином, на рис. 3. наведені найбільш небезпечні процеси, що відбуваються в ad hoc мережах. Окреме забезпечення автентичності 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 й пасивних атакуючих вузлів, забезпечення цілісності (Ц), конфіденційності (К), доступності (Д) та спостереженості (С) становиться складною науково-технічною задачею.

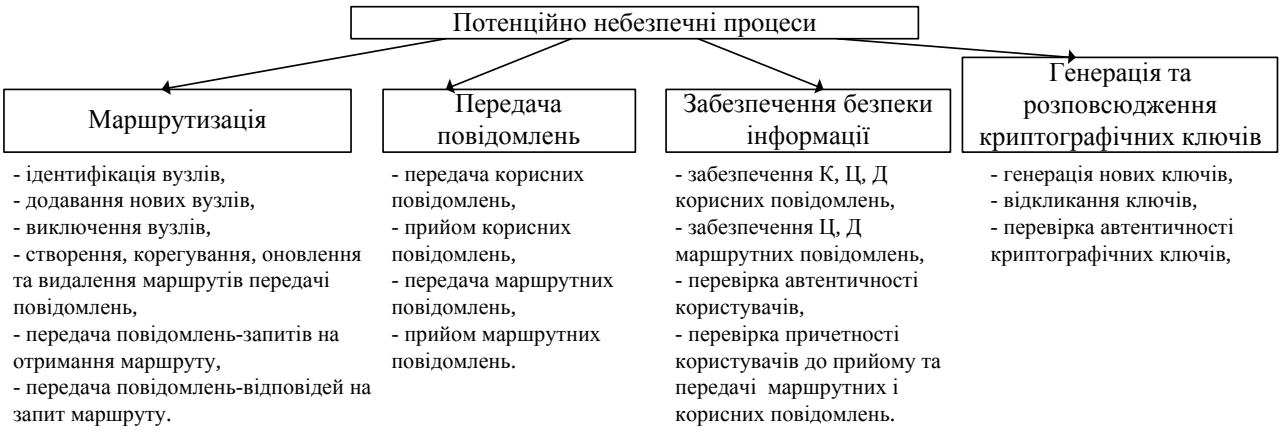

Рис. 3. Потенційно небезпечні процеси в ad hoc мережі

Для визначення шляхів вирішення цієї задачі проведемо аналіз існуючих атак проти ресурсів мережі та процесів маршрутизації, с позиції порушення цілісності та спостереженості. Усі атаки на ad hoc мережу розділяються на пасивні та активні (табл. 1).

Таблиця 1

Атаки на ad hoc мережу

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 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 Ц, С
Людина посередині (*men-in-the-middle*)	Підробка ідентифікаторів легальних вузлів для введення в оману пари легальних вузлів A та B в мережі з метою отримання трафіку, який циркулює між цією парою вузлів. Для цього генерується пара ключів K_{AC} та K_{CB} для розшифрування повідомлень, які передаються між вузлами A та B. *Необхідні умови*: порушник має доступ до ідентифікаторів легальних вузлів та можливість передавати та приймати повідомлення між два віддаленими легальними вузлами.	Порушення С, К
Ривок (*rushing attack*)	Підробка маршрутного повідомлення-відповіді та передача його легальному вузлу раніше ніж він отримує дійсне повідомлення-відповідь від легального вузла, що приводе до порушення процедури дослідження маршрутів та як наслідок процесу маршрутизації.	Порушення Ц, С

Продовження табл. 1

Атаки на ad hoc мережу		**Загроза безпеки**
Порушення процесів маршрутизації		
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 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 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
Створення перешкод	Створення у каналі сторонніх шумоподібних сигналів, що завдають перешкоду легальним вузлам при отриманні доступу до середовища. *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 аналізовувати 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 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 вузлам.	Порушення 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 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 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 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 Д

Перший тип реалізується на основі прослуховування трафіку 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 посередині”, “видалення повідомлення”, “спуфінг”, “відмова в обслуговуванні”). Втрати від цих атак можуть бути збільшені, якщо декілька вузлів вступають у зговір – так звані *Sybil*-атаки. На практиці ці атаки можуть використовуватись у комбінації.

В таблиці 1 виділені жирним шрифтом атаки на мережу, які є базовими атаками для побудови більш складних та потужних атак на ad hoc мережі. Для оцінки існуючих механізмів забезпечення цілісності та автентичності повідомлень представимо класифікацію методів автентифікації повідомлень (рис. 4).

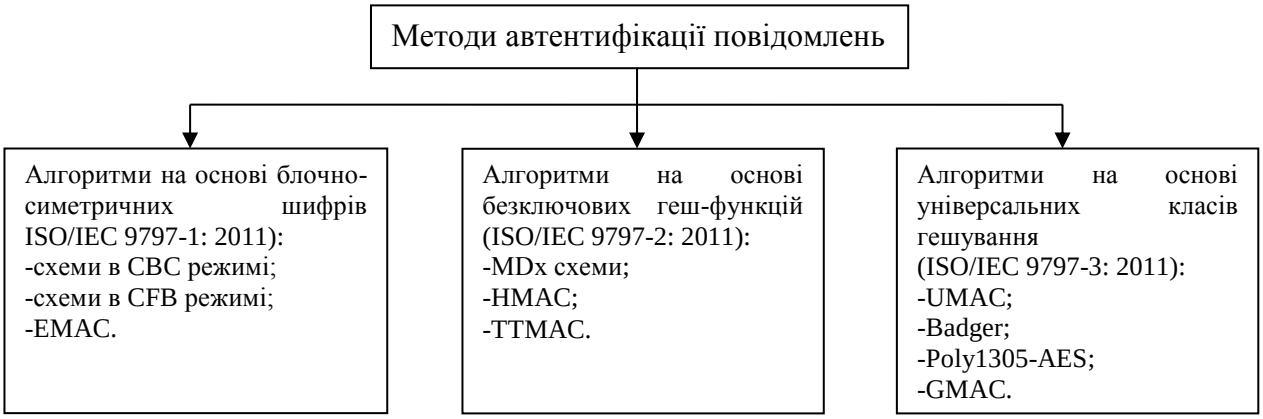

Рис. 4. Класифікація методів автентифікації повідомлень

Особливе місце серед усіх методів автентифікації повідомлень належить універсальним класам хешування, які дозволяють отримати теоретично доведену границю імовірності колізій. На рис. 5 наведена існуюча класифікація універсальних класів гешування.

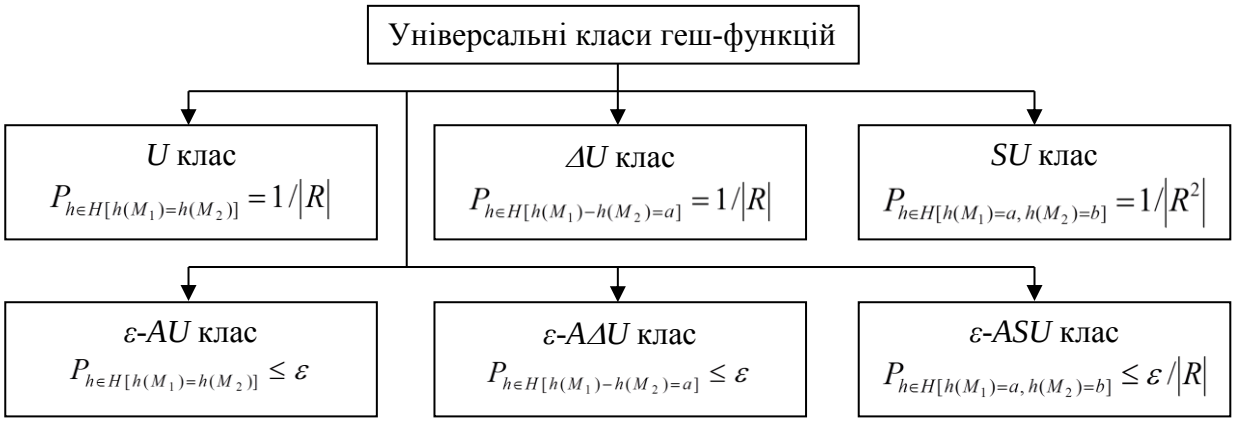

Рис. 5. Класифікація універсальних класів гешування

Аналіз існуючих результатів показав, що більш оптимальним з точки зору реалізації є ε-U та ΔU класи, ймовірність колізій для яких або обмежується значенням ε або знаходиться в межах $\varepsilon \pm \Delta$. Відмінна особливість універсальних класів гешування полягає у можливості теоретичного доказу статистично незалежного розподілу геш-кодів по множині первинних повідомлень, що дозволяє отримати зв’язок між розміром ключових даних та стійкістю до колізій для різних схем гешування. Одним з потужних алгоритмів ключового гешування на сьогодняшній день є алгоритм UMAC, який базується на 3 незалежних сімействах геш-функцій, що належать до універсальних класів гешування з ймовірністю виникнення колізій ε, що дорівнює 2^{-30}, 2^{-60}, 2^{-90} та 2^{-120} для UMAC-тегів довжиною 32, 64, 96 та 128 біт

відповідно [32]. Однак, криптографічна стійкість алгоритма UMAC визначена стійкістю його ключової функції, яка згідно чинного стандарту [32] реалізована на основі блочно-симетричних перетворень. Такий підхід дозволяє забезпечити лише обчислювальну стійкість алгоритму автентифікації, що не дає довготривалих гарантій в умовах постійного зростання потужності обчислювальних систем.

Аналіз підходів до побудови універсальних класів гешування дозволив виділити показники оцінки стійкості автентифікації та обчислювальних витрат на криптографічні перетворення для перспективних методів автентифікації: стійкість до колізій геш-функції, яка визначається показником універсального класу; стійкість алгоритму генерації раундових ключів для гешування; кількість примітивних операцій необхідних для здійснення одного раунду отримання значення геш-функції від повідомлення *M*; кількість примітивних операцій необхідних для отримання значення геш-функції від повідомлення *M*.

Збільшення рівня криптографічної стійкості методів гешування на основі універсальних класів є одним з найефективніших підходів до підвищення надійності та захищеності протоколів безпечної маршрутизації. Розглянемо сучасні протоколи безпечної маршрутизації, що використовують в якості механізмів забезпечення цілісності та автентичності повідомлень алгоритми ключового гешування UMAC або HMAC.

4. Протоколи безпечної маршрутизації

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

- протоколи, що використовують криптографічні перетворення;
- протоколи на основі моделі довіри;
- 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 2. У таблиці 2 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 2

Найбільш розповсюджені протоколи забезпечення безпеки в ad hoc мережі

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.	крипто-графічні 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 білу діру.	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 білу діру, крім того, кожен вузол на шляху прямування пакету повинен виконувати розшифрування та за шифрування пакету, що викликає затримки у передачі пакетів через мережу.	крипто-графічні 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 білу діру.	крипто-графічні функції

Продовження табл. 2

Протокол маршрут.	**Протокол безпечної маршрутизації**	**Основа протоколу**
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 модифікацію, спуфінг, фабрикування, білу діру.	модель довіри
	QoS Route Discovery – використовує дерева довіри для дослідження маршрутів. *Захист* від атак: модифікація, порушення цілісності, фабрикування. *Недоліки:* не забезпечує конфіденційність дослідження маршрутів мережі.	модель довіри
DSDV (Destination-Sequenced Distance Vector)	**SEAD** (secure link state routing protocol). Є додатком до протоколу DSDV, що використовує механізми автентифікації TESLA, HORS, TIK. Використовують однобічні геш-ланцюги для автентифікації оновлюючих маршрутних повідомлень: $h_0, h_1, h_2, .., h_n, h_0 = x = Random\_value$, $h_i = H(h_{i-1})$, $0 < i \le n$. Геш-ланцюг генерується кожним вузлом під час ініціалізації. Для перевірки кожної метрики, необхідно на основі отриманого відбитку h_{i-k}, $h_i = H_k(H_{k-1}..(H_{k-(k-1)}(h_{i-k}))..)$, що захищає метрики від модифікації. *Захист* від атак: модифікація, спуфінг, фабрикування, біла діра. *Недоліки:* не виявляє егоїстичність, викликає суттєві затримки у мережах з великою кількістю вузлів. Якщо зловмисник не змінює метрику оновлюючого повідомлення, через нього можуть бути передані маршрутні пакети.	криптографічні функції
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 білу діру та егоїстичність.	криптографічні функції
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 білу діру 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 мережі не дозволяє забезпечити гарантовану безпеку інформації в мережі від загроз цілісності та спостереженості. Сьогодні не має протоколів безпечної маршрутизації, що задовольняють підвищеним вимогам щодо швидкості обробки інформації та енерговитрат вузлів в сучасних мережах MANET. Сучасні можливості протоколів безпечної маршрутизації невзмозі забезпечити захист від існуючих загроз цілісності та спостереженості в MANET, якщо порушник не обмежений потужністю обчислювальних систем, а також може створювати групи вузлів у зговорі та здійснювати різні комбінації розглянутих атак. Аналіз можливостей сучасних протоколів безпечної маршрутизації показав, що перспективний протокол безпечної маршрутизації на основі моделі довіри повинен використовувати потужні криптографічні процедури генерації та верифікації MAC-кодів, стійкість яких є теоретично

доведеною. Протокол безпечної маршрутизації на основі криптографічних функцій повинен використовувати методи автентифікації повідомлень теоретично доведеної стійкості.

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 [33–35].

Висновки

Таким чином, в результаті проведеного аналізу можна виділити перспективні шляхи подальшого розвитку методів забезпечення цілісності та автентичності повідомлень в мережах MANET для підвищення захищеності протоколів безпечної маршрутизації. Так, перспективна система захисту інформації в MANET повинна включати в себе: 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 мережу.

На основі проведеного аналізу існуючих алгоритмів генерації кодів автентифікації були визначені показники оцінки їх якості та ефективності. В подальшій роботі планується вдосконалити існуючий алгоритм генерації та верифікації кодів автентичності повідомлень UMAC за рахунок використання криптоперетворень в групі точок еліптичної кривої, а також розглянути можливість побудови алгоритму UMAC з використанням в якості його ключової функції генератора псевдовипадкових послідовностей на основі перетворень в групі точок еліптичної кривої. Також планується розглянути можливість проведення аналізу оточення вузла з використанням криптографічних перетворень й генерації, а також розповсюдження криптографічних ключів на основі еліптичних кривих [36, 37].

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 з теоретично-доведеною стійкістю методів забезпечення безпеки інформації в MANET. Аналіз загроз безпеки інформації в ad hoc мережі дозволив виділити основні напрямки забезпечення безпеки – це захист від атак чорна діра, сіра діра, біла діра, людина посередині, фабрикація, спуфінг, модифікація повідомлень та егоїстичність. Розробка нових методів забезпечення цілісності та автентичності повідомлень в MANET дозволить підвищити надійність та криптографічну стійкість криптоперетворень в системах захисту інформації в MANET.

ЛІТЕРАТУРА

1. Миночкин А.И. Многопутевая маршрутизация в мобильных радиосетях / Миночкин А.И., Романюк В.А. // Зв'язок. – 2004. – № 6. – С. 65 – 69.
2. Миночкин А.И. Маршрутизация в мобильных радиосетях – проблема и пути решения / Миночкин А.И., Романюк В.А. // Зв'язок. – 2006. – № 7. – С. 49 – 55.
3. 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.
4. 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.
5. Anjum F. Security for Wireless Ad Hoc Networks / F. Anjum, P. Mouchtaris // John Wiley & Sons, Inc., Hoboken, New Jersey, 2007.
6. 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.
7. Xu Li. On Secure Mobile Ad hoc Routing / Xu Li, Amiya Nayak, Isabelle Ryl, David Simplot // Old City Publishing, Inc. Ottawa, Canada. 2007.
8. 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. PP.369 – 383.
9. Goldberg I. Anonymity and one-way authentication in key exchange protocols / Ian Goldberg, Douglas Stebila, Berkant Ustaoglu.

10. 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.
11. 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.
12. 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.
13. 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.
14. 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.
15. 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.
16. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах".
17. Постанова від 29 березня 2006 р. – №373. – Київ. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.
18. Shamir A. Identity Based Cryptosystems and Signature Schemes / A. Shamir // Proceedings of Advances in Cryptology – CRYPTO 1984, ser. LNCS 196, PP. 47 – 53, 1984.
19. 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.
20. 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.
21. 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.
22. Кулаков Ю.А. Алгоритмы безопасной маршрутизации для мобильных компьютерных сетей / Кулаков Ю.А., Деревянчук А.О. // Проблеми інформатизації та управління, 3 (27). – Київ – 2009.
23. Tor Project. Homepage, 2011. url: http://www.torproject.org/.
24. Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The second-generation onion router. In Proc. 13th USENIX Security Symposium. The USENIX Association, 2004. url: http://www.usenix.org/events/sec04/tech/dingledine.html/.
25. Ran Canetti and Hugo Krawczyk. Analysis of key-exchange protocols and their use for building secure channels. In Birgit Ptzmann, editor, Advances in Cryptology { Proc. EUROCRYPT 2001, LNCS, volume 2045, PP. 453-474. Springer, 2001. doi:10.1007/3-540-44987-6 28.
26. Brian LaMacchia, Kristin Lauter, and Anton Mityagin. Stronger security of authenticated key exchange. In Willy Susilo, Joseph K. Liu, and Yi Mu, editors, First International Conference on Provable Security (ProvSec) 2007, LNCS, volume 4784, PP. 1-16. Springer, 2007. doi:10.1007/978-3-540-75670-5 1.
27. 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.
28. 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.
29. 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.
30. 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.
31. 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.
32. ISO/IEC 9797-3: 2011. Information technology – Security techniques – Message Authentication Codes (MACs) – Part 3: Mechanisms using a universal hash-function.
33. 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.
34. 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.
35. 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, PP. 305 – 320. LNCS 4913. – 2008.
36. 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.
37. 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.

Надійшла: 03.10.2012 р.

Рецензент: д.т.н., професор Жуков І.А.