УДК 512.624.95

Чевардін В.Є.

МЕТОД БЕЗПЕЧНОЇ ДИСТАНЦІЙНО-ВЕКТОРНОЇ МАРШРУТИЗАЦІЇ ДЛЯ AD HOC МЕРЕЖ НА ОСНОВІ ПЕРЕТВОРЕНЬ У ГРУПІ ТОЧОК ЕЛІПТИЧНОЇ КРИВОЇ

Представлені результати аналізу протоколу безпечної маршрутизації SEAD. Визначені недоліки протоколу SEAD та методу побудови односпрямованих ланцюгів геш-дерев. Розроблений новий метод побудови ланцюгів дерев на основі перетворень у групі точок еліптичної кривої. В новому методі у якості односпрямованої функції використовується скалярний добуток точок еліптичної кривої. Це дозволило звести задачі зламу механізму ланцюгів дерев та зміни метрики маршрутних повідомлень до рішення задачі дискретного логарифмування у групі точок еліптичної кривої.

Ключеві слова: ad hoc мережа, протокол безпечної маршрутизації, геш-дерево, ланцюг геш-дерев, еліптична крива.

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 вже неможливо без використання децентралізованих радіомереж. Прикладом таких мереж є ad hoc мережі [1 – 2]. Їх особливістю є використання однотипних засобів зв'язку (низьких за вартістю та енергоживленням, невеликих у розмірі та автономних), які забезпечують прийом, передачу та ретрансляцію пакетів даних. Такі мережі позбавлені центрів управління мережею, авторизованих центрів генерації криптографічних ключів та видачі сертифікатів відкритих ключів. Це з одного боку забезпечує гнучкість, життєздатність телекомунікаційної мережі, а з іншого – ускладнює забезпечення безпеки інформації,циркулюючої в мережі. У зв'язку з цим, актуальним науковим завданням є розробка теоретичних основ щодо підвищення стійкості та надійності механізмів забезпечення безпеки інформації в сучасних ad hoc мережах.

Багато теоретичних підходів, що розглянуті в роботах [3-14], лягло в основу сучасних протоколів безпечної маршрутизації: *ARAN*, *SEAD*, *SAR*, *SRP*, *SLSP*, *BISS*, *IPsec*, *CONFIDANT* та інші, які мають як переваги так і певні недоліки. Одним з розповсюджених протоколів безпечної маршрутизації вважається протокол *SEAD* [12], автентифікація маршрутних оновлень в якому базується на механізмі побудови ланцюга геш-дерев [15]. *SEAD* є представником періодичних (проактивних) дистанційно-векторних протоколів, що використовують маршрутизацію на основі векторів відстаней. Обмежений енергоресурс роботи, обмежений об'єм пам'яті та невелика обчислювальна потужність створюють умови до появи нових потужних атак на інформаційні ресурси та процеси в мережі, що не дозволяє забезпечити ефективний захист з використанням класичних підходів.

Сучасні найбільш небезпечні атаки на маршрутні повідомлення (оновлення) в мережах ad hoc можна розділити на внутрішні та зовнішні. Зовнішні атаки: створення хибної маршрутної інформації, створення маршрутних петель, відокремлення частини мережі та її блокування створюються вузлами, що не належать мережі. Внутрішні атаки: створення хибної маршрутної інформації, модифікація переданих маршрутних повідомлень або знищення створюються скомпрометованими або завойованими вузлами та потребують подолання існуючих механізмів забезпечення безпеки в мережі, тобто є більш складними в реалізації. Загроза порушення цілісності маршрутної інформації (модифікація, створення нових або знищення маршрутних повідомлень) є однією з головних загроз безпеки процесів маршрутизації в мережах ad hoc.

Для захисту від визначених загроз цілісності маршрутних оновлень в протоколі *SEAD* передбачено використання методу побудови ланцюга геш-дерев Меркля, що забезпечує захист від зменшення метрики відстаней або створення хибних маршрутних оновлень с

існуючою метрикою. Однією з переваг цього методу вважається відсутність вимоги до наявності процедур синхронізації у часі усіх вузлів в мережі, що робить метод привабливим у використанні у великих мережах з гнучкою топологією. Однак, цей метод не позбавлений недоліків.

По-перше, це суттєве зростання числа процедур гешування у випадку його використання у великих мережах, що покращує умови проведення атак: відмова в обслуговуванні, розряджання батареї, егоїстичний вузол. Враховуючи, що базовий протокол *DSDV* використовує тригерні оновлення[1], при частих змінах топології мережі трафік це може викликати збільшення трафіку в мережі.Другим недоліком загальним для протоколів дистанційно-векторної маршрутизації є наявність петель. Для захисту від петель вводиться обмеження максимальної метрики в мережі, що іноді може викликати ускладнення в роботі великих мереж.Третім недоліком є залежність стійкості методу побудови ланцюга геш-дерев від стійкості алгоритму гешування, що вимагає постійного аналізу стійкості геш-функції та не дозволяє забезпечити теоретично доведену стійкість автентифікації в мережі.

Метою роботи є проведення аналізу механізму побудови ланцюга геш-дерев в протоколі *SEAD* для захисту від багато чисельних нескоординованих атак, що створюють некоректні маршрути та розробка нового методу безпечної маршрутизації на основі побудови ланцюга дерев Меркля з використанням перетворень в групі точок еліптичних кривих, що дозволить звести задачі зламу механізму забезпечення цілісності та автентичності маршрутних оновлень до рішення задачі дискретного логарифмування в групі точок еліптичної кривої.

Аналіз методу ланцюга геш-дерев Меркля. Використовуючи існуючі результати аналізу протоколу SEAD [12] детально розглянемо особливості побудови ланцюгів геш-дерев Меркля.

Забезпечення автентичності ключів протоколу SEAD. Основними проблемами сучасних протоколів основаних на векторах відстаней є створення маршрутних петель, створення хибних маршрутних повідомлень зі зменшеними значеннями метрики відстані, створення хибних повідомлень з найменшою існуючою метрикою. Ці проблеми можуть в певних умовах привести до відомих атак на мережу (Dos-атака, Wormhole-атака та інші [16 – 18]). У протоколі SEAD запропоновано ряд підходів щодо запобігання таких проблем з використанням ланцюгів геш-дерев Меркля. Відомо, що ланцюг геш-дерев складається із сукупності взаємопов'язаних та послідовно створених геш-дерев Меркля. Розглянемо властивості звичайного геш-ланцюга та ланцюга геш-дерев.

Забезпечення цілісності метрик протоколу SEAD на основі геш-ланцюгів. Структурні властивості геш-ланцюга дозволяють в однобічному порядку створювати власний ключ кожному вузлу, який з'являється в мережі, та перевіряти усім іншим вузлам його автентичність. Геш-ланцюг дозволяє забезпечити захист метрики d відповідного маршруту від спроб порушника його зменшити. Для захисту від створення маршрутних петель та повторення оновлюючих повідомлень використовують числові послідовності, які привласнюються кожному запису в таблиці та грають роль міток часу, тобто запис з більшою числовою послідовністю відповідає останній зміні певного маршруту. Також вводиться обмеження максимальне значення метрики маршруту $\max(d) = m - 1$. Між будь-якою парою вузлів створюється односпрямований геш-ланцюг для автентифікації метрик на кожному кроці передачі протягом всього шляху між вузлами i та j (рис. 1).

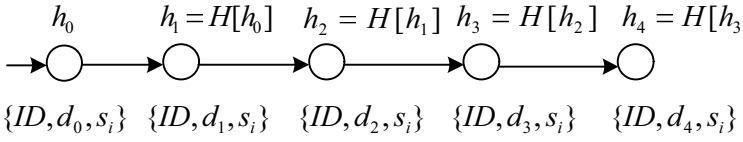

Рис. 1. Геш-ланцюг з п'яти елементів

[1] Тригерні оновлення – це маршрутні повідомлення, що передаються відразу після отримання оновлюючих повідомлень вузлом, які містять табличну інформацію стосовно вузлів-маршрутизаторів, які були змінені.

Для DSDV через кожен середньозважений проміжок часу вимагається відправляти для кожного призначення тригерне оновлення з найкращою метрикою для відповідної послідовності. Це зроблено для того щоб кожен вузол, розраховуючи середньозважене значення часу розсилання[2] чекав на отримання інших тригерних оновлень для певного маршруту та розсилав оновлення з найкращою метрикою. На відміну від нього SEAD використовує числові послідовності для визначення строку існування оновлення, тобто кожне оновлення, що містить зміни до існуючих метрик маршрутів містить новий порядковий номер повідомлення більшого за існуючий, ID = ID + 1. Тобто вузол, який отримує оновлення для існуючого в його таблиці маршруту, перевіряє отриману числову послідовність та у випадку, якщо воно перебільшує значення наявної послідовності, робить корекцію відповідного запису у своєї таблиці. Для захисту від петель використовують прапорці, які встановлюються у відповідному запису, коли отримано оновлення з мінімальною метрикою для певної числової послідовності та в подальшому оновлення для цієї послідовності ігноруються. Після власних змін у таблиці маршрутизації вузол передає далі оновлююче повідомлення, але для кожного запису в оновлюючому повідомленні він збільшує метрику на один крок, також додаючи до запису власне геш-значення зі свого геш-ланцюга.

Для забезпечення цілісності метрики маршруту кожен вузол використовує окремий наступний елемент свого геш-ланцюга у кожному маршрутному оновленні, яке він відправляє про себе (з метрикою 0). Геш-ланцюг забезпечує перевірку автентичності нижньої границі метрики для певного пункту призначення (вузла) в інших маршрутних оновленнях.

Властивість однобічності геш-ланцюга дозволяє забезпечити можливість зміни метрики тільки у більший бік у маршрутному оновленні. Практично, елемент з цього ланцюга, який використовується для автентифікації певного запису маршрутного оновлення, визначається метрикою, що міститься в цьому запису. Коли в SEAD відправляється маршрутне оновлення вузол включає одне геш-значення з кожним записом у маршрутній таблиці. За допомогою геш-значення, що отримує вузол з оновлюючого повідомлення, визначається маршрут до цього місця призначення. Якщо вузол створює запис про себе в оновлюючому повідомленні він встановлює у адресу відправника свою особисту адресу, нульову метрику, наступне значення своєї особистої числової послідовності та перший елемент свого геш-ланцюга, що зв'язаний з новою числовою послідовністю.

Приклад 1. Геш-ланцюг вузла представлений послідовністю $h_1, h_2, h_3, ..., h_n$, причому n ділиться на m. Для числової послідовності i в деякому записі маршрутного оновлення нехай значення $k = (n/m) - i$. Елемент цієї послідовності $h_{km}, h_{km+1}, h_{km+2}, .., h_{km+m-1}$ використовується для автентифікації цього запису. Якщо значення метрики j для цього запису знаходиться в межах $0 < j < m$, то значення h_{km+j} використовується для автентифікації числової послідовності цього запису у маршрутному повідомлені, тобто $\left\{d_0, s_i, h^{s_i}{}_{km+j}\right\}$. У цьому випадку, коли вузол передає маршрутне оновлення про себе, він передає числову послідовність i та геш-код h_{km}. Для інших місць призначень значення метрик та числових послідовностей вузол обчислює на основі власної маршрутної таблиці.

Вузли, що отримують оновлюючі повідомлення можуть легко автентифікувати їх кожний запис, скориставшись елементом геш-ланцюга, який знаходиться лівіше (рис. 1). Так, якщо вузол отримує оновлююче повідомлення від вузла призначення з ID_k, то використовуючи числову послідовність s_{i-1}, метрику d_{i-1}, відповідний геш-код h_{i-1}, які були отримані раніше від ID_k, та числову послідовність s_i, метрику d_i та відповідний геш-код h_i, які

[2] Середньозважене значення часу затримки розсилання – це середньозважене значення часу між отриманням вузлом першого оновлення для відповідного числового значення маршруту та отриманням оновлення з покращеним значенням метрики. Кожен вузол затримує на цей час отримане тригерне оновлення з надією отримати для цього числового значення оновлення з кращою метрикою та включити його до свого тригерного оновлення.

були отримані зараз від ID_k, він виконує гешування h_i певне число разів. Якщо виконується рівняння $H(h_i) = h_{i-1}$ отриманий запис вважається автентичним, інакше ігнорується.

Протокол SEAD також забезпечує захист адреси вузлів-передавачів, автентифікацію вузлів-передавачів, підтвердження відстані до передавача повідомлення та захист від інших атак на MAC – рівні з використанням симетричних криптографічних механізмів. В протоколі SEAD передбачена автентифікація однокрокових сусідів з використанням механізмів: TESLA, HORS, TIK в залежності від обраної політики безпеки. Це викликає додаткові обчислювальні витрати у випадках підвищення недовіри в мережі. У протоколі SEAD використовується ключ автентифікація для генерації MAC-кодів[3].

Однак звичайний механізм геш-ланцюга не дозволяє захистити вузли мережі від створення маршрутних повідомлень з однаковою метрикою, тобто атака з однаковими метриками. Для захисту від цієї атаки запропоновано використовувати ланцюги геш-дерев Меркля.

Забезпечення захисту від атаки з однаковими метриками на основі ланцюгів геш-дерев Меркля. Для запобігання можливості передавати порушнику вже передані повідомлення (клоновані – як ті, що він почув від сусідів) ідентифікатор відправника повідомлення також пов'язують з геш-значенням. Кожен елемент ланцюга геш-дерева кодує ідентифікатор вузла, тим самим примушує наступний вузол збільшити метрику щоб закодувати свій ідентифікатор.

На кожному кроці передачі ланцюг містить декілька значень для автентифікації певного вузла за допомогою дерева Меркля. А корінь дерева Меркля використовується для створення сукупності значень для автентифкації на наступному кроці. Цей підхід аналогічний реалізованому в схемі підпису HORS.

Розглянемо фрагмент ланцюга геш-дерев Меркля для захисту метрик відстаней від зменшення та клонування. На рис. 2. наведено ланцюг геш-дерев з трьох вузлів v_i, v_{i-1}, v_{i-2}. Зі значення v_i отримується множина значень b_0, b_1, …, b_n, як геш-функція $b_j = H[v_i \parallel j]$ для кожного j. На основі цих значень будується геш-дерево (дерево геш-значень) для автентифікації. Корінь геш-дерева стає початковим значенням ланцюга $v_{i-1=b_{0n}}$.

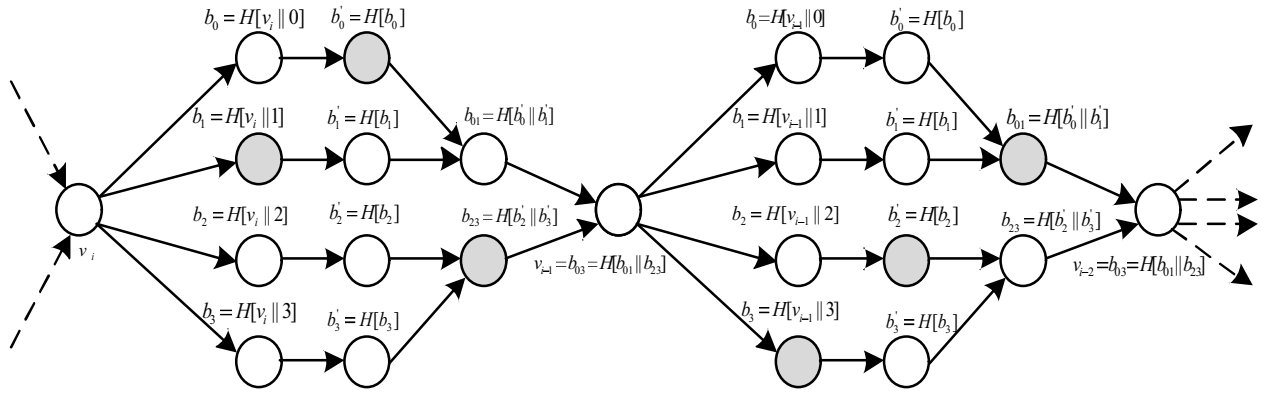

Рис. 2. Автентифікація на основі ланцюга геш-дерев: перша автентифікація за рахунок значень b_1, b_0', b_{23}; друга автентифікація за рахунок значень b_3, b_2', b_{01}

Приклад 2. Якщо вузол з ідентифікатором $i-1$ бажає перевірити автентичність ключа маршрутизатора з ідентифікатором 1 він використовуючи значення b_1, b_0', b_{23}, які йому надсилає власник v_1, здійснює перевірку умови $H[b_{23} \parallel H[b_0' \parallel H(b_1)]] = v_{i-1}$. У разі успішної верифікації вузол з ідентифікатором $i-1$ вважає що вузол з яким він обмінюється пакетами володіє автентичним ключем v_1.

[3] MAC-код – massage authenticated code – код автентифікації повідомлень або криптографічна геш-функція (ключова).

Якщо вузол з ідентифікатором $i-2$ бажає перевірити автентичність ближнього маршрутизатора з ID = 3, він за допомогою значень b_3, b_2', b_{01} здійснює перевірку $H[b_{01} \| H[b_2^{'} \| H(b_3)]] = v_{i-2}$. Аналогічно у разі успішної верифікації вузол з ідентифікатором $i-2$ вважає що вузол передавач володіє автентичним ключем v_3.

Таким чином, будь-який вузол може перевірити автентичність усіх своїх сусідів за допомогою дерева геш-значень. Для проведення автентифікації вузол отримує кортеж з трьох елементів, якщо урахувати сучасні вимоги до стійкості геш-функцій, то розмір геш-коду повинен бути не менш 256 бітів (SHA2-256), тобто розмір кортежу у такому випадку складе 1280 бітів. Для перевірки цілісності та справжності метрики маршрутного повідомлення вузлу достатньо значення якорю та кореневого значення ланцюга, що вимагає розміру кортежу 512 бітів.

Одним з головних показників методу ланцюгів дерев є висота дерева, яка залежить від кількості значень b_i, $i = 2^m$. З ростом числа m кількість операцій гешування на кожному кроці зростає, тому у великих мережах процедури обчислення та перевірки автентичності метрики відстаней можуть бути досить тривалими. Крім того, у великих мережах зростання кількості маршрутизаторів приводить до збільшення послідовності чисел, що використовуються для автентифікації, тобто використовуються γ - розмірні кортежі елементів геш-дерева.

На рис. 2 представлений ланцюг геш-дерев для випадку, коли число значень геш-дерева, що знаходиться між кожними двома значеннями геш-ланцюга є ступінь 2. Враховуючи той факт, що у великих мережах порушник може аналізувати кортежі елементів, що надходять до певного вузла від різних вузлів, та створювати своє власне тригерне оновлення з такою ж самою метрикою. Для захисту від подібних спроб порушника запропоновано кодувати ідентифікатори вузлів для кожного нового оновлення, що зводить ймовірність успіху порушника до найменшого значення. Або, якщо ідентифікатор вузла знаходиться у межах: $[0, \binom{2^m}{\gamma} - 1]$, то γ - значення (поточне значення ідентифікатора в конкретному оновленні) кодується $x = (ID + H[seq\_num] \bmod \binom{2^m}{\gamma}$. Для кожного seq_num γ - значення змінюється.

Перевищення перевірок автентифікаторів може бути викликане пропусканням декількох маршрутних оновлень. Порушник може примусити вузол-жертву виконувати процедури автентифікації зі складністю $O(ks)$, де k – максимальне число кроків передачі повідомлень, а s – максимальне число числових послідовностей, якими представлене геш-дерево. Для захисту від такої атаки запропоновано використання нового геш-ланцюга для кожної числової послідовності. Одним з варіантів для отримання кореня кожного дерева використовується псевдовипадкова функція f, $h_{0s} = f(K, s)$. Для проведення автентифікації створюють якір, $h_{k,s} = H^k[h_{0s}]$, де k – максимальна метрика. Будь-який вузол може перевірити автентичність числової послідовності s та метрики m, використовуючи геш-значення $h_{m,s}$.

Таким чином, для перевірки автентичності якоря $h_{k,s}$ кожен вузол будує своє власне геш-дерево. З кожним новим оновленням, з новим значенням s, він включає до повідомлення корінь геш-ланцюга $h_{0,s}$, якір геш-ланцюга $h_{k,s}$ та шлях до кореня геш-дерева. Для перевірки автентичності оновлення вузол перевіряє якір $h_{k,s}$, проходячи шлях до кореня геш-дерева, після цього перевіряє геш-значення $h_{k,s} = H^{k-m}[h_{m,s}]$. Враховуючи, що k – максимальна довжина геш-ланцюга, а перевірка якоря вимагає $O(\log(s))$ операцій, де s – число послідовностей, представлених будь-яким коренем, загальна складність обчислень для верифікації будь-якого оновлення обмежена $k + \log(s)$ операцій гешування. У великих

мережах границя $k+\log(s)$ може приймати досить велике значення, що додає великі часові затримки маршрутизації в мережі. Розглянемо можливість побудови нового односпрямованого ланцюга дерев на основі перетворень в групі точок еліптичної кривої.

Метод безпечної дистанційно-векторної маршрутизації на основі перетворень у групі точок еліптичної кривої. Крива E представлена множиною рішень (x, y) над полем F_p, що задовольняють рівнянню (1) разом з точкою на нескінченності, O. В залежності від порядку групи точок кривої, вона може бути або циклічною, або складатись з циклічних та нециклічних груп. На відміну від ланцюгів геш-дерев будемо використовувати дерево точок еліптичної кривої. Для цього зафіксуємо несуперсингулярну еліптичну криву E у афінній площині:

$$E: y^2 = x^3 + Ax + B, \mod p. \tag{1}$$

Для побудови методу безпечної маршрутизації в ad hoc мережі будемо використовувати тільки циклічні групи точок кривої E, тобто групи з простим порядком.

Нехай група точок кривої (1) E_p має простий порядок, $\#E_p$ – просте число.

Першою операцією для побудови дерева точок кривої буде буде скалярний добуток точки кривої:

$$P_j = k * Q = \sum_{i=1}^{k} Q_i., \tag{2}$$

де k – скаляр (ціле число); Q – базова точка кривої E.

Дерево точок еліптичної кривої представлено на рис. 3. Відкритими параметрами в мережі є базова точка Q, її порядок $\#Q$ та ціле число p (характеристика поля Галуа). Першим етапом побудови ланцюга дерев точок кривої є створення односпрямованого ланцюга на основі скалярного добутку точок кривої. Другим етапом є створення між кожною парою вузлів i та $i-1$ дерева точок кривої за рахунок розділення скалярного числа на n частин.

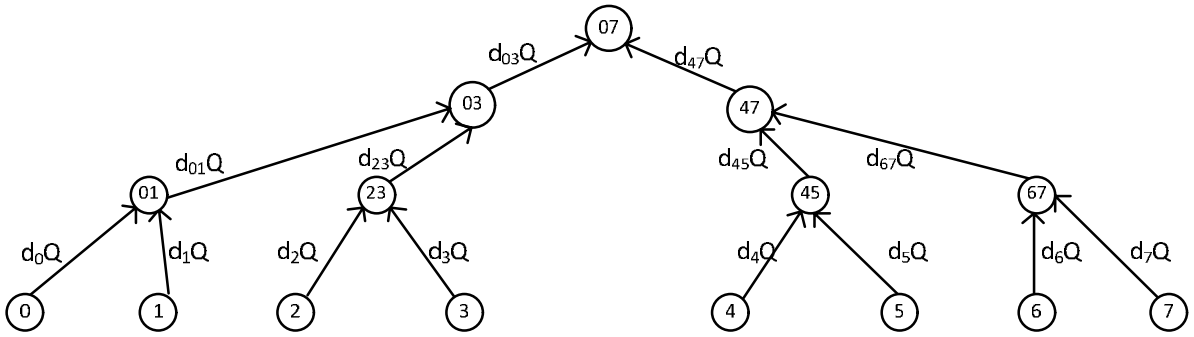

Рис. 3. Ієрархія значень дерева Меркля у новому методі безпечної маршрутизації в ad hoc мережі

Односпрямований ланцюг точок кривої. Для отримання односпрямованого ланцюга значень будемо використовувати операцію скалярного добутку причому на кожному кроці в якості скалярного значення буде використовуватись значення координати X на попередньому кроці:

$$P_i = X[P_{i-1}] * Q, \tag{3}$$

тобто ланцюг має вигляд:

$$P_0, P_1, ..., P_n = P_0, X[P_1] * Q, X[P_2] * Q, ..., X[P_{n-1}] * Q.$$

Таким чином, враховуючи властивості скалярного добутку точок кривої, задача порушника щодо відтворення попередніх значень елементів ланцюга по k відомим елементам, $P_r,...,P_{r+k}$, є задачею еквівалентною дискретному логарифмуванню в групі точок еліптичної кривої.

Односпрямований ланцюг дерев точок кривої. Для отримання дерева точок кривої використовується на кожному етапі ланцюга нове дерево точок кривої. Кореневий вузол (початковий) генерує базову точку кривої, точку Q_i, $\#Q = r$. Вузол генерує випадкове число $D_i < \#Q$. Далі виконується наступний алгоритм:

1. Вузол визначає кількість своїх однокрокових сусідів n.
2. Вузол розбиває ціле число D_i на n частин, $D_i = \sum_j d_{ij}$ та обчислює для кожного свого однокрокового сусіда його точку $P_{ij} = d_{ij} * Q$, після чого розсилає кожному з них P_{ij}.

3. Обробка точки вузлом. Кожен вузол отримуючи елементи дерева від дочірніх вузлів використовує односпрямоване перетворення (3), тобто:

- якщо вузол отримав точку від кореня дерева (кореневого вузла), $P_{i-1\,j}$, вузол використовує операцію (3) та передає далі результат скалярного добутку,

$$P_{ij} = X[P_{i-1\,j}]Q_i = X[d_{ij} * Q_i]Q_i;$$

- якщо вузол ij матиме декілька сусідів, (наприклад, другий рівень на рис. 3), то вузол додає усі точки, які він отримав від своїх однокрокових сусідів та помножує її на базову точку кривої

$$P_{ij} = X[P_{ij}']Q_i = X[\sum_j P_{i-1\,j}]Q_i.$$

4. Отримавши новий елемент дерева вузол i, j передає вузлу i+1, j кортеж елементів $\{P_{ij}, Q_i, P_{d_{\max}}\}$.

Таким чином, кожен вузол отримавши кортеж елементів ланцюга дерев точок кривої може перевірити метрику відповідного маршруту, а також упевнитись, що вузол який представив відповідні точки кривої дійсно є власником представленого ключа.

Приклад 3. Нехай обрана крива (1) над простим полем Галуа. Порядок циклічної групи точок є простим числом r, $\#Q = $ r. На початку ланцюга початковий вузол генерує базову точку кривої Q, порядку r, та обчислює для максимальної метрики $d_{\max}$ відповідну точку ланцюга:

$$P_{d_{\max}} = \underbrace{X[X[X[P_{i-1}]*Q]*Q...]*Q}_{d_{\max}} = \prod_{i=1}^{d_{\max}} X[P_{i-1}]*Q.$$

Маючи j однокрокових сусідів він генерує випадкові числа, що задовольняють умові $\sum_j d_{1\,j} = X[Q_i]$. Після чого для кожного з них початковий вузол обчислює точку кривої: $P_{ij} = d_{ij} * Q_i$ та відправляє кортеж $\{P_{ij}, Q_i\}$. Кожен наступний вузол отримує кортежі елементів від своїх однокрокових сусідів та обчислює $P_{ij} = X[P_{ij}']Q_i = X[\sum_{j=1,k} P_{i-1\,j}]Q_i$. Після чого відправляє також кортеж $\{P_{ij}, Q_i\}$.

Коли вузол 07 (рис. 3) забажає перевірити автентичність ключа вузла 2, він запитує автентифікаційні дані (новий кортеж елементів: $\{P_3, P_{01}, P_{47}\}$) та виконує перевірку рівняння (4). У випадку успіху вузол 07 визначає, що вузол 2 дійсно є власником ключа d_2.

$$P_{07} = X[P_{47} + X[P_{01} + X[P_2 + P_3]*Q_i]*Q_i]*Q_i. \quad (4)$$

Для перевірки цілісності та справжності метрики маршрутного повідомлення використовується кортеж елементів $\{P_{ij}, Q_i\}$. Якщо значення метрики d_i у маршрутному повідомленні і задовольняє умові

$$Q_{d_{\max}} = \underbrace{X[...X[X[P_{i-1}]*Q]*Q...]*Q}_{d_{\max}-i},$$

метрика вважається цілісною та справжньою.

Враховуючи, можливість стискання точок кривої можна зменшити розмір кортежу, та передавати координату X та індекс точки кривої (біт парності), тобто в маршрутному повідомленні можна передавати стиснуте значення точки кривої (X, ind). З урахуванням сучасних вимог до криптографічної стійкості мінімальний розмір характеристики поля Галуа потрібний бути не менше 163 біти, у такому випадку розмір звичайного кортежу елементів ланцюга дерев точок буде 328 бітів, що дозволяє зменшити надлишковість автентифікаційної інформації у 1.56 разів. Розмір кортежу для автентифікації буде 817 бітів, що дозволяє зменшити надлишковість автентифікаційної інформації у 1.56 разів.

Висновки. Таким чином, у результаті проведеного аналізу ланцюга геш-дерев Меркля та розробленого на його основі протоколу безпечної маршрутизації SEAD, було визначено ряд недоліків, які ускладнюють застосування SEAD в умовах підвищеної динаміки змін топології мережі ad hoc, а також в умовах частих поява нових вузлів. Крім того, одним зі слабких місць дерева Меркля є використання геш-функцій, що висуває додаткову вимогу на вибір стійкої геш-функції. В новому методі побудови ланцюга дерев Меркля на основі перетворень в групі точок еліптичної кривої використовується в якості односпрямованої функції скалярний добуток точки еліптичної кривої, причому скаляр отримується як частина точки попереднього кроку побудови геш-ланцюга. Це дозволило, звести задачу відтворення попередніх елементів ланцюга до рішення задачі дискретного логарифмування в групі точок еліптичної кривої. Також спроби порушника змінити метрику маршрутних повідомлень з використанням нового методу зводяться до вирішення ним задачі дискретного логарифмування. Враховуючи існуючі програмні бібліотеки операцій в групі точок еліптичної кривої для апаратно-програмних маршрутизаторів мережі ad hoc [19 – 21], реалізувати новий метод безпечної маршрутизації є реальним в найближчий час.

ЛІТЕРАТУРА

1. *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.

2. *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.

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

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

5. *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.

6. *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.

7. *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.

8. *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.

9. *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.

10. *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.

11. *IEEE 1609.2* – 2006 – Trial Use Standard for Wireless Access in Vehicular Environments (WAVE) – Security Services for Applications and Management Messages

12. *Hu Y.C.* SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks / Hu Y.C., Johnson D. B., Perrig A. // Ad Hoc Networks 1 (2003). – 2003. – P. 175 – 192.

13. *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.

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

15. *Merkle R.* Protocols for public key cryptosystems, in: 1980 IEEE / Merkle R. // Symposium on Security and Privacy, 1980.

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

17. *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), pages 494 – 503, 2007.

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

19. *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), pages 71 – 80, 2004.

20. *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), pages 245 – 256, 2008.

21. *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.

Надійшла: 12.08.2012р.

Рецензент: д.т.н., проф. Ленков С.В.