УДК 004.722.2, 004.056.5

В.М. Сокіл
Національний університет "Львівська політехніка",
кафедра електронних обчислювальних машин

СИСТЕМА ФОРМУВАННЯ РЕАКЦІЙ ВУЗЛІВ ДЕЦЕНТРАЛІЗОВАНИХ МОБІЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖ ДИНАМІЧНОЇ СТРУКТУРИ

На основі розробленої моделі довіри в інформаційних системах побудовано нову систему формування реакцій вузлів децентралізованих мобільних комп'ютерних мереж динамічної структури.

New system for generation of reactions of mobile ad-hoc networks' nodes, based on new model of trust in information systems, was developed.

Вступ. Дослідження різних аспектів побудови, функціонування та застосування децентралізованих мобільних комп'ютерних мереж динамічної структури (ДМКМДС) має більш ніж 30-річну історію [1]. Роботи з організації та використання радіомереж з пакетним передаванням даних почали проводились ще в 70-х роках XX століття. Початок XXI століття відзначається появою достатньо продуктивних, малогабаритних обчислювальних і вимірювальних засобів, та стрімким розвитком бездротових технологій передавання даних [2]. Ці фактори дають можливість широко застосовувати ДМКМДС для розв'язання різного типу завдань.

Особливостями ДМКМДС є функціонування в умовах відсутності центрального керування та жорстко фіксованої інфраструктури, бездротові зв'язки між вузлами для забезпечення їх мобільності та обмежені обчислювальні ресурси самих вузлів [3]. Мережі класу ДМКМДС, окрім військової, можуть використовуватись у таких галузях, як рятувальні роботи у зонах стихійних та техногенних лих, дослідження навколишнього середовища за допомогою мереж сенсорів, або забезпечення зв'язку між транспортними засобами або людьми у разі відсутності інших засобів комунікації [4].

Аналіз останніх публікацій. Основна увага у попередніх дослідженнях та під час побудови ДМКМДС, якими займалися Ж.-П. Хубаукс, К. Нарстедт, Я. Чакерез, А. Сігал та інші, була приділена розробці структур складових частин вузлів мереж, бездротовим технологіям передавання даних, протоколам мережевої та транспортної взаємодії, криптографічному закриттю інформації тощо [5–7]. Проте децентралізовані мобільні комп'ютерні мережі динамічної структури є малодослідженими з точки зору безпеки взаємодії вузлів таких мереж на прикладному рівні, а особливо питання перевірки допустимості проведення інформаційної взаємодії.

Постановка завдання. Оскільки ДМКМДС є децентралізованою системою, то рішення стосовно реакції на запити щодо проведення інформаційної взаємодії у певній ситуації приймаються самими вузлами мережі [8]. Враховуючи специфіку галузей застосування ДМКМДС, існує висока імовірність знищення або компрометації окремих вузлів таких мереж. Отже, для того, щоби ДМКМДС могла ефективно функціонувати, під час її побудови необхідне застосування засобів формування реакцій, які здатні адаптуватись в умовах швидкої зміни структури мережі та виявляти і належно реагувати на зміни поведінки вузлів мережі.

Функціонування класичних мереж з централізованим керуванням передбачає прийняття рішення щодо початку інформаційної взаємодії з певним вузлом на основі двох факторів: результату перевірки, чи справді вузол є тим, за кого він себе видає, тобто аутентифікацією, та політики безпеки [9]. Політика безпеки – це чітка та централізовано керована сукупність реакцій вузла на

запити щодо проведення інформаційної взаємодії у тій чи іншій ситуації. Якщо вузол успішно пройшов аутентифікацію, а також, згідно з політикою безпеки, отримав дозвіл на взаємодію, то взаємодія відбувається.

Застосування такого підходу для ДМКМДС, очевидно, майже унеможливлюється де централізованістю та вимогою адаптивності. За таких умов, під час оцінювання вузла на предмет допустимості інформаційної взаємодії, поряд з аутентифікацією виникає ще окреме питання довіри до вузла. Рішення відносно інформаційної взаємодії відбувається з урахуванням результату антентифікації та оцінки вузла з точки зору рівня довіри до нього. Сьогодні відомо декілька моделей визначення рівнів довіри [10–12], які дають змогу встановлювати нові та модифікувати наявні відношення довіри залежно від зміни структури мережі. Проте такі моделі не містять механізмів виявлення змін поведінки вузлів мережі, а тому не можуть адаптуватися до них.

Модель довіри в децентралізованих мобільних комп'ютерних мережах динамічної структури

Модель довіри в ДМКМДС та децентралізована адаптивна модель визначення адекватного рівня довіри ґрунтуються на концепції довіри в інформаційних системах, розробленій Е. Джерком [13]. Відповідно до цієї концепції довіра розглядається як впевненість одного об'єкта у поведінці іншого об'єкта стосовно певного предмета X на проміжку часу T: $A \xrightarrow[T]{X} B$. Відношення довіри застосовуються між двома вузлами та мають такі властивості: асиметричність $A \xrightarrow[T]{X} B \neq B \xrightarrow[T]{X} A$; нетранзитивність $\left(A \xrightarrow[T]{X} B \wedge B \xrightarrow[T]{X} C\right) \neq A \xrightarrow[T]{X} C$; недистрибутивність $A \xrightarrow[T]{X} \left(B \wedge C\right) \neq A \xrightarrow[T]{X} B \wedge A \xrightarrow[T]{X} C$; неасоціативність $\left(A \xrightarrow[T]{X} B \wedge A \xrightarrow[T]{X} C\right) \neq \neq A \xrightarrow[T]{X} \left(B \wedge C\right)$.

Згідно з загальною концепцією довіри відношення довіри між вузлами можна розглядати тільки в межах певного типу, або категорії взаємодії. Для відображення цього положення в модель введена скінченна множина категорій прикладної інформаційної взаємодії TC_A. Ця множина складається з усіх можливих категорії взаємодії між вузлами мережі для нормального її функціонування – $TC_A = \{ tc_1, tc_2 \ldots tc_n \}$, де tc – унікальний ідентифікатор категорії взаємодії.

Кожна з категорій взаємодії має такі характеристики:

- TV_{SC}^{tc} – мінімальний рівень довіри для оцінки вузла як "надійного" в межах категорії взаємодії tc; під "надійним" розуміється вузол, якому може бути передана або від якого може бути отримана інформація, тобто, ця характеристика відображає мінімальний рівень довіри для початку інформаційної взаємодії;
- TV_{CI}^{tc} – мінімальний рівень довіри для оцінки вузла як "компетентного" в межах категорії взаємодії tc; під "компетентним" розуміється вузол, інформація від якого вважається адекватною до дійсності, тобто правдивою.

Відповідно до другої властивості, відношення довіри є нетранзитивним, тому такий тип відношень не забезпечує встановлення нових відношень довіри під час взаємодії вузлів один з одним внаслідок побудови транзитивних ланцюжків довіри. Основним засобом встановлення нових відношень довіри є механізм рекомендацій. Такий механізм дає змогу встановити нове відношення довіри до вузла за відсутності інформації про попередню взаємодію з цим вузлом за рахунок рекомендацій, тобто інформації, отриманої про нього від інших вузлів. Для забезпечення можливості використання механізму рекомендацій застосовується додаткова характеристика категорії взаємодії TV_{MIN}^{tcr}, яка відображає мінімальний рівень довіри для використання рекомендацій від інших вузлів, та вводиться додаткова множина, що має назву множина рекомендацій $TC_R = \{ tcr \}$. Ця множина складається з одного елемента – категорії рекомендації. Загальна множина категорій довіри TC є об'єднанням множини категорій прикладної інформаційної взаємодії TC_A та множини рекомендацій TC_R, тобто $TC = TC_A \cup TC_R$.

Основні характеристики відношення довіри є: рівень довіри та часова функція довіри. Рівень довіри є кількісною характеристикою відношення довіри. Він визначається як вектор $TV_{ID} = \left[TV_{ID}^{tc_0}, \ \ldots \ , TV_{ID}^{tc_n}, \ TV_{ID}^{tcr} \right]$, $TV_{ID}^{tc_i} \in [0 \ldots 1)$, кожен елемент якого відображає рівень довіри до вузла з ідентифікатором ID стосовно визначеної категорії взаємодії tc_i. Часова функція відображає зміну в часі рівня довіри в існуючому відношенні довіри. На базі моделі відношення довіри побудовано нову децентралізовану модель визначення адекватного рівня довіри, що володіє властивістю адаптивності у двох складових:

- забезпечує механізми для встановлення стійких відношень довіри внаслідок взаємодії самих вузлів та модифікації наявних відношень залежно від зміни структури системи;
- дає змогу виявляти зміни у поведінці вузлів та модифікувати рівні довіри до них.

Встановлення нових відношень довіри відбувається за рахунок використання механізму рекомендацій (рис. 1).

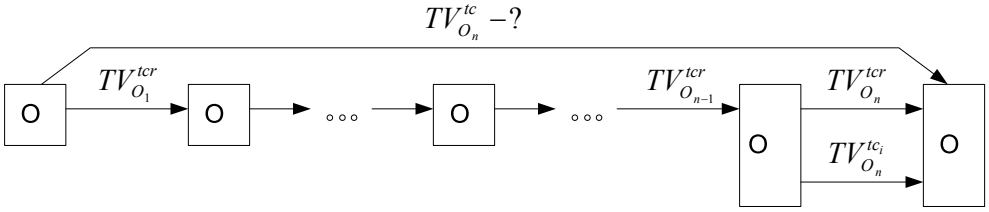

Рис. 1. Приклад ланцюжка рекомендацій

Під час побудови відношення довіри на базі ланцюжка рекомендацій елементи вектора рівнів довіри визначаються за такою формулою:

$$TV_{O_n}^{tc_i} = \begin{cases} 0 & , \text{ якщо } R < TV_{MIN}^{tcr_i}; \\ \left[\prod_{k=0}^{n-1} TV_{O_k}^{tcr} \right] TV_{O_n}^{tc_i}, & \text{якщо } R \geq TV_{MIN}^{tcr_i}, \end{cases}$$

де $R = \prod_{k=0}^{n} TV_{O_k}^{tcr}$, $i = \overline{0,\ldots,|TC|}$.

У разі визначення нульового рівня довіри за результатами рекомендацій початкове значення рівня довіри ініціалізується певним рівнем залежно від трьох профілів поведінки:

- "оптимізм" – згідно з цим профілем як ініціалізуюче значення застосовується TV_{CI};
- "песимізм" – згідно з цим профілем рівень довіри до вузла залишається дорівнювати нулю.
- "реалізм" – ініціалізуюче значення отримується зі співвідношення рівня оптимізму та песимізму згідно з критерієм Гурвіца.

Часова функція нового відношення довіри має вигляд $FT_{O_n} = \bigsqcup_{k=0}^{n} \left[FT_{O_k} \right]$, де під оператором $\bigsqcup_{k=0}^{n} [\ ]$ розуміється суперпозиція часових функцій усіх відношень довіри у ланцюжку згідно з певним правилом.

Для забезпечення можливості врахування змін в інформаційній поведінці вузлів вводиться залежність рівнів довіри від результатів інформаційної взаємодії. Оцінка результатів взаємодії дається на основі аналізу отриманих від вузла даних.

Інформаційний стан об'єкта до взаємодії визначається парою $\left\{ I_k^{tc} ; SRC \right\}$, де I_k^{tc} – інформація стосовно певного факту k з категорії взаємодії tc, SRC – ідентифікатор об'єкта, від якого отримано інформацію. Він однозначно визначає рівень довіри TV_{SRC}^{tc} до нього. Після взаємодії об'єкт отримує від респондента з ідентифікатором SRC' інформацію I_k^{tc} ' стосовно того самого факту.

Залежно від різниці наявної та отриманої інформації здійснюється коригування рівнів довіри за такими правилами:

якщо $I_k^{tc} = I_k^{tc}{}'$, то: $INC\left(TV_{SRC}^{tc}\right)$, $INC\left(TV_{SRC}^{tc}{}'\right)$, $I_k^{tc} = \left(I_k^{tc} + I_k^{tc}{}'\right)/2$,

$$SRC = \begin{cases} SRC\ , \text{якщо } TV_{SRC}^{tc} > TV_{SRC}^{tc}{}'; \\ SRC'\ , \text{якщо } TV_{SRC}^{tc} \le TV_{SRC}^{tc}{}'; \end{cases}$$

якщо $\left[I_k^{tc} \ne I_k^{tc}{}'\right] \wedge \left[\overline{TV}_{SRC}^{tc} = \overline{TV}_{SRC}^{tc}{}'\right]$, то:

якщо $TV_{SRC}^{tc} > TV_{SRC}^{tc}{}'$, то : $I_k^{tc} = I_k^{tc}$, $SRC = SRC$;

якщо $TV_{SRC}^{tc} \le TV_{SRC}^{tc}{}'$, то : $I_k^{tc} = I_k^{tc}{}'$, $SRC = SRC'$;

якщо $\left[I_k^{tc} \ne I_k^{tc}{}'\right] \wedge \left[\overline{TV}_{SRC}^{tc} \ne \overline{TV}_{SRC}^{tc}{}'\right]$, то:

якщо $TV_{SRC}^{tc} > TV_{SRC}^{tc}{}'$, то : $I_k^{tc} = I_k^{tc}$, $SRC = SRC$, $DEC\left(TV_{SRC}^{tc}{}'\right)$;

якщо $TV_{SRC}^{tc} < TV_{SRC}^{tc}{}'$, то : $I_k^{tc} = I_k^{tc}{}'$, $SRC = SRC'$, $DEC\left(TV_{SRC}^{tc}\right)$.

Загальна структура адаптивної системи формування реакцій

Основною задачею, що розв'язується системою формування реакцій на запити щодо проведення інформаційної взаємодії (СФР) є відповідь на питання, чи можна проводити інформаційну взаємодію з тим чи іншим вузлом мережі за певних обставин. Для відповіді на це питання використовують результати роботи таких основних підсистем (рис. 2): підсистеми обробки запитів, ідентифікації, аутентифікації, визначення рівня довіри та підсистеми формування реакцій вузла.

Підсистема обробки запитів здійснює приймання та первинну обробку запитів на проведення інформаційної взаємодії. Вона визначає вузол як систему масового обслуговування, модель якої можна подати так: $\left(\mathrm{M}/\mathrm{G}/1\right):\left(\mathrm{NPRP}/\mathrm{N}/\infty\right)$. Згідно з такою моделлю запити вибираються з черги на обслуговування з врахуванням пріоритетів, причому рівень пріоритету кожного вузла визначається рівнем довіри до нього. Напівдуплексний режим функціонування системи прийому-передавання інформації визначає опрацювання черги запитів без переривання обслуговування. Місткість вхідного буферу N повинна задовольняти таку нерівність:

$$N > \sum_{k=1}^{m}\left[\lambda_k \sum_{i=1}^{m}\lambda_i \left(E_i^2(t) + \mathrm{var}_i(t)\right) \Big/ 2\left(1 - S_{k-1}\right)\left(1 - S_k\right)\right],$$

де $E_i\{t\}$ та $\mathrm{var}_i(t)$ – відповідно, середнє значення та дисперсія функції розподілу часу обробки запиту, λ – інтенсивність надходження заявок у систему, $\rho_k = \lambda_k E_k(t)$, $S_k = \sum_{i=1}^{k}\rho_i < 1$, $S_0 = 0$.

Під час ідентифікації отримується інформація, що дозволяє ідентифікувати вузол серед множини інших вузлів мережі. Для забезпечення унікальності ідентифікації застосовується підхід з використанням локальних унікальних ідентифікаторів на рівні вузла мережі. Кожному відомому глобальному ідентифікатору ставиться у відповідність локальний унікальний ідентифікатор.

Залежно від результатів аналізу отриманого ідентифікатора відбувається первинна (ППрА – протокол первинної аутентифікації) або повторна (ППвА – протокол повторної аутентифікації) аутентифікація. Первинна аутентифікація проводиться у разі відсутності взаємодії з вузлом в минулому. Вона ґрунтується на застосуванні асиметричних криптосистем (АКС) та забезпечує високий ступінь достовірності. Успішне проходження первинної аутентифікації дає можливість узгодити спільну ключову інформацію для повторної аутентифікації, що ґрунтується на симетричних криптосистемах (СКС).

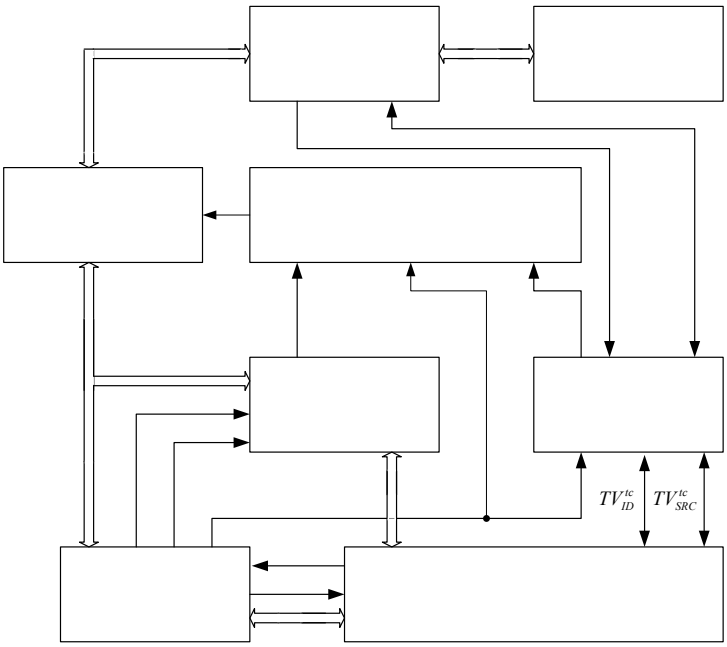

Рис. 2. Базова структура системи формування реакцій:
ID – глобальний ідентифікатор вузла; UID – локальний ідентифікатор вузла;
AT – тип аутентифікації; tc – категорія взаємодії; A –результат аутентифікації;
T – результат аналізу визначеного рівня довіри; IA – результат аналізу
отриманої інформації; N – реакція вузла

Основним механізмом для проведення аутентифікації використано механізм “запит–відповідь.” Для проведення первинної аутентифікації застосовано модифікований протокол Нідхема–Шредера, а для протоколу повторної аутентифікації – швидкий протокол “обміну рукостисканнями”. Криптографічна стійкість системи аутентифікації загалом залежить від стійкості криптографічних алгоритмів симетричних та асиметричних криптосистем і випадковості та непередбачуваності одноразових параметрів. Для генерування таких параметрів розроблено апаратний генератор випадкових чисел, що використовує як джерело недетермінованого сигналу тепловий шум в електронних компонентах (шум Джонсона) [14].

Підсистема формування реакцій визначає реакцію на запит щодо інформаційної взаємодії на основі результатів аутентифікації та оцінки вузла з точки зору рівня довіри до нього. Вона складається з трьох модулів: модуля визначення рівня довіри до вузла, модуля аналізу інформації та модуля формування реакцій. Модуль визначення рівня довіри побудовано на базі розроблених моделі відношення довіри та моделі визначення адекватного рівня довіри. Результатом роботи цього модуля є відповідь на запитання, чи володіє потрібний вузол необхідним рівнем довіри для того, щоб проводити в певній категорії інформаційну взаємодію з ним. Під час корегування рівнів довіри до вузлів використовуються результати роботи модуля аналізу інформації, отриманої під час взаємодії.

Модуль формування реакцій здійснює кінцеве визначення типу реакції вузла на основі тризначної логічної схеми з двозначними входами (таблиця). У роботі визначено три типи реакцій:

- *Позитивна реакція.* Формування позитивної реакції надає можливість розпочати інформаційну взаємодію у визначеній категорії. Окрім того, така реакція передбачає підвищення пріоритету вузла у цій категорії.
- *Негативна реакція.* Отримання негативної реакції забороняє інформаційну взаємодію у поєднанні з одночасним зниженням пріоритету вузла у визначеній категорії.
- *Нейтральна реакція.* Такий тип реакції, як і негативна реакція, передбачає заборону інформаційної взаємодії, однак, без зміни рівня пріоритету вузла.

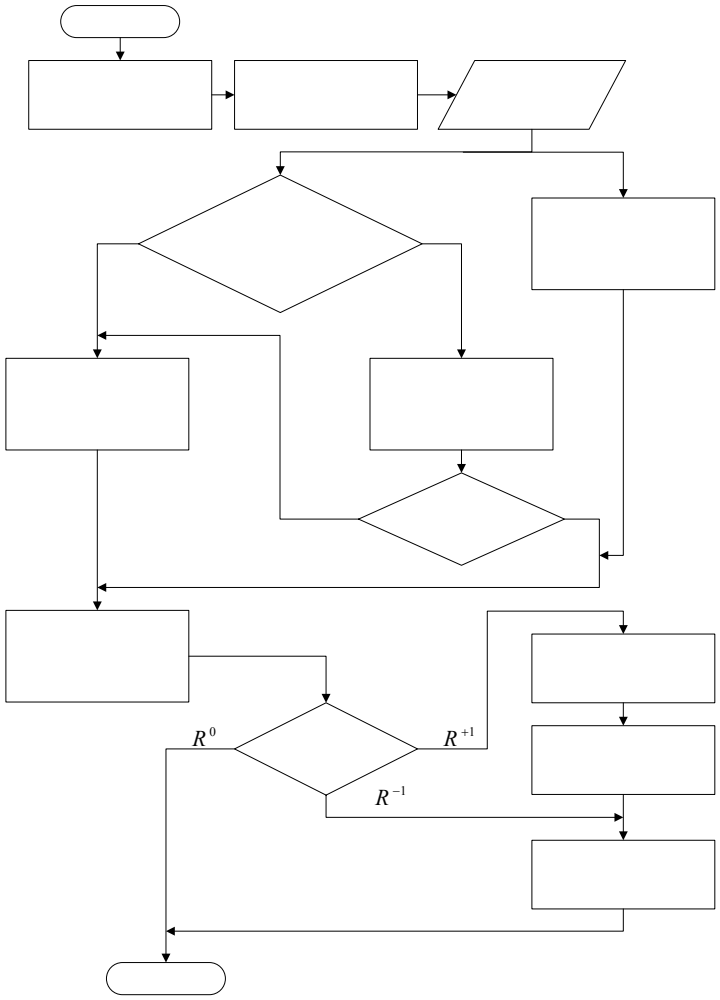

Рис. 3. Блок-схема роботи адаптивної системи формування реакцій

Правила формування реакцій вузла децентралізованої ДМКМДС

Вхідні значення		Вихідні значення
Результат аутентифікації	Оцінка рівня довіри	Реакція вузла
негативний	негативна	негативна
негативний	позитивна	нейтральна
позитивний	негативна	негативна
позитивний	позитивна	позитивна

Ефективності адаптивної системи формування реакцій

Визначимо показники ефективності основних підсистем та СФР загалом. Показником ефективності підсистеми ідентифікації є комунікаційна ефективність, що визначає об'єм трафіку, необхідного для виконання протоколу ідентифікації. Цей об'єм вимірюється у байтах і залежить від кількості повідомлень в протоколі та їх довжини. Комунікаційна ефективність підсистеми ідентифікації становить $T_{ID} = 2\,L_{ID}^{EXT}$, де L_{ID}^{EXT} – довжина зовнішнього ідентифікатора у байтах.

Як показники ефективності підсистеми аутентифікації використані такі характеристики, як комунікаційна ефективність та часова складність виконання протоколу аутентифікації. Комунікаційна ефективність підсистеми аутентифікації визначає об'єм трафіку, необхідного для виконання протоколу аутентифікації.

Комунікаційна ефективність ППрА підсистеми аутентифікації визначається за формулою $T_{PA} = 2\left[T_{DC} + 2N \cdot T_{RND}^{ENC}\right]$, де N – довжина випадкового числа у блоках шифрування, T_{DC} – довжина цифрового сертифіката у байтах, T_{RND}^{ENC} – довжина одного блока, зашифрованого секретним ключем АКС.

Комунікаційна ефективність ППвА підсистеми аутентифікації дорівнює $T_{SA} = 4\left\lceil N \cdot T_{RND}^{ENC} \right\rceil$, де T_{RND}^{ENC} – довжина одного блока, зашифрованого секретним ключем СКС.

Часова складність підсистеми аутентифікації визначає кількість елементарних криптографічних операцій, необхідних для виконання відповідного протоколу аутентифікації. Часова складність ППрА для вузла-ініціатора визначається за формулою $L_{PA}^{INIT} = DS_{VER} + G_{RND} + N\left(2E_{K_P} + D_{K_{\Pr}} + MD\right)$, а для вузла-респондента – $L_{PA}^{RESP} = DS_{VER} + G_{RND} + N\left(E_{K_P} + 2D_{K_{\Pr}} + MD\right)$, де N – довжина випадкового числа у блоках шифрування, DS_{VER} – операція перевірки цифрового підпису, G_{RND} – операція генерування випадкового числа, E_{KP} – операція шифрування відкритим ключем АКС, $D_{K\Pr}$ – операція дешифрування закритим ключем АКС, MD – операція обчислення значення хеш-функції.

Часова складність ППвА для вузла-ініціатора становить $L_{SA}^{INIT} = G_{RND} + N\left(2E_{K_S} + D_{K_S}\right)$, а для вузла-респондента – $L_{SA}^{RESP} = G_{RND} + N\left(E_{K_S} + 2D_{K_S}\right)$, де E_{K_S} / D_{K_S} – операція шифрування/ дешифрування секретним ключем СКС.

Оскільки повторна аутентифікація застосовується істотно частіше, ніж первинна та має вищу комунікаційну ефективність у поєднанні з меншою часовою складністю, то така комбінація двох методів, окрім виявлення колізій глобальних ідентифікаторів, дає змогу підвищити загальну ефективність підсистеми аутентифікації.

Показано, що загальна часова складність СФР для первинної взаємодії визначається за формулою $L_{SRF}^{PR} = 2K \cdot CMP_{EXT\_ID} + \max\left[K \cdot M\left[CMP_{INT\_ID} + L_{TVC}\right], \max\left(L_{PA}^{INIT}, L_{PA}^{RESP}\right)\right]$, а для повторної взаємодії – $L_{SRF}^{SE} = 2K \cdot CMP_{EXT\_ID} + \max\left[K \cdot M\left[CMP_{INT\_ID} + L_{TVC}\right], \max\left(L_{SA}^{INIT}, L_{SA}^{RESP}\right)\right]$, де $L_{PA}^{INIT} / L_{PA}^{RESP}$ – часова складність первинної аутентифікації для вузла-ініціатора та респондента відповідно, $L_{SA}^{INIT} / L_{SA}^{RESP}$ – часова складність повторної аутентифікації.

Висновки. Поява достатньо продуктивних, малогабаритних обчислювальних і вимірювальних засобів та стрімкий розвиток бездротових технологій передавання даних дають можливість широко застосовувати децентралізовані мобільні комп'ютерні мережі динамічної структури для розв'язання різного типу завдань. Для ефективного функціонування такого класу мереж під час їх побудови необхідне застосування засобів формування реакцій, які здатні адаптуватись в умовах швидкої зміни структури мережі та виявляти і належно реагувати на зміни поведінки вузлів мережі. У роботі була описана загальна структура та функціонування адаптивної системи формування реакцій вузлів децентралізованих мобільних комп'ютерних мереж динамічної структури.

1. Sounes G. Packet Radio: What? Why? How? // Articles and Information on General Packet Radio Topics, TARP. – 1995. – 132p. 2. Сокіл В.М. Мобільні мережі довільної структури – сучасні технології та застосування // Тези доп. Між нар. Наук. Конф. студентів, аспірантів та молодих науковців "Комп'ютерні науки та інженерія CSE2006". – Львів, 2006. – С. 72–75. 3. Hubaux J-P., Gross T. and other Toward Self-Organized Mobile Ad Hoc Networks: The Terminodes Project // IEEE Communications Magazine, 2001. – pp. 118–124. 4. Corson S., Freebersyser J. and Sastry A. (eds.). Mobile Networks and Applications (MONET) // Special Issue on Mobile Ad Hoc Networking, 1999. 5. Stojmenovic I. Handbook of sensor networks. Algorithms and architectures // Wiley Interscience, 2005. – 553 p. 6. Clare L. P., Pottie G. J. and Agreaa J. R. Self-Organizing Distributed Sensor Networks // Proc. Int. Conf. SPIE № 3713, 1999. – pp. 229–237. 7. Clare L., Pottie G. Agreaa J. R. Self-Organizing Distributed Sensor Networks // Proc. Int. Conf. SPIE № 3713, 1999. – pp. 229–237. 8. Blazevic L., Buttyan L., Čapkun S., Giordano S., Hubaux J.-P., and Le Boudec J.-Y. Self-Organization in Mobile Ad Hoc Networks: The Approach of Terminodes // IEEE Communications Magazine, June 2001. 9. Стоуллингс В. Криптография и защита сетей – Принципы и практика: Пер. с англ. // Вільямс, 2001. – 672с. 10. Maurer U. Modelling a public-key infrastructure // Computer Security –ESORICS '96, LNCS 1146, Springer Verlag, 1996. 11. The PGP Trust Model // www.pgpru.com. 12. Abdul-Rahman A. and Hailes S. A Distributed Trust Model // New Security Paradigms Workshop1997, ACM, 1997. 13. E. Gerck Toward Real-World Models of Trust: Reliance on Received Information, 2002. 14. Сокіл В.М. Генератор випадкових чисел // Вісник Нац. ун-ту "Львівська політехніка". Комп'ютерні системи та мережі. – 2004. – №523. – С. 127–134.