КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.25.229252
УДК 004.056:338.46

Костюк Юлія Володимирівна
доктор філософії, доцент кафедри інформаційної та
кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0001-5423-0985
y.kostiuk@kubg.edu.ua

Бебешко Богдан Тарасович
доктор філософії, доцент кафедри інформаційної та
кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0001-6599-0808
b.bebeshko@kubg.edu.ua

Крючкова Лариса Петрівна
доктор технічних наук, професор, професор кафедри
інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID:0000-0002-8509-6659
l.kriuchkova@kubg.edu.ua

Литвинов Валерій Андроникович
доктор технічних наук, професор
Інститут проблем математичних машин та систем НАН України, Київ, Україна
ORCID ID:0000-0001-5568-7629
litval@dr.com

Оксанич Ірина Миколаївна
кандидат технічних наук, с.н.с.
Інститут проблем математичних машин та систем НАН України, Київ, Україна
ORCID ID:0000-0002-1208-3427
inokc2018@gmail.com

Складанний Павло Миколайович
кандидат технічних наук, доцент, завідувач кафедри
інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID:0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

Хорольська Карина Вікторівна
доктор філософії
ТОВ «Газопостачальна компанія «Нафтогаз Трейдинг»», Київ, Україна
ORCID ID: 0000-0003-3270-4494
karynakhorolska@gmail.com

ЗАХИСТ ІНФОРМАЦІЇ ТА БЕЗПЕКА ОБМІНУ ДАНИМИ В БЕЗПРОВОДОВИХ МОБІЛЬНИХ МЕРЕЖАХ З АВТЕНТИФІКАЦІЄЮ І ПРОТОКОЛАМИ ОБМІНУ КЛЮЧАМИ

Анотація. Мобільність користувачів, передача сигналів через кіберпростір та необхідність низького споживання енергії мобільними пристроями спричиняють виникнення численних нових проблем, пов'язаних із захистом інформації у безпроводових мобільних мережах. Забезпечення надійного і безпечного інформаційного обміну в таких мережах є критично важливим, оскільки багато в чому залежить від рівня захищеності ключової інформації, яка

використовується для автентифікації користувачів мережі та шифрування даних, що передаються мережею. У статті розглянуто протокол, що забезпечує ефективну автентифікацію та безпеку у мобільних мережах, орієнтуючись на використання блокового шифру як основного алгоритму для шифрування з секретним ключем та базового шифру для хеш-функцій. Протокол передбачає мінімальні вимоги до учасників мережі, зокрема необхідність знання лише відкритого параметра та відкритого ключа центру сертифікації, що значно спрощує його впровадження та підвищує надійність. Додатково, в статті аналізується вплив протоколу на загальну безпеку та стійкість мобільних мереж до різноманітних загроз, включаючи кібератаки на протокол обміну ключами, спроби компрометації інформації під час її передачі, а також роль криптографії в цьому контексті. Особливу увагу приділено ролі центру управління ключами та криптосистем у забезпеченні захисту інформації та зниженні ризиків, пов'язаних з несанкціонованим доступом до даних у безпроводових мобільних мережах.

Ключові слова: захист інформації; автентифікація; безпека; інформаційний обмін; протокол обміну ключами; кіберстійкість; криптографія; безпроводові мобільні мережі; мобільний пристрій; криптосистема; центр управління ключами; кібератака.

ВСТУП

Типовою тенденцією на сучасному етапі розвитку електронних комунікацій є активне впровадження безпроводового зв'язку. Досконаліть розвитку технологій на високому рівні, включаючи досягнення в галузі криптографії, дозволяє створювати та розгортати безпроводові мобільні мережі, які знайшли своє застосування для вирішення широкого кола завдань, зокрема забезпечення обміну інформацією в режимі невідкладних ситуацій та в інтелектуальних системах.

У дослідженнях привертає увагу та викликає зростаючий інтерес питання безпеки та конфіденційності в мобільних мережах, які, порівняно з провідними, виявляються більш вразливими до різноманітних кібератак, таких як перехоплення та несанкціонований доступ. Проблема безпеки в мобільних мережах набуває особливого значення через їхню динамічну природу та потенційний ризик перехоплення конфіденційної інформації, що обмінюється між абонентами мережі. Одним з ключових аспектів є захищеність ключової інформації, яка використовується для автентифікації та шифрування, оскільки ця інформація є основною для забезпечення вірогідності та цілісності мережі.

Таким чином такі питання були детально розглянуті в рамках низки досліджень, зокрема в безпроводовій мережі стільникової цифрової пакетної передачі даних — Cellular Digital Packet Data (CDPD), де були запропоновані відповідні механізми безпеки та конфіденційності, а також обговорено можливі загрози та атаки, включаючи використання криптосистем для захисту інформації. Цей протокол подібний за своїм принципом до роботи WAP, але він працює лише для одного стандарту стільникового зв'язку AMPS.

Технологія CDPD визначається як стандарт передачі даних в безпроводових мобільних телефонних мережах і використовує технологію комутації пакетів, що дозволяє передавати дані у вигляді окремих пакетів, не встановлюючи постійний канал, як це характерно для голосового трафіку. Крім того, технологія CDPD обладнана модемним інтерфейсом з використанням АТ-команд. На відміну від радіомодемів, стільникові модеми виявляють свою відмінність у використанні не спеціально призначених антен та приймачів-передавачів, а замість цього використовують вбудовані пристрої, які входять до складу стільникових телефонів. Такий підхід визначається

технічною специфікою стільникових модемів, що робить їх більш компактними та зручними у порівнянні із традиційними радіомодемами, і водночас дозволяє ефективно використовувати вбудовані можливості телефонів для забезпечення безпроводового зв'язку.

Постановка проблеми. Для забезпечення безпеки в мобільних мережах запропоновано різні протоколи автентифікації та безпеки [1], [2], [9], [15] – [17]. Зокрема, в протоколі [11] – [15] використовується комбінація шифрування, включаючи криптографію з приватним і відкритим ключем, базуючись на розв'язанні двох обчислювально складних задач — факторизації та дискретного логарифмування. Однак в результаті аналізу протоколу виявлено декілька проблем. Перша проблема пов'язана з неефективністю цього протоколу, що викликало подальше дослідження в цьому напрямку, друга — з атаками на відтворення, які можуть бути застосовані проти протоколу. У статтях запропоновано протокол автентифікації та розподілу ключів, який використовував широкомовний канал для автентифікації мобільного користувача базової станції у фоновому режимі [13] – [18].

У зв'язку з обмеженням споживання енергії мобільними пристроями в мобільних мережах, актуальним стає розробка протоколу безпеки, який використовує найпростіші алгебраїчні операції та займає якомога менше місця в пам'яті мобільних пристроїв [11] – [16], [21], [23]. З цією метою важливо розробити протокол для автентифікації та безпеки, який є більш оптимізованим, ніж попередні протоколи щодо пропускної здатності мобільних пристроїв і має такий самий рівень безпеки, як і вони. Ключові особливості нового протоколу включають: необхідність знання лише відкритого параметра та відкритого ключа центру сертифікації всіма учасниками мережі; використання лише блокового шифру, який працює як алгоритм шифрування з секретним ключем, і як базовий блоковий шифр хеш-функції.

Безпека та надійність інформаційного обміну в безпроводовій мобільній мережі багато в чому залежить від захищеності ключової інформації, що слугує для автентифікації абонентів мережі та шифрування переданих мережею даних [1] – [4], [6] – [8]. Однак, враховуючи зростаючу кількість кібератак, що націлені на мобільні мережі, важливість впровадження надійної криптографії стає ще більш актуальною. Бездротова мобільна мережа, що є динамічною за своєю топологією, складається з різноманітних мобільних вузлів або абонентів мережі, які використовують радіоканал для передачі даних. Надійна криптосистема є основою забезпечення безпеки в таких мережах.

Аналіз останніх досліджень і публікацій. Останні дослідження у сфері безпеки безпроводових мобільних мереж [1] – [4] демонструють зростаючу складність проблем, пов'язаних із захистом інформації в умовах мобільності користувачів та обмежених ресурсів мобільних пристроїв. Важливим аспектом є забезпечення ефективної автентифікації та шифрування даних, що передаються через відкритий кіберпростір, де ризики перехоплення і несанкціонованого доступу є значними. Криптографія відіграє ключову роль у захисті таких мереж від можливих загроз.

Аналіз сучасних публікацій показує, що багато досліджень зосереджені на розробці нових протоколів автентифікації та шифрування, які повинні відповідати вимогам високої безпеки та низького споживання енергії. Зокрема, велику увагу приділено використанню блокових шифрів як основних алгоритмів для шифрування з секретним ключем, а також базових шифрів для хеш-функцій. Це обумовлено необхідністю створення ефективних і надійних механізмів для захисту даних у динамічних та часто небезпечних умовах безпроводових мереж [2] – [6], [9], [11], [14]. Окрім того, сучасні дослідження зосереджені на удосконаленні протоколів обміну ключами і їх стійкості до

атак. Виявлено, що проблеми з безпекою часто виникають через вразливості у протоколах обміну ключами та можливість компрометації інформації під час її передачі. Роль центру управління ключами у забезпеченні захисту інформації залишається критично важливою, адже він забезпечує ключовий механізм для мінімізації ризиків несанкціонованого доступу.

Мета статті. Метою дослідження є огляд протоколу, що забезпечує ефективну автентифікацію та безпеку в мобільних безпроводових мережах, використовуючи блоковий шифр для шифрування з секретним ключем і базовий шифр для хеш-функцій, з мінімальними вимогами до учасників мережі, такими як знання лише відкритого параметра та відкритого ключа центру сертифікації, що полегшує впровадження і підвищує надійність. Особливу увагу приділено детальному аналізу впливу цього протоколу на загальну безпеку мобільних мереж, оцінці його стійкості до різноманітних загроз, таких як кібератаки на протокол обміну ключами та спроби компрометації інформації під час передачі через кіберпростір, з акцентом на роль центру управління ключами у забезпеченні захисту інформації та зменшенні ризиків несанкціонованого доступу до даних. Важливо також розглянути криптографічні аспекти протоколу та його відповідність сучасним вимогам криптосистем.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

У контексті безпеки інформаційного обміну в безпроводовій мобільній мережі, ключовий акцент розміщений на забезпеченні конфіденційності, цілісності та автентифікації даних, які обмінюються між абонентами мережі. Захищена ключова інформація виступає як основа цих безпекових механізмів, гарантуючи, що тільки легітимні користувачі отримують доступ до мережевих ресурсів та інформації.

Динамічна топологія безпроводової мобільної мережі, яка може зазнавати змін через рух абонентів, створює додаткові виклики у забезпеченні безпеки. Важливо розглядати і розробляти ефективні заходи для захисту інформації під час постійної зміни топології мережі та руху абонентів. Однак ефективне управління ключовою інформацією, яка використовується для автентифікації та шифрування, може визначити успішність забезпечення інформаційної безпеки в таких умовах (рис. 1).

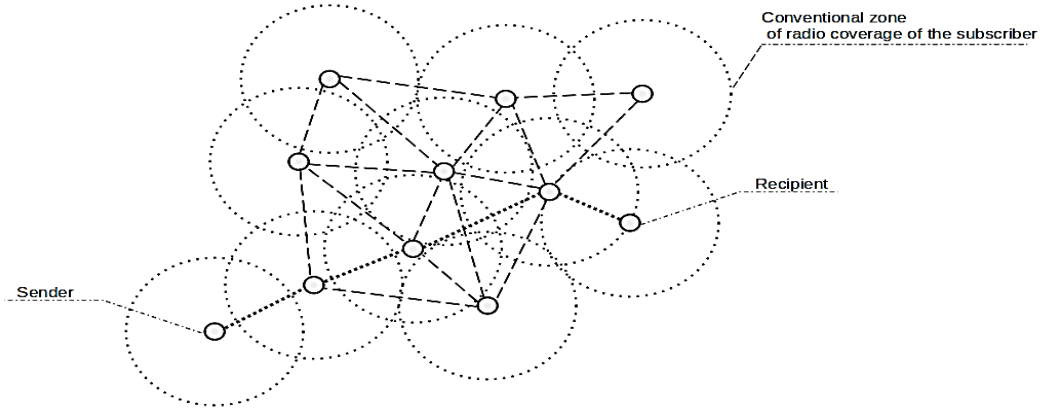

Рис. 1. Графічна інтерпретація процесу передачі інформації в безпроводовій мобільній мережі, що відображає рух даних від одного мобільного вузла до іншого через радіоканал
Джерело: розроблено автором в середовищі LibreOffice (знімок з екрану)

Розв’язання завдань інформаційної безпеки в безпроводовій мобільній мережі має певні відмінності від традиційних рішень, які використовуються для захисту інформації в провідних локальних мережах [3], [5] – [7], [10], [23]. Це пов’язано з тим в безпроводових мобільних мережах відсутні стаціонарні вузли, і абоненти, які беруть участь у процесі обміну інформацією, можуть переміщатися, змінюючи тим самим, топологію мережі. Через мінливість топології та обмеженість дальності радіовидимості зв’язки між абонентами можуть утворюватися і зникати.

Існуючі підходи до розв’язання задачі формування ключової інформації в безпроводовій мобільній мережі ґрунтується на використанні довіреного центру керування ключами, але його використання в безпроводовій мобільній мережі породжує проблему, пов’язану з можливістю неотримання інформації, який тимчасово перебуває поза мережею, поточної інформації, розподілюваної центром керування ключами. Тим самим існує ймовірність того, що абоненти, які «вийшли» з безпроводової мобільної мережі, «матимуть» застарілу ключову інформацію, що дасть змоги забезпечити їхню ідентифікацію іншими абонентами при поверненні назад у мережу [1] – [9], 11]. Загалом, завдання забезпечення ідентифікації абонентів є одним із найважливіших для забезпечення безпечного та сталого функціонування бездротового мобільної мережі.

Тому одним із можливих рішень цієї проблеми є формування ключової інформації безпосередньо в апараті самих абонентів мережі шляхом застосування процедури оновлення ключа, що ґрунтується на необоротному математичному перетворенні попередніх значень ключової інформації. У разі дотримання всіма абонентами мережі правила оновлення ключів у конкретний момент часу вони матимуть однакову ключову інформацію, що дасть змогу забезпечити ідентифікацію абонентів незалежно від їхнього стану зв’язності з іншими абонентами безпроводової мобільної мережі [2], [5].

Однак у такої процедури оновлення ключа є суттєвий недолік, який полягає в тому, що якщо зловмиснику стане відомий хоча б один із раніше використаних ключів, то вся подальша ключова послідовність G буде скомпрометована. Це може призвести до компрометації криптосистеми та її стійкості до кібератак. Виникає протиріччя між перевагами формування ключової інформації в апаратурі самих абонентів, що забезпечує підвищену ідентифікацію абонентів безпроводової мобільної мережі, та підвищеною ймовірністю компрометації ключової інформації, сформованої таким чином [3], [5] – [8], [19]. Розв’язання цієї задачі вимагає забезпечення криптостійкості процедури оновлення ключа на рівні не нижчому, ніж у разі використання центру управління ключами.

У контексті безпеки безпроводових мобільних мереж важливо регулярно переглядати та вдосконалювати стратегії шифрування та автентифікації. Нові технології, такі як штучний інтелект чи квантові обчислення, можуть впливати на ефективність існуючих методів захисту. Крім того, ростуть загрози від різноманітних видів атак, таких як кібератаки з використанням штучного інтелекту чи соціально-інженерні атаки. Оновлення стратегій безпеки також має враховувати особливості бездротового інформаційного обміну. Врахування динаміки топології мережі, мобільності вузлів та змін у спектрі частот може покращити ефективність заходів безпеки. Наукові дослідження та інновації у цій галузі є ключовими для забезпечення стійкості та надійності безпроводових мобільних мереж в умовах постійно зростаючого рівня загроз.

Таким чином, актуальним є завдання розробки алгоритму формування ключової інформації в апаратурі абонентів безпроводової мобільної мережі, що дає змогу підвищити ідентифікацію абонентів безпроводової мобільної мережі за умови збереження криптостійкості ключової інформації на основі центру управління ключами.

ISSN 2663 - 4023

Основною проблемою в безпроводовій мобільній мережі є підтримання «зв'язності» абонентів в єдиному мережевому просторі. Як показник «зв'язності» використовують ймовірність P геометричної радіодосяжності всіх вузлів, які є абонентами безпроводової мобільної мережі на обмеженій ділянці місцевості. Особливість центрізації ключового простору в безпроводовій мобільній мережі пов'язана з рухливістю її абонентів, коли можливі періодичні «виходи» та «повернення» абонентів мережі за межі зони та в зону радіообміну відповідно. Існують різні підходи до розв'язання розподілу та управління ключовою інформацією, засновані на використанні довіреного центру управління ключами [1] – [5], [9], [24]. Однак при використанні центру управління ключами можлива ситуація недовведення до абонента поточної ключової інформації, що розподіляється центром управління ключами, у момент виходу абонента з мережі [6], [9] – [10]. Тобто абонент стає «чужим для своїх» (рис. 2).

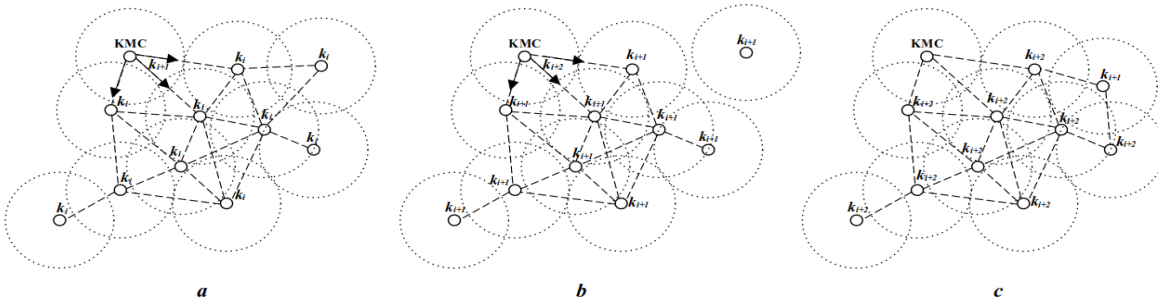

Рис. 2. Варіант розвитку ситуації під час використання довіреного центру управління ключами (ЦУК) у безпроводових мобільних мережах (а — абонент стає для «своїх свій», б — абонент знаходиться поза зоною радіообміну, в — абонент стає «чужим для своїх»)
Джерело: розроблено автором в середовищі LibreOffice (знімок з екрану)

Отже, при використанні центру управління ключами існує ймовірність того, що деякі абоненти безпроводової мобільної мережі матимуть «застарілу» ключову інформацію, що не дозволить їх ідентифікувати іншими абонентами мережі [7]. При цьому підвищення ідентифікаційної надійності абонентів безпроводової мобільної мережі не повинно впливати на зменшення криптостійкості ключової інформації [10], [24]. Як показник криптостійкості обирають ймовірність компрометації $P_{\text{компрометації}}$ ключової інформації, який дозволяє оцінити алгоритм формування ключової інформації з точки зору стійкості до атак, спрямованих на перехоплення інформаційних повідомлень, що містять або сформовані з використанням ключової інформації.

Важливо розробити алгоритм формування ключової інформації в безпроводовій мобільній мережі, що забезпечує [22] – [24]:

- підвищення ідентифікації абонентів безпроводової мобільної мережі порівняно з традиційною схемою розподілу ключової інформації, що використовує довірений центр управління ключами (ЦУК):

$$P_{\text{ідентифікація абонентів}} > P_{\text{ідентифікація ЦУК}}, \quad (1)$$

де $P_{\text{ідентифікація абонентів}}$ і $P_{\text{ідентифікація ЦУК}}$ — ймовірності ідентифікації абонентів безпроводової мобільної мережі для розроблюваного алгоритму формування ключової інформації і для традиційної схеми, що використовує ЦУК, відповідно;

• порівнянну з традиційною схемою, що використовує довірений ЦУК, крипостійкість ключової інформації матиме:

$$P_{\text{компрометація ключової інформації}} \cong P_{\text{компрометація ЦУК}}, \quad (2)$$

де $P_{\text{компрометація ключової інформації}}$ і $P_{\text{компрометація ЦУК}}$ — ймовірності компрометації ключової інформації для розроблюваного алгоритму формування ключової інформації і для традиційної схеми, що використовує ЦУК.

Розв'язання цієї задачі базується на процедурі оновлення ключа, що використовує необоротне математичне перетворення ключової інформації в апаратурі самих абонентів [1] – [5], [24]. При цьому чергове значення ключової інформації представляє собою перетворення попереднього значення (рис. 3).

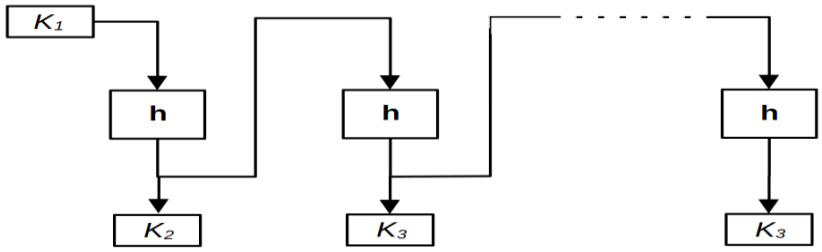

Рис. 3. Процедура оновлення ключа
Джерело: розроблено автором в середовищі LibreOffice (знімок з екрану)

У разі використання даної схеми абоненти починають з ключа K_1 і за допомогою функції незворотного перетворення $h(K_i)$ в заздалегідь визначені проміжки часу здійснюють ітерації:

$$h(K_1),\ h(h(K_1)), \dots, \underbrace{h(h(\dots\ h(K_1)\dots)}_{n} = h^n(K_1), \quad (3)$$

Таким чином, для i-го проміжку часу, $1 \le i \le n$ абоненти будуть володіти одним ключем K_1, який визначається як:

$$\mathrm{K}_i = h(K_{i-1}) = h^{i-1}(K_1) = h(h(\dots(h(K_1)\dots), \quad (4)$$

Однак в процедурі оновлення ключа є один суттєвий недолік, який полягає в тому, що, якщо порушнику стане відомий хоча б один із раніше використаних ключів, то вся подальша ключова послідовність, що формується згідно цієї процедури, може бути скомпрометована. Отже, для використання процедури оновлення ключа в безпроводовій мобільній мережі потрібне розроблення додаткових технічних рішень, що забезпечують підвищення криптостійкості. Важливу роль при цьому відіграє вибір функції незворотного перетворення.

Основні вимоги до функції незворотного перетворення, що використовується для формування ключової інформації [5] – [10], [24]:

- відповідність вимогам, що висуваються до криптографічно стійких хеш-функцій: незворотність і високий лавинний ефект (коефіцієнт розсіювання);
- відповідність вимогам, що висуваються до засобів генерації ключової інформації: випадковість, рівномірність розподілу і великий період вихідної послідовності;
- висока швидкодія.

Аналіз функцій незворотного перетворення (CRC, MD5, SHA-1, Whirlpool, SHA-256, MD5, RIPEMD, Tiger-2 тощо) показав, що функції, що мають високі криптографічні властивості, мають невисоку швидкодію. Для забезпечення високої швидкодії, як

функцію незворотного перетворення, можна використовувати дискретні відображення класу КА (клітинні автомати).

Для опису КА використовують наступну сукупність об’єктів:

$$KA = \{G, S, Q, R\}$$

де G — дискретний метричний простір над дискретною множиною елементів, що називається решіткою автомата;

S — скінченна множина можливих станів клітин. Стан окремо взятої i-ої клітини в момент t характеризується деякою змінною $S_i(t) \in \{S\}$. Сукупність станів усіх N клітин у момент t визначає стан решітки, який позначається A_t;

Q — скінченна множина, що визначає околицю клітини, тобто, кількість і місце розташування клітин множини $Q(i)$ що впливають на значення даної клітини: $i \in Q(i)$;

R — правило переходу, що визначає закон зміни стану решітки КА, що є функцією R від двох змінних — стану $S_i(t)$ самої клітини і суми станів її найближчих сусідів у попередній момент t:

$$S_i(t+1) = R(S_i(t), \sum_{j \in Q(i)} S_j(t)), \quad (5)$$

Класичні моделі КА, що функціонують за фіксованим правилом переходу $R - const$, мають низку недоліків, пов’язаних з їхньою чутливістю до початкового стану решітки та обраного правила переходу, внаслідок чого велика кількість правил і початкових станів решітки може призвести до зациклення або виродження процесу еволюції КА [24].

Для усунення вищевказаних недоліків введено поняття функції селектування «Або» правил переходу, що встановлює порядок зміни правил переходу на певних тактах функціонування КА:

$$f_R = f(R_i, k_j), \quad (6)$$

де R_i — фіксоване правило, що належить до обраної кінцевої множині правил $R = (R_0, R_1, \dots, R_n)$, k_j — коефіцієнт, що визначає такт роботи КА за правилом R_i, де $j = \overline{1, m}$.

Із наведених на рис. 4 графів переходів КА видно, що для КА із заданим вихідним станом A_0 і постійним правилом R, перехід з одного стану в інший строго фіксований. У межах одного циклу в стан A_l, потрапити можна тільки через стан A_{l-1}. У разі використання функції селектування правил переходу на кожному з кроків КА може перейти в один із декількох станів за рахунок чого збільшується період його роботи [23] – [24].

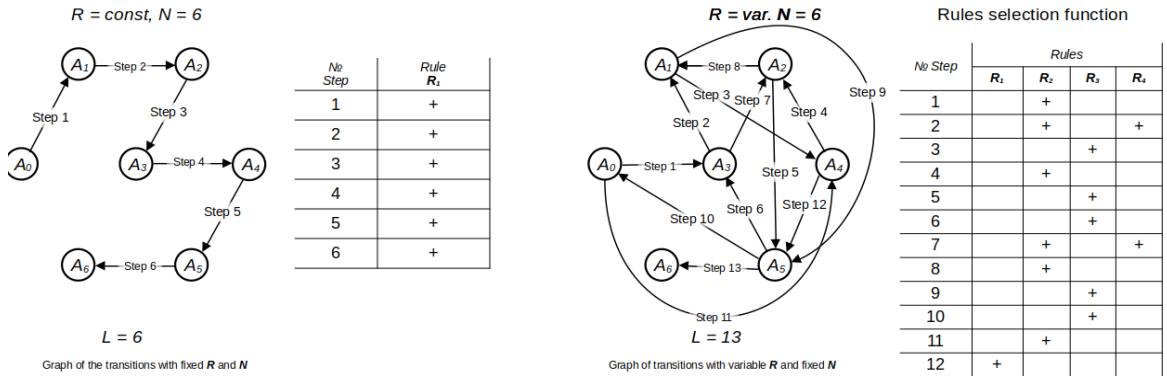

Рис. 4. Графічна інтерпретація збільшення періоду роботи КА в разі використання функції селектування правил переходу

Джерело: розроблено автором в середовищі LibreOffice (знімок з екрану)

Застосування функції селектування правил переходу дає змогу збільшити період КА від 5 до 100 разів залежно від початкових умов і обраних правил переходу. Таким чином, важливим фактором для завдання функції селектування є формування множини правил $R = (R_0, R_1, \dots, R_n)$. Загальна кількість «І» на решітці КА, що перебуває в i-му стані (на i-ій ітерації процесу еволюції) можна позначити як «вагу решітки» W_i:

$$W_i = \sum_{j=0}^{k} S_j(t_i), \quad (7)$$

Зміна «ваги решітки» W від числа ітерацій n процесу еволюції КА дає змогу зробити висновок, що незважаючи на різну «вагу» початкового стану решітки, у процесі еволюції КА «вага решітки» стабілізується. Отже, максимально можливе число станів Z, які може прийняти решітка КА в процесі еволюції, визначатиметься як:

$$Z = \sum_{i=W_{min}}^{W_{max}} C_k^i, \quad (8)$$

де W_{min} і W_{max} — мінімальна і максимальна «вага решітки» КА в процесі її еволюції.

Для всіх правил, що не призводять до виродженого або стійкого стану, справедливо $\eta_{max} - \eta_{min} \approx 10\%$, де $\eta_{min} = (\frac{W_{min}}{k}) \cdot 100\%$ і $\eta_{max} = (\frac{W_{max}}{k}) \cdot 100\%$ — мінімальне і максимальне значення процентного вмісту «1» на решітці КА в процесі його еволюції. Можна зробити висновок, що використання у функції селектування «різновагових» правил переходу дає змогу збільшити кількість можливих станів решітки КА, що призводить до збільшення простору значення ключової інформації і, отже, підвищує її крипостійкість.

У разі використання як функції незворотного перетворення інформації та моделі КА вихідне значення даної функції визначається як:

$$A_N = f_{KA}(A_0, f_R, N) = 011010011 \dots 011010_k, \quad (9)$$

де A_N — стан решітки на N-ій ітерації процесу еволюції КА, A_0 — початковий стан решітки КА, f_R — застосована функція селектування правил переходу (рис. 5).

$$f_R = (R_i, k_j), \quad (10)$$

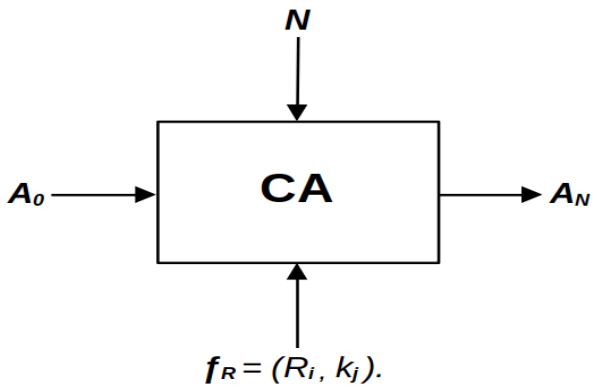

Рис. 5. Схема функції незворотного перетворення на базі модифікованої моделі КА з функцією селектування правил переходу (CA — клітинні автомати)
Джерело: розроблено автором в середовищі LibreOffice (знімок з екрану)

Розв'язання проблеми підвищення криптостійкості процедури оновлення ключа здійснюється шляхом зменшення передбачуваності значень ключової інформації, що формуються за допомогою неї [1] – [10], [24]. Для цього попередню схему (рис. 3) доповнено генератором випадкових чисел (ГВЧ), що формує випадкове число r, що визначає, скільки разів треба застосувати до поточної ключової інформації K_i функцію прямого незворотного перетворення для отримання наступного значення ключової інформації — K_{i+1} (рис. 6).

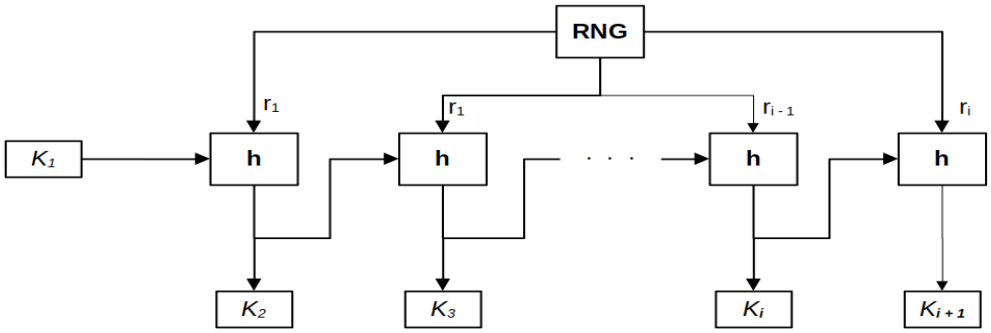

Рис. 6. Процедура випадкового багаторазового оновлення ключа
Джерело: розроблено автором в середовищі LibreOffice (знімок з екрану)

Для здійснення правильного функціонування цієї схеми ГВЧ всі абоненти мережі мають бути синхронізовані й у разі дотримання даної умови абоненти на передавальній і приймальній стороні, у конкретний момент часу матимуть однаковий ключ. У разі використання цієї схеми абоненти починають із ключа K_1, і за допомогою односпрямованої функції $h(K_i)$ у заздалегідь визначені проміжки часу проводять ітерації:

$$h^{r1}(K_1),\ h^2(h^1(K_1)), \dots, \underbrace{h^{r_n}(h^{r_{n-1}}(\dots\ h^{r_1}(K_1)\ \dots)}_{n} = h^{\sum_1^n r_i}(K_1), \quad (11)$$

Таким чином, для i-го проміжку часу, $1 \le i \le n$, абоненти мережі володітимуть ключем K_i який визначається як:

$$K_i = h^{r_i}(K_{i-1}) = h^{\sum_1^i r_j}(K_1) = \underbrace{h^{r_i}(h^{r_{i-1}} - (\dots\ h^{r_1}(K_1)\ \dots)}_{i-1}, \quad (12)$$

Процедура випадкового багаторазового оновлення ключа на базі моделі КА, що використовує функцію селектування правил переходу. Алгоритм формування ключової інформації відповідно до цієї схеми (рис. 7) виглядає таким чином:

1) синхронізація та встановлення однакових початкових налаштувань на ГВЧ усіх абонентів безпроводової мобільної мережі;

2) розподіл закритим чином між абонентами безпроводової мобільної мережі початкового значення ключової інформації — K_i;

3) ініціалізація початкового значення решітки КА $A_0 = K_i$;

4) формування всіма абонентами безпроводової мобільної мережі за допомогою ГВЧ випадкового числа r_i;

5) формування всіма абонентами безпроводової мобільної мережі у заздалегідь визначений проміжок часу наступного значення ключової інформації:

$$K_{i+1} = A_N = f_{KA}(A_0, f_R, N_i), \quad (13)$$

де A_N — вихідний стан решітки КА, отриманий після $N_i = r_i$ тактів його функціонування.

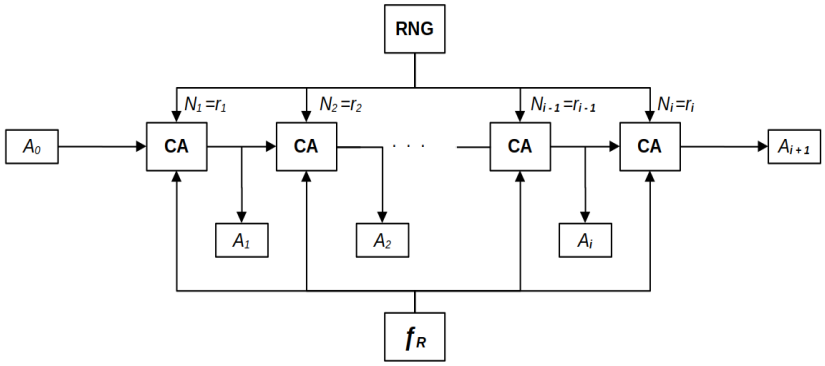

Рис. 7. Процедура випадкового багаторазового оновлення ключа на базі розробленої моделі КА з функцією селектування правил переходу (RNG — генератор випадкових чисел, CA — клітинні автомати)
Джерело: розроблено автором в середовищі LibreOffice (знімок з екрану)

Чергове значення ключової інформації формується шляхом повторення кроків 3–5 цього алгоритму. При цьому як початкове значення ключової інформації виступає ключова інформація, отримана під час попереднього проходу алгоритму. Згідно з цим алгоритмом, для i-го проміжку часу, $1 \le i \le n$, абоненти мережі володітимуть однаковим ключем A_{i+1}, який визначається:

$$A_{i+1} = f_{KA}(A_i, f_R, N_i) = f_{KA}(A_{i-2}, f_R, N_{i-2}), f_R, N_{i-1} + N_i) = f_{KA}\left(A_0, f_R, \sum_1^i N_k\right), \quad (14)$$

Для розробленого алгоритму формування ключової інформації проведено оцінку ймовірності ідентифікації абонентів безпроводової мобільної мережі у порівнянні з традиційним підходом розподілу ключової інформації, заснованим на центрі управління ключами [2], [5], [8] – [10], [24].

Для оцінки криптостійкості ключової інформації, що формується за алгоритмом, заснованим на довіреному центрі управління ключами, використано стандартну формулу для повного перебору. При цьому час доступу порушника $\mathrm{T}_{\text{доступу}}$ до ключової інформації буде обмежена періодичністю її оновлення $\mathrm{T}_{\text{оновлення}}$:

$$P_{\text{компроментації}} = \frac{n(t) \cdot \mathrm{T}_{\text{оновлення}}}{N}, \quad (15)$$

де N — простір значень, що приймаються ключовою інформацією, $n(t)$ — швидкість перебору.

В алгоритмі формування значення ключової інформації не є незалежними одне від одного величинами, тому періодичність оновлення ключової інформації не є обмежувальним фактором для порушника [3] – [7], [9], [24]. Алгоритм здійснення компрометації поточної ключової інформації, що формується за розробленим алгоритмом, для порушника полягатиме спочатку в отриманні одного з попередніх значень K_i і знаходженні потім кількості перетворень $\sum r$, які було здійснено над K_i, за той час, який він витратив на його знаходження. Тоді ймовірність компрометації для розробленого алгоритму становитиме:

$$P_{\text{компроментації}} = \sum \frac{\mathrm{T}_{\text{д}}}{\mathrm{T}^i_{\text{порушника}} + \mathrm{T}^{\sum r}_{\text{порушника}}}, \quad (16)$$

де $\mathrm{T}^i_{\text{порушника}}$ — час, необхідний порушнику для знаходження i-го значення ключової інформації, $\mathrm{T}^{\sum r}_{\text{порушника}}$ — час, необхідний порушнику на перебір $\sum r$ перетворень ключової інформації.

Час, необхідний порушнику для знаходження i-го значення ключової інформації, визначатиметься як:

$$\mathrm{T}_{\text{порушника}}^{\sum r} = \frac{N_{KA}}{n(t)}, \tag{17}$$

де N_{KA} — простір значень, прийнятий решіткою КА.

Час, необхідний порушнику на перебір $\sum r$ перетворень ключової інформації, визначатиметься як:

$$\mathrm{T}_{\text{порушника}}^{\sum r} = \sum r \cdot \mathrm{T}_{\text{порушника}}^{1}, \tag{18}$$

де $\sum r$ — максимально можливе число здійснених перетворень ключової інформації в апаратурі абонентів безпроводової мобільної мережі за час доступу $\mathrm{T}_{\text{доступу}}$ порушника; $\mathrm{T}_{\text{порушника}}^{1}$ — час, що витрачається порушником на виконання одного перетворення. Позначимо за $\mathrm{T}_{\text{ітерації}}$ час між ітераціями оновлення ключової інформації, тоді:

$$\mathrm{T}_{\text{порушника}}^{\sum r} = \frac{\mathrm{T}_{\text{д}} \cdot (\mathrm{T}_{\text{ітерації}} - \Delta\mathrm{T})}{\mathrm{T}_{\text{ітерації}} \cdot n(t)} \cdot \eta, \tag{19}$$

де ΔT=0,5 с — тимчасове припущення, що відводиться на затримки, які виникають при передачі інформації каналом зв'язку; η — продуктивність обчислювача абонента безпроводової мобільної мережі, що забезпечує перетворення інформації. Тоді, враховуючи (17) і (19), для розробленого алгоритму формування ключової інформації ймовірність компрометації ключової інформації за час доступу $\mathrm{T}_{\text{доступу}}$ до неї порушника становитиме:

$$P_{\text{компрометації}} = \frac{\mathrm{T}_{\text{д}}}{\frac{N_{KA}}{n(t)} + \frac{\mathrm{T}_{\text{д}} \cdot (\mathrm{T}_{\text{ітерації}} - \Delta\mathrm{T})}{\mathrm{T}_{\text{ітерації}} \cdot n(t)} \cdot \eta}, \tag{20}$$

З метою збільшення безпеки ключі повинні регулярно оновлюватися. Це може відбуватися під час періодичних переавтентифікацій або за допомогою протоколів обміну ключами.

Протокол автентифікації та безпеки для мобільних мереж ґрунтується на оригінальних схемах підпису Ель Гамаля [18] – [20], [24] і протоколі розподілу ключів Діффі-Хеллмана [19], [22], [25]. Безпека цих схем ґрунтується на складності обчислення дискретного логарифму в скінченному полі, порівняно з легкістю обчислення піднесення до ступеня в тому ж самому скінченному полі, порівняно з простотою обчислення експоненції у тому ж скінченному полі.

Одним із ключових аспектів безпеки цих схем є їхній фундаментальний базис на складності обчислення дискретного логарифму в скінченному полі. Цей математичний принцип визначає складність визначення аргументу під експонентою у відомому виразі, що надає високий рівень вірогідності захисту від несанкціонованого доступу та кібератак. Однак слід також враховувати, що простота обчислення піднесення до ступеня та експонентації у тому ж самому скінченному полі створює виклики в плані забезпечення стійкості криптосистем, оскільки це може підвищити ризик кібератак. Тому важливим завданням є постійний моніторинг та аналіз їхньої безпеки, а також впровадження додаткових заходів захисту для підвищення стійкості системи у змінних умовах мобільних мереж. Зважаючи на постійний розвиток технологій інформаційного обміну в безпроводових мобільних мережах, важливо враховувати динаміку цих систем та пристосовувати методи безпеки до нових викликів, таких як кібератаки на мобільні пристрої. Інформаційний обмін в безпроводових мережах вимагає постійного

вдосконалення криптографічних методів для забезпечення конфіденційності та цілісності даних.

Розглядаючи сценарій, в якому мобільний користувач прагне встановити сеанс зв'язку з базовою станцією, варто припустити, що в мобільній мережі існує довірений центр сертифікації, що відповідає за забезпечення відкритих ключів для учасників мережі, включаючи мобільних користувачів та базові станції. Довірений центр сертифікації надає важливу послугу сертифікації відкритих ключів з метою забезпечення безпеки та конфіденційності в обміні інформацією між учасниками мережі. В рамках цього процесу довірений центр сертифікації використовується для підтвердження відкритих ключів, які використовуються в криптографічних операціях мобільними пристроями. Мобільні користувачі та базові станції отримують сертифікати від довіреного центру, які підтверджують їхні відкриті ключі. Цей процес забезпечує не тільки автентифікацію, але і гарантує надійність відкритих ключів, використовуваних учасниками мережі.

Крім того, такий центр сертифікації створює основу для встановлення захищеного каналу зв'язку між мобільним користувачем і базовою станцією. Використовуючи сертифікати відкритих ключів, сторони можуть обмінюватися інформацією, яка зашифрована відповідно до забезпечених ключів, що забезпечує конфіденційність даних під час комунікації. Такий підхід впроваджує високий стандарт безпеки в процес налаштування сеансу зв'язку між мобільним користувачем та базовою станцією в мобільній мережі:

1. Відповідно до Стандарту цифрового підпису (DSS) [10], центр сертифікації обирає три параметри (p, q, g), де p — велике просте число, q — великий простий множник $p-1$, $p = h^{\frac{(p-1)}{q}} \ (mod\ p)$, де h — ціле число, що задовольняє вимогам стандарту $1 < h < p-1$ та $h^{\frac{(p-1)}{q}} \ (mod\ p) > 1$.

2. Кожен учасник мережі повинен згенерувати пару відкритих і секретних ключів. Пара відкритих ключів центру сертифікації має вигляд $(y_{\text{центра сертифікації}}, x_{\text{центра сертифікації}})$, де $y_{\text{центра сертифікації}} = g^{x_{\text{центра сертифікації}}} \ (mod\ p)$, та $x_{\text{центра сертифікації}}$ — це випадково обране таємне число з $GF(p)^{\star}$. Аналогічно, пара відкритих ключів мобільного користувача m позначається як (y_m, x_m), а пара ключів базової станції b позначається як $y_b, x_b)$. Після генерації своїх пар відкритих ключів мобільні користувачі можуть вивести q та g зі своєї пам'яті, щоб заощадити місце в пам'яті.

3. Усі учасники обчислюють свої хеш-значення. Наприклад, для мобільного користувача, використаємо формат сертифіката X.509 для побудови C_m [21] – [26]. Він може містити таку інформацію, як серійний номер сертифіката, термін дії, ідентифікатор m, відкритий ключ (y_m) m, ідентифікатор центру сертифікації, відкритий ключ $(y_{\text{центра сертифікації}})$ та інше. Потім обчислюємо хеш-значення $h(C_m)$ для C_m, використовуючи односторонню $2n$-бітову хеш-функцію, яка базується на $2n$-бітовому блочному шифрі з $2n$-бітовим ключем (наприклад, IDEA [22]) (рис. 8):

ISSN 2663 - 4023

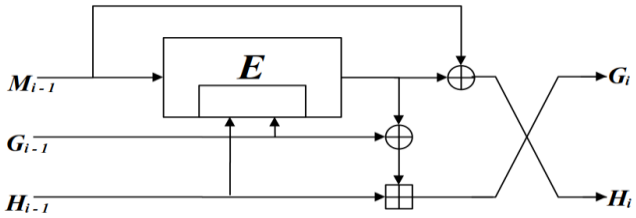

Рис. 8. Обчислювальний граф для функції хеш-раунду h
Джерело: розроблено автором в середовищі LibreOffice (знімок з екрану)

де M_i, G_i та H_i — n-бітові цілі числа; E — представляє n-бітовий блочний шифр з використанням $2n$-бітового ключа; $\oplus$ представляє побітово-виключне або з n-бітових блоків, в той час як $\boxplus$ вказує на додавання по модулю 2^n n-бітових цілих чисел [20] – [22], [24], [27].

Обчислювальний граф для функції хешування на один раунд (позначений як h) — це візуальне зображення, яке демонструє послідовні кроки, необхідні для обчислення значення хешу під час одного раунду. Вузли введення представляють вхідні дані для функції хешування на раунді. У контексті криптографічного хешування, це можуть бути оброблюваний блок даних, поточний стан хешу та, можливо, константа для конкретного раунду [20], [21], [23], [25], [26]. Вузли операцій представляють різні математичні операції, які виконуються під час раунду хешування. До них входять операції бітового зсуву, модулярного додавання та інші нелінійні функції. Вузли проміжного стану — проміжні стани обчислення хешу. На різних етапах графу дані піддаються трансформаціям через визначені операції. Вузол остаточного значення хешу відображає вихід функції хешу після завершення визначеної кількості раундів. Остаточне значення хешу зазвичай визначається кумулятивним ефектом всіх раундів на вхідні дані. Кожна стрілка в графі представляє потік даних від одного вузла до іншого, а з'єднання між вузлами вказує на послідовність виконання операцій.

Важливо пам'ятати, що конкретна структура обчислювального графа залежить від алгоритму функції хешування, який використовується (наприклад, SHA-256, MD5, RIPEMD, Tiger-2 і т. п.).

4. Центр сертифікації створює сертифікати для всіх учасників. Цифровий підпис центру сертифікації для повідомлення C складається з двох чисел, s та t, які визначаються наступним чином:

$$s = g^r (mod\ p), \tag{21}$$

$$t = -s - h(C) \cdot r \cdot x_{\text{центра сертифікації}}^{-1} (mod\ q), \tag{22}$$

де r — це випадкове число, вибране з $GF(p)^\star$.

Маючи (C^*, s^*, t^*), можна перевірити, чи дійсно (s^*, t^*) є справжнім підписом центру сертифікації для C^*, тільки перевіривши наступне рівняння:

$$y_{\text{центра сертифікації}}^{s^*+t^*} \cdot s^{h(C^*)} (mod\ p) = 1, \tag{23}$$

Можна прийняти цифровий підпис сертифікаційного центру на повідомлення C^*, якщо виконується наведене вище рівняння.

Взаємна автентифікація та розподіл ключів є важливими аспектами безпечного зв'язку в різних системах мереж. Ці процеси відіграють фундаментальну роль у забезпеченні можливості обох сторін у взаємному підтвердженні власної ідентичності та встановленні спільного секретного ключа для безпечного обміну даними.

Взаємна автентифікація представляє собою складний двосторонній процес перевірки, при якому обидві сторони, що взаємодіють, прагнуть підтвердити законність одна одної. В рамках цього процесу кожна сторона надає власні облікові дані або докази ідентичності, а обидві сторони здійснюють перевірку отриманої інформації з метою встановлення взаємного довіри. Під час взаємної автентифікації кожна сторона демонструє свою легітимність, надаючи переконливі облікові дані або використовуючи докази ідентичності, які підтверджують її правомірність у комунікації. Отримана інформація обмінюється обома сторонами, які активно перевіряють та аналізують її для забезпечення достовірності. Цей процес спрямований на запобігання несанкціонованому доступу та впевненість у тому, що комунікація відбувається тільки між взаємно автентифікованими та авторизованими сутностями.

В результаті взаємної автентифікації встановлюється взаємний рівень довіри, що є важливим аспектом в області забезпечення інформаційної безпеки. Цей процес гарантує, що обидві сторони в комунікації є справжніми та повноважними, сприяючи тим самим відсутності несанкціонованого доступу та надаючи основу для безпечної обміну даними.

Розподіл ключів представляє собою важливий етап в області криптографії, спрямований на безпечний обмін криптографічними ключами між автентифікованими сутностями. Основна мета цього процесу полягає в створенні спільних секретних ключів, які в подальшому використовуються для забезпечення конфіденційності та цілісності даних під час комунікації. Ключове значення розподілу ключів проявляється у забезпеченні безпеки взаємних комунікацій. Взаємна автентифікація, тобто процес взаємної перевірки ідентичності комунікуючих сторін, вимагає ефективного механізму для встановлення та обміну спільним секретним ключем. Цей спільний секретний ключ стає фундаментальним елементом для подальшої криптографічної захисту інформації, що передається між сторонами.

Важливість правильного виконання процесу розподілу ключів набуває особливого значення у сучасних мережевих та безпекових додатках, де конфіденційність та цілісність даних є критичними аспектами. Ефективний механізм розподілу ключів стає гарантією безпеки та відсутності несанкціонованого доступу до інформації, що обмінюється між взаємодіючими сутностями.

Разом взаємна автентифікація та розподіл ключів сприяють загальній безпеці мережевих систем, запобігаючи несанкціонованому доступу, захищаючи конфіденційність даних та гарантуючи цілісність обмінюваної інформації. Ці механізми особливо важливі у сценаріях, таких як безпечні онлайн-транзакції, комунікація між пристроями Інтернету речей та захист чутливої інформації в різноманітних застосунках.

Припустимо, що:

$$cert_{\text{центра сертифікації, } b} = (C_b, s_b, t_b), \quad (24)$$

$$cert_{\text{центра сертифікації, } m} = (C_m, s_m, t_m), \quad (25)$$

і припускаємо, що мобільний користувач m знаходиться у стільниковій мережі або блукає в зоні дії базової станції b, яку покриває базова станція b. Процес взаємної автентифікації між m та b, а також розподіл ключів від b до m узагальнено нижче:

1. Мобільний користувач $m \Longrightarrow$ базова станція b.

Коли мобільний користувач m бажає встановити сеанс зв'язку з базовою станцією, він надсилає базовій станції повідомлення SETUP та свій сертифікат $cert_{\text{центра сертифікації, } m}$, яку зберігається в його пам'яті.

2. Мобільний користувач $m \Longleftarrow$ базова станція b.

Базова станція може перевірити чи (s_m, t_m) є справжнім підписом центру сертифікації на C_m, перевіривши рівність (23). Якщо рівність виконується, значить мобільний користувач вже зареєструвався раніше, базова станція приймає цифровий підпис центру сертифікації на C_m. Потім вона надсилає мобільному користувачу повідомлення CONNECT, свій сертифікат $cert_{\text{центра сертифікації, } b}$ та $y_m^{-x_b} \cdot K(mod\ p)$ мобільному користувачу, де K – $2n$-бітове випадкове число.

3. Мобільний користувач $m \iff$ базова станція b.

Мобільний користувач може перевірити чи (s_b, t_b) є справжнім підписом центру сертифікації на C_b, перевіривши рівність (3). Якщо рівність виконується, мобільний користувач приймає цифровий підпис центру сертифікації на C_b. Потім він може визначити K з $y_m^{-x_b} \cdot K(mod\ p)$, обчисливши:

$$(y_b)^{x_m} \cdot (y_m^{-x_b} \cdot K)\ (mod\ p) = K, \tag{26}$$

Нарешті, інформація, що передається між мобільним користувачем та базовою станцією, може бути зашифрована та розшифрована блоковим шифром із $2n$-бітовим спільним ключем K. Блоковий шифр такий самий, як і базовий блоковий шифр у хеш-функції (рис. 8). Цей блоковий шифр використовується для забезпечення конфіденційності інформації, забезпечуючи високий рівень захисту даних під час їх передачі між мобільними користувачами та базовими станціями в безпроводових мобільних мережах. У зазначеному блоковому шифрі ключ K є спільним для обох сторін — мобільного користувача і базової станції. Це гарантує взаємне розуміння та співробітництво при шифруванні та розшифруванні даних. Крім того, блоковий шифр використовується у вигляді базового блокового шифру в хеш-функції, надаючи високий рівень захисту від несанкціонованого доступу та забезпечуючи цілісність переданих блоків інформації. Використання блокового шифру для забезпечення безпеки даних є стратегічно важливим, оскільки цей механізм дозволяє ефективно захищати інформацію від несанкціонованого доступу та забезпечує її конфіденційність [25] – [28]. Враховуючи, що блоковий шифр використовує спільний ключ K, важливо забезпечити безпеку обміну цим ключем між мобільним користувачем і базовою станцією, щоб уникнути можливих атак на криптографічні механізми. Вищезазначений процес можна показати, за допомогою рис. 9.

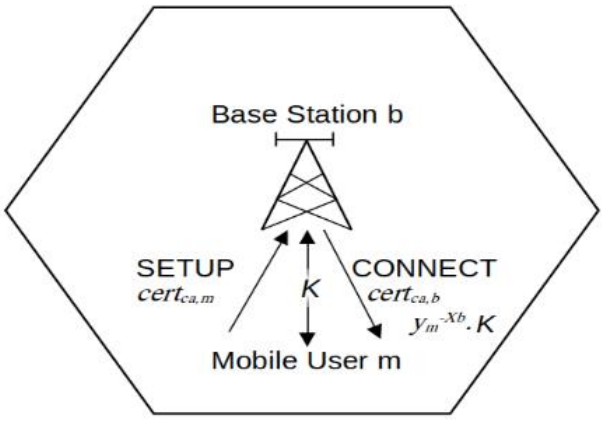

Рис. 9. Графічне зображення протоколу
Джерело: розроблено автором в середовищі LibreOffice (знімок з екрану)

ISSN 2663 - 4023

Через участь секретного ключа$x_{\text{центру сертифікації,}}$ центру сертифікації у формуванні цифрового підпису (s,t) центру сертифікації на повідомлення C, зловмисник не може використати рівняння (21) та (22) для того, щоб підробити справжню пару підписів (s,t).

Зловмисник може спробувати вибрати випадкове число s (або t), а потім знайти t (або s) з рівняння (23), щоб підробити справжню пару (s,t). Однак складність цієї задачі щонайменше дорівнює складності обчислення логарифма над скінченими полями.

Беручи до уваги, що зловмисник не знає, як обчислити $y_m^{x_b}$ (або $y_b^{x_m}$), і для чого потрібен секретний ключ x_b базової станції (або секретний ключ x_m мобільного користувача), він не може обчислити ключ K з $y_m^{-x_b} \cdot K\ (mod\ p)$.

У відповідності до запропонованого протоколу, відтворення кібератаки стає технічно неможливим завдяки вдосконаленим заходам безпеки [27] – [28]. Навіть у випадку, коли зловмисник здатен перехопити сертифікати мобільного користувача та базової станції, спроби використання їхньої ідентичності для надсилання запитів чи відповідей виявляться невдалими, оскільки він не отримає доступ до секретного ключа [1], [4] – [9]. Якщо виникають труднощі із відновленням відкритого тексту з зашифрованого, зв'язок між мобільним користувачем та базовою станцією буде негайно перервано, утруднюючи подальше втручання.

Порівняльний аналіз запропонованого протоколу з існуючими включає оцінку різних аспектів, що дозволяє визначити його переваги та недоліки. Ключові критерії для розгляду включають аналіз криптографічних механізмів, використаних у кожному протоколі, перевірку стійкості до потенційних загроз безпеки, таких як кібератаки «людина посередині», прослуховування та кібератаки повторного відтворення. Також важливим є оцінка стійкості протоколів до відомих криптографічних вразливостей, що підсилює рівень їхньої надійності в реальних умовах експлуатації.

Під час порівняння методів автентифікації користувача та базової станції важливо аналізувати ефективність та надійність процесу автентифікації для запобігання несанкціонованому доступу.

Оцінка механізмів розподілу ключів передбачає вивчення того, як в кожному протоколі вирішується цей процес, аналіз методів генерації, обміну та оновлення криптографічних ключів, а також оцінку стійкості до компрометації ключів та ефективності управління ними [7] – [11], [14].

Оцінка обчислювальних вимог кожного протоколу включає аналіз складності криптографічних операцій, використовуваних у процесах автентифікації та розподілу ключів, з урахуванням впливу на продуктивність системи та використання ресурсів.

Оцінка вимог до пам'яті кожного протоколу, особливо на мобільних пристроях, включає розгляд ефективності використання пам'яті для зберігання публічних ключів, сертифікатів та іншої важливої інформації.

Аналіз споживання енергії під час виконання кожного протоколу передбачає врахування впливу на тривалість роботи батареї мобільних пристроїв та загальної енергоефективності мережі.

Оцінка стійкості протоколів до різних типів атак, зокрема до вразливостей в процесах автентифікації та розподілу ключів, є важливою для забезпечення безпеки системи.

Розгляд масштабованості включає оцінку того, наскільки добре кожен протокол впорається зі зростанням кількості користувачів та пристроїв в мережі. Також важливо розглядати ефективність протоколу при обробці зростаючої кількості запитів на автентифікацію [22], [23] – [26].

ISSN 2663 - 4023

Оцінка практичності та реалізованості в кожному протоколі в реальних сценаріях та сумісність з існуючою інфраструктурою та пристроями є важливими факторами для успішної імплементації протоколу в реальному середовищі.

Важливим критерієм для нового протоколу автентифікації та забезпечення безпеки є врахування простоти алгебраїчних операцій та ефективного використання пам'яті мобільного користувача. Зокрема, для забезпечення оптимальної ефективності у безпроводових мобільних мережах, де обмін інформацією відбувається через безпровідний канал, важливо розглядати аспекти інформаційного обміну. Взаємодія між мобільним користувачем та базовою станцією передбачає постійний потік даних, що вимагає оптимізованих процесів автентифікації та обміну ключами. Протокол повинен мінімізувати кількість повідомлень та обчислювальні витрати, забезпечуючи при цьому надійний та безпечний обмін інформацією.

У контексті інформаційного обміну в безпроводових мобільних мережах, новий протокол повинен ефективно використовувати обмежені ресурси мобільних пристроїв, забезпечуючи при цьому високий рівень безпеки. Впровадження простих алгебраїчних операцій та оптимізованих процесів обміну ключами сприятиме покращенню продуктивності та зниженню навантаження на мобільні пристрої під час здійснення автентифікації та забезпечення безпеки в безпроводових мережах.

У порівнянні зі Стандартом цифрового підпису [19] – [25], [28] та протоколом [17], [26] – [28], нова пропозиція має наступні покращення:

1. Процедура перевірки сертифікату та операції за новою пропозицією є простішою, ніж у DSS, тому що DSS має обчислювати модуль q і множення, обернене до модуля q, окрім операцій за новою пропозицією. Це дозволяє знизити обчислювальні витрати та спростити реалізацію процедур на мобільних пристроях.

2. Згідно з DSS, всі учасники мобільної мережі зобов'язані спільно використовувати три публічні (відкриті) параметри $(p,\ q,\ g)$ та публічний (відкритий) ключ центру сертифікації ($y_{\text{центра сертифікації}}$). Це необхідно для процедури перевірки сертифікації. У новій пропозиції для перевірки сертифікації достатньо одного публічного (відкритого) параметра (p) та публічного ключа центру сертифікації ($y_{\text{центра сертифікації}}$). У зв'язку з цим мобільний користувач має звільнити q та g з пам'яті, щоб зекономити місце після того як він отримає свій сертифікат від центру сертифікації, тобто є додатковим ресурсом економії місця в пам'яті.

3. На етапі взаємної автентифікації між мобільним користувачем та базовою станцією мобільної мережі, мобільному користувачу в протоколі Чжена потрібен криптографічно стійкий генератор псевдовипадкових чисел (G), для формування справжньої пари (c_1, c_2) для передачі сеансового ключа K від мобільного користувача до базової станції. Це може суперечити з обмеженням низького енергоспоживання мобільного користувача. А в новій пропозиції функція генерації випадкових чисел розташована на базовій станції, спрощуючи таким чином обчислювальні завдання мобільного пристрою та зменшуючи його споживання енергії. Мобільний користувач повинен лише перевірити сертифікацію базової станції та відокремити сеансовий ключ K з $y_m^{-x_b} \cdot K\ (mod\ p)$.

Отже, у цій пропозиції блоковий шифр з секретним ключем E також виступає в якості базового блочного шифру хеш-функції (зображеної на рис. 8), щоб полегшити програмну та апаратну реалізацію нової пропозиції та зекономити місце в пам'яті. Це особливо важливо для мобільного користувача, який працює в умовах обмеженого енергоспоживання. Нова пропозиція поєднує простоту процедур, ефективне

використання ресурсів та збереження енергії, сприяючи покращенню безпеки та функціональності мобільних мереж.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Рух абонентів у мережі та зміна топології безпроводової мобільної мережі може становити виклики для ефективного управління безпекою в мобільних середовищах, включаючи захист від потенційних кібератак. Застосування передових криптографічних методик та розробка надійних криптосистем для захисту ключової інформації стають невід'ємною частиною зусиль у забезпеченні безпеки та конфіденційності даних у цих динамічних умовах. Формування ключової інформації у безпроводових мобільних мережах є критичним етапом для забезпечення безпеки передачі даних і захисту від несанкціонованого доступу. Ключова інформація, що генерується для мобільних пристроїв, використовується для шифрування та розшифрування даних, які передаються через бездротовий канал.

Формування ключової інформації у безпроводових мобільних мережах є складним та важливим процесом, спрямованим на забезпечення безпеки зв'язку між пристроями та базовими станціями. Перший етап цього процесу — автентифікація та реєстрація пристрою в мережі. Під час цього етапу відбувається перевірка правомірності доступу до мережі, а після успішної автентифікації формується ключова інформація. Ключова інформація включає в себе секретні ключі, які використовуються для шифрування та розшифрування даних. Генерація цих ключів зазвичай здійснюється за допомогою криптографічних протоколів, таких як Diffie-Hellman, забезпечуючи безпеку обмінюваних ключів у криптосистемах.

Одержані ключі використовуються для шифрування даних, що передаються через мережу, забезпечуючи їх конфіденційність. Додатково, для забезпечення цілісності та автентифікації даних можуть використовуватися коди автентифікації повідомлень. З метою збільшення безпеки ключі повинні регулярно оновлюватися. Це може відбуватися під час періодичних переавтентифікацій або за допомогою протоколів обміну ключами. Паралельно з цими процесами, мережі повинні вживати заходів безпеки для виявлення та запобігання атакам, спрямованим на злам ключової інформації, включаючи кібератаки. Системи виявлення вторгнень та інші методи виявлення аномалій є необхідними для ефективного реагування на потенційні загрози. Управління ключами відіграє ключову роль у безпеці мережі, забезпечуючи безпечний розподіл, оновлення та вилучення ключів. Ефективне управління ключами гарантує, що криптографічні засоби залишаються стійкими та відповідають сучасним вимогам безпеки. Усі ці процеси сприяють створенню безпечного та ефективного каналу зв'язку в безпроводових мобільних мережах, забезпечуючи конфіденційність, цілісність та доступність даних.

Запропонований протокол безпеки для мобільних мереж впроваджує інноваційні особливості, спрямовані на оптимізацію його функціоналу та ресурсоємності. У порівнянні з іншими протоколами, ключові аспекти включають обмежену кількість необхідних публічних (відкритих) параметрів (великого простого числа p та відкритого ключа центру сертифікації), які є обов'язковими для всіх учасників мережі, що спрощує обчислювальні процеси та зменшує обсяг інформації. У цьому протоколі блоковий шифр виступає не лише як алгоритм шифрування з секретним ключем, а й як базовий блочний шифр для хеш-функції. Такий підхід сприяє ефективній реалізації та економії пам'яті, оскільки той самий блоковий шифр використовується для різних криптографічних

завдань, спрощуючи процес програмування та зменшуючи обчислювальні витрати. Важливим етапом цього протоколу є забезпечення безпеки інформаційного обміну в безпроводових мобільних мережах. Запропоновані зміни не лише спрощують обчислювальні операції, а й покращують використання ресурсів, що робить протокол ефективним і перспективним у контексті сучасних технологій мобільних мереж.

Протокол безпеки для мобільних мереж, який був запропонований, виявляється винятковим у своїй спрощеній архітектурі та ефективному використанні ресурсів. У контексті автентифікації між мобільним користувачем та базовою станцією, протокол впроваджує інноваційний підхід до генерації випадкових чисел. Місце для криптографічно стійкого генератора випадкових чисел знаходиться в базовій станції, що мінімізує його використання в мобільному пристрої. Цей хід має важливі наслідки для передачі сесійного ключа K між користувачем та базовою станцією. Зокрема, спрощення використання генератора випадкових чисел у мобільному пристрої сприяє економії енергії та уникненню конфліктів із стриманим енергоспоживанням мобільного користувача. Такий підхід визначається як оптимальний в умовах обмеженої енергії мобільних пристроїв, забезпечуючи при цьому надійний та безпечний обмін інформацією між користувачем та мережею, що включає використання криптографічних методів для захисту даних від кібератак. Важливою особливістю протоколу є те, що секретний блоковий шифр E виконує функцію як алгоритм секретного шифрування, так і основний блоковий шифр для хеш-функції, що сприяє зручності в реалізації протоколу та економії місця в пам'яті, що надзвичайно важливо для мобільних пристроїв з обмеженим ресурсом енергії. Також, ефективне управління криптосистемою забезпечує належний рівень захисту від можливих загроз і зловживань. Безпека безпроводових мобільних мереж — це постійний процес, і стратегії безпеки повинні регулярно оновлюватися, враховуючи нові технології та загрози.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Li, G., Luo, H., Yu, J., Hu, A., & Wang, J. (2023). Information-Theoretic Secure Key Sharing for Wide-Area Mobile Applications. *Computing Research Repository, 2301.*
2. Maurer, U. M. (1993). Secret key agreement by public discussion from common information. *IEEE Trans. Inf. Theory, 39(3),* 733–742.
3. Li, G., Zhang, Z., Zhang, J., & Hu, A. (2021). Encrypting wireless communications on the fly using one-time pad and key generation. *IEEE Internet of Things Journal, 8,* 357–369.
4. Li, G., Yang, H., Zhang, J., Liu, H., & Hu, A. (2022). Fast and secure key generation with channel obfuscation in slowly varying environments. *IEEE INFOCOM, Virtual Conference*, 1–10.
5. Shibu, K. R., & Sujipramila, R. (2021). Secret Key Generation by Exploiting Traffic Load for Mobile Adhoc Networks. *Wireless Personal Communicatio*ns, *119(2).*
6. He, S., Zhu, L., Yao, C., Zeng, W., & Qin, Z. (2022). A Novel Approach Based on Generative Adversarial Network for Interference. *Detection in Wireless Communications" Wireless Communications and Mobile Computing*, *2*. https://doi.org/10.1155/2022/7050573
7. Mahshid, M.-K., & Eslamipoor, R. (2013). An optimized authentication protocol for mobile networks Neural. *Computing and Applications, 25(2).*
8. Martin, K. M., & Mitchell, C. J., (1999). Comments on an optimized protocol for mobile network authentication and security. A*CM SIGMOBILE Mobile Computing and Communications Review, 3(2).*
9. Chien, H.-Y., & Jan, J.-K. (2003). Robust and Simple Authentication Protocol. *The Computer Journal, 46(2).*
10. Костюк, Ю. В., & Шапран, В. О. (2024). Технології виявлення аномальних подій та сигнатур в реальному часі. *«Наука і техніка сьогодні» (Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»), 4(32),* 1069–1084.

11. Aziz, A. & Diffie, W. (1994). Privacy and authentication for wireless local area networks. *IEEE Personal Communications, 1(1),* 25–31.
12. Костюк, Ю. В. (2024). Стратегії захисту крайових пристроїв з використанням нейронних мереж Коско. *Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Збірник матеріалів доповідей та тез*, 17–18.
13. Brown, D. (1995). Technical for privacy and authentication in personal communications systems. *IEEE Personal Communications, 2(4),* 6–10.
14. Wilkes, J. (1995). Privacy and authentication needs of PCS. *IEEE Personal Communications, 2(4),* 11–15.
15. Frankel, Y., Herzberg, A., Karger, E., Krawczyk, H., Kunzinger, C., & Yung, M. (1995). Security issues in a CDPD wireless network. *IEEE Personal Communications, 2(4),* 16–27.
16. Beller, M., EChang, L., & Yacobi, Y. (1993). Privacy and authentication on a portable communications system. *IEEE Journal on Selected Areas in Communications, 11(6),* 821–829.
17. Aziz, A., & Diffie, W. (2012). Privacy and authentication for wireless local area networks. *IEEE Personal Communications, 1(1),* 25–31.
18. Zheng, Y. (1996). An Authentication and Security Protocol for Mobile Computing. *Mobile Communications - Technology, Tools, Applications, Authentication and Security (Proceedings of IFIP World Conference on Mobile Communications),* 249–257.
19. E1Gamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithm. *IEEE Trans. Info. Theory, IT31(4),* 468–472.
20. Diffie, W., & Hellman, M. (1976). New direction in cryptography. *IEEE Transactions on information theory, IT-22(6),* 472–492.
21. Lai, X. J., & Massey, J. L., (1991). A proposal for a new block encryption standard. *Advances in Cryptology, Proc. of EUROCRYPT'90, Lecture Notes in Computer Science, 473,* 389–404.
22. Yi, X., & Lam, K. Y., (1997). Hash function based on block cipher. *IEE Electronics Letters, 33(23).*
23. Kim, K., & Lee, D. (2015). Secure Route Optimization Scheme for Network Mobility Support in Heterogeneous Mobile Networks. *Wireless Personal Communications, 94(3).*
24. Dzaferagic, M., Kaminski, N., McBride, N., Macaluso, I., & Marchetti, N. (2018). A functional complexity framework for the analysis of telecommunication networks, *Journal of Complex Networks, 6(6),* 971–988. https://doi.org/10.1093/comnet/cny007
25. Костюк, Ю. В., Голинський, А. (2024). Стратегії інтегрованого захисту бездротових сенсорних мереж. «*Наука і техніка сьогодні» (Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»), 5(33),* 1232–1247.
26. Almeida, W. R., Andaló, F. A., Padilha, R., Bertocco, G., & Dias, W. (2020). Detecting face presentation attacks in mobile devices with a patch-based. *CNN and a sensor-aware loss function" PLoS ONE, 15(9).*
27. Zhang, J., & Liu, Q. (2023). New key management scheme lattice-based for clustered wireless sensor networks. *PLoS ONE, 18(8).*
28. Yap, K.-L., Chong, Y.-W., & Liu, W. (2020). Enhanced handover mechanism using mobility prediction in wireless networks. *PLoS ONE, 15(1).*

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023

Yuliia Kostiuk
PhD in Computer Science
Associate Professor of the Department of Information and
Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0001-5423-0985
y.kostiuk@kubg.edu.ua

Bohdan Bebeshko
PhD in Computer Science
Associate Professor of the Department of Information and
Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0001-6599-0808
b.bebeshko@kubg.edu.ua

Larysa Kriuchkova
Doctor of sciences, Professor
Professor of the Department of Information and
Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID:0000-0002-8509-6659
l.kriuchkova@kubg.edu.ua

Valerii Lytvynov
Doctor of Technical Sciences, Professor
Institute of Problems of Mathematical Machines and
Systems of NAS of Ukraine, Kyiv, Ukraine
ORCID ID: 0000-0001-5568-7629
litval@dr.com

Iryna Oksanych
PhD of Technical Sciences, Senior Researcher
Institute of Problems of Mathematical Machines and
Systems of NAS of Ukraine, Kyiv, Ukraine
ORCID ID: 0000-0002-1208-3427
inokc2018@gmail.com

Pavlo Skladannyi
PhD, Associate Professor, Head of the Department of Information and
Cyber Security named after Professor Volodymyr Buryachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

Karyna Khorolska
PhD in Computer Science
"LLC 'Gas Supply Company 'Naftogaz Trading", Kyiv, Ukraine
ORCID ID: 0000-0003-3270-4494
karynakhorolska@gmail.com

INFORMATION PROTECTION AND DATA EXCHANGE SECURITY IN WIRELESS MOBILE NETWORKS WITH AUTHENTICATION AND KEY EXCHANGE PROTOCOLS

Abstract. The mobility of users, signal transmission through open cyberspace, and the need for low energy consumption in mobile devices lead to numerous new challenges related to information protection in wireless mobile networks. Ensuring reliable and secure information exchange in such networks is critically important, as it largely depends on the level of protection of key information

used for network user authentication and data encryption during transmission. This article examines a protocol designed to provide effective authentication and security in mobile networks, focusing on the use of block cipher as the primary algorithm for secret key encryption and a basic cipher for hash functions. The protocol imposes minimal requirements on network participants, such as only needing to know the public parameter and the public key of the certification authority, which significantly simplifies its implementation and enhances reliability. Additionally, the article analyzes the protocol's impact on overall security and resilience of mobile networks against various threats, including cyberattacks on the key exchange protocol, attempts to compromise information during transmission, and the role of cryptography in this context. Special attention is given to the role of the key management center and cryptosystems in ensuring information protection and mitigating risks associated with unauthorized data access in wireless mobile networks.

Keywords: information protection; authentication; security; information exchange; key exchange protocol; cyber resilience; cryptography; wireless mobile networks; mobile device; cryptosystem; key management center; cyberattack.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Li, G., Luo, H., Yu, J., Hu, A., & Wang, J. (2023). Information-Theoretic Secure Key Sharing for Wide-Area Mobile Applications. *Computing Research Repository, 2301.*
2. Maurer, U. M. (1993). Secret key agreement by public discussion from common information. *IEEE Trans. Inf. Theory, 39(3),* 733–742.
3. Li, G., Zhang, Z., Zhang, J., & Hu, A. (2021). Encrypting wireless communications on the fly using one-time pad and key generation. *IEEE Internet of Things Journal, 8,* 357–369.
4. Li, G., Yang, H., Zhang, J., Liu, H., & Hu, A. (2022). Fast and secure key generation with channel obfuscation in slowly varying environments. *IEEE INFOCOM, Virtual Conference*, 1–10.
5. Shibu, K. R., & Sujipramila, R. (2021). Secret Key Generation by Exploiting Traffic Load for Mobile Adhoc Networks. *Wireless Personal Communicatio*ns, *119(2).*
6. He, S., Zhu, L., Yao, C., Zeng, W., & Qin, Z. (2022). A Novel Approach Based on Generative Adversarial Network for Interference. *Detection in Wireless Communications" Wireless Communications and Mobile Computing*, *2*. https://doi.org/10.1155/2022/7050573
7. Mahshid, M.-K., & Eslamipoor, R. (2013). An optimized authentication protocol for mobile networks Neural. *Computing and Applications, 25(2).*
8. Martin, K. M., & Mitchell, C. J., (1999). Comments on an optimized protocol for mobile network authentication and security. A*CM SIGMOBILE Mobile Computing and Communications Review, 3(2).*
9. Chien, H.-Y., & Jan, J.-K. (2003). Robust and Simple Authentication Protocol. *The Computer Journal*, *46(2).*
10. Kostiuk, Y. V., & Shapran, V. O. (2024). Technologies for detecting anomalous events and signatures in real time. *"Science and Technology Today" (Series 'Pedagogy', Series 'Law', Series 'Economics', Series 'Physical and Mathematical Sciences', Series 'Technology'), 4(32),* 1069–1084.
11. Aziz, A. & Diffie, W. (1994). Privacy and authentication for wireless local area networks. *IEEE Personal Communications, 1(1),* 25–31.
12. Kostiuk, Y. V. (2024). Strategies for protecting edge devices using Kosko neural networks. *Problems of cybersecurity of information and telecommunication systems: Collection of reports and abstracts*, 17–18.
13. Brown, D. (1995). Technical for privacy and authentication in personal communications systems. *IEEE Personal Communications, 2(4),* 6–10.
14. Wilkes, J. (1995). Privacy and authentication needs of PCS. *IEEE Personal Communications, 2(4),* 11–15.
15. Frankel, Y., Herzberg, A., Karger, E., Krawczyk, H., Kunzinger, C., & Yung, M. (1995). Security issues in a CDPD wireless network. *IEEE Personal Communications, 2(4),* 16–27.
16. Beller, M., EChang, L., & Yacobi, Y. (1993). Privacy and authentication on a portable communications system. *IEEE Journal on Selected Areas in Communications, 11(6),* 821–829.
17. Aziz, A., & Diffie, W. (2012). Privacy and authentication for wireless local area networks. *IEEE Personal Communications, 1(1),* 25–31.
18. Zheng, Y. (1996). An Authentication and Security Protocol for Mobile Computing. *Mobile Communications - Technology, Tools, Applications, Authentication and Security (Proceedings of IFIP World Conference on Mobile Communications),* 249–257.

19. E1Gamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithm. *IEEE Trans. Info. Theory, IT31(4),* 468–472.
20. Diffie, W., & Hellman, M. (1976). New direction in cryptography. *IEEE Transactions on information theory, IT-22(6),* 472–492.
21. Lai, X. J., & Massey, J. L., (1991). A proposal for a new block encryption standard. *Advances in Cryptology, Proc. of EUROCRYPT'90, Lecture Notes in Computer Science, 473,* 389–404.
22. Yi, X., & Lam, K. Y., (1997). Hash function based on block cipher. *IEE Electronics Letters, 33(23).*
23. Kim, K., & Lee, D. (2015). Secure Route Optimization Scheme for Network Mobility Support in Heterogeneous Mobile Networks. *Wireless Personal Communications, 94(3)*.
24. Dzaferagic, M., Kaminski, N., McBride, N., Macaluso, I., & Marchetti, N. (2018). A functional complexity framework for the analysis of telecommunication networks, *Journal of Complex Networks, 6(6),* 971–988. https://doi.org/10.1093/comnet/cny007
25. Kostiuk, Y. V., Golynskyi, A. (2024). Strategies for integrated protection of wireless sensor networks. *"Science and Technology Today" (Series 'Pedagogy', Series 'Law', Series 'Economics', Series 'Physical and Mathematical Sciences', Series 'Technology'), 5(33),* 1232–1247.
26. Almeida, W. R., Andaló, F. A., Padilha, R., Bertocco, G., & Dias, W. (2020). Detecting face presentation attacks in mobile devices with a patch-based. *CNN and a sensor-aware loss function" PLoS ONE, 15(9).*
27. Zhang, J., & Liu, Q. (2023). New key management scheme lattice-based for clustered wireless sensor networks. *PLoS ONE, 18(8).*
28. Yap, K.-L., Chong, Y.-W., & Liu, W. (2020). Enhanced handover mechanism using mobility prediction in wireless networks. *PLoS ONE*, *15(1).*