Прикарпатський національний університет імені Василя Стефаника
Фізико-технічний факультет
Кафедра комп'ютерної інженерії та електроніки

Карбовський Ніколай Всеволодович
Nikolai Karbovskyi

УДК 004:42

Спеціальність 123 «Комп'ютерна інженерія»

Кваліфікаційна робота
на здобуття освітнього ступеня бакалавра

Криптографічні методи захисту даних в комп'ютерних мережах
Cryptographic methods of data protection in computer networks

Науковий керівник:
Кандитат к.ф.-м-н, доцент комп'ютерної інженерії та електроніки, Мирослав ПАВЛЮК
Рецензент:
Кандидат к.ф.-м.н, професор кафедри фізики і хімії твердого тіла, Любомир НИКИРУЙ.

Івано-Франківськ
2024

Формат	Поз.	Позначення	Найменування	К-ть	Прим.
А4			Архітектура WSN	1	
А4			Дизайн архітектури запропонованої PRE WSN	1	
А4			Пояснювальна записка	44	

Змн.	Арк.	№ докум.	Підпис	Дата	123.КІ-41.06		
Розробив		Карбовський Н.В.			Специфікація	Літ.	Арк. 2 / Аркушів 1
Перевірив		Павлюк М.Ф.					
Н. Контр.							
Затвердив							

АНОТАЦІЯ

У сфері бездротових сенсорних мереж (WSN) збереження цілісності даних, конфіденційності та безпека від кіберзагроз має першочергове значення. Повторне шифрування проксі (PRE) відіграє ключову роль у забезпеченні безпечного внутрішньомережевого зв'язку. Однак існуючі рішення PRE стикаються з постійними проблемами, включаючи затримки обробки через передачу значної кількості даних на проксі для повторного шифрування та обчислювальна інтенсивність асиметричної криптографії. Ця робота представляє інноваційну схему PRE, яка ретельно налаштована для WSN для забезпечення безпечного зв’язку між вузлами всередині мережі та зовнішнього сервера даних. Запропонована схема PRE оптимізує ефективність шляхом інтеграції полегшених симетричних та асиметричних криптографічних методів, що мінімізує обчислювальні витрати під час PRE роботи та збереження енергії для вузлів з обмеженими ресурсами.

Крім того, схема включає складне керування ключами та цифрові сертифікати для забезпечення безпечної генерації та розповсюдження ключів, яка у свою чергу, полегшує безперебійну автентифікацію та масштабований обмін даними між об’єктами в WSN. Ця схема
підтримує шифрування даних сенсорних вузлів і делегує завдання безпечного повторного шифрування виключно головам кластера, тим самим зміцнюючи конфіденційність і цілісність даних. Комплексна оцінка безпеки, продуктивності та споживання енергії підтвердила надійність схеми.

Результати підтверджують, що запропонована PRE схема значно підвищує безпеку, ефективність і загальний термін служби мережі WSN.

ABSTRACT

In the field of wireless sensor networks (WSNs), maintaining data integrity, privacy and security against cyber threats is of paramount importance. Re-Encrypted Proxy (REP) plays a key role in ensuring secure intra-network communication. However, existing PFS solutions face persistent challenges, including processing delays due to proxying large amounts of data for re-encryption and the computational intensity of asymmetric cryptography. This work presents an innovative PSHP scheme that is carefully tuned for BSM to provide secure communication between nodes within the network and an external data server.

The proposed PPS scheme optimizes efficiency by integrating lightweight symmetric and asymmetric cryptographic methods, which minimizes computational costs during PPS operation and conserves energy for nodes with limited resources. In addition, the scheme includes sophisticated key management and digital certificates to ensure secure key generation and distribution, which in turn facilitates seamless authentication and scalable data exchange between entities in the BSM. This scheme supports data encryption of sensor nodes and delegates the task of secure re-encryption exclusively to cluster heads, thereby strengthening data privacy and integrity. A comprehensive assessment of safety, performance and energy consumption confirmed the reliability of the scheme.

The results confirm that the proposed PSHP scheme significantly increases the security, efficiency and overall service life of the BSM network.

ПЕРЕЛІК ОСНОВНИХ СКОРОЧЕНЬ

WSN (Wireless Sensor Node) – бездротові сенсорні мережі

PRE (Proxy Re-Encryption) – повторне шифрування проксі

SN (Sensor Node) – сенсорний вузол

CH (Cluster Head) – голова кластеру

БС – базова станція

ТД – точка доступу

ШОІ - шифрування на основі ідентичності

ШОР - шифрування на основі ролей

ШОА - шифрування на основі атрибутів шифрування

ШОС - шифрування на основі сертифікату

IoT (Internet of Things) – інтернет речей

ECC (Elliptic Curve Encryption)- криптографія з еліптичною кривою

Sk (Symmetric key) – симетричний ключ

XOR – виключне АБО

AES (advanced encryption standard) - розширений стандарт шифрування

DES (data encryption standard) - стандарт шифрування даних

ID (Identificator) – унікальний ідентифікатор сенсорного вузла

Pk (Public key) – публічний ключ

Prk (Private key) – приватний ключ

TAN (Trusted Authority Node) - довірений авторитетний вузол

Crt (Certificate) – сертифікат

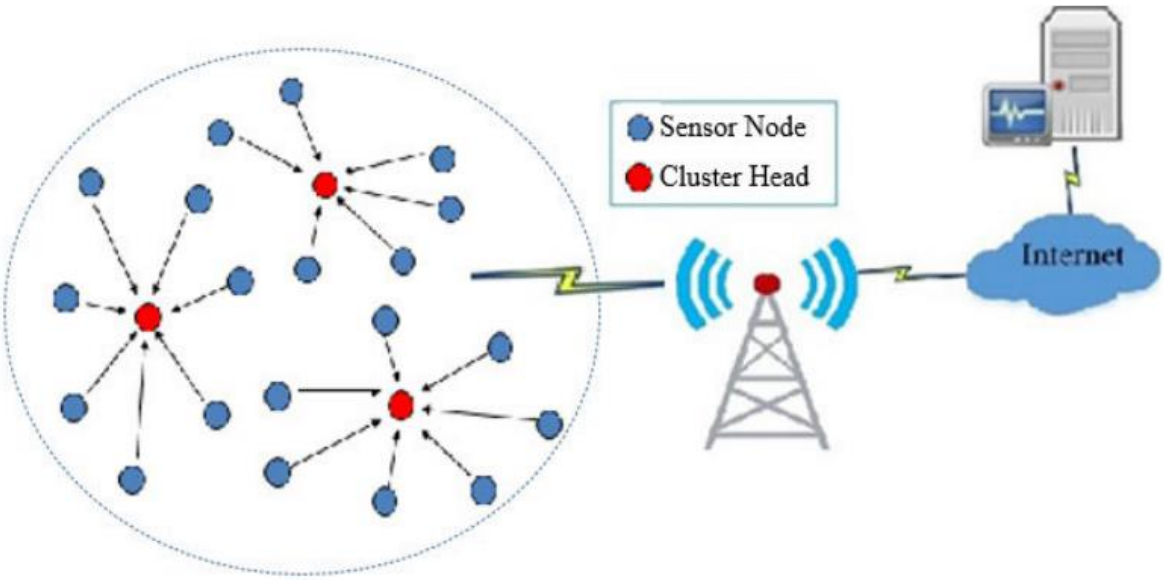
CID (Cluster ID) – ідентифікатор кластера

C (Cluster) – кластер

SID (SN ID) – унікальний ідентифікатор сенсорного вузла всередині кластеру

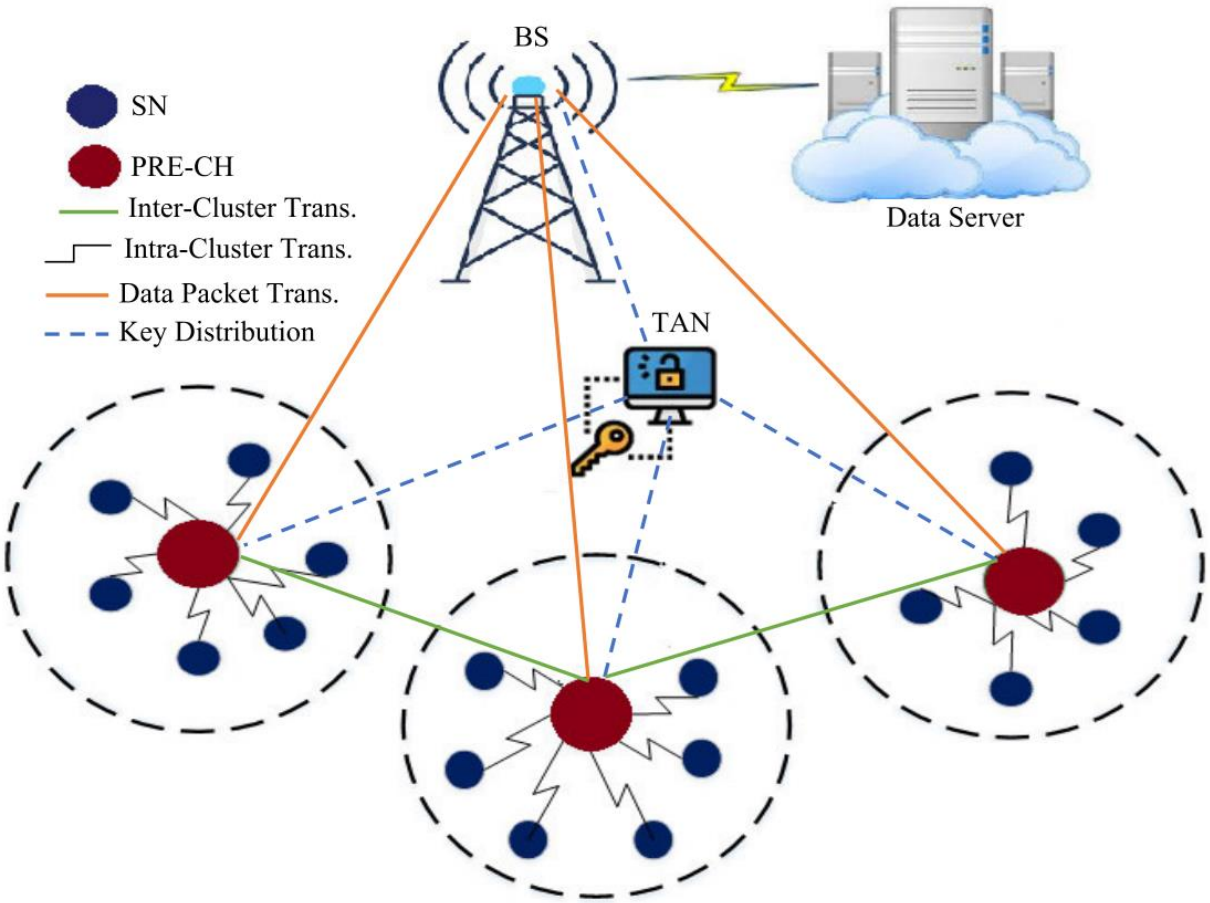
CrtSN – окремий сертифікат для кожного сенсорного вузла

CHID – унікальний ідентифікатор голови кластеру



					123.КІ-41.06
Змн.	*Арк.*	*№ докум.*	*Підпис*	*Дата*	
Розробив		Карбовський Н.В.			Архітектура WSN
Перевірив		Павлюк М,Ф.			
Н. Контр.					
Затвердив					

Літ.	*Арк.*	*Аркушів*
	5	1



					123.КІ-41.06		
Змн.	*Арк.*	*№ докум.*	*Підпис*	*Дата*			
Розробив		Карбовський Н.В.			Дизайн архітектури запропонованої PRE WSN	*Літ.*	*Арк.* 6 / *Аркушів* 1
Перевірив		Павлюк М.Ф.					
Н. Контр.							
Затвердив							

Пояснювальна записка

до кваліфікаційної роботи

на тему:

«Криптографічні методи захисту даних в комп’ютерних мережах»

					123.КІ-41.06		
Змн.	*Арк.*	*№ докум.*	*Підпис*	*Дата*			
Розробив		Карбовський Н.В.			Пояснювальна записка	*Літ.*	*Арк.* 7 / *Аркушів* 44
Перевірив		Павлюк М.Ф.					
Н. Контр.							
Затвердив							

ЗМІСТ

ВСТУП

Бездротові сенсорні мережі (WSN) є ключовим технічним логічним просуванням у все більш взаємопов’язаному світі. Ці мережі включають безліч малих сенсорних пристроїв з обмеженими ресурсами, які співпрацюють для збору та обміну даних з їхнього безпосереднього оточення. Ця спільна робота дає змогу WSN знаходити різноманітні застосування у сферах, таких як екологічний моніторинг та спостереження, промислова автоматизація та системи охорони здоров’я. Однак сенсорні вузли (SN) за своєю природою стикаються з обмеженнями, такі як обчислювальні потужності, енергетичні ресурси, пам'ять та пропускна здатность. Ці обмеження ведуть до виникнння багатофакторних проблем в складному завданні обміну інформацією всередині мереж, посилюючи важливість забезпечення безпеки та конфіденційності даних.

Крім того, SN вразливі до різних типів атак, включаючи фізичне втручання, перехоплення даних, коомпрометацію вузла та атаки на відмову в обслуговуванні (DoS). Ці CD які розгортаються віддалено та залишаються без контролю, особливо чутливі до цих загроз. Зловмисники можуть втручатися в роботу SN, щоб скомпрометувати їхню функціональність, викрасти цінні дані або вимкнути їх, щоб порушити роботу мережі. Атаки перехоплення можуть призвести до порушення конфіденційності даних, розкриття секретної інформації неавторизованим особам. Атаки на компрометацію вузлів можуть порушити цілісність даних, і DoS-атаки можуть порушити мережевий зв’язок і доступність SN.

Конфіденційність і цілісність інформації є найважливішими проблемами під час спілкування та обміну між SN, головою кластеру (CH) і базовими станціями (БС). Традиційні механізми безпеки, розгорнуті в WSN, часто покладаються на складні

криптографічні розрахунки. На жаль, ці механізми накладають значне енергетичне навантаження на SN, що значно перешкоджає ефективності спілкування. Враховуючи внутрішні енергетичні обмеження SN, це надмірне споживання енергії може призвести до виснаження їхньої продуктивності, що потенційно може

призвести до передчасного виходу з ладу, таким чином скорочуючи термін служби мережі. Зокрема, програми реального часу дуже чутливі до виснаження продуктивності, оскільки вони вимагають низької затримки для швидкого прийняття рішень.

CH, діючи як посередники між SN та зовнішньою мережевою інфраструктурою не захищені від вразливостей безпеки. Скомпрометовані CH можуть ненавмисно служити шлюзами для кібератак, які потенційно призводять до викриття зведених даних. Ці взлами становлять значний ризик для конфіденційності та цілісності даних, підкреслюючи критичну необхідність встановлення довіри до CH як фундаментального елементу безпеки мережі. Ефективність споживання енергії стала центральною проблемою для WSN, що вимагає розробки енергоефективних механізмів безпеки. Для досягнення гармонійного балансу між безпекою даних та енергозбереженням, інноваційні підходи, такі як легкі методи шифрування, мають бути досліджені. Безпечний обмін даними між вузлами, розташованими в різних кластерах вносить додаткові складності, вимагаючи впровадження централізованих систем управління для ефективного вирішення багатьох проблем, включаючи безпеку, затримку та масштабованість.

Технологія повторного шифрування проксі (PRE) забезпечує безпечну комунікацію та обмін даними у мережі, тобто напівдовірений проксі використовується для перетворення зашифрованих даних з одного пристрою на інший без розкриття фактичного вмісту чи будь-яких закритих ключів. Це плавне перетворення досягається за допомогою ключа повторного шифрування, наданого довіреною третьою стороною, яка гарантує, що дані залишаються конфіденційними та зашифроманими протягом усього процесу передачі. Однак, PRE є найефективнішим лиш тоді, коли розгорнуті на пристроях з багатими ресурсами, і значно менш ефективні при розгортанні на пристроях з обмеженим ресурсом, таких як SN. Первинниа причина такої зниженої ефективності походить від істотної обчислювальної затратності, пов’язаною зі складними криптографічними обчисленнями, які вимагає процес PRE. Ці ресурсомісткі

обчислення роблять PRE менш придатним для пристроїв з обмеженими обчислювальними можливостями та енергетичними ресурсами. Крім того, зі збільшенням обсягу обміну даними та включенням більшої кількості пристроїв у мережу, обчислювальне навантаження проксі-сервера зростає, що потенційно може призвести до затримок у процесі повторного шифрування, що у свою чергу може вплинути на загальниу ефективность мережі та передачу даних у реальному часі.

У цій роботі було вирішено ці обмеження за допомогою нової схеми PRE, спеціально розробленої для CH в WSN. Ця інноваційна схема використовує легкі шифрувальні методи для значного покращення безпеки зв’язку та обміну даними у WSN. Запропонована схема істотно полегшує проблеми безпеки, з якими може зіткнутися CH, наприклад фізичні атаки або перехоплення даних під час обробки агрегованих даних у момент передачі між проміжними CH на шляху до точки доступу (ТД). Схема також гарантує що дані завжди залишаються зашифрованими, що запобігає несанкціонований доступ або перегляд даних CH. Крім того, ця схема відіграє ключову роль у зменшенні затримки зв’язку та оптимізації енергоспоживання.

Основний внесок цієї роботи узагальнено таким чином:

1) У цій роботі було розроблену інноваційну схему PRE, спеціально винайдену для WSN. Ця схема призначена для вирішення унікальної задачі поставленої пристроями з обмеженими ресурсами в WSN, таким чином легка криптографія використовується для оптимізації процесів шифрування, повторного шифрування та дешифрування. Ця оптимізація підвищує ефективність спілкування між мережевими суб'єктами при цьому значно зменшуюючи витрати продуктивності та пом’якшує затримку передачі.

2) Витрати енергії під час роботи PRE були оптимізовані як для SN, так і для CH. Запропонована схема покращує безпечний обмін даними всередині та між кластерами, зберігаючи енергетичні ресурси. Цей енергоефективний підхід значно покращує рівні безпеки всієї мережі та продовжує термін експлуатації WSN з обмеженими ресурсами.

3) Ефективність запропонованої схеми було оцінено шляхом проведення комплексного аналізу безпеки та продуктивності. Результати підтверджують надійність запропонованої схеми PRE для забезпечення безпеки, конфіденційності і цілісності даних, а також висвітлює переваги її енергоефективності.

РОЗДІЛ 1. ПІДГОТОВКА ДЛЯ АНАЛІЗУ WSN

1.1. РОЗГЛЯД АРХІТЕКТУРИ WSN

Архітектура WSN складається з трьох фундаментальних компонентів: SN, CH і агрегації даних, які керуються протоколами зв'язку, як показано на рисунку 1.1:

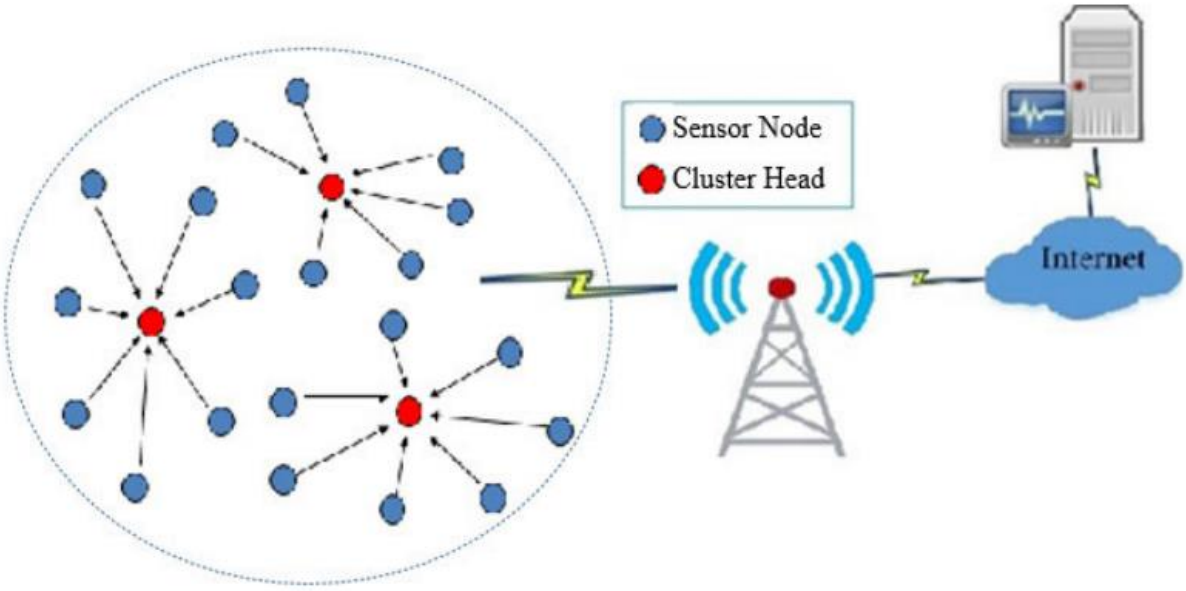


Рис.1.1 - Архітектура WSN

SN, оснащені спеціалізованими датчиками, служать основними вузлами мережі та стратегічно розташовані в цільовому просторі формуючи область для розподіленої мережі збору даних. Ефективне керування даними в мережах WSN здійснюється за допомогою формування кластерів, у яких SN організовуються в кластери на основі їх фізичної близькості. Кожен кластер складається з кількох SN під керівництвом CH. Ці CH мають критичну функцію збору даних, сгенерованими SN, і передачі їх на центральну базову станцію, використовуючи підхід з одним або кількома стрибками, яка широко відома як приймач або БС. Цей процес агрегування мінімізує надлишкову передачу даних, що призводить до значного енергозбереження.

Бездротові сенсорні мережі часто демонструють ієрархічну структуру, в якій можуть існувати кілька рівнів CH, що додатково підвищує масштабованість і ефективне управління даними. Крім того, стійкість мереж WSN зміцнюється за

рахунок механізмів резервування та самоорганізації, що забезпечує безперервну роботу навіть за наявності збоїв у вузлах або несприятливих умов.

Періодичні оновлення СН, що визначаються такими факторами, як рівень енергії та мережевий трафік, забезпечують ефективну роботу мережі. СН також служать основними точками підключення до БС та інших СН в різних кластерах, сприяючи обміну інформацією між міжкластерними вузлами, тим самим підвищуючи масштабованість мережі. Для забезпечення безперебійного зв'язку та передачі даних мережі WSN використовують різні бездротові протоколи та алгоритми маршрутизації. Ці методи включають методи агрегації даних, механізми виправлення помилок і енергоефективні стратегії маршрутизації, що були спеціально розроблені для продовження терміну служби мережі. Вибір протоколу, рішення щодо маршрутизації та впровадження заходів безпеки налаштовуються відповідно до унікальних вимог конкретних програм і вимог мережі.

Примітно, що заходи безпеки, такі як шифрування та автентифікація, набули більшого значення, враховуючи властиві вразливості та накладні витрати на ефективність, пов'язані з існуючими протоколами безпеки в WSN.

1.2. ІНТЕГРОВАНІ ЛЕГКІ МЕТОДИ ШИФРУВАННЯ

1.2.1. ЛЕГКЕ СИМЕТРИЧНЕ ШИФРУВАННЯ

У одній із робіт Speck було обрано як кращий легкий симетричний алгоритм шифрування для досягнення високої продуктивності в середовищах з обмеженими ресурсами, що робить його чудовим вибором для реалізації WSN. Speck, розроблений Агентством національної безпеки (NSA), винятково себе показує як і в апаратному, так і програмному забезпеченні. Використовуючи розмір блоку *(b)* 64 або 128 біт і підтримуючи розміри симетричного ключа *(Sk)* 128, 192 і 256 біт, Speck гнучко адаптується до конкретних вимог шифрування. Кількість раундів *(r)*, що використовуються в Speck, зазвичай коливається від 22 до 34, залежно від вибраних розмірів *b* і *Sk*, що дозволяє точно налаштувати для досягнення бажаних рівнів безпеки та ефективності.

Принципи проектування Speck віддають перевагу простоті та ефективності, надаючи надійні можливості шифрування, мінімізуючи обчислювальні витрати та використання пам’яті, які є ключовими факторами для WSN. Його внутрішня архітектура базується на простих операціях, включаючи зрушення бітів, додавання та операції виключне АБО (XOR). Ця спрощена та ефективна конструкція гарантує, що Speck шифрує дані в мережах WSN без значного навантаження на обчислення чи пам’ять. Особливістю Speck, яка виділяється, є його здатність шифрувати повні повідомлення без складних режимів роботи, спрощуючи процес шифрування та знижуючи ризики вразливості, пов’язані з більшими блоками або складними методами. Крім того, Speck демонструє надійні характеристики безпеки, так що навіть однобітна зміна вхідних даних може призвести до суттєво відмінного зашифрованого тексту. Ця невід'ємна властивість підвищує безпеку шляхом зменшення ризику атак методом вирізання та вставки, тим самим підвищуючи цілісність даних у WSN.

З точки зору споживання ресурсів, емпіричні дослідження послідовно демонструють перевагу Speck над ресурсомісткими алгоритмами шифрування, включаючи розширений стандарт шифрування (AES), стандарт шифрування даних (DES) та інші традиційні симетричні шифри. Координація між ефективністю, безпекою та адаптивністю до середовища з обмеженими ресурсами робить Speck дуже придатним для безпечного зв’язку в обмежених ресурсами мережах, бездоганно відповідаючи вимогам WSN.

1.2.2. ЛЕГКЕ ШИФРУВАННЯ ВІДКРИТИМ КЛЮЧЕМ

У запропонованій схемі ми використовуємо криптографію з еліптичною кривою (ECC) як легкий криптографічний метод із відкритим ключем, натхненний піонерською роботою Ель-Гамала щодо шифрування з відкритим ключем. Цей підхід передбачає приховування m через два значення, α^k і β^k, з β. що є результатом α, піднесеного до степеня a. У цьому контексті α є первісним коренем великого простого числа p, а k є цілим числом, вибраним навмання. Важливо, що параметри α, β і p є загальновідомими. Об’єкт-відправник використовує значення k для обчислення (α^k, β^k)перед передачею їх призначеному одержувачу.

Маючи це секретне знання, одержувач може розшифрувати вихідне повідомлення за допомогою формули

$$m = (\alpha^k)^{-a} * (\beta^k m) = (\alpha^a)^{-k} * (\beta^k m) = (\beta^{-k}) * (\beta^k m) \quad (1.1)$$

Поява ECC, незалежно один від одного представленого Кобліцем і Міллером, ознаменувала значні зміни в шифруванні з відкритим ключем. ECC використовує групи еліптичних кривих над кінцевим полем для реалізації криптосистеми з відкритим ключем Ель-Джамала і оперує точками еліптичної кривої над кінцевими полями, а не безпосередньо шифрує повідомлення. Це включає основні криптографічні функції, такі як кодування повідомлень у точки, декодування точок у повідомлення та перевірка відкритих ключів. Генерація ключа в ECC — це важливий процес, який включає такі кроки:

1) Вибір простої кривої: еліптична крива (позначена як E) визначається неособливим кубічним поліноміальним рівнянням із двома невідомими в скінченному полі F_p, де F_p представляє цілі числа діючи за модулем p. Еліптична крива E над F_p виражається як

$$y^2 = x^3 + ax + b(mod\ p), \quad (1.2.)$$

де $a, b \in F_p$. Безпечна криптосистема може бути забезпечена, коли $4a^3 + 27b^2 \neq 0(mod\ p)$. Скінченне поле містить цілі числа від 0 до $(p - 1)$, а стратегічний вибір p гарантує існування скінченної кількості точок на E, тим самим забезпечуючи безпеку.

2) Визначення ключових параметрів: на цьому етапі параметри α, β, p і крива C оприлюднюються. Тут як α, так і β представляють точки, розташовані на E, і мають важливе значення в інфраструктурі відкритих ключів.

Генерація ключів передбачає створення як закритих, так і відкритих ключів. Приватний ключ, позначений як d, обчислюється як випадкове ціле число в інтервалі $[1, n-1]$, де n представляє простий порядок циклічної підгрупи P еліптичної кривої E. Відповідний відкритий ключ Q створюється як $Q = d \times P$, встановлюючи унікальне та безпечне сполучення між ключами.

Основні криптографічні операції в ECC Ель-Джамала виконуються за визначеною процедурою. Під час шифрування відправник спочатку ділить m на менші блоки та представляє кожен блок як ціле число за модулем p. Згодом вибирається випадкове k для обчислення двох різних точок (s, w) на еліптичній кривій. Зокрема, відправник обчислює:

$$s = (x_s, y_s) = k \times \alpha \tag{1.3}$$

і визначає w як

$$w = (x_w, y_w) = (m + k \times \beta) \tag{1.4}$$

де β походить від α і k. Ця пара точок (s, w) разом представляє зашифровану форму повідомлення m, яке потім передається до призначеного адресата для подальшої обробки. У процесі дешифрування після отримання зашифрованих точок (s, w) кінцевий вузол ініціює процес дешифрування для відновлення повідомлення m. Він обчислює m за допомогою $m = y_w - a \times y_s$, де a — секретний параметр, відомий виключно одержувачу, а y_s і y_w виводяться з отриманих точок s і w. Цей процес дешифрування забезпечує безпечне отримання повідомлень.

РОЗДІЛ 2. ЗАПРОПОНОВАНА АРХІТЕКТУРА ДЛЯ WSN

У цьому розділі представлено архітектурний дизайн пропонованої WSN на основі PRE, за допомогою якого ця робота заглиблюється в тонкощі використовуваних криптографічних алгоритмів і детально розробляє побудову моделі безпеки в мережі.

2.1. ДИЗАЙН АРХІТЕКТУРИ

У цьому розділі досліджуються аспекти дизайну запропонованої WSN на основі PRE. Архітектурний проект складається з трьох основних етапів, як показано на рисунку 2.1:

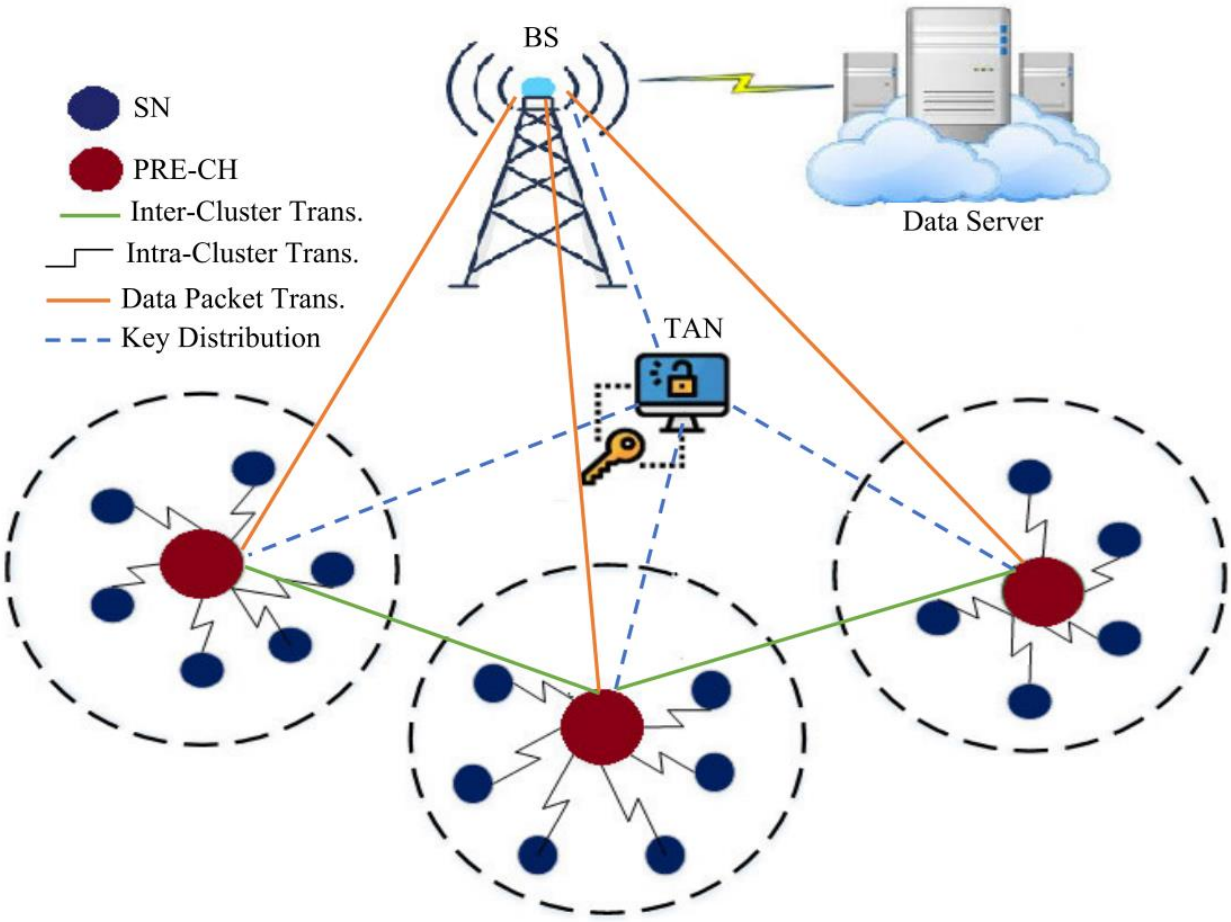


Рис2.1 - Дизайн архітектури запропонованої PRE WSN

На початковому етапі ключі та сертифікати генеруються для кожного вузла в мережі. Згодом для захисту даних, згенерованих SN, і пов'язаних з ними ключів шифрування було застосовано поєднання полегшених методів симетричного та асиметричного шифрування. На другому етапі механізм PRE реалізується на рівні

CH для забезпечення безпечної передачі даних. Нарешті, на третьому етапі впроваджується ефективний підхід до управління для забезпечення безпечного зв'язку та спільного використання зашифрованого тексту між об'єктами в WSN.

У запропонованій схемі архітектура мережі організована в кластери, кожен з яких містить SN, підключені до CH. Під час процесу налаштування вузла кожному вузлу призначається унікальний ідентифікатор (ID), зареєстрований у відповідному CH. Кожен SN у мережі, включаючи CH, має відмінну пару відкритих і закритих ключів, позначених як (Pk, Prk). Схема включає виділену групу вузлів CH, які служать проксі-серверами, щоб забезпечити безперебійне підключення та зв'язок між вузлами як всередині, так і понад кластером.

Враховуючи обмеженість ресурсів CH, де ресурсомісткі завдання, такі як генерація ключів, шифрування та повторне шифрування, можуть виснажити резерви потужності, спеціальний туманний/граничний сервер із більшими можливостями обробки, підключеним до всіх CH, позначається як повністю довірений авторитетний вузол (TAN). TAN відіграє ключову роль у нагляді за критично важливими функціями в мережі. Його обов'язки включають реєстрацію SN, генерацію загальнодоступних параметрів системи та безпечне створення криптографічних ключів для кожного CH та пов'язаних із ним SN. Крім того, він відповідає за створення цифрових підписів для забезпечення автентифікації кожного вузла в мережі. Примітно, що хоча TAN відіграє центральну роль у підтримці безпеки мережі, він залишається абсолютно байдужим до будь-якого аспекту функціональності PRE.

Під час процесу реєстрації SN у мережі кожному SN призначається сертифікат (*Crt*), який містить важливу інформацію. Цей *Crt* містить ідентифікатор кластера (*CID*), який позначає конкретний кластер (*C*), з яким пов'язаний вузол. Крім того, кожному SN призначається унікальний ідентифікатор (*SID*) у відповідному *C*, який забезпечує точну та ексклюзивну ідентифікацію. Нарешті, етап створення сертифіката *Crt* включає створення окремого сертифіката (*CrtSN*) для кожного SN. Цей *Crt* містить важливу інформацію, таку як *CID, SID,* Pk_{SN} і DS_{SN}. Потім він безпечно поширюється та зберігається в SN, забезпечуючи

автентифікацію та безпечну передачу інформації. Процедура реєстрації складається з наступних етапів:

1) Генерація ідентифікатора кластера (*CID*): Щоб створити унікальний *CID* для реєстрації нових SN в *C*, унікальне випадкове число генерується для кожного *C*. Кожна CH оснащена чітким ідентифікатором (*CHID*).) і пара відкритих приватних ключів (Pk_{CH}, Prk_{CH}). Ця інформація безпечно обмінюється між усіма CH мережі.

2) Генерація унікального ідентифікатора SN (*SID*), цифрового підпису (DS_{SN}) і пари публічно-приватних ключів (Pk_{SN}, Prk_{SN}): ці компоненти служать для унікального розрізнення та автентифікації кожного SN у межах призначеного *C*. Щоб досягти цього, унікальний серійний номер призначається кожному *SID*, а DS_{SN} генерується з використанням хешу Pk_{SN}. Крім того, кожному SN виділяється пара відкритий-приватний ключ еліптичної кривої (Pk_{SN}, Prk_{SN}).

3) Створення симетричного ключа (*Sk*): кожного разу, коли законний SN передає дані через мережу, для цієї конкретної мети створюється новий *Sk*. Створення цього *Sk* включає легку односторонню хеш-функцію. Ця функція є кращою через її обчислювальну ефективність і стійкість до інверсії. Згодом *Sk* використовується для шифрування даних, що надходять від SN, за допомогою легкого методу симетричного шифрування Speck.

4) Генерація сертифіката (*CrtSN*): кожен SN отримує свій унікальний *CrtSN*. Структура *CrtSN* містить ключову інформацію, включаючи *CID*, *SID*, DS_{SN} і Pk_{SN}. Згодом *CrtSN* безпечно поширюється та зберігається в SN. Його основна функція охоплює подвійну мету автентифікації та забезпечення безпечної передачі інформації.

2.2. РЕАЛІЗАЦІЯ МОДЕЛІ БЕЗПЕКИ

Запропонована схема PRE містить набір із п’яти алгоритмів, кожен з яких ретельно визначений відповідно до конкретних вхідних і вихідних параметрів, таким чином встановлюючи чітке розмежування їхніх відповідних функцій і взаємодій у системі.

2.2.1. ІНІЦІАЛІЗАЦІЯ СИСТЕМИ

Припустимо, що E (Fq) є еліптичною кривою, визначеною над кінцевим полем Fq, де q є значущим простим числом, а G представляє точку на E з порядком p. Крім того, дві мультиплікативні групи простого порядку p ідентифікуються як G1 і G2. У цьому контексті білінійне відображення — це функція, позначена як e, яка відображає елементи з G1 × G1 → G2, а s — елемент у $e(G1, G1)$, що належить G2. TAN ініціює алгоритм налаштування, використовуючи параметр безпеки a як вхідні дані для створення загальнодоступного системного параметра Sprm, який містить інформацію про E, q, p, e, G і s. Деталі ініціалізації системи представлені в Алгоритмі 1.

1. **Input** a
2. **Output** $Sprm_{SN}$
3. **Begin**
4. **for** $\forall C_i \in WSN$ **do**
5. $Compute\_ID() \rightarrow CID$
6. $Identify\_CH() \rightarrow CHID$
7. **for** $\forall SN_i \in C$
8. $Compute\_ID() \rightarrow SID$
9. $Generate\_Sprm() \rightarrow \mathrm{E}, q, p, e, \mathrm{G}, \mathrm{s}$
10. $Send\ (Sprm_{SN}) \rightarrow SN_i$
11. **end for**
12. **end for**
13. **End**

Рис.2.2 - Ініціалізація системи

2.2.2. ГЕНЕРАЦІЯ КЛЮЧІВ ШИФРУВАННЯ

Під час цієї процедури TAN використовує загальнодоступний системний параметр Sprm для обчислення пар ключів (Pk, Prk) і сертифіката (Crt) для вузлів A (відправник) і B (одержувач), де B може представляти різні сутності. Ці пристрої можуть включати в себе SN у тому самому кластері, що й A, SN, розташований в

іншому кластері в мережі, або навіть базову станцію чи сервер даних, відповідальний за отримання даних. Процедура також передбачає створення ключа повторного шифрування (rk), який використовується CH для повторного шифрування повідомлення між A та B. Ця гнучкість типів одержувачів підкреслює масштабованість і адаптивність системи, забезпечуючи безпечні дані передача та обмін даними між різними мережевими об'єктами.

Деталі процедури генерації ключів представлені в Алгоритмі 2.

1. **Input** *Sprm*
2. **Output** $Crt, r\ k, (Pk, P\ rk)$
3. **Begin**
4. $ChooseRandom() \rightarrow r \in \mathrm{F}_p^*$
5. $Compute\ (Prk_A) \rightarrow Prk_A = (\mathrm{a}r) \in \mathrm{F}_p^*$
6. $Compute\ (Pk_A) \rightarrow Pk_A = (\mathrm{a}rG) \in \mathrm{F}_p^*$
7. $Compute\ (Prk_B) \rightarrow Prk_A = (\mathrm{b}r) \in \mathrm{F}_p^*$
8. $Compute\ (Pk_B) \rightarrow Pk_A = (\mathrm{b}r\mathrm{G}) \in \mathrm{F}_p^*$
9. $Compute\ (rk) \rightarrow rk = (\mathrm{a}r)^{-1}\mathrm{b}r\mathrm{G} = (\mathrm{a})^{-1}\mathrm{b}\mathrm{G}$
10. $Compute\ (\mathrm{DS}) \rightarrow \mathrm{DS}_{SN} = Hash\ (Pk_{SN})$
11. $Create\ (Crt) \rightarrow Crt_{SN}\ (CID,\ SID,\ \mathrm{DS}_{SN},\ Pk_{SN})$
12. **End**

Рис.2.3 - Генерація ключів шифрування

2.2.3. ШИФРУВАННЯ СЕНСОРНОГО ВУЗЛА

Вузол-відправник ініціює процедуру шифрування даних для захисту повідомлення та криптографічних ключів. Ця процедура приймає m, K і Pk з A як вхідні дані. Потім алгоритм використовує Speck для шифрування розділених блоків (b) з m за допомогою обчисленого Sk, генеруючи зашифроване повідомлення (Cm). Далі ECC Ель-Джамала використовується для шифрування Sk і DS, який називається K, який потім використовується для шифрування

повідомлення вузла під час цього конкретного раунду. Згодом генерується зашифрована версія ключа шифрування, відома як CK.

Використання легкої конструкції Speck забезпечує надійну безпеку даних без надмірних обчислювальних витрат. Крім того, ECC Ель-Джамала спеціально вибрано для шифрування криптографічних ключів і сертифікатів. Хоча асиметричні шифри характеризуються відносно повільнішим характером, вони мають перевагу у захисті менших розмірів даних і сприяють обміну криптографічними ключами. У шифруванні ECC Ель-Джамала відкритий ключ має велике значення, оскільки він служить базовою точкою для приховування секретних значень за допомогою скалярного множення, забезпечуючи надійну конфіденційність даних і безпеку протягом усього процесу шифрування. Цей гібридний підхід із застосуванням Speck для шифрування даних і ECC для шифрування ключів і сертифікатів ефективно оптимізує безпеку та ефективність у середовищах WSN з обмеженими ресурсами. Інтеграція цього подвійного методу шифрування перетворює повідомлення та пов’язані з ними ключі в безпечні представлення зашифрованого тексту. Алгоритм 3 визначає процедуру шифрування на рівні сенсорного вузла, використовуючи цю гібридну комбінацію симетричного та асиметричного шифрування.

1. **Input** Pk_A, m, K
2. **Output** C_m, C_K
3. **Begin**
4. $OneWayHash\ () \longrightarrow Sk$
5. $Create\_Blocks(m) \longrightarrow b_1, .., b_n$
6. $Speck\_Enc\ (m, S\ k//b_1, .., b_n//r) \longrightarrow C_m$
7. $Generate\_SecretValue() \longrightarrow v \in \mathrm{F}_p^*$
8. $ECC\_Enc\ (k//Pk_A) \longrightarrow C_{k_A} = (\alpha, \beta)$
   $= (vPk_A, s^v\mathrm{G} + K)$
9. $A \leftarrow Return\ (C_m, C_K)$
10. **End**

Рис.2.4 - Шифрування сенсорного вузла.

2.2.4. ПЕРЕШИВРУВАННЯ ГОЛОВИ КЛАСТЕРА

Процедура повторного шифрування ініціюється, коли цільовий CH отримує переданий пакет від SN, що містить Crt вузла, зашифровані блоки даних Cm, зашифровані криптографічні ключі CH та ідентифікаційну інформацію одержувача $ВІД_B$. CH починається з перевірки автентичності SN через CrtSN. Після підтвердження автентифікації відповідний rk отримується з TAN.

Потім CH вибірково повторно шифрує частину CK, яка спочатку була зашифрована вузлом A, генеруючи новий перешифрований ключ шифрування, позначений як RCk. Цей RCK може бути розшифрований лише вузлом B. Примітно, що це повторне шифрування обмежено CK, який значно коротший за довжиною порівняно з розміром Cm. Отже, CH споживає мінімальне енергоспоживання під час цього процесу. Алгоритм 4 містить детальний опис цієї процедури.

1. **Input** C_K, SID_B, rk, Crt_A
2. **Output** RC_K
3. **Begin**
4. $Check\_Authentication\ (Crt_A)$
5. $ECC\_Enc\ (C_k//rk) \rightarrow RC_k = (\alpha', \beta')$
6. $Compute\ (\alpha') \rightarrow \alpha' = e(\alpha, r\ k) = e(var\mathrm{G}, rk)$
7. $Compute\ (rk) \rightarrow rk = \mathrm{a}^{-1}\mathrm{bG}$
8. $Compute\ (\beta') \rightarrow \beta' = \mathrm{s}^{v}\mathrm{G} + Pk_B$
9. $Compute\ (RC_K) \rightarrow RC_K = (\mathrm{s}^{v\mathrm{rb}}, \mathrm{s}^{v}\mathrm{G} + K)$
10. $CH \leftarrow Return\ (RC_K)$
11. **End**

Рис.2.5. Перешифрування голови кластеру.

2.2.5. ДЕШИФРУВАННЯ ПРИСТРОЮ

Процедура дешифрування починається, коли вузол-одержувач B отримує пакет даних, який містить Cm і RCK, від CH. Зауважте, що B може представляти SN у кластері, інший кластер, точку доступу або сервер даних. Використовуючи приватний ключ PrkB B, RCK розшифровується для відновлення K, який включає Sprm і Sk. Ці ключі згодом використовуються для дешифрування Cm і отримання вихідного повідомлення m. Алгоритм 5 описує процедуру дешифрування, яку виконує об'єкт B.

1. **Input** RC_K, C_m, Prk_B
2. **Output** m
3. **Begin**
4. $ECC\_Dec\ (RC_k//Prk_B) \longrightarrow K = \beta' - \left(\alpha'\right)^{\frac{1}{\mathrm{rb}}} \mathrm{G}$
5. $Compute\ \left(\beta'\right) \longrightarrow \beta' = \mathrm{s}^{v}\mathrm{G}$
6. $Compute\ \left(\alpha'\right) \longrightarrow \alpha' = \mathrm{s}^{v\mathrm{rb}}$
7. $Compute\ (K) \longrightarrow k = \mathrm{s}^{v}\mathrm{G} + K - \left(\mathrm{s}^{v\mathrm{rb}}\right)^{\frac{1}{\mathrm{rb}}} \mathrm{G} = K$
8. $Speck\_Dec\ (C_m, r \| Sk) \longrightarrow m$
9. $B \leftarrow Return\ (m)$
10. **End**

Рис.2.6 - Дешифрування пристрою

РОЗДІЛ 3. БЕЗПЕЧНА КОМУНІКАЦІЯ ТА ОБМІН ДАНИМИ

Коли зареєстрований SN у певному C ініціює зв'язок або обмін даними з іншим SN у тому ж кластері, різних кластерах або серверах даних, безпечне з'єднання встановлюється через пов'язаний CH. Під час цього процесу SN, що надсилає дані, передає свій Crt та ID одержувача CH для автентифікації. Якщо Crt успішно перевірено, CH дозволяє передачу даних; інакше автентифікація буде відхилена.

Після успішної автентифікації SN CH зв'язується з TAN, щоб отримати необхідні криптографічні ключі та Sprm. Згодом SN шифрує корисне навантаження в переданому пакеті даних, використовуючи згенерований Sk. Крім того, він шифрує K за допомогою власного PkSN і приєднує Ck до пакету даних.

Після отримання пакету даних CH він використовує отриманий rk для повторного шифрування CK і додає новий RCK до пакету даних перед тим, як пересилати його на цільовий кінцевий вузол на основі унікального ідентифікатора. У сценаріях із міжкластерним зв'язком відповідний CH або AP одержувача ініціює зв'язок із TAN, щоб отримати Crt, Prk, B і Sprm одержувача. Цей крок служить найважливішій меті автентифікації особи одержувача. Згодом CH або AP передає зашифроване повідомлення Cm разом із пов'язаними ключами до призначеного вузла. Отримавши зашифровані пакети даних, одержувач використовує свій PrkB для дешифрування K, таким чином отримуючи Sk для дешифрування Cm за допомогою шифру Speck.

У запропонованій схемі SN проходять реєстрацію та сертифікацію за сприяння відповідних CH. Коли SN, що спілкуються, належать до одного кластеру, їхні ідентифікатори та сертифікати зберігаються в цьому конкретному CH. Це дозволяє CH виконувати централізовану автентифікацію SN у своєму кластері.

Для SN, що належать до різних кластерів, процес реєстрації відбувається у відповідних CH. Ці CH можуть спілкуватися з TAN, дозволяючи їм автентифікувати SN з інших кластерів. Цей механізм ефективно полегшує обмін інформацією між кількома SN, що охоплюють різні кластери в WSN. Зокрема, у сценаріях, що передбачають зв'язок між кластерами або з сервером даних, CH не

надаються права доступу до даних і ключів шифрування. Їхня роль суворо обмежена керуванням зв’язком, полегшенням процедур автентифікації, взаємодією з TAN і виконанням процесу PRE для зашифрованого симетричного ключа.

3.1. ДОСЛІДИ ТА ДИСКУСІЯ

У цьому пункті представлено середовище моделювання та використовувані параметри, включаючи оцінку продуктивності запропонованої схеми PRE з точки зору часу виконання, обчислювальних витрат і споживання енергії. Нарешті, аналіз безпеки схеми розглядає типові атаки, спрямовані на WSN.

3.2. МОДЕЛЮВАННЯ ТА НАЛАШТУВАННЯ ПАРАМЕТРІВ

Змодельоване середовище WSN було створено з використанням симулятора NS2 для реалізації та оцінки запропонованої схеми PRE. Специфікації цього змодельованого середовища детально описано в Таблиці 1, де окреслюються різні параметри, включаючи розмір області WSN, кількість вузлів датчиків, час моделювання, стандарт модуляції та інші ключові фактори, що впливають на моделювання. Крім того, симуляції виконувалися на обладнанні, оснащеному процесором Intel Core i5-2450M 2,5 ГГц, 3 МБ кеш-пам’яті та 4 ГБ оперативної пам’яті. WSN, що охоплював квадратну площу 400 × 400 м2, містив різну кількість SN.

Таблиця 3.1 - Параметри симуляції.

Parameter	Value
WSN area size	400m × 400m
Number of sensor nodes	50 to 250 SNs
Simulation time	250 sec
Modulation standard	Zigbee/IEEE 802.15.4
Max data rates	250 kbps
Packet size	6400 bits
Control message size	200 bits
Initial power	3 J (joule)
Transmit/receive power level	50 nJ/bit
Power consumption per block size	0.001 for 32 bits
Power consumption per round	0.001 J
Data aggregation power	5 nJ/bit/signal
Free space loss	10 J/bit

У цих експериментах усі SN були налаштовані на передачу даних до CH за допомогою протоколу зв'язку Zigbee/IEEE 802.15.4. Для узгодженості ми прийняли стандартні параметри моделювання з конкретними значеннями параметрів. Щоб забезпечити надійність, зареєстровані результати являють собою середні значення, отримані з 30 різних прогонів запропонованого методу.

Запропонована схема PRE приділяє значну увагу підвищенню безпеки SN, передачі даних і обміну даними в мережах, приділяючи пріоритет покращенню енергоефективності та подовженню терміну служби WSN. Для оцінки ефективності запропонованої схеми були використані наступні ключові показники:

1) Криптографічна ефективність: суворе оцінювання включало вимірювання та порівняння часу виконання запропонованих методів легкого шифрування, повторного шифрування та дешифрування з традиційними алгоритмами шифрування. Це порівняння дозволило детально зрозуміти накладні витрати схеми та ефективність обробки.

2) Енергоспоживання вузла: моделювання було проведено в різних часових проміжках, щоб оцінити вплив схеми на енергоспоживання через SN і CH, зіставляючи ці результати зі стандартними сценаріями роботи. Аналіз включав співставлення моделей енергоспоживання щодо різних обсягів пакетів даних і тривалості передачі.

3) Пропускна здатність і термін служби мережі: прагнучи підвищити пропускну здатність WSN при оптимізації процесів шифрування, даний аналіз оцінив вплив схеми на термін служби WSN, ретельно порівнюючи її з підходами повного шифрування, повторного шифрування та дешифрування згенерованих даних. Крім того, різні початкові параметри живлення ретельно розглядалися, щоб перевірити їх вплив на тривалість життя мережі, фактично відображаючи тривалість енергоспоживання вузлів.

3.3. ОЦІНКА ЕФЕКТИВНОСТІ

У даному розділі була проведена послідовність експериментів моделювання, щоб оцінити запропоновану схему PRE. У початковому сценарії моделювання ми досліджували вплив методів шифрування, повторного шифрування та дешифрування на час обробки при використанні запропонованої схеми PRE, порівнюючи їх із повним шифруванням даних за допомогою стандартних шифрів, таких як AES-256 і RSA-1024. Аналіз включав вимірювання часу виконання криптографії, збереження параметрів шифрування постійними при поступовому збільшенні розміру даних. Моделювання було розпочато через 30 с із залученням 50 SN та 4 CH.

Під час початкового обміну даними між SN і відповідним CH було передано повідомлення даних розміром 16 КБ, згодом розмір даних поступово збільшувався. Загальний час обробки для SN, позначений як ΔT_{SN}, охоплює кілька компонентів, включаючи час, необхідний для SN для створення запиту на передачу, передачі пакету даних, виконання симетричного шифрування m і виконання асиметричного шифрування k, як виражено у Рівнянні (1).

$$\Delta TSN = T(SymEnc(m)) + T(AsymEnc(K)) + T(TranDP) \quad (3.1)$$

Для CH загальний час включає час, необхідний для автентифікації SN, зв’язку з TAN, повторного шифрування K і передачі пакету даних наступному об’єкту, як виражено в Рівнянні (2). Під час зв'язку з TAN отримуються ключі шифрування та параметри.

$$\Delta TCH = T(Auth(SN) + (TranTAN) + T(ReEnc(K)) + T(TranDP) \quad (3.2)$$

На рисунку 3.2 представлено огляд загального часу обробки, пов’язаного з криптографічними процесами в запропонованій схемі з використанням різних розмірів даних корисного навантаження. SN постійно демонструє надзвичайну ефективність, зберігаючи середній ΔT_{SN} 171 мс під час виконання операцій, детально описаних у Рівнянні (1). Це досягнення не залежить від можливої затримки мережі. Тим часом CH демонструє похвальну продуктивність, зберігаючи майже постійний ΔT_{SN} 28 мс під час виконання завдань, описаних у Рівнянні (2).

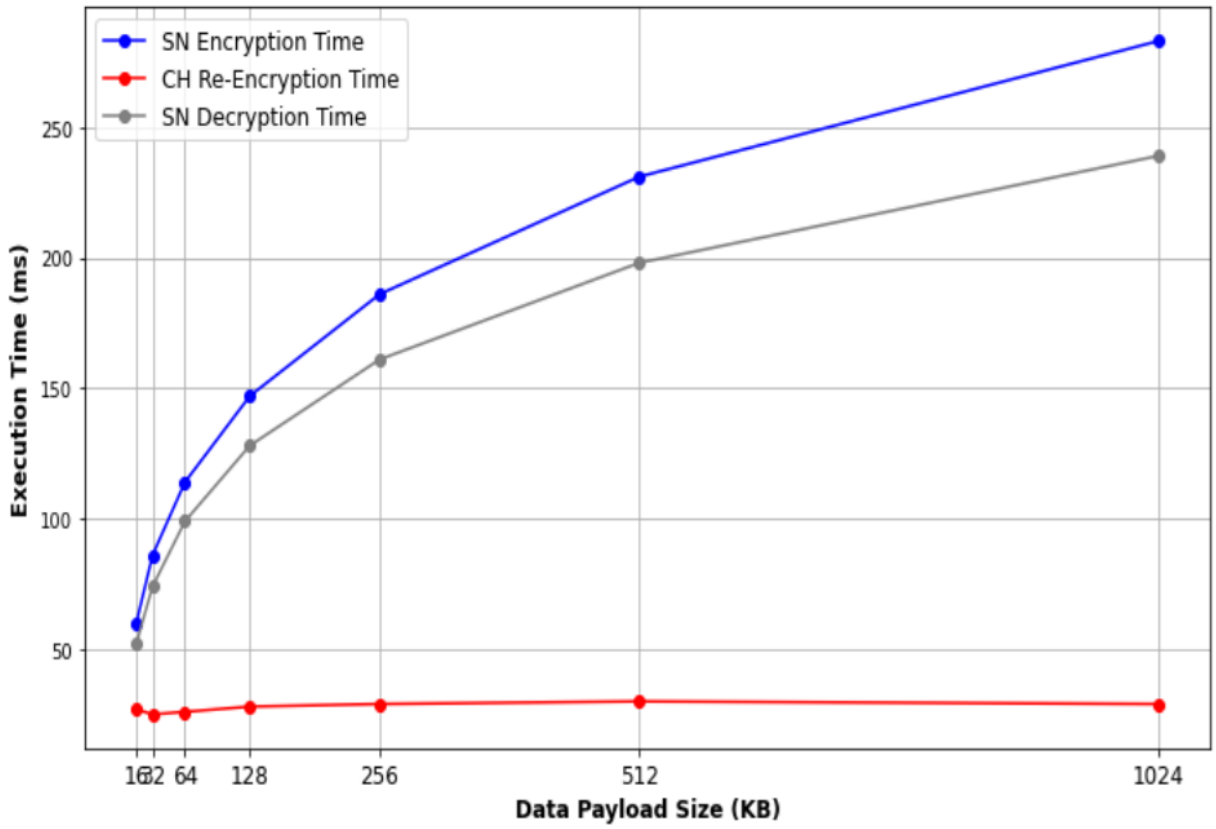


Рис.3.1 -Аналіз загального часу виконання криптографічних процесів у запропонованій схемі PRE.

Для порівняння, об’єкту-одержувачу потрібен середній час обробки 126 мс для отримання повідомлень такого самого розміру. Пропускна здатність запропонованої схеми PRE була додатково оцінена для швидкості транзакцій в секунду (TPS) в діапазоні від 20 до 200. Оцінка почалася зі швидкості пропускної здатності 20 TPS з використанням корисного навантаження 16 КБ протягом 60 с. Згодом швидкість надсилання була поступово збільшена до 200 TPS. Ця комплексна оцінка дозволила порівняти продуктивність запропонованої схеми зі стандартною передачею TPS, яка слугувала базовою без шифрування. Рисунок 4 ілюструє результати оцінювання. У середньому запропонована схема демонструє приблизно на 42% нижчу пропускну здатність, ніж стандартна передача.

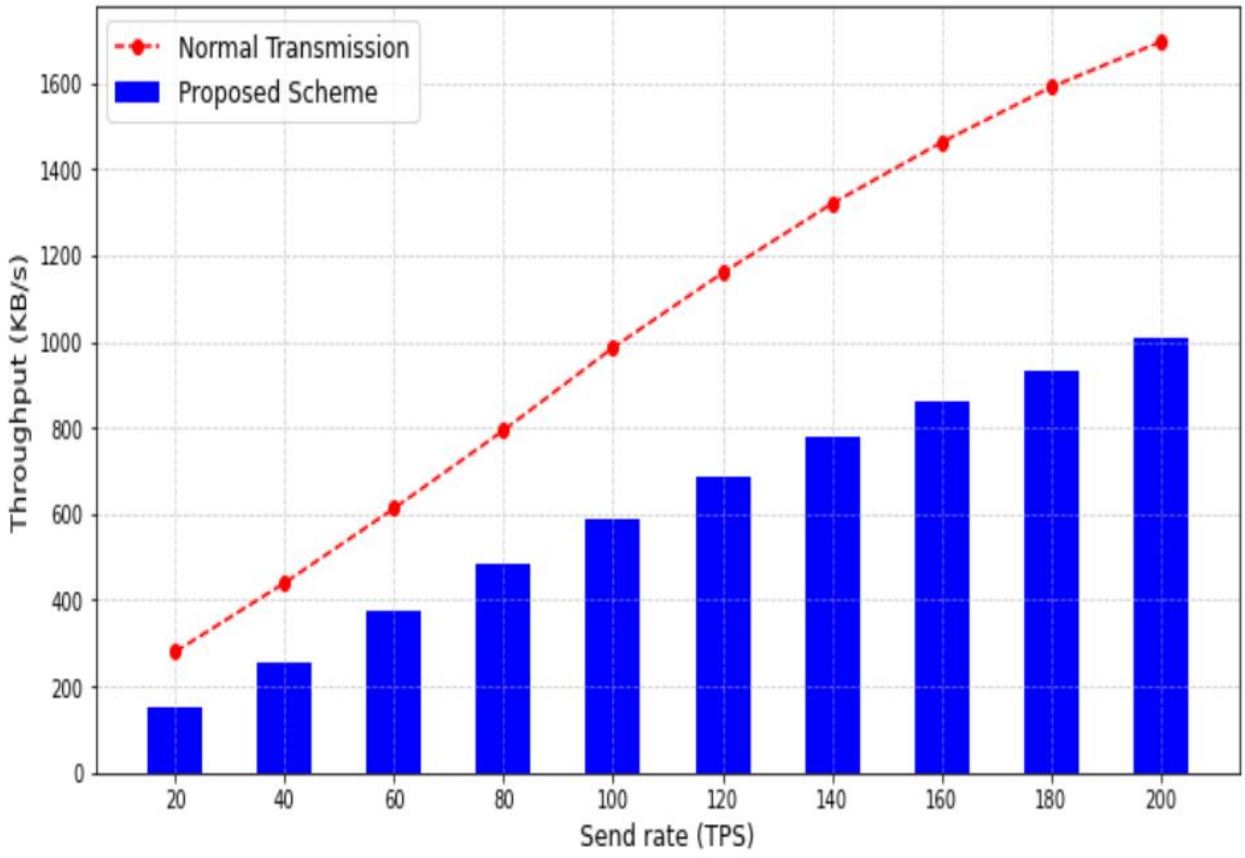


Рис.3.2 - Аналіз пропускної здатності запропонованої схеми PRE порівняно зі стандартною передачею без шифрування за різних налаштувань TPS.

Ці результати підкреслюють істотний вплив процесів шифрування та повторного шифрування на ефективність передачі даних за запропонованою схемою. Вони також підкреслюють властивий компроміс між підвищенням

безпеки та пропускною здатністю даних, особливо у застосуваннях із інтенсивним об’ємом даних у WSN.

У рамках порівняльного аналізу було введено шифри AES і Рівест-Шаміра-Адлемана (RSA) в мережу моделювання, щоб імітувати звичайний сценарій шифрування, який зазвичай використовується в більшості досліджень без використання PRE. Це дозволило оцінити відповідний час виконання порівняно з часом запропонованого методу PRE. У цьому підході повторного шифрування без проксі SN використовує AES-256 для шифрування всього повідомлення перед передачею. Крім того, RSA-1024 використовується на тому самому вузлі для повторного шифрування всього симетричного зашифрованого тексту для внутрішньокластерного зв’язку. Згодом на кінцевому вузлі для дешифрування використовувалися шифри RSA та AES, AES для розшифровування симетричного шифртексту і RSA, щоб відновити вихідне повідомлення. На Рисунку 5 представлено порівняння часу виконання для запропонованої схеми PRE зі звичайним підходом повторного шифрування без проксі для різних розмірів корисного навантаження даних.

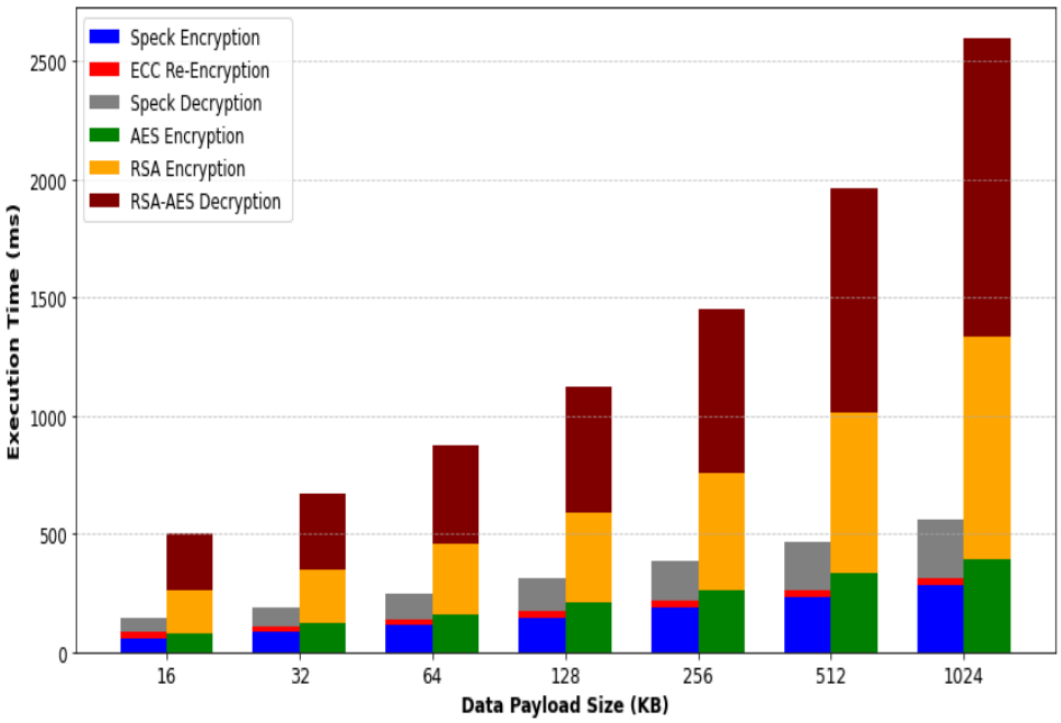


Рис.3.3 - Порівняльний час виконання запропонованої схеми PRE та підходу повторного шифрування без проксі.

З результатів стає очевидним, що запропонована схема PRE значно скорочує час обробки приблизно на 64% порівняно з підходом повторного шифрування без проксі, який використовує стандартні шифри. Це значне скорочення часу обробки можна віднести до ефективної роботи полегшених шифрів, які використовуються в криптографічних операціях.

Крім того, запропонована схема значно мінімізує обчислювальне та комунікаційне навантаження на CH під час процесу повторного шифрування, зосереджуючись виключно на шифруванні симетричного ключа. Отже, наш підхід є більш ресурсоефективним, враховуючи велике робоче навантаження, пов’язане з повним повторним шифруванням корисних даних.

Іншим важливим аспектом, який слід враховувати, є енергоспоживання SN під час операцій PRE. Загальне енергоспоживання, позначене як Pw, отримується множенням енергоспоживання вузла на час, необхідний для виконання кожної операції, як зазначено у Рівнянні (1) для SN та у Рівнянні (2) для CH під час передачі повідомлення m до кінцевого вузла. Загальний Pw SN у нашій схемі був розрахований шляхом імітації роботи протягом 30 с для різних розмірів корисного навантаження. Потім ці результати порівнювали з результатами, отриманими за допомогою відповідних схем PRE, як показано на Рисунку 6 (a).

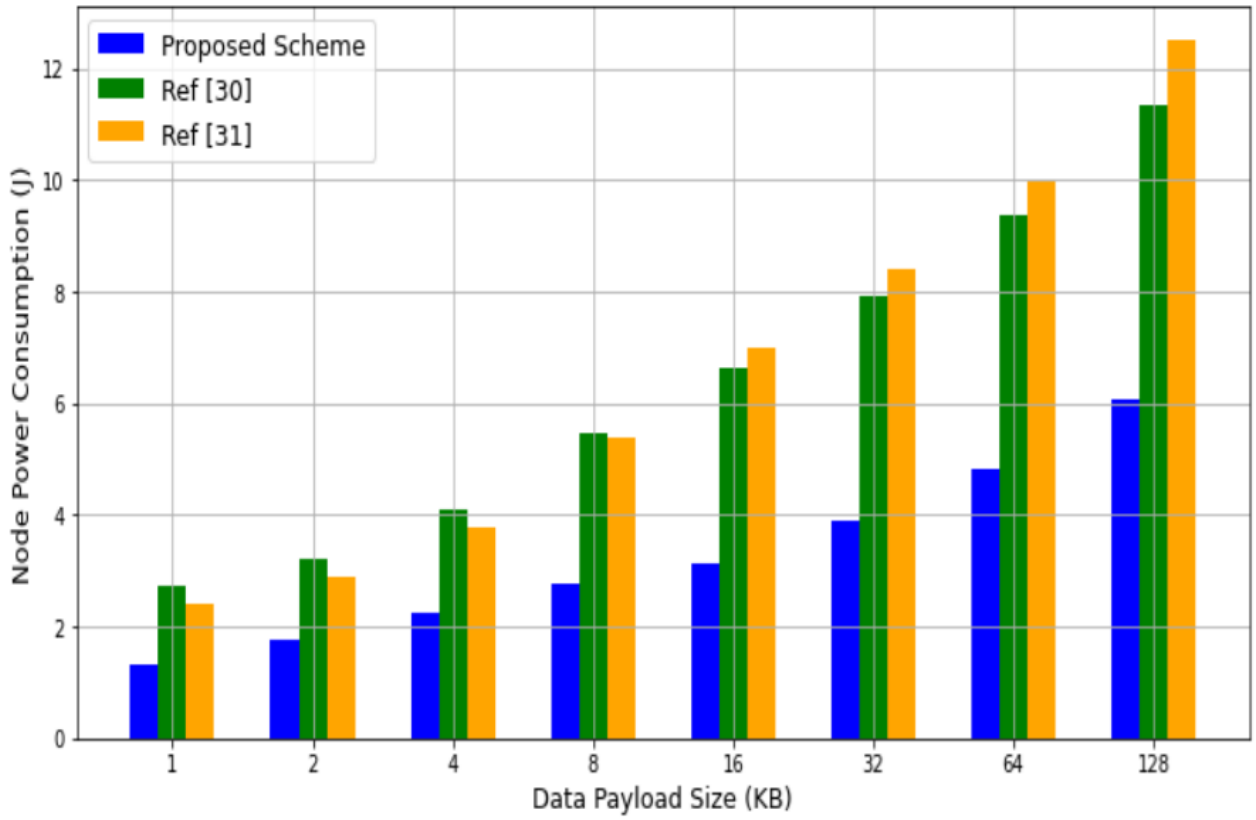


Рис.3.4(а). Енергоспоживання вузла для різних розмірів даних.

Запропонована схема PRE демонструє значно знижений Pw порівняно з подібними схемами. У середньому дана схема споживає 3,32 Дж, з яких 46% загальної потужності використовується SN для шифрування та передачі даних протягом періоду моделювання. CH несе в середньому 13% Pw для процесу повторного шифрування, із середніми витратами Pw 41% під час процесу дешифрування SN. Примітно, що ці енерговитратні процеси виявляють пряму кореляцію з кількістю задіяних пакетів даних. Для порівняння, вузли IoT, які дотримуються схем PRE з інших робіт, демонструють середні рівні Pw 6,28 Дж і 6,23 Дж відповідно під час обміну даними з кінцевими вузлами. Ці схеми потребують більшої потужності через значні інвестиції ресурсів, необхідні для асиметричного PRE.

У наступному моделюванні Pw і час життя мережі аналізуються за допомогою запропонованої схеми, а потім порівнюються зі схемами, представленими в інших роботах. Цей аналіз включав зміни в кількості SN, часу моделювання та кількості обміну даними між SN, як показано на Рисунках 6 (б),

(в) і (г), відповідно. Результати на Рисунку 6 (б) показують, що запропонована схема може ефективно зменшити Pw мережі приблизно на 40% для всіх SN порівняно зі схемами в інших роботах. Потім час моделювання було поступово збільшено з 30 с до 150 с, щоб забезпечити повне споживання електроенергії на деяких SN, а потім було проаналізовано вплив на мережу Pw.

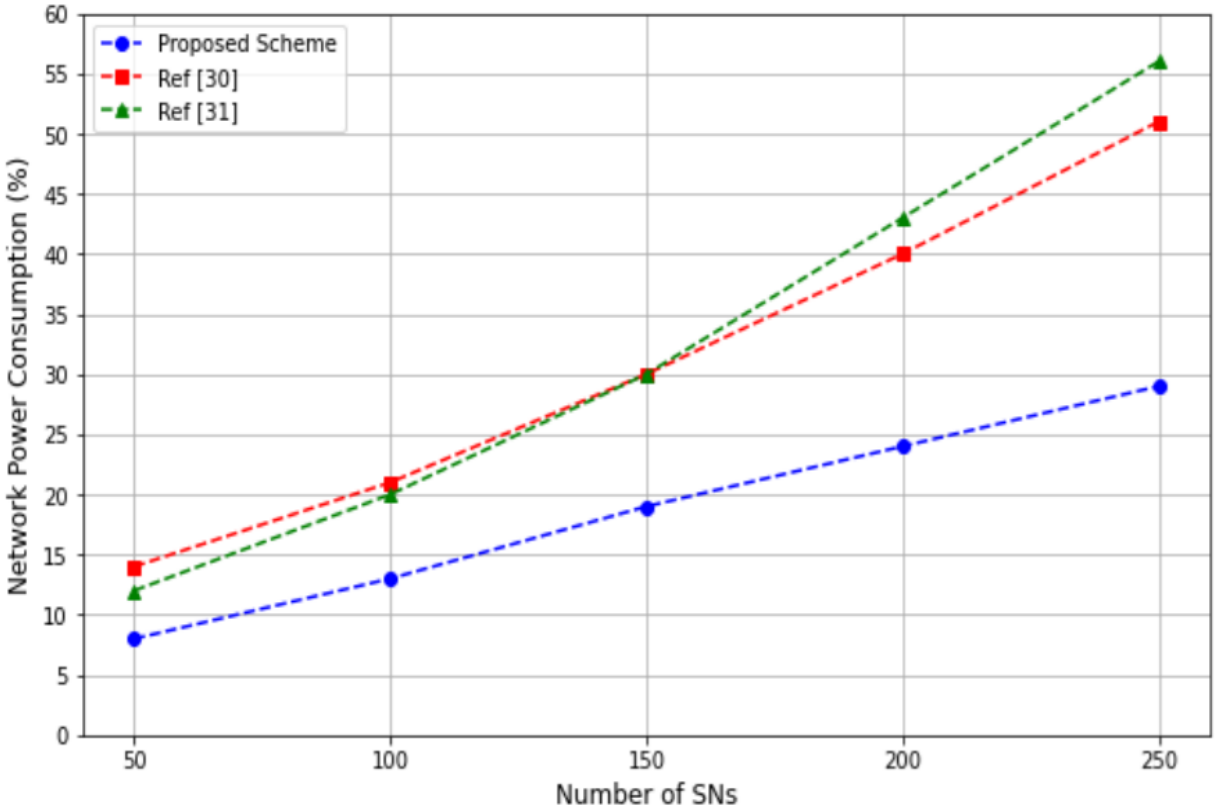


Рис.3.5(б). Співвідношення відсотку енергоспоживання мережі до кількості SN.

Результати на Рисунку 6 (в) показують, що запропонована схема зменшує споживання електроенергії мережею приблизно на 31,5% і 33% порівняно зі схемами в інших роботах.

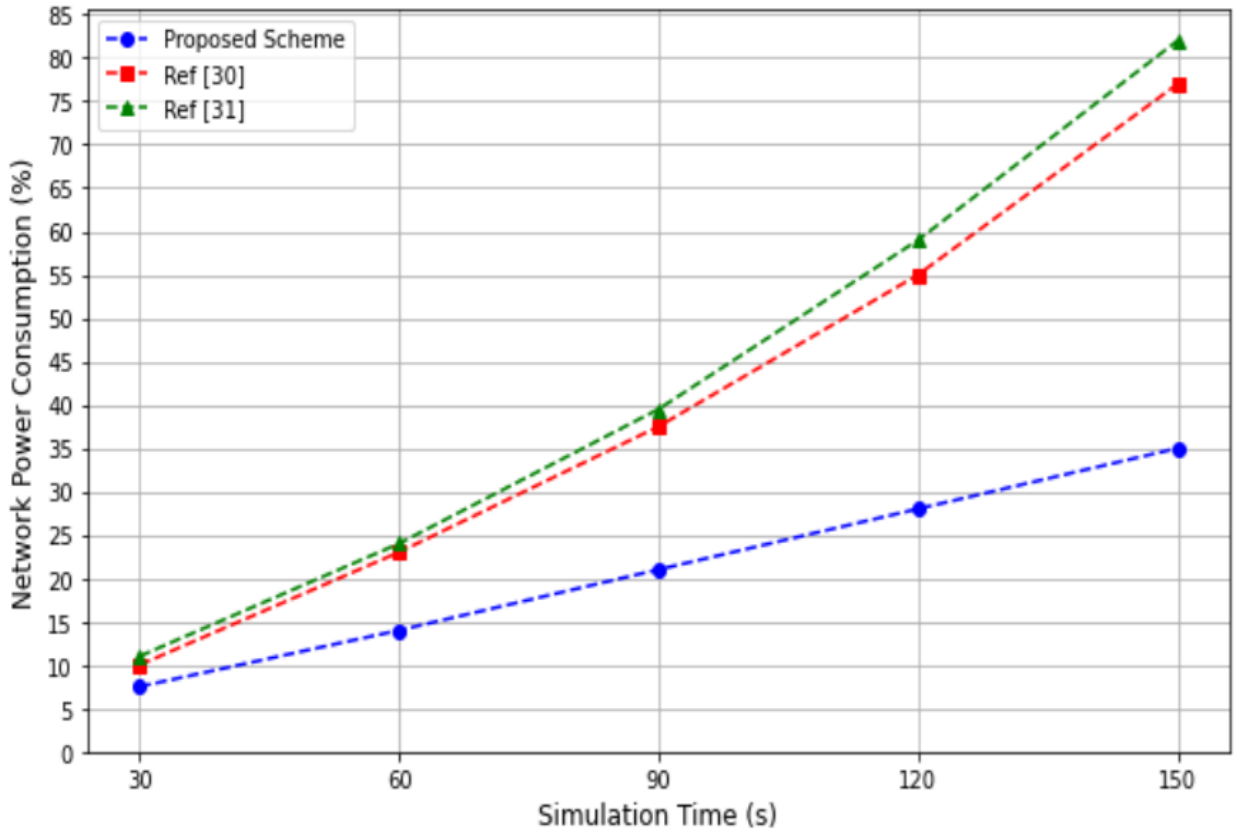


Рис.3.6(в). Співвідношення відсотку енергоспоживання мережі в до витраченого часу моделювання.

Згодом було проаналізовано вплив збільшення обсягу обміну даними між SN у різних кластерах на тривалість життя мережі за допомогою запропонованої схеми PRE та порівняно її з аналогічними схемами PRE. Результати на малюнку 6(d) показують, що тривалість життя мережі змінюється з 11 с до 29 с, оскільки кількість спільних даних збільшується з 50 до 250, незалежно від будь-яких проблем із затримкою мережі. Зміна тривалості життя мережі майже подвоюється в схемах в інших роботах, коли кількість спільних доступів досягає 250. Це пов’язано зі збільшенням енергоспоживання під час операцій PRE, яке зростає зі збільшенням обсягу даних, які спільно використовуються між вузлами.

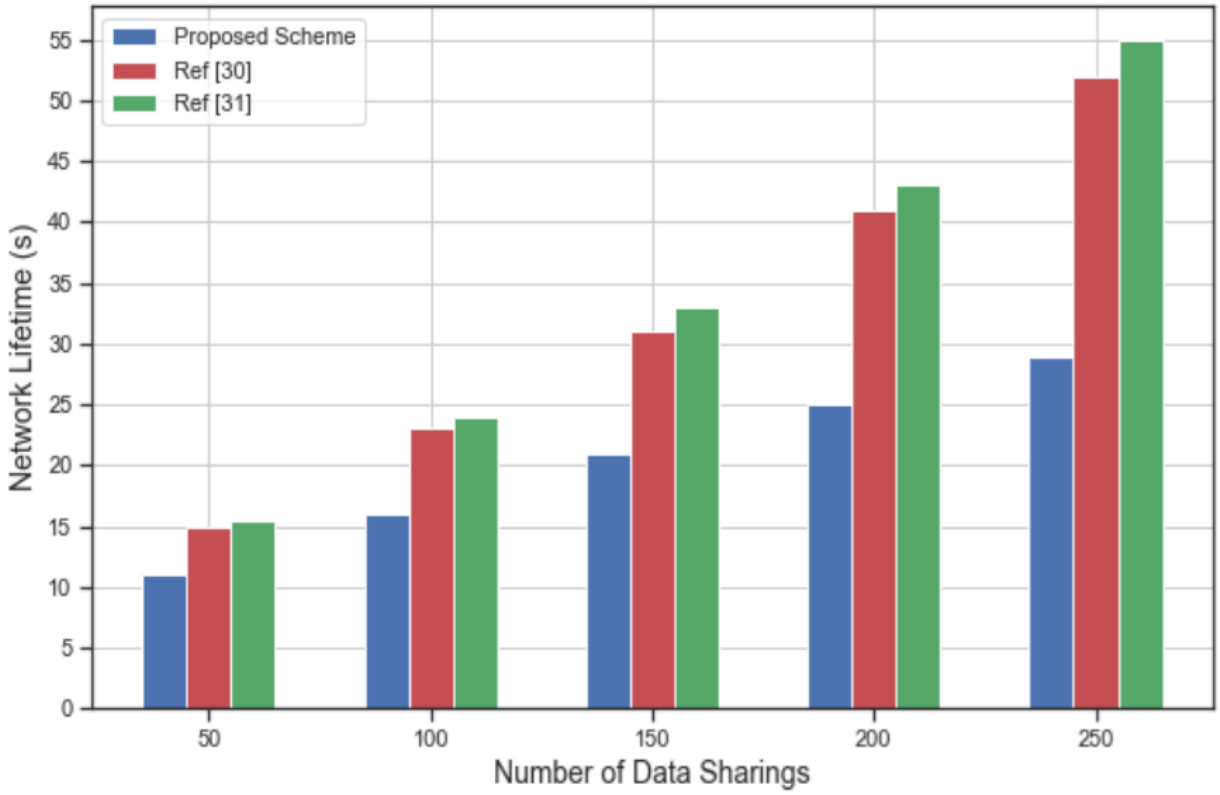


Рис.3.7(г). Співвідношення тривалості роботи мережі до кількості обмінів даними між SN.

Запропонована схема PRE покращує масштабованість за рахунок використання легких криптографічних методів, забезпечуючи цілісність даних, зберігаючи енергетичні ресурси CH. Інтеграція TAN оптимізує розподіл ключів, враховуючи збільшену кількість вузлів і передачу даних у WSN. Унікальна реалізація ключа для кожного сеансу між SN зміцнює безпеку та запобігає ризикам у всій мережі, пов'язаним із компрометацією ключа, дозволяючи розширювати мережу без уразливостей спільних або статичних ключів.

Динамічне керування ключами, адаптоване до сеансу або контексту даних, зменшує накладні витрати на розподіл, ефективно керуючи більшою кількістю вузлів. Крім того, впровадження ієрархічних або розподілених систем керування ключами посилює масштабованість, керуючи криптографічними операціями в масштабованих мережах вузлів для безпечного зв'язку на тлі зростаючих вимог WSN.

Завдяки інноваційному дизайну розподілу відповідальності за завдання PRE на різні CH в WSN дана схема ефективно пом'якшує обмеження, притаманні

існуючим схемам, які покладаються на один підключений хмарний сервер. Цей децентралізований підхід вирішує проблеми, пов’язані з балансуванням навантаження та окремими точками відмови, що відрізняється від централізованих проектів. Дана схема пропонує більш масштабоване та відмовостійке рішення, особливо зі збільшенням кількості підключених датчиків. На відміну від централізованих хмарних серверів, даний підхід розподіляє обчислювальне навантаження по всій мережі, підвищуючи масштабованість і стійкість з найменшим впливом на загальну продуктивність системи.

3.4. АНАЛІЗ БЕЗПЕКИ

У цьому розділі досліджується надійність безпеки запропонованої схеми PRE, щоб оцінити її стійкість до типових атак, спрямованих на WSN. Оцінка зосереджена на його ефективності у встановленні безпечного зв’язку та обміні даними в мережі, дотримуючись суворих вимог безпеки.

Щоб отримати всебічну інформацію про безпеку даної системи, цей аналіз надав пріоритет усуненню поширених загроз, таких як атаки Sybil, підробка даних, підслуховування та атаки man-in-the-middle. Дані методології ґрунтувалися на застосуванні криптографічної перевірки, реалізації наскрізного шифрування, перевірці підписів і генерації унікальних криптографічних ключів. Завдяки систематичній оцінці ці заходи були ретельно перевірені на потенційну вразливість. Завдяки систематичній оцінці ці заходи пройшли суворе тестування на наявність потенційних вразливостей.

У запропонованій схемі PRE кожному SN в кластері призначається унікальний ID, пов’язаний з CH. Цей ідентифікатор служить засобом перевірки автентичності вузла. Крім того, достовірність ідентичності SN підтримується за допомогою відповідного процесу перевірки.

Щоб забезпечити безпеку даних, які спільно використовуються між SN, було запроваджено наскрізне шифрування та використано криптографічні ключі. Ці ключі унікально генеруються TAN і безпечно передаються до певних вузлів, залучених до кожного сеансу передачі. Крім того, був застосований двофазний процес автентифікації. На першому етапі SN та пов’язаний з ним CH проходять

автентифікацію, щоб переконатися, що кожен SN підтверджений перед будь-якою передачею даних. На другому етапі CH перевіряє автентичність SN або кінцевий AP перед тим, як розпочати передачу повторно зашифрованих даних.

Ключі шифрування та параметри автентифікації належать виключно уповноваженим особам, і їх законність підтверджується здатністю одержувача розшифрувати K, пов'язаний з кожним пакетом даних. Конфіденційність даних захищено за допомогою асиметричного шифрування через відкритий ключ власника даних, що запобігає несанкціонованому доступу з боку CH та інших організацій. Крім того, тільки перевірені CH з унікальними ідентифікаторами отримують rk від TAN. Це запобігає неавторизованим CH доступ до ключів або брати участь у повторному шифруванні передачі даних. Отже, оскільки повідомлення передаються виключно через автентифіковані вузли, для зловмисника надзвичайно складно видати себе за легітимні SN або CH під час потенційної передачі даних, що включає в себе підроблені або фальсифіковані дані.

Кожен SN має єдиний зареєстрований ідентифікатор разом із CRT і парою ключів. Процес підписання повідомлення вимагає використання як DS, так і Crt відправника. Оскільки ідентифікатори SN за своєю суттю пов'язані з їхніми відповідними CH і TAN, ця конструкція ефективно запобігає створенню зловмисниками нових ідентифікаторів для ініціювання атак Sybil. Забезпечення цілісності даних у нашій передачі WSN має вирішальне значення для запобігання втручанню в роботу шкідливих вузлів. Це досягається за допомогою DSSN, згенерованого з використанням хешу PkSN відправника. Ці коди підтвердження додаються до зашифрованих пакетів даних. На кінцевому вузлі використовується перевірка на основі хешу для підтвердження кодів автентичності та забезпечення цілісності даних. Відповідні підписи не тільки підтверджують цілісність даних, але й перевіряють, чи відповідають вони очікуваним значенням. Одержувач не може створити дійсний підпис без знання хеш-значення. Отже будь-який неправильний DS означає несанкціоновані зміни даних об'єктом-одержувачем, демонструючи таким чином надійну підтримку цілісності даних у запропонованій схемі.

Кожна передача даних у даній схемі поєднується з Crt, що запобігає SN заперечувати автентичність повідомлення або хибно приписувати дії іншим особам із авторизованими SN, використовуючи свої унікальні Crt для ексклюзивного підпису своїх повідомлень, дозволяючи одержувачам перевіряти особу відправника для неспростування.

Крім того, оскільки TAN є єдиним органом, відповідальним за генерацію ключів шифрування та параметрів для різних вузлів, і кожен сеанс шифрування використовує унікальне випадкове значення r у межах Sprm, створення надлишкових ключових компонентів стає безглуздим. Таким чином, спроби змови за участю зловмисних SN або CH не можуть призвести до отримання ключа дешифрування. Отже, наша схема ефективно протистоїть змові та спробам відмови.

Якщо зловмисник намагається відновити ключі шифрування та параметри переданих даних із SN за допомогою атак «грубої сили», кожна частина даних, передана чи спільна, піддається шифруванню та повторному шифруванню за допомогою окремого набору ключів, згенерованого TAN. Крім того, кожен Sk шифрується за допомогою унікального Pk, пов’язаного з конкретним SN. Як наслідок, для зловмисника стає неможливо обчислити правильні значення ключів Sk, r k, P k і Prk, необхідних для відновлення інших даних, пов’язаних з тим самим SN або будь-яким іншим вузлом, використовуючи атаки «грубої сили». Складність вгадування випадкових значень ключів, необхідних для розшифровки даних, робить це надзвичайно складним завданням. Отже, запропонована схема PRE демонструє надійний захист від атак «грубої сили». Враховуючи можливість підслуховування зловмисником або атак «людина посередині» для перехоплення трафіку зв’язку між SN, CH і AP, навіть зловмисний противник зіткнеться зі значними труднощами в досягненні своїх цілей. Розшифровка секретних параметрів, включаючи випадкові r і секретні значення v, представляє величезну проблему. Крім того, отримання точок Prk і ECC об’єкта вважається неможливим для зловмисників через їх нездатність обчислити для цієї мети випадково

згенеровані високоентропійні точки ECC. Таким чином, наша схема є надійною для захисту від підслуховування та атак типу "людина посередині".

Актуальність даних передбачає перевірку того, що отримане повідомлення було нещодавнім і не підлягало повторному використанню чи відтворенню потенційним зловнисником. Щоб захистити мережу від потенційних атак повторного відтворення, свіжість повідомлення має бути автентифікована в межах лічильника передачі або визначеного періоду часу. У нашій схемі монотонно зростаючий лічильник використовується для зв'язку між SN і CH, а також між CH і AP. Цей лічильник гарантує, що повідомлення було надіслано нещодавно, і не дозволяє зловмисникам відтворювати старі повідомлення з SN або повторно шифрувати дані з CH, таким чином зберігаючи свіжість даних. У таблиці 3.2 представлено порівняльний аналіз характеристик безпеки та ефективності запропонованої схеми PRE та інших схем PRE, розроблених для обмежених мереж.

Таблиця 3.2 - Порівняльний аналіз запропонованих і споріднених схем PRE для обмежених у ресурсах мереж.

Feature	Ref [30]	Ref [31]	Ref [32]	Ref [24]	Proposed Scheme
PRE-cryptography	Lightweight asymmetric encryption	Lightweight asymmetric encryption	lightweight Asymmetric encryption	Lightweight asymmetric encryption	Lightweight symmetric and asymmetric encryption
Scheme environment	IoT networks	IoT networks	IoT-enabled smart grid	IoT-based Blockchain	WSNs
Authentication effectiveness	Moderate	Moderate	Strong	Strong	Strong
Data integrity	No	No	Yes	Yes	Yes
Network attack resistance	Moderate	Moderate	Moderate	Strong	Strong
Collusion and repudiation resistance	Moderate	Poor	Moderate	Moderate	Strong
Execution performance	Moderately efficient	Moderately efficient	Moderately efficient	Low efficiency	Highly efficient
Energy efficiency	Moderately expensive	Moderately expensive	Moderately expensive	Relatively expensive	Inexpensive

Ця всебічна оцінка однозначно підтверджує надійність системи щодо пом’якшення значних загроз безпеці, які зазвичай зустрічаються під час обміну даними в середовищах WSN. Це рішуче підтверджує ефективність наших стратегій у захисті системи від вразливостей. Крім того, впровадження цих заходів

підкреслює здатність системи зберігати цілісність і конфіденційність даних, демонструючи стійкість навіть у різноманітних і складних сценаріях.

РОЗДІЛ 4. РЕЗУЛЬТАТИ СПОРІДНЕНОЇ РОБОТИ

Численні схеми PRE, кожна з яких характеризується різними особливостями та можливостями, були вже раніше представлені в літературі. Ці схеми були розроблені, щоб запропонувати різноманітні властивості, включаючи односпрямованість, нетранзитивність, непередаваність, неінтерактивність, стійкість до змови, проксі невидимість, вихідний доступ і оптимальність ключа. Ці атрибути відіграють ключову роль в оцінці придатності схеми для конкретних застосувань і були широко досліджені в академічних дослідженнях.

Найновітніші схеми PRE часто розроблялися на основі поєднання цих властивостей, зосереджуючи їх оцінку на наявності цих специфічних атрибутів, щоб забезпечити що обрана схема відповідає бажаним цілям безпеки. Дослідники включили звичайні криптографічні методи, такі як шифрування на основі ідентичності (ШОІ), шифрування на основі ролей (ШОР), шифрування на основі атрибутів шифрування (ШОА) і шифрування на основі сертифікату (ШОС), щоб розширити область застосування рішень PRE. Ці криптографічні методи були інтегровані в фреймворки ШПШ, що забезпечує універсальне рішення для задоволення широкого спектру вимог до безпеки та обміну даними. Цей підхід сприяє диверсифікації механізмів безпеки в рамках PRE, надаючи дослідникам ширших можливостей вибору інструментів для адаптації своїх рішень до конкретних сценаріїв та обмежень.

Однак обчислювальна ефективність цих криптографічних методів PRE може змінюватися в залежності від різних факторів. У певних сценаріях, особливо складних політики доступу або великого обсягу даних, ці методи можуть призвести до високого рівня обчислювальні витрати під час дешифрування. Ці витрати в першу чергу пов’язані з операціями створення пари та забезпеченням політики. Крім того, управління криптографічним ключем та політикою доступу можуть стати особливо громіздкими у міру масштабування системи, що потенційно може призвести до адміністративних складнощів і вразливості безпеки, вони неефективні для впровадження в умовах обмежених ресурсів

пристроїв, у яких обчислювальні ресурси та енергозбереження мають першочергове значення.

Щоб усунути вищезазначені обмеження, дослідники доклали немалих зусиль для вдосконалення рішень PRE для пристроїв з обмеженими ресурсами. У цьому контексті схема PRE на основі ШОА була представлена дослідниками щоб підвищити безпеку на платформах інтернету речей (IoT), завдяки чому криптографічні накладні витрати були пом'якшені за допомогою еліптичної кривої шифрування для операцій шифрування, повторного шифрування та дешифрування. Крім того, питання про зашифровані тексти змінної довжини було розглянуто дослідниками раніше, де зашифрований текст розширюється у міру збільшення атрибутів. Ця схема PRE є цінною у сценаріях, коли скомпрометовані ключі дешифрування користувача можуть бути визнані недійсними, що призведе до створення стійкої до змови схеми шифру-політики ШОА. Крім того, введено покращений підхід щоб забезпечити постійну довжину зашифрованих текстів через PRE, зменшуючи накладні витрати на обчислення та зв'язок водночас підтримуюючи стійкість проти білінійної проблеми Діффі-Хеллмана. У іншій статті дослідники запропонували схему, яка базується на складності розв'язання білінійної оберненої задачі Діффі-Хеллмана, адаптованої до пристроїв IoT. Ця двонаправлена схема підтримує багатофункціональність, дозволяючи плавне перетворення завантажених зашифрованих текстів у декілька різних форм у мережах IoT без розшифрування. Схема PRE також була розроблена для перетворення зашифрованих текстів між ключами без необхідності повної довіри до проксі або інтенсивних обчислювальних операцій, реалізуючи цей проект через ефективну автентифікацію процедури узгодження ключа, реалізованою за допомогою повторного шифрування проксі-сервера, розробленого для програм IoT. Ця схема дозволяє встановити спільний секретний ключ між пристроями та використовує симетричний шифр для шифрування даних. Інше дослідження представило схему PRE на основі атрибутів із ізольованим ключем для пристроїв з обмеженими ресурсами. Цей підхід позначає зашифровані тексти атрибутами та приймає структурований підхід до привілеїв доступу користувачів. Делегатори

мають можливість генерувати ключі повторного шифрування за допомогою своїх особистих ключів і довіряти це завдання напівнадійному серверу даних. Тривалість життя системи розділена на окремі часові інтервали, кожен відзначається регулярним оновленням закритих ключів, які в свою чергу контролюють права доступу. Інші дослідження інтегрували блокчейн у підходи PRE для підвищення цілісності та безпеки даних. Ця інтеграція гарантує прозорі та захищені від підробки транзакції даних, додаючи додатковий рівень захисту для загальної безпеки системи.

Полегшене шифрування, яке добре підходить для середовищ з обмеженими ресурсами, є криптографічним підходом, призначеним для мінімізації накладних витрат на обчислення та пам’ять. Його головною метою є визначення пріоритету ефективності при збереженні прийнятного рівня безпеки, що робить його ідеальним вибором для розгортання в мережах з обмеженою обчислювальною потужністю та пам’яттю. Дослідники включили легке шифрування в схеми PRE. Ці схеми відіграють важливу роль у забезпеченні безпечного обміну даними та обміну даними в розподілених і децентралізованих системах. Однак традиційні методи PRE, що покладаються на симетричні шифри, часто вимагають розповсюдження унікальних попередньо-спільних секретних ключів, що потенційно створює вразливість безпеки. Щоб вирішити ці проблеми, для IoT були представлені схеми PRE, що використовують полегшене асиметричне шифрування з використанням криптографії з еліптичною кривою (ECC). Ці підходи забезпечують баланс між безпекою та ефективністю, що робить їх придатними для обмеженої у ресурсах мережі Інтернету речей.

Тим не менш, важливо зазначити, що при одночасному обміні зовнішніми даними з багатьма сторонами обчислювальне навантаження на проксі-сервер може суттєво зрости, що потенційно може призвести до обчислювальних витрат і затримок у відповіді на мережеві пристрої. Таким чином, незважаючи на те, що легке шифрування та його застосування в схемах PRE пропонують багатообіцяючі можливості для підвищення безпеки та ефективності в мережах з обмеженими

ресурсами, необхідно ефективно вирішувати проблеми, пов’язані з масштабованістю та керуванням обчислювальним навантаженням.

Незважаючи на суттєві покращення безпеки та ефективності PRE, особливо в контексті IoT, пристрої з обмеженими ресурсами створюють проблеми, які необхідно визнати, і певні критичні обмеження, пов’язані з унікальною архітектурою та обмеженнями WSN, ще не були належним чином усунені. Попередні дослідження не повністю розглядали тонкощі WSN, включаючи їх вимоги до ефективної маршрутизації, агрегації даних і самоорганізації. Отже, практичність і ефективність цих схем PRE можуть бути скомпрометовані в реальному розгортанні WSN. Крім того, інтеграція блокчейну та інших атрибутів у підходи PRE, водночас підвищуючи цілісність і безпеку даних, може створити проблеми, пов’язані з надлишком ресурсів, затримкою та масштабованістю, які є критичними для WSN. Таким чином, потрібне ефективне рішення для вирішення проблем інтеграції PRE в WSN і забезпечення бездоганного узгодження цих технологій.

ВИСНОВКИ

1. У даній роботі представлена інноваційна схема PRE, розроблена для вирішення унікальних проблем, що виникають у WSN. PRE пристосовується між CH, щоб сприяти безпечному внутрішньо- та міжкластерному зв'язку, обміну даними та автентифікації між вузлами WSN. Для оптимізації ефективності та економії ресурсів запропонована конструкція вправно керує криптографічними обчислювальними витратами за допомогою збалансованої комбінації легких симетричних і асиметричних методів шифрування. Симетричне шифрування Speck використовувалося для захисту даних SN, тоді як повторне шифрування покладалося на ECC для обробки симетричних ключів шифрування, доданих до зашифрованого тексту. Крім того, була розроблена ефективна техніка керування ключами, щоб забезпечити безпечне створення, розповсюдження та актуальність ключів у динамічному середовищі WSN.

2. Результати оцінювання надійно підтверджують ефективність нашої адаптованої схеми PRE в WSN, демонструючи її здатність значно підвищувати продуктивність шифрування, повторного шифрування та дешифрування, мінімізуючи навантаження на обмежені ресурси SN. Крім того, дана схема демонструє надзвичайну масштабованість, ефективно вирішуючи проблеми, які зазвичай пов'язані з централізованими підходами PRE. Крім того, розподіляючи завдання PRE через WSN, наша конструкція вміло зменшує ризик єдиної точки відмови, підвищуючи загальну міцність і надійність системи. Результати оцінювання демонструють помітне зниження енергоспоживання SN на 40% і зниження загального енергоспоживання мережі на 32% порівняно з існуючими рішеннями PRE, розробленими для середовищ з обмеженими ресурсами. Значне скорочення часу обробки в даній схемі PRE, пов'язане зі спрощеними методами повторного шифрування та проксі, підвищує ефективність CH, зберігаючи надійні заходи безпеки.

3.Аналіз безпеки підтвердив, що схема відповідає основним вимогам безпеки, включаючи конфіденційність, автентифікацію, цілісність і стійкість до змови та відмови. Запропонована схема демонструє надійність проти поширених

загроз WSN, таких як атаки відтворення, Sybil, атаки «людина посередині» та атаки «грубої сили».

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. O. A. Khashan, R. Ahmad, and N. M. Khafajah, ‘‘An automated lightweight encryption scheme for secure and energy-efficient communi- cation in wireless sensor networks,’’ Ad Hoc Netw., vol. 115, Apr. 2021, Art. no. 102448.
2. O. A. Khashan, S. Alamri, W. Alomoush, M. K. Alsmadi, S. Atawneh, and U. Mir, ‘‘Blockchain-based decentralized authentication model for IoT-based E-learning and educational environments,’’ Comput., Mater. Continua, vol. 75, no. 2, pp. 3133–3158, 2023.
3. I. Mashal, O. A. Khashan, M. Hijjawi, and M. Alshinwan, ‘‘The determi- nants of reliable smart grid from experts’ perspective,’’ Energy Informat., vol. 6, no. 1, pp. 1–23, Apr. 2023.
4. O. A. Khashan and N. M. Khafajah, ‘‘Efficient hybrid centralized and blockchain-based authentication architecture for heterogeneous IoT sys- tems,’’ J. King Saud Univ. Comput. Inf. Sci., vol. 35, no. 2, pp. 726–739, Feb. 2023.
5. A. Sufyan, K. B. Khan, O. A. Khashan, T. Mir, and U. Mir, ‘‘From 5G to beyond 5G: A comprehensive survey of wireless network evolution, challenges, and promising technologies,’’ Electronics, vol. 12, no. 10, p. 2200, May 2023.
6. F. H. El-Fouly, M. Kachout, Y. Alharbi, J. S. Alshudukhi, A. Alanazi, and R. A. Ramadan, ‘‘Environment-aware energy efficient and reliable routing in real-time multi-sink wireless sensor networks for smart cities applications,’’ Appl. Sci., vol. 13, no. 1, p. 605, Jan. 2023.
7. Z. A. Zukarnain, O. A. Amodu, C. Wenting, and U. A. Bukar, ‘‘A survey of Sybil attack countermeasures in underwater sensor and acoustic net- works,’’ IEEE Access, vol. 11, pp. 64518–64543, 2023.
8. O. A. Khashan, N. M. Khafajah, W. Alomoush, M. Alshinwan, S. Alamri, S. Atawneh, and M. K. Alsmadi, ‘‘Dynamic multimedia encryption using a parallel file system based on multi-core processors,’’ Cryptography, vol. 7, no. 1, p. 12, Mar. 2023.

9. K. Jain, P. S. Mehra, A. K. Dwivedi, and A. Agarwal, ‘‘SCADA: Scalable cluster-based data aggregation technique for improving network lifetime of wireless sensor networks,’’ J. Supercomput., vol. 78, pp. 13624–13652, Mar. 2022.
10. O. A. Khashan, ‘‘Parallel proxy re-encryption workload distribution for efficient big data sharing in cloud computing,’’ in Proc. IEEE 11th Annu. Comput. Commun. Workshop Conf. (CCWC), Jan. 2021, pp. 554–559.
11. M. Su, B. Zhou, A. Fu, Y. Yu, and G. Zhang, ‘‘PRTA: A proxy re-encryption based trusted authorization scheme for nodes on CloudIoT,’’ Inf. Sci., vol. 527, pp. 533–547, Jul. 2020.
12. S. M. Patil and B. R. Purushothama, ‘‘Non-transitive and collusion resistant quorum controlled proxy re-encryption scheme for resource constrained networks,’’ J. Inf. Secur. Appl., vol. 50, Feb. 2020, Art. no. 102411.
13. O. A. Khashan, ‘‘Hybrid lightweight proxy re-encryption scheme for secure fog-to-things environment,’’ IEEE Access, vol. 8, pp. 66878–66887, 2020.
14. G. Kan, C. Jin, H. Zhu, Y. Xu, and N. Liu, ‘‘An identity-based proxy re-encryption for data deduplication in cloud,’’ J. Syst. Archit., vol. 121, Dec. 2021, Art. no. 102332.
15. N. H. Sultan, V. Varadharajan, L. Zhou, and F. A. Barbhuiya, ‘‘A role- based encryption (RBE) scheme for securing outsourced cloud data in a multi-organization context,’’ IEEE Trans. Services Comput., vol. 16, no. 3, pp. 1647–1661, Jun. 2023.