АВТОМАТИЗОВАНИЙ МЕТОД МІКРОСЕГМЕНТАЦІЇ IOT-МЕРЕЖ ДЛЯ РЕАЛІЗАЦІЇ АРХІТЕКТУРИ ZERO TRUST

Нєдєльніцев І.В., Антіпов І.Є.
Харківський національний університет радіоелектроніки, Харків, Україна

Динамічні процеси розгортання великих і різнорідних IoT-систем, від розумних домівок до масштабних індустріальних мереж, створюють надлишкові та хаотичні канали зв'язку між вузлами. Така структурна ентропія має значний вплив на розширення поверхні атаки та створює ідеальні умови для горизонтального переміщення зловмисника після первинної компрометації одного з вузлів у середині периметру. Первинна компрометація часто відбувається через обхід застарілих заходів безпеки, експлуатацію вразливостей програмного забезпечення або використання легкодоступних пристроїв, таких як IP-камери чи сенсори. Це дозволяє зловмиснику використовувати функціонально надлишкові зв'язки та рухатися до критичних вузлів інфраструктури, таких як шлюзи чи хмарні сервіси. Тому розробка архітектурних підходів для протидії цим загрозам та впровадження парадигми Zero Trust є важливою науковою задачею [1].

Згідно зі стандартом NIST SP 800-207 [2], впровадження Zero Trust є відмова від довіри за замовчуванням, безперервна верифікація та мікросегментація системи. Мікросегментація – це сучасний метод забезпечення мережевої безпеки, який передбачає поділ центрів обробки даних та хмарних середовищ на невеликі ізольовані сегменти для впровадження детальних політик безпеки [3]. Сучасні мережі мають складну структуру взаємодії, що значно ускладнює розуміння легітимності шляхів передачі даних та ручне застосування класичних моделей сегментації або стандартних декларативних профілів, таких як MUD (Manufacturer Usage Description) [4], які хоч і задають політику за замовчуванням, але потребують адаптивної перевірки. Різноманіття пристроїв та їхні обмежені ресурси для обчислення ускладнюють перенесення традиційних механізмів ізоляції корпоративного рівня в IoT-середовище без втрати керованості саме тому є необхідність у пошуках методів та засобів автоматизації великих IoT мереж.

Метою доповіді є розробка гібридного математичного методу автоматизованої мікросегментації мережі, як один з аспектів Zero Trust архітектури, кардинально знизити ризики латерального руху та автоматично синтезувати політики безпеки на основі застосування спектральної кластеризації графів та евристичного прунінгу.

В доповіді наводяться результати застосування розробленого алгоритму, який математично моделює IoT-мережу як орієнтований зважений граф, де множина ребер $G = (V, E)$, поділяється на легітимні функціональні зв'язки E_{func} та паразитні шумові зв'язки E_{noise}. Для моделювання ентропії реального середовища генерується топологічний шум, ймовірність появи якого залежить від сумісності ролей: $P(u,v) = P_{base}(Role_u, Role_v) \times \sigma$ при цьому

враховується феномен «Rich get richer», коли центральні шлюзи мають вищу ймовірність отримати паразитні з'єднання. Мережа поділяється на 4 ієрархічні рівні:

1. L1 – сенсори, камери, актуатори;
2. L2 – агрегатори, хаби, контролери;
3. L3 – шлюзи;
4. L4 – хмарні сервіси, сервери.

Метод використовує матрицю Лапласа $L_{sym} = I - D^{-\frac{1}{2}}AD^{-\frac{1}{2}}$ [5] для знаходження власних векторів (зокрема вектора Фідлера, що кодує оптимальний розріз) та подальшого розбиття графа на ізольовані функціональні кластери.

Для усунення логічних вразливостей всередині кластерів додатково застосовується евристичний прунінг – фільтрація на основі жорстких правил. Зокрема, алгоритм блокує горизонтальну взаємодію між пристроями першого рівня – $L(u) = L(v) = 1$, забороняє зв'язки з різницею рівнів більше одиниці $|L(u) - L(v)| > 1$ – та існує $u \to w \to v$, відсікає надсилання команд до що не можуть їх приймати – $L(u) > L(v)$ та $R(v) \neq Actuator$, а також забороняє прямий доступ пристроїв рівня 1 та 2 до зовнішніх мереж в обхід проміжних вузлів.

Наведені дані експериментального моделювання, проведеного для трьох масштабів мереж (мала ~30, середня ~330, велика ~950 пристроїв) з інтенсивністю шуму σ від 0.0 до 5.0, показують, що на ефективність алгоритму безпосередньо впливають масштаб та зашумленість.

Для кількісної оцінки ефективності запропонованого методу пропонується вимірювати результати сегментації за допомогою спеціалізованих метрик:

– *wASR* (Weighted Attack-Surface Reduction) – зважене зменшення поверхні атаки;

– *wLMI* (Weighted Lateral Movement Index) – зважений індекс горизонтального переміщення;

– *FBR* (False Block Rate) – частка хибних блокувань легітимного трафіку;

– *PCR* (Policy Compression Ratio) – ефективність стиснення правил.

Зважене зменшення поверхні атаки(*wASR*), розраховується за формулою:

$$wASR = 1 - \frac{\sum_{(u,v)\in E_{policy}} Crit(v)}{\sum_{(u,v)\in E_{total}} Crit(v)},$$

де: E_{total}– множина всіх спостережуваних фізичних та логічних зв'язків у мережі до сегментації (включаючи ентропійну складову);

E_{policy} – підмножина зв'язків, дозволених синтезованою політикою;

$Crit(v) \in [0, 1]$ – коефіцієнт критичності вузла-приймача v.

Аналіз даних показує, що для середніх та великих мереж спостерігається стабільне лінійне зростання *wASR*; при $\sigma = 5$ досягається зменшення поверхні

атаки на 48%. Натомість у малих мережах показник стабілізується в межах 0.25 – 0.30 після досягнення рівня шуму $\sigma = 3$.

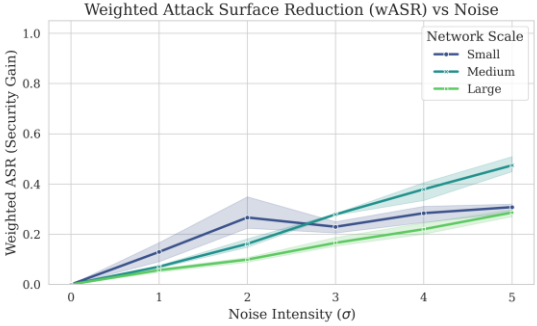

Рис. 1. Зважене зменшення поверхні атаки (wASR) відносно шуму

Для великомасштабних мереж алгоритм виявляє надзвичайно високу стійкість до зашумлення: при рівні шуму $\sigma = 2$ зважений ризик горизонтального переміщення (*wLMI*) стабільно знижується на 78.4%. Цей показник розраховується за формулою:

$$wLMI = \frac{1}{|V|} \sum_{u \in V} \frac{\sum_{v \in Reach(u, E_{policy})} Crit(v)}{\sum_{v \in V} Crit(v)}$$

де $Reach(u, E_{policy})$ представляє множину всіх вузлів, до яких існує шлях від вузла u.

Спостереження за частотою помилкових блокувань (*FBR*) свідчить про збереження високого рівня функціональної цілісності системи: для великих мереж при $\sigma = 2$ частка помилково заблокованих легітимних зв'язків становить лише 1.6%, що повністю відповідає експлуатаційним вимогам промислових середовищ (поріг < 5%).

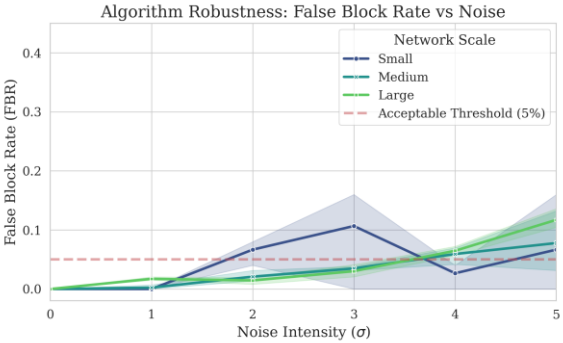

Рис. 2. Стійкість до топологічних шумів

Крім того, значення ефективності стиснення політик (*PCR*), що розраховується як $PCR = \frac{|E_{policy}|}{|E_{total}|}$, становить 0.81 для топологій з інтенсивним шумом $\sigma = 3$. Це доводить здатність системи автоматично відсікати до 19% аномальних з'єднань, оптимізуючи навантаження на мережеве обладнання, полегшуючи адміністрування та підтримку такої системи.

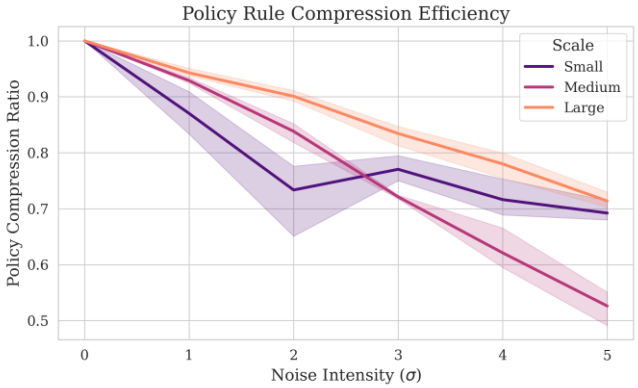

Рис. 3. Коефіцієнт стиснення політики

В зв'язку з цим актуальності набувають методи автоматизованого синтезу політик безпеки, засновані на використанні узагальнених математичних характеристик мережевої зв'язності.

Запропонований підхід забезпечує надійну локалізацію кіберінцидентів у межах однієї зони/сегменту, гарантуючи ізоляцію критичних вузлів інфраструктури від скомпрометованих периферійних пристроїв. Це дозволяє усунути операційну складність адміністрування та ефективно масштабувати парадигму Zero Trust в умовах сучасних високоентропійних IoT-систем, генеруючи компактні правила фільтрації (ACL) без ручного втручання.

Список літератури

1. Moskvin K., Sievierinov O. Zero Trust Architecture in Corporate Cybersecurity Systems // Computer and information systems and technologies : Seventh International Scientific and Technical Conference, 2024. – Kharkiv : NURE, 2024. – p. 54-55.

2. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. NIST Special Publication 800-207. 2020. С. 1–50. DOI: https://doi.org/10.6028/NIST.SP.800-207.

3. What is microsegmentation in networking? вебсайт. URL: https://www.cloudi-fi.com/glossary/what-is-microsegmentation (дата звернення: 29.03.2025).

4. Lear E., Droms R., Romascanu D. Manufacturer Usage Description Specification. RFC 8520. 2019. С. 1–45. DOI: https://doi.org/10.17487/RFC8520

Wang X. Complex network security using community structure and dynamical analysis: spectral clustering and VEIP-WQU model. Complex Intelligent Systems. 2025. С. 5–7. DOI: https://doi.org/10.1007/s41109-025-00717-8