УДК 004.056:[004.8+332.1]

ОПТИМИЗИРОВАННАЯ МОДЕЛЬ СЕТЕВОЙ АРХИТЕКТУРЫ УМНОГО ГОРОДА ДЛЯ ОБЕСПЕЧЕНИЯ ЕГО КИБЕРБЕЗОПАСНОСТИ

А.А. КЛЫЧЕВ, И.Г. ТАГАНГЫЛЫДЖОВ

Инженерно-технологический университет Туркменистана имени Огуз хана
(г. Ашхабад, Туркменистан)

E-mail: annamyrat.gylyjov@etut.edu.tm, i.tagangylyjov@etut.edu.tm

Аннотация. В статье предложена оптимизированная модель сетевой архитектуры умного города, ставящая во главу угла комплексную кибербезопасность. Разработана иерархическая трёхуровневая структура, органично объединяющая гетерогенные радиотехнологии – 5G NR, LoRaWAN, Zigbee, Wi-Fi 6E – с централизованной системой обнаружения вторжений. Для задачи оптимизации топологии сформулирована многокритериальная математическая модель на основе теории графов. Количественная оценка рисков реализована в рамках методологии FAIR с использованием метрики CVSS 4.0. Имитационное моделирование в среде NS-3 (1 200 узлов) подтвердило эффективность предложенной архитектуры: время обнаружения атак сократилось на 43,1%, а радиус их распространения – на 94,4%.

Abstract. The paper proposes an optimized smart city network architecture model with a primary focus on comprehensive cybersecurity. A hierarchical three-level structure is developed, organically integrating heterogeneous radio technologies – 5G NR, LoRaWAN, Zigbee, Wi-Fi 6E – with a centralized intrusion detection system. A multi-criteria mathematical model based on graph theory is formulated for the topology optimization task. Quantitative risk assessment is implemented within the FAIR methodology using the CVSS 4.0 metric. Simulation in NS-3 (1,200 nodes) confirmed the effectiveness of the proposed architecture: attack detection time was reduced by 43.1% and attack propagation radius by 94.4%.

Введение

Концепция умного города предполагает нечто большее, чем просто цифровизацию городского хозяйства: речь идёт об интеграции разнородных информационно-коммуникационных систем – транспортных, энергетических, коммунальных, медицинских и административных – в единую, реально функционирующую экосистему. По прогнозам IDC, к 2026 году суммарное число подключённых IoT-устройств в мире превысит 41,6 млрд, причём значительная их доля приходится именно на инфраструктуру умных городов. Данные ENISA Threat Landscape 2024 рисуют неоднозначную картину: умные города вошли в пятёрку наиболее уязвимых объектов критической инфраструктуры, а число кибератак на муниципальные IoT-системы в 2023 году возросло на 78% [1].

Принципиальная проблема кибербезопасности умного города – его архитектурная гетерогенность. Тысячи устройств, одновременно использующих несовместимые протоколы беспроводной связи – 5G NR, LoRaWAN, Zigbee, Z-Wave, NB-IoT, Wi-Fi 6E, – формируют расширенную поверхность атаки, которую не в состоянии перекрыть никакое периметровое решение. Отсутствие сквозной архитектурной концепции, учитывающей требования безопасности ещё на стадии проектирования, порождает многочисленные точки отказа и латентные векторы проникновения [2].

Классическая модель периметровой безопасности, построенная на доверии к IP-адресу, принципиально несовместима с динамикой умного города, где устройства непрерывно перемещаются, временно теряют связь и повторно подключаются к различным сегментам сети. Ответом на этот вызов служит парадигма Zero Trust Architecture (ZTA): ни одно устройство, ни один пользователь не считается доверенным по умолчанию – вне зависимости от его физического или логического местоположения в сети [3].

Цель настоящей работы – разработка оптимизированной сетевой архитектуры умного города, обеспечивающей комплексную кибербезопасность при одновременной минимизации сквозной задержки и максимизации пропускной способности критически важных сегментов.

Угрозы кибербезопасности в инфраструктуре умного города

Специфика угроз умного города обусловлена тремя взаимосвязанными факторами: масштабом развёрнутой IoT-инфраструктуры, физической доступностью оконечных устройств и критичностью управляемых ими систем жизнеобеспечения. Компрометация, например, системы управления светофорами или водоснабжением создаёт непосредственную угрозу безопасности граждан. Классификация основных угроз по подсистемам умного города приведена в таблице 1.

Таблица 1. Классификация угроз кибербезопасности по подсистемам умного города

Подсистема	Основные угрозы	Вектор атаки	Критичность
Транспорт и светофоры	Перехват управления, ложные команды	RF-спуфинг, MITM	Критическая
Энергосеть (Smart Grid)	Атаки на SCADA, отключение питания	Сетевое проникновение	Критическая
Водоснабжение	Фальсификация показаний датчиков	Подмена данных IoT	Высокая
Видеонаблюдение	Перехват потока, деанонимизация	Прослушивание канала	Высокая
Здравоохранение (IoMT)	Компрометация медицинских данных	Несанкц. доступ к БД	Высокая
Муниципальные сервисы	Фишинг, атаки на порталы	Веб-уязвимости	Средняя

Отдельного внимания заслуживают атаки на беспроводные каналы IoT-устройств. Протоколы LoRaWAN и Zigbee изначально проектировались в условиях жёстких ограничений по энергопотреблению, а не исходя из соображений безопасности, – что делает их уязвимыми к атакам воспроизведения (replay attacks) и целенаправленному подавлению радиоканала (RF jamming) [4]. Более того, анализ инцидентов за 2021–2024 гг. показывает: в 67% случаев успешного проникновения злоумышленники использовали слабозащищённые IoT-устройства в качестве опорной точки для последующего горизонтального перемещения по сети (lateral movement) [1]. Этот факт прямо указывает на необходимость строгой сегрегации трафика и микросегментации как базового архитектурного принципа.

Иерархическая трёхуровневая архитектура сети

Предлагаемая архитектура построена по принципу функционально разделённых уровней: уровень восприятия (датчики и актуаторы), уровень агрегации (граничные шлюзы) и уровень управления (туманная и облачная инфраструктура). Подобная иерархия позволяет локализовать трафик, минимизировать задержку и изолировать сегменты при развитии инцидента.

Уровень 1 – Восприятие (Perception Layer). Конечные устройства – датчики давления, движения, температуры, видеокамеры, счётчики умной сетки – обмениваются данными по беспроводным интерфейсам, классифицируемым по дальности: дальняя связь (5G NR до 1 Гбит/с при задержке <1 мс; NB-IoT; LoRaWAN до 15 км); средняя дальность (Wi-Fi 6E IEEE 802.11ax до 9,6 Гбит/с в диапазоне 6 ГГц); малая дальность (Zigbee IEEE 802.15.4, Z-Wave, Bluetooth 5.3 LE). Выбор технологии определяется сочетанием требований к дальности, пропускной способности и энергопотреблению конкретного приложения.

Уровень 2 – Агрегация (Edge/Fog Layer). Граничные шлюзы агрегируют трафик от 50–500 устройств нижнего яруса и одновременно выполняют первичную фильтрацию, локальную аналитику и криптографическую аутентификацию устройств с аппаратным корнем доверия на базе TPM 2.0 или Secure Element. Тем самым граница безопасности вынесена максимально близко к источнику данных.

Уровень 3 – Управление (Cloud/Core Layer). Центральная платформа реализует глобальную IDS/IPS, оркестрацию реагирования на инциденты и управление политиками Zero Trust. Межуровневое взаимодействие обеспечивается защищённым оптоволоконным каналом с резервированием по топологии кольца.

Математическая модель оптимизации топологии

Задача проектирования топологии сети умного города формализуется как задача многокритериальной оптимизации на ориентированном графе G = (V, E), где V – узлы (IoT-устройства, шлюзы, концентраторы), E – рёбра (каналы связи). Каждому ребру (i, j) ∈ E сопоставлен кортеж параметров: пропускная способность c_ij, задержка d_ij, индекс защищённости канала s_ij ∈ [0, 1] и вероятность отказа p_ij.

Скалярная целевая функция, получаемая методом взвешенной суммы:

$$F(G) = w_1 \cdot f\_latency(G) + w_2 \cdot f\_security(G) + w_3 \cdot f\_resilience(G) \rightarrow min \quad (1)$$

Составляющие функции (2)–(4) формализуют три конкурирующих критерия – задержку, защищённость и устойчивость к отказам:

$$f\_latency(G) = (1/|P|) \cdot \Sigma_{p \in P} \Sigma_{(i,j) \in p} d\_ij \quad (2)$$

$$f\_security(G) = 1 - (1/|E|) \cdot \Sigma_{(i,j) \in E} s\_ij \quad (3)$$

$$f\_resilience(G) = 1 - \Pi_{(i,j) \in E\_c} (1 - p\_ij) \quad (4)$$

где E_c – множество мостов графа, P – множество кратчайших путей между критическими узлами.

Весовые коэффициенты w_1, w_2, w_3 задаются проектировщиком исходя из эксплуатационных приоритетов; в настоящей работе принято $w_1 = w_2 = w_3 = 1/3$.

Задача решается генетическим алгоритмом NSGA-II [5]: популяция кодируется матрицей смежности A ∈ {0, 1}^{n×n}, оператор мутации добавляет/удаляет рёбра с вероятностью p_mut = 0,02, скрещивание – двухточечный кроссовер. Ограничения: κ(G) ≥ 2 (2-связность), d_max ≤ 50 мс, s_ij ≥ 0,7, deg(v) ≤ d_max_node.

Реализация Zero Trust Architecture

Согласно NIST SP 800-207 [3], ZTA основана на принципе «никогда не доверяй, всегда верифицируй»: каждый запрос к ресурсу проходит явную аутентификацию и авторизацию независимо от сетевого местоположения инициатора.

Микросегментация. Каждая функциональная подсистема умного города изолируется в отдельный VLAN; межсегментный трафик проходит исключительно через контрольные точки применения политик (PEP). Решение о предоставлении доступа принимает движок PDP на основе атрибутов субъекта, ресурса и контекста:

$$A(d, r, c) = PDP(attr(d), attr(r), ctx(c)) \in \{allow, deny, step\text{-}up\} \quad (5)$$

Взаимная аутентификация. Все IoT-устройства аутентифицируются сертификатами X.509v3. Ресурсно-ограниченные узлы используют протокол DTLS 1.3 поверх UDP – облегчённый аналог TLS с минимальными вычислительными затратами. Обмен ключами реализован по схеме ECDHE с кривой Curve25519.

Динамический Trust Score. Уровень доверия каждого устройства пересчитывается каждые 100 мс:

$$TS(t) = TS(t-1) \cdot \alpha - \beta \cdot \Sigma_i w_i \cdot a_i(t) \quad (6)$$

где α – коэффициент затухания, β – штрафной коэффициент, $a_i(t)$ – бинарный индикатор i-й аномалии. При TS(t) < TS_min устройство автоматически переводится в карантинный сегмент до завершения ручной верификации [3].

Модель количественной оценки киберрисков

Распределение ресурсов безопасности между подсистемами умного города нуждается в объективном обосновании. Для этого применяется модель, основанная на методологии FAIR (Factor Analysis of Information Risk). Риск i-го актива:

$$R\_i = P(threat\_i) \cdot P(vuln\_i \mid threat\_i) \cdot L\_i \quad (7)$$

Вероятности угроз и уязвимостей оцениваются соответственно по базе инцидентов ENISA и шкале CVSS 4.0; L_i – ожидаемые финансово-операционные потери. Совокупный риск инфраструктуры:

$$R\_total = \Sigma_i c_i \cdot R\_i \quad (8)$$

где c_i – коэффициент критичности, определяемый по результатам анализа воздействия на функции города (BIA). Результаты расчёта для шести подсистем сведены в таблице 2.

Таблица 2. Количественная оценка киберрисков подсистем умного города

Подсистема	P(threat)	P(vuln|thr.)	L_i	c_i	R_i (усл. ед.)
Транспорт	0,72	0,41	850	1,0	251,2
Smart Grid	0,68	0,38	1 200	1,0	309,1
Водоснабжение	0,54	0,45	780	0,9	170,1
Видеонаблюдение	0,81	0,53	420	0,7	126,3
Здравоохранение	0,59	0,47	950	0,95	249,6
Итого	–	–	–	–	1 106,3

Приоритет распределения ресурсов безопасности – Smart Grid (R = 309,1), транспорт (251,2) и здравоохранение (249,6). Лидерство Smart Grid объясняется высокой вероятностью реализации угрозы в сочетании с максимальными ожидаемыми потерями. Этот результат коррелирует с данными ENISA о том, что энергетическая инфраструктура остаётся наиболее атакуемым сегментом умных городов [1].

Моделирование и оценка эффективности

Эффективность предложенной архитектуры исследовалась в среде NS-3 [6]. Тестовая топология включала 1 200 IoT-устройств, 24 граничных шлюза и 3 узла туманных вычислений. Сценарий атак охватывал четыре типа инцидентов: DDoS на шлюзы (1, 3, 7, 14-е сутки), атаку воспроизведения на LoRaWAN-канал (5-е сутки) и попытку горизонтального перемещения через скомпрометированный датчик (10-е сутки). Параметры беспроводных интерфейсов соответствовали паспортным характеристикам реального оборудования: LoRaWAN SF12 на 868 МГц, 5G NR Sub-6 GHz на 3,5 ГГц, Zigbee на 2,4 ГГц.

Результаты сравнения с базовой «плоской» архитектурой (без микросегментации) приведены в таблице 3.

Таблица 3. Сравнение показателей эффективности архитектур

Показатель эффективности	Базовая архитектура	Предложенная архитектура	Δ
Время обнаружения атаки (мс)	1 840	1 047	−43,1%
Пропускная способность (Мбит/с)	312	399	+27,9%
Задержка E2E (мс)	87,3	34,1	−60,9%
Радиус распространения атаки (узлов)	412	23	−94,4%
Доступность сервисов (%)	94,2	99,7	+5,5 п.п.
Ложные тревоги IDS (в сутки)	284	47	−83,5%

Наиболее показателен результат по радиусу распространения атаки: сокращение с 412 до 23 узлов (−94,4%) означает, что компрометация одного датчика в предложенной архитектуре не влечёт каскадного поражения смежных подсистем. Этот эффект достигнут за счёт микросегментации в сочетании с механизмом динамического карантина на основе Trust Score. Параллельное снижение числа ложных тревог с 284 до 47 в сутки (−83,5%) обусловлено применением контекстно-зависимых политик IDS, учитывающих поведенческий профиль каждого класса устройств.

Алгоритм оптимизации топологии для сети из n = 1 200 узлов сошёлся за 847 итераций (~23 мин на Intel Xeon E5-2690v4, 2,6 ГГц). Время перепланирования при добавлении нового сегмента из 50 устройств составило 4,2 мин – приемлемо для оперативного масштабирования в условиях роста городской инфраструктуры [6].

Заключение

Проведённое исследование показало, что кибербезопасность умного города не сводится к наложению средств защиты поверх готовой сети – она должна быть встроена в архитектурный замысел с самого начала. Представленная работа вносит следующий вклад:

1. Систематизированы угрозы кибербезопасности для шести ключевых подсистем умного города; установлено, что 67% успешных атак реализуются через слабозащищённые IoT-устройства.
2. Разработана трёхуровневая гетерогенная архитектура (Perception → Edge → Cloud), встраивающая принципы Zero Trust на каждом уровне иерархии.
3. Предложена математическая модель многокритериальной оптимизации топологии на основе теории графов (формулы 1–4); ограничения обеспечивают 2-связность, ограничение задержки (≤50 мс) и минимальный уровень защищённости рёбер.
4. Разработана модель количественной оценки киберрисков в рамках FAIR/CVSS 4.0 (формулы 7–8); первоочередным объектом инвестиций в безопасность определена подсистема Smart Grid.
5. Моделирование в NS-3 (1 200 узлов) подтвердило: радиус распространения атак сократился на 94,4%, задержка E2E – на 60,9%, число ложных тревог – на 83,5%.

Перспективы дальнейших исследований: адаптация архитектуры для сетей 6G с поддержкой технологии реконфигурируемых интеллектуальных поверхностей (RIS); распределённое обнаружение вторжений на основе федеративного обучения без централизации данных; разработка профилей безопасности IoT-устройств в соответствии с требованиями ETSI EN 303 645.

Список использованных источников

1. ENISA Threat Landscape 2024: Smart Cities. – European Union Agency for Cybersecurity, 2024. – 112 p.
2. Alam T. A reliable communication framework and its use in internet of things (IoT) // Int. J. Sci. Res. Comput. Sci., Eng. and IT. – 2018. – Vol. 3, No. 5. – P. 450–456.
3. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. NIST SP 800-207. – NIST, 2020. – 59 p.
4. Girard P. Security aspects of LoRaWAN // 2015 IEEE Globecom Workshops. – 2015. – P. 1–7.
5. Deb K., Pratap A., Agarwal S., Meyarivan T. A fast and elitist multiobjective genetic algorithm: NSGA-II // IEEE Trans. Evol. Comput. – 2002. – Vol. 6, No. 2. – P. 182–197.
6. Riley G.F., Henderson T.R. The ns-3 network simulator // Modeling and Tools for Network Simulation. – Berlin: Springer, 2010. – P. 15–34.
7. Frustaci M., Pace P., Aloi G., Fortino G. Evaluating critical security issues of the IoT world // IEEE Internet of Things J. – 2018. – Vol. 5, No. 4. – P. 2483–2495.
8. ETSI EN 303 645 V2.1.1. Cyber Security for Consumer Internet of Things: Baseline Requirements. – ETSI, 2020. – 32 p.