УДК 004.056

Балансировка нагрузки для повышения достоверности обнаружения уязвимостей интерфейсов беспилотных транспортных средств при двухуровневой схеме формирования коллабораций в сетях 4GLTE-5G

Load balancing to increase the reliability of detecting vulnerabilities in the interfaces of unmanned vehicles with a two-level scheme for the formation of collaborations in 4GLTE-5G networks

Скатков / Skatkov A.
Александр Владимирович
(AVSkatkov@sevsu.ru)
доктор технических наук, профессор.
ФГАОУ ВО «Севастопольский государственный университет» (СевГУ), профессор кафедры информационных технологий и компьютерных систем.
г. Севастополь

Брюховецкий / Bryukhovetskiy A.
Алексей Алексеевич
(bryukhovetskiy@sevsu.ru)
кандидат технических наук, доцент.
СевГУ, заведующий кафедрой информационных технологий и компьютерных систем.
г. Севастополь

Моисеев / Moiseev D.
Дмитрий Владимирович
(DVMoiseev@sevsu.ru)
доктор технических наук, доцент.
СевГУ, профессор кафедры информационных технологий и компьютерных систем.
г. Севастополь

Ключевые слова: формирование кластеров – cluster formation; обнаружение уязвимостей – vulnerability detection; балансировка нагрузки – load balancing; булеан – boolean; коллаборационная стратегия – collaborative strategy; тестирование узлов – node testing.

Рассматривается подход, который базируется на совместном тестированиии состояний природно-технических объектов и систем. Развиваются методы динамического обнаружения уязвимостей интерфейсов устройств мобильных интеллектуальных сетей на основе децентрализованной обработки информационных потоков данных с учетом особенностей технологий 4GLTE-5G. Предметом исследования предлагаемой статьи является решение задачи балансировки нагрузки сети с использованием кластеров, которая включает алгоритм формирования ресурсов инфраструктуры и распределение узлов: тестировщиков и тестируемых по кластерам с целью обеспечения заданной вероятности обнаружения уязвимостей узлов при ограничениях на выделенные ресурсы. Повышение вероятности обнаружения уязвимостей обеспечивается двухуровневой схемой формирования коллабораций на основе модели с использованием булеана. Применение предложенного подхода позволит снизить неоправданный расход ресурсов, повысить вероятность обнаружения уязвимостей узлов, уменьшить риск принятия ошибочных решений.

The approach based on joint testing of the natural-technical objects and systems states is considered. Methods dynamic vulnerability detection of devices interfaces mobile intelligent networks based on decentralized processing of information data flows, taking into account the features of 4GLTE-5G technologies, are being developed. The research subject of the proposed article is the problem solution of the network load balancing using clusters, which includes an algorithm for the formation of infrastructure resources and the distribution of nodes: testers and tested across clusters in order to ensure a given probability of detecting node vulnerabilities under restrictions on allocated resources. An increase in the probability of vulnerability detection is provided by a two-level scheme for the formation of collaborations based on a model using Boolean. The application of the proposed approach will reduce the unjustified consumption of resources, increase the probability of detecting node vulnerabilities, and reduce the risk of making erroneous decisions.

Введение

Инновационная технология mmWave интегрирована в сети мобильной связи 5G. В отличие от 3G/4G, работающий на частоте менее 5 ГГц, радиостанции mmWave 5G работают на гораздо более высоких частотах от 24 до 53 ГГц (согласно 3GPP 38.101 [1]) со значительно большим свободным спектром. Несмотря на высокую полосу пропускания, короткая длина волны mmWave делает ее сигналы уязвимыми к ослаблению. Из-за псевдооптической природы луча сигналы чувствительны к препятствиям, таким, как пешеход или движущееся транспортное средство. Поэтому, чтобы сократить время выхода на рынок, операторы мобильной связи соединяют свое базовое сетевое оборудование 5G с существующей инфраструктурой 4GLTE в так называемом неавтономном развертывании (NSA). NSA использует 5G-NR для операций в плоскости передачи данных, сохраняя при этом свою инфраструктуру 4G для операций в плоскости управления [2]. NSA отличается от автономного развертывания (SA), которой присуща полная независимость от устаревших инфраструктур сотовой связи. В то же время все операторы, указанные в [3], используют модель NSA для своего первого коммерческого развертывания 5G. По сравнению с mmWave 5G, среднечастотный диапазон 5G обеспечивает лучшую мобильность благодаря всенаправленной радиосвязи. По той же причине 4G также демонстрирует гораздо лучшую стабильность при движении узлов сети. Поэтому эти факты указывают на необходимость совместного использования mmWave 5G и всенаправленной радиосвязи, такой, как 4G, в сценариях мобильности, где 4G может помочь гарантировать базовое подключение к данным.

Пусть в сети наблюдаются преднамеренные действия, которые инициируют неправильное поведение узлов, объектов и/или нарушают их нормальное функционирование, а в критических случаях прекращают их работу и создают аварийные ситуации. Эти действия направлены на причинение ущерба функционированию отдельных узлов и/или инфраструктуре сети. Будем говорить, что имеет место злоумышленное поведение отдельных узлов сети, которые могут скомпрометировать поведение других узлов. Будем также считать, что злоумышленник стремится организовать атаку или ставить помехи своего обнаружения и этим самым снизить вероятность обнаружения при тестировании с помощью имеющихся средств защиты своих неправомерных действий. Поэтому для повышения надежности сети против атак, ресурсы защиты сети должны распределяться надлежащим образом.

На практике решение задач, связанных с обработкой характеристик высокодинамичных объектов в условиях стохастической среды, требует больших вычислительных затрат. Как правило, при практическом интересе получения достоверных оценок, исследователи сталкиваются с размерностями задач, которые относятся к классу NP-сложных [4]. Их решение затруднено в реальном времени, так как требует полного перебора вариантов. Для большинства практических задач это неприемлемо из-за большой размерности (2^n), ограниченного времени и недостаточности ресурсов.

В предыдущей статье авторов [5] решается задача обнаружения уязвимостей интерфейсов БТС на основе коллаборационной стратегии, которая базируется на децентрализованных дисциплинах взаимного тестирования узлов. В ней отмечается, что решаемая задача относится к классу NP-сложных. Поэтому в качестве одного из подходов к снижению ее вычислительной сложности предложено перераспределение процессов обработки данных.

Предметом исследования предлагаемой статьи является решение задачи балансировки нагрузки сети с использованием кластеров, которая включает алгоритм формирования ресурсов инфраструктуры и распределение узлов тестировщиков и тестируемых по кластерам с целью обеспечения заданной вероятности обнаружения уязвимостей узлов при ограничениях на выделенные ресурсы.

В данной статье повышение вероятности обнаружения уязвимостей обеспечивается двухуровневой схемой формирования коллабораций на основе модели с использованием булеана [6]. Булеаном $B(X)$ множества X называется множество всех подмножеств множества X. Если мощность множества $|X|$ равна n элементов, его булеан содержит 2^n подмножеств. В решаемой задаче элементами таких подмножеств являются два класса устройств: k – тестировщики, $(n–k)$ – тестируемые. Поэтому булеан может быть подвергнут биссекции – разделению множеств на указанные классы. Теперь если использовать условия высечения из булеана нужных подмножеств, элементы которых удовлетворяют требованиям обработки данных, то возникает задача балансировки – распределения элементов выделенных подмножеств булеана. Такой подход позволит снизить размерность задачи и решать ее в реальном времени. Кроме того, отсутствие балансировки приводит к нежелательным последствиям в сети:

– неоправданный расход ресурсов;
– снижение пропускной способности каналов;
– увеличение задержки обработки данных;
– риск ошибок первого и второго рода и др.

Аналитические решения задачи балансировки не известны, поскольку они приводят к решению задач дискретной оптимизации, k-значной логики, задачам на графах. Поэтому предметом рассмотрения в статье являются регулярные алгоритмы эвристической природы, которые не зависят от вариаций наборов исходных данных и могут быть реализованы в сетях 4GLTE-5G.

Описание модели

Решается задача балансировки нагрузки сетевых устройств в интеллектуальных мобильных транс-

портных сетях архитектуры 4GLTE-5G / NLOS. Считается, что сигнал распространяется в непрямой видимости [7]. Балансировка предполагает:

– распределение тестировщиков – k и тестируемых узлов – n_c по кластерам – виртуальным группам, в которых осуществляется совместное тестирование,

– распределение ресурсов инфраструктуры по кластерам, в частности, ресурсов базовых станций, которые бы обеспечивали заданный уровень обнаружения уязвимостей при коллаборационной стратегии тестирования, учитывающей число тестировщиков и тестируемых в каждом кластере.

Задано:

n – число узлов всего,

k – число тестировщиков в кластере,

n_c – число узлов в кластере,

$P_{C_{\min}}$ – минимально допустимая вероятность обнаружения уязвимостей в j-ом кластере.

Требуется распределить тестировщиков и тестируемые узлы по кластерам с целью обеспечения минимально допустимой вероятности обнаружения уязвимостей $P_{C_{\min}}$ в каждом j-ом кластере при коллаборационной стратегии совместного тестирования узлов в составе кластеров:

$$P_j \geq P_{C_{\min}} \tag{1}$$

Введем обозначения:

N – число кластеров,

R – общий объем защитных ресурсов, выделяемый для всех узлов,

R_j – текущий объем защитного ресурса j-го кластера, выделяемый в процессе распределения ресурсов,

$R_{C_{\max}}$ – максимально возможный объем защитного ресурса, выделяемый для кластера,

r – объем защитного ресурса, выделяемый на одно тестирование одному тестировщику,

ΔR_j – доля защитного ресурса, используемая j-м кластером,

Δp_j – эффективность обнаружения уязвимостей в j-м кластере,

где

$$\Delta R_j = R_j / R_{C_{\max}},$$

$$\Delta p_j = P_j / P_{C_{\min}}, j = 1, 2, \ldots, N.$$

Лучшим распределением будем считать то, для которого отношение $f_j = \Delta p_j / \Delta R_j$ имеет максимальное значение. Оно достигается при меньшем использовании защитных ресурсов и большей вероятности обнаружения уязвимостей.

Далее рассматривается модель взаимодействия узлов в составе коллабораций. Подход на основе коллабораций позволяет организовать различные стратегии, отличающиеся эффективностью обнаружения уязвимостей при различных альтернативных критериях, которые оценивают затраты, время задержки передачи данных, скорость передачи данных, достоверность принятия решения, вероятность отказа тестирования и др.

В условиях коллаборационной модели имеет место совместное тестирование узлов в составе виртуальных групп – кластеров. Пусть в группе из n_c устройств взаимное тестирование выполняют k устройств, $1 \leq k \leq n_c$. Каждое из k устройств проводит k тестов: по одному тесту на каждое устройство. Тогда вероятность обнаружить атаку за k тестов при биномиальном распределении будет:

$$P(p(t), k, n_c) = C_{n_c}^k p^k(t)\left(1 - p^k(t)\right)^{n_c - k}, \tag{2}$$

где $p(t)$ – вероятность обнаружения уязвимости при однократном тестировании.

Введем следующие ограничения:

$$0 \leq R_j \leq R_{C_{\max}}, j=1, 2, \ldots, N,$$

$$\sum_{j=1}^{N_C} R_j \leq R. \tag{3}$$

Суммарный объем ресурсов кластеров R_j не может превышать общий объем ресурсов R. Когда объем защитного ресурса максимальный, то вероятность отказа при тестировании маленькая, и наоборот.

Пусть ресурс, выделяемый на одно тестирование, равен r. Тогда на k тестировщиков планируется rk^2 ресурсов. Объем ресурсов, выделенный под тестировщиков, не может превышать максимальный объем кластера:

$$rk^2 \leq R_{C_{\max}}. \tag{4}$$

Из отношения (4) определяется максимальное количество тестировщиков $k_{\max}$ в кластере:

$$k_{\max} = \left[\left(R_{C_{\max}} / r\right)^{\frac{1}{2}}\right]. \tag{5}$$

С учетом (3) минимальное число кластеров определится как:

$$N = \left[R / R_{C_{\max}}\right] \tag{6}$$

Если выражение (6) содержит дробную часть, то последний кластер будет иметь свободный ресурс, который может быть использован в решении задачи балансировки.

Определяем число узлов в первом $(N-1)$ кластере, считая кластеры гомогенными по используемым технологиям обработки/обмена данными между узлами на уровне базовой станции:

$$n_c = [n/(N-1)] \quad (7)$$

Последний кластер с номером N содержит n_N узлов :

$$n_N = n - n_c(N-1) \quad (8)$$

Значит, в последний кластер может быть добавлено n_+ узлов с других кластеров:

$$n_+ = n_c - n_N \quad (9)$$

Обозначим начальное распределение узлов по кластерам в виде вектора C:

$$C = (C_{01}, C_{02}, ...C_{0j}, ...C_{0,N})$$

В каждом j-м кластере $j = 1,2,...,(N-1)$ определено значение k_0 – число тестировщиков $1 \le k_0 \le k_{\max}$, при котором вероятность обнаружения уязвимостей имеет максимальное значение [5] и выполняется условие (1) для заданного $P_{C_{\min}}$.Во всех указанных кластерах используется сочетание $C_{n_c}^{k_0}$, $k_0 < n_c$. В последнем кластере содержится n_N узлов, и это количество может быть дополнено n_+ узлами с (N-1)-го кластера.

Ставится задача перераспределить n_- узлов с кластеров с номерами $j = 1,2,...,(N-1)$ при переносе их на последний кластер и сформировать распределение сочетаний C_n^k по всем кластерам. Каким образом можно это осуществить?

Можно снимать по одному узлу с каждого j-го кластера, $j = 1,2,...,(N-1)$ в различных сочетаниях: $C_{(N-1)}^{n_-}$, где $n_- = 1,2,...n_+$. В результате формируются сочетания из n_- длиной $(N-1)$. Будут построены двухэлементные C_{N-1}^2 подмножества, трехэлементные C_{N-1}^3 подмножества и так далее. Общее число различных подмножеств, содержащих всевозможные сочетаний снятия единиц с $(N-1)$ кластеров, равно

$$\sum_{n^-=1}^{n^+} C_{(N-1)}^{n^-} \quad (10)$$

В дальнейшем для построения модели формирования множества векторов, отличающихся различными сочетаниями C_n^k компонент, будем использовать понятие булеана $B(X)$ [6], которое содержит 2^n элементов и представляет собой множество всех подмножеств множества X мощностью n элементов.

В таблице 1 приведен пример формирования множества $B^1(N-1)$ из подмножества векторов $n_- = (n_1, n_2, ..., n_j, ..., n_{N-1})$размерностью $N-1$, где значение компоненты n_j обозначает снятие с j-го кластера указанного числа узлов. Столбец n_+ содержит добавляемое число узлов в последний кластер N.

Аналогично используются базовые множества $B_0^2(N-1), B_0^3(N-1)$, ..., $B_0^{n^+}(N-1)$ для формирования булеанов $B^2(N-1), B^3(N-1), \ldots, B^{n+}(N-1)$ при снятии двух, трех и т.д. n_+ узлов с каждого j-го кластера, $j = 1,2,...,(N-1)$ и приформирование этих узлов в последний кластер с соблюдением ограничения (7) на максимально возможное число узлов в кластере. После построения булеанов над ними с помощью операции декартова произведения с последующим суммированием значений соответствующих компонент n_j формируются всевозможные сочетания снятия одного, двух и т.д. узлов.

Обозначим операцию декартова произведения над булеанами

$$B^1(N-1) \times B^2(N-1) ... \times ... B^{n_+}(N-1)$$

$$DecSum(B^1, B^2 ... B^{n_+})$$

На практике достаточно ограничиться множествами сочетаний снятия одного и двух узлов, каждое из которых будет содержать 2^{N-1} векторов. Максимальное добавление узлов в последний кластер при снятии одного узла с кластера составит $(N-1)$по числу кластеров. Если одновременно снимается два узла с кластера, то максимальное добавление составит $2(N-1)$ узлов. Если сформировать всевозможные сочетания векторов первого и второго множества с

Таблица 1

Пример базового множества $B_0^1(N-1)$ снятия одного узла для формирования булеана $B^1(N-1)$

	Подмножество векторов n_-				
Номер вектора	n_1	n_2	n_1	n_{N-1}	n_+
1	0	0	….	0	0
2	1	0	….	0	1
	….	….	….	….	1
N	0	0	….	1	1

выполнением сложения содержимого соответствующих компонент, то мы получим всевозможные комбинации снятия узлов от 1 до $3(N-1)$. Для $N=5$ максимальное число узлов, которое может быть снято и добавлено в последний кластер, равно 12. Для числа узлов в кластере больше 10 становится проблематичным достигнуть высокую вероятность обнаружения уязвимостей в соответствии с (2) и выполнения (4) при ограниченных ресурсах на кластер.

В статье [5] авторами получены оценки выражения (2) в зависимости от числа *n, k* и $p(t)$ – вероятность обнаружения уязвимости при однократном тестировании. Установлены закономерности изменения значения $P(p(t), k, n)$ в зависимости от значений указанных параметров. Для фиксированного *n* и увеличивающемся значении *k* имеет место экстремум величины $P(p(t), k, n)$. Так имеют место следующие закономерности:

1) $p(t) \geq 0.5$:

P_j – уменьшается при увеличении *n* при заданном *k*.

P_j – увеличивается при увеличении *k* при заданном *n*.

2) $p(t) < 0.5$:

P_j – уменьшается при увеличении *n* относительно заданного *k*, обеспечивающем $P_j = \max$.

P_j – уменьшается и при увеличении *k* и при уменьшении *k* относительно заданного *n*, обеспечивающем $P_j = \max$.

Поэтому в процессе балансировки для каждого измененного значения n_c – числа элементов в кластере будет определено соответствующее значение *k* из диапазона $1 \leq k_0 \leq k_{\max}$, обеспечивающие максимальные оценки вероятности P_j обнаружения уязвимостей в *j*-м кластере, удовлетворяющие (1).

Таким образом, решение задачи балансировки сводится к формированию множества векторов $C_i = \{C_{i1}, C_{i2}, ..., C_{ij}, ...C_{iN}\}$ размерностью, равной числу кластеров *N*:

$$\begin{Bmatrix} C_{11}, C_{12}, ..., C_{1j}, ..., C_{1N} \\ C_{21}, C_{22}, ..., C_{2j}, ..., C_{2N} \\ C_i = C_{i1}, C_{i2}, ..., C_{ij}, ..., C_{iN} \\ C_{2,1}^{2N}, C_{2,2}^{2N}, ..., C_{2,j}^{2N}, ..., C_{2,N}^{2N} \end{Bmatrix} \quad (12)$$

где $i = 1,2,...,2^{2N}$, $C_{ij} = (n_j, k_j, f_j)$.

Каждая компонента C_{ij} вектора C_i содержит следующие характеристики:

n_{ij} – число узлов,

k_{ij} – число тестировщиков,

f_{ij} – показатель качества кластера.

Указанные характеристики *j*-й компоненты кластера позволяют оценить потребляемый объем ресурсов, обеспечивающий допустимую вероятность обнаружения уязвимостей. Из всего множества векторов распределений сочетаний узлов по кластерам необходимо выбрать тот, который при выполнении (1), (3), (4) обеспечивает:

$$\Delta R_i = 1/(N \cdot R_{C_{\max}}) \sum_{j=1}^{N} r k_{ij}^2 = \min,$$

$$\Delta p_i = 1/(N \cdot P_{C_{\min}}) \sum_{j=1}^{N} P_{ij}(p(t), k_{ij}, n_{ij}) = \max,$$

$$f_i = \Delta p_i / \Delta R_i = \max. \quad (13)$$

Базовый алгоритм балансировки ресурсов FunBal

Кластерная инфраструктура при двухуровневой схеме формирования коллабораций в сетях 4G-LTE/5G требует задания следующих исходных данных:

1. Исходные значения параметров для решения задачи балансировки:

1.1 Максимальное количество тестировщиков $k_{\max}$ в кластере:

$$k_{\max} = [(R_{C_{\max}} / r)^{\frac{1}{2}}].$$

1.2 Минимальное число кластеров:

$$N = [R / R_{C_{\max}}].$$

1.3 Число узлов в первые $(N-1)$ кластеры:

$$n_c = [n/(N-1)].$$

1.4 Число узлов n_N в последнем кластере с номером *N*:

$$n_N = n - n_c(N-1).$$

1.5 Число узлов n_+, которое может быть добавлено в последний кластер с других кластеров:

$$n_+ = n_c - n_N.$$

Алгоритм $FunBal(R, R_{C_{\max}}, r)$ содержит следующую последовательность действий:

1. Формируется начальное распределение узлов по кластерам в виде вектора *C*:

$$C = (C_{01}, C_{02}, ...C_{0j}, ...C_{0,N})$$

В каждом *j*-м кластере $j = 1,2,...,(N-1)$ определено значение k_0 – число тестировщиков $1 < k_0 < k_{\max}$, при котором вероятность обнаружения уязвимостей имеет максимальное значение для заданного n_c.

2. Формируются булеаны множеств $B^1(N-1)$, $B^2(N-1), ...B^{n_-}(N-1)$при снятии одного, двух и т.д. n_- узлов с каждого *j*-го кластера, $j = 1,2,...,(N-1)$.

3. Выполняется операция декартова произведения над булеанами $B^1(N-1) \times B^2(N-1)... \times ...B^{n_-}(N-1)$ с последующим суммированием соответствующих значений компонент

$$DecSum(B^1, B^2 ... B^{n_+}).$$

4. Формируется множество векторов C_i (12) мощностью 2^{2N} и размерностью N.

Для каждого вектора C_i выполняется перераспределение узлов между $(N-1)$ кластерами и последним кластером N. Пусть $f_{\max} = 0$.

5. На каждом i-м шаге $i = 1$ до $i = 1$ до 2^{2N}:

5.1 $j = 1, N$:

– для каждого измененного значения n_j определяется соответствующее значение k_j из диапазона $1 < k_0 < k_{\max}$, обеспечивающие $P_j(p(t), k_j, n_j) = \max$.

– если $P_j < P_{C_{\min}}$ и $j < N$, то переход на 6.1, иначе если $j = N$, то переход на 6.4.

– для каждой j-й компоненты вектора $C_{ij} = (n_j, k_j)$ оцениваются характеристики качества распределения узлов в кластере:

$$\Delta R_j = (1/R_{C_{\max}}) r k_j^2,$$

$$\Delta p_j = (1/P_{C_{\max}}) P_j(p(t), k_j, n_j).$$

– если $j < N$, то переход на 6.1.

5.2 Для каждого вектора C_i интегрально оцениваются характеристики качества распределения узлов по кластерам:

$$\Delta R_i = 1/(N \cdot R_{C_{\max}}) \sum_{j=1}^{N} r k_{ij}^2,$$

$$\Delta p_i = 1/(N \cdot P_{C_{\min}}) \sum_{j=1}^{N} P_{ij}(p(t), k_{ij}, n_{ij})$$

$$f_i = \Delta p_i / \Delta R_i.$$

5.3 Вычисленное значение f_i сравнивается с $f_{\max}$: если $f_i > f_{\max}$, то $f_{\max} = f_i$.

5.4 Если $i < 2^{2N}$, то переход на 6.1, иначе если $f_{\max} = 0$, то при заданных ресурсах r, R, $P_{C_{\max}}$, $P_{C_{\min}}$ решения нет и требуется изменение указанных параметров: увеличить объемы выделяемых ресурсов или/и уменьшить $P_{C_{\min}}$.

6. Решением является вектор C_i, содержащий компоненты распределений $C_{n_j}^{k_j} (j = 1,..N)$ по кластерам, для которого $f_i = \max$.

На основе модели *FunBal* разработана программная система, которая реализована на языке *Java*. Для исследования модели проведены целенаправленные эксперименты по балансировке нагрузки сети с использованием кластерной архитектуры при варьировании входных данных в различных сценариях. В таблице 2 представлены поддерживаемые сценарии по исследованию влияния параметров на значения целевых функций модели (13).

При проведении экспериментов входные параметры варьировались в следующих диапазонах: $360 \le R \le 510$, $70 \le R_{C_{\max}} \le 90$, $1 \le r \le 2$, $37 \le n \le 49$. При этом были сформированы значения параметров, которые изменялись в диапазонах: $5 \le k_{\max} \le 9$, $5 \le N \le 8, 5 \le n_c \le 10$.

Анализируя полученные результаты, следует отметить:

1. Наибольшее влияние на значения показателя качества f_j оказывает значение вероятности $P_j(p(t), k_j, n_j)$, которое в свою очередь, во-первых, зависит от вероятности обнаружения при однократном тестировании, во-вторых, от числа тестировщиков k_j и, наконец, от числа узлов n_j в кластере.

2. При $p \ge 0.5$ целесообразно использовать меньшие значения k_j, n_j, удовлетворяющие текущим ограничениям на $P_{C_{\max}}$ и R. Поскольку при их увеличении значения вероятности P_j уменьшается, а затраты кластерной памяти растут.

Таблица 2

Поддерживаемые сценарии модели FunBal

Поддерживаемые сценарии	Параметры влияния на значение целевых функций						
	r	R	$P_{C_{\max}}$	$P_{C_{\min}}$	$p(t)$	k	n
С1- исследование влияния объема ресурса r	*var*				*var*	*var*	*var*
С2- исследование влияния объема ресурса R		*var*			*var*	*var*	*var*
С3- исследование влияния объема ресурса $R_{C_{\max}}$			*var*		*var*	*var*	*var*
С4- исследование влияния $P_{C_{\min}}$				*var*	*var*	*var*	*var*

3. При $p < 0.5$ наблюдается другая тенденция. Имеет место увеличение значения вероятности P_j при увеличении k, а затем ее снижение. Поэтому в таких случаях выбирается оптимально допустимое значение k при заданном n, для которого $P_j = \max$.

4. При превышении числа узлов в кластере $n_j \geq 8$ достичь эффективного распределения становится проблематичным, т.к. для достижения высокого значения $P_j(p(t), k_j, n_j)$ требуется большее число тестировщиков, а это, в свою очередь, приводит к увеличению объема кластерной памяти. В результате рост показателя качества $f_j = \Delta p_j / \Delta R_j$ становится не очевидным.

Выводы

Представленные детерминированные модели в дополнение к разработанным авторами ранее получили дальнейшее развитие за счет включения новых модулей. Разработан базовый алгоритм балансировки ресурсов *FunBal* кластерной инфраструктуры при формировании коллабораций в сетях 4GLTE/5G, который включает следующие основные модули: формирования ресурсов инфраструктуры и распределение узлов тестировщиков и тестируемых по кластерам с целью обеспечения заданной вероятности обнаружения уязвимостей узлов при ограничениях на выделенные ресурсы. Повышение вероятности обнаружения уязвимостей обеспечивается двухуровневой схемой формирования коллабораций на основе модели с использованием булеана. Применение предложенного подхода позволит снизить неоправданный расход ресурсов, повысить вероятность обнаружения уязвимостей узлов, уменьшить риск принятия ошибочных решений. Результаты компьютерного моделирования при различных сценариях проведения экспериментов подтверждают целесообразность предложенного подхода, который позволяет реализовать альтернативные стратегии защиты устройств в интеллектуальных мобильных транспортных сетях 4GLTE/5G.

Исследование выполнено при финансовой поддержке РФФИ в рамках научных проектов № 19-29-06015, № 19-29-06023.

Литература

1. 3GPP Specification Series 38 : 3GPP privacy policy. Retrieved October 2019. – URL: https://www.3gpp.org/DynaReport/38-series.htm (дата обращения 24.02.2023).

2. Hillbur. 5G deployment options to reduce the complexity / A. Hillbur. – URL: https://www.ericsson.com/en/blog/2018/11/5g-deployment-options-to-reduce-the-complexity (дата обращения : 02.03.2023).

3. A First Look at Commercial 5G Performance on Smartphones / A. Narayanan, E. Ramadan, J. [et al.] // Proceedings of The Web Conference 2020 (WWW '20) (April 20–24, 2020, Taipei, Taiwan). – 2020. – P. 894–905.

4. Алгоритмы: построение и анализ / Т.Х. Кормен, Ч.И. Лейзерсон, Р.Л. Ривест, К. Штайн. – 2-е издание. – Москва : Вильямс, 2005. – 1296 с.

5. Скатков, А. В. Коллаборационные стратегии обнаружения уязвимостей интерфейсов информационно-измерительных сетей ПТС при технологиях 5G / А.В. Скатков, А.А. Брюховецкий // Системы контроля окружающей среды. – 2022. – № 49 (3). – С.84–97.

6. Андерсон, Д. А. Дискретная математика и комбинаторика / Д.А. Андерсон. – Москва : Вильямс, 2004. – 960 с.

7. Steering with eyes closed: mm-wave beam steering without in-band measurement / T. Nitsche, A.B. Flores, E.W. Knightly, J. Widmer // 2015 IEEE Conference on Computer Communications (INFOCOM) (Hong Kong, China). – 2015. – P. 2416–2424.

8. Скатков, А. В. Модели коллабораций обнаружения уязвимостей интерфейсов беспилотных транспортных средств в условиях противодействия на основе стандарта 5G / А.В. Скатков, А.А. Брюховецкий, Д.В. Моисеев // Информация и Космос. – 2022. – № 4. – С. 58–65.

9. Скатков, А. В. Методология организации мониторинговых процессов при решении крупномасштабных задач в облачных вычислительных средах / А.В. Скатков, А.А. Брюховецкий, Д.В. Моисеев // Информационные технологии и информационная безопасность в науке, технике и образовании "ИНФОТЕХ - 2017" : сборник статей Всероссийской научно-технической конференции (Севастополь, 18–20 сентября 2017). – Севастополь : Севастопольский государственный университет, 2017. – С. 78–80.

10. Мера Кульбака в задачах динамической кластеризации наблюдений состояния окружающей среды / А.В. Скатков, А.А. Брюховецкий, Д.В. Моисеев, Ю.Е. Шишкин // Системы контроля окружающей среды. – 2019. – № 3 (37). – С. 35–38.

11. Скатков, А. В. Мониторинг структурно-неоднородных объектов в облачных вычислительных средах / А.В. Скатков, А.А. Брюховецкий, Д.В. Моисеев // Экологическая, промышленная и энергетическая безопасность - 2017 : сборник статей по материалам научно-практической конференции с международным участием (Севастополь, 11–15 сентября 2017) / Под редакцией Ю.А. Омельчук, Н.В. Ляминой, Г.В. Кучерик. – Севастополь : Севастопольский государственный университет, 2017. – С. 1236–1238.

12. Адаптивный метод обнаружения уязвимостей интерфейсов беспилотных транспортных средств в инфраструктуре умного города / А.В. Скатков, А.А. Брюховецкий, Д.В. Моисеев, В.И. Шевченко // Инфокоммуникационные технологии. – 2020. – Т. 18, № 1. – С. 45–50.