УДК 004.56 DOI: 10.33075/2220-5861-2022-3-84-96

КОЛЛАБОРАЦИОННЫЕ СТРАТЕГИИ ОБНАРУЖЕНИЯ УЯЗВИМОСТЕЙ ИНТЕРФЕЙСОВ ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫХ СЕТЕЙ ПТС ПРИ ТЕХНОЛОГИЯХ 5G

А.В. Скатков, А.А. Брюховецкий

ФГАОУ ВО «Севастопольский государственный университет»,
РФ, г. Севастополь, ул. Университетская, 33
E-mail: a.alexir@mail.ru

Рассматривается стратегия обнаружения уязвимостей интерфейсов информационно-измерительных сетей, базирующаяся на децентрализованных дисциплинах обслуживания тестированием состояний природно-технических объектов (ПТО) и систем (ПТС). Развиваются методы динамического обнаружения аномалий в информационных потоках данных в интеллектуальных сетях с учетом особенностей технологий 5G. Повышается достоверность принимаемых решений в условиях стохастической высокодинамичной среды, характеризующейся быстро изменяющейся топологией сети, ее мобильностью, пространственной плотностью, локализацией узлов. Разработана модель, формирующая виртуальные коллаборации узлов сети и позволяющая перейти от обработки переменной структуры топологии сети к квазипостоянной.
Ключевые слова: децентрализованная обработка, коллаборации узлов, графовая модель, покрытие множеств, принятие решений, обнаружение уязвимостей

Поступила в редакцию: 08.08.2022. После доработки: 29.08.2022.

Введение. Технология 5G становится перспективной в мобильных сетях беспроводной связи. Концепция 5G включает [1, 2]:

- eMBB (расширенная мобильная широкополосная связь);
- uRLLC (сверхнадежная связь с малой задержкой);
- mMTC (массовая связь машинного типа).

Важный принцип беспроводной сети связи заключается в использовании диапазона высоких частот mmwave до 300 ГГц и плотности подключения устройств, превышающей 10^6/км^2. Поэтому, принимая во внимание гетерогенный характер технологий, необходимы передовые исследования в отношении различных особенностей связи. Мобильные граничные вычисления рассматриваются как одна из современных парадигм, позволяющих решить проблему вычислений высокой сложности и значительно снизить задержку передаваемых сигналов.

Для выполнения мер безопасности требуются передовые решения, обеспечивающие конфиденциальность, аутентификацию, целостность и доступность [3]. Поэтому точность этих параметров должна быть соблюдена. При этом время, затрачиваемое на обнаружение неправильного состояния устройства в сети, должно быть меньше времени передачи данных [4].

Одной из ключевых задач остается обеспечение безопасности интерфейсов при взаимодействии устройств, подключенных по гетерогенным технологиям к интеллектуальным мобильным сетям (рис. 1) [5].

Транспортные одноранговые сети представляют собой особые типы сетей с высокой степенью мобильности узлов. Эти сети поддерживают различные сервисы, такие как доступ к интернету, интеллектуальные мобильные системы, приложения для потокового онлайн-видео.

Согласно требованиям стандартов 3GPP, все решения для обеспечения безопасности, связанные с V2I и V2V, должны быть сосредоточены на трех основных элементах: конфиденциальности, целостности и доступности. В табл. 1 приводятся основные типы атак на инфраструктуру с указанием скомпрометированного элемента безопасности и эффекта от воздействия атак [6, 7].

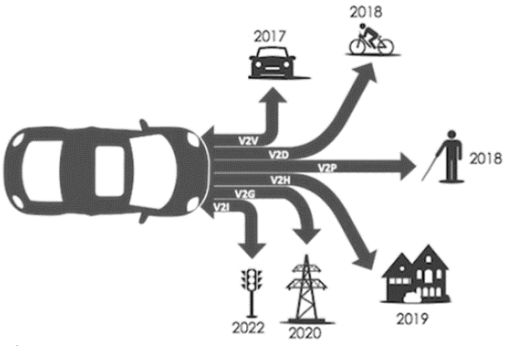

Рис. 1. Взаимодействие устройств в сетях 5G: устройство-устройство, устройство – инфраструктура, устройство – пешеход, устройство – электросеть, устройство – устройство
Fig. 1. Interaction of devices in 5G networks: vehicle-to-vehicle, (V2V), vehicle-to-infrastructure (V2I), vehicle-to-pedestrian (V2P), vehicle-to-grid (V2G), vehicle-to-device (V2D)

Таблица 1. Анализ основных типов атак на инфраструктуру V2I

Тип атаки	Скомпрометированный элемент безопасности			Эффект от атаки
	Доступность	Целостность	Конфиденциальность	
DDoS	Высокая	Умеренная	Низкая	Недоступность сервиса, крах сети, нарушение целостности сервиса
Атака с подменой	Низкая	Умеренная	Высокая	Нарушение работы сети, сокрытие личных данных и получение привилегий являются основными мотивами злоумышленника
Дублирование блоков сообщений	Умеренная	Высокая	Умеренная	Влияет на целостность и конфденциальность среды V2I, тем самым влияя на службу безопасности, предоставляемую RSU
Вредоносные программы и спам	Умеренная	Низкая	Высокая	Вредоносное ПО может привести к потенциальным серьезным сбоям в обслуживании RSU. Воздействие считается высоким из-за его длительных отключений. Вредоносное ПО может быть внедрено в систему во время обновления программного обеспечения RSU
Подслушивание	Низкая	Низкая	Высокая	Целью подслушивания является кража конфиденциальной и личной информацию, которая хранится в браузере

Сети транспортных средств очень динамичны и не имеют централизованного управления. Как следствие, обмен информацией между средствами не всегда надежен, учитывая гетерогенный характер технологий применяемых в сетях 5G. В настоящее время работы для обеспечения безопасности развиваются по следующим основным направлениям: реальные исследования на действующей инфраструктуре, аналитическое и имитационное моделирование [8, 9]. Как правило, на практике в подавляющем большинстве случаев используются имитационные модели, применение которых позволяет исследовать механизмы осуществления атак в различных сцена-

риях с применением гибких методов структурно-параметрической настройки.

В работах [10, 11] приводятся характеристики потоков связи мобильных средств. В табл. 2 представлены некоторые основные характеристики средств, которые доступны в интеллектуальных мобильных сетях 5G.

Таблица 2. Доступные характеристики мобильных средств

Обозначение	Описание
ID_v	Идентификатор средства
$Li(x,y)$	Местоположение -го средства с долготой x и широтой y
$Lrsu(x,y)$	Местоположение RSU с долготой x и широтой y
Si	Результирующая скорость -го средства
Ri	Дальность связи -го средства
$Rrsu$	Дальность связи RSU
$Ti,start$	Время, когда -е средство попадает в зону действия RSU
Ti,end	Время, когда -е средство покидает зону действия RSU
ei,j	Соседние отношения между -ым и j-ым средством
$Nrsu$	Количество средств в пределах диапазона связи RSU
$DRRi$	Скорость приема данных i-ым средством
PDR	Коэффициент отбрасывания пакетов
PSR	Коэффициент отправки пакетов
MDR	Коэффициент дублирования сообщений
$RSRP$	Мощность принятого сигнала
$RSRQ$	Качество принятого сигнала
$RSINR$	Отношение сигнал/шум
$THPut$	Пропускная способность
RSU_id	Указывает (анонимизированный) идентификатор RSU

Как показывают результаты исследований по обеспечению безопасности узлов в мобильных сетях 5G, создание универсальной модели обнаружения уязвимостей интерфейсов транспортных средств сопряжено с неразрешимыми проблемами.

Разработка универсальных подходов повышения достоверности о поведении мобильных средств должна быть направлена на снижение неопределенности внешней среды, учитывая:

- противоречивую функциональность устройств в условиях постоянно меняющейся топологии сети,
- распределенный характер транспортных средств,
- постоянное взаимодействие устройств друг с другом и другое.

В связи с этим разработка моделей на основе технологий 5G, обеспечивающих надежность и быстродействие механизма совместной работы устройств в условиях стохастической внешней среды, в значительной мере определяют достоверность оценок и эффективность принятия решений при обнаружении уязвимостей интерфейсов устройств в интеллектуальных мобильных сетях.

Описание структурно-функциональных элементов и их информационного взаимодействия в сети. Считается, что техническое средство (ТС) в предлагаемой модели является интеллектуальным устройством. Предполагается, что каждое средство имеет:

- уникальный зарегистрированный идентификатор (например, электронный номерной знак или электронный номер шасси, выданный производителем ТС),
- навигационную систему на основе глобальной системы позиционирования (GPS/ГЛОНАСС), чтобы знать информацию о его мобильности и географическом местоположении,
- локальные часы, которые синхронизированы с GPS.

На рис. 2 показана архитектура сети, состоящая из трех основных уровней: уровня датчиков, уровня базовых станций и облака. Подключенные средства могут взаимодействовать с внутренней (т.е. V2S (vehicle-to-sensor)) и внешней средами, такими как V2V и V2I, включая придорожные устройства – базовые станции (RSU), которые используют выделенную связь ближнего действия (DSRC).

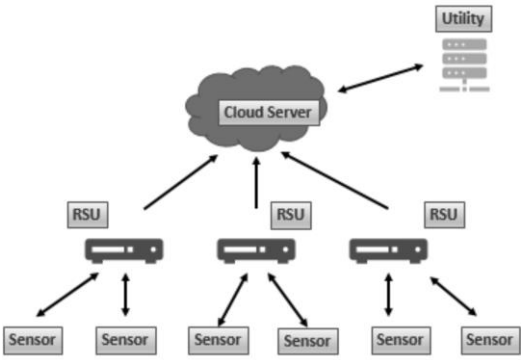

Рис. 2. Информационное взаимодействие структурно-функциональных элементов в сети
Fig. 2. Information interaction of structural and functional elements in the network

Бортовой блок, размещенный внутри транспортного средства, передает информацию в окружающую среду. RSU собирают данные с транспортных средств, а приложения, установленные в RSU, предоставляют запрошенную услугу. Вместе сеть датчиков обеспечивает мониторинг сети в режиме реального времени.

RSU – это устройства размещенные на границе сети по всей магистрали, которые способны собирать и передавать данные с множества датчиков к централизованно расположенной облачной системе маршрутизации.

Централизованное облако – доступная облачная сеть, обеспечивающая дополнительные возможности обработки при обнаружении уязвимостей на уровне датчиков. Определение уровня зоны выполняется на уровне RSU, в то время как более дорогостоящее с точки зрения вычислений уровня датчиков выполняется в облаке.

Предлагаемая модель включает в себя следующие основные компоненты:

- Обычный узел (TCn): узлы, которые взаимодействуют с другими узлами для обмена информацией в пределах диапазона связи друг с другом. Эти узлы образуют виртуальные группы. Каждый узел содержит идентификатор узла координатора, которому пересылается информация о текущем состоянии узла за период времени Δt. Транспортные средства-участники TCn, которые взаимодействуют друг с другом, отвечают за вычисление прямых значений приоритетов других участников.
- Узел координатор (KCh): узел с высоким приоритетом назначается в качестве узла координатора виртуальной группы в пределах диапазона связи с каждым TCn. Он отслеживает деятельность TCn и пересылает измеренные значения свойств TCn базовой станции (RSU). Кроме того, KCh отвечает за вычисление агрегированных значений приоритета и пересылку информации о потоке трафика достижимых узлов TCn в RSU.
- Базовая станция (RSU): принимает данные от координаторов, выполняет их обработку: формирует матрицу смежности, строит безызбыточные покрытия, формирует минимальные покрытия на основе количественной оценки (число связей), формирует коллаборации узлов с учетом веса каждого свойства узла – репутация узла, которая оценивается качественными значениями характеристик узлов, вычисляет оценки свойств с целью выявления случаев аномального поведения отдельных узлов и принятия обоснованного решения. В случае большой загрузки RSU передают данные с множества датчиков к централизованно расположенной облачной системе. Чтобы свести к минимуму задержки в сети, RSU располагают как можно ближе к датчикам устройств, и поскольку RSU являются маломощными устройствами, ограничивается максимальное количество датчиков, подключенных к одному RSU.

Положение и характеристики транспортного средства *TCi* фиксируются в каждый квант времени Δt. В предлагаемой модели средства *TCi* и *TCj* взаимодействует между собой и соседними RSU тогда и только тогда, когда они находятся в диапазонах связи друг с другом, т.е. RSU отвечает за прием сообщений маяка от соседних транспортных средств и делится этими сообщениями с соседними RSU. Формат сообщения маяка включает в себя идентификатор средства и содержит важные для контроля значения состояний некоторых характеристик узлов, перечисленных в табл. 2.

Кроме того, в каждый квант времени Δt базовая станция назначает приоритет *R* узлам, оценка которых определяется репутацией средства. Приоритет может назначаться в зависимости от числа и надежности связей, установленных в данный момент времени каждым *TC*. Поэтому в общем случае в зависимости от ситуации на дороге будет назначено множество узлов координаторов *KCi*, обладающих высоким приоритетом. Каждый такой узел *KCi* будет взаимодействовать с роем узлов *TCj*, с которыми установлена надежная связь и которые будут пересылать собранные данные узлу *KCi*. Именно узлы координаторы *KCi* вычисляют агрегированные значения приоритетов и передают полученную информацию со «своих» узлов *TCj* базовой станции.

Затем *RSU* обрабатывает информацию поступившую от транспортных средств в течение выделенного кванта времени Δt. *RSU* формирует выборки значений характеристик *TCj*, строит минимальные покрытия *C* и находит множества коллабораций C^K, обеспечивающих высокую достоверность оценок контролируемых характеристик. Далее вычисляются оценки достоверности поведения узлов в сети. Вычисленные оценки на временном интервале Δt сравниваются с оценками на интервале $\Delta(t\text{-}1)$. При обнаружении расхождений фиксируется уровень достоверности аномального поведения узлов. Базовая станция, в случае критической оценки узлов, принимает решение по ограничению их функционирования. В результате к следующему кванту времени $\Delta(t+1)$ формируются новые виртуальные группы, обновляется информация о приоритетах узлов, назначаются узлы *KC* с высоким приоритетом.

Постановка задачи формирования коллабораций. Цель – разработка модели кластерной виртуальной архитектуры топологии сети, ориентированной на децентрализованную обработку характеристик датчиков устройств в режиме реального времени и обеспечивающей достоверность принятия решений по обнаружению уязвимостей интерфейсов *TC*. Предлагаемая модель учитывает высокую мобильность узлов и изменения топологии сети. Модель разрабатывается на основе понятия коллаборации – совместного взаимодействия множества узлов, обеспечивающих достоверность оценок о их состояниях. Формирование коллаборации C^K и выбор координатора коллаборации *KC* основаны на уровне доверия транспортного средства, дальности передачи пакетов, низкой задержки и других. При формировании кластеров каждое средство отслеживает своих соседей в диапазонах связей и присваивает ему уровень доверия, которые агрегируются узлом координатором *KC*. При обнаружении подозрительного узла средство мониторинга *TC* пересылает идентификатор этого узла координатору *KC* для принятия решения – является ли этот подозреваемый узел вредоносным или нет. В коллаборации включаются узлы, которые имеют апробированные маршруты, устойчивую надежную связь с пунктом диспетчеризации, избыточные вычислительные ресурсы и др.

Для обеспечения качества функционирования системы обнаружения уязвимостей (СОУ) необходимо решить оптимизационную задачу максимизации значения выражения (1) при выборе коллаборационной стратегии обнаружения уязвимостей интерфейсов ПТС, направленной на формирование квазипостоянной топологии сети

$$Q(t_k, st_k, ks_k(kk_k, dk_k, dd_k, e_k), f_k, v_k, r_k, w_k, I_k, \xi) \rightarrow \max, \quad (1)$$

где Q – показатель качества функционирования СОУ, который определяется структурными решениями st_k и рядом следующих параметров:
t_k – терминальное операционное время,
ks_k (kk_k ,dk_k, dd_k, e_k) – коллаборационная стратегия обнаружения уязвимостей,
kk_k – характеристическое отношение,
dk_k – правила формирования коллабораций,
dd_k – агрегированные правила оценки достоверности по обнаружению уязвимостей,
e_k – тип тестирования,
f_k – частота тестирования,
v_k – полнота тестирования,
r_k – коэффициент относительности используемого процессорного времени,
w_k – объем резервного ресурса,
I_k – апостериорная информация, поступающая от СОУ,
ξ – помехи, неконтролируемые воздействия и т.п.

Решение задачи необходимо найти в области ее допустимых решений:

$$kk_k \in KK, dk_k \in DK, dd_k \in DD, e_k \in E,$$
$$st_k \in ST, f_k \in F, v_k \in V, r_k \in R, w_k \in W.$$

Сеть мобильных средств представляется в виде ориентированного двудольного графа $G = (TC,E,R,W, T)$, с единичной длиной пути достижимости (рис. 3), где $TC(t)$ – множество вершин – мобильных средств в сети в момент времени t.
$E(t) = \{e(i,j)\}$ множество дуг – связей между вершинами,
$R(t)$ – ранг вершины (число связей),
$W(t)$ – множество весов, приписанных дугам графа, $w(i,j)$ – вес дуги $e(i,j)$ обозначает взвешенный приоритет связи, которая обеспечивает достоверность характеристик узлов.
$TC=\{X,Y\}$, X – множество узлов координаторов, Y – множество обычных узлов (рис. 3).
$M(X,Y,R)$ – матрица смежности,
где X – множество строк, i=1,m;
Y – множество столбцов, j=1,n;

Элемент матрицы $(i, j) \in \{0;1\}$, «1» – означает, что узел Xi находится в диапазоне связи с узлом Yj.

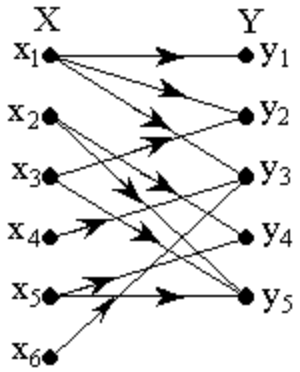

Рис. 3. Связи узлов КС с ТС
Fig. 3. Connections of CS nodes with TS

Ri – ранг вершины Xi – число связей с Yj, $Ri = |e(i,j)|$,
R^w_i – взвешенный ранг вершины Xi , $R^w_i = \sum_{j=1}^{n} w(i,j)$,
C – множество минимальных покрытий $C = \{C_1, C_2, \ldots C_r\}$,
C^K – множества коллабораций $\{C^K_1$, $C^K_2 \ldots C^K_r\}$,
V_{jl} – расчетная статистика (множество l-типов выборок контролируемых характеристик $\{V_1,V_2,\ldots V_l\}$ TCj, $V_{jl}=\{v_{jl1},v_{jl2}\ldots v_{jlk}\}$ – элементы j-го узла l-го типа выборки),
KR_{lt} – критическое значение для l-ой статистики, принятые в момент времени t,
COMP (V_{jl}, KR_{lt}) => σ_{lt} – бинарный сигнал (булевский) на выходе модуля сравнения, реализующего оператор управления для l-го критерия непараметрической статистики,
D_{Ci} – уровень доверия к множеству $C^K i$.

*Алгоритмы формирования коллабораций узлов.*Задача покрытия относится к классу оптимизационных комбинаторных задач. Она сводится к задаче поиска в некотором конечном множестве определённых подмножеств с заданными свойствами. В контексте разработки предлагаемой модели речь идет о фор-

мировании множества узлов координаторов, каждый из которых имеет надежную связь с другими узлами сети и обеспечивает достоверность оценок заданных характеристик узлов. Требуется построить множество покрытий *C* минимальной мощности, обеспечивающие качественные оценки характеристик ТС в пределах устойчивого диапазона связи.

Задача о покрытии относится к классу NP-сложных [10]. Ее решение в реальном времени, требующее полного перебора, для большинства практических задач неприемлемо из-за большой размерности решаемой задачи (2^m), ограниченного времени и недостаточности ресурсов. Поэтому предлагается снижать вычислительную сложность решения задачи за счет перераспределения процессов обработки данных.

Алгоритм содержит следующую последовательность действий:

1. Этап 1. Построение минимальных (по числу элементов множеств) покрытий *C* графа (невзвешенный случай – без учета весов дуг, учитываются только ранги Ri – число связей $|e(i,j)|$ между узлом *Xi* с узлами *Yj*).

1.1 Генерация графа $G(TC, E, R,W)$ на основе заданного множества вершин TC, $R \in [1;|e|]$,

1.1.1 Генерация для каждой TCi значения *Ri*,

1.1.2 Генерация связей $e(i, j)$.

1.2 Формирование матрицы смежности $M(X,Y,R)$.

1.3 Построение множества безызбыточных покрытий *C*.

1.4 Построение множества минимальных (по числу элементов подмножеств) покрытий *Ci* графа.

2. Этап 2. Формирование коллабораций C^K (взвешенный случай). Среди минимальных подмножеств выбирается подмножество с учетом оценок весов $w(i,j)$, полученных по заданным свойствам *TC*.

2.1 Агрегирование значений обработки характеристик *TCj* на уровне узлов.

2.1.1 Формирование *l*-ой расчетной статистики характеристик V_{jl} для каждого *TCj*.

2.1.2 Сравнение с критическими значениями $COMP(KR_{lt}, V_{jl})$.

2.1.3 Оценка рангов $R^w_{Ci,v}$ элементов множеств *Ci*.

2.2 Формирование структуры для оценки уровня доверия D_{Ci}.

2.3 Выбор коллабораций $C^K i$ для которых D_{Ci} =max.

2.4 Назначение узлов координаторов *KC*.

3. Этап 3. Интеграция оценок на уровне RSU для окончательного принятия решения о подозрительном поведении узлов.

Задача о покрытии формулируется как описано ниже [12]. Экземпляр (X,F) задачи о покрытии множества состоит из конечного множества *X* и такого семейства *F* подмножеств множества *X*, что каждый элемент множества *X* принадлежит хотя бы одному подмножеству из семейства *F*:

$$X = \mathrm{U}_{S \in F} S.$$

Подмножество $S \in F$ покрывает содержащиеся в нем элементы. Задача состоит в том, чтобы найти подмножество $C \subseteq F$ минимального размера, члены которого покрывают все множество *X*:

$$X = \mathrm{U}_{S \in C} S. \qquad (2)$$

Считается, что любое семейство *C*, удовлетворяющее уравнению (2), покрывает множество *X*. Размер семейства *C* определяется как количество содержащихся в нем подмножеств.

Алгоритм покрытия (X, F)

1 $U \leftarrow X$

2 $C \leftarrow \emptyset$

3 while U _= ∅

4 do выбирается подмножество $S \in F$, максимизирующее величину $|S \cap U|$

5 $U \leftarrow U - S$

6 $C \leftarrow C \cup \{S\}$

7 return *C*

Опишем принцип действия алгоритма. На каждом этапе его работы множество *U* содержит оставшиеся непокрытыми элементы. Множество *C* содержит покрытие, которое конструируется.

Строка 4 – это этап принятия решения в жадном методе.

Выбирается подмножество *S*, покрывающее максимально возможное количество еще непокрытых элементов. После выбора подмножества *S* его элементы удаляются из множества *U*, а подмножество *S* помещается в семейство *C*. Когда алгоритм завершает свою работу, множество *C* будет содержать подсемейство семейства *F*, покрывающее множество *X*.

Припишем строкам безызбыточной матрицы булевы переменные $s_1,\ldots,s_m$. Обозначим через *S* произвольное подмножество строк и положим $s_i = 1$, если и только если *i*-я строка принадлежит множеству *S*, то есть будем задавать подмножество *S* строк матрицы набором σ значений переменных $s_1,\ldots, s_m$ [12].

В соответствии с определением булевой функции $p(s_1,\ldots, s_m)$, принимающей значение единицы на тех и только тех наборах σ, которые задают покрытия матрицы, назовем функцией покрытия матрицы.

Тогда функция покрытия матрицы с *k* столбцами задается конъюнкцией вида

$D_1 \ldots D_k$, где D_j – дизъюнкция всех переменных, приписанных строкам с единицей в *j*-м столбце. Будем называть полученную формулу *конъюнктивной нормальной формой* (*КНФ*) функции покрытия:

$$КНФ_p = p(s_1, \ldots, s_m) = D_1 \wedge D_2 \ldots \wedge D_k. \quad (3)$$

Так как каждый элемент дизъюнкции D_j задает безызбыточное покрытие *j*-го столбца, то, перемножив дизъюнкции D_i и D_j, мы получим все безызбыточные покрытия столбцов *i* и *j* (но не только безызбыточные).

Обобщая приведенные рассуждения на все столбцы булевой матрицы, приходим к выводу, что для построения всех безызбыточных покрытий матрицы надо перемножать все дизъюнкции *КНФ* функции покрытия, выполняя при этом все возможные поглощения. В результате будет получена *ДНФ*, конъюнкции которой зададут все безызбыточные покрытия

$$ДНФ = C_1 \vee C_2 \ldots C_u. \quad (4)$$

Из полученного множества покрытий выбираются покрытия минимальной длины:

$$C = \{C_1, C_2, \ldots C_r\}.$$

На втором этапе алгоритма на основе вычисленных значений характеристик *Vj* каждому ребру графа приписываются оценки R^w по каждому контролируемому свойству, например: скорость приема данных, коэффициент отбрасывания пакетов, мощность принятого сигнала, качество принятого сигнала, пропускная способность и другие. В результате формируется структура матрицы (табл. 3) для оценки и выбора множества *Ci* с максимальным значением уровнем доверия $D_{Ci} = \max$.

Таблица 3. Структура минимальных множеств и контролируемых свойств узлов сети

	$\boldsymbol{C_1}$	$\boldsymbol{C_2}$		$\boldsymbol{C_r}$
$\boldsymbol{V_1}$	R^w_{11}	R^w_{12}	…..	R^w_{1r}
$\boldsymbol{V_2}$	R^w_{21}	R^w_{22}	…..	R^w_{2r}
….	…..	…..	…..	…..
….	…..	…..	…..	…..
$\boldsymbol{V_l}$	R^w_{1l}	R^w_{2l}	…..	R^w_{lr}
$\boldsymbol{D_{Ci}}$	D_{C1}	D_{C2}		D_{Cr}

Предлагается использовать трехзонную систему распознавания ситуаций и принятия решений. Будем полагать, что значение уровня доверия D_{Ci} каждого подмножества $C^K i$ оценивается интегрально по заданным свойствам *Vj* с использованием шкалы, содержащей три интервала [0; *Z*1; *Z*2; 1]:

$0 \le D_{Ci} < Z1$ – низкий,
$Z1 \le D_{Ci} < Z2$ – средний,
$Z2 \le D_{Ci} < 1$ – высокий.

Тогда интегральная оценка уровня доверия D_{Ci} будет вычислена как:

$$D_{Ci} = R^{w}_{ij} / \sum_{j=1}^{l} R^{w} ij \ . \qquad (5)$$

Узлы множества Ci, для которых D_{Ci} = max , будут включены в коллаборацию $C^{K}i$ и $Xi \in C^{K}i$ будут назначены в качестве координаторов KC в следующем временном такте обработки.

Рассмотрим преимущество использования подхода на основе коллаборации узлов, которые осуществляют взаимное тестирование характеристик в виртуальной группе. Введем обозначения событий в сети: A – атака/уязвимость, R – атака/уязвимость обнаружена.

Тогда вероятности появления событий при тестировании обозначим так:

$P(A,R)$ – атака есть и она обнаружена,

$Q(A,\bar{R})$ – атака есть, но она не обнаружена,

$S(\bar{A},R)$ – атаки нет, но она обнаружена,

$T(\bar{A},\bar{R})$ – атаки нет и она не обнаружена

1) Рассмотрим появление события $P(A,R)$. Пусть p – вероятность обнаружить атаку за одно тестирование одним устройством. Проведем k тестов. Тогда вероятность обнаружить атаку на k-ом тестировании:

$$P(p,k) = p\,(1\text{-}p)^{k-1}. \qquad (6)$$

2) Случай взаимного тестирования устройств. Будем считать вероятность обнаружения каждым устройством – p. Пусть в группе из n устройств взаимное тестирование выполняют k устройств, $1 \le k \le n$. Тогда вероятность обнаружить атаку за k тестов при биномиальном распределении будет:

$$P(p,k,n) = C^{k}_{n} p^{k} (1\text{-}p)^{n-k}. \qquad (7)$$

При больших n биномиальное распределение стремится к пуассоновскому.

Сравним вероятности одиночного $P(p,k)$ и совместного $P(p,k,n)$ тестирования. На рис. 4–7 показаны зависимости изменения вероятностей обнаружения уязвимостей при различных значениях p, k, n.

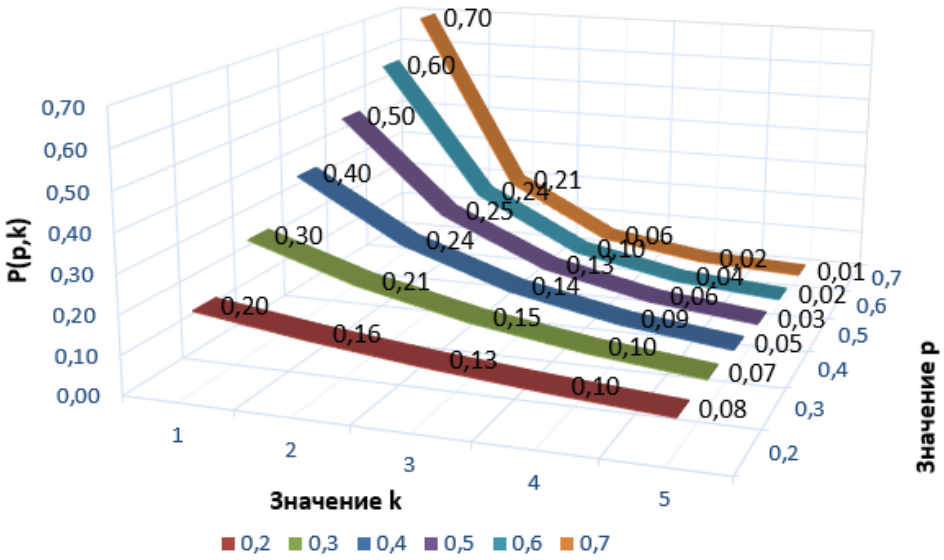

Рис. 4. Вероятность $P(p,k)$ одиночного обнаружения уязвимости на k-ом тесте
Fig. 4. Probability $P(p,k)$ of a single discovery of a vulnerability on the k-th test

При одиночном тестировании максимальная вероятность при заданном p достигается при $k = 1$. При увеличении p вероятность уменьшается. Кроме первого значения вероятности $P(p, k)$ не высокие и последующее тестирование избыточно.

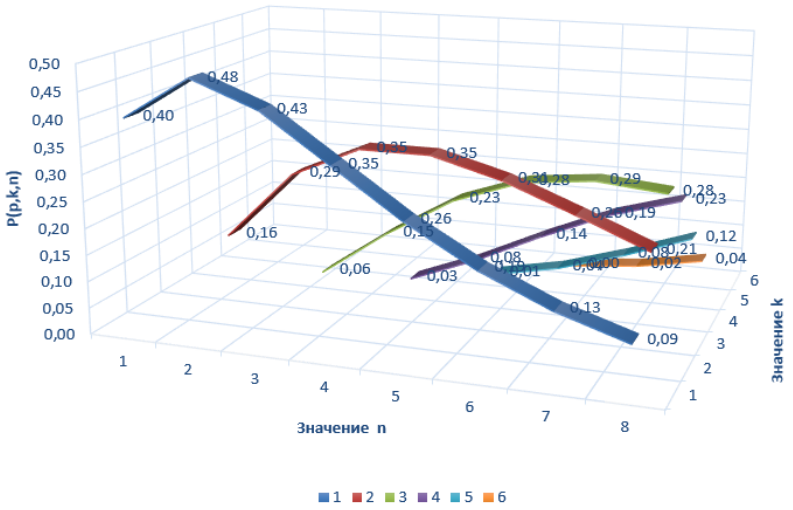

Рис. 5. Вероятность $P(p,k,n)$ совместного обнаружения уязвимости на k-ом тесте при малых значениях p (p = 0,4)
Fig. 5. Probability $P(p,k,n)$ of joint detection of a vulnerability on the k-th test for small values of p (p = 0,4)

При совместном тестировании при малых значениях p<= 0,4 наблюдается увеличение значения $P(p,k,n)$ при возрастании n и/или k. Однако затем оно снижается. Имеется экстремум, который дает максимальное значение вероятности $P_{max}(p,k,n)$.

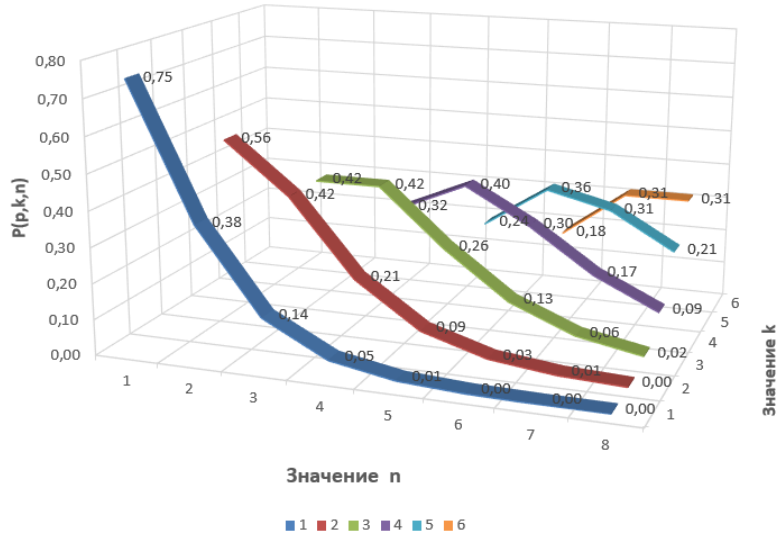

Рис. 6. Вероятность $P(p,k,n)$ совместного обнаружения уязвимости на k-ом тесте при больших значениях p (p = 0,75)
Fig. 6. Probability $P(p,k,n)$ of joint detection of a vulnerability on the k-th test for large values of p (p = 0,75)

Первичное тестирование при k=1 высокоэффективно при большом значении p=>0,75, т.к. имеем большое значение $P(p,k,n)$. При совместном тестировании при больших n обнаружение низкое и при малых и больших значениях k, т.к. обнаружение уязвимости происходит раньше.

Насколько необходимо повторное тестирование, если произошло обнару-

жение первый раз на шаге k=1, чтобы быть уверенным в достоверности оценки $P(p,k,n)$ обнаружения уязвимости? Может быть предложено следующее правило:

- Если p<= 0,4 , то повторное тестирование может быть оправдано, т.к. при увеличении n и/или k будет увеличиваться вероятность $P(p,k,n)$ до определенного значения P_{max} (p,k,n) при заданных p,k,n.
- Если p => 0,7 , то повторное тестирование нецелесообразно, т.к. значение $P(p,k,n)$ с увеличением n уменьшается.

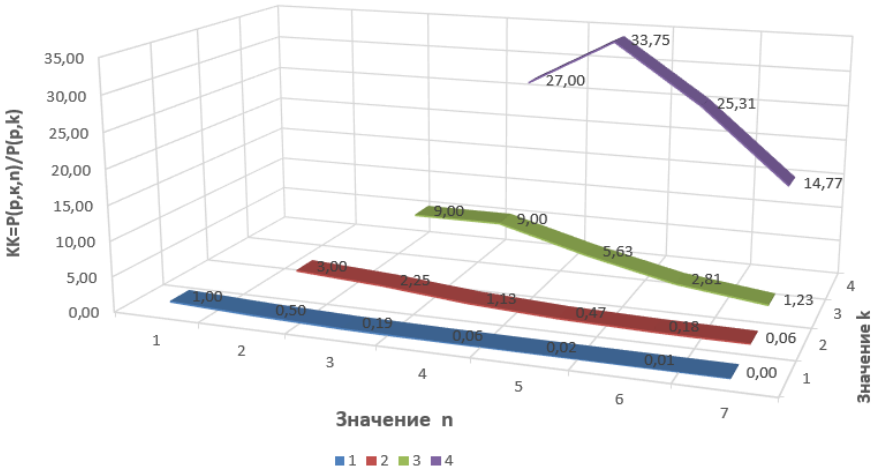

Рис. 7. Изменение величины характеристического отношения $KK=P(p,k,n)/P(p,k)$, p=0,75 в зависимости от мощности коллаборации

Fig. 7. Change in the value of the characteristic ratio $KK=P(p,k,n)/P(p,k)$, p=0,75 depending on the power of the collaboration

Исследование величины характеристического отношения $KK=P(p,k,n)/P(p,k)$ подтверждает следующее: чем больше KK, тем более оправдано использовать коллаборацию при заданных p,k,n, в случаях, когда при увеличении k и/или n KK продолжает возрастать, а значит применение подхода на основе коллабораций повышает достоверность по сравнению с одиночным тестированием. Построенный график $P(p,k,n)/P(p,k)$ позволяет определить зоны обнаружения уязвимостей для двух стратегий:

- менее эффективной, но более быстродействующей и менее затратной, когда с высокой вероятностью происходит обнаружение уязвимости на первом шаге, а на последующих шагах вероятность снижается,
- высокоэффективной, когда при последующем тестировании значение $P(p,k,n)$ увеличивается с возрастанием n и/или k – эффект коллаборации.

Таким образом, при совместном тестировании имеется возможность сформировать коллаборационную стратегию контроля, когда для заданной вероятности обнаружения задаются области необходимых значений параметров n и k, обеспечивающих высокое $P(p,k,n)$ по сравнению с $P(p,k)$.

Схема принятия решений предполагает для заданных событий P,Q,S,T определение мощности коллабораций, для которых оправдано их применение с точки зрения вероятностей обнаружения уязвимостей.

Заключение. Предложен подход, базирующийся на децентрализованной обработке при тестировании состояний природно-технических объектов интеллектуальной информационно-измерительной сети в условиях 5G. Первичные датчики измерений параметров окружающей среды в процессе эксплуатации выходят из строя из-за воздействия агрессивной среды и преднамеренных

действий. В результате встречаются систематические ошибки измерений контролируемых величин вследствии появления уязвимостей. Представленный подход в отличие от известных позволяет обнаруживать уязвимости интерфейсов устройств при совместном тестировании их свойств. Подход развивает методы динамического обнаружения аномалий в информационных потоках данных в интеллектуальных информационно-измерительных сетях. Применение предлагаемого подхода направлено на повышение достоверности принимаемых решений в условиях стохастической высокодинамичной среды, характеризующейся быстро изменяющейся топологией сети, мобильностью и плотностью узлов. Для этой цели формализована задача поиска оптимальной стратегии обнаружения уязвимостей, предложена графовая модель формирования виртуальных коллабораций узлов сети, которая позволяет перейти от обработки переменной структуры топологии сети к квазипостоянной. Приведен алгоритм формирования минимальных покрытий, проанализировано характеристическое отношение, величина которого подтверждает эффективность применения разработанного подхода на основе коллабораций по сравнению с традиционным одиночным тестированием.

Исследование выполнено при финансовой поддержке РФФИ в рамках научных проектов № 19-29-06015/20, № 19-29-06023/20.

СПИСОК ЛИТЕРАТУРЫ

1. *Jie Ji.* Service Security Issues in the 5G Core Network and How to Detect Them. https://nsfocusglobal.com/new-architecture-new-challenges-service-security-issues-in-the-5g-core-network-and-how-to-detect-them/ (дата обращения: 06.07.2022).

2. *Shafi M.* 5G: A tutorial overview of standards, trials, challenges, deployment, and practice // IEEE Journal on selected areas in communications. 2017. Vol. 35(6). P. 1201–1221.

3. *Rupprecht D., Dabrowski A., Holz T., Weippl E., Pöpper C.* On security research towards future mobile network generations // IEEE Communications Surveys & Tutorials. 2018. Vol. 20(3). P. 2518–2542.

4. *Chopra G., Jain S., Jha R.K.* Possible security attack modeling in ultradense networks using high-speed handover management // IEEE Transactions on Vehicular Technology. 2017. Vol. 67(3). P. 2178–2192.

5. *Engoulou R.G., Bellaïche M., Pierre S., Quintero A.* VANET security surveys // Computer Communications. 2014. Vol. 44. P. 1–13.

6. *Chen J.* Service-oriented dynamic connection management for software-defined internet of vehicles // IEEE Trans. Intell. Transp. Syst. 2017. Vol. 18(10). P. 2826–2837.

7. *Fatih S., Sevil S.* A Survey of Attacks and Detection Mechanisms on Intelligent Transportation Systems:VANETs and IoV // Ad Hoc Networks. 2017. № 61. P. 1570–8705.

8. *Скатков А.В.* Адаптивное обнаружение уязвимостей интерфейсов беспилотных транспортных средств / А.В. Скатков, А.А. Брюховецкий, Ю.В. Доронина и др. Симферополь: Изд-во «Ариал», 2020. 352 с.

9. *Скатков А.В., Моисеев Д.В., Брюховецкий А.А.* Структурный синтез каналов информационных обменов для беспилотных транспортных средств. Симферополь: Изд-во «Ариал», 2020. 320 с.

10. *Skanda V.* Cyberphysical risks of hacked internet-connected vehicles // Physical reviewe. July 2019. Vol. 100(1). P. 1–10. DOI:10.1103/PhysRevE.100.012316.

11. *Azam F., Yadav S.K., Priyadarshi N.* A comprehensive review of authentication schemes in vehicular ad-hoc network // IEEE Access. 2021. Vol. 9. P. 31309–31321.

12. *Новосёлов В.Г., Скатков А.В.* Прикладная математика для инженеров-системотехников. Дискретная математика в задачах и примерах: учебное пособие. Киев: УМК ВО, 1992. 200 с.

COLLABORATIVE STRATEGIES FOR DETECTING INTERFACE VULNERABILITIES OF INFORMATION AND MEASUREMENT NETWORKS OF NTS WITH 5G TECHNOLOGIES

A.V. Skatkov, A.A. Bryukhovetskiy

Federal State Educational Institution of Higher Education «Sevastopol State University»,
RF, Sevastopol, Universitetskaya St., 33

An approach to the construction of a strategy for detecting vulnerabilities of information and measurement network interfaces based on decentralized service disciplines based on mutual testing of the states of natural and technical objects (NTO) and systems (NTS) is considered. The proposed approach develops methods for dynamic detection of anomalies in information data flows in intelligent networks, taking into account the features of 5G technologies. The application of the proposed approach is aimed at increasing the reliability of decisions made in a stochastic highly dynamic environment characterized by a rapidly changing network topology, its mobility, spatial density, localization of nodes. For this purpose, a model has been developed that forms virtual collaborations of network nodes and allows moving from processing the variable structure of the network topology to a quasi-permanent one. One of the variants of the network architecture, a graph model of virtual collaborations, is presented, an algorithm for the formation of minimal coverages is given, estimates of the reliability of vulnerability detection are obtained.
Keywords: decentralized processing, node collaborations, graph model, set coverage, decision-making, vulnerability detection

REFERENCES

1. https://nsfocusglobal.com/new-architecture-new-challenges-service-security-issues-in-the-5g-core-network-and-how-to-detect-them/ (July 06, 2022)
2. *Shafi M.* 5G: A tutorial overview of standards, trials, challenges, deployment, and practice. *IEEE Journal on selected areas in communications*, 2017, Vol. 35(6), pp. 1201–1221.
3. *Rupprecht D., Dabrowski A., Holz T., Weippl E., and Pöpper C.* On security research towards future mobile network generations. *IEEE Communications Surveys & Tutorials*, 2018, Vol. 20(3), pp. 2518–2542.
4. *Chopra G., Jain S., and Jha R.K.* Possible security attack modeling in ultradense networks using high-speed handover management. *IEEE Transactions on Vehicular Technology*, 2017, Vol. 67(3), pp. 2178–2192.
5. *Engoulou R.G., Bellaïche M., Pierre S., and Quintero A.* VANET security surveys. *Computer Communications*, May 2014, Vol. 44, pp. 1–13.
6. *Chen J.* Service-oriented dynamic connection management for software-defined internet of vehicles. *IEEE Trans. Intell. Transp. Syst.*, Oct. 2017, Vol. 18(10), pp. 2826–2837.
7. *Fatih S. and Sevil S*. A Survey of Attacks and Detection Mechanisms on Intelligent Transportation Systems:VANETs and IoV. *Ad Hoc Networks*, march 2017, No. 61, pp. 1570–8705.
8. *Skatkov A.V., Bryuhoveckij A.A., Doronina Yu.V., Moiseev M.D., Skatkov I.A., and Chengar O.V.* Adaptivnoe obnaruzhenie uyazvimostej interfejsov bespilotnyh transportnyh sredstv (Adaptive vulnerability detection of unmanned vehicle interfaces). Simferopol: Arial, 2020, 352 p.
9. *Skatkov A.V., Moiseev D.V., Bryuhoveckij A.A., Doronina YU.V., Skatkov I.A., and Shevchenko V.I.* Strukturnyj sintez kanalov informacionnyh obmenov dlya bespilotnyh transportnyh sredstv (Structural synthesis of information exchange channels for unmanned vehicles). Simferopol: Arial, 2020, 320 p.
10. *Skanda V.* Cyberphysical risks of hacked internet-connected vehicles. *Physical reviewe*, July 2019, Vol. 100(1), pp. 1–10. DOI:10.1103/PhysRevE.100.012316.
11. *Azam F., Yadav S.K., and Priyadarshi N.* A comprehensive review of authentication schemes in vehicular ad-hoc network. *IEEE Access*, 2021, Vol. 9, pp. 31309–31321.
12. *Novosyolov V.G. and Skatkov A.V.* Prikladnaya matematika dlya inzhenerov-sistemotekhnikov. Diskretnaya matematika v zadachah i primerah (Applied mathematics for systems engineers. Discrete mathematics in problems and examples). Kiev: UMK VO, 1992, 200 p.