DOI 10.36622/VSTU.2023.26.1.004
УДК 004.732

ОЦЕНКА И РЕГУЛИРОВАНИЕ РИСКОВ НАРУШЕНИЯ ДОСТУПНОСТИ ИНФОРМАЦИИ ПРИ РЕАЛИЗАЦИИ АТАК НА СЕТИ ИНТЕРНЕТА ВЕЩЕЙ, ПОСТРОЕННЫЕ НА БАЗЕ ТЕХНОЛОГИИ SDN

С.А. Ермаков, И.И. Донсков, А.А. Болгов, О.Ю. Макаров, Р.Д. Бурцев

В данной статье предлагается методическое и алгоритмическое обеспечение количественной оценки рисков нарушения доступности систем Интернета вещей, построенных на базе программно-определяемых сетей (SDN). Предлагаемое обеспечение учитывает особенности построения выбранных сетей. Потенциальный ущерб складывается как из ценности защищаемых активов, так и из особенностей топологии рассматриваемой сети. Вероятность атаки определяется индивидуально для каждого типа злоумышленников, с учетом его ресурсов и мотивации. Представлена методика регулирования риска, представляющая собой механизм двойной маршрутизации с учётом рисков, основанный на эволюционном алгоритме. Предложенный алгоритм позволяет вычислить наиболее оптимальные настройки системы, обеспечивая при этом приемлемое время сходимости. Обширные результаты моделирования предложенного подхода демонстрируют повышение защищенности различных сетевых топологий без значительного ущерба производительности.

Ключевые слова: Интернет вещей, программно-определяемая сеть (SDN), риск, доступность, маршрутизация.

Введение

Концепция Интернета вещей (ИВ) уже успела прочно войти в нашу жизнь и сейчас применяется в различных сферах и отраслях человеческой деятельности: от небольших домашних сетей до внедрения ИВ в промышленность и здравоохранение. Непрерывное развитие технологии Интернета вещей приводит к масштабированию развертываемых сетей, увеличению количества устройств и данных, передаваемых и обрабатываемых в них. Но сейчас дальнейший рост производительности приложений ИВ упирается в ограниченные возможности традиционных телекоммуникационных сетей. При этом технология программно-определяемых сетей (SDN) позволяет подвести большинство статичных телекоммуникационных сетей под требования современного IT бизнеса: в первую очередь это высокая масштабируемость и эффективное централизованное управление [1].

Отсутствие общепринятых мер защиты SDN-сетей от разного рода атак делает такие сети приоритетной целью для злоумышленников. Наиболее актуальными атаками являются атаки, направленные на нарушение доступности [2]. Им может быть подвержен и уровень управления, и уровень данных, а атака на один из множества коммутаторов может вывести из строя всю сеть [3].

Применение сетей, построенных на базе технологии SDN, при проектировании систем интернета вещей открывает новые возможности для регулирования риска атак, направленных на нарушения их доступности. Программно-определяемые сети благодаря централизованному управлению при помощи SDN-контроллера и протоколу управления потоками способны оперативно реагировать на изменения конфигурации и топологии сети и применять установленные меры повышения защищенности в режиме реального времени. При этом, используемый подход к оценке и регулированию рисков должен учитывать все особенности защищаемой сети [4].

Традиционные подходы оценки риска атак нарушения доступности плохо подходят таким сетям, так как не берут во внимание ключевые особенности их построения: динамически изменяющуюся структуру сети, корреляцию между узлами и собираемую

контроллером информацию о сети [5]. В уже существующих методиках оценки риска нарушения доступности SDN-сетей авторы делают акцент на обобщенной оценке риска [6-7]. В данной работе предлагаются методы количественной оценки и регулирования риска нарушения доступности различных компонентов SDN-сетей.

Оценка риска угроз нарушения доступности

Оценка риска складывается из оценки величины воздействия реализующийся угрозы и вероятности её реализации. При оценке величины воздействия атак нарушения доступности на сети SDN учитывается ценность защищаемого актива, а также важность узла относительно сети. Показателем важности узла выступает центральность ($B(n_i)$), выраженная следующей формулой:

$$B(n_i) = \sum_{k,;\in N, k \neq l} \frac{b_{k,l}(n_i)}{b_{k,l}}, n_i \in N,$$

где $b_{k,l}(n_i)$ – число кратчайших путей между *k* и *l*, проходящих через узел n_i;

$b_{k,l}$ – общее число кратчайших путей между *k* и *l*.

Помимо центральности необходимо учесть степень узла, ведь если у узла более высокий уровень взаимодействия с другими элементами сети, значит он предоставляет больше услуг, и, следовательно, оказывает еще большее влияние на сеть в случае нарушения его доступности. Связь между центральностью и степенью узла выражается в виде несмещенной центральности:

$$\chi(n_i) = \frac{B(n_i)}{\delta_{n_i}}, \quad (1)$$

где $B(n_i)$ – центральность узла,

δ_{n_i} – степень узла.

Учитывая ценность актива (A_i), количественная значимость узла (I_{n_i}) выражается по формуле, приведенной ниже. Для нормализации значений ценности актива и несмещенной центральности используются весовые коэффициенты α и β. Присвоение веса позволяет различать важность каждой составляющей общей значимости.

$$I_{n_i} = \alpha \times \chi(n_i) + \beta \times A_i, \quad (2)$$

где α и β – весовые коэффициенты,

$\chi(n_i)$ – несмещенная центральность узла, вычисляемая по формуле (1),

A_i – ценность актива.

Определение стоимости активов производится путем экспертной оценки с дальнейшим нормированием полученных значений.

Вероятность атаки ($P(Atk_t)$) рассчитывается отдельно для каждого типа злоумышленников, принимая в расчёт взаимосвязь между ресурсами злоумышленника (бюджетом, навыками, невозможностью обнаружения и мотивацией) и вероятностью проведения им атаки. Эта зависимость выражается в виде следующей формулы путем перемножения соответствующих коэффициентов:

$$P(Atk_t) = K_B \times K_C \times K_U \times K_M \times \frac{CVSS}{10},$$

где K_B – коэффициент стоимости;

Kc – коэффициент сложности;

K_U – коэффициент необнаружаемости;

K_M - коэффициент мотивации;

$CVSS$ – оценка уязвимости.

Данные коэффициенты могут принимать значения от 0 до 1 и вычисляются путем оценки различных типов злоумышленников исходя из информации в открытых источниках.

Для проведения атак нарушения доступности наличие уязвимостей в системе не обязательно. В таких случаях $\frac{CVSS}{10}$ принимает значение равное 1.

Риск элемента ($Risk(n_i)$) для угроз нарушения доступности представляет собой произведение общей значимости узла и вероятности атаки со стороны злоумышленника и выражается формулой:

$$Risk(n_i) = I_{n_i} \times P(n_i), \forall n_i \in N,$$

где I_{n_i} – общая значимость узла, вычисляемая по формуле (2),

$P(n_i)$ – вероятность атаки со стороны злоумышленника.

Результирующим значением риска для некоторой подсистемы является среднее значение риска, рассчитанное для соответствующих узлов.

Регулирование рисков атак нарушения доступности

Сложность проектировании системы защиты для любой информационной системы (ИС) заключается в достижении этой ИС состояния максимальной эффективности, то есть в подборе наиболее оптимальных параметров производительности системы и возможного ущерба, в случае реализации атак на её узлы.

В качестве параметра, отражающего вероятность возможного ущерба, нанесенного системе, выступает медианное значение риска сети ($Risk_{Me}$). За параметр производительности системы выбирается величина сквозной задержки. Для большинства сетей Интернета вещей учет и минимизация задержки является важной задачей, так как большинство служб и сервисов ИВ чувствительны к увеличению задержки. Сквозная задержка ($T(Path_k)$) для рассматриваемого типа сетей складывается из задержки при обработке на контроллере (T_{Ct}), задержки в очереди на пересылку в каждом из коммутаторов (T_{Que}) и времени на передачу по физическому каналу связи каждой команды каждой из служб, и рассчитывается по следующей формуле:

$$T(Path_k) = T_{Ct} + N_{Sw} \times T_{Que} + \frac{1}{K_S \times c} \times \sum_{s_k \in S} l_{i,j} \forall n_i, n_j \in Path_S,$$

где T_{Ct} – задержки при обработке на контроллере,

N_{Sw} – количество коммутаторов,

T_{Que} – задержки в очереди на пересылку в коммутаторе,

$K_S \times c$ – скорость света в среде распространения сигнала,

$I_{i,j}$ – передаваемые по каналу связи команды,

s_k – службы.

Общая сквозная задержка для сети (T) представляет собой сумму задержек на всех возможных маршрутах ($T(Path_k)$):

$$T = \sum_{s_k \in S} T(Path_k), \forall Path_k \in P,$$

где $T(Path_k)$ – задержка на k-том маршруте.

Таким образом, задача выбора мер повышения защищенности системы заключается в приведении этой системы в состояние эффективности, при котором будет найдено наиболее оптимальное соотношение величин риска и сквозной задержки:

$$f(\overline{p(k)}) = \left[\min(T(\overline{p(k)})), \min(Risk_{Me}(\overline{p(k)}))\right],$$

где $\overline{p(k)} = [p(1), p(2), \ldots, p(k)]$ – вектор из k возможных решений безопасности.

Методика регулирования рисков

Наиболее распространенными решениями для повышения защищенности сетей, построенных на базе SDN, для регулирования риска атак нарушения доступности являются методы фильтрации аномального трафика и методы внедрения более оптимальных алгоритмов маршрутизации, основанных на подсчете риска. В рамках данной работы предлагается алгоритм маршрутизации, основанный на риске.

Применяемые методы заключаются в том, чтобы заранее продумать и задать альтернативные маршруты, которые будут представлять собой оптимальное решение между производительностью и защищенностью сети и применяться в случае недоступности основного маршрута.

Сравнение основного и альтернативного маршрута показано на рис. 1.

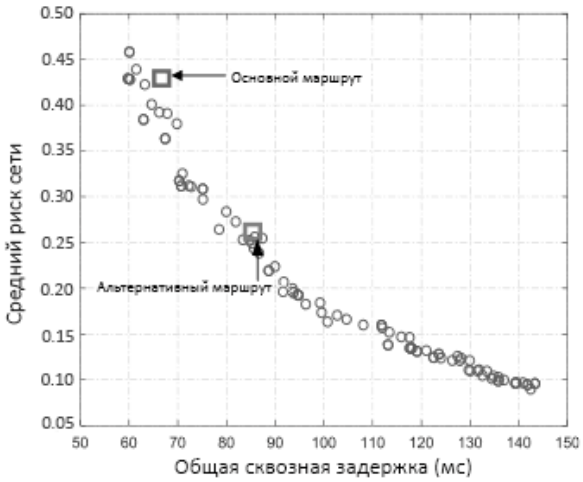

Рис. 1. Сравнение основного и альтернативного маршрутов для передачи трафика

Планирование альтернативных маршрутов сводится к задаче поиску оптимального решения исходя из выбранных параметров системы. Запуск процесса регулирования риска связан с обнаружением неисправности в системе. В первую очередь, серверы обработки данных выполняют анализ трафика и оценивают уровень качества обслуживания. Затем рассчитывается сетевой риск. Как только обнаруживается скачкообразный трафик, запускается механизм регулирования рисков, который состоит в создании сетевой модели и решении проблемы оптимизации для нее.

Чтобы получить минимальную сквозную задержку, предполагается, что все службы, как правило, используют одни и те же линки, находящиеся на кратчайших путях, поэтому часть линков будут простаивать. Следовательно, возникает необходимость в алгоритме, позволяющем производить балансировку сети.

Для поиска оптимального решения между быстродействием системы и её защищенностью используется генетический алгоритмом без доминирования. В данном случае каждая хромосома представляет собой общее решение для планирования маршрутизации нескольких служб. Каждый независимый сегмент хромосомы является маршрутом для определенной службы. Генами являются узлы в сети, а их местоположение в хромосоме указывает на превосходство. Для декодирования хромосом первым узлом в маршруте считается исходный узел для службы, а второй и каждый последующий определяется исходя из положения гена в хромосоме и матрицы смежности. Начальная популяция генерируется случайным образом. Приспособленность хромосом определяется уровнем недоминирования и мерой сходства для каждой хромосомы. Операция отбора опирается на турнирный подход, что позволяет сохранить лучшие хромосомы. При этом для рекомбинации применялась операция пересечения на основе положения.

Сортировка без доминирования позволяет разделить хромосомы на разные уровни, и выделить из них те, которые ближе к фронту Парето (наиболее оптимальные). Мера сходства отражает разнообразие популяции. Оно вычисляется в соответствии с локальными отличиями между каждой хромосомой и двумя соседними на том же уровне.

Предложенный алгоритм обеспечивает хорошую скорость сходимости и достигает заданного уровня точности уже после 100 итераций цикла (рис. 2).

Подробный алгоритм поиска оптимальных маршрутов, основанного на величине риска, показан на рис. 3 в виде блок-схемы.

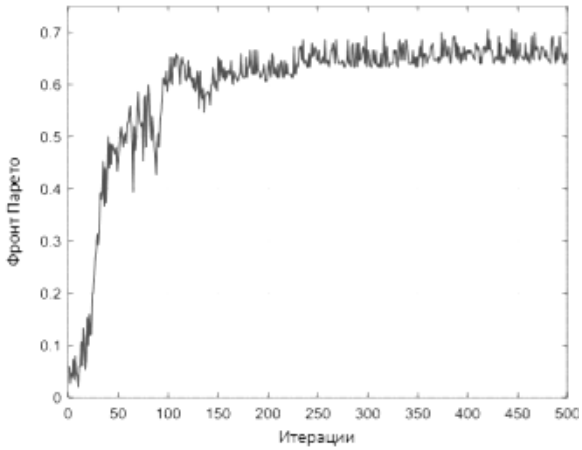

Рис. 2. Сходимость алгоритма расчёта маршрутов передачи трафика на основе оценки риска

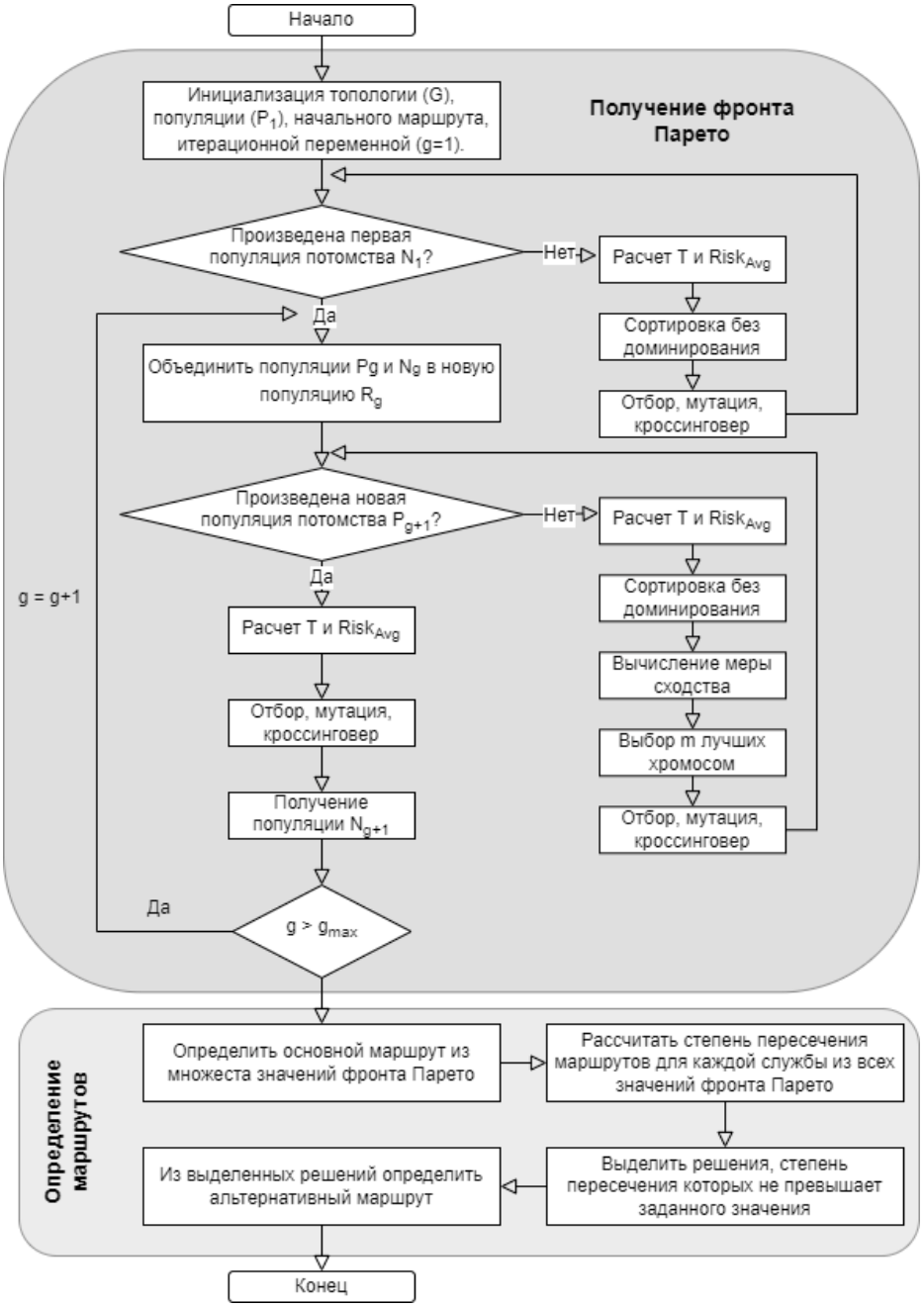

Рис. 3. Алгоритм маршрутизации трафика в сети на основе оценки риска

Оценка эффективности алгоритма маршрутизации, основанного на риске

Для экспериментальной оценки предложенного алгоритма было проведено моделирование на примере нескольких топологий, прототипами которых служат реальные сетей. Результаты предложенного алгоритма маршрутизации на основе рисков (AMOP) сравнили с обычным генетическим алгоритмом (ГА), а также с алгоритмом Дейкстры (АД) для поиска кратчайшего пути. На рис. 4 показан график отношения фронта Парето к количеству служб в сети.

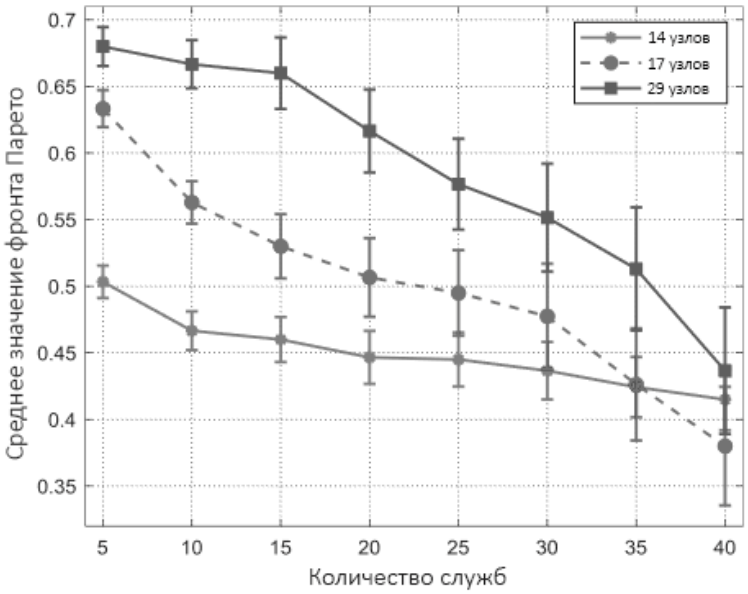

Рис. 4. Отношение среднего значения фронта Парето к количеству служб, передающих трафик в сети

Из графика (рис. 4) видно, что количество оптимальных решений во всех сетевых топологиях уменьшается с ростом количества служб. Это объясняется тем, что, когда количество сервисов небольшое, имеется больше свободных путей для организации маршрута. В то же время видно, что чем больше сеть, тем больше в ней оптимальных решений. Это связано с тем, что больший масштаб сети приводит к большему пространству для поиска решений, удовлетворяющих требованиям службы.

В предложенном алгоритме основной маршрут формируется из фронта Парето, с учетом минимальной сквозной задержки. Альтернативный маршрут представляет собой решение, учитывающее оптимальное значение между минимальной задержкой и минимальным риском. На рис. 5 (а) показаны значения среднего риска для сети при расчёте двойного маршрута с использованием различных алгоритмов. По графику видно, что алгоритм маршрутизации на основе риска позволяет снизить средний риск сети при планировании основного маршрута 20 процентов по сравнению с обычным генетическим алгоритмом, и почти вдвое по сравнению с алгоритмом Дейкстры. Для альтернативных маршрутов разница составила 19 и 72 процента соответственно. Можно заметить, что средний риск сети для основного маршрута выше чем для альтернативного у различных алгоритмов. Это связано с тем, что при расчёте основного маршрута выдвигаются требования к минимизации сквозной задержки, а для альтернативного маршрута важно снизить средний риск сети.

На рис. 5 (б) показан график изменения общей сквозной задержки для обоих маршрутов. При расчёте основного маршрута задержка при использовании алгоритма на основе рисков приближается к значению, полученному для алгоритма Дейкстры. В это же время оба значения меньше чем таковое для генетического алгоритма. При планировании альтернативного маршрута у риск-ориентированного алгоритма задержка возрастает на 32 процента из-за того, что трафик распределяется по непересекающимся путям. Однако это значение задержки все еще ниже, чем у генетического алгоритма.

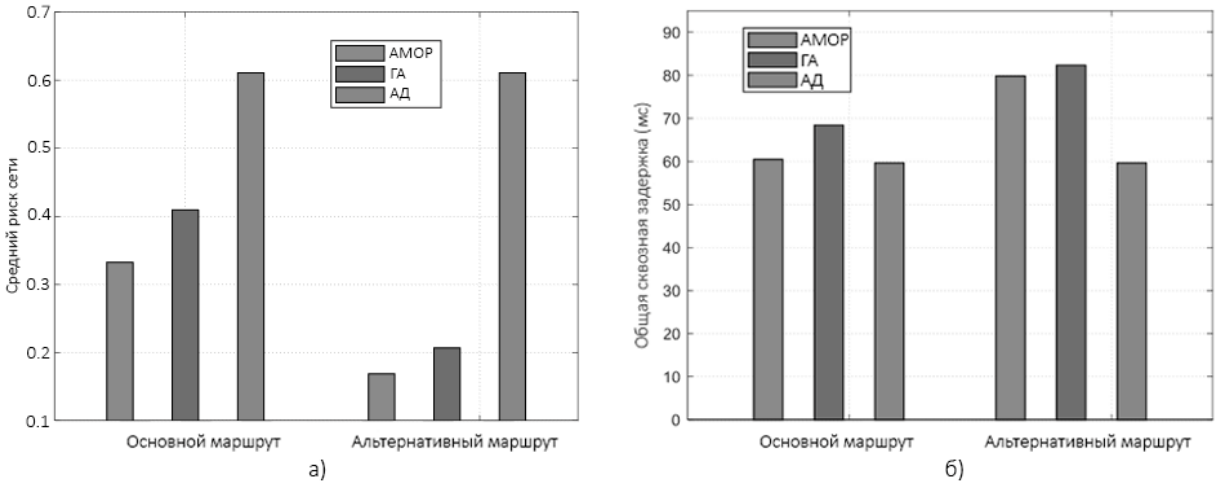

Рис. 5. Средний риск сети (а) и общая сквозная задержка при передачи трафика (б)

Заключение

Из-за особенностей построения сетей SDN в системах Интернета вещей, традиционный подход к оценке риска не позволяет получить адекватный результат. Поэтому была предложена методика, учитывающая как особенности узлов сети, так и возможности злоумышленников. Представленный подход позволяет получить наиболее точные количественные значения риска нарушения доступности систем интернета вещей, построенных на базе технологии SDN.

На основе рассчитанных значений риска был предложен метод его регулирования и алгоритм маршрутизации, основанный на риск-анализе. Результаты моделирования показали, что такой алгоритм гарантирует оптимальную сквозную задержку и снижает среднее значение риска в сети. Предложенное решение обеспечивает приемлемую скорость сходимости, что позволяет контроллеру SDN производить вычисления и менять конфигурацию сети в режиме реального времени. В дальнейшей перспективе развития проделанной работы видится разработка дополнительных мер повышения защищенности в сетях Интернета вещей, построенных на базе технологии SDN, таких как алгоритмы фильтрации трафика.

Список литературы

1. A Vision of Intelligent IoT — Trends, Characteristics and Functional Architecture. / Yuan Li, Wai Chen, Yu Ding, Yakun Qie, Chuntian Zhang, 2022, pp. 184-189.

2. A Survey: Typical Security Issues of Software-Defined Networking / Yifan Liu1, Bo Zhao, Pengyuan Zhao, Peiru Fan, Hui Liu, 2019, pp. 1-35.

3. Challenges of DDoS Attack Mitigation in IoT Devices by Software Defined Networking (SDN) / Farha Akhter Munmun, Mahuwa Paul, 2021, pp. 1-5.

4. Overview on SDN and NFV based architectures for IoT environments: challenges and solutions / Manare Zerifi, Abdellatif Ezzouhairi, Abdelhak Boulaalam, 2020, pp. 1-5.

5. Trend in SDN Architecture for DDoS Detection- A Comparative Study / Josy Elsa Varghese, Balachandra Muniyal, 2021, pp. 170-174.

6. Xinyu Zhou. A Novel Impact Analysis Approach for SDN-based Networks, 2019, pp. 10-18.

7. Laila M. Almutairi, Sachin Shetty. Generalized Stochastic Petri Net Model Based security risk assessment of software, 2017, pp. 545-550.

Концерн «Созвездие»
Concern «Sozvezdie»

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 21.01.2023

Информация об авторах

Ермаков Сергей Александрович – канд. техн. наук, Концерн «Созвездие», e-mail: mnac@comch.ru
Донсков Илья Игоревич – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru
Болгов Андрей Александрович – аспирант, Воронежский государственный технический университет, e-mail: mnac@comch.ru
Макаров Олег Юрьевич – д-р техн. наук, профессор, Воронежский государственный технический университет, e-mail: mnac@comch.ru
Бурцев Роман Дмитриевич – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

ASSESSMENT AND RISK MENAGEMENT OF INFORMATION AVAILABILITY OF SDN-BASED INTERNET OF THINGS NETWORKS

S.A. Ermakov, I.I. Donskov, A.A. Bolgov, O.Yu. Makarov, R.D. Burtsev

This article proposes methodology and algorithm for quantifying risks assessment of availability breaches of SDN-based Internet of things systems. The proposed methodology considers the features of selected networks structure. Potential damage consists both of the protected assets worth and the topology specificity. The probability of an attack is determined individually for each attacker type, taking into account his resources and motivation. A risk management methodology is proposed. It represents a risk-aware dual routing mechanism, based on evolutional algorithm. Proposed algorithm makes it possible to calculate the most optimal system settings, while providing an acceptable convergence time Extensive simulation results demonstrate an increase in security level in various network topologies without essential performance reducing.

Keywords: Internet of Things, software-defined network (SDN), risk, availability, routing.

Submitted 21.01.2023

Information about authors

Sergey A. Ermakov – Cand. Sc. (Technical), Concern «Sozvezdie», e-mail: mnac@comch.ru
Ilia I. Donskov – student, Voronezh State Technical University, e-mail: mnac@comch.ru
Andrey A. Bolgov – graduate student, Voronezh State Technical University, e-mail: mnac@comch.ru
Oleg Yu. Mekerov – Dr. Sc. (Technical), Professor, Voronezh State Technical University, e-mail: mnac@comch.ru
Roman D. Burtsev – student, Voronezh State Technical University, e-mail: mnac@comch.ru