На правах рукописи

ПЕТРОВ Иван Сергеевич

ОБНАРУЖЕНИЕ СКОМПРОМЕТИРОВАННЫХ КОММУТАТОРОВ В ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЯХ

Специальность 05.13.11 — математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

АВТОРЕФЕРАТ

диссертации на соискание ученой степени

кандидата физико-математических наук

Москва — 2019

Работа выполнена на кафедре автоматизации систем вычислительных комплексов факультета вычислительной математики и кибернетики Федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет им. М.В. Ломоносова».

Научный руководитель:	Доктор физико-математических наук, член-корреспондент РАН, профессор, Смелянский Руслан Леонидович.
Официальные оппоненты:	Доктор физико-математических наук, заведующая научно-учебной лабораторией процессно-ориентированных информационных систем факультета компьютерных наук Федерального государственного автономного образовательного учреждения высшего профессионального образования «Национальный исследовательский университет «Высшая школа экономики», профессор, Ломазова Ирина Александровна;
	Кандидат технических наук, начальник научно-технического центра перспективных технологий информационных процессов «ФГАНУ ЦИТиС», Селиванов Сергей Александрович.
Ведущая организация:	Федеральное государственное бюджетное образовательное учреждение высшего образования «Ярославский государственный университет им. П.Г. Демидова».

Защита состоится 16 мая 2019 года в 14:00 на заседании диссертационного совета Д 002.087.01 при Федеральном государственном бюджетном учреждении науки «Институт системного программирования им. В.П. Иванникова Российской академии наук» по адресу: 109004, Москва, ул. Александра Солженицына, 25.

С диссертацией можно ознакомиться в библиотеке и на сайте Федерального государственного бюджетного учреждения науки «Институт системного программирования им. В.П. Иванникова Российской академии наук».

Автореферат разослан «_____» _____ 20__ года.

Ученый секретарь
диссертационного совета Д 002.087.01
кандидат физико-математических наук С. В. Зеленов

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность работы. Программно-конфигурируемые сети (ПКС), по мнению ведущих производителей сетевого оборудования, являются одним из самых перспективных направлений сетевой индустрии на данный момент. ПКС – это концепция построения сети, в которой контур управления сетью (*control-plane*) отделен от контура передачи данных (*data-plane*). Согласно концепции ПКС, вся логика управления переносится на отдельное устройство — контроллер, который способен отслеживать работу всей сети и управлять сетевыми устройствами — коммутаторами.

С появлением новой концепции компьютерных сетей появляются и новые виды угроз, которые могут привести не только к материальным потерям, но и к утрате репутации и имиджа компаний, использующих подобные сети. Следовательно, во избежание негативных последствий компьютерных атак, необходимо производить анализ защищенности ПКС и разрабатывать механизмы защиты таких сетей.

В работе представлены результаты исследования проблемы обнаружения скомпрометированных ПКС коммутаторов. Под скомпрометированным ПКС коммутатором понимается коммутатор сети, управляемой ПКС контроллером, который, в действительности, находится под контролем злоумышленника. Возможность компрометации обусловлена тем, что коммутаторы могут иметь уязвимости, которые могут быть использованы злоумышленником для захвата коммутаторов.

Несмотря на то, что все функции управления сетью вынесены на контроллер, компрометация коммутатора является серьезной угрозой безопасности всей сети, так как атакующий может использовать подконтрольные ему коммутаторы для проведения различных атак как на контур данных, так и на контур управления.

Сложность задачи обнаружения скомпрометированного коммутатора заключается в том, что подобный коммутатор невозможно обнаружить средствами аутентификации устройства. Это обусловлено тем, что, получая контроль над коммутатором, злоумышленник получает доступ к криптографическим ключам, находящимся в памяти коммутатора и сможет провести процедуру аутентификации скомпрометированного коммутатора.

На основании вышесказанного следует, что необходимы методы, которые позволят обнаружить скомпрометированные коммутаторы по различным косвенным признакам, то есть по наличию атак на контур передачи данных и по влиянию этих атак на легитимные коммутаторы.

Цель работы. Целью диссертационной работы является разработка алгоритма обнаружения скомпрометированных коммутаторов в ПКС.

Для достижения поставленной цели в рамках настоящей работы было необходимо решить следующие задачи:

1. Провести обзор и сравнительный анализ существующих средств обнаружения скомпрометированных ПКС коммутаторов.

2. Разработать математическую модель ПКС сети для описания динамики изменения счетчиков правил маршрутизации.

3. Разработать алгоритм предсказания значения счетчиков правил маршрутизации, основанный на разработанной математической модели, и доказать его корректность.

4. Разработать алгоритм обнаружения скомпрометированных ПКС коммутаторов, который будет использовать алгоритм предсказания значений счетчиков правил маршрутизации, и обосновать его корректность.

Научная новизна. В диссертации разработана новая математическая модель, описывающая динамику изменения счетчиков правил маршрутизации в ПКС, в рамках которой сделана математическая постановка задачи. На основе математической модели был разработан новый алгоритм предсказания значений счетчиков правил маршрутизации при произвольной логике работы приложений на контроллере. Также был проведен анализ известных алгоритмов обнаружения скомпрометированных коммутаторов в ПКС, на основании которого сформулированы основные ограничения существующих алгоритмов.

В диссертации предложен новый алгоритм обнаружения скомпрометированных коммутаторов в ПКС, который свободен от ограничений существующих алгоритмов.

Теоретическая и практическая значимость. Теоретическая значимость работы состоит в проведении обзора существующих систем обнаружения скомпрометированных коммутаторов в ПКС, построении математической модели, описывающей изменение счетчиков правил маршрутизации, разработке алгоритма предсказания значений счетчиков правил маршрутизации и алгоритма обнаружения скомпрометированных коммутаторов в ПКС.

Практическая значимость работы обусловлена тем, что результаты работы могут быть использованы для обеспечения безопасности в сетях телеком-операторов и центрах обработки данных.

Положения, выносимые на защиту.

- Впервые разработана математическая модель, описывающая динамику изменения счетчиков правил маршрутизации в OpenFlow коммутаторах в ПКС, которая инвариантна к набору правил маршрутизации, установленных в OpenFlow коммутаторах, и логике работы приложений контроллера в ПКС.

- В рамках разработанной модели построен алгоритм предсказания значений счетчиков правил маршрутизации, корректность которого доказана.

- На основе алгоритма предсказания значений счетчиков построен алгоритм обнаружения скомпрометированных коммутаторов, для которого экспериментально получены оценки ошибок первого/второго рода и время обнаружения скомпрометированных коммутаторов на топологиях, используемых в сетях операторов связи и центров обработки данных. Показано, что представленный алгоритм обнаружения превосходит известные алгоритмы обнаружения, используемые в существующих системах обнаружения, по ряду практически важных критериев.

Апробация работы. Результаты, представленные в работе, докладывались на научных семинарах лаборатории Вычислительных комплексов кафедры Автоматизации систем вычислительных комплексов факультета ВМК МГУ под руководством чл.-корр. РАН, профессора Р.Л. Смелянского, семинаре кафедры Автоматизации систем вычислительных комплексов имени чл.-корр. РАН, профессора Л.Н. Королёва, научном семинаре кафедры Математической кибернетики факультета ВМК МГУ под руководством доктора физ.-мат. наук, профессора В.А. Захарова, заседании консорциума «ПКС в научно образовательной среде», проводимом Центром Прикладных Исследований Компьютерных Сетей, а также на 5 конференциях:

1. Всероссийской научной конференции «Ломоносовские чтения — 2017»
2. Международной научной конференции «REDS-2017»
3. Международной научной конференции «ElConRus-2018»
4. Всероссийской научной конференции «Ломоносовские чтения — 2018»
5. Международной научной конференции «MoNeTec-2018»

Публикации. По теме диссертации имеется 1 патент на изобретение и 12 публикаций. 5 публикаций [7,8,9,11,12] изданы в журналах, рекомендованных ВАК, 3 из них [7,8,9] изданы в журналах, цитируемых Scopus / Web of Science. Список публикаций приводится в конце автореферата.

В работе [3] вклад Шемякина Р.О. заключается в реализации системы обеспечения контроля доступа приложений к ресурсам контроллера и проведении экспериментального исследования. Петрову И.С. принадлежит постановка задачи и описание алгоритма обеспечения контроля доступа.

В работе [4] Шендяпин А.С. реализовал тестовые атаки Man-in-the-Middle с использованием скомпрометированного коммутатора и провел экспериментальное исследование. Вклад Петрова И.С. заключается в постановке задачи, разработке методов проведения тестовых атак и описании методики проведения экспериментального исследования.

В работах [5,6,7] вклад Смелянского Р.Л. заключается в постановке задач и описании методик проведения экспериментов. Петрову И.С. принадлежит разработка алгоритмов минимизации группового трафика и обнаружения скомпрометированных коммутаторов, обзоре существующих решений, реализации алгоритмов и проведении экспериментальных исследований.

В работе [9] Моргунова О.М. реализовала алгоритм минимизации количества правил маршрутизации и провела экспериментальное исследование. Вклад Петрова И.С. заключается в разработке алгоритма минимизации количества правил маршрутизации для анализа сетевой статистики и описании методики проведения экспериментального исследования.

В работе [10] Шендяпину А.С. принадлежит экспериментальное сравнение существующих средств обеспечения анонимности в программно-конфигурируемых сетях. Петрову И.С. принадлежит описание критериев сравнения и проведение обзора существующих средств.

В патенте [13] вклад Смелянского Р.Л. и Шалимова А.В. заключается в постановке задачи и описании методики анализа алгоритма минимизации группового трафика. Петрову И.С. принадлежит проведение обзора существующих решений и разработка алгоритма минимизации группового трафика в программно-конфигурируемых сетях.

Личный вклад автора. Все представленные в диссертации результаты получены лично автором.

Структура и объем диссертации. Диссертация состоит из введения, 6 глав, заключения и 1 приложения. Полный объём диссертации составляет 156 страниц с 17 рисунками и 2 таблицами. Список литературы содержит 83 наименования.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность диссертационной работы, сформулирована цель и аргументирована научная новизна исследований, показана практическая значимость полученных результатов, представлены выносимые на защиту научные положения и дано краткое описание задачи.

В первой главе приводится постановка задачи обнаружения скомпрометированных коммутаторов в ПКС. В *разделе 1.1* вводится понятие скомпрометированного коммутатора. В *разделе 1.2* рассматривается задача обнаружения скомпрометированных коммутаторов в ПКС и описываются проблемы, связанные с этой задачей.

Во второй главе приведено описание атак, которые злоумышленник может производить при помощи скомпрометированного ПКС коммутатора. В *разделе 2.1* рассматриваются атаки на контур передачи данных, такие как атаки на канал передачи данных и атаки на коммутаторы.

В *разделе 2.2* рассматриваются атаки на контур управления, а именно атаки на канал управления и атаки на контроллер.

Большой спектр атак, которые злоумышленник может проводить при помощи скомпрометированного коммутатора, показывает серьезность угрозы захвата коммутатора и необходимость разработки средств для обнаружения скомпрометированных коммутаторов и обнаружения атак, проводимых при помощи таких коммутаторов.

В третьей главе проводится обзор существующих систем обнаружения скомпрометированных коммутаторов в ПКС, выделяются их основные недостатки и также определяются требования к разработке системы обнаружения скомпрометированных коммутаторов.

В *разделе 3.1* сформулированы требования к системе обнаружения скомпрометированных коммутаторов в ПКС:

- **К1** — Обнаружение двух и более скомпрометированных коммутаторов.

  Злоумышленник может захватить несколько коммутаторов в сети и организовать их согласованную работу так, чтобы избежать обнаружения.

- **К2** — Верификация данных, поступающих от каждого коммутатора.

  Злоумышленник может так скоординировать действия скомпрометированных коммутаторов, что на контроллер будет поступать некорректная статистика, искаженная так чтобы скрыть факт наличия атаки, либо заставить систему обнаружения подозревать легитимный коммутатор.

- **К3** — Разграничение вредоносного и легитимного сброса пакетов.

  Важным критерием сравнения является возможность системы отличать вредоносный сброс пакета на коммутаторе, вследствие атаки, от легитимного сброса пакета в силу наличия в памяти коммутатора соот-

ветствующего правила обработки пакетов, либо из-за перегрузки легитимного коммутатора. Если система не способна различать эти случаи сброса пакетов, то обнаружение скомпрометированных коммутаторов будет сопровождаться большим количеством ошибок первого рода, когда сброс пакетов из-за перегрузки в сети будет восприниматься как атака.

- **K4** — Отсутствие требования модификаций контура передачи данных.

  Применение системы обнаружения скомпрометированных коммутаторов не должно требовать изменений в существующих протоколах и логике работы коммутаторов в контуре передачи данных. Изменения в логике работы коммутаторов могут быть дорогостоящими и в некоторых ситуациях неприемлемым решением. Поэтому для того, чтобы система могла быть применима в реальной сети, необходимо, чтобы она не требовала внесения изменений в существующие протоколы и логику работы коммутаторов.

- **K5** — Обнаружение атаки вне зависимости от ее длительности.

  Этот критерий описывает возможность системы обнаруживать атаки, время которых незначительно по сравнению со временем жизни потока данных в сети. К таким атакам могут относиться кратковременный сброс пакетов, кратковременная *DoS* атака на некоторого пользователя или атака на определенные пакеты некоторого потока в сети.

- **K6** — Независимость от используемых в сети алгоритмов и политик маршрутизации.

  Этот критерий предполагает возможность системы работать при использовании в сети разнообразных алгоритмов и политик маршрутизации. Поскольку концепция ПКС дает большую свободу в управле-

нии сетевым трафиком, то заранее предвидеть сложность алгоритмов и политик маршрутизации невозможно. Так же система не должна зависеть от применяемых в сети механизмов маршрутизации и оптимизации потоков таких, как агрегация потоков, балансировка нагрузки, перенаправление трафика в случае изменений в топологии из-за ошибок в сети.

- **К7** — Отсутствие влияния на атаки.

  Процедура обнаружения атаки может влиять на состояние сети, например, устанавливать новые правила маршрутизации, генерировать новые служебные пакеты. Поэтому могут возникнуть ситуации, когда процедура обнаружения может повлиять на саму атаку, проводимую в сети. Из-за такого влияния атака может прекратиться, и, таким образом, она не будет обнаружена системой.

Эти требования используются в качестве критериев сравнения систем обнаружения в обзоре.

В *разделе 3.2* приведен обзор систем обнаружения скомпрометированных коммутаторов в ПКС, а в *разделе 3.3* проводится сравнительный анализ этих систем. В таблице 1 представлены сводные результаты анализа и сравнение существующих систем обнаружения скомпрометированных ПКС коммутаторов.

В *разделе 3.4* описан вывод по результатам обзора. Из проведенного обзора средств обнаружения скомпрометированных ПКС коммутаторов следует, что для надежного выявления скомпрометированных коммутаторов необходимо разработать систему, которая будет работать при условии использования в сети различных сложных механизмов и оставаться прозрачной для атакующего. Для этого система должна не зависеть от внутренней логики работы контроллера.

	K1	K2	K3	K4	K5	K6	K7
ATPG	✔	✔		✔		✔	✔
FADE		✔		✔	✔		
FlowMon				✔		✔	✔
FDWD		✔		✔		✔	
MLPC				✔			
PDMD				✔			✔
SPHINX	✔	✔		✔	✔		✔
RDDF	✔	✔		✔		✔	✔
WedgeTail	✔	✔				✔	✔
DYNAPFV				✔	✔		✔

Таблица 1: Сравнение систем обнаружения скомпрометированных коммутаторов

Также важно, чтобы система обнаружения учитывала информацию о пакетах, сброшенных вследствие перегрузки в сети, так как такие пакеты могут приводить к ошибкам первого рода при обнаружении скомпрометированных коммутаторов.

В четвертой главе проводится описание разработанной математической модели ПКС сети, описывающей динамику изменения счетчиков правил маршрутизации в сети с произвольной комбинацией установленных правил маршрутизации.

К настоящему моменту существует несколько математических моделей ПКС сетей. Однако, одни модели нацелены на проверку сетевых политик и корректности протоколов, в то время как другие нацелены на обнаружение ошибок администрирования сети, таких как циклы маршрутизации или нарушение связности сети, и решение проблем с изоляцией и утечкой трафика. Ни одна из существующих моделей не описывают динамику изменения счетчиков правил маршрутизации.

Разработанная математическая модель ПКС сети описывает значения счетчиков правил маршрутизации как потоковую функцию на графе зависи-

мостей правил. Представление сети в виде графа зависимостей правил позволяет описывать произвольные комбинации правил маршрутизации, установленные в сети. Таким образом, возможно описание как сложных механизмов маршрутизации (агрегация потоков и балансировка нагрузки), так и ошибок маршрутизации (конечные циклы маршрутизации).

В *разделе 4.1* вводится определение графа зависимостей правил. *Графом зависимостей правил* назовем ориентированный граф $G = G(V, A)$, где V — множество вершин, и A — множество ориентированных ребер. Вершинами в графе зависимостей правил являются правила маршрутизации, установленные на коммутаторы, а ребрами — возможные переходы пакетов между правилами маршрутизации. Также для каждого порта p коммутаторов добавим в множество V пару вершин s и t, называемых *источником* и *стоком порта* p. Эти вершины описывают клиентов, подключенных к коммутаторам. Множества всех источников и стоков в графе G будем обозначать как S и T соответственно.

Каждой вершине $v \in V$ поставим в соответствие *передаточную функцию* $T_v : \mathcal{N} \to 2^{\mathcal{N}}$:

$$T_v(n) = \{n_1, n_2, \ldots, n_{\gamma(v)}\}, \tag{1}$$

где $n, n_1, \ldots, n_{\gamma(v)} \in \mathcal{N}$. Передаточная функция T_v моделирует работу правила v по обработке пакетов. Число $\gamma = \gamma(v)$ называется *степенью дублирования вершины* v.

Доменом D_{T_v} *передаточной функции* T_v назовем множество всех доменов n, которые не преобразуются передаточной функцией в пустое множество:

$$D_{T_v} = \{n \mid T_v(n) \neq \varnothing\}. \tag{2}$$

Домен D_{T_v} описывает множество пакетов, которые обрабатываются правилом, соответствующим вершине v.

Каждой вершине v поставим в соответствие множество $D_v \subseteq \mathcal{N}$, называемое *доменом вершины* v. Под доменом вершины v понимается множество заголовков пакетов, которые могут быть обработаны этим правилом с учетом приоритета, то есть:

$$D_v = D_{T_v} \setminus \bigcup_{w \succ v} D_{T_w}, \tag{3}$$

где «$\succ$» это отношение частичного порядка на множестве вершин V.

В *разделе 4.2* приводится модель ПКС сети, описывающей динамику изменения счетчиков правил маршрутизации. В *подразделе 4.2.1* вводятся определения модели и доказываются основные свойства модели.

Определение 1. *n-доменным потоком* в графе G назовем пару функций $f_n : V \to \mathbb{N}$ и $\hat{f}_n : A \to \mathbb{N}$, таких что $\forall v \in V \setminus S$ и $\forall vw \in A$:

$$f_n(v) = \begin{cases} \sum\limits_{uv \in A} \hat{f}_n(u, v), & \text{если } n \in D_v, \\ 0, & \text{если } n \notin D_v. \end{cases} \tag{4}$$

$$\hat{f}_n(v, w) = \begin{cases} \sum\limits_{m \in \Phi_v^{-1}(n)} f_m(v), & \text{если } n \in D_{vw}, \\ 0, & \text{если } n \notin D_{vw}. \end{cases} \tag{5}$$

и $\forall s \in S$:

$$f_n(s) = f_n^s, \tag{6}$$

где $f_n^s \in \mathbb{N}$ начальный поток из истока s.

Величина $f_n(v)$, где $n = (h, p)$, описывает количество пакетов с заголовком h, пришедших на порт p и обработанных правилом v. Величина $\hat{f}_n(v, w)$, где $n = (h, p)$, обозначает количество пакетов, обработанных правилом v, получивших заголовок h, отправленных на порт p и обработанных правилом w — то есть прошедших по ребру vw.

Определение 2. *Доменным потоком* в графе G назовем пару функций $f : V \to \mathbb{N}$ и $\hat{f} : A \to \mathbb{N}$, таких что $\forall v \in V$ и $\forall vw \in A$:

$$f(v) = \sum_{n \in D_v} f_n(v), \tag{7}$$

$$\hat{f}(v, w) = \sum_{n \in D_{vw}} \hat{f}_n(v, u). \tag{8}$$

Значения $f(v)$ и $\hat{f}(v, w)$ описывают суммарное количество пакетов, обработанных правилом v и суммарное количество пакетов, прошедших по ребру vw, соответственно. Значение $f(v)$ описывает значение счетчика, установленного на правиле маршрутизации v.

В разделе доказывается принцип прохождения доменного потока через вершину v (теорема 1).

Теорема 1.

$$f(v) = \sum_{uv \in A} \hat{f}(u, v) \qquad \forall v \in V \setminus S, \tag{9}$$

$$f(v) = \frac{1}{\gamma(v)} \sum_{vw \in A} \hat{f}(v, w) \qquad \forall v \in V \setminus T, \tag{10}$$

где $\gamma(v)$ — степень дублирования вершины v.

Этот принцип описывает, как изменяется доменный поток при прохождении вершины в графе зависимостей правил.

Пусть $P : \ v_0, v_1, \ldots, v_l$ — ориентированный путь в графе G. Обозначим домен, в который преобразуется домен n после прохождения пути P, как:

$$\Phi_P(n) = \Phi_{v_l}\Big(\ldots \big(\Phi_{v_0}(n)\big) \ldots \Big). \tag{11}$$

Если путь P пустой, то есть не содержит вершин, то $\Phi_P(n) = \{n\}$.

Определение 3. *D-доменным путем* назовем ориентированный путь $P : v_0, v_1, \ldots, v_l$ в графе G, такой что $\forall n \in D$ выполняется:

- $n \in D_{v_0}$;
- $\forall i \in [1, l] \Rightarrow \Phi_{v_0,\ldots,v_{i-1}}(n) \cap D_{v_i} \neq \varnothing$.

Определение 4. *Потоком D-доменного пути* $P_D \in \mathscr{P}$ из вершины v в вершину w при $D \subseteq D_v$ назовем функцию $F : \mathscr{P} \to \mathbb{N}$, такую что:

$$F(P_D) = \sum_{n \in D} f_n(v), \tag{12}$$

где $\mathscr{P}$ — множество всех доменных путей в графе G.

Поток D-доменного пути описывает количество пакетов с заголовками h и входными портами p, такими что $(h, p) \in D$, которые вышли из вершины v и двигались вдоль этого пути.

Определение 5. *Подпространством доменных путей в вершину* v назовем

$$\mathcal{P}(v) = \{P_n : u \to v \mid n \in \mathcal{N}, u \in S\}. \tag{13}$$

Введем следующее обозначение:

$$F\big(\mathcal{P}(v)\big) = \sum_{P_n \in \mathcal{P}(v)} F(P_n). \tag{14}$$

В разделе также доказывается следующая теорема, описывающая отношение между потоком через вершину v и потоком через подпространство доменных путей $\mathcal{P}(v)$.

Теорема 2. Для любой вершины $v \in V$ графа верно:

$$f(v) = F\big(\mathcal{P}(v)\big). \tag{15}$$

Построим следующее множество:

$$\mathbb{P}(v) = \left\{ P_D \ : \ D = \bigcup_{\substack{P_n \in \mathcal{P}(v) \\ E(P_n)=E(P)}} D(P_n) \right\}, \tag{16}$$

где $E(P)$ — множество ребер пути P. И также определим поток по доменным путям $P_D \in \mathbb{P}(v)$ как:

$$F(P_D) = \sum_{n \in D} F(P_n). \tag{17}$$

Из построения следует, что все пути из $\mathbb{P}(v)$ различны, таким образом, из теоремы 2 следует, что:

Следствие 1. Для любой вершины $v \in V$ выполняется следующее:

$$f(v) = F\big(\mathbb{P}(v)\big). \tag{18}$$

Из доказанных ранее теорем следует основная теорема:

Теорема 3.

$$f(v) = \sum_{P \in \mathbb{P}(v)} \sum_{P' \in \mathbb{P}(T) \cap \mathbb{P}|_P} \frac{F(P')}{\hat{\gamma}(P' - P)}. \tag{19}$$

Из теоремы 3 следует, что поток через каждую вершину можно однозначно предсказать, используя значения потоков по путям в $P_D \in \mathbb{P}(T)$, которые в свою очередь равны значениям потоков $f_D(s)$.

В *подразделе 4.2.2* приведено описание алгоритма предсказания значений потоковой функции $f(v)$ и доказана его корректность. Формальное описание представлено в алгоримте 1. Алгоритм использует теорему 3 для предсказания значений потоков в вершинах v графа G по значениям потока в вершинах $s \in S$.

Для построения алгоритма предсказания значений $f(v)$ также определим граф $\mathcal{G}$, который назовем *путевой разверткой графа* G. Путевая развертк-

ка представляет собой множество корневых деревьев с корнями в вершинах $t \in T$. Каждая ветвь такого корневого дерева является доменным путем в графе G.

Построение путевой развертки описано в алгоритме 2. Функция *prune_branch*$(\tilde{v})$ удаляет ветвь дерева путевой развертки, оканчивающуюся в вершине $\tilde{v}$. Функция *create_domain_partition*$(\widetilde{S})$ создает набор новых вершин $\mathscr{S}$, доменами которых являются все попарные пересечения доменов вершин из $\widetilde{S}$.

Algorithm 1 Предсказание потока

Input: Путевая развертка $\mathcal{G}(\widetilde{V}, \widetilde{A}, \mathscr{S})$
Output: Значение $f(v)$ для всех вершин $v \in V$

procedure PREDICT_FLOW($\mathcal{G}$)
  for $\xi \in \mathscr{S}$ **do**
    $Q \leftarrow \xi$
  while $Q \neq \varnothing$ **do**
    $\tilde{v} \leftarrow Q$
    $v \leftarrow \rho^{-1}(\tilde{v})$
    $f(v) \leftarrow f(v) + f(\tilde{v})/\hat{\gamma}(\tilde{v})$
    for $\tilde{w} \in \delta^{out}(\tilde{v})$ **do**
      $f(\tilde{w}) \leftarrow f(\tilde{w}) + f(\tilde{v})$
      $visited \leftarrow visited \cup \{\tilde{w}\}$
      if $\delta^{in}(\tilde{w}) \subseteq visited$ **then**
        $Q \leftarrow \tilde{w}$
  return f

В пятой главе приведено подробное описание разработанного алгоритма обнаружения скомпрометированых коммутаторов в ПКС. В *разделе 5.1* приведено общее описание разработанного алгоритма, состоящего из двух основных фаз:

1. Установка дополнительных правил;
   - Построение графа зависимостей правил;

Algorithm 2 Построение путевой развертки

Input: Граф зависимостей правил G
Output: Путевая развертка $\mathcal{G}(\widetilde{V}, \widetilde{A}, \mathscr{S})$

procedure CREATE_PATH_SCAN(G)
  for $t \in T$ **do**
    $\tilde{t} \leftarrow$ **create_node**$(t, \mathcal{N}, 1)$
    $\widetilde{V} \leftarrow \widetilde{V} \cup \{\tilde{t}\}$
    $Q \leftarrow \tilde{t}$
  while $Q \neq \varnothing$ **do**
    $\tilde{v} \leftarrow Q$
    $v \leftarrow \rho(\tilde{v})$
    for $u \in \delta^{in}(v)$ **and** $D_{uv} \cap D_{\tilde{v}} \neq \varnothing$ **do**
      if $\delta^{in}(u) = \varnothing$ **and** $u \notin S$ **then**
        prune_branch$(\tilde{v})$
      else
        $D \leftarrow \Phi_u^{-1}(D_{uv} \cap D_{\tilde{v}})$
        $\gamma \leftarrow \gamma(u)\hat{\gamma}(\tilde{v})$
        $\tilde{u} \leftarrow$ **create_node**(u, D, γ)
        $\widetilde{V} \leftarrow \widetilde{V} \cup \{\tilde{u}\}$
        $\widetilde{A} \leftarrow \widetilde{A} \cup \{\tilde{u}\tilde{v}\}$
        if $u \in S$ **then**
          $\widetilde{S} \leftarrow \tilde{u}$
        else
          $Q \leftarrow \tilde{u}$
  $\mathscr{S} \leftarrow$ **create_domain_partition**$(\widetilde{S})$
  return $\mathcal{G}(\widetilde{V}, \widetilde{A}, \mathscr{S})$

- Построение путевой развертки;
- Создание дополнительных правил;
- Установка правил.

2. Анализ сетевой статистики.
   - Предсказание значений счетчиков;
   - Обнаружение скомпрометированных коммутаторов.

Краткое описание приведено в алгоритме 3. В описании алгоритма 3 используются следующие обозначения:

- $T(v)$ — уровень доверия коммутатора, содержащего правило v;
- δ — порог ошибки предсказания значений счетчиков;
- Δ — потог уровня доверия коммутаторов;
- γ_1 и γ_2 — коэффициенты изменения уровней доверия коммутаторов;
- t — интервал времени между запросами (в миллисекундах).

В *разделе 5.2* подробно описана первая фаза алгоритма, которая предполагает установку в сеть дополнительных правил маршрутизации. Каждое такое правило маршрутизации ставится в соответствие некоторому доменному пути из путевой развертки, который определяет поля *match* этих правил маршрутизации — поля, описывающие заголовки обрабатываемых пакетов. Поля *match* устанавливаются таким образом, чтобы дополнительные правила обрабытывали только пакеты из соответствующих им доменных путей. Это необходимо для того, чтобы счетчики дополнительных правил маршрутизации отражали значения потоковых функций на доменных путях.

Algorithm 3 Обнаружение скомпрометированых коммутаторов

Input: Набор правил маршрутизации, установленных в сети
Output: Скомпрометированный коммутатор S

Построить граф зависимостей правил $G(V, E)$
Построить путевую развертку $\mathcal{G}$
Получить множество $\mathscr{S}$ дополнительных вершин из $\mathcal{G}$
for $\xi \in \mathscr{S}$ **do**
    Создать правило r_ξ, обрабатывающее пакеты с заголовками из D_ξ
    Установить правило r_ξ на коммутатор, определяемый вершиной ξ
while True do
    for $v \in V$ **do**
        $P(v) = \frac{1}{T(v)} / \sum_{w \in V} \frac{1}{T(w)}$
    Выбрать случайное правило v с учетом функции вероятности P
    Предсказать значение $f_{pred}(v)$ счетчика правила v
    Запросить реальное значение $f_{real}(v)$ счетчика правила v
    if $\left|f_{pred}(v) - f_{real}(v)\right| < \delta$ **then**
        $T(v) = T(v) + \gamma_2$
    else
        $T(v) = T(v)/\gamma_1$
        if $T(v) < \Delta$ **then**
            return коммутатор S, соответствующий правилу v
    sleep(t)

В *разделе 5.3* подробно описана вторая фаза алгоритма, которая предполагает предсказание значений счетчиков правил маршрутизациии и сравнение этих значений с реальными, предоставляемыми коммутаторами в сети.

Для предсказания значения счетчика правила, соответствующего некоторой вершине v графа зависимостей правил, выполняется следующий набор действий:

1. Определяется набор $\mathcal{V}$ вершин путевой развертки, соответствующих вершине v графа зависимостей правил.

2. Следуя по ветвям деревьев путевой развертки с корнями в множестве $\mathcal{V}$, выбираются вершины, соответствующие дополнительным правилам.

3. В сеть отправляются запросы статистики для набора выбранных дополнительных правил маршрутизации.

4. После получения статистики по дополнительным правилам маршрутизации выполняется алгоритм предсказания значений счетчиков.

5. В качестве предсказанного значения счетчика правила, соответствующего вершине v, возвращается сумма значений потоков вершин из множества $\mathcal{V}$.

6. Значения потока в вершинах путевой развертки сохраняются для того, чтобы при новом запросе учитывать только изменение счетчика правила маршрутизации по сравнению с предыдущим значением.

Для обнаружения скомпрометированного коммутатора из сети запрашивается реальное значение счетчика правила машрутизации и сравнивается с предсказанным значением, и, если в сети проводится атака на контур передачи данных, то эти значения будут отличаться.

В шестой главе представлено описание разработанного прототипа системы обнаружения скомпрометированных коммутаторов и результаты его экспериментального исследования. В *разделе 6.1* приведена архитектура системы обнаружения скомпрометированных коммутаторов в ПКС.

В *разделе 6.2* описаны результаты экспериментального исследования разработанного прототипа системы обнаружения скомпрометированных коммутаторов. Экспериментальное исследование было нацелено на определение следующих свойств реализуемой системы обнаружения:

1. Погрешности предсказания значений счетчиков;
2. Времени работы алгоритма;
3. Точности обнаружения скомпрометированных коммутаторов.

Эксперименты на топологиях размером до 300 коммутаторов и интенсивности потоков до 1 Гбит/с показывают, что предложенный алгоритм способен обнаружить скомпрометированный коммутатор менее, чем через 15 секунд после начала атаки, при этом ошибки первого и второго рода составляют 3.7% и 6.6% соответственно. Негативное влияние на сеть, представляемое задержкой реакции контроллера на изменение состояния сети, не более 420 мс.

В заключении формулируются основные результаты работы.

В **Приложении А** подробно описаны компоненты разработанной системы обнаружения скомпрометированных коммутаторов.

ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

Полученные автором результаты изложены в следующих работах:

1. Петров И.С. Задача обнаружения скомпрометированных коммутаторовв SDN сетях // REDS: Телекоммуникационные устройства и системы. — 2017. — Vol. 7, no. 4. — P. 515–518.

2. Петров И.С., Смелянский Р.Л. Обнаружение скомпрометированных коммутаторов в SDN сетях // Ломоносовские чтения. Тезисы докладов научной конференции. — 2017. — P. 82–83.

3. Шемякин Р.О., Петров И.С. Обеспечение контроля доступа приложений к ресурсам контроллера программно конфигурируемых сетей // Программные системы и инструменты. Тематический сборник. Под общей редакцией Р.Л. Смелянского. — 2017. — P. 61–72.

4. Шендяпин А.С., Петров И.С. Исследование методов проведения атаки Man-in-the-Middle в программно-конфигурируемых сетях // Программные системы и инструменты. Тематический сборник. Под общей редакцией Р.Л. Смелянского. — 2017. — P. 73–82.

5. Петров И.С., Смелянский Р.Л. Алгоритм обнаружения скомпрометированных коммутаторов в SDN // Ломоносовские чтения 2018 ф-т ВМК МГУ. — 2018. — P. 98–99.

6. Петров И.С., Смелянский Р.Л. Минимизация группового трафика и обеспечение его отказоустойчивости в программно-конфигурируемых сетях // Известия Российской академии наук. Теория и системы управления. — 2018. — no. 3. — P. 64–75.

7. Petrov I., Smeliansky R. Minimization of multicast traffic and ensuring its

fault tolerance in software-defined networks // Journal of Computer and Systems Sciences International. — 2018. — Vol. 57, no. 3. — P. 407–419.

8. Petrov I. Mathematical model for predicting forwarding rule counter values in SDN // Young Researchers in Electrical and Electronic Engineering (EIConRus), 2018 IEEE Conference of Russian / IEEE. — 2018. — P. 1313–1317.

9. Petrov I., Morgunova O. Forwarding rule minimization for network statistics analysis in SDN // 2018 International Scientific and Technical Conference Modern Computer Network Technologies (MoNeTeC) / IEEE. — 2018. — P. 1–6.

10. Петров И.С., Шендяпин А.С. Обзор средств обеспечения анонимности в SDN // Программные системы и инструменты. Тематический сборник. Под ред. В. В. Балашов, Е. И. Большакова, Д. Ю. Волканов и др. — Т. 18. — МАКС Пресс Москва, 2018. — С. 78–88.

11. Петров И.С. Системы обнаружения скомпрометированных коммутаторов в программно-конфигурируемых сетях // Информационные технологии. 2019. Т.25, №3. С.131-142.

12. Петров И.С. Алгоритм минимизации количества правил маршрутизации в ПКС // Моделирование и анализ информационных систем. 2019. Т. 26, №1. С. 122–133.

13. Способ минимизации многоадресного трафика и обеспечение его отказоустойчивости в ПКС сетях: Патент 2676239 МПК H04L 12/869 (2013.01) / Петров И.С., Шалимов А.В., Смелянский Р.Л. (RU); патентообладатель Некоммерческое партнерство «Центр прикладных исследований компьютерных сетей»; — No 2017122409; опубл. 26.12.2018, Бюл. No 36; приоритет 11.09.2017.