**ЎЗБЕКИСТОН РЕСПУБЛИКАСИ АХБОРОТ ТЕХНОЛОГИЯЛАРИ ВА КОММУНИКАЦИЯЛАРИНИ РИВОЖЛАНТИРИШ ВАЗИРЛИГИ**

**МУҲАММАД АЛ-ХОРАЗМИЙ НОМИДАГИ ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ**

**ЎЗБЕКИСТОН РАДИОТЕХНИКА, ЭЛЕКТРОНИКА ВА АЛОҚА ИЛМИЙ-ТЕХНИКА ЖАМИЯТИ**

# ИҚТИСОДИЁТНИНГ РЕАЛ ТАРМОҚЛАРИНИ ИННОВАЦИОН РИВОЖЛАНИШИДА АХБОРОТ–КОММУНИКАЦИЯ ТЕХНОЛОГИЯЛАРИНИНГ АҲАМИЯТИ

Республика илмий-техник анжуманининг

## МАЪРУЗАЛАР ТЎПЛАМИ
**3-ҚИСМ**

# СБОРНИК ДОКЛАДОВ

Республиканской научно-технический конференции

# ЗНАЧЕНИЕ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В ИННОВАЦИОННОМ РАЗВИТИИ РЕАЛЬНЫХ ОТРАСЛЕЙ Э КОНОМИКИ

**ЧАСТЬ 3**

**6-7 апрел 2017 йил**

ТОШКЕНТ – 2017

основанием и дополнительным сердечником позволяют получить информацию – сигнала о несимметрии трехфазных токов электрической сети в виде выходных напряжении $U_{эвыха}$ , $U_{эвыхв}$ , $U_{эвыхс}$ , которые появляются при неравенстве магнитных потоков $Ф_1 \neq Ф_2 \neq Ф_3$ и следовательно первичных токов $I_{эвхА}$, $I_{эвхВ}$, $I_{эвхС}$ трехфазной электрической сети ЭС.

Выводы по работе:

1. Подтверждено, что трехфазная электрическая сеть ЭС является сбалансированной или симметричной, когда напряжения и токи каждой из фаз имеют одинаковую амплитуду, а сдвиг амплитуды по фазе равен $120^0$. Если не выполняется хотя бы одно из этих условий и этот фактор должень быть учтен при управлении источниками электроэнергии.

**2**. Установлено, что значение частоты при преобразовании несиметрии трехфазного тока ЭС должно определяться требованиями к коэффициенту мощности в режиме передачи энергии по электрическим сетям ЭС.

3. Разработана конструкция электромагнитного преобразователя тока в напряжение, в которой при преобразовании несимметрии трехфазных первичных токов во вторичное напряжение магнитная система выполняется в виде параллельных стержней.

## ИДЕНТИФИКАЦИЯ И УПРАВЛЕНИЕ СЕТЕВЫМ ТРАФИКОМ С ПОМОЩЬЮ СТАТИСТИЧЕСКИХ МЕТОДОВ КЛАССИФИКАЦИИ

*Х.Н. Тешабоев (ТУИТ,магистрант)*
*А.Т. Шокиров (ТУИТ, магистрант)*

Использование в современных телекоммуникационных сетях (ТС) большего количества сетевых сервисов и приложений, аппаратного и программного обеспечения приводит к появлению в сети большого разнообразия трафиков. При этом для проведения эффективного мониторинга и управления ТС решение задачи точной идентификации и классификации трафиков относительно сетевых сервисов, приложений и протоколов является очень важной. Потому, что сетевой трафик является одним из важнейших фактических показателей работы ТС. Сетевой трафик является носителем информации о поведении пользователей и функционировании ТС. На основе статистического анализа сетевого трафика можно косвенно определить статистические характеристики поведения КС. Идентификация и классификация сетевого трафика особенно важна для решения таких задач, как определение приоритетов при формировании полосы пропускания для отдельных трафиков, установление правил по управлению сети, обеспечение безопасности сети, диагностический мониторинг ТС.

Прежде чем классифицировать сетевой трафик, очень важно определить их классификационные характеристики. Эти характеристики могут быть определены в результате анализа свойств, описывающих сетевой трафик, к которым могут относиться различные особенности общего сетевого трафика ТС. Классификацию сетевого трафика можно определить как анализ трафиков, созданных различными сетевыми приложениями. Для классификации сетевого трафика обычно применялись простые методы, основанные на анализе информации, характеризующей пакеты (номера портов, IP адреса отправителей и получателей, типы приложений и протоколов и т.д.). Наиболее часто применяемые виды классификации трафика на основе известного номера порта и исследовании полезной нагрузки сетевых пакетов имеют ряд ограничений. Для их преодоления используются статистические методы распознавания шаблонов сетевого трафика. В связи с актуальностью на сегодняшний день проблемы распознавания трафика возникла задача исследования статистических методов классификации. Классификация IP-трафика основывается на исследовании TCP и UDP номеров портов пакетов (классификация, основанная на портах), реконструкции сигнатуры протокола из его полезной нагрузки (классификация, основанная на полезной нагрузке), статистических методов анализа

характеристик обмена пакетами между хостами и статистических свойств сетевого трафика. Каждый из подходов обладает своими достоинствами и недостатками.

В некоторых случаях шифрование IP уровня может запутать TCP и UDP заголовки, что делает невозможным определение фактического номера порта. Чтобы избежать полной зависимости от номеров портов и собрать сведения об используемом протоколе, многие современные промышленные продукты используют восстановление состояния сеанса и прикладную информацию из содержимого каждого пакета.

Рассмотрим проблемы классификации трафика с точки зрения возможных методов проверки, а также перечень методов обработки, которые могут быть использованы в рамках классификации на основе полезной нагрузки.Можно выделить четыре различных степени проверки:

-Первая степень проверки основана на сигнатуре, ее цель состоит в поиске некоторых сигнатур в рамках полезной нагрузки прикладного уровня. Так, например, HTTP-пакет начинается с команды, следующей за URL и версией протокола, в то время как большинство Edonkey пакетов имеет поля, содержащие размер полезной нагрузки. Метод на основе сигнатур строится на соответствии полезной нагрузки (или ее части) с сигнатурой, определенной для данного протокола. Сигнатуры, как правило, являются регулярными выражениями;

-Второй уровень проверки – синтаксический. Он может рассматриваться как более точная версия сигнатурной проверки, поскольку направлен на проверку правильности переданных данных с синтаксической точки зрения (к примеру, предполагается, что полезная нагрузка HTTP должна содержать HTTP заголовки). В этом случае необходимо декодировать все поля, содержащиеся в сообщении, и гарантировать, что сообщение является хорошо сформированным;

-Третья степень контроля связана с протоколом соответствия. Например, она контролирует, что на HTTP GET запрос от клиента следует действительно ответ от сервера. Такая форма контроля является более точной, поскольку она может проверять в соответствии со спецификацией реальное поведение протокола;

-Четвертая степень контроля относится к семантике данных. К примеру, она способна проверить, является ли объект, передаваемый по протоколу HTTP, изображением или какой-либо другой формой содержания. Такой контроль очень полезен для обнаружения "туннелей", в которых приложение использует другой протокол для транспортировки данных. На данный момент это наиболее неформализованный метод.

Рассмотрим различные методы обработки, которые могут быть использованы в рамках классификации на основе полезной нагрузки.

Простейшим методом является PBNS, который работает, проверяя значения некоторых полей (например, TCP/UDP порты), присутствующих в каждом пакете. Этот метод очень прост с точки зрения вычислений (должны быть обработаны только заголовки пакета до L4), для него не требуется хранить состояния.

Второй метод – PBFS требует реализации таблицы сеансов, в которой каждая запись включает идентификатор сеанса (пять кортежей IP источник/назначения, транспортный протокол, порт источника/назначения), и соответствующий протокол прикладного уровня (ID протокола). Каждая таблица занимает по нескольку десятков байт.

Работа третьего метода MBFS основана на сообщениях. Для этого метода требуется модуль нормализации3 TCP/IP пакетов. Технологии на основе MBFS могут выполнить те же самые проверки, что и PBFS, но работают на сообщениях, следовательно, их средства управления могут быть расширены на все сообщение целиком взамен первого сегмента данных. В таком случае, требуемые объемы памяти увеличиваются из-за дополнительной информации о состояниях, которая должна быть сохранена для каждого сеанса (например, порядковый номер TCP) и из-за буферов, требуемых TCP/IP нормализатором. Все эти параметры сильно зависят от природы

трафика, то есть от количества фрагментированных пакетов и “ненормальных” (с пропущенными сегментами и т.д.) TCP сеансов. В зависимости от реализации, некоторые продукты могут выполнить синтаксическую проверку для всех сообщениях.

Четвертая категория MBPS точно интерпретирует, что передает и получает каждое приложение. Обработчик MBPS понимает не только семантическую часть сообщения, но и различные этапы обмена сообщениями (например, HTTP GET, должен сопровождаться соответствующим кодом ответа от веб-сервера), так как этот метод полностью понимает конечный автомат протокола. Требуемые объемы памяти становятся еще большими, потому что надо учитывать не только состояние транспортного сеанса, но также и состояние каждого сеанса прикладного уровня. Производительность является самой высокой среди всех методов – все данные прикладного уровня должны быть обработаны, чтобы проверить соответствие протокола. Реализации, основанные на технологии PBFS, обычно с каждым сеансом связывают некоторое дополнительное состояние, чтобы выполнить более точную классификацию. Например, некоторые приложения (Skype, VoIP), могут быть обнаружены, проверяя шаблон из нескольких последовательных пакетов.

Однако использование в модели классификации сетевого трафика метода обучения без учителя может создать определенные преимущества. Основным преимуществом является то, что модель позволит идентифицировать новые приложения и группировать их в новый кластер, тогда как модели, использующие методы обучения с учителем, могут идентифицировать трафики, для которых созданы обучающие примеры, и не могут обнаружить новых приложений.

При классификации сетевого трафика методы без учителя не нуждаются в начальной ручной разметке входных данных, они только основываются на подобии между классифицируемыми объектами и в качестве входных данных используются статистические характеристики потока сетевых данных. Для создания модели классификации сетевого трафика в качестве метода обучения без учителя в работах предложено использовать кластеризацию.

## ПРИМЕНЕНИЕ ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЙ В ОБРАБОТКЕ РЕЧЕВЫХ СИГНАЛОВ

*У.Р. Хамдамов (доцент, ТУИТ)*

Вейвлет – математическая функция, позволяющая анализировать различные частотные компоненты данных. График функции выглядит как волнообразные колебания с амплитудой, уменьшающейся до нуля вдали от начала координат. Однако это частное определение - в общем случае анализ сигналов производится в плоскости вейвлет-коэффициентов. Вейвлет-коэффициенты определяются интегральным преобразованием сигнала.

В начале развития области употреблялся термин «волночка». Английское слово «wavelet» означает в переводе «маленькая волна», или «волны, идущие друг за другом». Вейвлеты - это семейство функций, которые локальны во времени и по частоте, и в которых все функции получаются из одной посредством её сдвигов и растяжений по оси времени.

Разработка вейвлетов и идеи использования теории вейвлетов в задачах обработки сигналов были связаны с несколькими отдельными нитями рассуждений, начавшимися с работ Хаара в начале XX века. Например, Хаар опубликовал в 1910 году полную ортонормальную систему базисных функций с локальной областью определения. Эти функции называются теперь вейвлетами Хаара.

В конце XX века появился инструментальные средства по вейвлетам в системах компьютерной математики Mathcad, MATLAB и Mathematica. В настоящее время