УДК 004.853 DOI: 10.25045/jpit.v12.i2.04

Шыхалиев Р.Г.
Институт Информационных Технологий НАНА, Баку, Азербайджан
ramiz@science.az

ОБ ОДНОМ МЕТОДЕ ИНТЕЛЛЕКТУАЛЬНОГО ПРОАКТИВНОГО МОНИТОРИНГА КОМПЬЮТЕРНЫХ СЕТЕЙ

Daxil olmuşdur: 20.04.2021 Düzəliş olunmuşdur: 27.04.2021 Qəbul olunmuşdur: 04.05.2021

В статье предлагается метод для интеллектуального проактивного мониторинга компьютерных сетей (КС). Для обеспечения проактивности мониторинга КС предлагается использовать методы искусственного интеллекта, в частности глубокого обучения (ГО). Традиционные системы мониторинга в основном не имеют функции проактивного мониторинга. Несмотря на то, что сегодня в КС имеются достаточные вычислительные мощности, полосы пропускания и объемы памяти, все же идентификация важных событий среди огромных объемов данных мониторинга остается проблемой. Следовательно, несвоевременное обнаружение проблем КС может привести к перебоям в работе сети, предоставлении сетевых услуг и снижению безопасности КС. В отличие от традиционного мониторинга, интеллектуальный проактивный мониторинг может предоставлять больше информации о состоянии КС. Проактивность мониторинга КС основывается на прогнозировании поведения сети. При этом одним из основных требований для интеллектуального проактивного мониторинга КС является точность прогнозов, которая характеризует способность метода прогнозирования. Для достижения точности прогнозов при проактивном мониторинге КС используется однородный ансамбль, который состоит из одинокого базового алгоритма обучения. В качестве базового алгоритма обучения используется модель LSTM (Long Short-Term Memory − LSTM). Для создания базовых моделей обучения ансамбля LSTM используется «Bagging»-алгоритм. Предложенный в этой работе метод позволит обеспечить относительно высокую точность прогнозирования проблем КС, следовательно, гарантировать достаточную эффективность системы проактивного мониторинга КС.

Ключевые слова: *компьютерные сети, проактивный мониторинг компьютерных сетей, глубокое обучение, LSTM, прогнозирование.*

Введение

Сегодня бесперебойное функционирование и безопасность компьютерных сетей имеют большое значение для социального благополучия, экономического роста и национальной безопасности разных стран. Для обеспечения бесперебойного функционирования и безопасности КС ключевым шагом является создание эффективной инфраструктуры интеллектуального мониторинга и управления, которая должна постоянно осуществлять мониторинг производительности сети, использования трафика, сетевых сервисов, сетевых приложений и т.д. При этом мониторинг, как одна из основных функций системы управления КС, может применяться к различным сетевым компонентам, таким как коммуникационное оборудование, приложения, системы безопасности, компьютеры и т.д. Всеобъемлющий мониторинг может способствовать лучшему пониманию функционирования КС в целом и планированию ее будущего расширения.

Мониторинг КС может быть как реактивным, так и проактивным. Реактивность мониторинга заключается в том, что он осуществляется тогда, когда в КС происходят проблемы. При реактивном мониторинге требуется информация о состоянии сети, чтобы отреагировать на определенные аварийные ситуации, которые могут возникнуть в сети [1]. В свою очередь проактивный мониторинг КС заключается в упреждении возникновения

потенциальных проблем и оценки рисков возникновения проблем, чтобы избежать больших потерь. Поэтому проактивный мониторинг очень важен для обеспечения бесперебойного функционирования и безопасности КС и должен позволять определять и прогнозировать состояние сети в реальном времени. Проактивный мониторинг может помочь сетевым администраторам устранять аномалии в КС, избегать потенциальных узких мест и т.д. При этом для получения информации о состоянии сети сбор данных может быть осуществлен как пассивным, так и активным способом. Для повышения эффективности процесса мониторинга и управления КС необходимо собирать, хранить и анализировать огромные объемы данных мониторинга. Эффективность мониторинга во многом зависит от качества собранных данных и точности используемых методов анализа данных.

Обычно при мониторинге КС постоянно осуществляются сбор данных в лог-файлах различных сетевых компонентов, а также захват данных из потока трафика и не рассматриваются вопросы прогноза проблем сети. Традиционно администраторы сетей находят проблемы КС, вручную просматривая собранные в лог-файлах данные. Однако этот метод поиска проблем КС устарел и не позволяет учитывать всевозможные проблемы потому, что состояние КС очень быстро меняется и сложно определить нормальный профиль и деятельности. Поэтому сетевые администраторы тратят много времени на мониторинг и устранение проблем своих сетей. Для решения этой задачи необходимо проактивно определить нормальный профиль КС и прогнозировать поведение КС на ближайшее будущее, основываясь на предыдущем нормальном поведении. Следовательно, значительные отклонения от нормального профиля следует рассматривать как аномалию. При этом основной задачей является эффективное управление сбором, хранением, анализом и предоставлением большого объема мониторинговых данных.

Сегодня в КС имеются достаточные вычислительные мощности, полосы пропускания и объемы памяти. Несмотря на это, при мониторинге КС идентификация важных событий среди огромных объемов данных мониторинга остается проблемой. Даже мониторинг КС в реальном времени не может дать точную или сжатую информацию о причинах любой проблемы КС. Поэтому очень актуальна разработка нового интеллектуального проактивного метода мониторинга КС, основанного на методах искусственного интеллекта, в частности глубокого обучения (ГО) (Deep learning (DL)), поскольку постоянно растут размеры КС и объем данных мониторинга. Вовремя не обнаруженные незначительные проблемы КС впоследствии могут перерасти в более серьезные проблемы.

ГО является областью искусственного интеллекта и одним из самых перспективных методов интеграции с традиционными решениями для повышения их точности. С помощью методов ГО можно изучать сложные и абстрактные признаки. Их можно эффективно использовать для достижения более высокой точности прогнозирования. ГО может обработать непрерывные информационные потоки и адаптироваться к различным ситуациям. Поэтому, используя ГО в системах мониторинга, можно обеспечить проактивность мониторинга КС.

Целью данной статьи является разработка метода проактивного мониторинга КС для обнаружения аномальных состояний КС. Для разработки метода проактивного мониторинга КС предлагается использовать ГО.

Концептуальная модель системы проактивного мониторинга КС

Известно, что несвоевременное обнаружение проблем КС может привести к перебоям в работе сети, предоставлении сетевых услуг и снижению безопасности КС. Следовательно, требуется найти и решить такие проблемы, прежде чем они возникнут, то есть требуется система мониторинга с возможностью проактивного мониторинга. При этом основной функцией проактивного мониторинга КС является раннее выявление тенденций и

закономерностей как в сетевом трафике и приложениях, так и в компонентах сети.

Сегодня большинство работ, имеющихся в литературе и посвященных мониторингу КС, сосредоточено на мониторинге сетевого трафика. Ясно, что в нынешней ситуации традиционные системы мониторинга больше не могут адекватно поддерживать администраторов сетей по управлению сбоями, настройкой, производительностью и безопасностью. По сути, традиционные системы мониторинга создают модель текущего поведения КС, представляющую текущее рабочее состояние КС, которая используется для коррекции поведения КС и устранения текущих проблем [2, 3, 4]. В основном администраторам сетей необходимо контролировать рабочее состояние КС, чтобы гарантировать, что ее параметры находятся в допустимых пределах. При этом традиционные системы мониторинга в основном не имеют функцию проактивного мониторинга. В отличие от традиционного статистического мониторинга, проактивный мониторинг может предоставлять больше информации о состоянии КС в режиме реального времени, что позволит также создавать статистические модели на основе собранной информации.

В этой работе для обеспечения проактивности мониторинга КС предлагается концептуальная модель системы проактивного мониторинга КС (рис. 1).

Рис. 1. Концептуальная модель системы проактивного мониторинга КС

Предложенная концептуальная модель состоит из нескольких уровней. На самом низком, то есть на уровне сбора данных, монитор осуществляет сбор данных мониторинга из КС. На этом уровне осуществляется как захват данных из потока данных, которые должны обрабатываться на лету, так и отбор данных из предварительно собранных в лог-файлах данных, которые могут быть предварительно структурированы во временных хранилищах. Далее данные мониторинга передаются на уровень предварительной обработки данных. На этом уровне осуществляются очистка данных, отбор выборок, нормализация данных, преобразование данных, выделение признаков и отбор признаков.

Необходимо подчеркнуть, что на этом уровне посредством динамического регулирования отбором выборок можно изменять точность и эффективность мониторинга КС. При этом значимость и актуальность выделенных и отобранных признаков зависят от ряда факторов, таких как вид сетей, цели мониторинга, вид приложений, вид сервисов и т.д. Например, значимыми и актуальными могут быть мониторинг задержки при взаимодействии клиентов и сервера приложений, значение полосы пропускания, перегрузка сети, задержка в очереди, отказ сети, определение узких мест и т.д. Вместе с тем четыре основные характеристики КС, такие как латентность (latency), потеря пакетов (packet loss), обнаружение пути (path detection) и полоса пропускания (bandwidth), могут быть использованы при вычислении других характеристик КС.

Кроме того, на уровне предварительной обработки данных они должны быть преобразованы так, чтобы формат данных не зависел от вида приложений, то есть чтобы можно было стандартизировать предоставление данных для следующего уровня. На уровне прогнозирования состояния КС, которое определяет проактивность системы мониторинга, используются методы прогнозирования. При этом проактивность мониторинга КС основывается на прогнозировании поведения сети, чтобы предсказать потенциальные проблемы КС. Именно на этом уровне определяется модель прогнозирования текущего и будущего поведения КС. Результаты прогнозирования передаются на уровень управления КС для интерпретации и на основании этих результатов создаются соответствующие решения. В свою очередь эти решения в виде действия могут быть осуществлены либо администраторами КС, либо агентами. При прогнозировании потенциальной проблемы КС принимаются соответствующие решения, чтобы предотвратить или смягчить прогнозируемую проблему. Например, прогнозируемая перегрузка каналов КС может привести к перебоям в ее работе и во избежание этой ситуации необходимы соответствующие действия со стороны администратора КС. При этом прогнозы должны иметь высокую точность, так как, например, ложноотрицательные прогнозы могут привести к тому, что необходимые действия по предотвращению или смягчению истинных проблем КС будут упущены. В свою очередь это может привести к снижению эффективности мониторинга, следовательно, к снижению эффективности функционирования и безопасности самой КС.

В литературе вопросы того или иного уровня представленной выше концептуальной системы проактивного мониторинга КС в отдельности достаточно исследованы. Однако работ, посвященных исследованию вопросов уровня прогнозирования состояния КС, который определяет проактивность системы мониторинга, недостаточно. Поэтому основное внимание в данной работе уделяется исследованию вопросов именно этого уровня, то есть вопросу проактивного мониторинга КС.

Теоретическая база работы

Как было сказано выше, проактивность мониторинга КС основывается на прогнозировании поведения сети. В свою очередь прогнозирование поведения сети основывается на методах искусственного интеллекта, которые используются для анализа данных мониторинга. Если мониторинг КС основан на упорядоченных по времени последовательностях данных, то интеллектуальный анализ данных с использованием моделирования последовательностей, особенно прогнозирования временных рядов [5], является более подходящим. Существуют различные методы прогнозирования временных рядов, такие как статистические методы, методы машинного обучения, метаэвристические методы и глубокие нейронные сети.

Статистические методы, такие как авторегрессионное интегрированное скользящее среднее (Autoregressive Integrated Moving Average – ARIMA), авторегрессионное скользящее среднее (Autoregressive Moving Average – ARMA), скользящее среднее (Moving

Average – MA), для прогнозирования будущих значений временного ряда используют регрессию по прошлым значениям зависимой переменной и моделирование их стохастической части [6], например, для обнаружения отказов [7]. Однако из-за линейности они не подходят для нестационарных временных рядов, то есть среднее значение, дисперсия и автокорреляция должны быть приблизительно постоянными во времени. Вместе с тем с ростом размера наборов данных [8] статистические модели не могут описывать нелинейные закономерности, чтобы охватить разнообразие, характерное для данных динамических последовательностей [9], какими являются данные мониторинга КС.

Методы машинного обучения (Machine Learning – ML), такие как дерево решений (Decision Tree), машины опорных векторов (Support Vector Machine – SVM), искусственные нейронные сети (Artificial Neural Network – ANN) и k-ближайшие соседи (k-Nearest Neighbors – kNN), в основном используются в реактивном режиме. Например, они могут быть использованы для обнаружения отказов в высокопроизводительной вычислительной системе [10]. Основным недостатком методов ML является относительно низкая точность прогнозирования.

Метаэвристические методы основываются на естественных (природных) алгоритмах [11] и считаются более высоким уровнем эвристического подхода, вместе с тем более обобщенными и менее зависимыми от предметной области. Эти алгоритмы заключаются в нахождении лучшего, но не обязательно оптимального решения за приемлемый промежуток времени. К этим алгоритмам относятся: генетические алгоритмы (Genetic Algorithms – GA) [12], оптимизация роя частиц (Particle Swarm Optimization – PSO) [13], оптимизация коралловых рифов (Coral Reefs Optimization – CRO) [14], оптимизация галактического роя (Galactic Swarm Optimization – GSO) [15], алгоритм оптимизации китов (Whale Optimization Algorithm – WOA) [16], а также их комбинация.

Искусственные нейронные сети являются одним из методов ML, который обеспечивает преимущества нелинейного моделирования. Считается, что глубокие нейронные сети способны изучать высокоуровневые функции с большей сложностью и абстракцией из-за большего количества скрытых слоев. Их можно эффективно использовать для достижения более высокой точности в задачах вывода [17].

Модели ГО широко используются в проактивном прогнозировании, а также в обнаружении аномалий в упорядоченных по времени данных [18]. Одной из моделей ГО являются рекуррентные нейронные сети (Recurrent Neural Network – RNN) [19] с внутренними замкнутыми ячейками. Благодаря способности моделировать длительные нелинейные зависимости во времени, RNN используются во многих областях. Однако в RNN имеются проблемы исчезающего градиента и «взрывного» роста градиента.

Для устранения недостатков RNN была разработана долговременная краткосрочная память − LSTM, которая является специальным блоком RNN [19]. LSTM может учиться на временных рядах с большими временными интервалами и считается наиболее точной благодаря своим характеристикам прогнозирования временных рядов. Она также обеспечивает большую согласованность в прогнозах во времени по сравнению с моделями машинного обучения, такими как дерево решений или SVM [20]. Обычный блок LSTM состоит из ячейки, входного элемента, выходного элемента и элемента забывания (рис. 2), которые описываются следующими уравнениями:

$$\text{входной элемент: } i_t = \sigma\left(x_t U^i + h_{t-1} W^i\right) \quad (1);$$

$$\text{элемент забывания: } f_t = \sigma\left(x_t U^i + h_{t-1} W^f\right) \quad (2);$$

$$\text{скрытое состояние: } \tilde{C}_t = tanh(x_t U^g + h_{t-1} W^g) \quad (3);$$

внутренняя память: $C_t = \sigma\left(f_t * C_{t-1} + i_t * \check{C}_t\right)$ (4);

выход скрытого состояния: $h_t = tahn(C_t) * o_t$ (5);

выходной элемент: $o_t = \sigma(x_t U^o + h_{t-1} W^o)$, (6),

где x является входным вектором; W^i, W^f, W^g, W^o − повторяющееся соединение на предыдущем и текущем скрытом слое; U − весовая матрица, соединяющая входы с текущим скрытым слоем; $*$ − операция поэлементного умножения и игнорирования смещения; σ − логистическая сигмоидная функция; $\tilde{C}$ − скрытое состояние, вычисленное на основе текущего входа и предыдущего скрытого состояния.

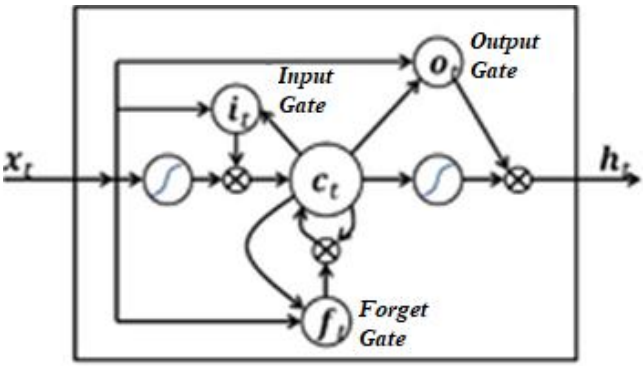

Рис. 2. Долговременная краткосрочная память (LSTM)

Имеются различные варианты LSTM, такие как двунаправленный LSTM (Bidirectional LSTM) [21], LSTM на основе внимания (Attention-based LSTM – AT-LSTM) [22], составные LSTM (Stacked LSTM) и т.д.

Связанные работы

В работе [23] предлагается метод проактивного мониторинга для обеспечения безопасности и защиты вычислительных сетей. Авторы предлагают интеллектуальный модуль в виде приложения машинного обучения с использованием моделирования глубокого обучения, чтобы расширить функциональные возможности системы обнаружения вторжений, контролирующей потоки сетевого трафика. Правильное объединение ГО и масштабируемой предварительной обработки данных обеспечивают высокое качество и стабильность работы модели в динамических и быстро меняющихся средах, например, в мониторинге сетевого трафика.

В работе [24] изучаются вопросы влияния приложений на потребление ресурсов в компьютерных сетях. Исследование сосредоточено на анализе показателей производительности, собранных из реальных сетей с использованием скриптов и доступных программ, созданных специально для мониторинга приложений и сети в режиме реального времени. Однако мониторинг производительности в реальном времени не дает точной или сжатой информации о причинах любого снижения производительности сети или приложений. Анализ показателей производительности за определенный период и обнаружение корреляции между показателями и приложениями дают гораздо более актуальную информацию о первопричине проблем. Автор использует методы прогнозной аналитики, машинного обучения и бизнес-аналитики, чтобы предсказать, может ли приложение ухудшить производительность сети или потреблять ресурсы компьютерных

сетей. Результаты показали, что существует корреляция между определенными показателями производительности, помимо корреляции, обнаруженной между показателями и приложениями.

В работе [25] предлагается кооперативная IDS (Intrusion Detection System) на основе машинного обучения, которая эффективно использует исторические данные обратной связи, чтобы обеспечить возможность проактивного принятия решений. В частности, предлагаемая модель основана на DA (Denoising Autoencoder), который используется для построения глубокой нейронной сети. Преимущество DA заключается в способности к восстановлению обратной связи IDS на основе частичной обратной связи. Это позволяет заблаговременно принимать решения о подозрительных вторжениях даже при отсутствии полной обратной связи из IDS.

В работе [26] предлагается проактивный мониторинг для гетерогенных сетей, в котором выполняются управляющие действия, чтобы избежать возникновения ситуаций, на которые необходимо реагировать. В случае возникновения таких ситуаций проактивный мониторинг позволяет на них реагировать, как в стандартной реактивной системе. Была представлена идея объединения методов пассивного и активного мониторинга сети в проактивную систему и предложена архитектура системы проактивного мониторинга.

Метод интеллектуального проактивного мониторинга КС

Постановка задачи. Как упоминалось выше, одним из основных требований для проактивного мониторинга КС является точность прогнозов. Известно, что точность прогнозирования характеризует способность метода прогнозирования прогнозировать как можно больше истинных проблем, генерируя при этом как можно меньше ложных тревог [27]. Точность прогнозов при проактивном мониторинге КС очень важна, поскольку точные прогнозы позволяют определить больше истинных проблем и, следовательно, инициируют больше необходимых действий, направленных на предотвращение или смягчение прогнозируемых проблем. При этом каждое пропущенное необходимое действие может привести к упущению возможности предотвращения или смягчения конкретной проблемы КС. С другой стороны, точные прогнозы инициируют меньше ложных срабатываний и, следовательно, меньше ненужных действий. Обычно при ненужных действиях используются дополнительные время и ресурсы системы и администратора сети, при этом не решаются реальные проблемы КС. С другой стороны, эти прогнозы должны быть ранними, поскольку это тоже очень важно для эффективности мониторинга, так как для действий по предотвращению или смягчению прогнозируемых проблем КС остается больше времени. Однако между этими двумя требованиями существует важный компромисс, то есть необходимо определить компромисс между точностью прогноза и своевременностью. По сути, более поздние прогнозы обычно имеют более высокую точность, поскольку доступно больше информации о текущем состоянии КС. Чтобы решить эту проблему, предлагается использовать ансамбль моделей ГО, которые могут производить прогнозы в произвольных моментах времени и позволить оценить надежность (reliability) для каждого прогноза. Оценки надежности, вычисленные из ансамбля моделей прогнозирования, могут обеспечить более точные оценки вероятности того, что индивидуальный прогноз верен.

Ансамбль глубокого обучения для проактивного мониторинга КС. Для проактивного мониторинга КС используется однородный ансамбль, который состоит из одинокого базового алгоритма обучения (рис. 3). В качестве базового алгоритма обучения используется модель LSTM. Известно, что прогнозирование на основе ансамбля является методом мета-прогнозирования, в котором прогнозы m моделей объединяются в один прогноз [28].

Предположим, что прогнозы можно делать на различных этапах (точках) выполнения мониторинга КС (например, определенные моменты времени – часы, дни, месяцы). При этом точка, для которой делается прогноз, принимается в качестве контрольной точки.

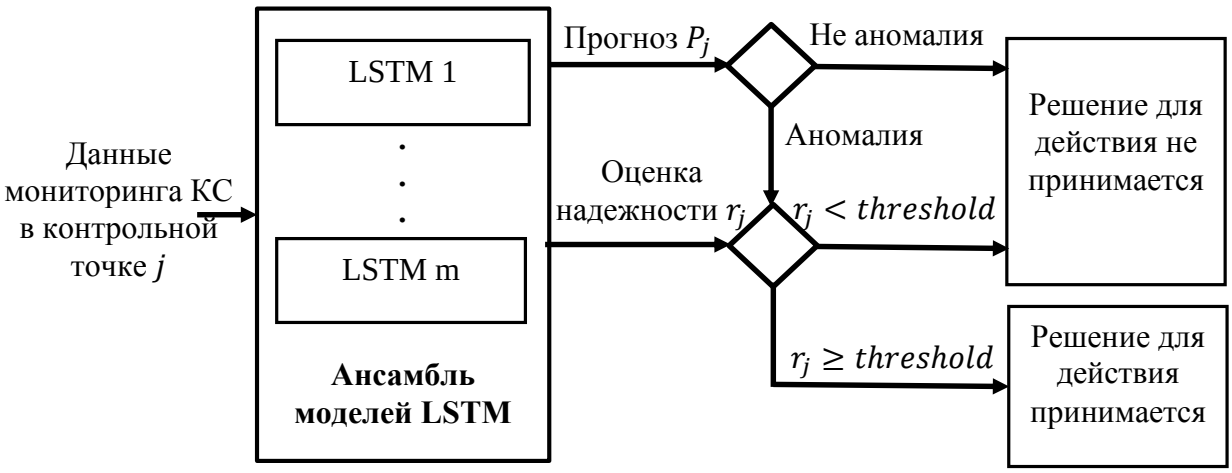

Рис. 3. Ансамбль LSTM для проактивного мониторинга КС

Предложенный метод заключается в том, что ансамбль моделей LSTM на основании данных мониторинга КС создает прогноз P_j в каждой потенциальной контрольной точке j (рис. 3) процесса мониторинга и обеспечивает оценку надежности r_j для этого прогноза. Если ансамбль прогнозирует проблему КС в контрольной точке j, то может потребоваться решение для действия по предотвращению или смягчению спрогнозированной проблемы. Однако при этом решение для действия по предотвращению или смягчению проблемы КС принимается только в том случае, если надежность прогноза r_i равна или превышает предварительно определенный порог (threshold), то есть, если прогноз является достаточно надежным.

Для вычисления ансамблевых прогнозов P_j и оценок надежности r_j для каждой контрольной точки j используется стратегия, определенная в [29]. Предполагается, что в каждой контрольной точке j каждая из базовых моделей ансамбля предоставляет результат прогнозирования $P_{i,j}$ $(i = 1, \dots, m)$, где $P_{i,j}$ относится к классу «аномалия» или «не аномалия». При этом прогноз ансамбля для контрольной точки j вычисляется по следующей форме:

$$P_j = \begin{cases} \text{«аномалия»}, & \left|i : P_{i,j} = \text{«аномалия»}\right| \geq m/2 \\ \text{«не аномалия»}, & \text{в противном случае.} \end{cases}$$

Оценка надежности r_j прогноза P_j вычисляется как доля базовых моделей, которые предсказали большинство классов:

$$r_j = max_{i=1,\dots,m}\left(\frac{\left|i: P_{i,j} = \text{«аномалия»}\right|}{m}, \frac{\left|i: P_{i,j} = \text{«не аномалия»}\right|}{m}\right)$$

Для создания базовых моделей обучения ансамбля LSTM используется «Bagging»-алгоритм [28]. «Bagging»-алгоритм генерирует m новых наборов обучающих данных из всего обучающего набора путем однородной выборки из всего обучающего набора данных с заменой. Для каждого из m новых наборов обучающих данных обучаются отдельные

модели LSTM. При этом использование «Bagging»-алгоритма обеспечивает масштабируемость подхода, поскольку обучение базовых алгоритмов обучения может происходить параллельно. «Bagging»-алгоритм имеет следующий вид:

Input: Data set $D = \{(x_1 y_1), (x_2 y_2), \dots, (x_m y_m)\}$;
Base learning algorithm £;
Number of base learners T.
Process:
1. for $\boldsymbol{t = 1, \dots, T}$:
2. $\boldsymbol{h_i} = £(\boldsymbol{D}, \mathfrak{D}_{\boldsymbol{bs}})$ % $\mathfrak{D}_{\boldsymbol{bs}}$ is the bootstrap distribution
3. end
Output: $H(x) = \arg\max_{y \in Y} \sum_{t=1}^{T} [\![(h_t(x) = y)]\!]$

Заключение

Для обеспечения бесперебойного и безопасного функционирования КС ключевым шагом является создание эффективной инфраструктуры интеллектуального мониторинга. При этом всеобъемлющий мониторинг может способствовать лучшему пониманию функционирования КС в целом и планированию ее будущего расширения.

Обычно в процессе мониторинга КС приходится собирать, хранить и анализировать огромные объемы данных мониторинга, и эффективность мониторинга зависит от качества собранных данных и точности используемых методов анализа данных.

Традиционно администраторы сетей находят проблемы КС, вручную просматривая собранные данные мониторинга. Однако этот метод поиска проблем КС устарел и не позволяет учитывать всевозможные проблемы. Для решения этой задачи необходимо проактивно определить нормальный профиль и прогнозировать поведение КС на ближайшее будущее, основываясь на предыдущее нормальное поведение. При этом основной задачей является эффективное управление сбором, хранением, анализом и предоставлением большого объема мониторинговых данных.

В данной работе для обеспечения проактивности мониторинга КС предлагается концептуальная модель системы интеллектуального проактивного мониторинга КС. При этом основной функцией проактивного мониторинга КС является раннее выявление тенденций и закономерностей как в сетевом трафике и приложениях, так и в компонентах сети.

Проактивность мониторинга КС основывается на прогнозировании поведения сети, чтобы предсказать потенциальные проблемы КС. При этом одним из основных требований к проактивному мониторингу КС является точность прогнозов, поскольку позволяет определить больше истинных проблем. При этом прогнозы должны быть ранними, поскольку это тоже очень важно для эффективности мониторинга, так как для действий по предотвращению или смягчению прогнозируемых проблем КС остается больше времени.

Одной из основных задач при проактивном мониторинге КС является необходимость определения компромисса между точностью прогноза и своевременностью. По сути, более поздние прогнозы обычно имеют более высокую точность, поскольку доступно больше информации о текущем состоянии КС. Для решения этой задачи предлагается использовать ансамбль моделей глубокого обучения, состоящий из одинокого базового алгоритма обучения (однородный ансамбль), которые могут производить прогнозы в произвольных моментах времени и позволить оценить надежность (reliability) для каждого прогноза. Оценки надежности, вычисленные из ансамбля моделей прогнозирования, могут обеспечить более точные оценки вероятности того, что индивидуальный прогноз верен.

В качестве базового алгоритма обучения используется модель LSTM. Для создания базовых моделей обучения ансамбля LSTM используется «Bagging»-алгоритм.

Литература

1. M. Dilman and D. Raz Efficient Reactive Monitoring // IEEE Journal on Selected Areas in Communications, vol. 20, no. 4, 2002, pp. 668−676.
2. R. Khan, S. U. Khan, R. Zaheer and M. I. Babar An Efficient Network Monitoring and Management System // International Journal of Information and Electronics Engineering, vol. 3, no. 1, 2013, pp.122−126.
3. S. Lee, K. Levanti, H. S. Kim Network monitoring: Present and future // Computer Networks vol. 65, no. 2, 2014, pp. 84–98.
4. V. Sekar, M. K. Reiter, W. Willinger, H. Zhang, R. R. Kompella, David G. Andersen CSAMP: A System for Network-Wide Flow Monitoring / Proceedings of the 5th USENIX Symposium on Networked Systems Design & Implementation, 2008, pp. 233−246.
5. T. Fu, A review on time series data mining // Engineering Applications of Artificial Intelligence, vol. 24, no. 1, 2011, pp. 164−181.
6. Makridakis S., Spiliotis E. and Assimakopoulos V. Statistical and machine learning forecasting methods: Concerns and ways forward // PLOS ONE, vol. 13, no. 3, 2018, 26 p. https://dx.plos.org/10.1371/journal.pone.0194889
7. Baptista M., Sankararaman S., de Medeiros I. P., Nascimento C., Prendinger H. and Henriques E. M. Forecasting fault events for predictive maintenance using data-driven techniques and arma modeling // Computers Industrial Engineering, vol. 115, 2018, pp. 41–53.
8. Cerqueira V., Torgo L. and Soares C. Machine learning vs statistical methods for time series forecasting: Size matters, arXiv preprint arXiv:1909.13316, 2019. Available: https://arxiv.org/abs/1909.13316
9. Kajitani Y., Hipel K. W. and Mcleod A. I. Forecasting nonlinear time series with feed-forward neural networks: a case study of canadian lynx data // Journal of Forecasting, vol. 24, no. 2, 2005, pp. 105−117.
10. Mohammed B., Awan I., Ugail H. and Younas M., Failure prediction using machine learning in a virtualised hpc system and application // Cluster Computing, 2018, pp. 1−15.
11. Abdel-Basset M., Abdel-Fatah L. and Sangaiah A. K. Metaheuristic algorithms: A comprehensive review // Computational Intelligence for Multimedia Big Data on the Cloud with Engineering Applications. Elsevier, 2018, pp. 185−231.
12. Holland J. H., Adaptation in Natural and Artificial Systems, An Introductory Analysis with Applications to Biology, Control, and Artificial Intelligence. The MIT Press, 1992, 211 p.
13. Kennedy J. Particle swarm optimization // Encyclopedia of machine learning, 2010, pp. 760–766.
14. Salcedo-Sanz S., Del Ser J., Landa-Torres I., Gil-López S., and Portilla-Figueras J., The coral reefs optimization algorithm: a novel metaheuristic for efficiently solving optimization problems // The Scientific World Journal, vol. 2014, 2014.
15. Muthiah-Nakarajan V. and Noel M. M. Galactic swarm optimization: A new global optimization metaheuristic inspired by galactic motion // Applied Soft Computing, vol. 38, 2016, pp. 771–787.
16. Mirjalili S. and Lewis A. The whale optimization algorithm // Advances in Engineering Software, vol. 95, 2016, pp. 51–67.
17. Goodfellow I., Bengio Y. and Courville A., Deep Learning (AdaptiveComputation and Machine Learning series). MIT press, 2016.
18. Gamboa J. C. B. Deep learning for time-series analysis // arXiv preprint arXiv:1701.01887, 2017. https://arxiv.org/abs/1701.01887
19. Hochreiter S. and Schmidhuber J. Long short-term memory // Neural computation, vol. 9, no. 8, 1997, pp. 1735–1780.

20. Bruneo D. and De Vita F. On the use of lstm networks for predictive maintenance in smart industries / IEEE International Conference on Smart Computing. IEEE, 2019, pp. 241−248.
21. Schuster M. and Paliwal K. Bidirectional recurrent neural networks // IEEE Transactions on Signal Processing, vol. 45, no. 11, 1997, pp. 2673−2681.
22. Luong T., Pham H. and Manning C. D. Effective approaches to attention-based neural machine translation, 2015, pp. 1412−1421.
23. G. Nguyen, S. Dlugolinsky, V. Tran, Á. L. García Deep learning for proactive network monitoring and security protection, IEEE Access, vol. 8, 2016, pp. 19696−19716.
24. Elmasry M. Predict Network Application Performance Using Machine Learning and Predictive Analytics / Thesis, Rochester Institute of Technology, 2019.
25. A. Abusitta, M. Bellaiche, M.Dagenais, T. Halabi A deep learning approach for proactive multi-cloud cooperative intrusion detection system // Future Generation Computer Systems vol. 98, 2019, pp. 308−318.
26. J. R.de Santiago Proactive Measurement Techniques For Network Monitoring In Heterogeneous Environments / Doctoral thesis, Universidad Autónoma de Madrid, 2013.
27. Salfner, F., Lenk, M., Malek, M.: A survey of online failure prediction methods // ACM Computing Surveys vol. 42, no. 3, 2010, pp.1−42.
28. R.Herbrich and T. Graepel, Ensemble Methods: Foundations and Algorithms, Taylor & Francis Group, LLC, 2012, 222 p.
29. A. Metzger and F. Focker, Predictive Business Process Monitoring Considering Reliability Estimates / International Conference on Advanced Information Systems Engineering CAISE 2017, pp 445−460.

UOT 004.853

Ramiz Şıxəliyev H.
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
ramiz@science.az

Kompüter şəbəkələrinin intellektual proaktiv monitorinqi metodu haqqında

Məqalədə kompüter şəbəkələrinin (KŞ) intellektual proaktiv monitorinqi üçün konseptual metod təklif olunur. KŞ-nin proaktiv monitorinqini təmin etmək üçün süni intellekt metodlarından, xüsusən də dərin təlim (DT) metodundan istifadə etmək təklif olunur. Ənənəvi monitorinq sistemlərində ümumiyyətlə proaktiv monitorinq funksiyası yoxdur. Bu gün KŞ-nin kifayət qədər hesablama gücünə, buraxma zolağının genişliyinə və böyük yaddaşa malik olmasına baxmayaraq, böyük həcmli monitorinq verilənlərindən mühüm hadisələrin müəyyənləşdirilməsi problem olaraq qalır. Nəticə etibarilə, KŞ problemlərinin vaxtında aşkarlanmaması şəbəkənin və şəbəkə xidmətlərinin işinin və KŞ-nin təhlükəsizliyinin pozulmasına səbəb ola bilər. Ənənəvi monitorinqdən fərqli olaraq, intellektual proaktiv monitorinq KŞ-nin vəziyyəti haqqında daha çox məlumat verə bilər. KŞ-nin proaktiv monitorinqi şəbəkənin davranışını proqnozlaşdırmağa əsaslanır. Eyni zamanda, KŞ-nin intellektual proaktiv monitorinqi üçün əsas tələblərdən biri, proqnozlaşdırma metodunun imkanını xarakterizə edən proqnozların dəqiqliyidir. KŞ-nin proaktiv monitorinqi zamanı proqnozların dəqiqliyinə nail olmaq üçün vahid baza öyrənmə alqoritmindən ibarət olan bircins ansambldan istifadə olunur. Əsas öyrənmə alqoritmi kimi LSTM (Long Short-Term Memory) modeli istifadə olunur. LSTM ansamblı üçün əsas öyrənmə modelləri yaratmaq üçün "Bagging" alqoritmindən istifadə olunur. Bu işdə təklif olunan metod KŞ-lərin problemlərinin proqnozlaşdırılmasının nisbətən yüksək dəqiqliyini təmin etməyə imkan verəcək, buna görə də KS-nin proaktiv monitorinq sisteminin kifayət qədər səmərəliliyini təmin edəcəkdir.

***Açar sözlər**: kompüter şəbəkələri, kompüter şəbəkələrinin proaktiv monitorinqi, dərin təlim, LSTM, proqnozlaşdırma.*

Ramiz H. Shikhaliyev
Institute of Information Technology of ANAS, Baku, Azerbaijan
ramiz@science.az

One method for intellectual proactive monitoring of computer networks

The article proposes a method for intelligent proactive monitoring of computer networks (CN). To ensure proactive monitoring of the CN, it is proposed to use artificial intelligence methods, in particular, deep learning (DL). Network monitoring systems now work well in near real-time. However, traditional monitoring systems generally do not have a proactive monitoring function. Despite the fact that today the CN has sufficient computing power, bandwidth and memory, the identification of important events among the huge volumes of monitoring data remains a problem. Consequently, untimely detection of CN problems can lead to network disruptions, the provision of network services and a decrease in CN security. Unlike traditional monitoring, intelligent proactive monitoring can provide more information about the state of the CN. Proactive monitoring of the CN is based on predicting the behavior of the network. At the same time, one of the main requirements for intelligent proactive monitoring of CN is the accuracy of predictions, which characterizes the ability of the prediction method. To achieve the accuracy of predictions during proactive monitoring of the CN, a homogeneous ensemble is used, which consists of a single basic learning algorithm. As a basic learning algorithm. the LSTM (Long Short-Term Memory) model is used. To create basic learning models for the LSTM ensemble, the "Bagging" algorithm is used. The method proposed in this work will make it possible to ensure a relatively high accuracy of prediction the problems in the CN, therefore, to ensure sufficient efficiency of the proactive monitoring system of the CN.

Keywords*: computer networks, proactive monitoring of computer networks, deep learning, LSTM, prediction.*