ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ В ЗАДАЧАХ ОБНАРУЖЕНИЯ DDoS-АТАК ПРИКЛАДНОГО УРОВНЯ

К.Ф. Слесарчик

Академия ФСО России, Орел, Российская Федерация

Рассматривается способ обнаружения распределенных атак на отказ в обслуживании, направленных на прикладной уровень инфокоммуникационной сети. Рассмотрены особенности применения искусственных нейронных сетей в задаче обнаружения DDoS-атак прикладного уровня.

Ключевые слова: низкоинтенсивная атака, деструктивное информационное кибернетическое воздействие, многовекторная DDoS-атака, искусственная нейронная сеть, прикладной уровень.

THE USE OF ARTIFICIAL NEURAL NETWORKS IN TASKS OF DETECTION OF DDoS ATTACKS APPLICATION LAYER

K.F. Slesarchik

Academy FSO of Russia, Orel, Russian Federation

The article deals with the method of detection of distributed denial - of-service attacks aimed at the applied level of the infocommunication network. The features of application of artificial neural networks in the problem of detection of DDoS-attacks of the applied level are considered.

Keywords: low-intensity attack; destructive information cybernetic impact; multi-vector DDoS-attack; artificial neural network; application level.

Введение

Анализ статистики деструктивных информационных кибернетических воздействий (ДИКВ) за 2018 год показал, что более 34 % всех DDoS-атак проводились в отношении протоколов прикладного уровня (рис. 1), при этом более 8 % атак от общего числа пришлось на протоколы HTTP(S) (рис. 2). Анализ динамики DDoS-атак на HTTP и HTTPS протоколы указывает на выравнивание интереса злоумышленников к использующим их службам инфокоммуникационной сети (рис. 3) [1].

Рис. 1. Соотношение количества атак на протоколы прикладного и сетевого уровня

Наиболее часто используемые методы обнаружения и идентификации DDoS-атак представлены [2]. Они обладают рядом недостатков, усложняющих их применение для обнаружения DDoS-атак прикладного уровня, например применение статистических методов вызывает проблему определения граничных (пороговых) значений отслеживаемых характеристик.

Рис. 2. Соотношение видов DDoS-атак в 2018 году

Рис. 3. Динамика DDoS-атак на HTTP и HTTPS протоколы

Исключение составляют методы на основе мягких решений, но и они имеют недостатки, снижающие эффективность их применения, главный из которых необходимость предварительного обучения. Кроме того, точность результатов полученных на основе методов мягких решений, зависит от качества наборов характеристик атаки [3].

В работе предлагается использовать метод анализа динамики градиента характеристик трафика для обнаружения DDoS-атак на протоколы прикладного уровня [3].

Метод обнаружения DDoS-атаки через анализ динамики градиента характеристик трафика предполагает анализ траектории движения показателя тревоги $\overline{K_{тр}}$, который описывается выражением (1) и является точкой, взятой в ортонормированном базисе пространства состояний, независимых функций:

$$\overline{K_{тр}} = [P_1, \dots, P_N], N = 1, 2, 3 \dots \quad (1)$$

где $P_1, \dots, P_N$ – признаковые характеристики DDoS-атаки.

Признаковые характеристики DDoS-атаки должны удовлетворять условию: при появлении элементов атаки в анализируемом трафике они стремятся к нулевым значениям; чем больше таких элементов, тем выше динамика градиента движения точки к нулевой координате, описываемой $\overline{K_{тр}}$ (рис. 4).

Рис. 4. Метод обнаружения DDoS-атаки через анализ динамики градиента характеристик трафика

Расстояние между точками $\overline{K_{тр}}$ будем называть метрикой M . Значение M используется для описания траектории движения $\overline{K_{тр}}$. Типовые траектории движения $\overline{K_{тр}}$ могут быть описаны системами неравенств:

$$\begin{aligned}
 &\left\{ \begin{array}{l} M_1 > 0, \\ M_2 > 0, \\ |M_2| > |M_1| \end{array} \right. \quad (a) \quad \left\{ \begin{array}{l} M_1 < 0, \\ M_2 > 0, \\ |M_2| - |M_1| > |M_1| \end{array} \right. \quad (б) \quad \left\{ \begin{array}{l} M_1 > 0, \\ M_2 > 0, \\ |M_2| < |M_1| \end{array} \right. \quad (в) \quad \left\{ \begin{array}{l} M_1 < 0, \\ M_2 > 0, \\ |M_2| - |M_1| < |M_1| \end{array} \right. \quad (г) \\
 &\left\{ \begin{array}{l} M_1 < 0, \\ M_2 < 0, \\ |M_2| > |M_1| \end{array} \right. \quad (д) \quad \left\{ \begin{array}{l} M_1 > 0, \\ M_2 < 0, \\ |M_2| - |M_1| > |M_1| \end{array} \right. \quad (е) \quad \left\{ \begin{array}{l} M_1 > 0, \\ M_2 > 0, \\ |M_2| < |M_1| \end{array} \right. \quad (ж) \quad \left\{ \begin{array}{l} M_1 > 0, \\ M_2 < 0, \\ |M_2| - |M_1| < |M_1| \end{array} \right. \quad (з) \quad (2)
 \end{aligned}$$

Особое внимание следует уделить варианту траектории движения $\overline{K_{тр}}$ – «раскачивание» (рис. 5), траектория описывается системой неравенств:

$$\left\{ \begin{array}{l} M_{1i} < 0, \\ M_{2i} + M_{1i} > 0, \\ M_{1i-1} < 0, \\ M_{2i-1} + M_{1i-1} > 0, \\ M_{1i-2} < 0, \\ M_{2i-2} + M_{1i-2} > 0, \end{array} \right. \quad (3)$$

Рис. 5. Траектории движения метрик показателя тревоги при атаке «раскачивания»

Обнаружение DDoS-атак прикладного уровня

Рассмотрим использование метода обнаружения DDoS-атаки через анализ динамики градиента характеристик трафика для идентификации атак прикладного уровня на примере «низкоинтенсивной» DDoS-атаки на HTTP(S) протокол.

Возможность проведения низкоинтенсивной DDoS-атаки объясняется уязвимостью протокола HTTP и необходимостью обязательного ожидания сервером конца передачи POST-запроса. При реализации низкоинтенсивной DDoS-атаки злоумышленник фрагментирует POST-запрос на пакеты малой длины и отправляет их серверу с периодичностью меньше, чем значение времени ожидания окончания соединения. В результате чего сервер вынужден ожидать окончания приема POST-запросов злоумышленника, в тот момент как запросы легитимных пользователей игнорируются ввиду отсутствия свободного ресурса, при этом общий объем трафика DDoS-атаки ниже объема обычного трафика к службе HTTP (рис. 6).

Рис. 6. Сравнение объемов общего и вредоносного при низкоинтенсивной DDoS-атаке на протоколы HTTP и HTTPS

Низкоинтенсивная DDoS-атака характеризуется продолжительными периодами между передачей пакетов для одной сессии и большим значением фрагментации пакетов в данной сессии для передачи контентной информации.

Низкоинтенсивная атака включает два этапа (рис. 7): начальный (характеризуется резким увеличением динамики скорости градиента показателя тревоги в направлении нулевой координаты) и насыщения (постепенное уменьшение градиента показателя тревоги) [3]. Траектории движения показателя тревоги при проведении атаки можно описать системами неравенств (2а, б, д, е, и) и (3).

Рис. 7. Траектории движения показателя тревоги при проведении «низкоинтенсивной» DDoS-атаки на протокол HTTP(S)

Для идентификации вышеперечисленных траекторий необходимо проверить десять условий (табл. 1): строки 1–2 и 9 – начальный этап атаки; 3–4 – этап насыщения DDoS-соединениями.

Таблица 1

Условия идентификации атаки по траектории показателя тревоги

	Траектория движения показателя тревоги	Результат выполнения условия					
	Формулировка условия	$M_1 > 0$	$M_2 > 0$	$ M_2 > M_1 $	$ M_2 - M_1 > M_1 $	$ M_2 < M_1 $	$ M_2 - M_1 < M_1$
к нулевой координате с увеличением скорости							
1	А)	истина	истина	истина	–	–	–
2	Б)	ложь	истина	–	истина	–	–
от нулевой координаты с увеличением скорости							
3	Д)	ложь	ложь	истина	–	–	–
4	Е)	истина	ложь	–	истина	–	–
к нулевой координате с уменьшением скорости							
5	В)	истина	истина	–	–	истина	–
6	Г)	ложь	истина	–	–	–	истина
от нулевой координаты с уменьшением скорости							
7	Ж)	истина	истина	–	–	истина	–
8	З)	истина	ложь	–	–	–	истина
атака «раскачивания»							
	Формулировка условия	$M_{1i} < 0$	$M_{2i} + M_{1i} > 0$	$M_{1i-1} < 0$	$M_{2i-1} + M_{1i-1} > 0$	$M_{1i-2} < 0$	$M_{2i-2} + M_{1i-2} > 0$
9	И)	истина	истина	истина	истина	истина	истина

С учетом условий (2а, б, д, е, и) и (3) для идентификации траекторий атаки используется искусственная нейронная сеть (ИНС), схема нейрузла показана на рисунке рис. 8. Нейрузел представляет собой четырехслойную ИНС по 11 нейронов в слое с одиннадцатью входами и двумя выходами.

Рис. 8. Узел обнаружения низкоинтенсивной DDoS-атаки на основе искусственной нейронной сети

При обучении ИНС с целью сужения бесконечного множества возможных значений показателя тревоги на входе нейронной сети до конечного дискретного на входы ИНС подаются результаты операций сравнения систем неравенств (см. табл. 1). На входы нейроузла будут поступать одиннадцать результатов сравнения, образующих множество значений мощностью 2^{11} , элементы множества принимают одно из двух возможных значения: «0» и «1».

Обучение ИНС производилось методами, описанными в [4–6]. В результате по окончании обучения были правильно распознаны все представленные комбинации, а среднее значение абсолютной погрешности по всему набору обучающей выборки составило значение $7,329 \cdot 10^{-15}$, что свидетельствует о достаточной точности результатов идентификации, получаемых с использованием обученной ИНС.

Выводы

На примере «низкоинтенсивной» DDoS-атаки показана возможность обнаружения атак прикладного уровня посредством метода анализа динамики градиента характеристик трафика. Для реализации идентификации траекторий движения показателя тревоги выбран аппарат ИНС.

Применяя метод анализа динамики градиента характеристик трафика, можно обнаруживать многовекторные DDoS-атаки на протоколы прикладного уровня посредством использования совокупности нейроузлов, объединенных по выходным нейронам (рис. 9).

На рис. 9 представлена схема узла обнаружения многовекторной атаки вида LowDDoS-memcached-SSDP на основе ИНС.

Классификатор трафика реализован на основе однослойной ИНС с 88 входами и 7 выходами с вероятностью ошибки классификации, не превышающей значение 10^{-4} . На основе

параметров, выдаваемых классификатором, для каждого окна анализа рассчитываются вероятностные и энтропийные характеристики. Для каждого базиса рассчитываются метрики и определяются результаты их сравнений, которые подаются на входы соответствующих нейроузлов анализатора.

Рис. 9. Схема обнаружения многовекторной DDoS-атаки с помощью нейроузлов

В результате реализации предложенного способа идентификации DDoS-атак на существующих ПЛИС как импортного, так отечественного производства (с частотами 200-750 МГц) может быть достигнуто значение скорости анализируемого трафика в 10 Гб/с (табл. 2). Узким местом в данном случае является реализация классификатора пакетов, скорости работы непосредственно анализатора DDoS-атак в 10 раз выше.

Таблица 2

Возможности современных ПЛИС

Семейства ПЛИС	Число логических элементов	Мах объем памяти, Кбайт	Тактовая частота, МГц	Мах скорость трафика при решении задач	
				Классификация пакетов	Анализ DDoS-атак
APEX20K фирмы ALTERA	466944	38	66	100 Мб/с	500 Мб/с
Virtex фирмы XILINX	21 168	36,75	>500	1 Гб/с	>100 Гб/с
Actel Corporation	16000	61,57	>250	350 Мб/с	>10 Гб/с
Speedster22i HD Achronix	1725000	145000	>2800	10 Гб/с	>100 Гб/с

СПИСОК ЛИТЕРАТУРЫ

1. Threat Report Distributed Denial of Service (DDoS) Q1-Q4 2018, Q1 2019. URL: <https://www.nexusguard.com/> (дата обращения: 05.07.2019).
2. Браницкий А.А., Котенко И.В. Анализ и классификация обнаружения сетевых атак // Труды СПИИРАН. 2016. Вып. 2 (45). С. 204–244.
3. Слесарчик К.Ф. Анализатор низкоинтенсивных DDoS-атак со случайной динамикой характеристик периодичности и фрагментации // Техника радиосвязи. № 1 (40). 2019. С.67–81. DOI: 10.33286/2075-8693-2019-40-67-88.

4. Хайкин С. Нейронные сети: полный курс / пер. с англ. Н.Н. Куссуль, А.Ю. Шелестова. 2-е изд., испр. М.: Вильямс, 2008. 1103 с.
5. Sorsa A., Peltokangas R. Real-coded genetic algorithms and nonlinear parameter identification, University of Oulu, Control Engineering Laboratory, Report A №34, April 2008. 32 p.
6. Дударов С.П. Математические основы генетических алгоритмов: учеб. пособие. М.: РХТУ им. Д.И. Менделеева, 2012. 56 с.