Нейронечеткая система классификации инцидентов кибербезопасности в условиях неопределенности

Д.И. Парфёнов[1], И.П. Болодурина[1], Л.С. Забродина[1], А.Ю. Жигалов[1]

[1]*Оренбургский государственный университет, проспект Победы 13, Оренбург, Россия, 460018*

Аннотация

В данной статье представлена нейронечеткая сеть ANFIS, позволяющая проводить идентификацию и классификацию аномального трафика сети. Экспериментально установлено, что предложенное решение позволяет идентифицировать сетевые атаки с точность 84,79%, что сопоставимо по точности с алгоритмами случайного леса, экстра-деревьев и классификатора на основе многослойного персептрона.

Ключевые слова

Нечеткая нейронная сеть, сетевые атаки, ANFIS, база знаний, нечеткие правила

1. Введение

В настоящее время большую актуальность приобрели вопросы обеспечения безопасности вычислительных сетей [1]. При этом современным системам обнаружения вторжений приходится проводить анализ сетевого трафика в условиях неопределенности [2-3], формирующимися из-за сниженного качества исходных данных. Существуют объективные показатели неопределенности (пропущенные значения, шумы и др.) и лингвистическая неопределенность, возникающая из-за субъективной оценки эксперта или группы экспертов. Данная работа направлена на разработку решения, основанного на нейронечеткой сети ANFIS, которая на базе нечетких правил позволяет снизить лингвистическую неопределенность и осуществить эффективную классификацию аномального трафика.

2. Основная часть

Рассмотрим типовую конфигурацию сети, в которой необходимо провести идентификацию фрагментов аномального трафика. Пусть данные сетевого трафика поступают непрерывно и фиксируются как множество записей $R=\{r_1, r_2, ..., r_m\}$, где каждая запись $r_i=\{r_{i1}, r_{i2}, ..., r_{ik}\}$ представляет собой набор характеристик, фиксируемых в параметрах трафика.

Каждый объект сети соответствует подмножеству фиксируемых на нем характеристик трафика с соответствующими метками классов различных типов атак $Y=\{1, ..., K\}$, включающими нормальное поведение устройств сети. Требуется построить многоклассовый классификатор $f_c(R): R \to Y$, который каждому элементу множества записей сетевого трафика с некоторых объектов сети $R=\{r_1, r_2, ..., r_m\}$ сопоставляет метку y_j, определяющую тип атаки.

Рассмотрим структуру адаптивной нейро-нечеткой системы вывода ANFIS для решения задачи идентификации сетевых атак:

Слой 1. Входной слой сети представляет собой значения признаков некоторой записи объектов, которые представляют собой количественные или качественные характеристики.

Слой 2. Слой фаззификации сопоставляет значениям признаков значения лексических переменных и вычисляет степени принадлежности к заданным нечетким множествам.

Слой 3. Слой нечетких правил позволяет оценить принадлежность полученных значений нечетких переменных к определенным меткам класса.

Слой 4. Слой вычисляет нормированные уровни активации правил и дает возможность построить единую систему оценки важности результатов нечетких правил и их градации.

Слой 5. Выполняет дефаззификацию результатов и приведение их к четкости.

Слой 6. Данный слой предназначен для взвешенного суммирования значений предыдущего слоя и формирует единый результат – метку класса.

Для эффективного подбора параметров весовых коэффициентов на основе размеченного набора данных UNSW-NB15 использован алгоритм *Back propagation*. Результаты экспериментов показали, что нейронечеткий классификатор ANFIS позволяет определять тип сетевой атаки с точностью 84,79%. Наибольшую точность нейронечеткий классификатор показал при идентификации таких атак как Exploits, Fuzzers, DoS и Generic.

В рамках эксперимента алгоритм нейронечеткой классификации ANFIS сопоставлен по точности с другими методами машинного обучения: *Случайный лес* (Random Forest), *Экстра-деревья* (ExtraTree) и *многослойный классификатор персептрона* (MLP).

Таблица 1

Результаты сравнительного анализа эффективности методов идентификации сетевых атак

Методы	Точность	F1- мера	Полнота
ANFIS	0,914	0,891	0,911
Random Forest	0,871	0,771	0,869
ExtraTree	0,863	0,894	0,929
MLP	0,747	0,721	0,743

Система нейронечеткой классификации ANFIS в целом показала хорошую обобщающую способность относительно MLP, однако алгоритм ExtraTree в свою очередь показал преимущество согласно F-мере, так как является ансамблевым методом.

3. Заключение

В результате данного исследования разработана адаптивная нейронечеткая сеть классификации ANFIS, позволяющая проводить анализ аномального трафика сети и более точно идентифицировать актуальные атаки по их типам. В связи с этим, метод нейронечеткой классификации может использоваться как эффективный инструмент анализа инцидентов кибербезопасности.

4. Благодарности

Исследование выполнено при финансовой поддержке РФФИ (проект 20-57-53019) и гранта Президента Российской Федерации для государственной поддержки молодых российских ученых - кандидатов наук (МК-2959.2021.1.6), а также стипендии Президента Российской Федерации молодым ученым и аспирантам (СП-3652.2021.5).

5. Литература

[1] Bolodurina, I. The development and study of the methods and algorithms for the classification of data flows of cloud applications in the network of the virtual data center / I. Bolodurina, D. Parfenov // International Journal of Computer Networks and Communications – 2018. – Vol. 10(2). – P. 15-22.

[2] Alsirhani, A. DDoS Detection System: Using a Set of Classification Algorithms Controlled by Fuzzy Logic System in Apache Spark / A. Alsirhani, S. Alsirhani, P. Bodorik // IEEE Transactions on Network and Service Management. – 2019. – Vol. 16(3). – P. 936-949.

[3] Jin, S. Intrusion Detection System Enhanced by Hierarchical Bidirectional Fuzzy Rule Interpolation / S. Jin, Y. Jiang, J. Peng // IEEE International Conference on Systems, Man, and Cybernetics (SMC) Miyazaki. – 2018. – P. 6-10.