расположения, атакующего и атакуемого узлов для экспериментальных данных и смоделированных данных представлены на рисунке 2.

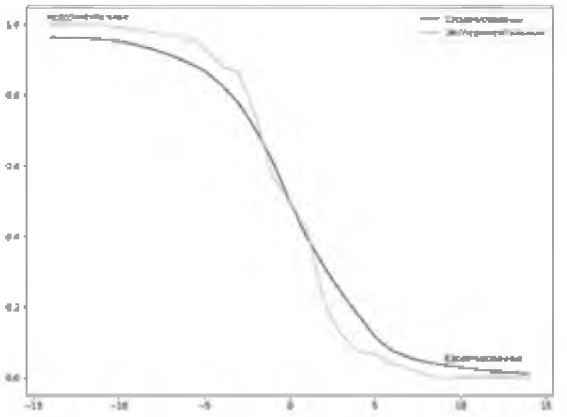

Рисунок 2 - Сравнение модели на основе экспериментальных данных

Для оценки точности модели была рассчитана ошибка аппроксимации по алгоритму среднеквадратичного отклонения, которая составила 0.078.

Список использованных источников

1. Олифер, В. Компьютерные сети. Принципы, технологии, протоколы [Текст]/В. Олифер, Н. Олифер. – СПб.: Питер, 2021.-1008 с.
2. Дэвис, Р. Искусство тестирования на проникновение в сеть [Текст]/Р. Дэвис. – М.: ДМК Пресс, 2021.-310 с.
3. Макаренко, С.И. Защита компьютерных сетей и телекоммуникаций [Текст]: учебное пособие/С.И. Макаренко. – СПб.: Наукоёмкие технологии, 2024.-311 с

Князьков Сергей Александрович, инженер 2 категории, филиал НИЦ Телеком в г. Самаре, knyazkovsa@nic-t.ru

УДК 004.056.57, 004.054

ПРИМЕНЕНИЕ ФУНКЦИИ РАСПРЕДЕЛЕНИЯ ВРЕМЕННЫХ ЗАДЕРЖЕК РАСПРОСТРАНЕНИЯ ПАКЕТА В ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ ДЛЯ АНАЛИЗА ВЕРОЯТНОСТИ УСПЕШНОЙ СПУФИНГОВОЙ АТАКИ

С.А. Князьков
Филиал НИЦ Телеком в городе Самаре, г. Самара

Ключевые слова: локальная вычислительная сеть, информационная безопасность, сетевая атака, задержка распространения пакета

Анализ работы протоколов, их уязвимостей, и методов проведения атак в локальных вычислительных сетях позволяет сделать вывод, что наиболее опасными атаками являются те методы, которые рассчитаны на подмену пакетов атакуемого компьютера. Такие атаки могут как не оказывать заметного влияния на работоспособность сети, являясь средством для выполнения более серьёзной атаки, так и существенно парализовать сеть [1].

Многие протоколы характеризуются тем, что узел, отправляющий запрос, обрабатывает только первый полученный ответ на него. Это свойство протокола создаёт уязвимость к типу таких атак, при которых, злоумышленник может отправить изменённый пакет, который придёт и будет обработан первым, что, в свою очередь, внесёт те или иные изменения в работоспособность атакуемого узла в зависимости от предназначения протокола [2]. Таким образом, можно сделать вывод о том, что задержка времени распространения пакета играет ключевую роль в вероятности успешной атаки.

Сами по себе задержки являются случайными величинами, поэтому необходимо выявить некие закономерности в характере их распределения с помощью различных методов статистической обработки информации.

Основным инструментом статистики является гистограмма распределения оцениваемой случайной величины. Каждый результат измерения является единичным значением случайной величины, а в совокупности они образуют выборку значений случайной величины [3].

Представим, что сеть состоит из цепочки N коммутаторов/маршрутизаторов. В сети существуют конечные узлы A, B, C. Количество межсетевых переходов от C до A и B обозначим как L^A и L^B соответственно. Узел C является тестирующим, то есть он посылает широковещательный запрос, например, ARP-запрос, и ожидает ответ от узлов A и B. При этом, узел B пытается выполнить подмену (спуфинг), путём отправки ложного пакета.

Представим, что есть некая дискретная функция, отражающая зависимость времени доставки от времени проведение эксперимента: $T_i(t)$ и $T_j(t)$, где $i - L^A$, $j - L^B$. При том, функции время доставки $T_i(t)$ и $T_j(t)$, являются неэквидистантными временными рядами. Если взять функцию распределения $T_i(t) - F_i(t)$, а $T_j(t) - F_j(t)$ то, используя следующую формулу, можно оценить вероятность успешной атаки:

$$P_{ij} = \max_t \left(\sqrt{(1 - F_i(t)) \cdot F_j(t)} \right)$$

где P_{ij} – вероятность успешной атаки для i -го расстояния и j-го расстояния;

$F_i(t)$ – функция распределения задержек распространения для i -го расстояния;

$F_j(t)$ – функция распределения задержек распространения для j -го расстояния.

Таким образом, используя известную вероятность атаки в зависимости от L^A и L^B, можно оценить влияние задержек распространения пакетов на вероятность успешной спуфинговой атаки при текущей топологии ЛВС и предпринять соответствующие меры по её защите.

Список использованных источников

1. Макаренко, С.И. Защита компьютерных сетей и телекоммуникаций [Текст]: учебное пособие/С.И. Макаренко. – СПб.: Наукоёмкие технологии, 2024.-311 с
2. Дэвис, Р. Искусство тестирования на проникновение в сеть [Текст]/Р. Дэвис. – М.: ДМК Пресс, 2021.-310 с.
3. Олифер, В. Компьютерные сети. Принципы, технологии, протоколы [Текст]/В. Олифер, Н. Олифер. – СПб.: Питер, 2021.-1008 с.

Князьков Сергей Александрович, инженер 2 категории, филиал НИЦ Телеком в г. Самаре, knyazkovsa@nic-t.ru

УДК: 004.738.2.

МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДАННЫХ В РАСПРЕДЕЛЁННЫХ СИСТЕМАХ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Р. А. Олин, В. В. Бондаренко
«Самарский национальный исследовательский университет имени академика С.П. Королёва», г. Самара

Ключевые слова: децентрализованный искусственный интеллект, федеративное обучение, блокчейн, византийская устойчивость

Децентрализованный искусственный интеллект представляет собой современный подход к обучению моделей, при котором обработка данных происходит на распределенных, территориально удаленных устройствах, при этом параметры модели передаются для последующей агрегации. Такой метод позволяет существенно снизить риск утечки обучающих датасетов, поскольку исходные данные не покидают устройство, что особенно важно в условиях жестких требований к информационной безопасности и защиты персональных данных [1]. Традиционный централизованный подход, несмотря на высокую точность моделей, создает проблему единой точки отказа, что вынуждает переходить к распределенным схемам обучения, например, к федеративному обучению, где обмен информацией осуществляется через передачу градиентов или весов, а не сырых данных [2].