

ПРИМЕНЕНИЕ МЕТОДОВ ТЕОРИИ ПЕРКОЛЯЦИИ В ЗАДАЧАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ IoT-СЕТЕЙ УМНОГО ДОМА

Д.Е. Куспанова¹, В.А. Бердников¹

¹Самарский университет, г. Самара
e-mail: kyspanova@icloud.com

Аннотация

Применена теория перколяции для моделирования устойчивости IoT-сетей умного дома к ВПО. Предложен графовый подход: узлы – устройства, рёбра – каналы связи. Разработана модель, определяющая критический порог перколяции, при превышении которого защищённые узлы образуют гигантский кластер с высокими затратами на поддержание связности. Разработан алгоритм перехода от модели IoT-сети к перколяционной матрице и проведён анализ алгоритмом Дейкстры полученных перколяционных матриц для оценки способности защищённых сегментов блокировать глобальную атаку. Подход позволяет прогнозировать уязвимости и разрабатывать стратегии защиты, поддерживающие фрагментированную кластерную структуру, что обеспечивает локализацию ВПО и минимизацию затрат на безопасность.

Ключевые слова: перколяция, информационная безопасность, интернет вещей, умный дом, распространение вредоносного ПО, порог перколяции, защищенные узлы.

Введение

Современные системы умного дома представляют собой сложные распределённые сети, объединяющие десятки и сотни IoT-устройств: датчики, системы видеонаблюдения и управления доступом. Рост числа таких устройств, их разнородность и недостаточный уровень защищённости создают благоприятную среду для распространения вредоносного программного обеспечения (ВПО). Особую опасность представляет возможность заражения, при котором компрометация одного устройства приводит к быстрому распространению ВПО на всю систему с целью поражения основного управляющего узла с последующей компрометацией всей сети и ее участников.

Теория перколяции, изначально разработанная для описания процессов протекания жидкости через пористые среды, предоставляет мощный математический аппарат для анализа распространения инфекций в сетях.

Целью данной работы является разработка математической модели на основе теории перколяции для анализа структурной связности защищённых устройств в IoT-сетях умного дома, позволяющей определять такую концентрацию активных узлов, при которой достигается экономический баланс между достаточным уровнем кластеризации защищённых устройств и минимизацией затрат на поддержание их связности.

1. Теория перколяции

Перколяция – это теория, описывающая возникновение связанных кластеров в случайных системах. Она изучает, как при увеличении вероятности связи узлов формируется «бесконечный» кластер, проходящий через всю систему. Переход к глобальной связности происходит при достижении критической вероятности – порога перколяции [1, 2, 3].

В контексте информационной безопасности перколяционный подход позволяет анализировать структуру кластеров защищённых устройств. При малой доле защищённых узлов они образуют множество изолированных фрагментов, что затрудняет координацию и снижает устойчивость к атакам. По мере увеличения их концентрации кластеры растут, после достижения некоторого значения разросшиеся кластеры начинают сливаться, образуя один большой сильно связный кластер с множеством обрывающихся путей. При достижении критического порога перколяции формируется единый гигантский кластер защищённых устройств, охватывающий всю сеть. Однако такой кластер обладает достаточно разреженной структурой, множеством висячих путей и, возможно, не одним естественным перколяционным путем вдоль направления движения перколяции. Такая структура обеспечивает высокий уровень координации и защиты, однако её поддержание сопряжено со значительными эксплуатационными затратами.

2. Модель IoT-сети умного дома

IoT-сеть умного дома может быть представлена в виде неориентированного графа.

Каждый узел характеризуется вероятностью заражения при контакте с заражённым соседом, а также наличием или отсутствием средств защиты. Каждое ребро характеризуется вероятностью успешной передачи ВПО, которая может зависеть от сетевых протоколов, шифрования и наличия межсетевых экранов.

В рамках модели считается, что устройство может находиться в одном из двух состояний:

- уязвимое;
- защищенное.

В рамках данной работы с целью упрощения вычислений рассматривались только квадратные матрицы с манхэттенской логикой движения по кластеру, то есть перемещение осуществлялось только вверх, вниз, вправо и влево, движение по диагонали – исключено.

3. Метод двухфазных операций

Для повышения устойчивости сети к распространению вредоносного программного обеспечения (ВПО) применяется метод двухфазных операций на графе [1, 2, 4]:

1. Фаза 1: создание опорной перколяционной матрицы с небольшой концентрацией защищенных объектов.
2. Фаза 2: прокладывание искусственных перколяционных путей.

4. Экспериментальные результаты

Для проверки предложенного подхода была разработана программная реализация. В основе модели лежит алгоритм Дейкстры, адаптированный для поиска пути минимальной стоимости от верхней границы матрицы до нижней.

Стоимость прохода через чёрный (защищенный) узел составляет 1 единицу, через белый (уязвимый) – $L^2 + 1$ единиц, где L – размер матрицы.

По формуле 1 производился расчет относительная стоимости $P_{отн}$.

$$P_{отн} = 1.7 * p + 1.7 * R * \frac{\varphi^2(p)}{L^2(p)} \quad (1)$$

где p – концентрация стохастической базы, R – отношение стоимостей объектов, $\varphi(p)$ – доля белых шагов в общем пути, $L(p)$ – нормализованная длина пути перколяции.

Экономия (%) – относительная эффективность применения предлагаемого подхода.

На рисунке 1 представлена зависимость количества шагов перехода от концентрации защищенных узлов, стоимость переходов между перколяционными кластерами, относительная стоимость перколяции и экономия использованных ресурсов.

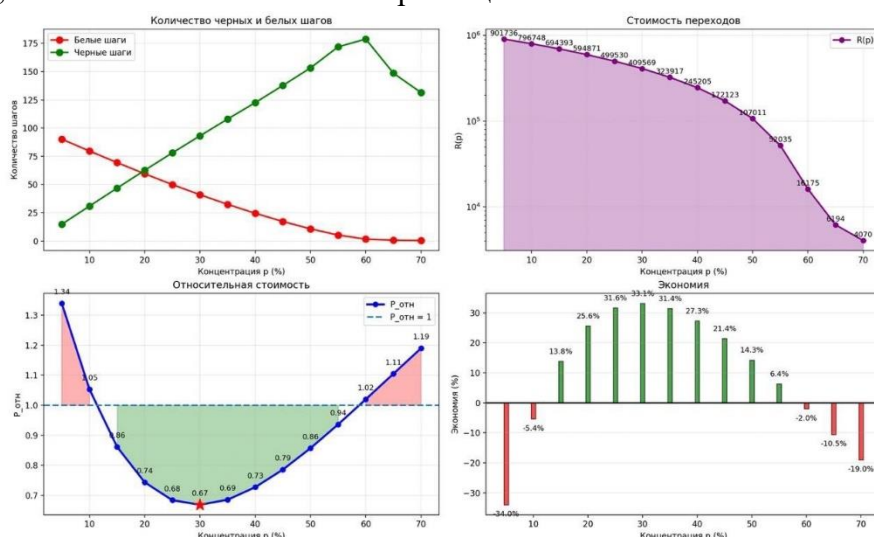


Рисунок 1 – Статистика эксперимента при различных значениях концентрации защищенных узлов (размер матриц 100x100)

Заключение

В работе разработана математическая модель на основе теории перколяции для анализа устойчивости IoT-сетей умного дома к распространению вредоносного программного обеспечения (ВПО).

В ходе работы получены следующие результаты:

1. Разработана модель, позволяющая оценивать способность сети блокировать распространение ВПО в зависимости от концентрации защищённых узлов.
2. Экспериментально определён критический порог перколяции $p \in [25, 30]\%$ для создания искусственного сквозного кластера защищённых устройств.
3. Установлено, что защищённые узлы эффективно сдерживают распространение атаки в диапазоне концентраций до 55-60%.
4. Подтверждена экономическая эффективность предложенного подхода: максимальная экономия достигает 33,13% при концентрации защищённых узлов около 30%.

5. Практическая значимость работы заключается в возможности прогнозирования уязвимостей IoT-инфраструктуры умного дома и разработки стратегий защиты, направленных на поддержание оптимальной концентрации защищённых устройств, обеспечивающей надёжную блокировку распространения ВПО при минимизации эксплуатационных затрат.

Список использованных источников

1. Мостовой, Я. А., Моделирование оптимальных двухфазных операций в случайных операционных средах / Я. А. Мостовой // Автометрия. – 2015. – Т. 51, № 3. – С. 35–41.

2. Мостовой, Я. А., Двухфазные операции в больших сетях наноспутников / Я. А. Мостовой // Компьютерная оптика. – 2013. – Т. 37, № 1. – С. 120–130.

3. Galam, S. Universal formulas for percolation thresholds / S. Galam, A. Mauger // Phys. Rev. E. – 1996. – V. 53, № 3, – P. 2177–2181.

4. Mostovoy, Y. A. Statistical modeling of a scale network of nanosatellites / Y. A. Mostovoy, V. A. Berdnikov // Journal of Physics: Conference Series. – IOP Publishing, 2018. – V. 1096, №1. – P. 012184.

APPLICATION OF PERCOLATION THEORY METHODS TO INFORMATION SECURITY PROBLEMS FOR SMART HOME IoT NETWORKS

D. E. Kuspanova¹, V. A. Berdnikov¹

*¹Samara University, Samara
e-mail: kyspanova@icloud.com*

Abstract

Percolation theory is applied to model the resilience of smart home IoT networks to higher education. A graph approach is proposed: nodes are devices, edges are communication channels. A model has been developed that defines a critical percolation threshold, above which protected nodes form a giant cluster with high connectivity costs. An algorithm for the transition from an IoT network model to a percolation matrix has been developed and Dijkstra's algorithm has analyzed the obtained percolation matrices to assess the ability of protected segments to block a global attack. The approach allows you to predict vulnerabilities and develop protection strategies that support a fragmented cluster structure, which ensures the localization of high-risk situations and minimizes security costs.

Keywords: percolation, information security, Internet of Things, smart home, malware propagation, percolation threshold, protected nodes.