Исследование методов обнаружения вторжений в компьютерные системы путем имитационного моделирования

Неплохов Алексей Андреевич, гр. 522

Санкт-Петербургский государственный университет
Математико-механический факультет
Кафедра статистического моделирования

Научный руководитель: к.ф.-м.н., доц. Кривулин Н.К.
Рецензент: к.ф.-м.н., доц. Христинич В.Б.

Санкт-Петербург
2007г.

Введение

- Данная работа посвящена теме компьютерной безопасности.
- Повсеместное внедрение компьютерных систем и объединение их в сети делают проблему обеспечения безопасности очень актуальной.
- Создание эффективного средства обнаружения вторжений — достаточно сложная задача по целому ряду причин:
  - сложные и разнообразные компоненты изучаемых систем;
  - широкая география элементов сетей, большое их количество;
  - малоизученность проблемы в связи с относительно недавним возникновением последней.

Основные подходы к обнаружению вторжений

- Средства анализа сценариев. Сравнивают сетевую активность и поведение отдельных элементов системы с фиксированной базой данных сценариев.
  - Достоинства: высокая скорость работы, малое число ложных срабатываний.
  - Недостатки: необходимость обновления, необнаружение новых типов атак.
- Методы обнаружения аномалий. Оперируют статистическими данными по сетевой активности. Выявляют отклонения от нормального поведения.
  - Достоинства: невысокая потребность в обновлениях, широкий спектр применений.
  - Недостатки: сложность создания и развертывания, необходимость анализа результатов.

Основные подходы к обнаружению вторжений

- Средства анализа сценариев. Сравнивают сетевую активность и поведение отдельных элементов системы с фиксированной базой данных сценариев.
  - Достоинства: высокая скорость работы, малое число ложных срабатываний.
  - Недостатки: необходимость обновления, необнаружение новых типов атак.
- Методы обнаружения аномалий. Оперируют статистическими данными по сетевой активности. Выявляют отклонения от нормального поведения.
  - Достоинства: невысокая потребность в обновлениях, широкий спектр применений.
  - Недостатки: сложность создания и развертывания, необходимость анализа результатов.

Ограничения в контексте данной работы

В данной работе был рассмотрен определенный класс вторжений : атака на отказ в обслуживании.

Отличительные особенности:

- в основе этого типа атак лежат различные методы захвата системных ресурсов жертвы;
- цель атаки — прекращение нормального функционирования системы вплоть до выведения ее из строя.

Причина выбора этого типа атак — популярность, как следствие простоты их реализации и высокой эффективности. Сыграла свою роль и доступность данных, необходимых для анализа.

Ограничения в контексте данной работы. Цель работы.

Отличительные особенности протокола TCP/IP:

- любой элемент сети имеет IP адрес;
- соединение между элементами производится посредством порта;
- обмен данными между элементами сети происходит пакетами, в заголовке каждого из которых указан адрес, порт отправителя и получателя.

Основная цель работы : изучение методов обнаружения аномалий в сетевой активности и сравнение их эффективности.

Первый метод: оценка разветвленности

- Поток — последовательность пакетов с одинаковыми адресами отправителя и адресами получателя в заголовке.
- Разветвленность источника — параметр элемента сети, напрямую зависящий от количества исходящих потоков.
- Супер-источник — элемент сети, генерирующий большое количество исходящих потоков.

- Результатом работы метода на основе анализа разветвленности источника является таблица.
- Каждая строка таблицы содержит адрес источника и оценку его разветвленности.
- Данные в таблице анализируются на предмет поиска источника со значительно превышающей среднее значение степенью разветвленности.

Первый метод: оценка разветвленности

- Поток — последовательность пакетов с одинаковыми адресами отправителя и адресами получателя в заголовке.
- Разветвленность источника — параметр элемента сети, напрямую зависящий от количества исходящих потоков.
- Супер-источник — элемент сети, генерирующий большое количество исходящих потоков.

- Результатом работы метода на основе анализа разветвленности источника является таблица.
- Каждая строка таблицы содержит адрес источника и оценку его разветвленности.
- Данные в таблице анализируются на предмет поиска источника со значительно превышающей среднее значение степенью разветвленности.

Первый метод: оценка разветвленности. Алгоритм.

1. p — вероятность выбора пакета из потока.
2. $r = h(< pkt.src, pkt.dst >)$ р.р. на интервале $[1, \ldots, w]$.
3. Если $G[r] = 1$, то поток с соответствующей меткой обрабатывался ранее.
4. Если $G[r] = 0$, то $\tilde{N}_s := \tilde{N}_s + \frac{w}{u}$, $G[r] := 1$.
5. Для уменьшения погрешности введем u_{min}. Как только окажется, что $u < u_{min}$, запускаем новый период наблюдений.
6. Итоговая оценка разветвленности получается масштабированием $\frac{1}{p}$:

$$\tilde{F}_s = \frac{1}{p}\tilde{N}_s.$$

Второй метод: наблюдение за IP адресами источников

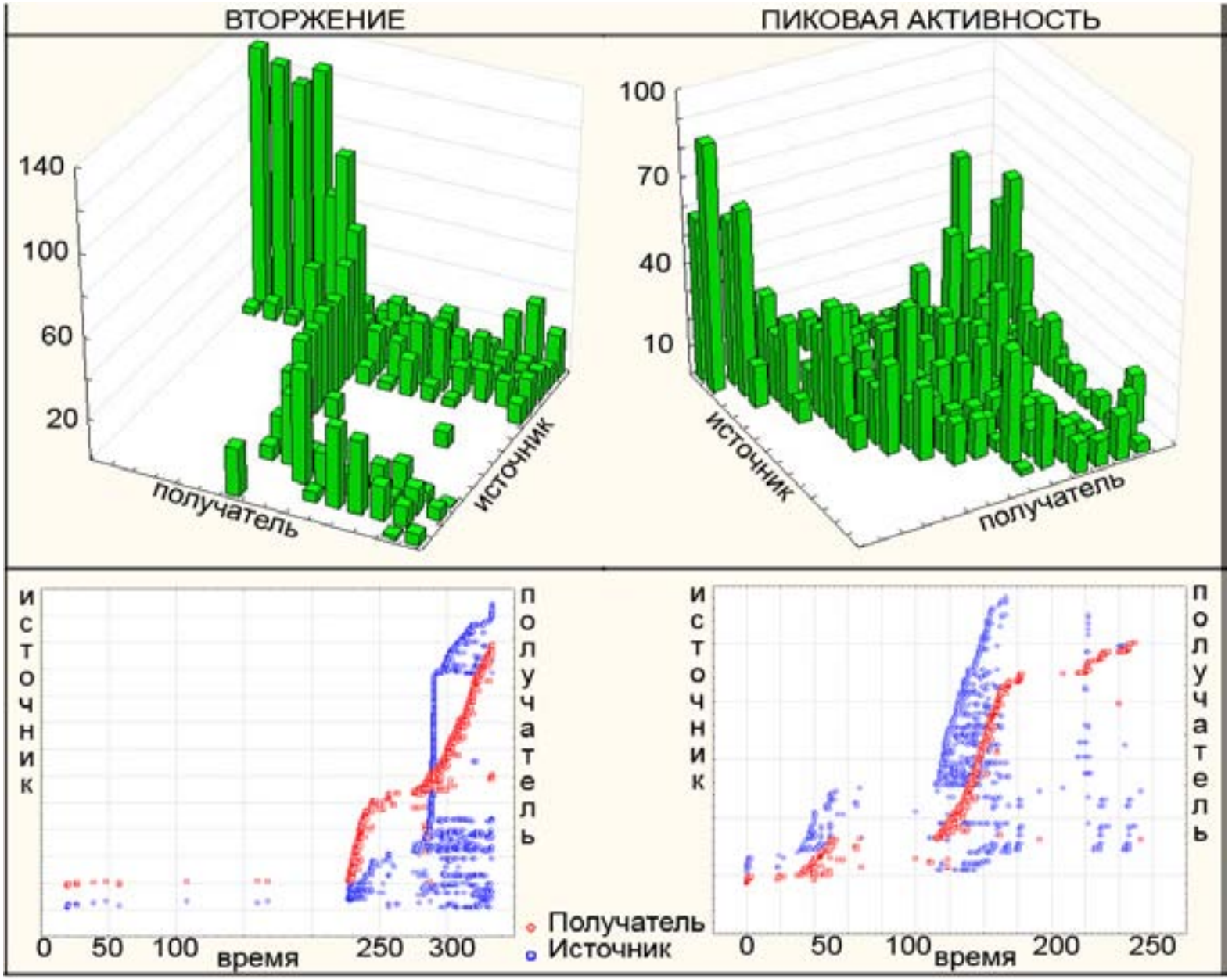
Определим типы активности:

- нормальное поведение,
- пиковая активность,
- атака на отказ в обслуживании.

Проблема: учет числа пакетов не позволяет различать пиковую активность и вторжение.

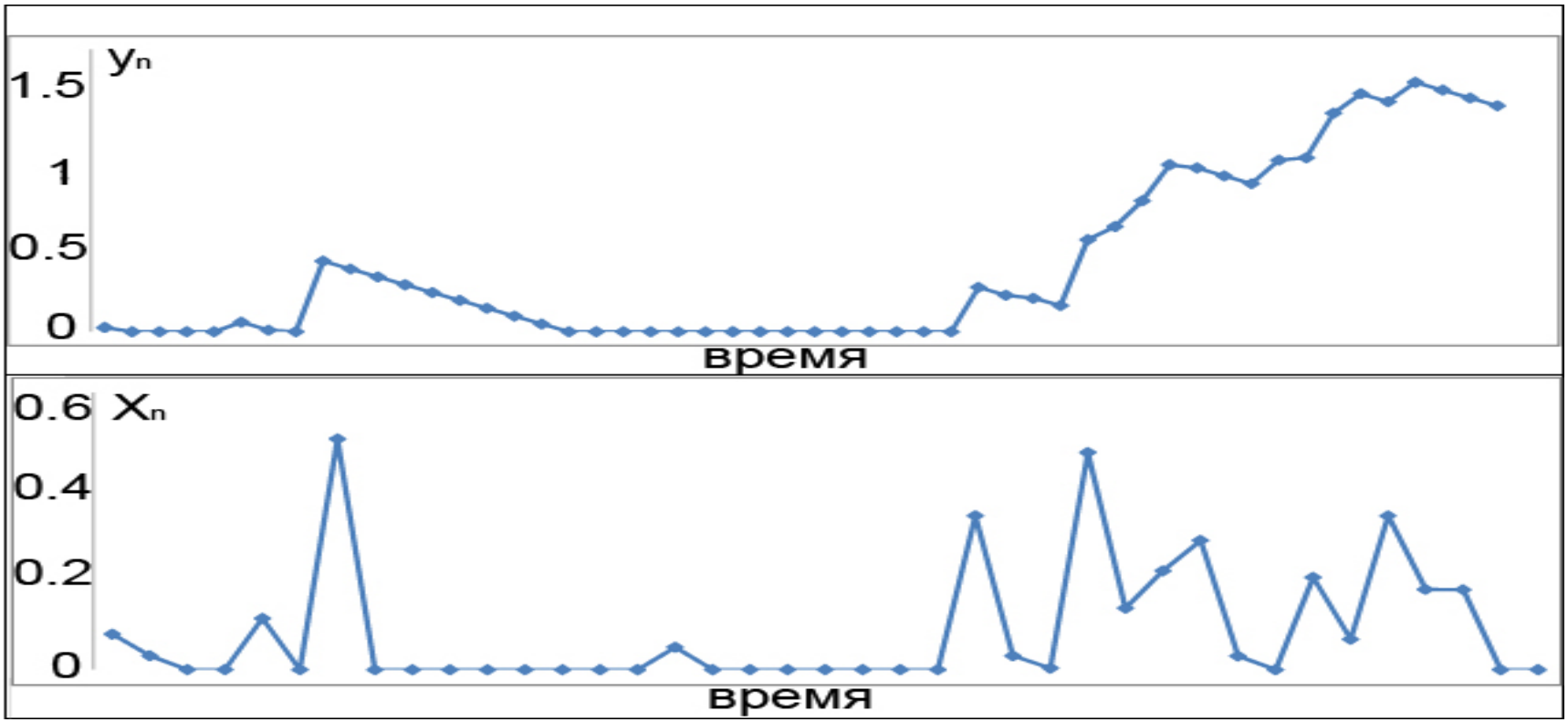
Решение: более адекватные результаты дает наблюдение за количеством новых адресов отправителей в единицу времени.

Второй метод: наблюдение за IP адресами источников



Второй метод: наблюдение за IP адресами источников

- X_n — доля ранее не встречавшихся источников за очередной промежуток времени Δ_n.
- y_n — накапливает значения X_n, значительно превышающие средние при нормальных условиях.



Второй метод. Алгоритм.

1. Весь период наблюдений разбиваем на интервалы Δ_n.
2. $X_n = \dfrac{|\tau_n - \tau_n \cap \zeta_n|}{\tau_n}$, где
   $E(X_n) = \alpha << 1$ при нормальных условиях.
3. $Z_n = X_n - \beta$.
4. $y_n = (y_{n-1} + Z_n)^+, \quad y_0 = 0.$
5. $d_N(y_n) = \begin{cases} 0 & y_n \le N \\ 1 & y_n > N \end{cases}$.
6. $d_N(y_n) = 1$ означает вторжение на Δ_n.

Созданные программные средства

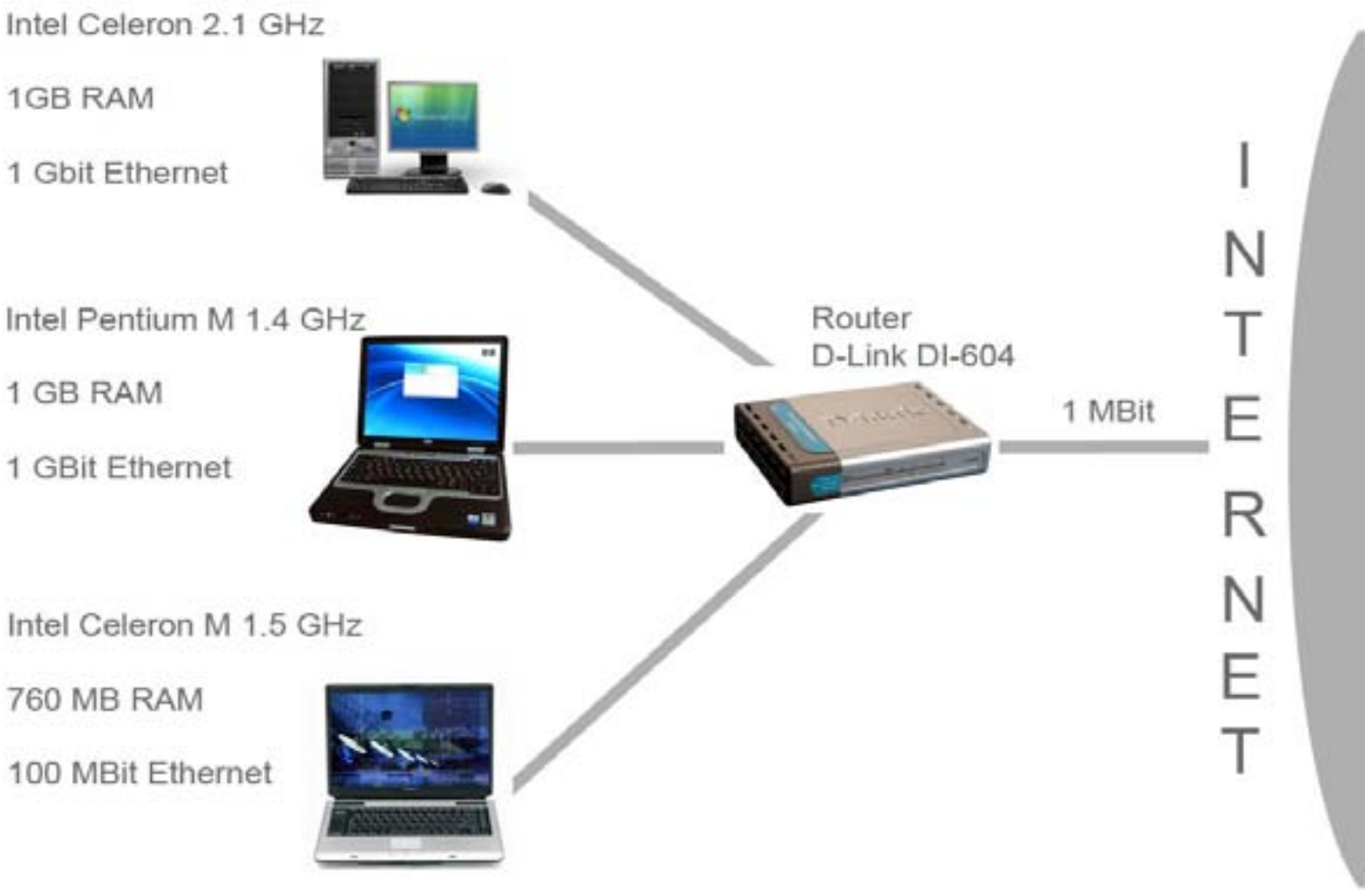
Модули программного комплекса.

- Эмулятор атаки: создает сетевую активность, характерную для атак на отказ в обслуживании.
- Конвертор: преобразовывает журнал сетевой активности к виду, необходимому для дальнейшей обработки.
- Подготовка данных: отбирает из всех пакетов только те, что предназначены „жертве“, хеширует данные.
- Реализация метода на основе анализа разветвленности.
- Реализация метода наблюдения за адресами источников.

Взаимодействие элементов программного комплекса

Условия проведения экспериментов

Основные компоненты локальной вычислительной сети (ЛВС):



Условия проведения экспериметнов

Основные типы рассматриваемой активности :

Таблица с результатами эсперементов

Тип активности	Время начала атаки	Время сигнала первого метода	Время сигнала второго метода
"Атака 1"	**129**	не опред.	не опред.
"Атака 1"	**400**	не опред.	не опред.
"Атака 1"	**797**	**814-817(вер.)**	не опред.
"Атака 2"	**553**	**528-530(лож.)** **595-598(вер.)**	**555-570(вер.)** и далее
"Атака 2"	**682**	**682 (вер.)**	**555-570(вер.)**
"Атака 3"	**287**	**289-292(вер.)**	**315-330(вер.)**
"Норм.1"	нет атаки	не опред.	не опред.
"Пиковая"	нет атаки	не опред.	не опред.
"Исключ."	нет атаки	не опред.	**15-30(лож.)**
"Норм.2"	нет атаки	не опред.	не опред.

Результаты. Выводы.

Проведенная работа включала в себя:

- изучение предметной области;
- исследование некоторых из методов обнаружения вторжения;
- получение алгоритмов и написание программного комплекса;
- проведение серии экспериментов и сравнение эффективности методов.

Были сделаны выводы:

- исследованные методы эффективно распознают угрозу;
- эффективность второго метода оказалась незначительно выше чем у первого;
- первый метод показал более адекватные результаты в неоднозначных ситуациях при слабой активности.