УДК 004.052:004.738.2 (045)

Минаев Ю.Н., д.т.н.,
Толстикова Е.В.

МЕТОД ЭФФЕКТИВНОЙ ПЕРЕДАЧИ ДАННЫХ ПРИ НАЛИЧИИ АНОМАЛИЙ В СЕТЯХ РАДИОДАТЧИКОВ

Національний авіаційний університет

Рассмотрены задачи эффективной передачи данных в специализированных сенсорных сетях (сетях радиодатчиков) при наличии аномалий трафика. Аномальное состояние определяется по величинам инвариантов тензора трафика, коэффициентов характеристического уравнения или систем правил. Разработан метод передачи данных типа многоадресной (multicast) рассылки в сенсорной сети с управлением допустимыми траекториями передачи.

Введение

Особенность сетей радиодатчиков заключаются в том, что передача одного бита информации по радиоканалу даже сверхмалой мощности эквивалентна выполнению тысячи команд процессором точечного сенсора. При этом ограниченные вычислительные ресурсы и динамический характер сети приводят к тому, что функциональность сенсора время от времени изменяется. Необходимо решение противоречивой задачи – минимизации объема кода, реализующего программу заданного уровня сложности.

Традиционные приемы построения ОС реального времени и привычные отработанные архитектурные решения здесь неприменимы. В результате вся ОС и ее компоненты построены по принципу конечных автоматов – переходов из состояния в состояние.

Для обеспечения возможности доступа в сеть и обмена данными в ответ на стандартные запросы, очевидно, необходим соответствующий механизм коммуникации. Новый метод реализации сетевых протоколов каждого сенсора получил название "Направленная диффузия" (*directed diffusion*). Основу механизма направленной диффузии составляют принцип адресации, в котором вместо адреса получателя используется собственно смысл запроса, и принцип многопутевого распространения (диффузии) запросов по сети. Постановка задачи – запрос – представляется множеством пар атрибутов и значений, а для реализации процесса диффузии запросов и организации доступа во внешние сети, в частности, в региональные и корпоративные сети, необходим интерфейс согласования протокола направленной диффузии и стандартных протоколов внешних сетей.

Задача усложняется из-за неизбежного возникновения аномалий сетевого трафика. Помимо аномалий, присущих любой информационно-вычислительной сети, при использовании радиоканалов передачи возникают специфические аномалии. Для их обнаружения и локализации необходимы более совершенные методы идентификации.

Цель исследования

Разработка метода эффективной передачи данных в сети радиодатчиков в условиях возникновения аномалий сетевого трафика. Критерием эффективности является обеспечение требуемой скорости и достоверности при ограниченном энергопотреблении датчиков.

Современное состояние исследований

Системы обнаружения аномалий, сетевых вторжений и выявления признаков компьютерных атак на

информационные системы уже давно применяются как один из необходимых рубежей обороны информационных систем.

Системы обнаружения аномального поведения (*anomaly detection*) основаны на том, что СОА известны некоторые признаки, характеризующие правильное или допустимое поведение объекта наблюдения.

В обнаружении аномалий обычно используют следующие методы:

–пороговые значения: наблюдения за объектом выражаются в виде числовых интервалов. Выход за пределы этих интервалов считается аномальным поведением. В качестве наблюдаемых параметров могут быть, например, количество файлов, к которым обращается пользователь в данный период времени, число неудачных попыток входа в систему, загрузка центрального процессора и т.п.;

–статистические методы: решение о наличии атаки принимается на основании результатов количеству собранных данных путем их статистической предобработки;

–параметрические или непараметрические методы: для выявления атак строится специальный "профиль нормальной системы" на основе априорных данных (шаблонов) или с учетом апостериорных данных, полученных в процессе наблюдения за объектом в период обучения;

–анализ сигнатур и протоколов;

–другие методы: нейронные сети, генетические алгоритмы, позволяющие классифицировать некоторый набор видимых сенсору-датчику признаков.

Достоинства и недостатки различных методов подробно описаны в литературе. К сожалению, практически все существующие системы обнаружения компьютерных атак лишены функциональности, позволяющей связывать риски и угрозы безопасности с происходящими в сетевой и локальной вычислительной среде событиями.

В работе [1] показано, что достаточно адекватным представлением объекта исследований (измерений) есть представление в виде тензорной модели как матричной проекции в разных системах координат. Соответственно, и аномалией может считаться необычное сочетание параметров, что можно определить на основании значений инвариантов тензора псевдотрафика.

Параметры трафика авторами работы [1] в общем виде определены следующим образом:

$$\mathbf{x} = \{x_i\}, \quad i = 1,9$$

x_1 – Protocol *ID* – протокол, связанный с событием (*TCP*=0, *UDP*=1, *ICMP*=2, *unknown*=3);

x_2 – номер порта источника;

x_3 – номер порта хоста назначения;

x_4 – *IP*-адрес источника;

x_5 – *IP*-адрес приемника;

x_6 – *ICMP Type* тип *ICMP*-пакета (*Echo Request or Null*);

x_7 – *ICMP Code* кодовое поле из *ICMP*-пакета (*None or Null*);

x_8 – *Raw Data Length* – длина данных в пакете;

x_9 – *Raw Data* – порция данных в пакете.

В этом смысле псевдотрафик – тензорное произведение вектора параметров трафика и специального единичного вектора с последующей сверткой: $T=x\otimes\mathbf{1}^{(s)}$, где $x=\{x_i\}, i=1, 9$; $\mathbf{1}^{(s)}=\{1\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 1\}$, $\otimes$ – символ Кронекерова произведения.

Основная часть исследования

Используя результаты исследований, описанных выше, можно построить систему эффективной передачи трафика беспроводных сенсорных сетей (сетей радиодатчиков) с локализацией узлов или маршрутов, на которых наблюдаются аномальные состояния сетевого трафика. Благодаря такому подходу удается реализовать

принципиально новую концепцию обнаружения компьютерных угроз, а не атак [2].

Для решения проблем повышения энергоэффективности и пропускной способности сенсорных сетей разработана модель распределенной сенсорной сети с так называемыми «мобильными агентами» [3]. Здесь целесообразно применять стохастические мобильные агенты – программный код, при передаче которого исходный объем данных может быть уменьшен посредством ликвидации избыточности методами стохастической оптимизации.

В качестве модели механизма стохастической оптимизации избыточности передачи данных в плотной сети радиодатчиков применяется управляемый диффузионный марковский процесс $\xi = \xi(t)$, переходная плотность вероятности $p(t,x,y)$ которого в ε-окрестности каждой внутренней точки x удовлетворяет обратному уравнению Колмогорова [4]:

$$\frac{\partial}{\partial t} = Lp, \quad L = \mathbf{A}(x)\frac{\partial}{\partial x} + \mathbf{B}(x)\frac{\partial^2}{\partial x^2}, \quad \mathbf{B}(x) = \frac{1}{2}\mathbf{R}(x), \quad (1)$$

где $\mathbf{A}(x)$ – вектор коэффициентов сноса размерностью N; $\mathbf{B}(x)$ – матрица коэффициентов диффузии размерностью $N \times N$; $\mathbf{R}(x)$ – корреляционная матрица размерностью $N \times N$. Коэффициенты $a_i(x)$ и $b_{ij}(x)$, $i, j = \overline{1,N}$, непрерывны, причем $b_{ij}(x) > 0$, удовлетворяют условию Липшица

$$\left|a_i(x) - a_i(y)\right| \le C_1 \left|x - y\right|,$$

$$\left|b_{ij}(x) - b_{ij}(y)\right| \le C_2 \left|x - y\right|,$$

где C_1 и C_2 – константы.

В случае плотного распределения датчиков на поверхности или в пространстве ε-окрестность внутренней точки x достаточно мала. Тогда можно рассматривать случайный процесс $\xi(t)$ как процесс, управляемый векторным стохастическим дифференциальным уравнением вида:

$$d\xi(t) = \mathbf{A}\left[\xi(t)\right]dt + \mathbf{R}\left[\xi(t)\right]d\eta(t), \quad (2)$$

где

$$\eta(t) = \frac{\xi(t) - \xi(t) - \left[\mathbf{A}(t) - \mathbf{A}(t_0)\right]}{\sqrt{\left|D(t) - D(t_0)\right|}}, \quad \left|D(t) - D(t_0)\right| = \int_{t_0}^{t} \left\|\mathbf{B}(\tau)\right\| d\tau$$

– процесс броуновского движения; $\left\|\cdot\right\|$ – норма матрицы.

Таким образом, рассматриваемый процесс передачи, по существу, представляет собой процесс направленной диффузии, управляемой (стохастическими) мобильными агентами.

Задача управления заключается в оптимальном выборе величин $\mathbf{A}(x)$ и $\mathbf{B}(x)$, при котором минимизируется объем трафика для простого поиска оптимального числа маршрутов с ограничением на энергопотребление и с учетом асимметрии качества связи между последовательными узлами.

В задаче также накладываются ограничения на допустимые траектории доставки данных. В качестве допустимых рассматриваются те траектории, на которых не обнаружено аномалий сетевого трафика. На рис. 1 изображен сегмент беспроводной сенсорной сети с разрешенными и запрещенными траекториями. Из разрешенных траекторий доставки данных выбирается оптимальная траектория. Выбор осуществляется по критериям энергоэффективности, пропускной способности и др.

Определим среднюю задержку доставки от источника до пункта сбора для случаев обычной направленной диффузии (нд) τ_{dd} и направленной диффузии с мобильными агентами (ндма) τ_{ma}. с учетом всех возможных задержек распространения данных до пункта сбора

$$\tau_{dd} = \frac{\tau_e}{n_p} + \left(\frac{s_d + s_h}{d_{MAC}} + \tau_c + \tau_a\right)\left(N_h + n_h\right), \quad (3)$$

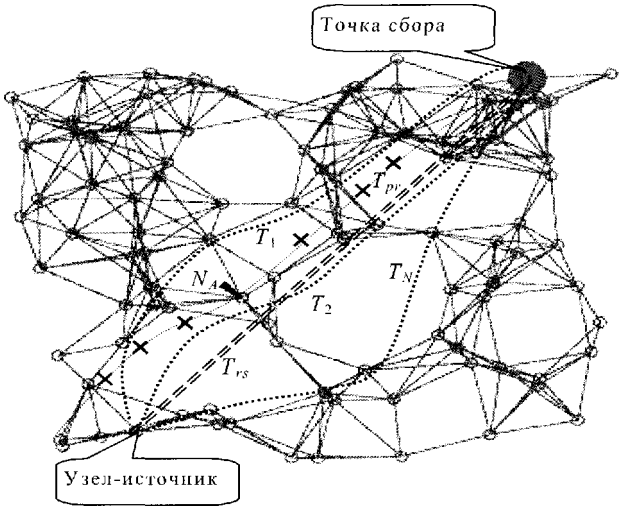

Рис. 1. Конфигурация сенсорной сети со стохастическими мобильными агентами.
T_{rs} – оптимальная траектория доставки данных;
$T_1, T_2, \ldots, T_N$ – возможные траектории; N_A – аномальный узел;
T_{pr} – запрещенная траектория

где τ_e – среднее время генерации траектории доставки; n_p – число доставляемых пакетов; s_d и s_h – размер данных в пакете и размер заголовка пакета соответственно; d_{MAC} – задержка данных на уровне доступа к среде; τ_c и τ_a – средние задержки управления и доступа соответственно; N_h – число переходов вдоль оптимальной траектории с минимальным числом узлов; $N_h + n_h$ – среднее число переходов по всем допустимым траекториям.

Если число пакетов, доставляемых к пункту сбора, много больше единицы, выражение (3) упрощается:

$$\tau_{dd} \approx + \left(\frac{s_d + s_h}{d_{MAC}} + \tau_c + \tau_a \right) \left(N_h + n_h \right). \quad (4)$$

При доставке данных с использованием мобильных агентов соответствующее выражение для задержки доставки имеет вид:

$$\tau_{ma} = \sum_{k=1}^{K} \left(\tau_{ama} + \frac{s_d}{\tau_p} + \frac{s_{ma,k} + s_{pc} + s_h}{d_{MAC}} + \tau_c \right), \quad (5)$$

где K – число узлов-источников; τ_{ama} – задержка доступа мобильного агента, т.е. доставки данных на пункт сбора; τ_p – коэффициент расхода времени на обработку; s_{pc} – общий объем доставленных данных; $s_{ma,i}$ – размер данных мобильного агента на k-м узле.

С использованием выражений (3-5) были выполнены расчеты среднего расхода энергии на доставку и задержки доставки данных с разными общими объемами (рис. 2, 3) в сети, состоящей из 100 сенсоров. использовалось 10 мобильных агентов с объемом программного кода, примерно на порядок меньше объема передаваемых данных. Из графиков видно, что в широком диапазоне задержск доступа стохастических мобильных агентов имеет мсто выигрыш в задержке доставки, причем он тем больше, чем выше корреляция между данными на близко расположенных сенсорах.

Выводы

Для многих применений беспроводных сенсорных сетей методы доставки данных с помощью

стохастических мобильных агентов оказываются более эффективными, чем с помощью детерминированных мобильных агентов, и, тем более, чем традиционные методы с архитектурой клиент-сервер. Скорость доставки

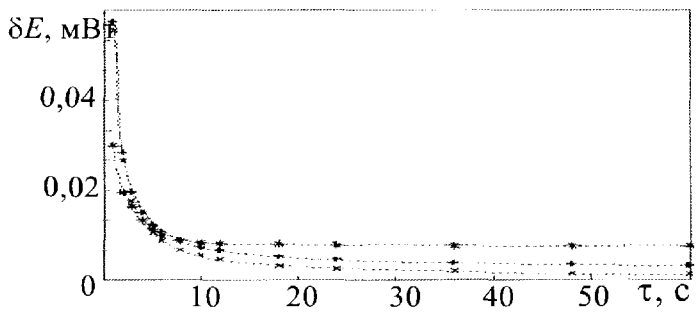

Рис. 3. средний расход энергии при передаче:

------✳------ архитектура «клиент-сервер»;

мобильные агенты:

------┼------ коэффициент корреляции данных от разных сенсоров 0,8;

------✕------ коэффициент корреляции данных от разных сенсоров 0,9

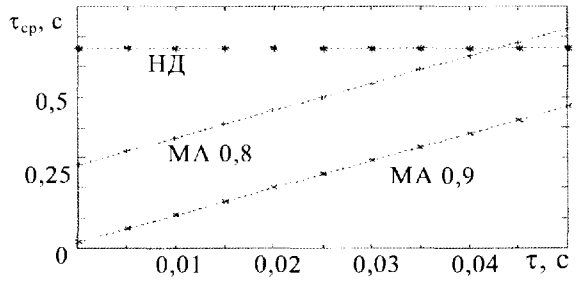

Рис. 4. Зависимость задержки доставки от средней задержки $\tau_{зд}$ доступа стохастических мобильных агентов при разных коэффициентах корреляции данных на сенсорах (для сравнения приведен график задержки для клиент-серверной доставки НД)

оптимизируется путем выбора оптимального маршрута при ограничениях на потребный расход энергии сенсоров. Применена теория управляемых марковских процессов для формирования пучка маршрутов. При Это особенно актуально для специализированных сенсорных сетей, которые, во-первых, не подлежат обслуживанию и текущему контролю, а во-вторых, подвергаются атакам и несанкционированным вторжениям.

Список литературы

1. Минаев Ю.Н., Гузий Н.Н., Филимонова О.Ю. Идентификация аномальных состояний трафика компьютерных сетей на основе парадигмы многомерных сетей // Проблемы информатизации и управления 2010. – №3. – С. 83-89.

2. Аграновский А.В., Хади Р.А. Новый подход к защите информации - системы обнаружения компьютерных угроз // Информационный бюллетень Jet info 2007. – № 04 (167) – 22 с. // http://www.jetinfo.ru/Sites/info/Uploads/2007_4.16EFCBFFB6F045AE8EFB7F26B414789F.pdf

3. H. Qi, Y. Xu, and X.Wang, "Mobile-agent-based collaborative signal and information processing in sensor networks," Proceedings of the IEEE, vol. 91, №8, 2003. – P. 1172-1183.

Дынкин Е.Б., Юшкевич А.А. Управляемые марковские процессы и их приложения. – М.: Наука, 1975. – 338 с.