УДК 004.942 (045)

Домарев Д.В.

МАТЕМАТИЧЕСКОЕ ОПИСАНИЕ ПРОЦЕССОВ АТАК НА КОМПЬЮТЕРНЫЕ СЕТИ

Институт компьютерных технологий
Национального авиационного университета

Рассмотрены атаки класса DOS, Марковская модель ветвящейся атаки, Марковские процессы гибели и размножения атак, Полумарковские процессы как модели процессов атак на компьютерные сети. Приведен расчет основных параметров защищенности системы на основе рассмотренных моделей. Сделан вывод о применимости Полумарковских процессов в исследовании процессов атак

DOS-атаки

На сегодняшний день существует мало математических исследований в области описания процессов атак на компьютерные сети при том, что количество методов атак растет.

Известным классом являются атаки типа "отказ в обслуживании" (*DOS*-атаки). Смысл данных атак заключается в посылке большого количества пакетов на заданный узел или сегмент сети, что может привести к его перегрузке и выведению этого узла или сегмента из строя, поскольку он не сможет обрабатывать запросы авторизованных пользователей [3].

Традиционная модель атаки основана на принципе "один к одному" (рис. 1 *а*) или "один ко многим" (рис. 1 *б*), т.е. атака исходит из одного источника. В модели скоординированной или распределенной (*Distributed DOS*, или *DDOS*) атаки используются принципы отношения "много к одному" и "много ко многим" (рис. 1 *в* и рис. 1 *г* соответственно). В случаях присутствия нескольких целей, могут иметь место процессы гибели и размножения атак, изучение которых позволит разработать алгоритмы блокирования и контратак.

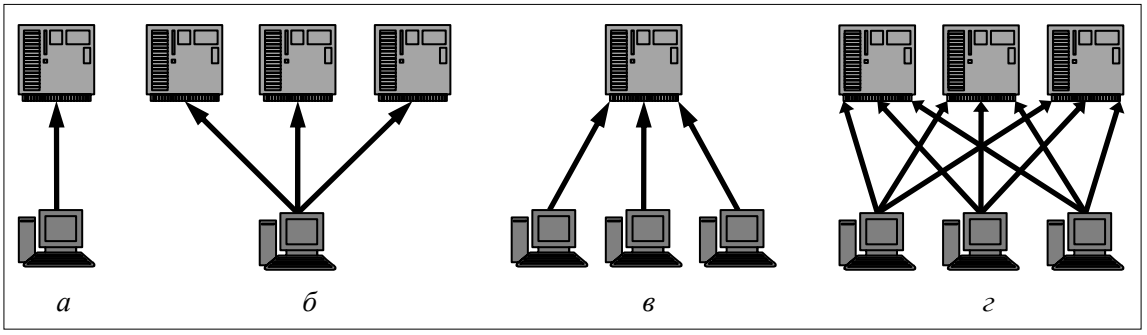

Рис. 1. Простые (*а*, *б*) и распределенные (*в*, *г*) *DOS*-атаки

Марковская модель ветвящегося процесса. Предельные вероятности состояния сетевого узла

Распределенная атака, в которой нападающие компьютеры не только воздействуют на цель атаки, но и "заражают" другие узлы (устанавливая вредоносное ПО, либо передавая определенные команды), присоединяя их к числу атакующих, может быть описана как случайный ветвящийся процесс. Ветвящаяся атака (рис. 2) представляется как частица, которая с течением времени порождает подобные себе частицы, либо исчезает (прекращение атаки конкретным узлом).

В [5] изложены доказательства следующего. Вероятности $p_k(t)$ того, что за время t частица, независимо от других, с вероятностью $p_k(t)$ превратится в k частиц, и вероятности $p_{ij}(t)$ того, что i частиц

за время t превратятся в j частиц, задаются производящими функциями:

$$x(t,z)=\sum_{k=0}^{\infty}p_k(t)z^k,$$

$$x_i(t,z)=\sum_{j=0}^{\infty}p_{ij}(t)z^j.$$

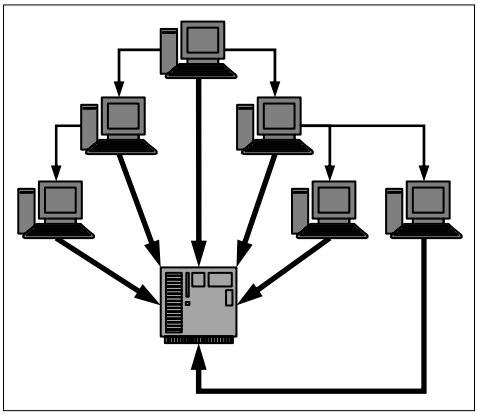

Рис. 2. Ветвящаяся атака

В случае непрерывного времени, производящие функции могут быть получены из дифференциального уравнения

$$\frac{d}{dt}x(t,z)=\varphi[x(t,z)],$$

где $\varphi(z)=\sum_{k=0}^{\infty}\lambda_k z^k$, λ_k – вероятности перехода из состояния 1 в состояние k (λ_1=-λ), $z\in[0;1]$ – числовой параметр, начальное условие $x(0,z)=z$. Из решения уравнения в неявной форме

$$t=\int_z^x\frac{dz}{\varphi(z)},$$

определяется функция $x=x(t,z)$. из разложения которой получаются вероятности $p_k(t)$.

Пусть в исходный момент t_0=0 имеется i частиц, тогда:

– вероятность прекращения атаки за время t (вероятность вырождения):

$$P\{\tau<t\}=[x(t,0)]^i,$$

где τ – момент, когда все частицы исчезнут (j=0);

– среднее количество атакующих через время t (для непрерывного распределения):

$$M\xi(t)=ie^{at},\ a=\lim_{n\to\infty}x(n,z)\in[0;1);$$

– вероятность образования бесконечного количества атакующих (вероятность взрыва) через время t:

$$p_\infty(t)=\begin{cases}0, & \exists z_0:\int_{z_0}^1\frac{dz}{\varphi(z)}=-\infty,\\ 1-x_0(t), & \int_{z_0}^1\frac{dz}{\varphi(z)}>-\infty\ \forall z_0,\end{cases}$$

где $x_0(t)$ – минимальное решение дифференциального уравнения $x'=1/\varphi(x)$ с начальным условием $x(0)=1$;

– вероятности конечных состояний системы описываются предельным распределением

$$\eta(t)=\xi(t)\frac{1-x(t,0)}{M(t)},\quad t\to\infty.$$

При a=0 или $a\to0$ оно является показательным:

$$F_{\eta(t)}(y)\Rightarrow F(y)=\begin{cases}0, & y<0,\\ 1-e^{-y}, & y>0.\end{cases}$$

Марковские процессы гибели и размножения

Процессы гибели и размножения описывают состояние атаки с несколькими целями. Атакуемая система может находиться в одном из состояний $E_0,E_1,E_2,\ldots E_i$, где i – количество узлов, выведенных из строя атакой. Переход $E_n\to E_{n-1}$ означает восстановление (отражение атаки) одного узла, а переход $E_n\to E_{n+1}$ – выход из строя одного узла. Если переходы $E_n\to E_{n+1}$ невозможны, то процесс называется процессом гибели (атак). Если возможны только переходы $E_n\to E_{n+1}$, то процесс называется процессом размножения (атак). Например, процесс обслуживания простейшего потока заявок представляет собой процесс чистого размножения. Процесс обслуживания с ожиданием в системе из m обслуживающих устройств является процессом гибели и размножения.

В [2] представлено математическое описание состояния процесса гибели и

размножения. Пусть вероятность перехода $E_n \to E_{n+1}$ по истечении времени (t_n, t_n+h) равна $\lambda_n h+o(h)$, а перехода $E_n \to E_{n-1}$ соответственно $\mu_n h+o(h)$. Здесь $o(h)$ – величина второго порядка малости по сравнению с первым слагаемым, которой в инженерных расчетах можно пренебречь. Вероятности переходов описываются системой дифференциальных уравнений (1).

$$\begin{cases} P_0'(t) = -\lambda_0 P_0(t) + \mu_1 P_1(t), \\ P_k'(t) = -(\lambda_0 + \mu_k) P_k(t) + \lambda_{k-1} P_{k-1}(t) + \mu_{k+1} P_{k+1}(t) \; \forall k \geq 1, \end{cases} \quad (1)$$

где $P_k(t)$ – вероятность того, что система в момент t находится в состоянии E_k. Для описания атаки, предположим, что начальное состояние системы было E_0, т.е. до атаки отсутствуют неисправные узлы.

Процесс распределенной атаки похож на процесс массового обслуживания в системе с потерями: система может находиться лишь в состояниях $E_0, E_1, \ldots E_m$ и вероятности переходов

$$P(h)\{E_k \to E_{k+1},\ k<m\} = \lambda h + o(h),$$

$$P(h)\{E_k \to E_{k-1},\ k>0\} = k\mu h + o(h),$$

$$P(h)\{E_k \to E_k,\ k<m\} = 1-\lambda h - k\mu h + o(h),$$

где λ – параметр распределения вероятности атаки. Условия схемы процесса:

$$\begin{cases} \lambda_k = \lambda \; \forall k < m, \\ \lambda_k = 0 \; \forall k \geq m, \\ \mu_k = 0, \quad k = 0, \\ \mu_k = k\mu, \quad 1 \leq k \leq m. \end{cases}$$

Решение (1) при этих условиях для любого распределения длительности атак со средним значением $1/\mu$ имеет вид (2).

$$P_k = \frac{\frac{1}{k!}\rho^k}{1+\rho+\frac{1}{2}\rho^2+\ldots+\frac{1}{m}\rho^m}, \quad \rho = \lambda/\mu, k \in [0;m]. \quad (2)$$

При $k=m$, из (2) находится вероятность отказа системы (все узлы выведены из строя):

$$P_m \frac{\frac{1}{m!}\rho^m}{\sum_{k=0}^{m}\frac{1}{k!}\rho^k}.$$

Из (2) также находится среднее количество выведенных из строя узлов:

$$a_m = \sum_{k=0}^{m} k P_k = \rho(1-P_m).$$

Полумарковские процессы как модели процессов атак на компьютерные сети

Атака на сеть с несколькими слоями защиты может быть описана обычным Полумарковским процессом. В [4] изложен вариант такого описания.

Текущее состояние процесса атаки на сеть представлено как частица, а процесс перехода из одного состояния в другое – как процесс случайного блуждания этой частицы. Пусть число экранов системы защиты равно N, а состояние s_0 – отражение атаки от внешнего экрана. Состояние s_{1i} – прохождение атакующего субъекта через i-й экран, а состояние s_2 – преодоление всех защитных экранов и проникновение в ядро защищаемого объекта.

Перемещение частицы может происходить из состояния s_0 через состояния s_{1i} в состояние s_2 и обратно. Очевидно, состояние s_{1i} является неким идеальным состоянием, вероятность которого $p_{1i}=P(s=s_{1i})$ равна нулю. Поэтому, для приведения процесса к Марковскому введены некоторые дополнительные состояния $s_{1i+\varepsilon}$ и $s_{1i-\varepsilon}$ в малых окрестностях точек s_{1i}.

Процесс рассмотрен как блуждания частицы между упругими жесткими экранами S_0 и S_{1i} и поглощающим экраном S_2

(рис. 3). Наличие экранов означает следующее:

– если частица попадает в точку S_0, то в следующий момент времени частица с вероятностью r попадет в точку $S_{0+\varepsilon}$ либо с вероятностью $1–r$ останется в точке S_0;

– если частица попадает в точку S_2, то в следующий момент времени частица с вероятностью q попадет в точку $S_{2-\varepsilon}$ либо с вероятностью $1–q$ останется в точке S_2.

На рис. 4 изображен граф состояний системы с вероятностями переходов для частного случая N=1 (s_{1i}=s_1, $s_{1i}\pm\varepsilon$=$s_1\pm\varepsilon$).

Изменения во времени соответствующих вероятностей состояния p_0, $p_{1-\varepsilon}$, $p_{1+\varepsilon}$, p_2 удовлетворяют уравнения Колмогорова (3) [1, 6].

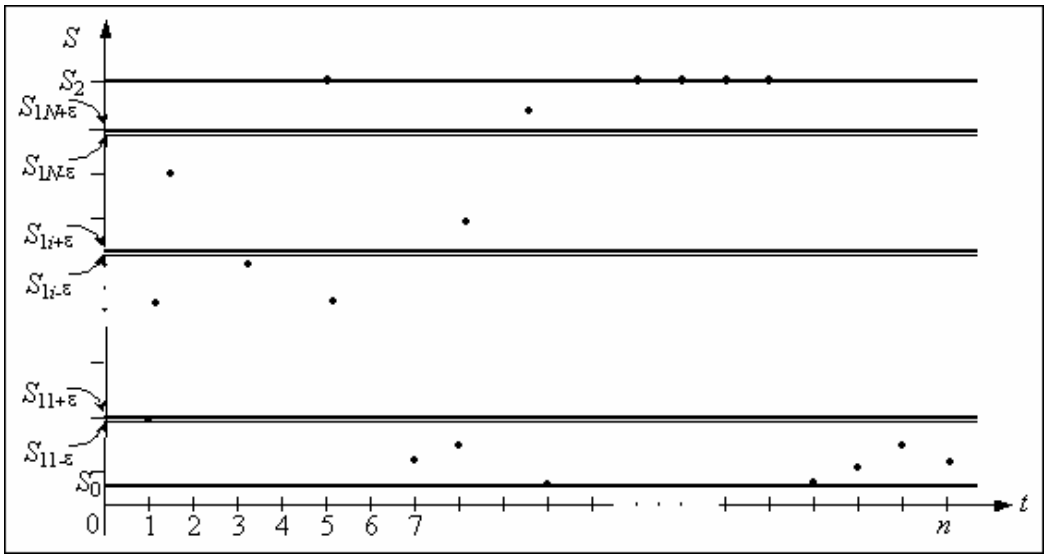

Рис. 3. Процесс блуждания частицы между экранами

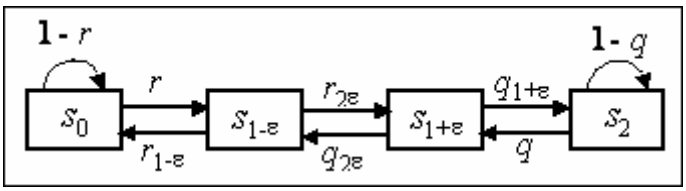

Рис. 4. Граф состояний для частного случая

$$\begin{cases} P_0'(t) = -rP_0(t) + (1-r)P_0(t) + r_{1-\varepsilon}P_{1-\varepsilon}(t), \\ P_{1-\varepsilon}'(t) = -r_{1-\varepsilon}P_{1-\varepsilon}(t) - r_{2\varepsilon}P_{1-\varepsilon}(t) + rP_0(t) + q_{2\varepsilon}P_{1+\varepsilon}(t), \\ P_{1+\varepsilon}'(t) = -q_{2\varepsilon}P_{1+\varepsilon}(t) - qP_{1+\varepsilon}(t) + r_{2\varepsilon}P_{1-\varepsilon}(t) + q_{1+\varepsilon}P_2(t), \\ P_2'(t) = -qP_2(t) + (1-q)P_2(t) + q_{1+\varepsilon}P_{1+\varepsilon}(t). \end{cases} \quad (3)$$

Интегрируя эту систему уравнений при заданных начальных условиях, получаем вероятности состояний как функции времени. Для примера, которому соответствует график на рис. 3, начальные условия таковы:

$$P_{11-\varepsilon}=1,\ P_0=P_{11+\varepsilon}=P_2=0.$$

В свою очередь, вероятности переходов определяются отношением мгновенной интенсивности атак $\lambda_{мгн}$ к скорости реакции системы защиты (интенсивности потока обслуживания атак) μ. Для случая постоянной на интервале наблюдения интенсивности атак λ, решение системы уравнений (3) тривиально. Оно представляет собой экспоненциальную функцию, параметры которой полностью определяются соотношением λ/μ и начальным состоянием системы.

В случае переменной интенсивности трафика получаем систему параметрических дифференциальных уравнений первого порядка, общее решение которой имеет следующий вид (пример для вероятности p_0):

$$P_0(t) = e^{\left\{-\int\left[1-2r(t)\right]dt\right\}} \int P_{1-\varepsilon}(t)\, r_{1-\varepsilon}(t)\, e^{\left[\int r(t)dt\right]}\, dt + C\, e^{\left\{-\int\left[1-2r(t)\right]dt\right\}},$$

где C – постоянная величина, определяемая из начальных условий.

Таким образом, можно получить количественные оценки эффективности отражения атак в зависимости от интенсивности входного потока и скорости обработки в устройстве защиты.

Выводы

С учетом вышеуказанного, выделены следующие состояния сетевого узла, относительно атак:

1. Норма (N) – обычный режим работы;
2. Атакуемый (A_i) – попытка несанкционированного доступа (НСД):
   - 2.1. Прохождение 1-го слоя защиты;
   - …
   - 2.n. Прохождение n-го слоя защиты;
3. Защита (R_i) – остановка НСД:
   - 3.1. Восстановление n-го слоя защиты;
   - …
   - 3.n. Восстановление 1-го слоя защиты;
4. Контратака (C) – блокировка угрожающего узла;
5. Отказ (F) – выход узла из строя;
6. Атакующий (I) – присоединение к группе атакующих узлов.

Граф состояний представлен на рис. 5. Параметры функций переходных вероятностей могут быть рассчитаны, основываясь на статистических результатах наблюдений сетевой активности.

Марковские процессы имеют широкую применимость в моделировании состояний систем при атаках, так как позволяют абстрагироваться от закона распределения времени прихода сообщений. Это позволяет отдельно исследовать состояния системы, рассчитывать вероятности успеха атаки или ее отражения, конечное состояние системы, а так же показатели эффективности защиты.

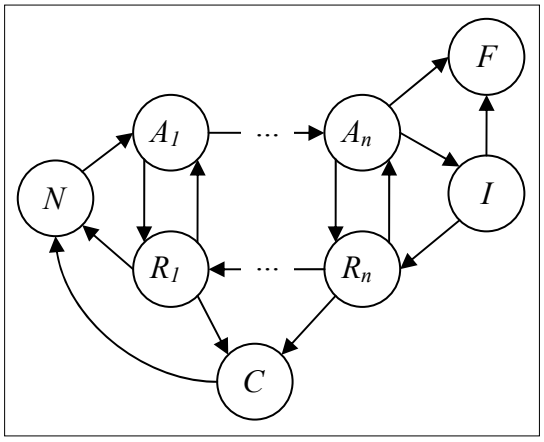

Рис. 5. Граф состояний атакуемого сетевого узла

Список литературы

1. *Вентцель Е.С.* Исследование операций. – М.: Сов. радио, 1972. – 552 с.

2. *Гнеденко Б.В., Коваленко И.Н.* Введение в теорию массового обслуживания. – М.: Наука, 1987. – 336 с. Разд. 1.2 – 1.4.

3. *Лукацкий А.В.* Мир атак многообразен. Журнал "Сетевой", №11, 2001.

4. *Милокум Я.В.* Метод последовательного обнаружения угроз компьютерной сети. Наукові записки УНДІЗ, №4(6), 2008. – С. 79–88.

5. *Прохоров Ю.В., Розанов Ю.А.* Теория вероятностей. Основные понятия. Предельные теоремы. Случайные процессы – М.: Наука, 1967. – С. 282–296.

6. *Тихонов В.И., Миронов М.А.* Марковские процессы. – М.: Сов. радио, 1977. – 488 с.

Подано до редакції 10.03.10