УДК 004.942:004.056.53

А.И. Михалев, Ю.О. Калиберда

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ИММУННОГО ОТВЕТА НА ВТОРЖЕНИЕ В КОМПЬЮТЕРНУЮ СЕТЬ

Введение

В настоящее время основные параметры практически всех технологических процессов контролируются компьютерными системами под управлением мощных серверов, которые, как правило, соединены между собой в локальные или корпоративные сети предприятий. Для повышения надежности и долговечности такого класса сложных технических систем необходима защита сетей как от вторжений извне, так и от ошибок пользователя.

В то же время, современные программные средства обеспечения информационной безопасности, реализующие методы сигнатурного анализа для выявления вторжений, или методы статистического анализа для выявления аномалий, не могут обеспечить гарантированной или даже приемлемой защиты кибернетического пространства компьютерных систем и корпоративных сетей от нарастающей угрозы все новых и разнообразных атак [2].

В данной работе рассмотрена математическая модель отражения атак извне, основанная на принципах иммунного ответа [1,3]

Математическая модель иммунного ответа

Пусть основными действующими факторами вторжения и иммунного ответа являются следующие величины:

$V(t)$ — концентрация антигенов в момент времени t. Под антигеном понимается количество вторжений и вредоносных действий.

$F(t)$ — концентрация антител в момент времени t. Под антителами понимаются, принятие соответствующих правила и действий, способствующие предотвращению негативного воздействия на компьютерную сеть.

$C(t)$ — концентрация детекторов. Количество детекторов, способных определить вредоносный код, несанкционированные действия, аномальное поведение сети, и т.д.

Математическое описание динамики иммунного ответа представляет собой систему трех дифференциальных уравнений.

Первое уравнение характеризует изменение числа антигенов:

$$dV = \beta V dt - \gamma F V dt . \quad (1)$$

Здесь, первый член уравнения описывает прирост антигенов dV за интервал времени dt. Как видно, он пропорционален V и некоторому числу β, которое будем называть коэффициентом «размножения» антигенов. В данном контексте размножение следует понимать как увеличение количества атак или вредоносных действий на компьютерную сеть. При этом член $\gamma FVdt$ описывает число антигенов, нейтрализуемых антителами F за интервал времени dt, где γ — коэффициент, связанный с вероятностью предотвращения несанкционированных действий.

Второе уравнение описывает рост числа детекторов. При этом число детекторов зависит от количества вторжений в данный момент времени:

$$dC = \alpha V(t - \tau)dt - \mu_c dt . \quad (2)$$

В данном уравнении, первый член в правой части описывает генерацию детекторов; τ — время, в течение которого осуществляется формирование каскада детекторов. В свою очередь, второй член в этой формуле описывает уменьшение числа детекторов, μ_C — коэффициент, характеризующий время работы детектора.

Третье уравнение математической модели иммунного ответа характеризует баланс числа антител, реагирующих с антигеном:

$$dF = \rho C dt - \eta\gamma F V dt - \mu_f F dt . \quad (3)$$

Здесь, первый член ρCdt описывает генерацию антител детекторами за интервал времени dt; ρ — скорость производства антител одним детектором. Слагаемое $\eta\gamma FVdt$ описывает уменьшение числа антител в интервале времени dt за счет взаимодействия с вторжениями;

 ISSN 1562-9945

$\mu_f Fdt$ описывает уменьшение популяции антител за счет прекращения активности данного вторжения; μ_f — коэффициент, характеризующий время работы антител.

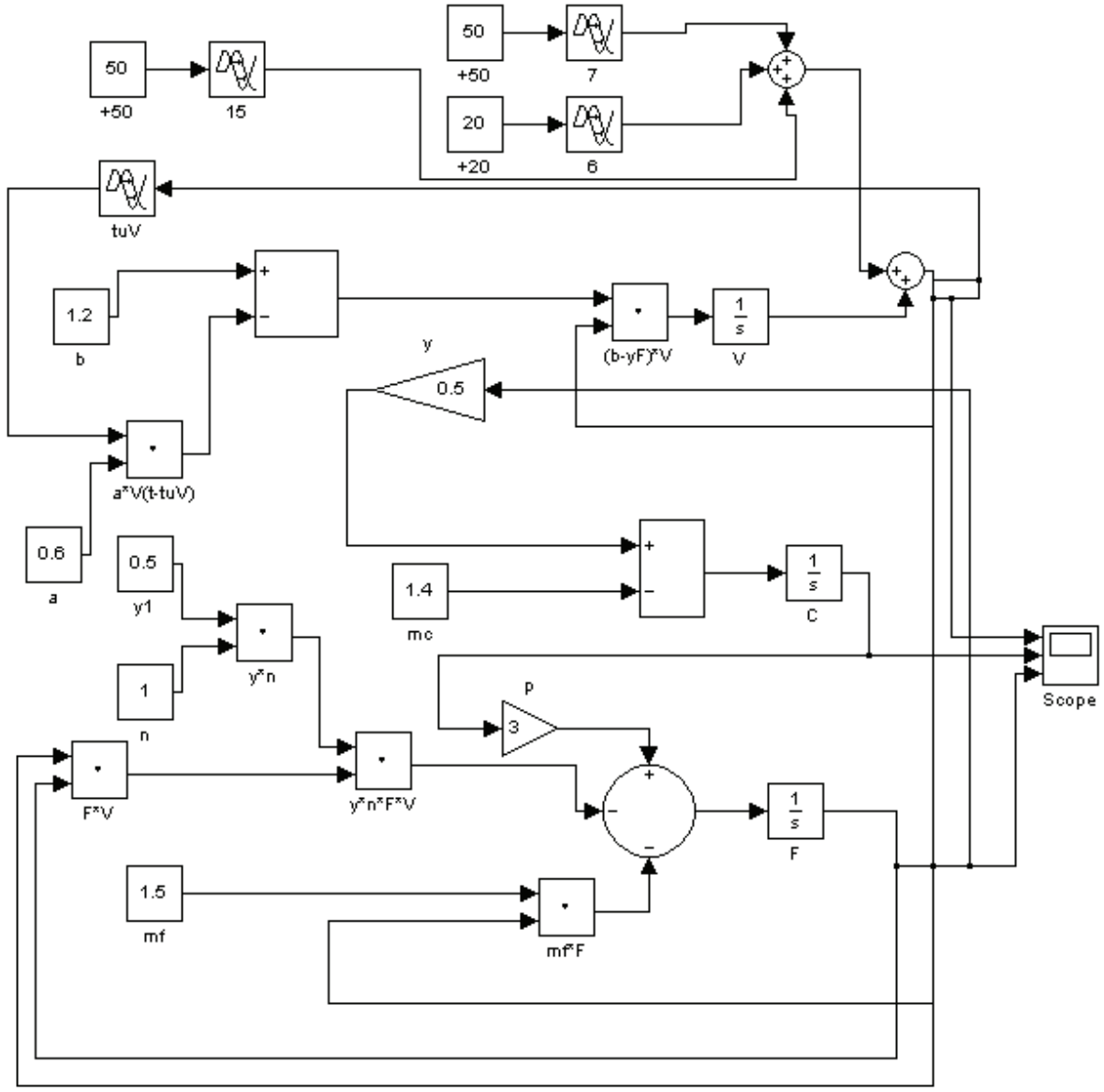
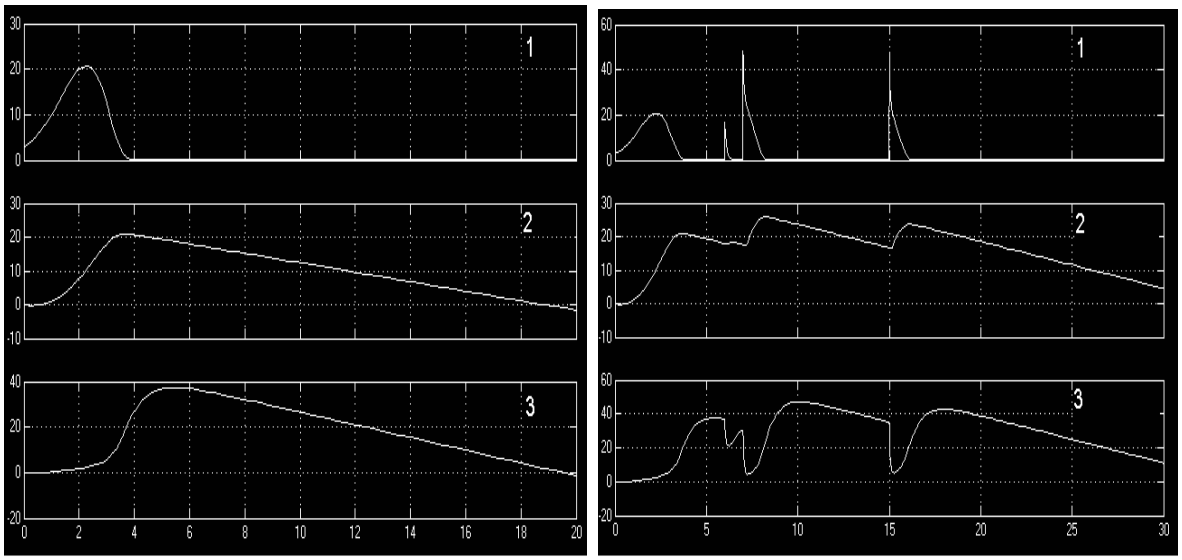


Рисунок 1 – Программная реализация модели (1-3) в среде Simulink



а) б)

Рисунок 2 – Иллюстрация работы системы (1 – количество атак; 2 – количество детекторов; 3 – количество антител): а) – система подвергнута единственной атаке; б) – система подвергнута нескольким атакам через некоторый промежуток времени;

Вывод

Как видно из приведенного выше, система, испытавшая атаку, вырабатывает антитела, которые предотвращают данное вторжение (рис.2.а). Однако, в случае повторной атаки, когда система еще не вышла из режима повышенной защиты, возникающие вновь атаки, также эффективно пресекаются, не нагружая при этом систему для выработки новых антител (рис 2.б).

ЛИТЕРАТУРА

1. Михалев А.И., Калиберда Ю.О. Применение искусственных иммунных систем для выявления аномалий в сетевом трафике // Міжнародна наукова конференція Інтелектуальні системи прийняття рішень та прикладні аспекти інформаційних технологій (ISDMIT` 2006) 2006 (2) - с.215-217.
2. D. Dasgupta and S. Forrest. Artificial Immune Systems in Industrial Applications. In the proceedings of the Second International Conference on Intelligent Processing and Manufacturing of Materials (IPMM), Honolulu, July 10-15, 1999.
3. Dominik Wodarz. Mathematical and Computational Approaches to Immunology, 2007.

Получено 17.03.2008 г.