УДК 621.396:004.056

ЗАСТОСУВАННЯ НЕЧІТКОЇ ЛОГІКИ ДЛЯ ВИЯВЛЕННЯ DDOS-АТАК

Іванько І.К.
Науковий керівник – к.т.н., старший викладач Василенко Т.О.
Харківський національний університет радіоелектроніки, каф. КРіСТЗІ,
м. Харків, Україна
e-mail: iryna.ivanko@nure.ua

In order to detect a DDoS attack and not to resort to full network monitoring and check all received packets, since detecting this type of attack is quite simple using signs that can be seen without using special equipment and specialized programs. The ability to use the command line and view the Internet interface of the router is enough. With the help of fuzzy logic variables and membership functions, these features are generalized, for the possibility of using the previously developed method of protecting wireless networks, based on fuzzy logic, without using large-scale calculations and building new membership functions every time.

Розглянемо узагальнений підхід до нечіткого опису станів бездротової мережі з метою виявлення аномального її стану, що дозволяє використання методу [1] на будь-якій мережі, без використання масштабних обчислень.

Великим недоліком у визначенні атак є те, що всі ознаки неможливо виразити в чіткому чисельному показнику, що змушує вдаватися для захисту мережі до величезних витрат: купувати дорогі програми, які детально вивчають трафік переданий в мережі.

Всі ці показники можна вимірювати за допомогою нечітких описів, що призводить до необхідності використання апарату нечіткої логіки. За допомогою нечіткої логіки можливо не робити масштабні обчислення і не витрачати часу на моніторинг, що дозволить зберегти витрати на захист бездротової мережі і зберегти її безпеку.

Розглянемо узагальнений підхід до нечіткого опису станів бездротової мережі з метою виявлення її аномального стану. Нехай маємо безліч ознак (параметрів мережі) $Y = \{y_1, y_2, \dots, y_j\}$, на підставі яких визначається аномальний стан мережі. Ведемо коефіцієнт інформативності кожної ознаки d_i, $d_i = [0,1]$, $i = \overline{1,j}$.

Кожна ознака y_j описується лінгвістичною змінною – $\langle N, y_j, T_j, U_j, G, M \rangle$, де:

N – назва лінгвістичної змінної (у нашому випадку – «ступінь аномальності бездротової мережі»); y_j – назва ознаки (параметр мережі); $T_j = \langle T_j^1, T_j^2, \dots, T_j^K \rangle$ – базова терм-множина лінгвістичної змінної j-ї ознаки або безліч її значень (термів); U_j – базова множина ознаки y_j ; G – синтаксична процедура; M – семантична процедура.

В якості терм-множин для всіх ознак пропонується впорядкована множина: T_j ={нормальна робота мережі; аномальний стан, ступінь аномальності низький; аномальний стан, ступінь аномальності середня; аномальний стан, ступінь аномальності висока}.

Так як наша множина складається з кінцевої кількості елементів, визначення сумарного ступеня належності по всій множині ознак, що використовуються, з урахуванням ступеня їх інформативності для кожного терма здійснюється з виразу: $\mu_{T^k}(y_1, y_2, \dots, y_j) = \sum_{j=1}^{J} d_j \mu_{T_j^k}(y_j)/y_j$.

Розглянемо, як експерт визначає ступінь аномальності бездротової мережі, за допомогою поняття «низька аномальність», «нормальна робота» та «велика аномальність», при цьому мінімальне завантаження маршрутизатора 0%, а максимальне – 100%.

Формалізація цього опису може бути проведена за допомогою лінгвістичної перемінної $\langle N, y_j, T_j, U_j, G, M \rangle$, де:

N – аномальність бездротової мережі (що експерт визначає); y – завантаження маршрутизатора (параметр, який оцінює експерт); T – {«низька аномальність», «нормальна робота», «велика аномальність»} (базова терм-множина); U – [0, 100] (межі, в яких може змінюватися завантаження маршрутизатора); G – процедура утворення нових термів за допомогою зв'язок «і», «або» та модифікаторів типу «дуже», «не», «злегка» та ін. Наприклад, «дуже низька аномальність», «дуже висока аномальність» та ін; M – процедура завдання на U = [0, 100] нечітких підмножин A1 = «низька аномальність», A2 = «нормальна робота», A3 = «велика аномальність».

Функція належності нечітких множин A1, A2, A3 може мати вигляд показаний на Рис.1.

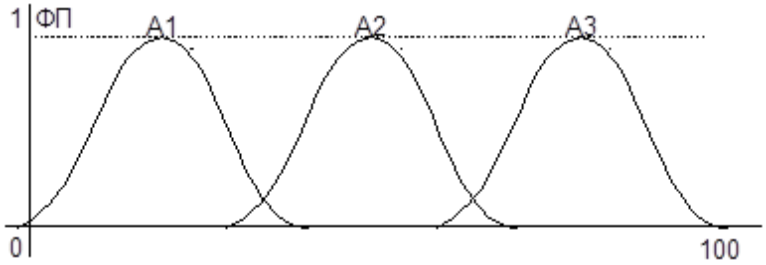

Рис. 1

За допомогою запропонованих механізмів можна узагальнити різні мережі і для застосування потрібно буде знати лише межі нормального завантаження маршрутизатора мережі, або будь-якої іншої ознаки атаки.

Список використаних джерел:

1. Антипов И. Е. Применение нечеткой логики для повышения безопасности беспроводных сетей на базе технологии Wi-Fi / И. Е. Антипов, Т. А. Ященко, Нух Таха Насиф // Радиотехника: материалы Всеукр. межвед. науч.-техн. сб. 2011. Вып. 165. С. 103-106.