УДК 681.3
© І.Тишик[6], 2015

ВИЯВЛЕННЯ АНОМАЛІЙ В МЕРЕЖЕВОМУ ТРАФІКУНА ОСНОВІ ВЕЙВЛЕТ-ПЕРЕТВОРЕННЯ

У статті подано механізм виявлення атак перехоплення сеансу зв'язку в бездротових мережах. Запропонований механізм виявлення базується на визначенні аномалій у прийнятих сигналах. Розроблена математична модель, яка описує зміну рівня сигналу протягом сесійної атаки (поява аномалії). Запропоновано алгоритм оптимальної фільтрації на основі вейвлет-перетворення для виявлення таких аномалій.

Ключові слова: механізм виявлення, атаки перехоплення, бездротові мережі, математична модель, алгоритм оптимальної фільтрації.

This paper presents a mechanism for detecting hijacking attacks session in wireless networks. The proposed scheme is based on detecting of anomalies in the received signals. A mathematical model to describe the signal strength during a hijacking session (anomaly's appearance) has been developed. The algorithm of optimal filtration by wavelet transformations has been designed for the purpose of such anomalies detection.

Keywords: detecting mechanism, hijacking attacks, wireless networks, mathematical model, algorithm of optimal filtration.

1. ВСТУП

Серед різноманітних атак,які загрожують бездротовим локальним мережам, атака типу перехоплення сеансу зв'язку є однією з найпоширеніших. В перехоплені сеансу зв'язку зловмисник примушує користувача спочатку припинити зв'язок його хоста з точкою доступу (ТД), після чого зловмисник зв'язується з цієюТД маскуючись під MAC-адресою даного користувача та привласнює його сеанс. Сучасні методи виявлення такого типу атаки в основному ґрунтуються на передбачені та виявлення зміни параметрів, наприклад, зміна послідовності чисел при обміні даними [1].

У статті розглядається механізм виявлення сесійних атак за допомогою періодичного моніторингу та контролю за рівнем прийнятого сигналу для конкретної MAC-адреси. Якщо зловмисник підміняє MAC-адресу деякого користувача, то

[6] Національний університет "Львівська політехніка"

моніторинг покаже різку зміну рівня сигналу (аномалію)для профілю MAC-адреси цього користувача. У праці[2] показано, що будь-яка непередбачувана динамічна зміна рівня сигналу від вузла зв'язку може вказувати на підозрілу активність. Проте, на рівень сигналу впливає як його розсіювання, так і затінення, що може привести до непередбачених змін рівнів отриманих від вузла сигналів у кожен наступний момент часу [3]. Для того, щоб відрізняти такого виду втрати енергії сигналу від атаки, у ряді наукових робіт проводяться подальші дослідження [2-4].

У роботі з метою розроблення механізму виявлення сесійної атаки була розроблена математична модель, яка описуєзмінурівнів сигналу для різногочасового періоду, при цьому вважається, що відбувається атака типу перехоплення сеансу.

Різка зміна рівня сигналу, обумовлена згаданим видом атаки, приймається за "сигнал", а змінайого рівня, викликана сумою різних видів енергетичних втрат, розглядається як "шум". Оскільки "шум" має складну форму спектральноїгустинипотужності, то розробка та застосування оптимальних фільтрів на основіперетворень Фур'є не є достатньо ефективним, враховуючи те, що аналіз сигналів нескінченої крутизни лише у частотній області не забезпечує якісного виявлення їх особливостей. Показано, що техніка вейвлет-перетворення потенційно здатна ефективніше вирішити дану проблему, представляючи "сигнал" в часо-частотній області [5].

Використовуючи добре локалізований в часі базис вейвлет-функції, було запропонованівідповідний алгоритм оптимальної фільтрації, що дозволить ефективно виявляти аномалії "сигналів" на тлі завад.

2. МАТЕМАТИЧНА МОДЕЛЬ ДЛЯ СИГНАЛУ В МОМЕНТ ПЕРЕХОПЛЕННЯ СЕАНСУ

В роботі використовується модель оцінки втрат L(дБ) на шляху поширення сигналу, згідно якої співвідношення для отриманого P_{r} та переданого сигналів P_{u}, подається як [6]:

$$L = \frac{P_r}{Pu} = K + \gamma \lg d + \varphi + \Phi , \qquad (1)$$

де $\gamma \lg d$ –коефіцієнт втрат, який залежить від відстані d між передавачем та приймачем; K – безрозмірна константа, яка залежить від середовища поширення сигналу; φ– коефіцієнт тіньового

затухання;*Ф*– представляє енергетичні втрати, викликані розсіюванням сигналу і залежить як від середовища поширення, так і від швидкості переміщень користувачів бездротової мережі.

Робиться припущення, що користувач і зловмисник знаходяться в середовищі поширення сигналу з параметрами [K_i, γ_i , φ_i , Φ_i], де i=0 для користувача та i=1 для зловмисника. Тоді моніторинг рівня сигналу *x(t)* визначаєтьсяяк:

$$x(t) = N(t) + f(t) = N(t) + \Delta m * u(t - t_0), \quad (2)$$

де *f(t)* представляє "сигнал" і *N(t)* представляє "шум"; *u(t)* – одиничний стрибок, який з'являється у деякий момент часуt_0. Амплітуда стрибка функції *f(t)* у момент часуt_0подається як:

$$\Delta m = K_1 - K_0 + \gamma_1 \lg d_1(t_0) - \gamma_0 \lg d_0(t_0), \quad (3)$$

де $d_0(t_0)$– відстань між бездротовим користувачем до ТД у момент часу t_0; $d_1(t_0)$– відстань між бездротовим зловмисником до ТД.

При розробленні математичної моделі для моментів перехоплення сеансу використовується неперервна в часі модель сигналу. Припускається, що користувач і зловмисник можуть як переміщатися один відносно одного, так і залишатися стаціонарними.

$$N(t) = \begin{cases} N_1(t), t \le t_0 \\ N_2(t), t \ge t_0 \end{cases}, \quad (4)$$

де $N_1(t) = K_0 + \gamma_0 \lg d_0(t) + \varphi_0 + \Phi_0$, а

$$N_2(t) = K_0 + \gamma_0 \lg d_0(t_0) + \gamma_1 \lg \frac{d_1(t)}{d_1(t_0)} \varphi_1 + \Phi_1$$

Розглянута модель актуальна для таких випадків поширення сигналу як: закритий офіс, пішохідне переміщення із закритого приміщення у відкритий простір, переміщення автомобілем [6]. Несуча частота сигналу $\omega_c = 2.4 \times 10^9$ Гц, що є типовим в мережах, заснованих на стандарті IEEE 802.11.

Для приміщення дисперсія затухаючого сигналу становить 12 Дб. Для відкритого простору дисперсія становить 10 Дб. Якщокористувач і зловмисник знаходяться в приміщенні, товеличина затухання сигналу *N(t)* має однаковий статистичний розподіл до і після атаки. Якщо один із них знаходиться у відкритому просторі, то*N(t)* зменшується, що робить виявлення *f(t)* простішим.

3. ОПТИМАЛЬНИЙ ВЕЙВЛЕТ-БАЗИС

Відомо, що аналіз сигналу на основі вейвлет-перетворення є ефективним, якщо необхідно виявити його особливості, наприклад, перепади рівня. Ефективність вейвлет-перетворення обумовлена забезпеченням ним постійної роздільної здатності сигналів у їх широкому частотному діапазоні, яка досягається за рахунок зміни масштабу базової вейвлет-функції та її ітеративного зміщення, що дає змогу забезпечити пропорційну роздільну здатність у кожній частотній смузі розкладу. Це дає можливість при вейвлет-перетворенні враховувати різкі зміни сигналів при аналізі їх високочастотних компонент [7].

У ключі даної роботи вейвлет-перетворення описується як $d_x(j,k)=\langle x,\ \psi_{j,k}\rangle$, де $d_x(j,k)$ –вейвлет коефіцієнти сигналу $x(t)$ на масштабіj та в часі k, а $\psi_{j,k}\psi(t)$– вейвлет-функція, отримана з материнської $\psi(t)$.[5, 7]

Для виявлення сигналу, який являє собою ступінчасту функцію у шумовому тлі, використовується вейвлет Хара $\psi(t)$,оскільки він найкраще придатний до апроксимації сигналів з перепадами нескінченої крутизни, а тому може бутиоптимальним фільтромдля поданого сигналу.Крім того, вейвлет Хара є нескладним у реалізації чисельними методами [5, 7].

Завдяки лінійним перетворенням, вейвлет-перетворення$x(t) = N(t) + f(t)$ подається як:

$$d_x(j,k) = d_N(j,k) + d_f(j,k), \tag{5}$$

де $d_f(j,k)$ – вейвлет-коефіцієнтидеталізації кроку функції $f(t) = \Delta m * u(t-t_0)$. Прийнявши $I_\psi(t) = \int_{-\infty}^{t} \psi(u)du$, отримаємо:

$$d_f(j,k) = -\Delta m \cdot 2^{\frac{j}{2}} I_\psi(t_0 2^{-j} - k) \tag{6}$$

Варто зауважити, що $d_f(j,k)$ є детермінованим процесом, а$d_N(j,k)$ – вейвлет-коефіцієнти стохастичного процесу $N(t)$. Відношення сигнал-шум SNRв області вейвлет-перетворенняумомент часу t_0 та на масштабі jописуєтьсярівнянням:

$$\gamma(j) = \frac{\left|d_f(j,k)\right|^2}{\mathrm{var}(d_N(j,k))} = \frac{\Delta m^2 2^j \left|I_\psi(2^j t_0 - k)\right|^2}{\mathrm{var}(d_N(j,k))} = \frac{\Delta m^2 2^j \left|I_\psi(0)\right|^2}{\mathrm{var}(d_N(j,k))}, \tag{7}$$

де $t_0 = 2^j k$ і var() представляють дисперсію стохастичного сигналу.

Оскільки SNR детектора прямо пропорційний Δm^2, то з (7) випливає, що чим дальше зловмисник знаходиться від користувача, тим легше він виявляється. Враховуючи, що чисельник у рівнянні (7) пропорційний 2^j, то надалі доцільноздійснювати опрацювання сигналу на великих масштабах, що відповідає великим значенням j в часо-масштабнійобласті.

4. АЛГОРИТМ ФІЛЬТРАЦІЇ НА ОСНОВІ ВЕЙВЛЕТ-ПЕРЕТВОРЕННЯ

Враховуючи, що $N(t_0) = N_1(t_0) + N_2(t_0) + N_3(t_0)$ є сумою трьох незалежних один від одного компонентів: розсіювання, тіньового затухання та енергетичних втрат, обумовлених переміщеннями, то з врахуванням вищеподаного отримаємо:

$$\mathrm{var}(d_N(j,k)) = \mathrm{var}(d_{N1}(j,k)) + \mathrm{var}(d_{N2}(j,k)) + \mathrm{var}(d_{N3}(j,k)) \quad (8)$$

де $\mathrm{var}(d_{N1}(j,k))$, $\mathrm{var}(d_{N2}(j,k))$, $\mathrm{var}(d_{N3}(j,k))$ є представленням компонентів $N_1(t_0), N_2(t_0), N_3(t_0)$ на масштабі j відповідно. Вейвлет-коефіцієнти $d_{Ni}(j,k)$ (для i=1,2,3) дорівнюють нулю при стаціонарному процесі. У момент часу t_0 та масштабі j, $\mathrm{var} d_{Ni}(j,k)$ представляє енергію шуму $N_i(t)$ навколо частоти $2^{-j}\omega_0$, де ω_0 є максимумом частоти $N(t)$ та подається як:

$$\mathrm{var}(d_{Ni}(j,k)) = \int S_{Ni}(\omega) \cdot 2^j \left|\Psi(2^j \omega)\right|^2 d\omega, \quad (9)$$

де $\Psi(\omega)$ – частотний образ функції $\psi(\omega)$; $S_{Ni}(\omega)$ – спектральнагустинапотужності для N_i.

Для реалізації механізму щодо виявлення аномалій у прийнятому сигналі $x(t)$, необхідно цей сигнал представити у дискретній послідовності $x[n]$. Масштаб j обмежений нерівністю $0 \le j \le J_{\max}$, де $J_{\max} = \lfloor \log_2(M) \rfloor$ є максимальним масштабом розкладу і обмежується довжиною вхідної послідовності вибірок сигналу M.

Представляючи послідовність вибірок прийнятого сигналу як $x[n] = [x_1; \ldots; x_M]$, пропонований алгоритм виявлення описується наступними кроками:

1) Застосовуючи дискретне вейвлет-перетворення для $x[n]$, одержують коефіцієнти $d(k,j)$ при максимальному масштабі $J_{\max} \le \lfloor \log_2(M) \rfloor$, де k=1,..,M/2.

2) Порівнюють $d(k,j)$ з обчисленим значенням порогу $Thr_j = s/2$.

3) Формування сигналу тривоги, якщо $d(k,j) > Thr_j$ для деякого k.

Поріг $Thr_j = s/2 = \min\Delta m \cdot 2^{\frac{j}{2}-1}\left|I_\psi(0)\right|$ для вибраного масштабу j, при $\left|I_\psi(0)\right|$=0,5. Значення $\min\Delta m$ обчислюється емпірично дляконкретного випадку поширення сигналу [1].

5. ВИСНОВОК

Розроблено математичну модель, яка описує перепади рівня (аномалії) сигналу при реалізації атаки типу перехоплення сеансу зв'язку в бездротових мережах, обґрунтовано використання вейвлет-перетворення для ідентифікації появи таких аномалій. Запропоновано алгоритм оптимальної фільтрації на основі вейвлет-перетворення щодо виявлення аномалій у прийнятому сигналі.

1. R. Gill, J. Smith and J. A. Clark, "Detecting Session Hijacking Attacks inIEEE 802.11 Networks," Proceedings of Fourth Australasian InformationSecurity Workshop, pp. 221-230, vol.54, January 2006. 2. M. Flament and M. Unbehaun, "Impact of shadow fading in a mmwaveband wireless network," The 3rd Symposium on Wireless PersonalMultimedia Communications IEEE, Bangkok, Thailand, November 2000. 3. T. Odgen and O. Parzen, "Change-Point Approach to Data AalyticThresholding," Transanctions of Statistics and Computing, pp. 93-99,vol. 6, no. 2, November 2004.4. M. Raimondo and N. Tajvidi, "A Peaks Over Threshold Model ForChange-Point Detection By Wavelets," Statistica Sinica, pp. 395C412,vol. 14, part. 2, 2004. 5. Тишик І.Я. Комп'ютеризовані засоби оцінювання параметрів руху об'єктів на основі малохвильового (вейвлет) перетворення сигналів зондування: дис. кандидата технічних наук 05.13.05 / Тишик Іван Ярославович. – Л. 2014. – 256 с. 6. X. Lu, Y. Sang, J. Zhang, Y. Fa, "A Pipeline Leakage etectionTechnology Based on Wavelet Transform Theory," Proceedings of IEEEInformation Acquisition, pp. 1432-1437, vol.20, August 2006.7. M. Chabert, J.-Y.Tourneret, F. Castanie, "Additive and MultiplicativeAbrupt Jump Detection Using The Continuous Wavelet Transform,"Proceedings of IEEE Acoustics, Speech, and Signal Processing, pp. 3002-3005, vol.5, May 1996.