В.И.ЛЕТУН

СИСТЕМА КРИТЕРИЕВ И ПОКАЗАТЕЛЕЙ ЭФФЕКТИВНОСТИ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ РАДИОСИСТЕМ, СОГЛАСОВАННАЯ С ПОКАЗАТЕЛЯМИ КАЧЕСТВА РАДИОСВЯЗИ

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь, начальник научно-исследовательской лаборатории систем и устройств связи

В настоящее время радиосистемы широко применяются для передачи служебной и конфиденциальной информации в органах государственного управления, силовых структурах, на транспорте и в промышленности. Открытость радиотракта делает такие системы уязвимыми для перехвата сообщений, навязывания ложной информации, постановки преднамеренных помех, поэтому их функционирование невозможно без технических средств защиты (шифрование, скремблирование, скачкообразная перестройка рабочей частоты, аутентификация абонентов и др.) [2]. При этом любое средство защиты вносит в радиотракт собственные искажения и потери, ухудшая показатели качества радиосвязи. Вследствие этого оценка эффективности технических средств защиты в отрыве от показателей качества функционирования радиосистем методически некорректна: «идеально стойкая» защита может оказаться неприемлемой, если она срывает связь или существенно снижает ее качество.

Целью работы является разработка системы критериев и показателей эффективности технических средств защиты радиосистем, согласованной с показателями качества радиосвязи и обеспечивающей сопоставимость альтернативных вариантов построения защиты.

В работе предложено формировать систему критериев в три взаимосвязанные группы. Первая группа – критерии защищенности: стойкость к перехвату (трудоемкость раскрытия ключа или сообщения), вероятность навязывания ложной информации, стойкость к подавлению и обнаружению сигнала, время срыва защиты при активном воздействии нарушителя [1, 5]. Вторая группа – критерии согласованности с качеством радиосвязи, характеризующие деградацию радиотракта при включении средств защиты: приращение вероятности ошибки на бит $\Delta P_{ош}$, потеря энергетического запаса ΔE (дБ), вносимая задержка и расширение полосы занимаемых частот, снижение коэффициента готовности канала за счет дополнительных режимов синхронизации и распределения ключей [3]. Третья группа – критерии эффективности построения: аппаратные и временные затраты, стоимость внедрения и сопровождения защиты, массогабаритные и энергетические характеристики.

Согласование критериев с показателями качества радиосвязи выполняется через систему нормирующих ограничений. Каждому показателю качества (вероятность ошибки на бит, отношение сигнал/помеха на входе демодулятора, коэффициент готовности, время установления соединения) ставится в соответствие допустимое значение деградации, задаваемое тактико-техническим заданием. Показатели второй группы нормируются относительно этих допусков, благодаря чему требования к защите формулируются не абстрактно, а в едином измерительном пространстве с показателями качества радиосвязи. Сопоставление вариантов защиты выполняется по интегральному показателю $Э = \Sigma\, w_i \cdot K_i$, где K_i – относительные (нормированные) значения показателей, w_i – весовые коэффициенты, отражающие приоритеты конкретного применения [4]; вариант считается допустимым, только если все ограничения по качеству радиосвязи выполняются.

Структурная схема предложенного подхода приведена на рисунке 1.



Рисунок 1 – Структурная схема согласования критериев эффективности технических средств защиты с показателями качества радиосвязи

Практическая значимость подхода состоит в том, что он позволяет обоснованно выбирать рациональный вариант защиты для конкретной радиосистемы. Так, для узкополосных систем с жестким энергетическим бюджетом предпочтительными оказываются средства шифрования на канальном уровне с минимальной служебной избыточностью, тогда как в широкополосных системах с избыточностью по полосе оправдана скачкообразная перестройка частоты, повышающая стойкость к подавлению при умеренной деградации качества связи.

Таким образом, разработанная система критериев и показателей: обеспечивает методически корректную оценку эффективности технических средств защиты радиосистем за счет явного учета их влияния на качество радиосвязи; позволяет нормировать требования к средствам защиты через допустимые деградации показателей

качества функционирования; дает сопоставимую численную базу для выбора рационального варианта построения защиты при проектировании и модернизации радиосистем.

Ключевые слова: защита информации, радиосистемы, технические средства защиты, критерии и показатели эффективности, качество радиосвязи, оценка защищенности.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. ГОСТ Р ИСО/МЭК 15408-1-2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. – Москва : Стандартинформ, 2013.

2. Защита информации в системах мобильной связи : учеб. пособие для вузов / А. А. Чекалин [и др.] ; под ред. А. В. Заряева, С. В. Скрыля. – Москва : Горячая линия-Телеком, 2005. – 171 с.

3. Зюко, А. Г. Помехоустойчивость и эффективность систем передачи информации / А. Г. Зюко, А. И. Фалько, И. П. Панфилов [и др.]. – Москва : Радио и связь, 1985. – 272 с.

4. Вентцель, Е. С. Исследование операций: задачи, принципы, методология / Е. С. Вентцель. – Москва : КНОРУС, 2010. – 192 с.

5. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации. – Москва : Государственная техническая комиссия при Президенте РФ, 1992.

P.P.URBANOVICH[1], M.D.PŁONKOWSKI[2], D.V.SAZONOVA[3], N.M.GULEVICH[4]

SYNCHRONIZATION OF TWO TPM NEURAL NETWORKS ON THE USE OF A COMBINATION OF INTEGER AND HYPERCOMPLEX NUMBER ALGEBRAS

[1]*Belarusian State Technological University, Minsk, Belarus, Professor at the Department of Information Systems and Technologies, Doctor of Science in Engineering*

[2]*The John Paul II Catholic University of Lublin, Poland, Assistant Professor at the Department of Applied Computer Science, Candidate of Technical Sciences*

[3]*Belarusian State Technological University, Minsk, Belarus, Senior Lecturer at the Department of Information Systems and Technologies*

[4]*Belarusian State Technological University, Minsk, Belarus, student*

The development of distributed computing systems, the Internet of Things, edge devices, and software-defined information environments is increasing the demand for key agreement methods that feature low computational complexity and the ability to adapt to changing interaction conditions. One promising approach involves tree parity machines (TPM) – a specific class of neural networks capable of synchronizing internal weight parameters through the exchange of output signals over an open channel. The resulting synchronized state can be used to generate a shared data sequence, including in experimental neural-network-based key agreement schemes.

The idea of using two mutually learning neural networks TPM as an alternative to the Diffie-Hellman algorithm belongs to I. Kanter, W. Kinzel, Kanter E. [1]. Learning means that the synaptic weights (w_{ij}, $1 \le i \le K$, $1 \le j \le N$; K – number of neurons in the first layer of the network, N – number of inputs of each neuron; $w_{ij} \in \mathbb{Z}$; $w_{ij} \in \{-L, -L+1, \dots, L\}$;$K, N \in \mathbb{N}$) of the hidden neurons (the outputs of which for networks A and B we designate as $(\sigma_j = x_{ij}\, w_{ij})^A$ and $(\sigma_j = x_{ij}\, w_{ij})^B$, respectively) of both networks (A and B) are adapted according to certain rules for input (x_{ij}, $x_{ij} \in X^A$, X^B; $X^{A/B} \in \{-1, 1\}$) – output (τ^A, τ^B; $\tau^{A/B} \in \{-1, 1\}$) pairs according to certain rules. The training of the networks (TPM$^{A/B}$(K-N-L)) concludes when the weights become equal, and these weights can be used as a shared cryptographic key. The general structure of the TRM network is shown in fig. 1.

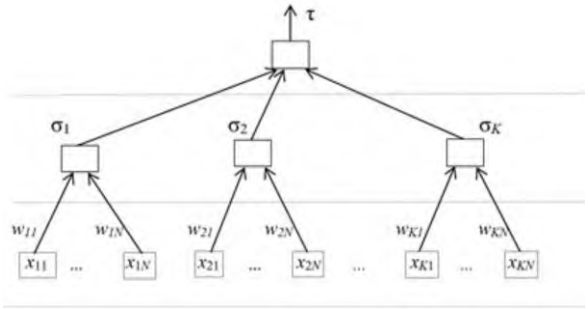


Fig.1 – The general structure of the TPM network

The development of the TPM architecture has been directed toward increasing the complexity of computational arithmetic to ensure a higher level of cryptographic resistance. To date, research results concerning the synchronization of TPM based on the extension of real numbers – specifically complex numbers (TPCM), quaternions (TPQM) and octonions (TPOM) – have been published in [2–6].

The work we present contains the results of a study of the synchronization process of the TPM based on the use of a combination of two different algebras relating to integers ($\mathbb{Z}$), complex numbers ($\mathbb{C}$), quaternions ($\mathbb{H}$), and octonions (O).

We assume that using a combination of different algebras – the most obvious combination being the real numbers as one algebra and one of the hypercomplex number systems as the other—in the training of an individual TPM interacting with another analogous TPM until they reach synchronization may, in certain cases or under certain learning rules, offer advantages over systems operating on the basis of a single algebra. The first potential advantage is an increase in the information capacity of a single logical weight: a complex-valued weight contains two real components, a quaternion-valued weight contains four, and an octonion-valued weight contains eight. With KK and NN remaining unchanged, the internal state space of the TPM increases even in purely formal terms. The second advantage is associated with mixing components based on different algebras. In theory, this may make it more difficult for a third, attacking network to reconstruct the state of the legitimately synchronizing networks on a component-by-component basis. The third advantage is the possibility of obtaining several groups of key material within a single synchronization process. The fourth advantage lies in expanding the space of possible learning rules, activation functions, norms, and projections. This creates additional opportunities for optimizing the trade-off between synchronization time and attack success rates.

Given the four levels of each network (the input, the weights, the hidden-neuron output, and the network output), as well as the known characteristics of the principal network learning rules (Hebbian, anti-Hebbian, and random-walk learning), a combination of integers and one of the hypercomplex numbers appears to be the most obvious and relatively simpler option.

If, for example, X^B, $X^{A/B} \in \mathbb{Z}$ and w_{ij}, σ_j, $\tau \in \mathbb{C}$, then for convenience we will denote the network architecture as $\mathbb{Z}$-$\mathbb{C}$-$\mathbb{C}$-$\mathbb{C}$. It follows from this that all intermediate calculations, weighting coefficients, as well as outputs from each of networks *A* and *B* are represented by complex numbers. We have conventionally called this architecture ICTPM (Integer-Complex TPM). The ICTPM network is a hybrid of the TPM and TPCM networks. The first-level elements are perceptrons with *N*-element weight vectors ($[w_{i1}, w_{i2}, ..., w_{iN}]$, where $1 \le i \ge K$), whose values are complex numbers ($w_{ij} = (a_1)_{ij} + \boldsymbol{i}(a_2)_{ij}$; $(a_1)_{ij}$ and $(a_2)_{ij} \in [-L, L]$). As in the case of the TPM architecture, the above elements are limited to the range $[-L, L]$x$[-L, L]$. The proposed approach ensures the compatibility of the model with classical weight updating rules, including the Hebbian rule and its modifications. To compare the parameters of the network synchronization process based on the proposed ICTPM architecture and TPM, TPCM architectures a software tool based on Python was developed. Using the developed application, experimental simulations of weight coefficient synchronization for networks with different *K*-*N*-*L* (1000 experiments for each architecture) were conducted. Formally, different channels connecting networks *A* and *B* were used: the trained networks were hosted on the same computer, and on different ones connected to the same LAN.

The $\mathbb{Z}$-$\mathbb{C}$-$\mathbb{C}$-$\mathbb{Z}$ architecture. If the output is determined solely by the real part of the field and the update affects only the real part of the weight, the imaginary part retains its initial value. With independent initialization of *A* and *B*, full synchronization is often not achieved under any of the three learning rules. For a meaningful comparison, it is necessary to introduce a predefined mechanism for updating both components of the complex number – such as alternating between the two projections. However, this approach does not yet ensure resilience against attacks.

The $\mathbb{C}$-$\mathbb{Z}$-$\mathbb{Z}$-$\mathbb{Z}$: complex-valued input, real-valued weights, and real-valued output. If the output and the update rule utilize only the real part of the input, the imaginary part does not affect the protocol. In this configuration, comparing the three rules effectively amounts to the same comparison as that for a standard TPM with real-valued inputs.

It is evident that, based on combinations of integers and complex numbers, other TPM architectures can also be considered.A crucial conclusion supporting the practical value of the proposed approach is the well-known asymmetry: the time required for the legitimate synchronization of *A* and *B* grows only polynomially with the weight depth *L*, whereas the number of networks an attacker needs for a successful genetic or majority attack grows exponentially with *L*. This remains the primary argument for continuing research in the direction analyzed.

REFERENCES

1. Kanter I., Kinzel W., Kanter E. Secure Exchange of information by synchronization of neural networks. Europhysics Letters, 2002, 57:141–147. https://doi.org/10.1209/epl/i2002-00552-9.

2. Płonkowski, M., Urbanowicz, P., Lisica, E. Wykorzystanie kwaternionów w protokole uzgadniania klucza kryptograficznego, opartym na architekturach sieci neuronowych TPQM. Przeglad Elektrotechniczny, 2010, 7(86):90-91.

3. Płonkowski M. Urbanowicz P. Liczby podwójne i ich modyfikacje w neurokryptografii. Przegląd Elektrotechniczny, 2012, 11b (88):340–341.

4. Dong T. and Huang T. Neural Cryptography Based on Complex-Valued Neural Network. IEEE Transactions on Neural Networks and Learning Systems, 2020, 11(31):4999–5004. https://doi.10.1109/TNNLS.2019.2955165.

5. Urbanovich P. P. Shutko N. P. Usage of hypercomplex numbers in a cryptographic key agreement protocol based on neural networks. Journal of the Belarusian State University. Mathematics and Informatics, 2024, 2:81–92. EDN: MIPTIK.

6. Urbanovich P. P., Płonkowski M. D., M. Dolecki. Neural network technologies in cryptographic applications [monograph]. - Minsk: BSTU, 2024. – 221 p. (In Russian). URL: https://elib.belstu.by/ handle/ 123456789/65182.