Отложенный перебор в задаче формирования общего секрета с помощью синхронизируемых искусственных нейронных сетей

В.Ф. Голиков, Ксеневич А.Ю.

В работах[1-3] предложен способ формирования общего криптографического ключа с помощью двух ИНС, соединенных открытым каналом связи и синхронизируемых общими случайными воздействиями.

Наименее доказанным в этом способе, на наш взгляд, является стойкость формируемого ключа к возможным атакам на него со стороны третьей стороны, «прослушивающей» канал связи, по которому синхронизируемые сети обмениваются информацией. Это объясняется отсутствием строгих математических моделей, адекватно описывающих процесс синхронизации, ввиду высокой сложности процесса изменения весовых коэффициентов сетей как дискретных временных рядов.

Анализ процессов, происходящих при этом, возникающие проблемы и возможные атаки третьей стороны проведены, например, в [4-7]. В этих работах рассматриваются атаки, организованные следующим образом.

Если обозначить сети абонентов, формирующих общий криптографический ключ, А и В, а третьего абонента, тайно пытающегося узнать этот ключ, - Е, то схема взаимодействия сетей абонентов представляется рис.1.

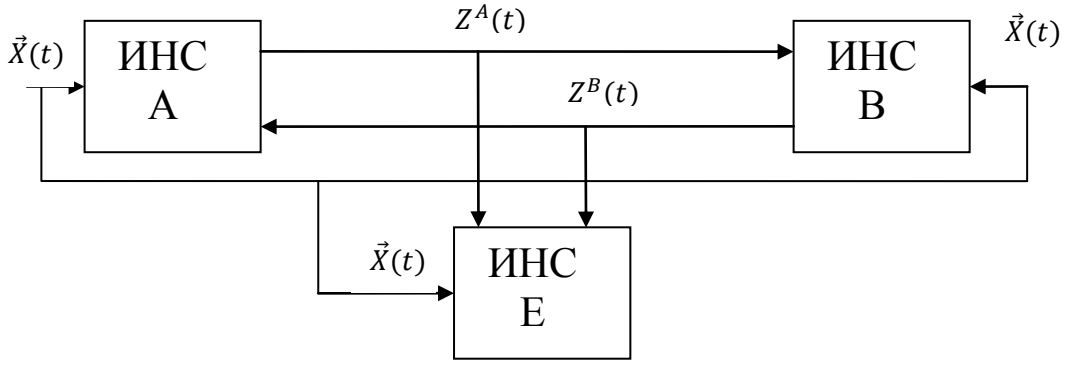


Рис.1.

где t – номер такта синхронизации, $\vec{X}(t)$ – вектор синхронизирующих случайных воздействий, $Z^A(t), Z^B(t)$ –выходные величины сетей А и В соответственно. Архитектура и параметры всех сетей идентичны (рис.2). На этом рисунке каждый персептрон имеет n входов, на каждый из которых поступает случайное число $x_{ij}\ (t) \in [-1,1]$ (одна из компонент $\vec{X}(t)$, $j = 1,2,\dots,n; i = 1,2,\dots,K$). Каждый персептрон описывается вектором весовых коэффициентов $\overrightarrow{W_i}(t)$ с компонентами $w_{ij}\ (t) \in [-L, L]$, где L – целое положительное число.

Выходные величины персептронов $Y_i(t) \in [-1,1]$перемножаются и образуют выходы сетей $Z(t) \in [-1,1]$.

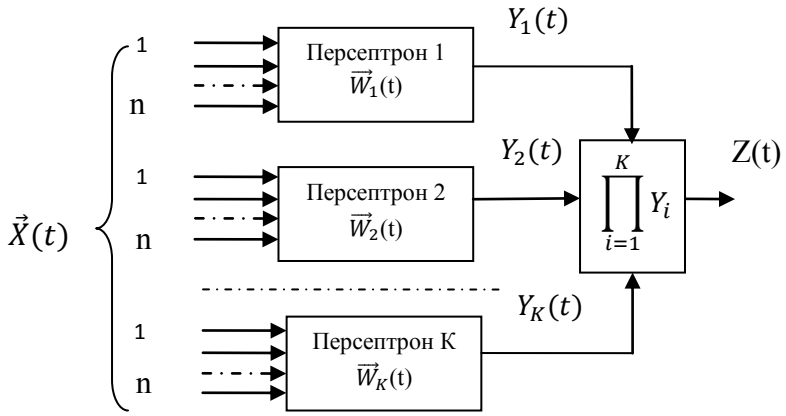


Рис.2

Начальные значения весовых коэффициентов персептронов сетей *A* и *B* $\vec{W}^A(0), \vec{W}^B(0)$ выбираются абонентами случайно, независимо друг от друга и сохраняются в секрете [6]. Подавая синхронно на входы своих сетей вектор $\vec{X}(t)$, абоненты *A* и *B* вычисляют выходные величины сетей $Z^A(t)$ и $Z^B(t)$, обмениваются ими и корректируют значения весовых коэффициентов персептронов своих сетей таки образом, что через некоторое число тактов t_{AB} наступает равенство

$$\vec{W}^A(t) = \vec{W}^B(t). \quad (1)$$

Атакующая сеть *E,* используя значения $\vec{X}(t)$, вычисляет $Z^E(t)$ и сравнивает его с перехваченными $Z^A(t)$ и $Z^B(t)$, корректирует значения весовых коэффициентов персептронов своей сети по определенному алгоритму и через некоторое число тактов t_{AE} добивается равенства

$$\vec{W}^E(t) = \vec{W}^A(t) = \vec{W}^B(t). \quad (2)$$

В зависимости от выбранного абонентом *E* алгоритма коррекции различают несколько видов атак. Наиболее эффективной считается «геометрическая атака» [4]. Исследования показали, что независимо от вида атаки обеспечивается

$$P(t_{AB} \le d) > P(t_{AE} \le d), \quad (3)$$

где d – назначенное сторонами *A* и *B* предельное число тактов, достаточное для наступления полного синхронизма их сетей. Выражение (3), однако, совсем не означает, что в процессе атаки обязательно произойдет событие $t_{AB} \le t_{AE} \le d$. Т.е. могут иметь место успешные атаки, при которых окажется $t_{AE} \le t_{AB}$, что приведет к выполнению (2). С наличием таких реализаций и связаны основные сомнения в безопасности анализируемого метода открытого формирования общего секрета. На рис.3 приведены зависимости $P(t_{AB} \le d)$, $P(t_{AE} \le d)$ от d при n=25, K=3, L=8, полученные методом имитационного моделирования

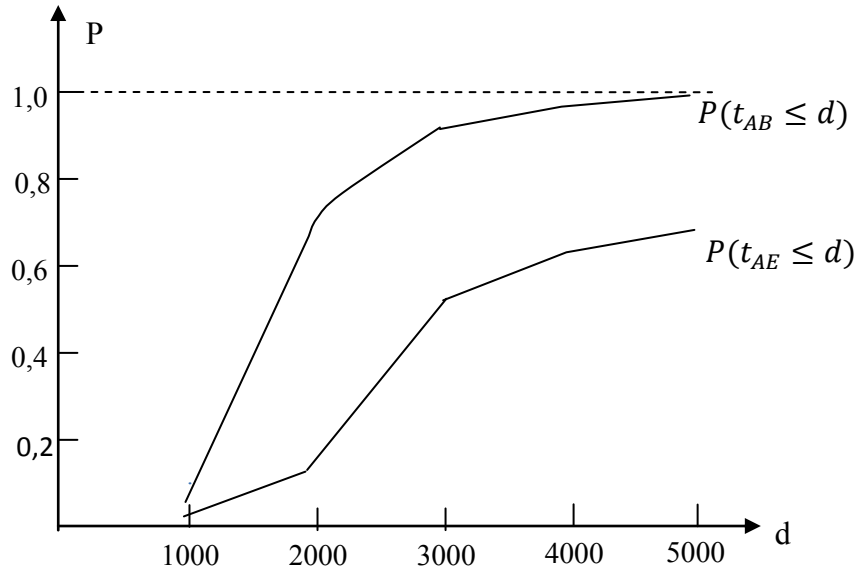


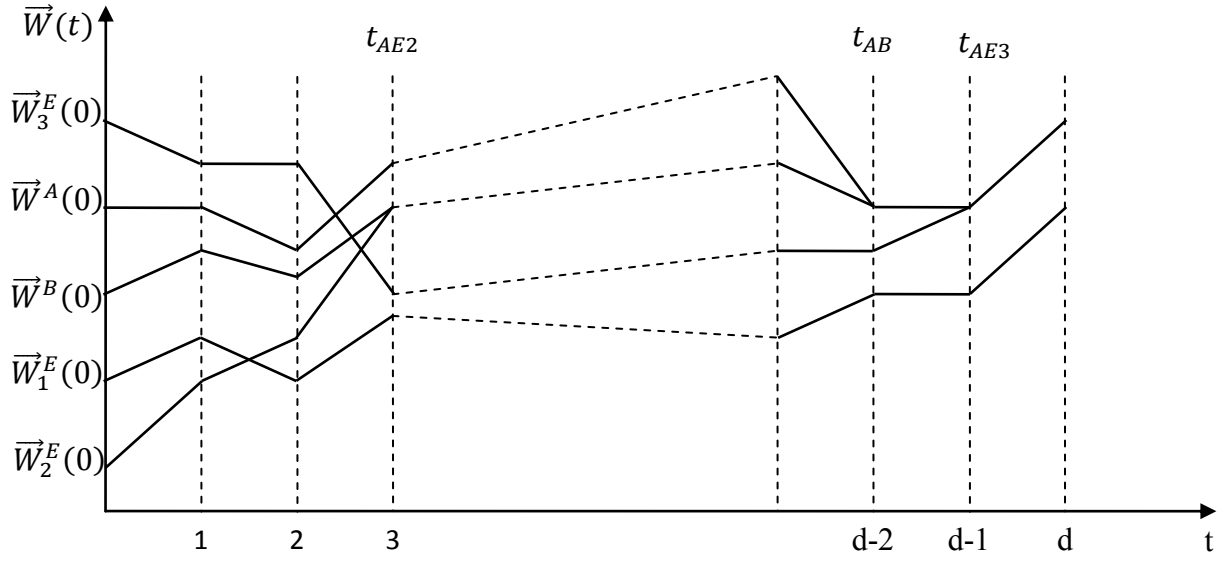
Рис.3

Из приведенных графиков видно, что для ИНС, с выбранными параметрами для достижения синхронизма с вероятностью более 0,95 следует выбрать *d*=3500. При этом $P(t_{AE} \le d) \approx 0{,}55$. Т.е. в половине реализаций атакующая сеть *E* успевает войти в синхронизм с сетью А за отведенное число тактов аналогично сети В. Однако в [4] показано, что вероятность успешной атаки можно снизить за счет увеличения параметров *n* и *L*. Например, при *n*=1000, *K*=3, *L*=57 удается обеспечить $P(t_{AE} \le d) \approx 10^{-4}$. Но при этом для того, чтобы обеспечить синхронизм защищаемых сетей необходимо обеспечить $d = 1{,}6 \cdot 10^5$. С практической точки зрения столь длительный процесс обмена данными делает анализируемый метод бесперспективным, тем более, что достигаемая малость вероятности успешной атаки отнюдь не является безопасной.

Проанализировав используемый процесс синхронизации сетей можно разработать атаку эффективную практически при любых параметрах сетей.

Как уже указывалось выше, в процессе синхронизации сетей за счет общих входных воздействий и специального алгоритма коррекции происходит постепенное сближение значений весовых коэффициентов персептронов сетей. Количество тактов синхронизации, за которое наступит равенство весов, зависит от их начальных значений и от последовательности $\vec{X}(t)$. Общепринято считать, что атака абонента *E* методом перебора начальных значений весовых коэффициентов персептронов своей сети обречена на неудачу, т.к. количество этих значений даже для сети с небольшими значениями *n, K, L* требует очень больших временных затрат. Можно показать [6], что количество возможных начальных значений вектора весовых коэффициентов персептронов сети не менее $M = (2L+1)^{nK}$. Поэтому, например, для формирования двоичного общего секретного числа размером 256 бит нужно выбрать *L*=4, *nK*=84 при этом получим $M = 9^{84} \approx 1{,}43 * 10^{80} \approx 2{,}145 * 2^{380}$. Т.е. абоненту *E* следует создать *M* ИНС и попытаться синхронизировать их с сетями *A* и *B*. При указанных выше количествах подобная задача не реализуема. Однако изучение процесса синхронизации сетей показало, что абоненту *E* совершенно необязательно угадать истинное значение $\vec{W}^A(0)$ или $\vec{W}^B(0)$, т.к. существует достаточно большое множество начальных значений вектора весовых коэффициентов $\vec{W}^E(0)$, движение из которых при благоприятных траекториях $\vec{X}(t)$ позволяет обеспечить $t_{AE} \le t_{AB} \le d$ (рис.4). На этом рисунке показаны условные траектории изменения векторов весовых коэффициентов сетей *A, B,* в процессе синхронизации. Сеть *E* представлена тремя траекториями. Траектории $\vec{W}^A(t)$ и $\vec{W}^B(t)$ совпали при $t = d-2$, траектории $\vec{W}^A(t)$ и $\vec{W}_1^E(t)$ не совпали за назначенное время синхронизации *d*, траектории $\vec{W}^A(t)$ и $\vec{W}_2^E(t)$, $\vec{W}_3^E(t)$ совпали, причем время достижения синхронизации второй сети *E* меньше, чем у сетей *A* и *B*.

Кроме того, абоненту *E* нет необходимости строить модель, состоящую из *M* ИНС, используя для этого огромные вычислительные ресурсы. Атаку на сформированное *A* и *B* общее число можно организовать, располагая одной или относительно небольшим числом ИНС, в «отложенном» по времени режиме. Для этого абонент *E,* прослушивая канал связи между *A* и *B,* запоминает значения $\vec{X}(t), Z^A(t), Z^B(t), d$. Затем случайным образом генерирует $\overrightarrow{W_1^E}(0)$, используя $\vec{X}(1)$, формирует $Z^E(1)$ и сравнивает его с $Z^A(1)$, проводит коррекцию $\overrightarrow{W_1^E}(0) \to \overrightarrow{W_1^E}(1)$ в соответствии с выбранным алгоритмом. Этот процесс продолжается такт за тактом.



Если к моменту назначенного конечного такта $t = d$ устанавливается факт наступления синхронизации по одному из принятых критериев [7], то принимается решение о совпадении $\overrightarrow{W_1^E}(d)$=$\overrightarrow{W_1^A}(d)$=$\overrightarrow{W_1^B}(d)$. В противном случае следует выбрать другое значение $\overrightarrow{W^E}(0)$ и вновь провести синхронизацию. Процесс повторяется до первой успеха.

Оценим необходимый объем отложенного моделирования. Обозначим вероятность успешной синхронизации абонента *E* в одной попытке P_{AE}^1. С учетом предыдущих обозначений $P_{AE}^1 = P(t_{AE} < d)$. Вероятность того, что в m попытках событие $t_{AE} < d$ произойдет не менее одного раза, равна

$$P_m(i \geq 1) = 1 - P_m(i = 0) = 1 - (1 - P_{AE}^1)^m. \quad (4)$$

Потребуем, чтобы эта вероятность была не менее заданной γ. Тогда

$$1 - (1 - P_{AE}^1)^m \geq \gamma. \quad (5)$$

Из (5) найдем

$$m = \frac{\ln(1-\gamma)}{\ln(1-P_{AE}^1)} \quad (6)$$

Используя (6), можно оценить объем отложенного моделированного, например, для выше рассмотренных данных, в которых $P_{AE}^1 = 10^{-4}$. Зададимся γ=0,98, получим

$$m = \frac{\ln(1-0{,}98)}{\ln(1-10^{-4})} \approx 3{,}9 \cdot 10^4.$$

Такое количество экспериментов легко реализуется за очень короткое время. Из (6) несложно вывести значение P_{AE}^1, при котором объем отложенного моделирования будет соизмерим с объемом перебора значений ключа длиной 256 битов симметричного алгоритма шифрования. Для этого упростим (6). Известно, что при $x \ll 1$ справедливо $\ln(1-x) \approx -x$, т.е. $\left(\ -P_{AE}\right) \approx -P_{AE}$. С учетом этого из (6) получим

$$P_{AE} = -\frac{(\ -\gamma)}{m}.$$

При $m =$ имеем $P_{AE} =$, $\cdot$ $^{-}$. Такое значение вероятности P_{AE} практически невозможно обеспечить подбором параметров ИНС.

Литература

1. Kanter, I. The Theory of Neural Networks and Cryptography, Quantum Computers and Computi g / I. Ka t er, W.Ki z e .−2005. Vo . 5, .1. – P. 130−140.

2. Kinzel, W. Neural Cryptography / W.Kinzel, / I. Kanter // 9th International Conference on Neural Information Processing, Singapore, 2002.

3. Kanter, I. Secure exchange of information by synchronization of neural networks/ I. Kanter, W. Kinzel, E.Kanter//arxiv: cond/0202112v1,[cond-mat.stat-mech], 2002.

4. Ruttor, A. Dynamics of neural cryptography / A. Ruttor, I. Kanter, and W. Kinzel // Phys. Rev. E, 75(5):056104, 2007

5. Голиков, В.Ф. Механизм синхронизации весовых коэффициентов в искусственных нейронных сетях Кинцеля и проблемы безопасности / Н.В. Брич, В.Ф. Голиков // Электроника ИНФО. – №6(96). – С.185-188.

6. Голиков В.Ф. Вероятностные свойства начальных значений весовых коэффициентов в синхронизируемых искусственных нейронных сетях Кинцеля / В.Ф. Голиков, Н.В. Брич // Системный анализ и прикладная информатика. – 2013. - №1-2. – С. 33-37.

7. Голиков В.Ф. О некоторых проблемах в задачах распределения криптографических ключей с помощью искусственных нейронных сетей / В.Ф. Голиков, Н.В. Брич, В.Л. Пивоваров// Системный анализ и прикладная информатика, №1-3, 2014. С.42-46.