В этой работе для повышения качества распознавания малочисленных атак в ходе обучения классификатора первого уровня использовались псевдоатаки, алгоритм генерирования которых рассмотрен в разделе 3. В результате использования записей о псевдоатаках удалось добиться незначительного повышения качества распознавания записей, относящихся к классам атак, с которыми традиционно возникают проблемы – U2R и R2L. На одной и той же тестовой выборке были опробованы два идентичных нейросетевых классификатора А и В, но при подготовке классификатора В в обучающую выборку были добавлены записи о псевдоатаках (см. таблицу 4).

Таблица 4. Результат обучения с использованием записей о псевдоатаках (А – без псевдоатак; В – с псевдоатаками)

	Классификатор A	Классификатор B
Записи класса U2R	73,08%	78,85%
Записи класса R2L	75,13%	98,67%

Заключение. В данной работе была предложена мультиагентная система обнаружения атак, позволившая в той или иной мере решить следующие задачи:

1. Выполнить двухуровневую классификацию сетевой активности: как по классам, так и по типам атак. Причем каждый последующий уровень иерархии нейросетевых детекторов используется для подтверждения или опровержения решения сгенерированного на вышестоящем уровне;
2. Сократить в мультиагентной системе количество задействованных в принятии окончательного решения детекторов, тем самым снизить нагрузку на требуемые для работы системы вычислительные ресурсы. Эта задача была решена посредством использования набора правил взаимодействия агентов, заданного направленным графом, в узлах которого представлены отдельные классификаторы;
3. Снизить количество ложных срабатываний, благодаря использованию мнений нескольких детекторов и продуманной стратегии обработки пакета в системе;
4. Расширить обучающую выборку образами о псевдоатаках, т.е. пополнить обучающую выборку образами, представленными в недостаточном количестве.

СПИСОК ЦИТИРОВАННЫХ ИСТОЧНИКОВ

1. Kaspersky Security Bulletin 2009. Основная статистика за 2009 год. [Электрон. ресурс]. – Режим доступа: http://www.securelist.com/ru/downloads/vlpdfs/ksb_09_malware2_ru.pdf.
2. Kumar, S. A software architecture to support misuse intrusion detection / S. Kumar and E. H. Spafford. // In Proceedings of the 18th National Conference on Information Security – 1995. – P. 194–204.
3. Ilgun, K.USTAT: A real-time intrusion detection system for Unix. Master's Thesis.University of California at Santa Barbara. – Santa Barbara, CA, 1992.
4. Lunt, T. Detecting intruders in computer systems // In Proceedings of the 1993 Conference on Auditing and Computer Technology, 1993.
5. Anderson, D. Next-generation intrusion detection expert system (NIDES): A summary / D. Anderson, T. Frivolt and A. Vakdes. – SRI-CSL-95-07 (May), 1995.
6. 1999 KDD Cup Competition. Information on: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.
7. Головко, В.А. Нейронные сети: обучение, организация и применение. Кн. 4: учеб. пособие для вузов / Общая ред. А.И. Галушкина. – М.: ИПРЖР, 2001. – 256 с.
8. Головко, В.А. Нейронная сеть как элемент системы обнаружения вторжений // X Всероссийская научно-техническая конференция "Нейроинформатика-2008": сборник научных трудов. В 2-х частях / В.А. Головко, Л.Ю. Войцехович – Москва: Московский инженерно-физический институт, 2008. – Ч. 2. – С. 86–93.
9. Golovko, V. Boosting Algorithms for Ensembles of Neural Network Classifiers in Intrusion Detection Domain / V. Golovko and L. Vaitsekhovich // In Proceedings of the International Conference on Neural Networks and Artificial Intelligence (ICNNAI-2008) – Minsk, 2008. – P. 70–74.
10. Vaitsekhovich, L. Multiagent Intrusion Detection Based on Neural Network Detectors and Artificial Immune System / L. Vaitsekhovich, V. Golovko, U. Rubanau // In Proceedings of the 10th International Conference on Pattern Recognition and Information Processing (PRIP-2009) – May 19-21, 2009. – Minsk, Belarus. – P. 285–289.

Материал поступил в редакцию 10.11.10

VAITSEKHOVICH L.U., GOLOVKO V.A., KUROSH MADANI Construction of system of detection of attacks with use the column of interaction of the agents

In this article a multiagent model of intrusion detection system have been addressed. Its structure and operation algorithm were described. In this model the multilayer architecture of agent hierarchy was applied. The algorithm of agent interaction can be described with a directed graph. The model is able to perform a classification of network intrusions by classes as well as by types. The experiments indicate that such model can decrease the level of false positives. The neural network agents were adapted with the application of pseudoattack samples.

УДК 004.75

СУ ЦЗЮНЬ, ЯЦКИВ В.В., САЧЕНКО А.А.

[illegible]
[illegible]

Введение. Беспроводные сенсорные сети (БСС) являются одним из современных перспективных направлений развития отказоустойчивых распределенных, самоконфигурируемых систем мониторинга и управления ресурсами и процессами [1, 2]. Вместе с тем использование БСС в ряде областей, в частности, в системах управления технологическими процессами, пожарно-охранных системах, системах безопасности, системах мониторинга реального времени выставляет повышенные требования к надежности их функционирования на всех уровнях модели OSI.

В общем, для повышения надежности передачи данных используют следующие подходы: передача данных на основе методов расширения спектра сигналов (DSSS, FHSS), корректирующие коды (циклическая проверка четности, Рида – Соломона, Боуза – Чеудхури – Хоквингхема и другие) [1]. Кроме того, в [3] разработан модифицированный метод, который базируется на расширении спектра сигнала скачкообразной перестройкой частоты и преобразования системы остаточных классов, которая дает возможность осуществлять помехоустойчивое кодирование и распараллеливание обработки информации

Су Цзюнь, *аспирант Тернопольского национального экономического университета.*

Яцкив Василий Васильевич*, доцент кафедры специализированных компьютерных систем Тернопольского национального экономического университета.*

Саченко Анатолий Алексеевич*, заведующий кафедрой информационно-вычислительных систем и управления Тернопольского национального экономического университета.*

без значительного осложнения вычислительных средств. Однако все перечисленные выше подходы повышают надёжность передачи данных только на физическом уровне беспроводных сетей.

Вместе с тем остается актуальной задача обеспечения надежности и безопасности передачи данных на сетевом уровне. Потеря пакетов на сетевом уровне БСС обусловлена перегрузкой узлов, выходом из строя или недоступностью узлов при изменении топологии сети. В свою очередь повторная передача пакета приводит к росту времени задержки доставки сообщения, увеличения трафика в сети и, как следствие, к увеличению энергетических затрат.

Одним из наиболее эффективных способов повышения надежности передачи данных на сетевом уровне БСС является использование многопутевой маршрутизации [1, 2]. В алгоритмах многопутевой маршрутизации для каждого адресата вычисляется несколько непересекающихся путей, что позволяет оптимально использовать каналы связи и повышать их общую пропускную способность. Кроме того, многопутевая маршрутизация обеспечивает простой механизм для увеличения вероятности надежной доставки данных за счет отправления нескольких копий данных за разными маршрутами. Однако использование протоколов многопутевой маршрутизации приводит к увеличению энергетических затрат и повышению трафика сети.

Более эффективным алгоритмом является разделение сообщения на части и передача частей разными маршрутами, при этом для защиты от ошибок к каждой части сообщения добавляется корректирующий код [4]. Недостатком данного алгоритма является невозможность возобновления сообщения при отсутствии хотя бы одной части. Кроме того, ограниченные вычислительные ресурсы беспроводного сенсора усложняют выбор эффективных корректирующих кодов.

В качестве алгоритма разделения пакета данных на части используют методы распределения секрета [1, 2]. В данных методах количество частей, которые необходимые для возобновления сообщения, могут отличаться от того, на сколько частей мы разделили сообщение. Такие алгоритмы называют еще пороговой схемой, где n – количество частей, на которые разделяется секрет, а t – количество частей, необходимых для возобновления секрета. В криптографии для распределения секрета используются схемы: Шамира, Блекли, Асмута – Блума и др. [5].

Однако следует заметить, что использование известных пороговых схем распределения секрета позволяет возобновить данные при наличии только t частей, то есть при потере $n-t$ частей сообщения, в то же время использование искаженной части сообщения может помешать возобновлению пакета данных. Поэтому авторами предложен метод разделения пакетов данных в беспроводных сенсорных сетях на основе преобразование системы остаточных классов, описанный ниже.

Метод многопутевой маршрутизации на основе преобразования системы остаточных классов. В предложенном методе разделения пакетов данных в БСС на n частей используется преобразование системы остаточных классов (СОК), причем, передавая полученные части (подпакеты) разными маршрутами, подпакеты образуются в результате получения остатка от деления пакета на взаимно простые модули p_i.

Кодирование на основе системы остаточных классов. Пусть заданная система с основами $\left(p_1, p_2, \dots, p_n\right)$ и диапазоном [6]

$$\wp = \prod_{i=1}^{n} p_i .$$

Известно, что любое число из диапазона $\left[0, \wp\right)$ можно представить в виде остатков по выбранным взаимно простым основаниям $M = \left(b_1, b_2, \dots, b_n\right)$.

Заданной системе оснований однозначно отвечает система ортогональных базисов

$$B_1, B_2, \dots, B_n ,$$

таких, что число M в позиционной системе исчисления можно представить как

$$M \equiv \sum_{i=1}^{n} b_i \cdot B_i (\mathrm{mod}\, \wp) . \quad (1)$$

Ортогональные базисы вычисляются по формуле:

$$B_i = m_i \cdot \frac{\wp}{p_i} \equiv 1 (\mathrm{mod}\, P_i) ,$$

где $1 \le m_i \le P_i - 1$ – вес ортогонального элемента.

Для уменьшения сложности обратного преобразования можно использовать совершенную форму СОК, при которой $m = 1$.

К преимуществам системы остаточных классов необходимо отнести:

- независимость образования разрядов, в результате чего каждый разряд несет информацию обо всем числе;
- малая разрядность остатков, которые представляют число.

В предложенном методе многопутевой маршрутизации на основе СОК для разделения пакета данных M на части (t, n) выберем взаимно простые числа $p_i < p_{i+1} 1$, произведение которых $\prod_{i=1}^{t} p_i > M$.

Пакет данных M разделяем на части по формуле:

$$b_i = M \bmod p_i .$$

В результате разделения формируется массив данных

$$\left\{\wp, p_i, b_i\right\} ,$$

который передаётся по непересекающимся маршрутам (рис. 1). Возобновление пакетов осуществляется по формуле (1).

Для реализации возможности возобновления сообщения по t частям из n рассмотрим систему с основаниями $p_1, p_2, \dots, p_i, \dots, p_t$ и диапазоном $P = p_1 \cdot p_2 \cdot \dots \cdot p_t$. Диапазон P будем называть рабочим диапазоном. Введем основы $p_{t+1}, p_{t+2}, \dots, p_n$, взаимно простые с любой из принятых ранее основ и будем представлять числа в системе с основами $p_1, \dots, p_n$. Это значит, что будем передавать и выполнять операции над числами, которые находятся в диапазоне $\left[0, P\right)$ в более широком диапазоне $\left[0, \wp\right)$, где $\wp = P \cdot p_{t+1} \cdot \dots \cdot p_n$.

Все числа, с которыми работает алгоритм кодирования, должны находиться в диапазоне $\left[0, P\right)$. Следовательно, если в результате передачи получено число, больше P, это значит, что была допущена ошибка.

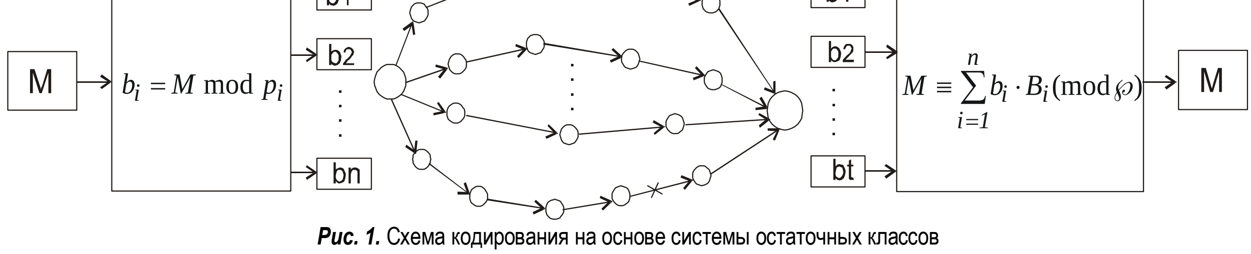

Рис. 1. Схема кодирования на основе системы остаточных классов

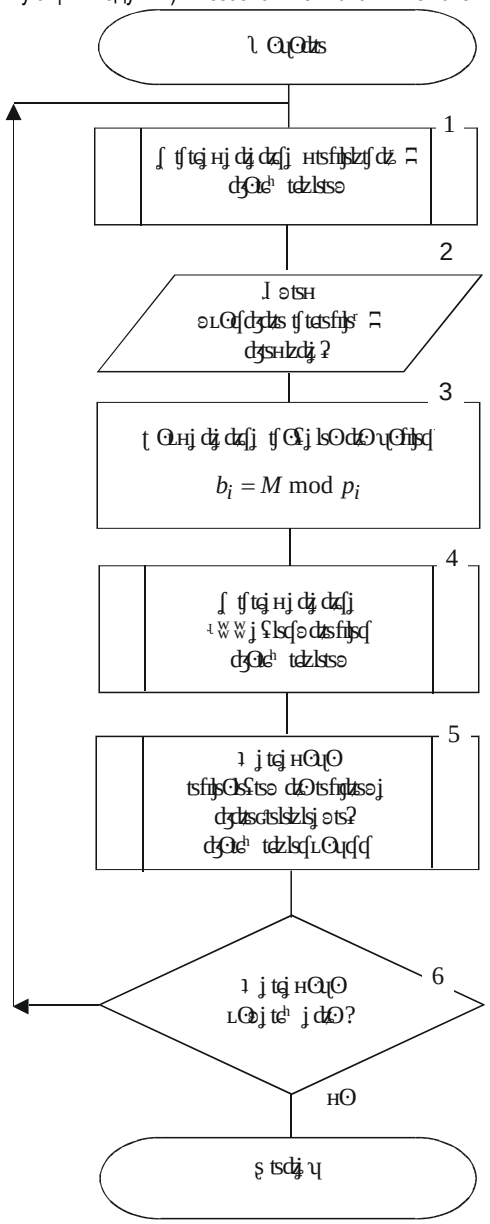

Рис. 2. Блок–схема алгоритма многопутевой маршрутизации на основе системы остаточных классов

Сравнительная оценка методов разделения сообщения на части. Для оценки качества методов маршрутизации используют следующие критерии [7]: 1) корректность – доставка пакета по назначению; 2) эффективность – отправка пакетов по «наилучшим» путям; 3) сложность – экономно расходовать время и память; 4) устойчивость – работа сети при изменении топологии; 5) адаптивность – распределение нагрузки каналов сети; 6) справедливость – равноправное обслуживание всех станций сети.

Кроме перечисленных критериев оценки качества, важным также является, (для БСС с автономным питанием), оценка избыточности сообщений при многопутевой маршрутизации.

Сравним избыточность кодирования данных при разделении сообщения на части с использованием существующих пороговых схем разделения секрета (Шамира, Асмута-Блума) и предложенного алгоритма. Для этого вычислим объем сообщения при заданных значениях: количество частей (маршрутов), размер пакета данных 24 бита.

Пороговая схема разделения секрета Шамира. Чтобы разделить пакет данных M, в схеме Шамира выбирается простое число P, $P > M$, которое задает размер конечного поля [5]. Над этим полем строится многочлен размерности $t-1$:

$$F(x) = \left(a_t \cdot x^t + a_{t-1} \cdot x^{t-1} + ... + a_1 \cdot x + M\right) \bmod P .$$

Коэффициенты многочлена $a_t, a_{t-1} ... a_1$ выбираются случайно. После этого вычисляются координаты n точек:

$$t_i = F(i) = \left(a_t \cdot i^t + a_{t-1} \cdot i^{t-1} + ... + a_1 \cdot i + M\right) \bmod P .$$

В результате формируются поток данных

$$\{P, t-1, t_i, j\},$$

где t_i – коэффициенты, которые вычисляются; j – номера коэффициентов; $t-1$ – размер многочлена; P – модуль.

Объем одной части сообщения

$$v_1 = \lceil \log_2 P \rceil + \lceil \log_2 (t-1) \rceil + \lceil \log_2 t_i \rceil + \lceil \log_2 j \rceil \text{ (бит)}.$$

Следовательно, для каждого из десяти маршрутов передачи формируется пакет данных размером v_1 бит.

Пороговая схема разделения секрета Асмута-Блума. Пороговая схема разделения секрета Асмута-Блума построена с использованием простых чисел [5]. Выбираем простое число P из условия $P > M$ и n взаимно простых чисел p_1, p_2, ..., p_n таких, что $p_i > P$; $p_i < p_{i+1}$, то есть

$$p_1 \cdot p_2 \cdot ... \cdot p_t > P \cdot p_{n-t+2} \cdot p_{n-t+3} ... p_n .$$

Вычисляем $M' = M + r \cdot P$,

где r – случайное число, и находим части сообщения

$$b_i = M' \bmod p_i .$$

В результате формируется массив данных $\{P, p_i, b_i\}$, а объем одной части сообщения

$$v_2 = \lceil \log_2 P \rceil + \lceil \log_2 p_i \rceil + \lceil \log_2 b_i \rceil \text{ (бит)}.$$

Схема кодирования на основе СОК. При использовании преобразования СОК объем одной части сообщения

$$v_3 = \lceil \log_2 \wp \rceil + \lceil \log_2 p_i \rceil + \lceil \log_2 b_i \rceil .$$

Для вычисления объема данных, который формируется в результате разделения пакета на части (при заданных значениях), выбираем взаимно простые модули $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$, $p_6 = 17$, $p_7 = 19$, $p_8 = 23$, $p_9 = 29$, $p_{10} = 31$.

Так как разрядность остатков изменяется в зависимости от величины модулей p_i, то целесообразно определить минимальный и максимальный объем сообщения:

$$v_{3\min} =]\log_2 \wp[+]\log_2 p_{i\min}[+]\log_2 b_{i\ \min}[\text{ (бит)};$$

$$v_{3\max} =]\log_2 \wp[+]\log_2 p_{i\ \max}[+]\log_2 b_{i\ \max}[\text{ (бит)}.$$

Из приведенных аналитических выражений и рис. 3 видно, что предложенный метод разделения сообщения на части обеспечивает в 1,5 раза меньшую избыточность при аналогичных параметрах возобновления данных.

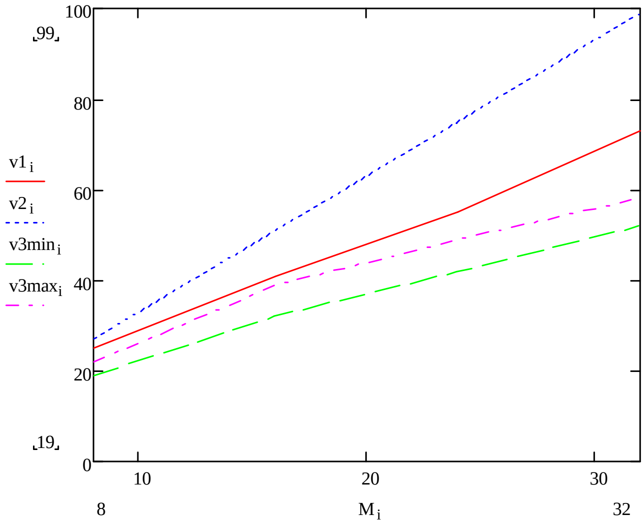

Рис. 3. Зависимость объема данных v от разрядности пакета данных M для разных пороговых схем разделения: $v1$ – схема Шамира; $v2$ – схема Асмута-Блума; $v3$ – разделение на основе системы остаточных классов

Экспериментально установлено, что уменьшить объемы данных при использовании пороговых схем для разделения сообщения на части можно следующим образом: передавая лишь пакеты с переменными коэффициентами, при этом постоянные составляющие, необходимые для возобновления данных, передаются отдельным пакетом (рис. 4).

Заключение. Предложен метод разделения сообщения на основе системы остаточных классов, которая характеризуется меньшей избыточностью в сравнении с пороговыми схемами разделения секрета:

- в 1,5 раза – при передаче служебных данных с каждой частью пакета;
- в 5 раз – при передаче служебных данных отдельным пакетом.

Еще одним преимуществом предложенного метода является то, что в результате разделения сообщения на части формируются подпакеты (остатки) разной разрядности – это дает возможность распределять их в зависимости от интегральной оценки качества маршрута.

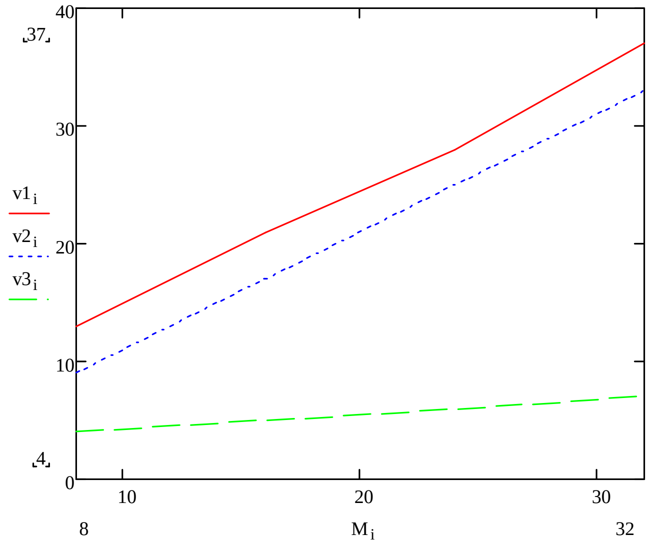

Рис. 4. Зависимость объема данных v от разрядности пакета данных M без учета постоянных составляющих: $v1$ – схема Шамира; $v2$ – схема Асмута-Блума; $v3$ – разделение на основе системы остаточных классов

СПИСОК ЦИТИРОВАННЫХ ИСТОЧНИКОВ

1. Lou, W. An efficient N-to-1 mutlipath routing protocol in wireless sensor networks: Proceedings of IEEE international Conference on Mobile Ad-hoc and Sensor Systems (MASS). – Washington, DC, November 2005.
2. Жуков, И.А. Способы повышения надежности и безопасности сбора информации в системах управления реального времени / И.А. Жуков, В.И. Дрововозов // Проблемы информатизации и управления.– 2008. – №1(23). – С. 262–276.
3. Sachenko, A. Modified Method of Noise-Immune Data Transmission in Wireless Sensors Networks / A. Sachenko, V. Yatskiv, R. Krepych // International Conference on Networks Security, Wireless Communications and Trusted Computing, “NSWCTC 2009”, 25–26 April 2009. – Wuhan, Hubei, China. – Volume 2. – P. 847–850.
4. Lou, W. SPREAD: Enhancing data confidentiality in mobile ad hoc networks, IEEE INFOCOM 2004 / W. Lou, W. Liu, Y. Fang. – HongKong, China, March 2004.
5. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2002. – 816 с.
6. Червяков, Н.И. Модулярные параллельные вычислительные структуры нейро-процессорных систем / Под. ред. Н.И. Червякова [и др.] – М.: ФИЗМАТЛИТ, 2003. – 288 с.
7. Телль, Ж. Введение в распределенные алгоритмы / Пер. с англ. В.А. Захарова. – М.: МЦНМО, 2009. – 616 с.

[illegible] 29.11.10

SU CZUN, YACKIV V.V., SACHENKO A.O. Increase of efficiency of transfer given in wireless touch networks on the basis of multitravelling routing

The method of data coding and transmission is proposed in the wireless networks on the basis of multipath routing and Residue Number System transformation, which is allowed to reduce the redundancy of data burst sharing and improved the reliability of data transmission.

[illegible] 004.056.57:032.26

[illegible]

[illegible]

Введение. В настоящее время проблема борьбы с компьютерной преступностью стала одной из первостепенных. Число компьютерных преступлений увеличивается ежегодно на 30–40 процентов [1]. Развитие глобальной сети Интернет способствует развитию ком-

***Безобразов Сергей Валерьевич**, к.т.н., доцент кафедры интеллектуальных информационных технологий Брестского государственного технического университета.*
Беларусь, БрГТУ, 224017, г. Брест, ул. Московская, 267.