УДК 004.056: 004.73 DOI 10.23683/2311-3103-2017-5-16-25

А.С. Басан, Е.С. Басан, О.Б. Макаревич

МЕТОД ПРОТИВОДЕЙСВИТЯ АКТИВНЫМ АТАКАМ ЗЛОУМЫШЛЕННИКА В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ*

Целью исследования является разработка метода, который позволит эффективно обнаруживать активные атаки злоумышленника на основе анализа сетевого трафика и физических параметров узлов беспроводной сенсорной сети (БСС). Проведен анализ физических показателей узла, на которые может быть направлена атака злоумышленника. Разработан метод выявления злоумышленного узла при нарушении физических показателей узла сети. Разрабатываемый метод основан на использовании вероятностных функций, вычислении доверительного интервала и вероятности отклонения текущих показателей от доверительного интервала. Новизна метода состоит в том, что при выявлении злоумышленного узла функция распределения текущего узла не сравнивается с эталонным распределением, а оценивается попадание текущего значения функции в доверительный интервал. Кроме того, новизна метода заключается в анализе физических параметров узлов сети для обнаружения злоумышленника, тогда как существующие системы обнаружения атак (СОА) основаны на методах анализа только сетевого трафика. Преимущество состоит в том, что в мобильных БСС существует большая вероятность не только сетевых атак, но и атак, направленных на нарушение физической активности узла (нарушение передвижения узлов, исчерпание энергетических ресурсов, зашумления канала передачи). Проведено моделирование мобильной беспроводной сенсорной сети. Проведен ряд атак на мобильную БСС. Оценена эффективность обнаружения атак с использованием разработанного метода. Анализ параметров остаточная энергия и загруженность узла удалось расширить спектр атак, которым способна противодействовать сеть, по сравнению с аналогами системы. К данным атакам относятся атаки «Отказ в обслуживании», «атака Сибиллы», «атаки на истощение ресурсов».

Атака; обнаружение атак; безопасность; беспроводные сенсорные сети; доверие; вероятностные методы.

A.S. Basan, E.S. Basan, O.B. Makarevich

THE METHOD OF RESISTANCE TO ACTIVE ATTACKS IN WIRELESS SENSOR NETWORKS

The purpose of the research is to develop methods and systems which can effectively detect active attacks of intruders based on the analysis of wireless and network parameters of wireless sensor networks (WSN). Analysed are the physical indicators which can be attacked by an intruder. Developed is the method for detecting a malicious node with physical characteristics of the network. The developed method is based on the use of probability functions, the calculation of the confidence interval and the probability of deviation of current indicators from the confidence interval. The novelty of the method is that when a malicious action is detected, the distribution of the current state is not compared with the reference distribution, and its influence in the confidence interval is also estimated. In addition, the novelty of the method is that it contains analytical tools for detecting an intruder, as well as methods for detecting attacks (IDS), based on methods of analyzing only network traffic. The advantage is that in mobile WSN there is a high probability of not only network attacks, but also attacks aimed at violation of physical activity (violation of movement of nodes, exhaustion of energy resources, and transmission of packages). A mobile wireless sensor network has been simulated. A series of attacks on mobile WSN are given. The effectiveness of using the developed method, compared to analogues, is evaluated. Having analysed the parameters of residual energy and congestion of the node we succeeded in expanding the range of attacks the network is able to counter in comparison with the analogs of the system. These attacks include "denial of service" attacks, "Sibyll attack", "resource depletion attacks".

Attack, attack detection; security, wireless sensor networks; trust; probabilistic methods.

* Работа поддержана грантом РФФИ №17–07–00106_А «Разработка метода и эффективной системы защиты беспроводных сенсорных сетей от активных атак злоумышленников».

Введение. Беспроводные сенсорные сети получили наибольшую популярность при использовании в качестве средства мониторинга и управления объектами. При этом узлы сети могут располагаться вне контролируемой зоны и подвергаться воздействию со стороны злоумышленника. Кроме того, беспроводные сенсорные сети (БСС) имеют большое количество уязвимостей, связанных с передачей данных по незащищенным беспроводным каналам. В связи с этим актуальной является задача разработки метода, который позволит эффективно обнаруживать активные атаки злоумышленника на основе анализа сетевого трафика и физических параметров узлов беспроводной сенсорной сети (БСС). Для обеспечения защиты БСС от активных атак злоумышленника существует две группы методов: системы обнаружения атак и вторжений и системы вычисления доверия [1]. В качестве способа защиты от активных атак злоумышленника в данной статье рассматривается метод вычисления доверия. Методы вычисления доверия позволяют не только обнаружить аномальное поведение и атаку в сети, но и поддерживать доверенные отношения между узлами, что позволяет предотвращать некоторые типы атак [2]. На сегодняшний день существует два типа систем вычисления доверия: распределенные и централизованные [3]. На основе анализа атак [4] были выявлены наиболее вредоносные атаки такие как: «Отказ в обслуживании (DOS)» [5], «Блокировка узла», «Блокировка узла с наличием условий» [6], «Туннелирование» [7], «Атака Сибиллы» [8]. Распределенные и централизованные системы вычисления доверия имеют свои достоинства и недостатки [9], но общим для них недостатком является неспособность противодействовать атакам «Отказ в обслуживании» и «Атака Сибиллы». Каждый тип методов может использовать различный математический аппарат для вычисления доверия. Вероятностные методы хорошо сочетаются с концепцией доверия, если определить доверие, как ожидание того, что узел сети ведет себя надлежащим образом по отношению к другим узлам, и выполняет свои обязательства при передаче данных, а также не нарушает работу других узлов и сети в целом [10].

Постановка задачи. Таким образом, основной задачей исследования является разработка метода вычисления доверия, который бы устранил недостатки распределенных и централизованных схем вычисления доверия и позволил бы расширить спектр атак, которым способна противодействовать система вычисления доверия, а именно атакам «Отказ в обслуживании» и «Атака Сибиллы».

Разработка метода вычисления доверия для противодействия активным атакам. Для осуществления многих активных атак, злоумышленнику требуются значительные энергетические ресурсы [11]. Для осуществления данных атак злоумышленнику необходимо отправлять большое количество пакетов, таким образом, узел должен расходовать большое количество энергии. Сравнив уровень остаточной энергии *Q(E)* и загруженность узла *L* (общее количество пакетов в заданный промежуток времени) можно увидеть пропорциональную закономерность [12]. Для вычисления значения доверия узла учитываются параметры загруженность *L* и остаточная энергия *Q(E). Загруженность* – это общее количество пакетов проходящих через узел [13]. *Остаточная энергия* – это уровень энергии, имеющийся у заданного узла в заданный промежуток времени [14].Чтобы узел считался доверенным, уровень его остаточной энергии не должен превышать максимально заданный уровень энергии в сети E_{max} и не был значительно ниже, чем у соседних узлов. При этом уровень загруженности узла не должен значительно превышать уровень загруженности соседних узлов и не должен быть ниже минимально необходимого уровня загруженности (т.е. минимальное количество пакетов, которые должен иметь узел за активный сеанс связи). Используем нормальный закон распределения для показателей загруженности *L* и остаточной энергии *Q(E)* для вычисления доверительных интервалов и вероятности попадания текущего значения в доверительный интервал.

$$L_i(t) \sim N(\overline{L}, \sigma_L^2),\ Q(E)_i(t) \sim N(\overline{Q(E)}, \sigma_{Q(E)}^2), \quad (1)$$

где $\sigma_{Q(E)}, \sigma_L$ – общее для группы узлов кластера; $\overline{L}$, $\overline{Q(E)}$ – математическое ожидание для загруженности и остаточной энергии узла.

Использование нормального закона распределения обусловлено тем, что он широко применяется в сетях массового обслуживания для представления распределения количества требований на интервале в среднюю длительность обслуживания, что схоже с распределением загруженности и остаточной энергии узла. А также был проведен анализ квантильных диаграмм для подтверждения данного факта. Для нахождения доверительного интервала необходимо сначала вычислить генеральную среднюю $\overline{Q(E)}$, $\overline{L}$ для значений остаточная энергия $Q(E)_i$ и загруженность L_i для группы узлов, входящих в кластер для каждого временного интервала:

$$\overline{Q(E)} = \sum Q(E)_i / n,\ \overline{L} = \sum L_i / n. \quad (2)$$

Далее необходимо вычислить дисперсию D и среднеквадратическое отклонение σ:

$$D_{Q(E)} = \left(\sum_i^N (Q(E)_i - \overline{Q(E)})^2 \right) / n,\ D_L = \left(\sum_i^N (L_i - \overline{L})^2 \right) / n, \quad (3)$$

где n – это объем выборки; $D_{Q(E)}$ дисперсия для остаточной энергии; D_L дисперсия для загруженности.

$$\sigma_{Q(E)} = \sqrt{D}_{Q(E)},\ \sigma_L = \sqrt{D}_L. \quad (4)$$

При определении доверия, важно, чтобы текущие значения узла не выходили за пределы доверительного интервала, то есть загруженность узла, и остаточная энергия не превышали допустимые значения. Узел вычисляет нижнюю b_{min} и верхнюю b_{max} границу доверенного для загруженности узла и остаточной энергии a_{min}, a_{max} по формулам:

$$a_{\min} = \overline{Q(E)} - t \cdot \sigma_{Q(E)} / \sqrt{n},\ a_{\max} = \overline{Q(E)} - t \cdot \sigma_{Q(E)} / \sqrt{n} \quad (5)$$

$$b_{\min} = \overline{L} + t \cdot \sigma_L / \sqrt{n},\ b_{max} = \overline{L} + t \cdot \sigma_L / \sqrt{n}, \quad (6)$$

$t * \sigma / \sqrt{n}$ – точность оценки; t – аргумент функции Лапласа; $\Phi(t) = \frac{\alpha}{2}$ – функция Лапласа; α – заданная надежность.

Для остаточной энергии верхняя граница интервала всегда равна E_{max}, так как узлы могут мигрировать из кластера в кластер и могут появляться новые узлы с максимальным значением остаточной энергии, чтобы избежать ошибки первого рода необходимо учитывать данный фактор. Вычисление нижней границы доверительного интервала производится только для значения остаточной энергии. Так как нижняя граница для загруженности узла выявляется согласно минимально необходимому количеству пакетов прошедших через узел за сеанс связи. Далее происходит вычисление вероятности попадания в доверительный интервал текущих значений загруженности и остаточной энергии узла, согласно формулам:

$$P_{Q(E)}(a_{\min} < Q(E)_i < a_{\max}) = \Phi\left(\frac{a_{\max} - \overline{Q(E)_в}}{\sigma_{Q(E)в}} \right) - \Phi\left(\frac{a_{\min} - \overline{Q(E)_в}}{\sigma_{Q(E)в}} \right), \quad (7)$$

$$P_L(b_{\min} < L_i < b_{\max}) = \Phi\left(\frac{b_{\max} - \overline{L_в}}{\sigma_{L_в}} \right) - \Phi\left(\frac{b_{\min} - \overline{L_в}}{\sigma_{Lв}} \right), \quad (8)$$

где Φ – функция Лапласа; $P_{Q(E)}$, P_L – вероятности попадания остаточной энергии узла и уровня загруженности узла в пределах доверительного интервала.

Для того чтобы вычислить значение среднеквадратического отклонения и математического ожидания необходимо сократить интервал для которого вычисляется значение и учитывать только предыдущее L_{i-1}, $Q(E)_{i-1}$ и текущие L_i, $Q(E)_i$ значения узла. Если брать значения по всему временному интервалу, то среднеквадратическое отклонение слишком увеличивается, за счет большой разницы между начальными и конечными значениями. Кроме того математическое ожидание не будет давать точное значение. Если брать значение соседних интервалов, то это позволит оценить попадание текущего значения в доверительный интервал без потери точности вычисления. Для получения значения доверия необходимо использовать комбинацию значений $P_{Q(E)}$, P_L прямого значения доверия T_{cent} в работе [15] представлен алгоритм комбинирования значений доверия с помощью теоремы Байеса. В результате формула для вычисления значения доверия примет вид:

$$T_{cent} = P_{Q(E)} * P_L \quad (9)$$

Моделирование беспроводной сенсорной сети для проведения экспериментального исследования. Для проведения экспериментального исследования и оценки эффективности системы управления защитой разработана модель кластерной БСС. Для реализации концептуальной модели БСС выбрана система моделирования NS–2 (версия 35). NS–2 является объектно-ориентированным программным обеспечением, ядро которого реализовано на языке C++ [16]. В табл. 1 представлены параметры моделируемой сети. NS–2 реализует стандарт IEEE 802.15.4, который является базовой основой для протоколов ZigBee, WirelessHART, MiWi, ISA100.11 [17].

Анализ экспериментальных данных. Анализ экспериментальных данных был проведён с помощью программы анализа данных и оценки доверия в БС, разработанной с использованием языка Perl [18]. Разработанный программный модуль полностью повторяет архитектуру системы вычисления доверия и использует разработанную методику для вычисления уровня доверия.

Таблица 1

Параметры моделируемой сети

Количество узлов в сети, N	25
Время моделирования, с	400
Интервал вычисления значения доверия, с	10
Начальный уровень энергии, Дж	30
Мощность передачи, мВт	0,4
Размер передаваемых пакетов, байт	512
Интервал передачи пакетов доверенным узлом,	0,8–1.5
Интервал передачи пакета злоумышленником, с	0,1 – 0,5
Протокол маршрутизации	AODV
Тип трафика	CBR
Протокол передачи данных	UDP

Данный программный модуль является кросс–платформенной программой, которая может быть установлена на различные операционные системы, в том числе и те, которые используют сенсорные узлы. Основной задачей данного программного

модуля является выявление злоумышленных узлов и оповещение доверенных узлов о наличие злоумышленника с целью его блокирования. Программный модуль выполняет следующие функции: разделение пакетов на группы согласно методике; вычисление значения доверия; определение является ли узел доверенным/ не доверенным/ неопределенным. В процессе моделирования сети формируется файл трассировки, который содержит в себе информацию обо всех узлах, пакетах сети, а также информацию о местоположении и остаточной энергии узлов. На основании этих данных программный модуль проводит анализ и выявляет злоумышленные узлы.

Оценка эффективности разработанного метода противодействовать активным атакам. Оценка эффективности проводилось на основании наличия ошибок 1 и 2 рода при обнаружении злоумышленника. Ошибка первого рода – это ложное срабатывание, возникающее в результате блокировки доверенного узла. Данное значение вычисляется согласно следующему выражению:

$$P_{1error} = \frac{n_{error1}}{N_{all}},$$

где n_{error1} – количество временных интервалов для всех доверенных узлов сети, на которых уровень доверия не превышал значение 0,5; N_{all} – общее количество временных интервалов для всех доверенных узлов сети.

Ошибка второго рода – это ложное срабатывание, возникающее в результате не определения злоумышленного узла. Вероятность возникновения ошибок второго рода вычисляется следующим образом:

$$P_{2error} = \frac{n_{error2}}{N_{all2}},$$

где n_{error2} – количество временных интервалов для всех злоумышленных узлов сети, на которых уровень доверия превышает значение 0,5; N_{all2} – общее количество временных интервалов для всех доверенных узлов сети.

Оценка эффективности противодействия атаке «Отказ в обслуживании». Атака «Отказ в обслуживании» направлена на свойство доступности узлов в сети [19]. В данной атаке узел злоумышленника посылает пакеты в сеть с большей интенсивностью, чем доверенные узлы, при этом интенсивность отправки пакетов злоумышленником составляет 24 пакета/сек, а доверенным узлом 0,9 пакетов/сек. При этом основной целью проведения данного ряда экспериментов является оценка уровня ложных срабатываний при наличии большого количества злоумышленных узлов. Ложное срабатывание может возникнуть по причине того, что большое количество злоумышленных узлов имеют высокую загруженность и при этом границы доверительного интервала смещаются так, что доверенный узел в них не попадает. Кроме того, при проведении атаки загруженность доверенного узла также повышается, что может привести к ошибкам 1 рода. Первый ряд экспериментов проводился для случая, когда уровень начальной энергии E_{max} для злоумышленных узлов и для доверенных узлов был одинаковым. При этом один узел злоумышленника целенаправленно атаковал один доверенный узел. В первой строке табл. 2, показана вероятность возникновения ошибки первого рода. Возникновение ошибок первого рода обусловлено тем, что уровень загруженности доверенных узлов повышается в связи с увеличением принимаемых пакетов. Далее уровень ложных срабатываний снижается, так как уровень загруженности злоумышленников значительно повышается.

Таблица 2

Вероятность ошибки 1 рода (P1error) атака «DOS»

Превышение начальной энергии узлами злоумышленника	Количество узлов злоумышленника, %								
	5	10	20	25	30	35	40	45	50
Emax	0,09	0,07	0	0	0	0	0	0	0
1,5 Emax	0,03	0,02	0,05	0,02	0,02	0,02	0,02	0,05	0,1
2Emax	0,04	0,02	0,04	0	0	0,02	0	0	0

Возникновение ошибок второго рода обусловлено тем, что при увеличении числа злоумышленников до 50 % значительно повышается предел верхней границы доверительного интервала, что приводит к снижению уровня обнаружения злоумышленников. В табл. 3 представлена вероятность возникновении ошибок второго рода при изменении двух параметров: уровень начальной энергии и количество узлов злоумышленника. Обнаружение злоумышленника происходит во всех случаях проведения эксперимента. Эффективность обнаружения снижается, когда количество злоумышленных узлов подходит к порогу 50 %.

Наибольшая эффективность обнаружения наблюдается, когда превышение уровня начальной энергии находится в промежутке $E_{max} < E_i < 2E_{max}$.

Оценка эффективности противодействия «атаке Сибиллы». При проведении «атаки Сибиллы» злоумышленник представляется несколькими сущностями в системе.

Таблица 3

Вероятность ошибки 2 рода (P2error) атака «DOS»

Превышение начальной энергии узлами злоумышленника	Количество узлов злоумышленника, %									
	5	10	15	20	25	30	35	40	45	50
E_{max}	0	0	0,02	0,05	0,09	0,15	0,2	0,3	0,3	0,43
1,5 E_{max}	0	0	0	0	0	0,1	0,19	0,2	0,2	0,38
$2E_{max}$	0	0	0	0,02	0,06	0,15	0,17	0,19	0,2	0,43

В данном случае злоумышленник представляется узлами и пытается захватить наибольшее влияние сетью. Основной целью проведения эксперимента является оценка возможности обнаружения «атаки Сибиллы» при заданных условиях и эффективности обнаружения данной атаки при изменении параметров проведения атаки. В табл. 4 и 5 представлена оценка вероятности возникновения ошибки первого и второго рода в зависимости от изменения показателей количества узлов злоумышленника и количество узлов подверженных атаке. В случае если в сети имеется 1 злоумышленный узел, наибольшая эффективность обнаружения злоумышленника наблюдается, когда количество жертв составляет 15 %. То есть злоумышленник оказывает влияние на небольшую часть сети. Далее злоумышленный узел пытается взять под влияние другие узлы. При этом эффективность падает, так как узлы находятся в недоступной близости от злоумышленника.

Наибольшая эффективность обнаружения злоумышленника наблюдается, когда злоумышленник перенаправляет на себя все пакеты близлежащих узлов, чтобы осуществить атаку потребовалось 4 узла злоумышленника.

Заключение. В результате исследования был разработан метод вычисления доверия, позволяющий проводить оценку показателей загруженность узла и остаточная энергия узла сети. Оценка данных показателей с помощью порогового анализа, когда оценивается попадание текущих значений узла в доверительный интервал, позволяет обнаружить отклонение в поведении узла, при проведении им атаки.

Таблица 4

Вероятность ошибки 1 рода (P1error) «атака Сибиллы»

Количество узлов злоумышленника	Количество узлов подверженных атаке, %								
	5	10	20	30	40	50	60	65	70
1	0	0	0,1	0,06	0,04	0,08	0,06	0,06	0,06
2	0,05	0,04	0,05	0,04	0,05	0,04	0,04	0,03	0,04
3	0	0	0	0	0	0,08	0,04	0,08	0,06
4	0,05	0,05	0,01	0,01	0,01	0,01	0,06	0,08	0,07

Таблица 5

Вероятность ошибки 2 рода (P2error) «атака Сибиллы»

Количества узлов злоумышленника	Количество узлов подверженных атаке, %							
	5	10	20	30	40	50	60	70
1	0,67	0,4	0,4	0,4	0,28	0,4	0,28	0,57
2	0,67	0,4	0,14	0,4	0,28	0,28	0,28	0,57
3	0,67	0,4	0,14	0,14	0,4	0,28	0,28	0.28
4	0,67	0,57	0,4	0,4	0,4	0,28	0,1	0,1

При этом была проведена оценка возникновения ошибок 1 и 2 рода. Порог возникавших ошибок при количестве злоумышленных узлов менее 70 % позволяет с достаточной точностью выявлять злоумышленные узлы и блокировать их. При количестве злоумышленных узлов более 70 % точность обнаружения снижается, при этом, как правило, в реальной ситуации, когда узлы сети располагаются на достаточно большом расстоянии друг от друга и их количество измеряется тысячами узлов, злоумышленнику достаточно сложно превысить порог даже 50 % злоумышленных узлов в сети. При этом системы распределенного и централизованного вычисления доверия [20–23] не способны противодействовать «атакам Сибиллы» и «Отказ в обслуживании», так как анализируют только успешные/неуспешные события узла сети, а при реализации данных типов атак злоумышленник не производит неуспешных событий, а только способствует увеличению/перенаправлению трафика.

БИБЛИОГРАФИЧЕСКИЙ СИСОК

1. *Абрамов Е.С., Басан Е.С.* Разработка модели защищенной кластерной беспроводной сенсорной сети // Известия ЮФУ. Технические науки. – 2013. – № 12 (149). – С. 48-56.
2. *Басан Е.С., Макаревич О.Б., Абрамов Е.С.* Разработка системы обнаружения атак для кластерной беспроводной сенсорной сети // Информационное противодействие угрозам терроризма. – 2013. – № 20. – С. 134-140.
3. *Govindan K., Mohapatra P.* Trust computations and trust dynamics in mobile adhoc networks // A survey IEEE Communications Surveys & Tutorials. – No. 14 (2). – P. 279-298.
4. *Абрамов Е.С., Басан Е.С.* Анализ сценариев атак на беспроводные сенсорные сети // Материалы XIII Международной научно-практической конференции «ИБ–2013». Ч. 1. – Таганрог: Изд–во ТТИ ЮФУ, 2012. – С. 60-65.
5. *Шелухин О.И. , Симонян А.Г., Иванов Ю.А.* Особенности DDoS атак в беспроводных сетях // T–Comm – Телекоммуникации и Транспорт. – 2012. – № 11. – С. 67-71.
6. *Бельфер Р.А., Огурцов И.С.* Защита информационной безопасности сенсорной сети кластерной архитектуры с помощью механизма обнаружения вторжения // Вестник МГТУ им. Н.Э. Баумана: электронное издание. – 2013. – С. 1-7.
7. *Deepali Virmani, Manas Hemrajani, Shringarica Chandel.* Exponential Trust Based Mechanism to Detect Black Hole attack in Wireless Sensor Network // International Journal of Soft Computing and Engineering (IJSCE). – 2014. – P. 14-16.
8. *Гришечкина Т.А.* Анализ атак на сетевые протоколы в мобильных сенсорных сетях Ad Hoc // Известия ЮФУ. Технические науки. – 2012. – № 12 (137). – С. 68-74.
9. *Басан А.С., Басан Е.С., Макаревич О.Б.* Methodology of Countering Attacks for Wireless Sensor Networks Based on Trust.2016 // International Conference on Cyber–Enabled Distributed Computing and Knowledge Discovery. – P. 409-4012.
10. *Басан А.С., Басан Е.С., Макаревич О.Б.* Development of the Hierarchal Trust management System for Mobile Cluster–based Wireless Sensor Network // Proceeding SIN '16 Proceedings of the 9th International Conference on Security of Information and Networks. – 2016. – P. 116-122.
11. *Абрамов Е.С., Басан Е.С.* Разработка защищенного протокола управления мобильной кластерной сенсорной сетью // Информационное противодействие угрозам терроризма. – 2014. – № 23 (23). – С. 46-51.
12. *Abramov E.S., Basan E.S., Makarevich O.B*. Development of a secure Cluster–based wireless sensor network model // SIN'13. Proceedings of the 6th International Conference on Security of Information and Networks – November 26–28 2013, Aksaray, Turkey. – P. 372-375.
13. *Абрамов Е.С., Басан Е.С.* Разработка набора метрик для выбора главы кластера в мобильной сенсорной сети // Информационное противодействие угрозам терроризма. – 2014. – No. 23 (23). – С. 52-55.
14. *Теплицкая С.Н., Хусейн Я.Т.* Энергетически эффективный алгоритм самоорганизации в беспроводной сенсорной сети // Восточно-Европейский журнал передовых технологий. – 2012. – No. 2/9 (56). – С. 25-29.
15. *Mohammad Momani*. Bayesian Fusion Algorithm for Inferring Trust in Wireless Sensor Networks // Journal of Networks. – 2010. – No. 5 (7). – P. 815-822. DOI: 10.4304/jnw.5.7.815–822.
16. *Elmar Schoch, Michael Feiri, Frank Kargl, Michael Weber.* Simulation of Ad Hoc Networks: ns–2 compared to JiST/SWANS // SIMUTools. Marseille, France, 2008.
17. *Shelby Z., Bormann C.* 6LoWPAN: The Wireless Embedded Internet // Wiley Series on Communications Networking & Distributed Systems. – 2010. – P. 245.
18. *Басан А.С., Басан Е.С., Макаревич О.Б.* Программа анализа данных и вычисления доверия в беспроводной сенсорной сети. Свидетельство о государственной регистрации программы для ЭВМ №2016615606, 2016 г.
19. *Abramson N.* The Throughput of Packet Broadcasting Channels // IEEE Transactions on Communications. – 1977. – Vol. 25, No. 1. – С. 117-128.
20. *Ho J.W.* Zone–based trust management in sensor networks // in IEEE International Conference on Pervasive Computing and Communications. – 2009. – С. 1-2.
21. *Renjian Feng, Xiaona Han, Qiang Liu, and Ning Yu*. A Credible Bayesian–Based Trust Management Scheme for Wireless Sensor Networks // Hindawi Publishing Corporation International Journal of Distributed Sensor Networks. – С. 1-9. DOI: http://dx.doi.org/10.1155/2015/678926.

22. *Chen–xu Liu, Yun Liu, and Zhen–jiang Zhang*. Improved Reliable Trust–Based and Energy–Efficient Data Aggregation for Wireless Sensor Networks // Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2013. – C. 1-11. DOI: http://dx.doi.org/10.1155/2013/652495.
23. *Ganeriwal S., Balzano L.K., and Srivastava M.B.* Reputationbased framework for high integrity sensor networks // ACM Trans. Sen. Netw. – 2008. – Vol. 4, No. 3. – P. 1-37.

REFERENCES

1. *Abramov E.S., Basan E.S.* Razrabotka modeli zashchishchennoy klasternoy besprovodnoy sensornoy seti [Development of a model of a protected cluster wireless sensor network], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2013, No. 12 (149), pp. 48-56.
2. *Basan E.S., Makarevich O.B., Abramov E.S.* Razrabotka sistemy obnaruzheniya atak dlya klasternoy besprovodnoy sensornoy seti [Development of a system for detecting attacks for a cluster wireless sensor network], *Informatsionnoe protivodeystvie ugrozam terrorizma* [Information Counteraction to Terrorism Threats], 2013, No. 20, pp. 134-140.
3. *Govindan K., Mohapatra P.* Trust computations and trust dynamics in mobile adhoc networks, *A survey IEEE Communications Surveys & Tutorials*, No. 14 (2), pp. 279-298.
4. *Abramov E.S., Basan E.S.* Analiz stsenariev atak na besprovodnye sensornye seti [Analysis of attack scenarios for wireless sensor networks], *Materialy XIII Mezhdunarodnoy nauchno-prakticheskoy konferentsii «IB–2013»* [Proceedings of XIII International scientific-practical conference "Information security 2013"]. Part 1. Taganrog: Izd–vo TTI YuFU, 2012, pp. 60-65.
5. *Shelukhin O.I., Simonyan A.G., Ivanov Yu.A.* Osobennosti DDoS atak v besprovodnykh setyakh [Features of DDoS attacks in wireless networks], *T–Comm – Telekommunikatsii i Transport* [T–Comm – Telecommunications and Transport], 2012, No. 11, pp. 67-71.
6. *Bel'fer R.A., Ogurtsov I.C.* Zashchita informatsionnoy bezopasnosti sensornoy seti klasternoy arkhitektury s pomoshch'yu mekhanizma obnaruzheniya vtorzheniya [Protection of information security, sensor network cluster architecture is a mechanism for intrusion detection], *Vestnik MGTU im. N.E. Baumana: elektronnoe izdanie* [Herald of the Bauman Moscow State Technical University: electronic edition], 2013, pp. 1-7.
7. *Deepali Virmani, Manas Hemrajani, Shringarica Chandel.* Exponential Trust Based Mechanism to Detect Black Hole attack in Wireless Sensor Network, *International Journal of Soft Computing and Engineering (IJSCE)*, 2014, pp. 14-16.
8. *Grishechkina T.A.* Analiz atak na setevye protokoly v mobil'nykh sensornykh setyakh Ad Hoc [Analysis of attacks in mobile Ad Hoc networks using vulnerabilties in network protocols], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2012, No. 12 (137), pp. 68-74.
9. *Basan A.S., Basan E.S., Makarevich O.B.* Methodology of Countering Attacks for Wireless Sensor Networks Based on Trust.2016, *International Conference on Cyber–Enabled Distributed Computing and Knowledge Discovery*, pp. 409-4012.
10. *Basan A.S., Basan E.S., Makarevich O.B.* Development of the Hierarchal Trust management System for Mobile Cluster–based Wireless Sensor Network, *Proceeding SIN '16 Proceedings of the 9th International Conference on Security of Information and Networks*, 2016, pp. 116-122.
11. *Abramov E.S., Basan E.S.* Razrabotka zashchishchennogo protokola upravleniya mobil'noy klasternoy sensornoy set'yu [Developing a secure management Protocol for mobile cluster sensor network], *Informatsionnoe protivodeystvie ugrozam terrorizma* [Information Counteraction to Terrorism Threats], 2014, No. 23 (23), pp. 46-51.
12. *Abramov E.S., Basan E.S., Makarevich O.B*. Development of a secure Cluster–based wireless sensor network model, *SIN'13. Proceedings of the 6th International Conference on Security of Information and Networks – November 26–28 2013, Aksaray, Turkey*, pp. 372-375.
13. *Abramov E.S., Basan E.S.* Razrabotka nabora metrik dlya vybora glavy klastera v mobil'noy sensornoy seti [Develop a set of metrics to select the cluster head in mobile sensor networks], *Informatsionnoe protivodeystvie ugrozam terrorizma* [Information Counteraction to Terrorism Threats], 2014, No. 23 (23), pp. 52-55.
14. *Teplitskaya S.N., Khuseyn Ya.T.* Energeticheski effektivnyy algoritm samoorganizatsii v besprovodnoy sensornoy seti [Energetically effective algorithm of self–organization in a wireless sensor network], *Vostochno-Evropeyskiy zhurnal peredovykh tekhnologiy* [East–European Journal of Advanced Technologies], 2012, No. 2/9 (56), pp. 25-29.

15. *Mohammad Momani*. Bayesian Fusion Algorithm for Inferring Trust in Wireless Sensor Networks, *Journal of Networks*, 2010, No. 5 (7), pp. 815-822. DOI: 10.4304/jnw.5.7.815–822.
16. *Elmar Schoch, Michael Feiri, Frank Kargl, Michael Weber.* Simulation of Ad Hoc Networks: ns–2 compared to JiST/SWANS // SIMUTools. Marseille, France, 2008.
17. *Shelby Z., Bormann C.* 6LoWPAN: The Wireless Embedded Internet, *Wiley Series on Communications Networking & Distributed Systems*, 2010, pp. 245.
18. *Basan A.S., Basan E.S., Makarevich O.B.* Programma analiza dannykh i vychisleniya doveriya v besprovodnoy sensornoy seti. Svidetel'stvo o gosudarstvennoy registratsii programmy dlya EVM №2016615606, 2016 g. [Program data analysis and computing of trust in wireless sensor networks. The certificate of state registration of computer programs №2016615606, 2016].
19. *Abramson N.* The Throughput of Packet Broadcasting Channels, *IEEE Transactions on Communications*, 1977, Vol. 25, No. 1, pp. 117-128.
20. *Ho J.W.* Zone–based trust management in sensor networks, *in IEEE International Conference on Pervasive Computing and Communications*, 2009, pp. 1-2.
21. *Renjian Feng, Xiaona Han, Qiang Liu, and Ning Yu*. A Credible Bayesian–Based Trust Management Scheme for Wireless Sensor Networks, *Hindawi Publishing Corporation International Journal of Distributed Sensor Networks*, pp. 1-9. DOI: http://dx.doi.org/10.1155/2015/678926.
22. *Chen–xu Liu, Yun Liu, and Zhen–jiang Zhang*. Improved Reliable Trust–Based and Energy–Efficient Data Aggregation for Wireless Sensor Networks, *Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2013*, pp. 1-11. DOI: http://dx.doi.org/10.1155/2013/652495.
23. *Ganeriwal S., Balzano L.K., and Srivastava M.B.* Reputationbased framework for high integrity sensor networks, *ACM Trans. Sen. Netw*., 2008, Vol. 4, No. 3, pp. 1-37.

Статью рекомендовал к опубликованию д.т.н., профессор Н.И. Витиска.

Басан Елена Сергеевна – Южный федеральный университет; e-mail: ebasan@sfedu.ru; 347922, г. Таганрог, ул. Чехова, 2; тел.: +79515205488; кафедра безопасности информационных технологий; к.т.н.; ассистент**.**

Басан Александр Сергеевич – e-mail: asbasan@sfedu.ru; тел.: +79885370958; кафедра безопасности информационных технологий; к.т.н.; доцент.

Макаревич Олег Борисович – e-mail: mak@tsure.ru; тел.: +78634361518; кафедра безопасности информационных технологий; д.т.н.; профессор.

Basan Elena Sergeevna – Southern Federal University; e-mail: ebasan@sfedu.ru; 2, Chekhov street, Taganrog, 347922, Russia; phone: +79515205488; the department of information security; cand. of eng. sc.; assistant.

Basan Alexander Sergeevich – e-mail: asbasan@sfedu.ru; phone: +79885370958; the department of information security; cand. of eng. sc.; associate professor.

Makarevich Oleg Borisovich – e-mail: mak@tsure.ru; phone: +78634361518; the department of information security; dr. of eng. sc.; professor.

УДК 004.021 DOI 10.23683/2311-3103-2017-5-25-37

Л.К. Бабенко, Е.А. Ищукова, Е.А. Толоманенко

ДИФФЕРЕНЦИАЛЬНЫЙ АНАЛИЗ ШИФРА КУЗНЕЧИК*

Целью данной работы является исследование, разработка и реализация алгоритма Кузнечик, который является частью стандарта ГОСТ Р 34.12-2015, а также алгоритма для его дифференциального анализа. В ходе проведения исследований рассмотрен алгоритм Кузнечик, разработана рабочая программа шифрования и расшифрования на основе данно-

* Работа выполнена при поддержке гранта РФФИ №17-07-00654-а.