13. *Anishchenko B.C., Astakhov V.V., Vadivasova T.E., Neyman A.B., Strelkova G.I.* Nelineynye effekty v khaoticheskikh i stokhasticheskikh sistemakh [Nonlinear effects in chaotic and stochastic systems]. Moscow-Izhevsk: Institut komp'yuternykh issledovaniy, 2003, 544 p.
14. *Takens F.* Detecting Strange Attractors in Turbulence, in Dynamical Systems and Turbulence: Lecture Notes in Mathematics, Vol. 898 [ed. by D. Rang and L.S. Young]. Springer, Berlin, Heidelberg, 1980, 366 p.
15. *Bezruchko B.P., Smirnov D.A.* Matematicheskoe modelirovanie i khaoticheskie vremennye ryady [Mathematical modeling and chaotic time series]. Saratov: GosUNTs «Kolledzh», 2005, 320 p.
16. *Malinetskiy G.G., Potapov A.B.* Sovremennye problemy nelineynoy dinamiki [Modern problems of nonlinear dynamics]. 2nd ed. Moscow: Editorial URSS, 2002, 360 p.
17. Fonem [The phoneme]. Available at: http://ru.wikipedia.org/wiki/Fonema (accessed: 15 October 2015).
18. Bortovye informatsionnye sistemy: kurs lektsiy [On-Board information systems: lectures]. Available at: http:// window.edu.ru/catalog/pdf2txt/082/59082/29039 (accessed: 15 October 2015).
19. *Kopytov V.V., Yakushev D.V.* Metody kodirovaniya rechevykh signalov s pomoshch'yu rekonstruirovannoy modeli rechevogo protsessa [Methods of coding of speech signals with the help of the reconstructed model of speech process], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2013, No. 1 (138), pp. 37-44.

Статью рекомендовал к опубликованию д.т.н., профессор В.В. Копытов.

**Иванов Илья Игоревич** – Институт информационных технологий и телекоммуникаций Северо-Кавказского федерального университета, г. Ставрополь; e-mail: lollol@bk.ru, 267701@mail.ru; 355026, г. Ставрополь, ул. Пригородная, 235/1, кв. 29; тел.: +79187570745; кафедра организации и технологии защиты информации; аспирант.

**Ivanov Ilya Igorevich** – Institute of Information Technologies and Telecommunications, North-Caucasus Federal University, Stavropol; e-mail: lollol@bk.ru, 267701@mail.ru; 235/1, Prigorodnaya street, kv. 29, Stavropol, 355026, Russia; phone: +79187570745; the department of Information Security of Automated Systems; postgraduate student.

УДК 004.056: 004.73

**Е.С. Абрамов, Е.С. Басан, А.С. Басан**

## РАЗРАБОТКА СИСТЕМЫ УПРАВЛЕНИЯ УРОВНЕМ ДОВЕРИЯ В МОБИЛЬНОЙ КЛАСТЕРНОЙ БЕСПРОВОДНОЙ СЕНСОРНОЙ СЕТИ*

*Проблема обеспечения безопасности беспроводных сенсорных сетей (БСС) активно исследуется как за рубежом, так и в России. В данной статье представлены результаты разработка системы управления уровнем доверия (СУУД). Работа системы основана на сборе информации о соседних узлах и обмене данными соседних узлов между собой, и вычислении значений доверия на основе полученных наборов признаков. СУУД позволяет справиться с угрозами исходящими от внутреннего злоумышленника сети и с угрозой компрометации узла, обнаружить и изолировать аномальный узел. Основной целью создания системы управления доверием является защита БСС от вредоносных действий злоумышленника. Разработанная система сочетает в себе свойства энергетической эффективности и надежности. Основными свойствами системы управления доверием являются: обнаружение неправомерных действий злоумышленника; блокирование вредоносных узлов; предотвращение реализации атаки злоумышленником; определение подлинных узлов; установление доверенных соединений между подлинными узлами; определение неисправных узлов и блокирование их работы. СУУД позволяет не только устанавливать доверенные отношения между узлами-сенсорами, но обнаруживать и блокировать вторжения со стороны злоумышленника. Обнаружение вторжений возможно за счет анализа количества и качества трафика и сравнение этого показателя с уровнем остаточной энергии узла. Таким образом, если злоумышленник проводит активную атаку, к примеру, производит задержку пакетов, то система сможет его вычислить и предпринять дейст-*

* Работа выполнена при поддержке гранта РФФИ № 14-37-50914.

*вия для его блокировки. Данная система не сможет зафиксировать атаки типа пассивное прослушивание и перехват информации, для защиты от подобных атак необходимо использование криптографических методов. В результате проведения экспериментов выявлено, что разработанная система имеет наименьшее энергопотребление по сравнению с аналогами и удовлетворительные результаты при определении узлов злоумышленника.*

*Беспроводные сенсорные сети; кластеризация; атаки; доверие; протокол; алгоритмы; обнаружение аномалий; подлинность; оценка уровня доверия.*

**E.S. Abramov, A.S. Basan, E.S. Basan**

## DEVELOPMENT OF DEVELOPMENT OF THE TRUST MANAGEMENT SYSTEM FOR MOBILE WIRELESS SENSOR NETWORK

*To date, there are a large number of papers on various aspects of security in wireless sensor networks. We developed the trust management system (TMS). The system is based on data collection and exchange between neighboring nodes and a calculation of the trust values based on received metrics. This system helps to resist from threats posed by malicious insiders and the threat of compromised nodes, to detect and isolate anomalous node. The main purpose of this system is to protect the WSN from malicious actions of the attacker. To achieve the goal we need to perform the following tasks: detecting misconduct attacker; blocking malicious nodes; prevent the implementation of attacks; determining the authenticity of the nodes; establish trusted connections between honest nodes; identification of faulty nodes and blocking their work. The trust system allows not only establishing trust relationship between neighboring nodes, but also allows detecting and blocking invasion by the attacker. Intrusion detection is possible by analyzing the quantity and quality of forwarding packets and compares this value with the level of residual node energy. Thus, if an attacker realized an active attack, for example, a packet delay; the system can detect it and take action to block it. This system will not be able to fix passive listening attack and interception of information, to protect against such attacks requires the use of cryptographic techniques.*

*Wireless sensor networks; clustering; attack; trust; protocol; algorithms; anomaly detection; authenticity; confidence level.*

**Введение**. Проблема создания энергетически эффективной и надежной системы обеспечения безопасности в БСС является наиболее актуальной в связи с ограниченностью ресурсов узлов сети, а также уязвимостью сети к воздействиям злоумышленника. Беспроводная среда передачи, динамически изменяющаяся топология, отсутствие инфраструктуры, большой поток данных, неограниченное количество узлов сети – все эти факторы позволяют злоумышленнику достаточно легко провести анализ сети на уязвимости и реализовать атаку, которая может нарушить работу, как самой сети, так и объекта в целом. Основным недостатком большинства работ в данной области является завышенное потребление ресурсов, которое происходит по следующим причинам: большая вычислительная нагрузка на сенсоры, большое количество передаваемых сообщений, не рациональный выбор топологии сети. Для снижения истощения ресурсов необходимо снизить обмен пакетами между узлами, так как именно на отправку и получение сообщений приходится наибольший расход энергии, необходимо уменьшить размер передаваемых пакетов, выполнение наиболее сложных вычислений мощными узлами. Поэтому предложено использовать кластеризацию сети, которая позволит разделить сеть на кластеры и выбрать в каждом кластере главу, который возьмет на себя основные вычисления. Целью проекта является разработка энергетически эффективной системы защиты сети, объединяющей в себе возможности системы обнаружения атак (СОА) [1] и системы управления доверием (СУД). Для достижения поставленной цели необходимо выполнить следующие задачи: обнаружение неправомерных действий злоумышленника; блокирование вредоносных узлов; предотвращение реализации атаки злоумышленником; определение подлинных узлов; установление доверенных соединений между подлинными узлами; определение неисправных узлов и блокирование их работы.

Ключевым понятием при создании СУУД является доверие. Определим доверие, как значение в диапазоне [0,1], показывающее степень уверенности узла A относительно узла B, в том что B ведет себя нормально т.е. может надлежащим образом передавать пакеты другим узлам. Значение доверия вычисляется статистически из полученных путем наблюдения данных. Значение доверия близкое к 0 подразумевает, что соседний узел является ненадежным для передачи пакетов, но если значение доверия ближе к 1, то узел надежно передает пакеты [2].

Распределенные вычисления доверия на основе прямых наблюдений за соседом – это такие вычисления, где каждый узел наблюдает за соседями по их отчетам о событиях и сохраняет эти отчеты в памяти. Узел, измеряющий уровень доверия сравнивает отчеты, полученные самостоятельно с теми отчетами, которые получил от соседа, уровень доверия которого он измеряет, и с отчетами от других соседей [3]. Распределенные вычисления при получении рекомендаций от соседей могут быть реализованы: путем голосования [4], на основе отчетов об угрозах [5]. Смешанный (гибридный) метод основан на том, что уровень доверия рассчитывается, как на основе прямых наблюдений, так и рекомендаций от других узлов. Централизованные методы вычисления доверия в основном используют Доверенных Агентов, которые достижимы для всех узлов сети и вычисляют доверие для всей группы или помогают другим узлам вычислить доверие путем предоставления им начального значения уровня доверия [6].

**Аналоги разработанной системы.** Особенность EigenTrus [7] заключается в назначении уникального глобального значения уровня доверия каждому узлу, на основании предыдущей истории узлов. Локальный уровень доверия точки i к точке jопределяется следующим образом:

$$S_{ij} = sat(i,j) – unsat(i,j),$$

т.е., разница между удовлетворительными и неудовлетворительными результатами взаимодействия узлов. Глобальное значение уровня доверия узла i получается путем сбора локальных значений уровня доверия от соседних узлов, взвешенное относительно глобального уровня доверия соседних узлов путем опроса соседних узлов, так узел-сенсор «зарабатывает» репутацию.

BTRM-WSN [8] это модель доверия для беспроводных сенсорных сетей на основе муравьиного алгоритма. Она позволяет находить наиболее доверенные пути, опираясь на авторитетные узлы сети. Набор муравьев (агентов) проходит через всю БСС и пока они находят наиболее авторитетные пути, они оставляют за собой следы феромонов в каждой связи между двумя узлами. Феромоны между сенсорами a и b определяются, как $\tau_{ab}$ – узел a ищет наиболее доверенный путь через узел b.

PowerTrust это надежная система на основе обратного степенного закона [9]. Степенное распределение означает, что узел небольшим количеством обратных связей встречается чаще, чем узел с большим количеством обратных связей. Только несколько узлов имеют большую степень, чем другие, и, в частности те узлы, которые динамически выбирают в качестве передающих узлов и считается наиболее авторитетными в системе. Узлы передатчики могут быть динамически заменены, если они становятся менее активными или показывают не доверенное поведение.

ATSN [10] СУД на основе агентов, которые оценивают уровень доверия узлов и составляют их рейтинг. Узлы-сенсоры получают этот рейтинг от агентов. Согласно полученной информации, сенсоры принимают решения о том, с какими узлами лучше взаимодействовать. Значение доверия вычисляется согласно параметрам T = (pt, nt, ut), где p это положительное событие, n отрицательное событие и u неопределенное, по заданной формуле:

$$\begin{cases} pt = c\dfrac{p+1}{p+n+2} \\ nt = c\dfrac{n+1}{p+n+2} \\ ut = 1 - pt - nt \end{cases}$$

где с это определенность события.

TTSN [11] СУД на основе задач для БСС, здесь узел-сенсор сохраняет информацию о репутации соседних узлов для различных задач и использует репутацию для оценки уровня доверия. В БСС каждый узел может выполнять различные задачи по отношению к различным соседям. Узел имеет различный уровень доверия для различных задач и различных соседей. TTSN рассчитывает доверие с помощью модуля «задачи и управления доверием». Данный модуль включает три основных компонента: модуль мониторинга, управление репутацией и модуль задач и управления доверием.

**Атаки на схемы вычисления доверия в БСС.** В [12] представлен перечень атак, реализуемых в БСС. В таблице 1 представлено соотношение схем управления доверием в сети и атак, которые могут быть реализованы в БСС:

- Атака плохие рекомендации (АПРе (Bad mouthing attack)) возникает, когда узел намеренно дает плохие рекомендации о своих соседях [13].
- Атака противоречивое поведение (АПП (Conflicting behaviour attack)) злоумышленник дает хорошие рекомендации одной группе узлов и плохие рекомендации другой группе узлов по отношению к одному и тому же узлу.
- Атака маскировки (АМ) (Camouflage) злоумышленник пытается выстроить доверительные отношения, представляя отчеты в соответствие с наблюдениями большинства. После того, как он получил достаточное количество значений доверия, он осуществляет злоумышленные действия [14].
- Атака сговор (АС (Collusion attack)) реализуется несколькими злоумышленниками, состоящими в сговоре и дающими ложные рекомендации нормальным узлам [15].
- Атака «новичок» (АН (Newcomer attacks))злоумышленник выходит из сети и присоединяется снова, чтобы избавиться от предыдущей плохой истории и накапливать новый уровень доверия [16].

Таблица 1

**Сравнение схем вычисления доверия относительно атак на БСС**

| Схемы управления доверием | Виды атак | | | | |
|---|---|---|---|---|---|
| | АПРе | АПП | АМ | АС | АН |
| Распределенное вычисление доверия | | | | | |
| Прямые наблюдения | *v* | ***V*** | × | *v* | × |
| Рекомендации | × | ***V*** | × | × | *v* |
| Смешанные | *v* | ***V*** | *v* | *v* | *v* |
| Централизованное вычисление доверия | | | | | |
| Методы на основе агентов доверия | *v* | ***V*** | *v* | *v* | *v* |

**Разработка СУУД.** Централизованная схема наиболее приемлема для кластерной БСС [17], так как: в централизованной схеме учитывается иерархическая структура сети; доверенные агенты, в роли которых выступают ГК, берут на себя большую часть вычислений, что продлевает жизнь сети и снижает загруженность канала.

СУУД состоит из нескольких модулей, комбинация которых зависит от, того на каком узле установлена система. В представленной сети, имеется три вида узлов: узел-сенсор, глава кластера и базовая станция. Каждый тип узлов выполняет собственные функции и имеет разные вычислительные возможности, а также энергетические ресурсы, поэтому данная система адаптирована для каждого вида узлов. Архитектура СУУД представлена на рис. 1.

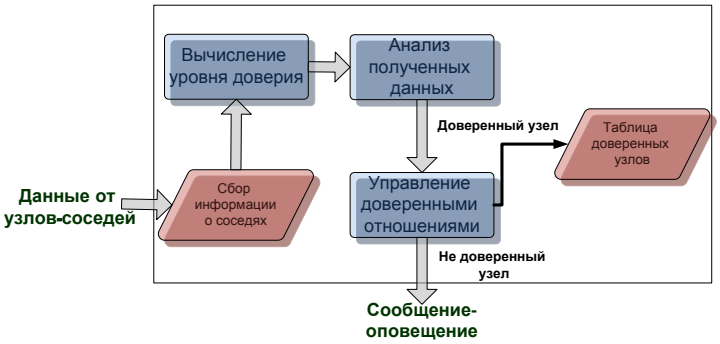


*Рис. 1. Система управления уровнем доверия*

На модуль сбора информации поступают данные от узлов-соседей, затем происходит вычисление уровня доверия, исходя из полученных данных. Далее происходит анализ результатов вычисления, который проводится разными способами в зависимости от типа узла. Следующий модуль управления доверенными отношениями отсутствует у узла-сенсора, он определяет действие с информацией об узле, если узел прошел проверку благополучно, то данные о нем заносятся в таблицу доверенных узлов, и рассылается сообщение другим узлам в кластере, что узел доверенный. Если после анализа узел-сенсор выяснил, что узел доверенный, то он заносит его в свою таблицу, если узел не доверенный, то данная информация отправляется на проверку главе кластера и с помощью модуля управления доверенными отношениями он решает, что делать.

**Сбор информации о соседях.** Два узла считаются соседними, если они находятся в одном радиодиапазоне передачи и приема сообщений. В силу широковещательной природы беспроводных сетей, заданный узел может собирать информацию о передаче пакетов соседями напрямую путем отслеживания всех принимаемых пакетов на MACуровне и составления статистики. В случае с КБСС необходимо дополнить, что узлы также должны находиться в одном кластере. Одной из задач системы является обнаружение вредоносного поведения злоумышленника. Следующим шагом является выявление признаков, по которым будет определяться наличие атаки. В [18] приводится перечень таких параметров, к примеру: полученные/отправленные/перенаправленные пакеты с данными, пакеты маршрутизации, управляющие пакеты, пакеты уровня доверия, точность управляющих пакетов, пакетов маршрутизации, пакетов с данными, изменение адреса пакета, процент изменения записей маршрута, количество соседей.

**Анализ полученных данных.** В [19] даны формулы для расчета уровня доверия. На данном этапе необходимо рассчитать следующие параметры: $Q_{ik}(E)$ – уровень остаточной энергии; $DT_n$ – суммарный уровень доверия узла A относительно узда B; $M_y$ – уровень мобильности узла; d – расстояние до базовой станции; S – уровень стабильности. Приведем расчеты для уровня доверия.

$$T_i^{A,B} = \frac{a_i s_i^{A,B} - b_i F_i^{A,B}}{c_i s_i^{A,B} + d F_i^{A,B}},$$

где $T_i^{AB}$ – это значение доверия узла A относительно узла B. $S_i^{AB}$ – это количество успешных событий типа i, которые измерил узел A для узла B. $F_i^{AB}$ – это количество неудачных событий типа i, которые измерил узел A для узла B и $a_i$,$b_i$,$c_i$,$d_i$ вес/значимость успешных событий по сравнению с весом/значимостью неуспешных событий. Данное значения уровня доверия рассчитывается для каждого события сети, которое рассмотрено в таблице.

Эти значения доверия, связанные с поведением, умножаются на весовой коэффициент ($W_i$), отражающий их значение в иерархии безопасности и затем суммируются, для вычисления общего значения надежности узла, как показано в следующем уравнении.

$$DT^{A,B} = \sum_{i=1}^{k} W_i * T_i{}^{A,B}$$

**Управление доверенными отношениями.** В СУУД проводится дополнительная проверка, позволяющая установить, является ли узел доверенным. Данный модуль работает согласно следующему алгоритму.

**Алгоритм определения доверия к узлу**

```
1: CH get parameters from analyzer
2: CH request Qik(E), DTn from Ni  Qik(E)
3: CH calculate DTch
      if DTch  =   DTn
            then continue
                  else Ni (  DTn ) = untrusted
4: CH:
      if Qik(E) =  max and Total pack = [min,average]
Qik(E) = average; Total pack = [average, thresold], Qik(E)
= max and min<Total pack<max
      then  Ni= trusted
            else
            if MAX (packet type) = Manage_pack
                  then Ni = untrusted
            if MAX (packet type) = Route_pack
                  then Ni = untrusted
            if MAX (packet type) = Data_pack
                  then Ni = uncertain
```

Глава кластера (CH) пересчитывает присланные узлами-сенсорами (Ni) значения уровня доверия и проверяет их корректность, если узел прислал неверные значения, то он признается не доверенным. Далее CH проверяет соотношения уровня остаточной энергии узлов и количество отправленных пакетов. Энергия узла должна уменьшаться пропорционально количеству отправленных пакетов. Далее, если было обнаружено несоответствие, то узел делает качественную проверку пакетов, определяя количество какого типа пакетов отправлено больше всего: Manage_pack – управляющие пакеты; Route_pack – пакеты; маршрутизации Data_pack – пакеты с данными. При этом должны выполняться условия:

1) $\begin{cases} Q_i^k(E) = \text{максимальное} \\ \text{Total pack} = \text{минимальное, среднее} \end{cases}$

2) $\begin{cases} Q_i^k(E) = \text{среднее} \\ \text{Total pack} = \text{среднее, пороговое} \end{cases}$

3) $\begin{cases} Q_i^k(E) = \text{максимальное} \\ \text{минимальное} < Total\ pack < \text{максимальное} \end{cases}$

**Оценка эффективности СУУД.** Моделирование системы проводилось с использованием эмулятора TRMSim–WSN5.0 [20], который содержит набор реализованных моделей доверия, а также позволяет добавлять собственные модели. Для моделирования использовалась сеть, состоящая из 50 % сенсоров, 10 % базовых станций, 40 % узлов злоумышленника, диапазон радиочастот 42,8 МГц (7 м), сеть является динамической, пример сети представлен на рис. 2. Также в данном эмуляторе есть возможность выбора поведения злоумышленника, на основании которого реализуются следующие типы атак: Атака плохие рекомендации; Атака сговор; Атака маскировки (шантаж); Атака плохие рекомендации; Атака блокировка узла; Атака блокировка узла с наличием условий; Сибил атака; Атака противоречивое поведение.

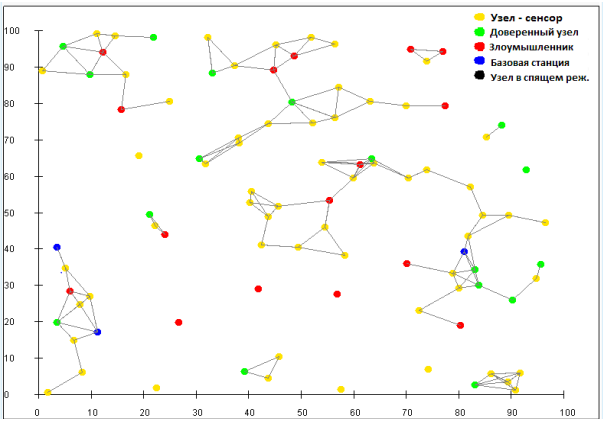


*Рис. 2. БСС развернутая в TRMSim–WSN 5.0*

В качестве параметров для оценки эффективности использовалось:

- Accuracy (точность) – точность работы модели, т.е. точность выбора доверенного узла для передачи данных.
- Pathlength (длина пути) - количество переходов ("прыжков") необходимое для каждого узла сети, чтобы достичь доверенный узел (глава кластера или базовая станция).
- Energy consumption (потребление энергии) – количество энергии потребляемое каждым видом узлов сети.

Результат моделирования для EigenTrus показан на рис. 3. Количество прыжков необходимое для достижения доверенного сервера в среднем составило 5,25, а точность выбора доверенного сервера вместо злоумышленного в среднем 43,04 %. График точности слишком скачкообразный, скачки обусловлены тем, что каждые 20 раундов алгоритма происходит атака злоумышленника.

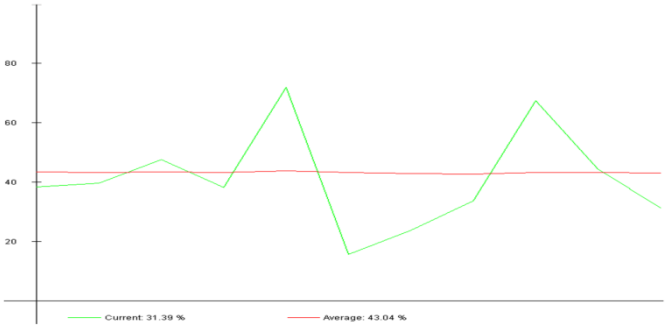


*Рис. 3. Оценка точности метода управления доверием EigenTrus*

Результаты для BTRM-WSN представлены на рис. 4. Средняя точность выбора доверенного узла и количество прыжков, также значительно выше и составляет соответственно 64,3 % и 2,89.


*Рис. 4. Оценка точности метода управления доверием BTRM-WSN*

На рис. 5 изображены результаты для модели PowerTrust, которая демонстрирует достаточно низкий результат для точности выбора доверенного узла всего 37,82 %, среднее количество прыжков 3,91.

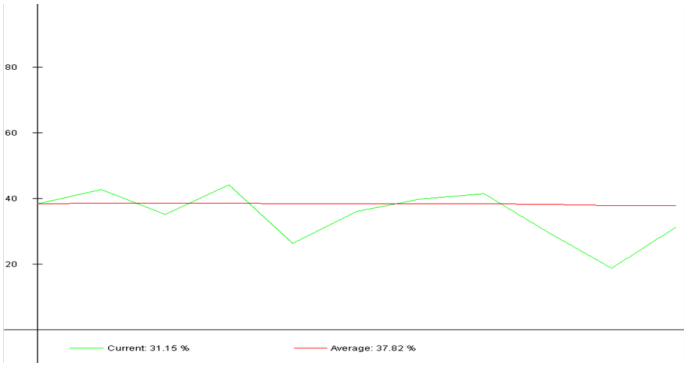


*Рис. 5. Оценка точности метода управления доверием PowerTrust*

Модель PowerTrust показывает лучшие результаты, когда не реализуются атаки: Атака сговор; Атака маскировки (шантаж); Атака плохие рекомендации. Точность является наиболее критичным параметром и характеризует способность сети справляться с атаками.

На рис. 6 изображены результаты для СУУД. Длина пути не самая низкая составляет 4,92. При этом точность работы системы составляет 86,72 %.

Результаты моделирования всех аналогов и разработанной системы представлены в табл. 2.

В табл. 3 представлены результаты оценки эффективности противодействия атакам, полученные в результате моделирования, а также в результате теоретических исследований. Как видно из таблицы потребление энергии у СУУД на много ниже, чем у аналогов, что и требовалось при разработке системы.

Таким образом, можно отметить, что СУУД и BTRM-WSN являются наиболее эффективными системами в отношении противодействия атакам.

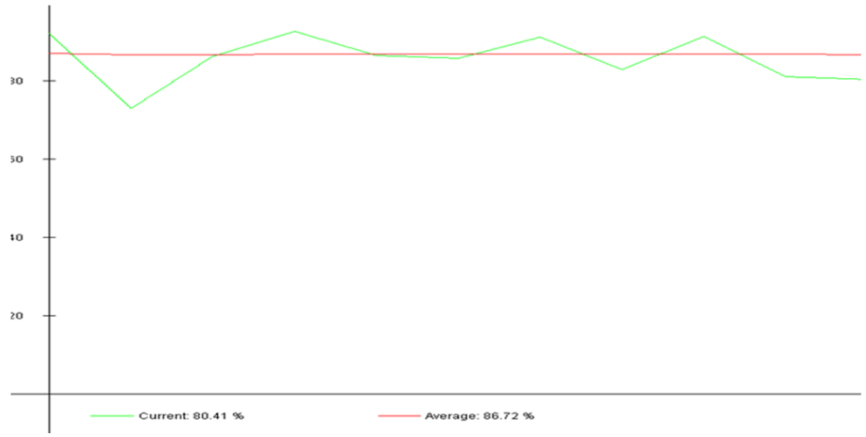


*Рис. 6. Оценка точности системы управления уровнем доверия*

Таблица 2

**Сравнительная таблица результатов моделирования**

| СУД | Параметры сравнения систем | | | | |
|---|---|---|---|---|---|
| | Точность, % | Потребление энергии, Дж | Длина пути, | Max точность, % | Min точность, % |
| EigenTrus | 43,04 | $6,2*10^{11}$ | 5,25 | 85 | 18 |
| BTRM-WSN | 64,3 | $6,1*10^{13}$ | 2,89 | 80 | 50 |
| PowerTrust | 37,82 | $4,0*10^{10}$ | 3,91 | 45 | 20 |
| СУУД | 86,72 | $5,8*10^{9}$ | 4,92 | 93 | 75 |

Таблица 3

**Сравнительная характеристика способности моделей доверия противодействовать атакам**

| Атаки | **МОДЕЛИ ДОВЕРИЯ** | | | |
|---|---|---|---|---|
| | EigenTrus | BTRM-WSN | PowerTrust | СУУД |
| Плохие рекомендации | | | | |
| Сговор | | | | |
| Маскировка (шантаж) | | | | |
| Блокировка узла | x | | X | |
| Блокировка с условиями | x | | X | |
| Сибил атака | | x | X | x |
| Противоречивое поведение | x | x | X | |

**Заключение**. По результатам моделирования и теоретических оценок разработанной системы можно отметить следующее:

- Решена задача разработки энергетически эффективной системы, данная система затрачивает наименьшее количество энергии по сравнению с аналогами.

- СУУД показывает стабильный результат в определении доверенного узла, для дальнейшей передачи данных, при этом не наблюдается больших скачков между максимальным и минимальным значениями;
- В отношении параметра длина пути, данный параметр имеет не самое высокое значение, но при разработке системы он не являлся критичным.
- СУУД показывает удовлетворительные результаты в отношении противодействия атакам, система не может противостоять только Сибил атаке.

Таким образом, СУУД удовлетворяет заданным требованиям и решает поставленные задачи. Дальнейшее исследование предполагает моделирование большего количества атак, и сравнение с большим количеством аналогов. Также необходимо увеличить количество параметров оценки эффективности. К примеру, оценивать пропускную способность сети, время блокировки узла злоумышленника, уровень доверия между узлами сети, а также ложные срабатывания.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК


1. *Mitrokotsa A., Dimitrakakis C.* Intrusion detection in MANET using classification algorithms: The effects of cost and model selection // Ad Hoc Networks. – 2013. – № 11. – P. 226-237.
2. *Ho J.W.* Zone-based trust management in sensor networks // in IEEE International Conference on Pervasive Computing and Communications. – 2009. – P. 1-2.
3. *Jiang T., Baras J.S.* Trust evaluation in anarchy: A case study on autonomous networks // 25th IEEE International Conference on Computer Communications, INFOCOM'06. –2006. – P. 1-12.
4. *Liu Z., Joy A.W., Thompson R.A.* A dynamic trust model for mobile ad hoc networks // IEEE International Workshop on Future Trends of Distributed Computing Systems, FTDCS'04. – 2004. – P. 80-85.
5. *Josang A., Ismail R., Boyd C.* A survey of trust and reputation systems for online service provision // Decis. Support Syst. – 2007. – Vol. 43, № 2. – P. 618-644.
6. *Dressler F.* A Study of Self-Organization Mechanisms in Ad Hoc and Sensor Networks // Computer Communications. – 2008. – Vol. 31, № 13. – P. 3018-3029.
7. *Kamvar S., Schlosser M., Garcia-Molina H.* The EigenTrust Algorithm for Reputation Management in P2P Networks, // Proceedings of the 12th international conference on World Wide Web. – 2008. – P. 640-651.
8. *Velloso P.B., Laufer R.P., Pujolle G.* A trust model robust to slander attacks in adhocnetworks // IEEE International Conference on Computer Communications and Networks (ICCCN08). – 2008. – P. 1-6.
9. *Gomez Marmol F., Martínez Perez G.* Providing Trust in Wireless Sensor Networks using a Bio-inspired Technique // Telecommunication Systems Journal. – 2011. –Vol. 46, № 2. – P. 163-180.
10. *Zhou R., Hwang, K.* PowerTrust: A Robust and Scalable Reputation System for Trusted Peer-to-Peer Computing // IEEE Transactions on Parallel and Distributed Systems. – 2007. – Vol. 18, №. 4. – P. 460-473.
11. *Handy M.J., Haase M., Timmermann D.* Low energy adaptive clustering hierarchy with deterministic Cluster-Heads selection // 4th International Workshop on Mobile and Wireless Communications Network. – 2002. – P. 368-372.
12. *Chen H., Wu H., Zhou X.* Agent-based trust model in wireless sensor networks // 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing. – 2007. – P. 119-124.
13. *Chen H.* Task-based trust management for wireless sensor networks // International Journal of Security and Its Applications. – 2009. – Vol. 3, № 2. – P. 21-26.
14. *Teodor-Grigore*. Main Types of Attacks in Wireless Sensor Networks // Proceeding SSIP'09/MIV'09. – USA, 2009. – P. 180-185.
15. *Lima M.N.,. dos Santos A.L. and Pujolle G*. A survey of survivability in mobile ad hoc networks // IEEECommun. Surveys Tuts. – 2009. – Vol. 11, №. 1. – P. 66-77.
16. *Karan Singh, YadavR. S., Ranvijay.* A reviewpaperonadhocnetworksecurity // International Journal of Computer Science and Security. – 2007. – Vol. 1, № 1. – P.52-69.
17. *Mitrokotsa A., Dimitrakakis C.* Intrusion detection in MANET using classification algorithms: The effects of cost and model selection. AdHocNetworks // Ref.Libr. – 2013. – Vol. 11, № 1. – P. 226-237.

18. *Абрамов Е.С., Басан Е.С.* Разработка модели защищенной кластерной беспроводной сенсорной сети // Известия ЮФУ. Технические науки. – 2013. – № 12 (149). – С. 48-56.
19. *Abramov E., Basan E., Makarevich O.* Development of a secure Cluster-based wireless sensor network model // SIN'13. Proceedings of the 6th International Conference on Security of Information and Networks. – 2013. – P. 372-375.
20. *Felix Gomez Marmol and Gregorio Martnez Perez.* TRMSim-WSN. Trust and Reputation Models Simulator for Wireless Sensor Networks // In Proceedings of the IEEE International Conference on Communications, Communication and Information Systems Security Symposium, Dresden, Germany. – 2009. – P. 1-5.

REFERENCES

1. *Mitrokotsa A., Dimitrakakis C.* Intrusion detection in MANET using classification algorithms: The effects of cost and model selection, *Ad Hoc Networks*, 2013, No. 11, pp. 226-237.
2. *Ho J.W.* Zone-based trust management in sensor networks, *in IEEE International Conference on Pervasive Computing and Communications*, 2009, pp. 1-2.
3. *Jiang T., Baras J.S.* Trust evaluation in anarchy: A case study on autonomous networks, *25th IEEE International Conference on Computer Communications, INFOCOM'06*, 2006, pp. 1-12.
4. *Liu Z., Joy A.W., Thompson R.A.* A dynamic trust model for mobile ad hoc networks, *IEEE International Workshop on Future Trends of Distributed Computing Systems, FTDCS'04*, 2004, pp. 80-85.
5. *Josang A., Ismail R., Boyd C.* A survey of trust and reputation systems for online service provision, *Decis. Support Syst*., 2007, Vol. 43, No. 2, pp. 618-644.
6. *Dressler F.* A Study of Self-Organization Mechanisms in Ad Hoc and Sensor Networks, *Computer Communications*, 2008, Vol. 31, No. 13, pp. 3018-3029.
7. *Kamvar S., Schlosser M., Garcia-Molina H.* The EigenTrust Algorithm for Reputation Management in P2P Networks, *Proceedings of the 12th international conference on World Wide Web*, 2008, pp. 640-651.
8. *Velloso P.B., Laufer R.P., Pujolle G.* A trust model robust to slander attacks in adhocnetworks, *IEEE International Conference on Computer Communications and Networks (ICCCN08)*, 2008, pp. 1-6.
9. *Gomez Marmol F., Martínez Perez G.* Providing Trust in Wireless Sensor Networks using a Bio-inspired Technique, *Telecommunication Systems Journal*, 2011,Vol. 46, No. 2, pp. 163-180.
10. *Zhou R., Hwang, K.* PowerTrust: A Robust and Scalable Reputation System for Trusted Peer-to-Peer Computing, *IEEE Transactions on Parallel and Distributed Systems*, 2007, Vol. 18, No. 4, pp. 460-473.
11. *Handy M.J., Haase M., Timmermann D.* Low energy adaptive clustering hierarchy with deterministic Cluster-Heads selection, *4th International Workshop on Mobile and Wireless Communications Network*, 2002, pp. 368-372.
12. *Chen H., Wu H., Zhou X.* Agent-based trust model in wireless sensor networks, *8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing*, 2007, pp. 119-124.
13. *Chen H.* Task-based trust management for wireless sensor networks, *International Journal of Security and Its Applications*, 2009, Vol. 3, No. 2, pp. 21-26.
14. *Teodor-Grigore*. Main Types of Attacks in Wireless Sensor Networks, *Proceeding SSIP'09/MIV'09*. USA, 2009, pp. 180-185.
15. *Lima M.N.,. dos Santos A.L. and Pujolle G*. A survey of survivability in mobile ad hoc networks, *IEEECommun. Surveys Tuts*, 2009, Vol. 11, No. 1, pp. 66-77.
16. *Karan Singh, YadavR. S., Ranvijay.* A reviewpaperonadhocnetworksecurity, *International Journal of Computer Science and Security*, 2007, Vol. 1, № 1, pp.52-69.
17. *Mitrokotsa A., Dimitrakakis C.* Intrusion detection in MANET using classification algorithms: The effects of cost and model selection. AdHocNetworks, *Ref. Libr*., 2013, Vol. 11, No. 1, pp. 226-237.
18. *Abramov E.S., Basan E.S.* Razrabotka modeli zashchishchennoy klasternoy besprovodnoy sensornoy seti [Development of a secure cluster-based wireless sensor network model], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2013, No. 12 (149), pp. 48-56.

19. *Abramov E., Basan E., Makarevich O.* Development of a secure Cluster-based wireless sensor network model, *SIN'13. Proceedings of the 6th International Conference on Security of Information and Networks*, 2013, pp. 372-375.
20. *Felix Gomez Marmol and Gregorio Martnez Perez.* TRMSim-WSN. Trust and Reputation Models Simulator for Wireless Sensor Networks, *In Proceedings of the IEEE International Conference on Communications, Communication and Information Systems Security Symposium, Dresden, Germany*, 2009, pp. 1-5.

Статью рекомендовал к опубликованию к.т.н. М.Н. Казарин.

**Абрамов Евгений Сергеевич** – Южный федеральный университет; e-mail: abramoves@sfedu.ru; 347928, г. Таганрог, пер. Некрасовский, 44; тел.: +78634371905; кафедра безопасности информационных технологий; зав. кафедрой; к.т.н.; доцент.

**Басан Елена Сергеевна** – e-mail: ele-barannik@yandex.ru; кафедра безопасности информационных технологий; аспирантка.

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

**Abramov Evgeny Sergeevich** – Southern Federal University; e-mail: abramoves@sfedu.ru; 44, Nekrasovskiy, Taganrog, 347928, Russia; phone: +78634371905; the department of IT Security; head of the department; cand. of eng. sc.; associate professor.

**Basan Elena Sergeevna** – e-mail: ele-barannik@yandex.ru; the department of IT Security; postgraduate student.

**Basan Alexander Sergeevich** – e-mail: asbasan@sfedu.ru; department of IT Security; associate professor.