РАСЧЕТ РИСКА БЕЗОПАСНОСТИ АТАК DOS СБОРНЫХ СЕНСОРНЫХ УЗЛОВ НА БАЗЕ МЕТОДА FUZZY-AHP ДЛЯ ОПРЕДЕЛЕНИЯ АРХИТЕКТУРЫ ВЗАИМОДЕЙСТВИЯ МЕЖДУ НАЗЕМНЫМИ СЕНСОРНЫМИ СЕТЯМИ И FANET В ЛЕТАЮЩЕЙ СЕНСОРНОЙ СЕТИ[1]

Басараб М.А.[2], Бельфер Р.А.[3], Соцкий В.В.[4]

Одним из направлений исследовательских работ в области летающих сенсорных сетей (ЛСС), включающих наземные всепроникающие сенсорные сети (WSN) и летающие Ad Hoc сети (FANET) является выбор архитектуры взаимодействия между этими сетями. Решение этой задачи определяется многими показателями, одним из которых является обеспечение защиты от атак DoS в собирающих сенсорных узлах. Реализация злоумышленником таких атак может привести к значительному ущерб, выраженному в потере или нелегитимном изменении информации сенсорных датчиков. Решение поставленной задачи основано на определении уровня риска безопасности собирающих сенсорных узлов. Анализ этих количественных значений позволяет принять наиболее эффективную схему взаимодействия сетей. Количественные значения этих уровней могут быть использованы для усиления защищенности некоторых сборных сенсорных узлов с повторным расчетом уровней безопасности указанных атак DoS. Безопасность сборных сенсорных узлов является не единственным критерием, определяющим структуру взаимодействия WSN и FANET. При решении этой задачи следует учитывать такие характеристики, как стоимость, технические возможности взаимодействия сетей и др.

Для решения поставленной задачи. 1. Приведена классификация методик количественной оценки уровня безопасности угроз сетей связи и выбран математического метод для поставленной задачи; 2. Приводится описание алгоритма методики на основе Fuzzy–AHP оценки уровня безопасности атак DoS для сборных сенсорных узлов летающих сенсорных сетей; 3. Приведен пример расчета по предложенной методике уровней риска безопасности атак DoS; 4. Проанализированы пути дальнейших мер по использованию полученных результатов расчета с целью продолжения работ по выбору схемы взаимодействия сенсорной сети с FANET.

***Ключевые слова**: беспроводная сенсорная сеть WSN, сборный узел, риск безопасности атаки DoS, метод нечетких множеств, метод анализа иерархий AHP, метод анализа пар SPA*

Введение.

В работах [1,2] рассматривается новое направление исследовательских работ в области беспроводных сенсорных сетей WSN (wireless sensor network) – летающие сенсорные сети (ЛСС). ЛСС является гетерогенной сетью, включающей, кроме WSN всепроникающие сенсорные сети и летающие Ad Hoc сети (FANET) с беспилотными летающими аппаратами БПЛА. В работе [3] исследованию подлежит одно из направлений обеспечения информационной безопасности ЛСС от воздействия атак DoS с потенциально высоким ущербом при их реализации. Таким уязвимым местом являются сборные сенсорные узлы в WSN. На иерархической трехуровневой схеме WSN проанализированы атаки DoS злоумышленника на сборные сенсорные узлы различных уровней и способы защиты. Настоящая работа посвящена разработке метода расчета количественной оценки этих атак. Эти значения предназначены для использования на этапе проектирования для принятия решения по выбору архитектуры ЛСС в части взаимодействия через шлюзы сборных сенсорных узлов сети WSN с беспилотными летающими аппаратами (БПЛА) в сети FANET.

Классификация методик количественной оценки уровня безопасности угроз сетей связи.

В работах [5,6] приведена классификация известных нам методик количественной оценки угроз безопасности сетей связи с целью определе-

1 Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта N15-07-09431а “Разработка принципов построения и методов самоорганизации для летающих сенсорных сетей”

2 Басараб Михаил Алексеевич, профессор, доктор физико-математических наук, МГТУ им. Н.Э. Баумана, Москва, bmic@mail.ru

3 Бельфер Рувим Абрамович, доцент, кандидат технических наук, МГТУ им. Н.Э. Баумана, Москва, a.belfer@yandex.ru

4 Соцкий Виталий Витальевич, МГТУ им. Н.Э. Баумана, Москва, wetal91@gmail.com

ния особенностей поставленной в работе задачи. Методики можно разделить по источнику разработки методики (созданные ETSI или разработанные специалистами), по функции сети, по однородности сети (гетерогенные и однородные), по этапу проектирования или эксплуатации сетей связи, по области использовании технологий сетей связи (для всех типов сетей связи, для конкретной сети или группы сетей), по применимости для различных типов угроз безопасности, по использованному для расчета математическому аппарату (умножение, метод нечетких множеств (fuzzy sets theory), метод анализа иерархий AHP (Analytic Hierarchy Process), метод анализа пар SPA (Set Pair Analysis)). Во всех этих методиках с помощью математических аппаратов производится расчет уровня безопасности угроз в сетях связи с использованием субъективных экспертных данных. Использование различных экспертных характеристик для этих расчетов не позволяет произвести сравнение методик по достоверности полученных количественных оценок уровней безопасности одних и тех же угроз.

Сформулируем в соответствии с приведенной классификацией поставленную в настоящей работе задачу - разработать методику оценки уровня безопасности атак DoS для сборных сенсорных узлов сети WSN, входящей в состав гетерогенной сети ЛСС. Эта методика рассматривается в качестве исследовательской работы в области летающих сенсорных сетей и предназначена для использования на этапе их проектирования.

В основу использования математического аппарата методики для поставленной задачи примем методику, разработанную без предоставления алгоритма в Пекинском университете связи [4], построенную на теории AHP, SPA и нечетких множеств и предназначенную для оценки уровня безопасности атак DoS в системе сигнализации SIP сети связи следующего поколения VoIP. Все приведенные выше методики предназначены для использования результатов расчета риска ИБ с целью определения угроз, безопасность которых имеет наиболее высокий уровень риска с последующим принятием мер по повышению защиты от этих угроз. Методика для гетерогенной сети Интернета вещей IoT [7] построена так же на теориях AHP, SPA и нечетких множествах. Указанная методика, в отличие от остальных, предназначена для расчета риска безопасности не каждой угрозы, а групп угроз, принадлежащих разным уровнях этой гетерогенной сети связи. Целью расчета в IoT является сравнение уязвимости ИБ к угрозам безопасности на различных уровнях этой гетерогенной сети связи. При этом алгоритм расчета приводится не в полном виде. Настоящая работа посвящена разработке методики для ЛСС на базе этих же теорий AHP, SPA и нечетких множеств с полным изложением алгоритма. Эта методика предназначена для расчета риска безопасности каждой атаки DoS с целью принятия решения по выбору архитектуры ЛСС в части взаимодействия через шлюзы сборных сенсорных узлов сети WSN с беспилотными летающими аппаратами БПЛА в сети FANET. Выбору одних теорий для расчета риска ИБ способствует для IoT и ЛСС такие общие положении, как гетерогенность сетей, сложность проблем обеспечения ИБ, большое число источников данных и их разнообразие, начальный этап проведения исследований в области безопасности [1,2,8]. Будем называть Fuzzy-AHP (как это принято во многих зарубежных работах [4,7 и др.]) теории AHP, SPA и нечетких множеств, на которых базируется подлежащая в настоящей работе методика для ЛСС.

Алгоритм методики оценки уровня безопасности атак DoS в сборные сенсорные узлы летающих сенсорных сетей основе Fuzzy-AHP.

В настоящем разделе приводится алгоритм предлагаемой методики оценки уровня безопасности атак DoS в сборные сенсорные узлы (ССУ) на примере упрощенной по сравнению с приведенной в работе [3] иерархической трехуровневой схемы WSN. Как видно из рисунка 1, эта упрощенная WSN состоит из одной базовой станции (БС), выполняющей на верхнем уровне функцию сборных сенсорных узлов, и двух ССУ транзитного уровня (ССУ1 и ССУ2). БС собирает информацию сенсорных датчиков с ССУ1 и ССУ2, а каждый из этих ССУ собирает информацию датчиков с двух головных кластеров [9].

Предлагаемый алгоритм методики вычисления уровня риска атак DoS включает четыре этапа.

Этап 1. Структуризация задачи в виде иерархической модели AHP с несколькими уровнями. На рис. 2 приведена иерархическая модель последствий атак DoS в сборные сенсорные узлы летающих сенсорных сетей.

На верхнем уровне приводится глобальная характеристика последствий атаки DoS на ССУ транзитного и верхнего уровней, на промежуточном – разделение последствий атак на ущерб базовой станции и ущерб сборного сенсорного узла транзитного уровня. Нижний уровень характеризует следующие потери: потери от реализации атаки DoS в ССУ1 транзитного уровня - C_1; потери от реализации атаки DoS в ССУ2 - C_2; потери от реализации атаки DoS в БС - C_3.

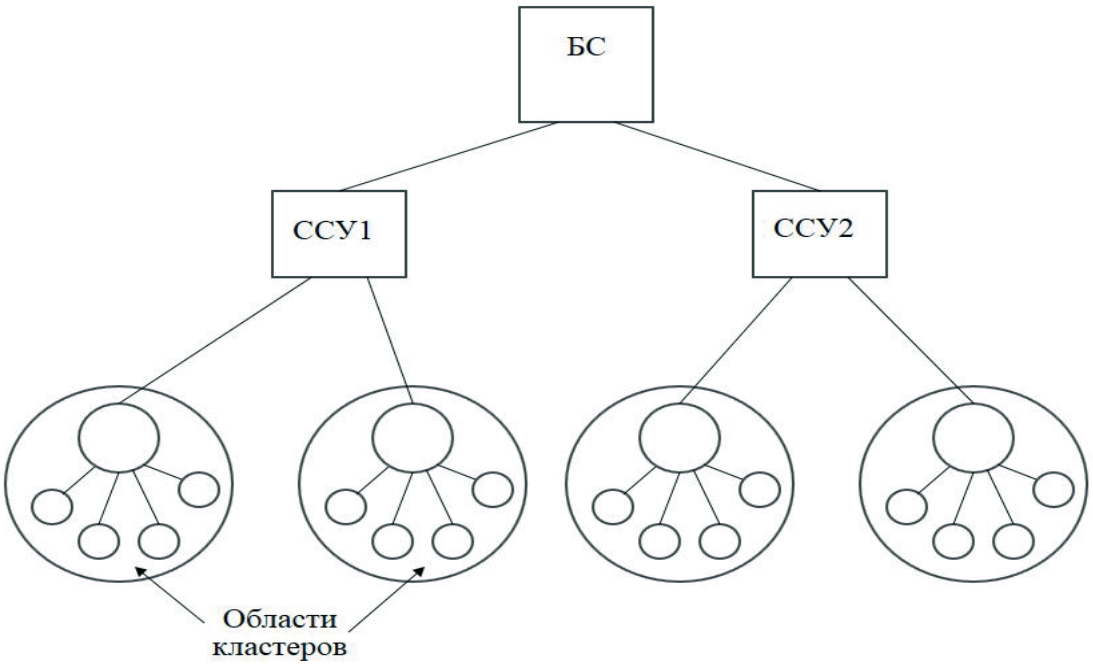

***Рис.1**. Схема иерархии уровней сборных узлов WSN*

Эти потери (или ущерб) зависят от конкретных приложений сенсорных датчиков. Например, в сенсорной сети «умный город» (smart city) такими приложениями могу быть: мониторинг шума, света, загрязнения окружающей среды, движения транспортных средств, противоугонная защита, экстренная медицинская услуга и др. [3]. Как отмечено в работе [4], более высокая достоверность ранжирования безопасности угроз достигается при одинаковой размерности ущерба. В данном примере сенсорной сети для многих из приведенных приложений последствия атак DoS могут быть выражены финансовыми потерями.

Этап 2. Составление матрицы парных сравнений характеристик атак DoS на основе нечетких экспертных оценок. Эксперты составляют нечеткую квадратную матрицу парных сравнений $\tilde{\mathbf{A}} = (\tilde{a}_{ij})_{3\times3}$ характеристик C_i потерь от реализации атак DoS на основании собственного опыта. В этой матрице экспертом указываются результаты попарного сравнения принятых характеристик C_i потерь. В предлагаемом алгоритме суждение эксперта в виде треугольного нечеткого числа формируется следующим образом. Эксперт оценивает значимость одной характеристики финансовых потерь по отношению к другой тройкой чисел (a_1, a_2, a_3), смысл которой состоит в том, что степень важности первой характеристики потерь по сравнению со второй находится в пределах от a_1 до a_3, но, вероятнее всего, она равна a_2.

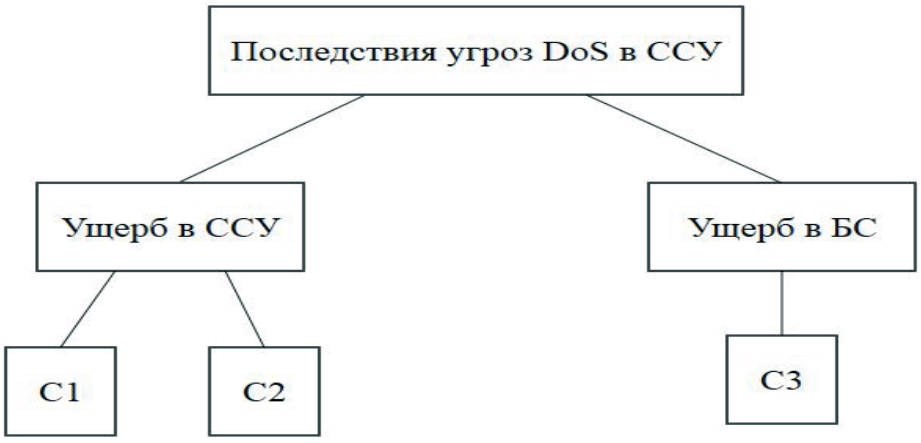

***Рис.2.** Иерархическая модель последствий атак DoS сборных сенсорных узлов*

Этап 3. Получение вектора нечетких весов из составленной матрицы. Введем понятие веса W – количественной информации об относительной важности (приоритете) каждой характеристики потерь от реализации атаки DoS C_i, представляемой в виде нечеткого весового вектора $\tilde{W} = \{\tilde{w}_{C1}, \tilde{w}_{C2}, \tilde{w}_{C3}\}$.

Для получения нечеткого весового вектора $\tilde{W} = \{\tilde{w}_{C1}, \tilde{w}_{C2}, \tilde{w}_{C3}\}$из матрицы парных сравнений $\tilde{\mathbf{A}} = (\tilde{a}_{ij})_{3\times3}$, где $\tilde{a}_{ij} = (l_{ij}, m_{ij}, u_{ij})$, эта нечеткая матрица раскладывается на три матрицы с четкими (точечными) значениями: $\mathbf{A_L} = (l_{ij})_{3\times3}$, $\mathbf{A_M} = (m_{ij})_{3\times3}$ и $\mathbf{A_U} = (u_{ij})_{3\times3}$.

Далее вычисляем весовой вектор каждой матрицы как среднее геометрическое значение по строкам $w_i' = \sqrt[n]{a_{i1} \cdot \ldots \cdot a_{in}}$, где n – порядок матрицы; i – номер строки матрицы, получая при этом вектор $W' = (w_1', \ldots, w_n')$. Затем элементы этого вектора нормируются и формируется весовой вектор $\tilde{W} = \{\tilde{w}_{C1}, \tilde{w}_{C2}, \tilde{w}_{C3}\}$, где $\tilde{w}_{Ci} = (w_{Ci_L}, w_{Ci_M}, w_{Ci_U})$, который для дальнейших расчетов необходимо дефаззифицировать.

В предлагаемом алгоритме дефаззификация проводится по методу биссектрисы (медианы) – медианного значения нечеткого числа, предложенному китайским математиком С.М. Ченом (S.M. Chen) для треугольных нечетких чисел [10, 12].

После дефаззификации нечеткого весового вектора $\tilde{W} = \{\tilde{w}_{C1}, \tilde{w}_{C2}, \tilde{w}_{C3}\}$ получаем вектор W $\{w_{C1}, w_{C2}, w_{C3}\}$, где w_{Ci} – дефаззифицированное значение элемента $\tilde{w}_{Ci}$, который будет использоваться в дальнейших расчетах.

Этап 4. Определение уровня атак DoS и их последующее ранжирование на основании полученных интервальных весов и результатов опроса экспертов с помощью нечетких комплексных решений и метода анализа пар SPA. Определяется лингвистическое множество слов $L = \{l_1, \ldots, l_s\}$, представляющее собой выбранный набор критериев оценки экспертами уровней потерь от реализации рассматриваемых атак DoS.Примем множество уровней потерь, состоящее из трех элементов: l_1, l_2, l_3, соответственно как «большие», «средние» и «незначительные» потери.

Запишем матрицу результатов опроса экспертов $\mathbf{E} = (e_{ij})_{3k\times3}$ размера $3k \times 3$, где k – количество рассматриваемых атак DoS, состоящую из элементов, представляющих собой экспертную оценку каждой характеристики ущерба от реализации каждой из рассматриваемых атак DoS по выбранным критериям оценки L.

В соответствии с методом анализа пар SPA составляются k (по количеству рассматриваемых атак DoS) матриц $\mathbf{B} = (\mu_{mn})_{3\times3}$ степеней связи каждой характеристики ущерба от реализации определенной атаки DoS. Элемент матрицы μ_{mn} есть анализируемая с помощью метода SPA степень связи элемента C_m с уровнем потерь l_n.

Далее по формуле $\mathbf{R} = W \bullet \mathbf{B} = (\mu_{Rmn})_{1\times3}$ с помощью нечеткой операции умножения "$\bullet$" вычисляются оценочные (учитывающие относительный вес каждой характеристики финансовых потерь) матрицы $\mathbf{R_k}$ для каждой из рассматриваемых атак DoS. В матрице $\mathbf{R}$ первый столбец соответствует уровню финансовых потерь «большие», второй – «средние», третий – «незначительные».

Затем для каждого элемента $\mu_{Rk_{mn}} = a_{Rk_{mn}} + b_{Rk_{mn}} i + c_{Rk_{mn}} j$ каждой матрицы Rk (т.е. для каждой из рассматриваемых атак DoS) вычисляется мощность связи shi (set pair power) по формуле $shi_{Rk_{mn}} = \frac{a_{Rk_{mn}}}{c_{Rk_{mn}}}$, и для каждой из рассматриваемых атак DoS выбирается максимальное значение $shi_{Rk_{MAX}}$. В зависимости от того, в каком из трех столбцов матрицы $\mathbf{R_k}$ содержится максимальное значение мощности связи $shi_{Rk_{MAX}}$, анализируемой атаке DoS присваивается соответствующий уровень риска безопасности.

Последний шаг алгоритма заключается в ранжировании рассматриваемых атак DoS на основании соответствующих им уровней риска безопасности и сравнения значений их максимальных мощностей связи в пределах своего уровня. Большему значению характеристики мощности связи shi соответствуют более высокий риск информационной безопасности (в пределах соответствующего уровня).

Пример использования методики ранжирования атак DoS. Приведем пример ранжирования по уровню риска ИБ трех конкретных атак DoS: Y_1, Y_2 и Y_3. в WSN системы сигнализации по SIP для действующей сети связи одного из операторов связи России на основании экспертных данных, полученных по результатам анализа защищенности соответственно ССУ1, ССУ2 и БС.

В соответствии с принятой иерархической моделью последствий атак DoS на основе метода усреднения значений оценок экспертов составляется нечеткая матрица парных сравнений $\tilde{\mathbf{A}} = (\tilde{a}_{ij})_{3\times3}$ характеристик потерь от реализации атак DoS:

$$\tilde{\mathbf{A}} = \begin{pmatrix} (1,1,1) & (\frac{1}{5},\frac{1}{4},\frac{1}{3}) & (\frac{1}{5},\frac{1}{3},1) \\ (3,4,5) & (1,1,1) & (2,3,4) \\ (1,3,5) & (\frac{1}{4},\frac{1}{3},\frac{1}{2}) & (1,1,1) \end{pmatrix}$$

Для получения нечеткого весового вектора $\tilde{W}$ разложим нечеткую матрицу парных сравнений $\tilde{\mathbf{A}}$ на три матрицы с четкими значениями: $\mathbf{A_L}$, $\mathbf{A_M}$ и $\mathbf{A_U}$:

$$\mathbf{A_L} = \begin{pmatrix} 1 & \frac{1}{5} & \frac{1}{5} \\ 3 & 1 & 2 \\ 1 & \frac{1}{4} & 1 \end{pmatrix}; \qquad \mathbf{A_M} = \begin{pmatrix} 1 & \frac{1}{4} & \frac{1}{3} \\ 4 & 1 & 3 \\ 3 & \frac{1}{3} & 1 \end{pmatrix};$$

$$\mathbf{A_U} = \begin{pmatrix} 1 & \frac{1}{3} & 1 \\ 5 & 1 & 4 \\ 5 & \frac{1}{2} & 1 \end{pmatrix}.$$

Вычислим весовой вектор каждой из этих матриц:

$$w'_{L1} = \sqrt[3]{1 \cdot \frac{1}{5} \cdot \frac{1}{5}} = 0,342 \ ;$$

$$w_{L1} = \frac{0,342}{0,342 + 1,81 + 0,63} = 0,12 \ ;$$

$$w'_{L2} = \sqrt[3]{3 \cdot 1 \cdot 2} = 1,81 \ ;$$

$$w_{L2} = \frac{1,81}{0,342 + 1,81 + 0,63} = 0,65 \ ;$$

$$w'_{L3} = \sqrt[3]{1 \cdot \frac{1}{4} \cdot 1} = 0,63 \ ;$$

$$w_{L1} = \frac{0,63}{0,342 + 1,81 + 0,63} = 0,23 \ ;$$

Весовой вектор матрицы

$$\mathbf{A_L}: W_L = (0.12, 0.65, 0.23);$$

$$w'_{M1} = 0,437 \ , \ w'_{M2} = 2,29 \ , \ w'_{M3} = 1 \ ;$$

$$w_{M1} = 0,13 \ , \ w_{M2} = 0,61, \ w_{M1} = 0,26.$$

Весовой вектор матрицы

$$\mathbf{A_M}: W_M = (0.13, 0.61, 0.26);$$

$$w'_{U1} = 0,69 \ , \ w'_{U2} = 2,71, \ w'_{U3} = 1,36;$$

$$w_{U1} = 0,14 \ , \ w_{U2} = 0,57, \ w_{U1} = 0,29.$$

Весовой вектор матрицы

$$\mathbf{A_U}: W_U = (0.14, 0.57, 0.29);$$

Из полученных значений весовых векторов W_L, W_M и W_U этих трех матриц соберем, в обратном порядке, нечеткий весовой вектор $\tilde{W}$:

$$\tilde{W} = \{(0.12, 0.13, 0.14), (0.57, 0.61, 0.65), (0.23, 0.26, 0.29)\}.$$

Проведем дефаззификацию нечеткого весового вектора $\tilde{W}$ по методу медианы:

$$W = \{0.13, 0.61, 0.26\}.$$

После этого десять экспертов производят оценку каждой характеристики ущерба от реализации каждой из рассматриваемых атак DoS по принятым критериям оценки L: «большие» (l_1), «средние» (l_2) и «незначительные» (l_3) потери (табл. 1).

***Табл. 1** - Результаты опроса экспертов*

Атаки DoS	Оценки	Потери от реализации атаки		
		C_1	C_2	C_3
Y_1	l_1	3	3	8
	l_2	6	5	1
	l_3	1	2	1
Y_2	l_1	5	2	5
	l_2	5	7	4
	l_3	0	1	1
Y_3	l_1	6	0	7
	l_2	3	1	3
	l_3	1	9	0

В соответствии с методом анализа пар SPA составим три матрицы степеней связи $\mathbf{B} = (\mu_{mn})_{3\times3}$ каждой характеристики потерь от реализации определенной атаки DoS. В матрице B первый столбец соответствует уровню потерь «большие», второй столбец – «средние» и третий – «незначительные»:

$$\mathbf{B}_1 = \begin{pmatrix} 0.3+0.6\mathrm{i}+0.1\mathrm{j} & 0.6+0.3\mathrm{i}+0.1\mathrm{j} & 0.1+0\mathrm{i}+0.9\mathrm{j} \\ 0.3+0.5\mathrm{i}+0.2\mathrm{j} & 0.5+0.3\mathrm{i}+0.2\mathrm{j} & 0.2+0\mathrm{i}+0.8\mathrm{j} \\ 0.8+0.1\mathrm{i}+0.1\mathrm{j} & 0.1+0.8\mathrm{i}+0.1\mathrm{j} & 0.1+0\mathrm{i}+0.9\mathrm{j} \end{pmatrix};$$

$$\mathbf{B}_2 = \begin{pmatrix} 0.5+0.5\mathrm{i}+0.0\mathrm{j} & 0.5+0.5\mathrm{i}+0.0\mathrm{j} & 0.0+0\mathrm{i}+1.0\mathrm{j} \\ 0.2+0.7\mathrm{i}+0.1\mathrm{j} & 0.7+0.2\mathrm{i}+0.1\mathrm{j} & 0.1+0\mathrm{i}+0.9\mathrm{j} \\ 0.5+0.4\mathrm{i}+0.1\mathrm{j} & 0.4+0.5\mathrm{i}+0.1\mathrm{j} & 0.1+0\mathrm{i}+0.9\mathrm{j} \end{pmatrix};$$

$$\mathbf{B}_3 = \begin{pmatrix} 0.6+0.3\mathrm{i}+0.1\mathrm{j} & 0.3+0.6\mathrm{i}+0.1\mathrm{j} & 0.1+0\mathrm{i}+0.9\mathrm{j} \\ 0.0+0.1\mathrm{i}+0.9\mathrm{j} & 0.1+0\mathrm{i}+0.9\mathrm{j} & 0.9+0\mathrm{i}+0.1\mathrm{j} \\ 0.7+0.3\mathrm{i}+0.0\mathrm{j} & 0.3+0.7\mathrm{i}+0.0\mathrm{j} & 0.0+0\mathrm{i}+1.0\mathrm{j} \end{pmatrix}.$$

Вычислим оценочные матрицы $\mathbf{A_{rk}}$ для каждой из рассматриваемых атак DoS по формуле $\mathbf{R} = W \bullet \mathbf{B} = (\mu_{\mathrm{Rmn}})_{1\times 3}$. В матрице $\mathbf{R}$ первый столбец соответствует уровню потерь «большие», второй – «средние» и третий – «незначительные».

$$\mathbf{R}_1 = (0,43+0,409\mathrm{i}+0,161\mathrm{j} \quad 0,409+0,43\mathrm{i}+0,161\mathrm{j} \quad 0,161+0\mathrm{i}+0,839);$$

$$\mathbf{R}_2 = (0,317+0,596\mathrm{i}+0,122\mathrm{j} \quad 0,596+0,317\mathrm{i}+0,122\mathrm{j} \quad 0,122+0\mathrm{i}+0,878);$$

$$\mathbf{R}_3 = (0,26+0,178\mathrm{i}+0,562\mathrm{j} \quad 0,178+0,26\mathrm{i}+0,562\mathrm{j} \quad 0,562+0\mathrm{i}+0,438).$$

Определим для каждого элемента каждой матрицы $\mathbf{R_k}$ мощность связи *shi* и выберем для каждой из рассматриваемых атак максимальное значение этой мощности:

$$shi_{\mathrm{Y1_{MAX}}} = \max(2,67 \quad 2,54 \quad 0,192) = 2,67;$$

$$shi_{\mathrm{Y2_{MAX}}} = \max(2,6 \quad 4,88 \quad 0,14) = 4,88;$$

$$shi_{\mathrm{Y3_{MAX}}} = \max(0,46 \quad 0,317 \quad 1,28) = 1,28.$$

Присвоим каждой анализируемой атаке DoS соответствующий уровень риска безопасности в зависимости от того, в каком из трех столбцов матрицы $\mathbf{R_k}$ содержится максимальное значение мощности связи. В результате имеем, что атака DoS Y_1 имеет высокий уровень риска информационной безопасности, Y_2 – средний, а угроза Y_3 – незначительный.

Таким образом, если ранжировать атаки DoS от более опасной к менее опасной, получим $Y_1 > Y_2 > Y_3$.

Этот пример показывает, что использование предложенного метода оценки риска безопасности атак DoS в сборные сенсорные сети дает возможность провести анализ с целью выбора архитектуры взаимодействия между наземными сенсорными сетями и FANET.

Выводы. В плане проведения исследовательских работ по определению архитектуры WSN, используемой в качестве составной части летающих сенсорных сетей, предложен метод оценки уровня риска безопасности атак DoS в сборные сенсорные узлы. Метод основан на теории Fuzzy-AHP и может быть использован при выборе архитектуры взаимодействия между наземными сенсорными сетями и FANET.

Рецензент: Матвеев Валерий Александрович, доктор технических наук, профессор, v.a.matveev@bmstu.ru

Литература:

1. Кучерявый А.Е. и др. Летающие сенсорные сети. //Электросвязь. – 2014. – № 9. – С. 2-5.
2. Кучерявый А.Е., Владыко А.Г., Киричек Р.В. Теоретические и практические направления исследований в области летающих сенсорных сетей. //Электросвязь. – 2015. – № 7. – С. 9-11.
3. Матвеев В.А., Бельфер Р.А., Глинская Е.В. Угрозы и методы защиты в сборных сенсорных узлах летающих сенсорных сетей. Вопросы кибербезопасности (настоящий выпуск). 2015. №5(13).
4. Yao Jiang, KangFeng Zheng. Evaluation Model for DoS Attack Effect in Softswitch Network // International Conference on Communications and Intelligence Information Security (ICCIIS). – 2010. – pp. 88-91.
5. Матвеев В.А., Морозов А.М., Бельфер Р.А. Оценка уровня риска угрозы безопасности фрода в сети VoIP по протоколу SIP // Электросвязь. – 2014. – №6 – С. 35–38
6. Матвеев В.А., Морозов, А.М., Бельфер Р.А. Методика ранжирования угроз фрода и DoS в системе SIP, основанная на методах анализа иерархий и анализа пар // Электросвязь. – 2013. – № 8. – С. 25–27.
7. Zhang, Baoquan; Zou, Zongfeng; Liu, Mingzheng, Evaluation on security system of internet of things based on Fuzzy-AHP method, E -Business and E -Government (ICEE), International Conference on6 2011, pp. 1-5.
8. Zhi-Kai Zhang (and others). IoT Security: Ongoing Challenges and Research Opportunities, Service-Oriented Computing and Applications (SOCA), 2014 IEEE 7th International Conference on, 2014, pp. 230 – 234.
9. Гольдштейн Б.С., Кучерявый А.Е. Сети связи пост-NGN, СПб.: БХВ-Петербург, 2013, 160 с.
10. Wang Juan-Ru, Yang Jin. Evaluation on the Independent Innovation Capability of Equipment Manufacturing Enterprises // International Conference on Management and Service Science. – 2009. – pp. 1-4.
11. S.M. Chen, Evaluating the Rate of Aggregative Risk in Software Development Using Fuzzy Set Theory // Cybernetics and Systems: International Journal. – 1999. – pp. 57-75.
12. Hamedi S. (and others). Inegrattng wireless sensor networks and mobile Ad Hoc networks for an enhanced end-user experience // Kaleidoscope Academic Conference. – 2010. – pp. 1–7.

THE CALCULATION OF THE SECURITY RISK OF DOS ATTACKS OF COLLECTING SENSOR NODES BASED ON FUZZY-AHP METHOD TO DETERMINE THE ARCHITECTURE OF INTERACTION BETWEEN SENSOR NETWORKS AND FANET IN FLYING SENSOR NETWORK

Basarab M.A.[5], Bel'fer R.A.[6], Sotskiy V.V.[7]

One of the directions of research in the field of flying sensor networks (FSN), including wireless sensor networks (WSN) and flying Ad Hoc Networks (FANET), is the choice of the architecture of interaction be–tween these networks. The solution to this problem depends on many parameters, one of which is to provide protection against DoS attacks in collecting sensory nodes. Implementation of such malicious attacks can cause significant damage, expressed in the loss or illegitimate change of information of sensors. The solution of this problem is based on determining the level of security risk of collecting sensor nodes. The analysis of these quantitative values allows taking the most effective scheme of interoperability. Quantitative values of these levels can be used to enhance the security of some collecting sensor nodes to re–calculate the level of safety of these attacks DoS. Security collecting sensor nodes are not the only criterion for determining the structure of the interaction between WSN and FANET. In solving this problem one should take into account such characteristics as cost, technical interoperability, and others.

To solve this problem:– the classification methodology for quantifying the level of security threats to networks and mathematical methods chosen for the task is given;– the algorithm methodology based on Fuzzy–AHP for assessing the safety of DoS attacks in the collecting sensor nodes flying sensor networks is described;– an example of the proposed method of calculating security risks levels for DoS attacks – is shown; further measures on the use of the results of calculation in order to continue work on the choice of the scheme of interaction with the sensor network FANET are presented.

***Keywords**: Wireless Sensor Network, sink node, security risk of DoS attack, fuzzy sets theory, Analytic Hierarchy Process, Set Pair Analysis*

References

1. Kucheryavyy A.E. i dr. Letayushchie sensornye seti. //Elektrosvyaz'. – 2014. – № 9. – S. 2-5.
2. Kucheryavyy A.E., Vladyko A.G., Kirichek R.V. Teoreticheskie i prakticheskie napravleniya issledovaniy v oblasti letayushchikh sensornykh setey. //Elektrosvyaz'. – 2015. – № 7. – S. 9-11.
3. Matveev V.A., Bel'fer R.A., Glinskaya E.V. Ugrozy i metody zashchity v sbornykh sensornykh uzlakh letayushchikh sensornykh setey. Voprosy kiberbezopasnosti (this issue).
4. Yao Jiang, KangFeng Zheng. Evaluation Model for DoS Attack Effect in Softswitch Network // International Conference on Communications and Intelligence Information Security (ICCIIS). – 2010. – pp. 88-91.
5. Matveev V.A., Morozov A.M., Bel'fer R.A. Otsenka urovnya riska ugrozy bezopasnosti froda v seti VoIP po protokolu SIP // Elektrosvyaz'. – 2014. – №6 – S. 35–38.
6. Matveev V.A., Morozov, A.M., Bel'fer R.A. Metodika ranzhirovaniya ugroz froda i DoS v sisteme SIP, osnovannaya na metodakh analiza ierarkhiy i analiza par // Elektrosvyaz'. – 2013. – № 8. – S. 25–27.
7. Zhang, Baoquan; Zou, Zongfeng; Liu, Mingzheng, Evaluation on security system of internet of things based on Fuzzy-AHP method, E -Business and E -Government (ICEE), International Conference on6 2011, pp. 1-5.
8. Zhi-Kai Zhang (and others). IoT Security: Ongoing Challenges and Research Opportunities, Service-Oriented Computing and Applications (SOCA), 2014 IEEE 7th International Conference on, 2014, pp. 230 - 234
9. Gol'dshteyn B.S., Kucheryavyy A.E. Seti svyazi post-NGN, SPb.: BKhV-Peterburg, 2013, 160 s.
10. Wang Juan-Ru, Yang Jin. Evaluation on the Independent Innovation Capability of Equipment Manufacturing Enterprises // International Conference on Management and Service Science. – 2009. – pp. 1-4.
11. S.M. Chen, Evaluating the Rate of Aggregative Risk in Software Development Using Fuzzy Set Theory // Cybernetics and Systems: International Journal. – 1999. – pp.
12. Hamedi S. (and others). Inegrattng wireless sensor networks and mobile Ad Hoc networks for an enhanced end-user experience // Kaleidoscope Academic Conference. – 2010. – pp. 1–7.

5 Mihail Basarab, Professor D.Sc. Bauman Moscow State Technical University, Moscow, bmic@mail.ru
6 Ruvim Belfer, Associated Professor, Ph.D., Bauman Moscow State Technical University, Moscow, a.belfer@yandex.ru
7 Vitaliy Sotsky, Bauman Moscow State Technical University, Moscow, wetal91@gmail.com