АНАЛИЗ И РАЗРАБОТКА СРЕДСТВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДЛЯ СИСТЕМ ГРУППОВОГО УПРАВЛЕНИЯ АВТОНОМНЫМИ МОБИЛЬНЫМИ РОБОТАМИ

Басан А. С.[1], Басан Е. С.[2] , Макаревич О.Б.[3]

Основной задачей данной статьи является анализ способов обеспечения безопасности для систем группового управления мобильными роботами (СГУР). А также разработка защищенных алгоритмов группового управления, позволяющих обеспечить безопасное выполнение некоторых этапов работы СГУР, связанных со стратегическим и тактическим этапами управления. Решение данной задачи подразумевает изучение особенностей систем группового управления и роботизированных систем с точки зрения безопасности. Основной проблемой связанной с разработкой системы обеспечения защиты для сети мобильных роботов, является отличие данного типа сети от привычных компьютерных сетей. Что требует разработки особых методов и подходов, которые должны учитывать следующие факторы: ограниченность вычислительных и энергетических ресурсов роботов. Предлагаемое решение для СГУР основывается на использовании концепции доверия, для определения подлинности узлов, дающих команду группе роботов, а также при определении целей. Предлагаемый набор алгоритмов учитывает несколько параметров при вычислении доверия, что позволяет расширить спектр атак злоумышленника, которым способно противодействовать система по сравнению с существующими решениями.[4]

***Ключевые слова**: системы группового управления, мобильные роботы, атаки, безопасность, протоколы, доверие, угрозы.*

DOI: 10.21681/2311-3456-2017-5-42-49

Введение

На сегодняшний день направление, связанное с робототехникой активно развивается. Основной упор делается на разработку протоколов, методов, алгоритмов группового управления роботами.

При этом роботизированные системы активно внедряются в промышленное производство, а также в военную отрасль. Высокий темп развития данных систем приведет к тому, что они будут использоваться и в повседневной жизни, уже сейчас компании Omron [1], SMP Robotics [2] активно разрабатывают программное и аппаратное обеспечения для создания роботов, а также осуществляют их продажу. Такое повсеместное применение и внедрение роботизированной техники рано или поздно приведет к вопросам безопасности ее использования, что особенно важно для стратегических объектов. В настоящее время, уже имеются работы посвященные разработке системы безопасности для роботов, но в них отсутствует комплексный подход к обеспечению защиты.

Роботизированная система или сеть роботов во многом отличается от привычных компьютерных сетей. В данной системе злоумышленник может воздействовать, как на процесс обмена сообщениями – то есть проводить сетевые атаки, так и на физическую безопасность роботов – то есть поводить кибер-атаки, а также оказывать воздействие непосредственно на систему управления роботами и на процесс взаимодействия робота с базовой станцией. Таким образом, актуальность обусловлена следующими факторами:

- На сегодняшний день направление, связанное с робототехникой активно развивается. Основной упор делается на разработку протоколов, методов, алгоритмов группового управления роботами. При этом роботизированные системы

1 Басан Александр Сергеевич, кандидат технических наук, доцент, Южный Федеральный Университет, г. Таганрог, Россия. E-mail: tftrtu@mail.ru

2 Басан Елена Сергеевна, кандидат технических наук, ассистент, Южный Федеральный Университет, г. Таганрог, Россия. E-mail: ele-barannik@yandex.ru

3 Макаревич Олег Борисович, доктор технических наук, профессор, Южный Федеральный Университет, г. Таганрог, Россия. E-mail: mak@tsure.ru

4 Работа выполнена при поддержке гранта Министерства образования и науки РФ №2.6244.2017/8.9 «Разработка метода обнаружения атак и вторжений, методики аутентификации узлов для масштабируемой беспроводной сенсорной сети»

активно внедряются в промышленное производство, а также в военную отрасль.

- Повсеместное применение и внедрение роботизированной техники рано или поздно приведет к вопросам безопасности ее использования, что особенно важно для стратегических объектов.
- Основной проблемой связанной с разработкой системы обеспечения защиты для сети мобильных роботов, является отличие данного типа сети от привычных компьютерных сетей. Что требует разработки особых методов и подходов, которые должны учитывать следующие факторы: ограниченность вычислительных и энергетических ресурсов роботов, что делает применение таких математических решений, как искусственный интеллект, для обнаружения злоумышленника, сложным и ресурсоемким.

1. Анализ работ посвященных обеспечению безопасности СГУР

На сегодняшний день мировая наука активно изучает проблемы обеспечения безопасности связанные с роботизированными системами. При этом существует некоторое разделение между данными системами. В статье [3] автор выделяет следующие типы роботизированных систем: мультиагентные роботизированные системы, мобильные сенсорные сети, мобильные Ad-Hoc сеть (MANETs), роботизированные системы с роевым интеллектом, а также можно выделить класс телеуправляемых роботов. Каждая из данных систем имеет собственные особенности с точки зрения построения системы безопасности, поэтому основная задача исследователей найти уникальный подход и учесть особенности каждой системы.

К примеру, коллективом авторов И.А. Зикратова, Т.В. Зикратова, И.С. Лебедева, А.В. Гуртов [4] рассматривается проблема построения механизмов защиты мультиагентных робототехнических систем от атак со стороны роботов-диверсантов. В данной работе рассмотрены механизмы «мягкой» безопасности или второй линии защиты. В своей работе авторы строят систему безопасности, опираясь на методы, используемые в мультиагентных компьютерных системах (МАС). Авторы говорят о том, что для защиты МАС от подобных скрытых атак могут использоваться метод Ксюдонга [5], «товарищеская» модель безопасности (Buddy Security Model, BSM) [6,7], которые хорошо согласуется с принципами построения децентрализованных систем. В своей работе [8] авторы описывают подход на основе репутации и доверия. В работе описаны два алгоритма для вычисления уровня доверия между узлами. Узлы формируют вектор оценки, и в результате формируется массив оценок членов коллектива. Данные оценки формируются на основании достоверности информации о расстоянии до цели. В итоге функция репутации узла описывается распределением Вейбулла–Гнеденко. Недостатком данного подхода является то, что доверие вычисляется в конкретный момент времени и при выполнении определенной задачи. Узлы анализируют только один параметр – расстояние до цели. Злоумышленник может проводить большое количество различных активных атак на сеть, которые не будут связаны с точностью и достоверностью передачи данных, при этом данная система не сможет распознать злоумышленника.

В работе [9] авторами разработан подход к оценке стабильности работы алгоритмов, основанных на модели доверия и репутации. При этом авторы используют следующие параметры для оценки: радиус взаимодействия, количество агентов, представляющих рой и процент диверсантов среди общего числа агентов. Фиксировались результаты, отражающие процент правильно выявленных легитимных агентов, агентов-диверсантов, а также среднее число агентов различного типа, попадающих в радиус взаимодействия. В результате проведения экспериментального исследования авторами получен положительный результат, доказано, что модель доверия способна противодействовать диверсантам вне зависимости от их количества. Основными недостатками данного подхода к оценке защищенности сети, является недостаточное количество параметров, используемых при проведении оценки. На основании представленных параметров можно определить только определенный тип злоумышленника. Модель поведения злоумышленника описана только для определенного типа нарушения информационной безопасности.

В статье [10] авторами разрабатывается подход на основе анализа поведения узлов. В данном подходе группа роботов при выполнении определенной задачи подчиняется набору правил. Далее роботы наблюдают за поведением друг друга и обмениваются данной информацией. Поведение роботов описывается с помощью формальной системы, разработанной авторами. В основе разработки системы обнаружения вторжений лежит следующий принцип: протокол, которых при определенных условиях поведения, позволяет отдельным роботам обнаруживать наличие отклонения от нормального поведения роботов, находящихся в их окружении и изменять свое

поведение, чтобы оградить других роботов от действий злоумышленника. При этом протокол имеет два основных компонента это: монитор, который устанавливается для отдельных роботов и позволяет им наблюдать за поведением соседей. Второй компонент это алгоритм, позволяющий посредством общения комбинировать «мнения» различных мониторов. Авторами проведен ряд экспериментов, по результатам, которых было выявлено, что для максимально точного обнаружения злоумышленника необходимо наличие шести роботов-мониторов, которые обмениваются между собой информацией.

Недостатком подхода является следующее: при обнаружении злоумышленника оценивается только показатель - поведение узла, который в основном определяется правильность перемещения узла по заданной траектории; таким образом, другие типы атак на роботов, не фиксируются системой; для точного обнаружения злоумышленника системе требуются специальные узлы-мониторы, которые отслеживают поведение соседей, при этом их количество должно быть не менее 6, что накладывает определенные ограничения на функционирование сети; авторами не проведен анализ, при котором количество злоумышленников в сети изменялось, нет данных относительно того, с каким количеством злоумышленников способна справится система.

В статье [11] авторами рассмотрена система обнаружения атак на основе использования дерева решений C 5.0 применительно к группе роботизированных автомобилей. Достоинством представленного подхода является то, что авторы рассматривают кибер-атаки. Для обнаружения данных атак авторы наряду с четырьмя признаками для анализа коммуникации и обработки информации, которые называются кибер-функциями ввода, используют четыре параметра для анализа физических свойств робота, которые авторы называют физическими характеристиками входного сигнала. Далее авторы проводят 5 типов деструктивного воздействия на робота и таким образом получают набор правил для построения дерева принятия решений. Недостатком подхода является то, что в данной работе рассмотрены атаки только на одного робота, а не на сеть роботов. При этом авторами рассмотрен ограниченный набор атак: атаки типа отказ в обслуживании и атак направленных на нарушение физических параметров. Кроме того, основным недостатком подобных систем является необходимость постоянного добавления правил для обнаружения новых атак.

Таким образом, можно отметить следующее:

– Тематика, связанная с обеспечением безопасности роботизированных систем активно рассматривается как за рубежом, так и в России. Авторами предлагаются различные подходы к обеспечению безопасности роботов.

– Недостатком существующих решений является недостаточное исследование в области возможных угроз и уязвимостей роботов, а также факторов и параметров, влияющих на проведение атак на роботизированную систему.

– Отсутствие комплексного подхода к обеспечению безопасности в сети мобильных роботов на сетевом, физическом уровнях и уровне управления.

При этом необходимо отметить, что данные подходы также не рассматривают особенности систем группового управления, не оценивают угрозы характерные конкретно для данных систем и алгоритмов. Данное исследование направлено на изучение угроз характерных для СГУР и определение способов защиты, которые позволят противодействовать влиянию со стороны злоумышленника.

2. Анализ безопасности СГУР

С точки зрения информационной безопасности наибольший интерес представляют угрозы воздействия на сетевой уровень и уровень управления мобильными робототехническими системами. Атаки, относящиеся к реализации данных угроз, связаны между собой. Для того чтобы осуществить перехват управления мобильным роботом, злоумышленнику необходимо проникнуть в сеть. Далее описываются некоторые угрозы, которые отсутствуют в Банке данных угроз ФСТЭК и характерны конкретно для СГУР и методов управления роботами.

1. Угроза перехвата процессом кластеризации СГУР. Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к информационной инфраструктуре за счёт получения права управления узлами, входящими в ее состав. Данная угроза обусловлена возможностью несанкционированного доступа к данной системе посредством перехвата информации, передающейся по беспроводному каналу. Реализация данной угрозы злоумышленником возможна при условии способности злоумышленника генерировать поддельные пакеты, которые содержат искаженные данные о физических возможностях злоумышленного узла, а также при наличии у злоумышленника более мощного (в отношении ресурсов: наличие более мощного приемо-передатчика сигналов, мощного заряда аккумулятора) устройства, чем предусмотрено в сети.

2. Угроза подмены данных об узле путем посылки ложных сообщений. Угроза заключается в том, что в некоторых системах группового управления узлы отправляют информацию не только о собственных данных, но и информацию о соседних узлах которые находятся в непосредственной близости от них. Злоумышленник может отправить поддельные данные о соседнем узле, чтобы скомпрометировать его. Кроме того, злоумышленник может перехватить подлинный узел сети, так как узлы могут располагаться вне контролируемой зоны и отравлять ложные сообщения о его состоянии. Третьим вариантом реализации атаки, является внедрение злоумышленником собственного узла в сеть и отправка ложных сообщений о самом себе, чтобы быть выбранным для выполнения цели и в дальнейшем нарушить процесс ее выполнения.

3. Угроза искажения информации о целях, передаваемой для составления общей матрицы целей. Узлы группы передают информацию об эффективности выполнения той или иной цели из списка заданных целей. Внедрившись в группу в качестве легитимного пользования, злоумышленник может посылать ложные данные об эффективности выполнения той или иной цели, чтобы в дальнейшем выбрать ее и не выполнить, нарушив работу системы. Злоумышленник может оказывать влияние на окружающую среду или сенсорную систему конкретных роботов, а также на саму цель, чтобы нарушить процесс выбора и распределения целей.

4. Угроза нарушения итерационного процесса выбора действий и целей узлами группы. В процессе выбора действий узлы выбирают действия из заданного списка необходимые им для выполнения задания, выбранные действия распространяется между всеми узлами группы. Злоумышленник может повлиять на увеличение времени выполнения итерационной процедуры выбора действия, путем выбора излишних действий, что приведёт к увеличению времени как этапа выбора действий, так и этапа выполнения действий, так как узлы будут выполнять все выбранные действия. Далее злоумышленник может воздействовать на процесс выбора целей, когда матрица целей сформирована узлы, согласно заданному алгоритму выбирают цели. Нарушить алгоритм злоумышленник может следующим образом: злоумышленник будет выбирать неэффективные для себя цели, злоумышленник попытается подделать номер узла и осуществить выбор цели вместо подлинного узла сети.

5. Угроза наличия недекларированных возможностей у роботов. Появление инсайдера в сети возможно из-за наличия недекларированных возможностей, заложенных в робота при его сборке/разработке. Из-за того что большинство роботов и комплектующих для роботов производятся иностранными разработчиками и зачастую не проходят сертификацию уполномоченными органами Российской Федерации. Имеется вероятность наличия недекларированных возможностей в роботах.

6. Угроза несанкционированного доступа к программно-аппаратному обеспечению роботизированных средств за счет их расположения вне контролируемой зоны. Как правило, роботы располагаются в незащищенных и неконтролируемых средах, при этом злоумышленник может достаточно легко перехватить любой узел в свое пользование. Как правило, программное обеспечение роботов строится на основе Linux- подобных ОС, причем количество существующих типов как самих микроконтроллеров или бортовых вычислителей, так и программного обеспечения для них является ограниченным. Злоумышленник, обладающий знаниями об особенностях устройства таких систем, сможет внедрить собственный код и изменить конфигурацию системы.

7. Угроза подмены узла, выполняющего роль лидера группы злоумышленным узлом. Если в системе не предусмотрен выбор доверенного или проверенного узла в качестве лидер группы, то злоумышленник, внедрившийся в сеть, может подделать передаваемые данные о своих возможностях, в частности расположение по отношению к цели, оставшийся запас энергии и будет выбран в качестве лидера группы.

3. Разработка защищенных алгоритмов для СГУР

Многие угрозы, представленные в разделе 2, связаны с воздействием злоумышленника на лидера группы, а также на процессы, протекающие на стратегическом уровне управления. Безусловно, для СГУР характерно на много большее количество угроз, но в данном исследовании мы остановимся на основных угрозах стратегического уровня. В данном исследовании представлен набор алгоритмов, который включает в себя методы вычисления доверия для реализации механизмов обеспечения безопасности. Предложенные методы на основе доверия способствуют не только установлению доверительных отношений между узлами группы, но и выявлению аномального поведения узлов группы. Кроме того, предложенный набор алгоритмов позволяет контролировать

процесс безопасного выбора главы группы.

3.1 Вычисление значения доверия

Ранее в работах авторов рассматривались вопросы, посвященные вычислению доверия [12]. Основным достоинством предлагаемого подхода является использование нескольких параметров для оценки доверия, что позволяет расширить спектр атак, которым способна противодействовать сеть. Авторами был предложен метод вычисления доверия, где использовались следующие показатели:

- соотношение количества отправленных/перенаправленных/принятых пакетов и отброшенных с учетом весовых коэффициентов, рассчитанных для каждого типа пакетов;
- загруженность узла – общее количество пакетов в единицу времени, прошедших через узел;
- остаточная энергия узла – текущий запас энергии узла на данный момент времени.

Выбор данных параметров основан на анализе возможных атак на беспроводную сеть [14]. При реализации активны атак воздействует на один из вышеперечисленных параметров, оценивая его изменение можно зафиксировать факт проведения атаки.

Для вычисления доверия использовался вероятностный подход. Для представления показателя отправленных/принятых/перенаправленных пакетов и отброшенных пакетов использовалось бета-распределение и показателям доверия служило математическое ожидание от бета – функции распределения, показатель ожидания того, каким будет поведение узла [13]. Итоговая формула для вычисления прямого доверия выглядит следующим образом:

$$T_{dir}[R_{A,B}] = \sum w_i \frac{s_{A,B}(\Delta t)+1}{s_{A,B}(\Delta t)+f_{A,B}(\Delta t)+2} * \gamma_i , \qquad (1)$$

где фактор наказания - γ, количество успешных s и неуспешных f событий, T – это есть доверие узла A относительно узла B.

Для представления показателей загруженность и остаточная энергия использовалось нормальное распределение. Происходит вычисление вероятности попадания текущего значения узла в доверительный интервал, затем данные вероятности комбинируется с помощью теоремы Байеса. Ниже представлены формулы для вычисления доверия по двум показателям: загруженность и остаточная энергии. Изменение данных показателей говорит о том, что узел проводит атаку, связанную с увеличением трафика в сети, а также атаки связанные с перенаправлением трафика на себя. Оценка параметров загруженность и остаточная энергия позволит выявить отклонения от доверительного интервала, который вычисляется на основе сбора информации от всех узлов группы. Формула 2 описывает вероятность попадания текущего значения остаточной энергии узла в доверительный интервал, формула 3 описывает вероятность попадания значения загруженности в доверительный интервал:

$$P_{Q(E)}(a_{\min} < Q(E)_i < a_{\max}) =$$

$$= \Phi\left(\frac{a_{\max} - \overline{Q(E)_в}}{\sigma_{Q(E)в}}\right) - \Phi\left(\frac{a_{\min} - \overline{Q(E)_в}}{\sigma_{Q(E)в}}\right), \qquad (2)$$

$$P_L(b_{\min} < L_i < b_{\max}) = \Phi\left(\frac{b_{\max} - \overline{L_в}}{\sigma_{L_в}}\right) - \Phi\left(\frac{b_{\min} - \overline{L_в}}{\sigma_{Lв}}\right), \quad , \qquad (3)$$

где Ф – функция Лапласа; $P_{Q(E)}$, P_L – вероятности попадания остаточной энергии узла и уровня загруженности узла в пределах доверительного интервала, среднеквадратическое отклонение, нижняя b_{min} и верхняя b_{max} границу доверенного для загруженности узла и остаточной энергии a_{min}, a_{max}, L - загруженность узла, $Q(E)$ - остаточная энергия.

Таким образом, в отличие от подхода, представленного [6], где в качестве показателя доверия используется только наличие неточностей в определении расстояния для цели. В данном случае используется комплексное решение, которое учитывает также и физические показатели узла сети, и поведение узла по отношению к другим узлам в целом.

3.2 Разработка алгоритмов группового управления с использованием доверия

Основной особенностью функционирования алгоритмов группового управления является выбор наилучшего лидера группы, для дальнейшего распределения целей между узлами группы и управления взаимоотношениями между членами группы. Поэтому с позиции злоумышленника целесообразно внедриться в сеть именно на данном этапе, который является стратегически важным. Для того чтобы сократить риск реализации угроз злоумышленником в данной работе предлагается использовать механизмы защиты, основанные на концепции доверия. Итак, одним из наиболее важных этапов, реализуемых на стратегическом уровне, является выбор лидера группы.

Разрабатываемый алгоритм выбора лидера группы (GL) состоит из двух этапов. Первый этап включает в себя предварительный выбор GL. На данном этапе управляющий узел (CN) выбирает из всех узлов сети наиболее подходящие узлы на

роль GL. Основным показателем при выборе является уровень доверия к узлу и уровень остаточной энергии. На втором этапе роботы выбирают, к какому временному GL они присоединятся. Временный GL, набравший большее количество голосов, становится действующим GL.

3.2.1 Алгоритм предварительного выбора лидера группы

1. CN высылает сообщение о начале выборов лидера группы ECH-Msg всем узлам (N_m), где $1 \le N \le m$, m – это максимальное количество узлов-роботов в данной системе. Данное сообщение несет информацию для узлов о том, что необходимо вычислить уровень стабильности S для соседних узлов. Стабильность узла выражается в том, что он имеет наивысшие показатели уровня остаточной энергии и доверия, и имеет наименьшую мобильность и загруженность.

$$S = \frac{Q(E) + T_{dir}}{M_Y + L}, \quad (4)$$

где M_Y – это мобильность узла сети.

2. Узлы-роботы N_m вычисляют прямое значение доверия T^{Ni}_{dir}, значение остаточной энергии $Q(E)_{Ni}$, значение загруженности L_{Ni}, стабильность S_{Ni}.

3. N_m отправляют данные значения CN.

4. CN вычисляет значение доверия T_{dir}, T_{cent} для каждого узла N_i, а также среднее S_{aver} и максимальное S_{max} значение стабильности для узлов.

5. CN проводит собственные наблюдения за узлами и проводит вычисление значений S_{GLi} и T^{GLi}_{dir}.

6. CN сравнивает равенство между вычисленными значениями и полученными от узлов $T^{Ni}_{dir} = T^{GLi}_{dir}$, $S_{Ni} = S_{GLi}$. Если между этими значениями для какого-либо узла имеются несоответствия, то узел исключается из процесса выбора претендента на лидера группы. И также исключается из процесса дальнейшего голосования, он вступит в дальнейшем в уже сформированную группу к ближайшему лидеру группы.

7. CN определяет претендентов на роль GL, которые должны удовлетворять условиям: $T_{dir} * T_{cent} \ge 0{,}8$; значение стабильности $S_{aver} \le S \le S_{max}$.

8. CN рассылает сообщения всем узлам N_m о том, какие узлы назначены потенциальными лидерами группы - *GL_temp*.

3.2.2 Алгоритм перевыборов GL

С выбором лидера группы связана еще одна проблема, это потеря доверия к текущему лидеру группы, либо нестабильная работа узла, выполняющего роль лидера группы. Особенностью системы группового управления роботами является то, что состояние узлов системы постоянно изменяется и в процессе работы системы необходимо учитывать то, что лидер группы перестанет соответствовать предъявляемым требованиям. Данную ситуацию необходимо вовремя отследить и скорректировать работу группы. Это позволяет сделать разработанный алгоритм перевыборов лидера группы (GL).

Алгоритм перевыборов GL:

1. CN рассылает запрос параметров $(Q(E)_{GLi}, T^{GLi}_{sum}, M^{GLi}_{Y}, d_{GLi})$ всем GL (GL_m).

2. Получив ответ от GL_m, CN проверяет совпадают ли полученные значения с теми, что CN вычислил самостоятельно. Если значения не совпадают, то GL_i исключается из дальнейшего процесса и становится простым узлом сети.

2. Проведя начальную проверку, CN проверяет выполнение условий:

(1) $T^{GLi}_{sum} \ge 0{,}5$;

(2) $Q(E)_{GLi} > (E\_intital)_{GLi} / 2)$,

(3) $M^{GLi}_{Y} < M^{GLi}_{max}$;

(4) $d_{GLi} \ne d_{GLmax}$.

3. Если не выполняется условие (1) для GLi, то CN блокирует работу GLi и самостоятельно проводит процедуру перевыборов GL, переход к пункту 5.

4. Если не выполняется любое условие кроме (1) для GLi, то CN инициирует процедуру выбора GL для данного узла, рассылая сообщения узлам Ni данного кластера.

5. Nm вычисляют значения $(Q(E)_{Ni}, T^{Ni}_{dir}, M^{Ni}_{Y})$ и отправляют их действующему GLi.

6. GLi вычисляет значение стабильности (S) значение доверия T_{dir} и T_{cent} для каждого узла группы N_m.

7. GLi выбирает узел Ni с наибольшим значением стабильности S_{max} и $T_{dir} * T_{cent} > 0.8$.

8. Если определены несколько конкурентов, то узлы с близкими значениями вычисляют значение d (расстояние до цели) и высылают его GLi.

9. GLi выбирает Ni в качестве временного GL - GL_temp, если его $di < dj$.

10. Если процедуру перевыборов проводила CN, то GL_temp оповещает соседние узлы о том, что он новый лидер группы GLi, иначе переход к пункту 11 алгоритма.

11. GL_temp рассылает свои данные $(Q(E)_{GLi}, T^{GLi}_{sum}, M^{GLi}_{Y}, d_{GLi})$ соседним GLi и CN.

12. GLi вычисляют прямое значение доверия T_{dir} для GL_temp_i и отправляют сообщение-подтверждение, если $Tdir > 0{,}5$.

13. GLi оповещает узлы группы N_m, соседние GL_m, CN о том, что он новый GL.

Процедура перевыборов GLi является достаточно уязвимой к атаке злоумышленника. Злоумышленный узел может попытаться предложить свою кандидатуру в качестве нового GLi. Данный алгоритм учитывает этот фактор, поэтому временный GL_temp_i проходит дополнительную проверку соседними GLi. После того как определена процедура выбора и перевыборов лидера группы, можно перейти к процедуре разбиения узлов на группы.

3.2.3 Группирование узлов

CN инициирует начало алгоритма группирования узлов. Суть алгоритма заключается в том, что каждый временный GL_temp_i вычисляет расстояние d_{GL_tempi} до цели и рассылает его вместе с предложением вступить в группу Msg-Inv всем соседним узлам-роботам. Узел Ni получает значения от GL_temp и определяет значение d_{Ni} до какого GL_temp_i меньше d_{min} $(d_i<d_{min})$ и отвечает ему. В свою очередь каждый потенциальный лидер группы сравнивает свое значение со значениями соседей (GL_temp_j) и если его значение наименьшее, то он провозглашает себя лидером группы (GLi) и оповещает об этом всех соседей и CN, а роботы, которым он оправил значение d_{GLi}, могут к нему присоединиться. Иначе, GL_temp_i присоединится к GL_temp_j, значение di, которого больше, и оповестит об этом Ni, которым он отправлял Msg-Inv. Блок-схема алгоритма представлена в статье [14]. Особенностью алгоритма является то, что GLi может быть выбран только тот узел, который прошел проверку CN, что повышает защищенность данного алгоритма.

4. Заключение

Представленный в данной статье набор алгоритмов направлен на обеспечение безопасности СГУР с использованием концепции доверия. Представлен метод вычисления доверия с использованием параметров остаточная энергия, загруженность и соотношение отправленных/ перенаправленных/ принятых и отброшенных пакетов. Анализ данных параметров позволяет оценить изменение поведения узла. К примеру, при реализации атаки отказ в обслуживании и или атаки Сибиллы [12] у атакующего узла изменяется показатель загруженности, это связано с тем, что злоумышленник либо генерирует большое количество трафика, либо перенаправляет его на себя. Кроме того, существует ряд атак на исчерпание ресурсов узлов сети, так как запас энергии является критически важным параметром, контролируя его изменение можно зафиксировать такие атаки. При возникновении отброшенных пакетов, превышающих норму, можно сделать вывод, что злоумышленник проводит такие атаки как «Черная дыра», «Серая дыра», которые направлены на то чтобы «отрезать» узел или группу узлов от других роботов группы. Таким образом, использование данных показателей доверия позволяет ликвидировать большинство угроз, которые свойственно СГУР.

В основном, предложенные варианты обеспечения безопасности направлены на защиту от активного воздействия злоумышленника и не всегда смогут защитить от искажения информации и таких атак, как человек посередине. Данный методы сработают только в том случае, если злоумышленник будет совершать непредвиденные в системе действия, которые нарушают работу системы. В дальнейших исследованиях предполагается изучения проблематики подмены сообщений и данных, а также тех типов атак, которые связаны с вмешательством злоумышленника в работу системы и блокированием злоумышленных узлов.

***Рецензент**: Дворянкин Сергей Владимирович, доктор технических наук, профессор кафедры информационной безопасности Финансового университета при Правительстве Российской Федерации, Москва, Россия. E-mail: SVDvoryankin@fa.ru*

Литература

1. Omron manufacturer site. Access mode -http: //www.mobilerobots.com/Mobile_Robots.aspx - free.
2. The site of the manufacturer SMP Robotics. Access mode - http://smprobotics.com/ - free.
3. Fiona Higgins, Allan Tomlinson and Keith M. Martin. Threats to the Swarm: Security Considerations for Swarm Robotics. International Journal on Advances in Security, vol 2 no 2&3, year 2009.
4. I.A. Zikratov, T.B. Zikratova, I.S. Lebedev, A.V. Gurtov. Building a model of trust and reputation for the objects of multi-agent robotic systems with decentralized control. Scientific and Technical Journal of Information Technologies, Mechanics and Optics Scientific and Technical Journal of Information Technologies, Mechanics and Optics 2014, No. 3 (91), pp. 30-38.
5. Xudong G., Yiling Ya., Yinyuan Y. POM-a mobile agent security model against malicious hosts // Proceedings of the 4th International Conference on High Performance Computing in the Asia-Pacific Region. 2000. V. 2. P. 1165–1166.
6. Karnik N.M., Tripathi A.R. Security in the Ajanta mobile agent system // Software - Practice and Experience. 2001. V. 31. N 4. P. 301–329.
7. Sander T., Tschudin Ch.F. Protecting mobile agents against malicious hosts // In Giovanni Vigna (ed.) Mobile Agents and Security, LNCS, Springer, 1998. P. 44–60.
8. Renjian Feng , Xiaofeng Xu, Xiang Zhou and Jiangwen Wan. Trust Evaluation Algorithm for Wireless Sensor Networks Based on Node Behaviors and D-S Evidence Theory. Sensors 2011, 11, pp. 1345-1360; doi:10.3390/s110201345.
9. Ilya I. Viksnin, Radda A. Iureva, Igor I. Komarov, Anastasia L. Drannik. Assessment of Stability of Algorithms Based on Trust and Reputation Model. Proceeding of the 18th conference of FRUCT association .pp.364-369.

10. A. Fagiolini G. Dini A. Bicchi . Distributed Intrusion Detection for the Security of Industrial Cooperative Robotic Systems Preprints of the 19th World Congress The International Federation of Automatic Control Cape Town, South Africa. August 24-29, 2014.
11. Tuan Phan Vuong, George Loukas, Diane Gan, Anatolij Bezemskij: Decision tree-based detection of denial of service and command injection attacks on robotic vehicles. WIFS 2015: 1-6.
12. E.S. Abramov, E.S. Basan, O.B. Makarevich. Trust management system for mobile cluster-based wireless sensor network. Proceedings of the 8th International Conference on Security of Information and Networks. P. 203-209.2015.
13. E.S. Abramov, A.S. Basan, E.S. Basan. Development of of the trust management system for mobile wireless sensor network. Izvestiya SFedU. Engineering Sciences. No 7(168). P. 42-52. 2015.
14. Alexander Basan, Elena Basan, Oleg Makarevich. Methodology of Countering Attacks for Wireless Sensor Networks Based on Trust. 2016 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery Publication Year: 2016, Page(s):409 – 412.

ANALISYS OF WAYS TO SECURE GROUP CONTROL FOR AUTONOMUS MOBILE ROBOTS

Basan A.[5], Basan E.[6], Makarevich O.[7]

The aim of this paper is to analyze the ways of providing security for mobile robots groups control (MRGC) and to develop a security protocol for MRGC under limited computational and power resources away from the controlled area. The solution for this problem assumes features of group control systems and robot systems from the security point of view. The main problem connected with the development of a security system for mobile robots is the distinction of this type of the network from other networks. This demands the development of special methods and approaches that should take many specific factors such as limitations of computational resources and power into account. The proposed solution for MRGC is based on the use of trust concept for finding the validity of nodes and finding targets. In contrast to the existing approaches, this protocol uses several parameters to evaluate the trust that allows to expand the range of repelled attacks..

Keywords*. Group Control, security, trust, vulnerabilities, intrusion, attacks, security, trust, protocols*

References

1. Omron manufacturer site. Access mode -http: //www.mobilerobots.com/Mobile_Robots.aspx - free.
2. The site of the manufacturer SMP Robotics. Access mode - http://smprobotics.com/ - free.
3. Fiona Higgins, Allan Tomlinson and Keith M. Martin. Threats to the Swarm: Security Considerations for Swarm Robotics. International Journal on Advances in Security, vol 2 no 2&3, year 2009.
4. I.A. Zikratov, T.B. Zikratova, I.S. Lebedev, A.V. Gurtov. Building a model of trust and reputation for the objects of multi-agent robotic systems with decentralized control. Scientific and Technical Journal of Information Technologies, Mechanics and Optics Scientific and Technical Journal of Information Technologies, Mechanics and Optics 2014, No. 3 (91), pp. 30-38.
5. Xudong G., Yiling Ya., Yinyuan Y. POM-a mobile agent security model against malicious hosts // Proceedings of the 4th International Conference on High Performance Computing in the Asia-Pacific Region. 2000. V. 2. P. 1165–1166.
6. Sander T., Tschudin Ch.F. Protecting mobile agents against malicious hosts // In Giovanni Vigna (ed.) Mobile Agents and Security, LNCS, Springer, 1998. P. 44–60.
7. Renjian Feng , Xiaofeng Xu, Xiang Zhou and Jiangwen Wan. Trust Evaluation Algorithm for Wireless Sensor Networks Based on Node Behaviors and D-S Evidence Theory. Sensors 2011, 11, pp. 1345-1360; doi:10.3390/s110201345.
8. Ilya I. Viksnin, Radda A. Iureva, Igor I. Komarov, Anastasia L. Drannik. Assessment of Stability of Algorithms Based on Trust and Reputation Model. Proceeding of the 18th conference of FRUCT association .pp.364-369.
9. A. Fagiolini G. Dini A. Bicchi . Distributed Intrusion Detection for the Security of Industrial Cooperative Robotic Systems Preprints of the 19th World Congress The International Federation of Automatic Control Cape Town, South Africa. August 24-29, 2014.
10. Tuan Phan Vuong, George Loukas, Diane Gan, Anatolij Bezemskij: Decision tree-based detection of denial of service and command injection attacks on robotic vehicles. WIFS 2015: 1-6.
11. A.S. Basan, E.S. Basan, O.B. Makarevich Analysis of security problems in mobile autonomous robotechnical systems. Perspective systems and management tasks: materials of the Twelfth All-Russian Scientific and Practical Conference and the Eighth Youth School-Seminar «Information Management and Processing in Technical Systems» / Southern Federal University. 2017. pp. 75-85
12. E.S. Abramov, E.S. Basan, O.B. Makarevich. Trust management system for mobile cluster-based wireless sensor network. Proceedings of the 8th International Conference on Security of Information and Networks. P. 203-209.2015.
13. E.S. Abramov, A.S. Basan, E.S. Basan. Development of OF the trust management system for mobile wireless sensor network. Izvestiya SFedU. Engineering Sciences. No 7(168). P. 42-52. 2015.
14. Alexander Basan, Elena Basan,Oleg Makarevich. Methodology of Countering Attacks for Wireless Sensor Networks Based on Trust. 2016 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery Publication Year: 2016, Page(s):409 – 412.

5 Alexander Basan, Southern Federal University, Taganrog, Russia. E-mail: tftrtu@mail.ru
6 Elena Basan, Southern Federal University, Taganrog, Russia, E-mail: ele-barannik@yandex.ru
7 Oleg Makarevich, Southern Federal University, Taganrog, Russia, E-mail: mak@tsure.ru