УДК 623.4.01

© *В. В. Коваленко*[1], *В. Ю. Корчак*[2], *А. И. Хилько*[3], *В. Л. Чулков*[2]
[1]Научный совет по комплексной проблеме «Гидрофизика» РАН, Москва
[2]Секция прикладных проблем при Президиуме РАН, Москва
[3]Институт прикладной физики РАН, Н. Новгород
hydrophys@mail.ru

ВОПРОСЫ ПРОТИВОДЕЙСТВИЯ СЕТЕВЫМ СИСТЕМАМ ПОДВОДНОГО НАБЛЮДЕНИЯ И ОБЕСПЕЧЕНИЯ ИХ БЕЗОПАСНОСТИ

Статья посвящена важной проблеме подводного наблюдения, в связи с которой констатируется устойчивое развитие и эффективность распределенных сетевых сенсорных систем. Формулируются задачи противодействия таким системам и обеспечения их безопасности. Описываются различные виды атак на сетевые сенсорные системы с акустической подводной связью, а также способы защиты от них. Подчеркиваются специфические особенности подводных сетей, отличающие их от беспроводных наземных сетей. Делается вывод о необходимости создания средств борьбы с подводными сетями как целостными образованиями, использующими акустическую связь. Другой вывод сводится к необходимости создания средств их защиты на основе отмеченных в статье приемов.

Ключевые слова: системы подводного наблюдения, сенсорные сети, распределенные сетевые системы, противодействие сенсорным сетям и их безопасность.

V. V. Kovalenko[1], *V. Yu. Korchak*[2], *A. I. Khil'ko*[3], *V. L. Chulkov*[2]
[1]Hydrophysical Scientific Council RAS, Moscow, Russia
[2]Defense Problem Section RAS, Moscow, Russia
[3]Institute of Applied Physics of RAS, Nizhny Novgorod, Russia

COUNTERMEASURES AND SECURITY FOR UNDERWATER SENSOR NETWORK SYSTEMS

The paper describes the important problem of underwater surveillance which causes the stable development of distributed sensor network systems and their efficiency. Countermeasures objectives for underwater sensor network systems and their safety providing are considered. Different types of attack against underwater acoustic sensor and communication networks as well as security aspects are discussed. The unique characteristics of the underwater networks which differ from wireless ground-based networks are specified. The necessity of fight methods creation regarding underwater networks as entire formations that use acoustic communication is stated in the conclusion. Another statement is the necessity of finding security measures for such systems due to the methods given in the paper.

Key words: underwater surveillance systems, sensor networks, distributed surveillance systems, network countermeasures, security of sensor networks.

Причины появления сетевых систем подводного наблюдения (ССПН), принципы и технологии создания, требования к ним и предложения по их рациональному облику изложены в работах [1—3]. Беспроводная сенсорная сеть — пространственно-распределенная совокупность автономных сенсоров, предназначенная для мониторинга полей и объектов в природных средах и для прохождения по сети данных мониторинга к пунктам назначения [4].

Из работ [1—3] следует, что ССПН способны быть устойчивыми и эффективно решать поставленные задачи. Очевидно, что развитие ССПН формирует угрозу тем объектам, наблюдение за которыми они призваны осуществлять. В связи с этим нейтрализация такой угрозы является актуальной задачей. По существу, речь идет о противодействии новому, специфическому виду систем, которые имеют пространственное распределение своих элементов и содержат как позиционные, так и мобильные составляющие. Возникает также задача защиты ССПН от возможного противодействия им. Обе задачи объединяются в общее понятие борьбы систем. Как правило, акустическая связь является средством, с помощью которого элементы ССПН объединяются в целостные структуры, поэтому такая борьба получила название «акустической войны». Попытку свести борьбу

с сетевыми системами к борьбе с отдельными их элементами, например, с необитаемыми аппаратами [5] нельзя признать удачной. Нельзя признать и то, что существующие средства гидроакустического противодействия способны к эффективной нейтрализации сетевых систем. Нужны постановки новых задач.

Последующие представления о противоборстве сетевых систем требуют изложения дополнительной информации по отношению к [1—3]. Общее представление о принципиально важных характеристиках сенсорных сетей включает их архитектуры, протоколы и позиционирование. Выделим протоколы, делающие сетевую систему целостным образованием. **Протоколы** — это стандарты связи и наборы правил, в соответствии с которыми взаимодействуют друг с другом источники и получатели данных. Они же определяют размеры пакетов данных, идентификацию корреспондирующих элементов, сжатие, проверку на наличие ошибок и передачу данных. Из характерных элементов связи выделим физические: трансиверы (излучатели и приемники), модемы, а также организацию функциональных слоев. Сенсорная часть системы состоит из аппаратной и программной частей физических сенсоров (акустических и неакустических).

Объектами атаки на акустические сенсорные сети могут быть собственно сенсоры, позиционные, дрейфующие и размещаемые на необитаемых аппаратах, а также сетевая связь. Физическая ликвидация сенсорных станций может входить в число мер по противодействию, но лишь как составная часть общих усилий. Чтобы ликвидировать элементы сетевых структур их надо обнаружить, а это сложная задача. К тому же особенностью сетевых структур является сохранение их работоспособности при утрате отдельных элементов. Задача атакующей стороны — лишить работоспособности сеть как целостную структуру или ту ее часть, которая представляет угрозу.

Отметим имеющееся в мире стремление к унификации и модульности физических элементов, с тем чтобы сделать их недорогими, пригодными для массового производства и применения, а также оптимизированными под решаемую задачу и условия среды. Это стремление распространяется на платформы-носители сенсоров, сами сенсоры и связное оборудование. Существуют указания на то, что ССПН изначально должны создаваться в расчете на условия «акустической войны» путем организации их защиты от атак [6].

Одно из схематических представлений сенсорных сетей приведено на рис. 1. Показано устройство получения информации, частным случаем которого может быть центральный элемент групп сенсоров или шлюз (промежуточные получатели), или конечный получатель (расположенный обычно на управляющей платформе). Этот рисунок иллюстрирует основные качества сенсорной сети. Кроме получателей информации сеть имеет ряд позиционных сенсоров, в том числе тех, которые служат ретрансляторами. Такая сеть позволяет прохождение данных по различным путям с множеством транзитных участков. Сеть также содержит мобильные элементы. Пример приборов, формирующих подобную сенсорную сеть, представлен на рис. 2.

Каждое устройство, входящее в сенсорную сеть, имеет акустические или комбинированные (акустика-радио) модемы. В связи с возрастающей ролью мобильных элементов сенсорных сетей (аппаратов) опишем типовой алгоритм функционирования таких сетевых структур.

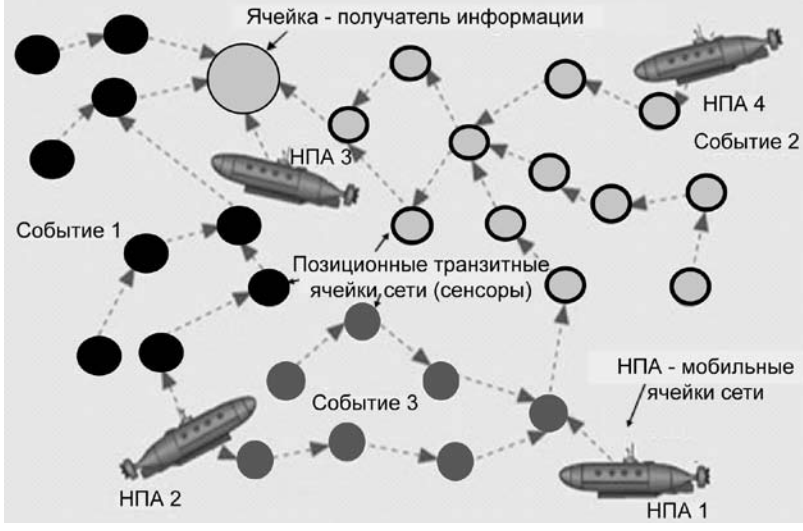

Рис. 1. Схематическое представление подводной сенсорной сети.

Рис. 2. Пример совокупности приборов, формирующих сенсорную сеть.
а — шлюз; *б* — мобильные ячейки; *в* — позиционная ячейка. Все автономные элементы имеют термисторные цепочки и средства защиты данных.

Каждый сенсор осуществляет операции по подводному наблюдению. Операции сводятся к сбору данных и их встроенной обработке. Обработка ориентирована на автоматическое обнаружение, распознавание и оценку параметров объектов. Данные от сенсоров передаются промежуточным получателям (например, шлюзам). От промежуточных получателей данные от сети поступают конечному получателю, где подвергаются совместной обработке и принятию решений. После решения по сети передаются команды управления, в том числе на реконфигурацию сети путем изменения положения мобильных элементов и на перехват ими цели. Далее цикл повторяется. Рис. 1 иллюстрирует также тот важный факт, что сенсорная сеть приводится в действие внешними событиями типа обнаружения объекта, точнее, данными, связанными с этими событиями. Уязвимой частью описанной системы является сетевая связь. Пример стека протоколов приведен на рис. 3 (фрагмент слева — из работы [7], справа — детальная и укрупненная структура стека). Охарактеризуем процесс обмена данными и протоколы слоев ССПН, поскольку наиболее эффективное противодействие системе связано с воздействием на особенности, соответствующие этим протоколам. Взаимодействуют соседние уровни по вертикали. В процессе передачи данные у отправителя переходят с верхнего уровня на нижний. При этом осуществляются: разбиение данных на пакеты-сообщения и их обрамление служебной информацией. В точках приема с помощью служебной информации происходит обратный процесс.

Физический уровень — это уровень аппаратных элементов (модемов), основными функциями которого являются создание или прием сообщения. Здесь осуществляется определение полос, пропускной способности и используются различные схемы модуляции. Учтены свойства канала, техника обработки, помехоустойчивости, синхронизации и криптографирования.

	Детальная структура слоев	Укрупненная структура слоев
Sensor or Vehicle Control System (APP)	Прикладной уровень. Управление с платформы или сенсора	Прикладной уровень
Presentation Layer (CCL)	Презентационный уровень. Язык управления заданиями	Транспортный уровень
Network/Routing (NET)	Сетевой уровень	Сетевой уровень
Medium Access Control (MAC)	Подуровень управления доступом	Связной уровень
Modem Interface & Driver (API)	Интерфейс и драйвер модемов	
Modem Hardware (PHY)	Физический уровень. Аппаратная часть модемов	Физический уровень

Рис. 3. Уровневая архитектура сетей. Стек протоколов ССПН PLUSNet [7].

Связной уровень управляет доступом к соседним ячейкам и динамическое управление дальностью связи. Осуществляется кодирование с целью корректирования ошибок, регулировка активного и ждущего состояния, определение размеров пакетов. Осуществляется управление энергетикой узлов сети и контроль исправности.

Сетевой уровень содержит маршрутизаторы. С их помощью выбираются траектории и учитываются возможности прохождения данных на транзитных участках. Определяется приоритетность различных путей с учетом имеющихся ограничений на полосу и принятых критериев. Часто используется критерий минимума затрат ресурсов. В связи с этим существует понятие энергетически эффективной маршрутизации. Маршрутизатор периодически проверяет, функционируют ли соседние ячейки, и в зависимости от этого меняет направления передачи. Таким образом, осуществляется самоорганизация, в том числе при потере работоспособности отдельных ячеек.

Транспортный уровень ответственен за обеспечение прохождения информации от источника к получателю. Для подводных акустических сетей решается проблема больших временных задержек. Сетевой уровень не гарантирует доставки пакетов в нужном порядке, так что транспортному уровню нужно осуществлять сборку сообщений.

Прикладной уровень обеспечивает решение конечных задач. Для этого он обеспечивает необходимую реконфигурацию сети, проверку на подлинность ее ячеек, осуществляет их синхронизацию. Здесь осуществляется управление кластерами сети и сетью в целом.

Стремление к лишению сенсорных сетей работоспособности достигается различными мерами (атаками). Атаки осуществляются в расчете на уязвимые особенности сетей. В качестве наиболее опасных выделяются те из них, которые преследуют цель вывести из строя всю сеть или большую ее часть. Поэтому наиболее опасными являются атаки на сетевую связь, объединяющую сенсоры и получатели информации, а не на отдельные физические элементы. Атаки условно делятся на пассивные и активные. Пассивные атаки — это разведка нахождения чужих сетей, оценка использующихся ими сигналов и режимов. Такая атака-разведка может осуществляться развертываемыми средствами типа тех, которые показаны на рис. 2. Последние, вследствие возможности контроля района, особенно привлекательны. Надежд на обнаружение физических элементов чужих сетей немного. Но провоцирование чужой сети и перехват сигналов связи является реальным.

Основой противодействия являются активные атаки. Их цель — выведение из состояния работоспособности сенсорной сети фрагментарно или целиком. Для осуществления активной атаки нужно знать с точностью до района расположение сети противника и примерные ее характеристики. Физическим средством борьбы с сетями являются **посторонние ячейки**, позиционные и мобильные. Они внедряются в предполагаемый район нахождения атакуемой сенсорной сети и имеют сходные с ее элементами свойства. Их работа направлена на разрушение сообщений внутри атакуемой сети и дезорганизацию ее работы. Посторонние ячейки представляют собой тоже сети, предназначенные для борьбы с сетями противника, и в этом смысле они соответствуют рекомендациям в работе [6]. В литературе описан ряд атак. Можно найти исследование эффективности ряда из них, особенно тех, которые признаются наиболее опасными, в частности атак типа «отказ в обслуживании» [8]. Отметим, что атакам подвергаются, в основном, физический, связной, сетевой и транспортные слои. К видам противодействия относятся: 1) подавление помехами; 2) образование ложных каналов связи типа «червоточина»; 3) образование ложных получателей информации; 4) образование потока ложных предложений к соединению; 5) образование потока ложных соединений; 6) избирательно ложная переадресация; 7) образование множеств ложных источников информации. На рис. 4, *а* схематически представлена **атака типа подавления сети помехами**.

Воздействие помехами в общем случае должно быть распределенным. Важно, чтобы генераторы помех осуществляли свою работу достаточно долговременно в расчете на необходимый период блокирования сети. Рабочие частоты и полосы помех должны соответствовать тем, на которых осуществляется связь. При известном положении ячеек этот вид атаки может быть усилен тем, что, заняв положение между ячейками и внеся искажения в сигнал, источник помехи может повторять атаки уже как источник искаженных данных, замещающий полезные данные. Режимы работы генераторов помехи могут быть различными во времени и выбираются исходя из нескольких критериев, в том числе экономичности. Общим защитным приемом является применение сигналов с увеличенной сложностью. Применение сигналов с частотной манипуляцией оказалось привлекательным по причине их повышенной устойчивости к помехам и многолучевой интерференции. Но атакующая сторона может «испортить» и широкополосный сигнал или даже воздействовать на последовательность частотной манипуляции. Автономные сети при атаке помехами должны сохранять энергетику. В процессе непрерывной и/или продолжительной атаки сеть (или ее часть) должна

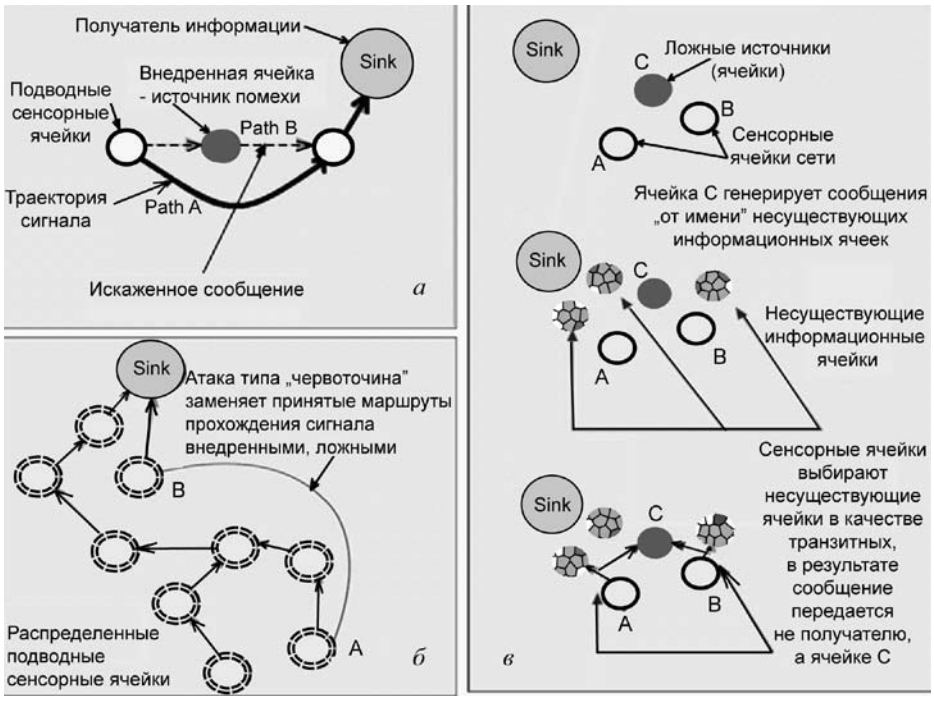

Рис. 4. Схематическое представление некоторых видов атак на сенсорные сети.
а — путем внедрения источников помех; *б* — путем формирования ложных каналов связи («червоточина»); *в* — путем использования ложных источников информации (ячейки «Sybil»).

быть способной перейти в «спящий» режим, периодически «просыпаясь» для контроля состояния атаки. При прерывистой помехе сеть должна быть способной буферировать пакеты сообщений, посылая приоритетные из них только в периоды возникновения «брешей» в атакующих действиях. Для подвергшейся атаке сенсорной сети считается полезным использовать следующий прием. Надо, чтобы часть сети, оказавшаяся ближе к источникам помехи, была способной обнаруживать «сигнал помехи», с передачей сообщения об этом другим ячейкам. На основе таких сообщений возможно изменение маршрутов передачи информации с обходом участков, подвергшихся атаке. Для редкой сети, что характерно для акустики, реализовать такую защиту затруднительно. При малом числе сенсоров и увеличенных расстояниях между ними разделить сенсорное поле на «здоровую» и «пораженную» части с изменением маршрутов прохождения данных трудно. Но в некоторых случаях это возможно, и такую возможность надо иметь в виду.

Атака типа «червоточина» — это образование ложных каналов связи между ячейками сенсорной сети (рис. 4, *б*). Этот вид атаки опирается на технологии образования связей между точками сети с меньшими задержками и более широкой полосой, чем при обычной связи. Технологии для образования меньших задержек, используют, в частности, надповерхностный радиоканал передачи данных (туннелей-червоточин) между пунктами связи, не предусмотренными маршрутизатором, подвергаемой атаке сети. При атаке «червоточина» вредоносная ячейка передает пакеты сообщений, принятых в одной точке «прокладываемого туннеля», в точку на другом его конце, создавая, таким образом, «незаконные» связи. В результате каждая из ячеек ошибочно считает, что находится вблизи другой. Такая атака дезорганизует сеть полностью. Маршрутные протоколы выбирают пути, содержащие «червоточины», т. е. иллюзорно короткие транзитные участки. Таким образом, можно контролировать трафик, задерживать и убирать пакеты данных. Один из методов обнаружения «червоточин» заключается в оценке реальных расстояний между ячейками для проверки их соседской взаимосвязи. Если измеренная дистанция оказывается больше, чем та, которая вытекает из характера самой связи, то считается, что ячейки соединены через «червоточину». Однако оценка расстояния зависит от точности локализации и синхронизации. Для подводных сенсорных сетей точная локализация и синхронизация остаются в целом проблемными задачами, хотя в случае позиционных якорных устройств позиционирование элементов сети для обнаружения «червоточин» осуществляется. В связи с проблемой выявления «червоточин», в ряде работ была предложена процедура, названная «распределенной визуализацией червоточин» (рис. 5, *а*, *б*). Согласно этой процедуре путем многократной прокрутки прохождения сигналов по сети накапливаются оценки

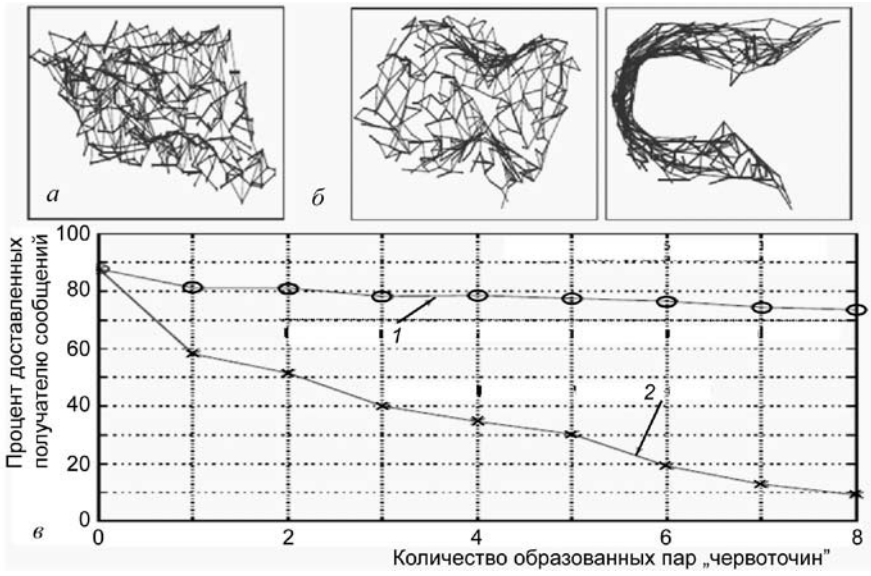

Рис. 5. Реконструкция поля транзитных переходов сообщений в случайно распределенной по пространству сенсорной сети в случаях нормальной работы (*а*) и атаки (*б*).
Пример количественной характеристики влияния на подводные сенсорные сети атак типа «червоточина» (*в*).
1 – сеть с принятыми мерами по противодействию wormhole – атаке; *2* – сеть, подвергшаяся wormhole – атаке.

расстояний до ближайших соседей сенсора по временным задержкам. Таким образом, вокруг каждого сенсора строится виртуальное представление о локальной нормальной топологии сети в пределах двух транзитных участков. Внедрение «червоточины» изменяет топологию целостного изображения в некоторых его частях. И эти изменения могут обнаруживаться. Искажения размеров границ рассчитываются как разница измеренных расстояний между соседними сенсорными ячейками и расстояний, соответствующими реконструированным связям. В подводных сенсорных сетях для их сопротивляемости атакам типа «червоточина» предусматриваются изменения в протоколах, обеспечивающие высокую вероятность такой защиты. Решение основывается на оценках направлений приходов акустических сигналов, которые в свою очередь зависят от относительных положений передатчиков и приемников. Судя по известным результатам моделирования [8], атаки «червоточина» являются одними из наиболее опасных. Из принятых критериев качества работы сетей отметим долю правильно доставленных пакетов сообщений относительно количества переданных. Надо сказать, что и в естественных условиях функционирования сетей на этот показатель влияют помеховый фон акватории и условия распространения звука. Оценки же влияния атак «червоточина» свидетельствуют о практически полной потере работоспособности сетей. Один из результатов модельных исследований показан на рис. 5, *в*. Вредоносная ячейка с множеством идентификаторов может восприниматься как находящаяся одновременно во множестве мест. Это **атаки типа Sybil («образование ложных источников информации»)** (рис. 4, *в*). Защитой от атак этого вида является проверка ячеек и их позиций на подлинность. **Атаки типа «образование ложных сенсорных ячеек — получателей информации»** используют вредоносные ячейки, задачей которых является замыкание трафика сообщений в какой-либо части сенсорной сети на себя. Это осуществляется путем предоставления вредоносными ячейками приоритетных маршрутов.

Привязка выбираемых сетью маршрутов к географическим координатам и установление подлинности принадлежащих сети ячеек являются мерами защиты от **атаки типа «образование потока ложных предложений к соединению»**. Обычно при вступлении в связь ячейка принимает пакет-предложение к соединению. Будучи сгенерированным вредоносной ячейкой, такое предложение может быть воспринято как полученное от ячейки-соседа по сети. Использование повышенной мощности при передаче может приводить к тому, что ячейки такую передачу будут оценивать, как содержащую предложение к соединению. Защитой от этих атак может быть организация двусторонней связи с верификацией. Однако взаимное перемещение ячеек и большие времена запаздываний делают такую защиту не надежной. Установление подлинности ячеек является эффективной защитной мерой. Внедренные в сеть вредоносные ячейки могут прослушивать предусмотренные протоколами пакеты. Затем они же могут использовать эту информацию путем передачи этих пакетов ближайшим к ним ячейкам, образуя ложные соединения. В таких условиях имеет место

повышенный уровень знаковых ошибок и потери соединений. Указанный способ атаки нацелен на манипуляции с маршрутной схемой прохождения сигналов. Противодействие атакам этого вида может быть осуществлено путем шифрования пакетов сообщений. **Атаки типа «избирательно ложная переадресация»** характеризуются тем, что вредоносные ячейки с целью нарушения трафика опускают некоторые сообщения вместо того, чтобы переадресовывать их. В подводных сетях необходимо осуществлять проверку того факта, что приемник не получает информацию в результате такой атаки а не из-за того, что находится в неблагоприятных условиях распространения звука. Внедрение множественности маршрутов и проверка ячеек на подлинность являются защитными мерами. Но такая защита увеличивает нагрузку на сеть. Краткая сводка объектов атаки, методов противодействия сенсорным сетям и методов защиты сетей от этих атак приведена в таблице.

При создании сетевых систем подводного наблюдения к их безопасности предъявляется ряд требований:

Подлинность. Проверка на подлинность означает верификацию того, что данные были переданы законным источником.

Конфиденциальность. Информация является недоступной неавторизированному получателю.

Целостность. Информация не должна изменяться под внешним воздействием.

Доступность. Данные должны быть доступны авторизованному пользователю. Потеря доступности вследствие атак класса «отказ в обслуживании» будет особо чувствительной, если сеть предназначена для решения задач, критичных по отношению ко времени. Такими задачами являются задачи тактического подводного наблюдения.

Сводка методов борьбы подводных сетевых сенсорных систем

Слой сети	Вид атаки	Метод защиты
Физический	Подавление помехами (источники помех — тоже ячейки)	Использование сложных широкополосных сигналов (спред-спектральных), определение приоритета сообщений, картирование региона, изменение режима работы)
	Физическая нейтрализация	Обеспечение устойчивости и скрытности элементов сети
Связной	Прицельное по частоте и времени воздействие на сообщения с целью вызвать его искажение	Использование корректирующих ошибки кодов
	Принуждение связи работать на истощение источников питания	Ограничения на скорость связи
	Совместное применение атак на связной уровень	Использование фреймов малых размеров
Сетевой	Избирательно ложная переадресация	Фильтрация, идентификация, мониторинг
	Образование ложных получателей информации «Sinkhole»	Проверка на избыточность
	Образование ложных сенсорных ячеек («Sybil») как источников информации	Процедуры проверки на аутентичность, избыточность. Мониторинг
	Образование не предусмотренных ложных каналов связи — «червоточин» («Wormhole»)	Идентификация, пробные испытания
	Образование потока ложных предложений к соединению («Hello Flood»)	Идентификация, увязка пакетов с помощью географической и временной информации
	Образование потока ложных соединений	Идентификация, идентификация двунаправленной связи, верификация
Транспортный	Десинхронизация	Сопоставление сообщений от источников, идентификация

***

Можно приветствовать разумные усилия, направленные на поиск путей увеличения дальности обнаружения локальным наблюдателем подводных объектов. Можно приветствовать также рачительное отношение к опоре на имеющийся опыт и существующие разработки. Но в существующих условиях бурного развития пространственно-распределенных сетевых систем подводного наблюдения оба названных пути оказываются все более рискованными. Попытки найти способ существенного увеличения дальности обнаружения из одной точки могут привести к некоторому улучшению существующего положения, но в системном отношении не будут состоятельными. А использование устаревшей идеологии послевоенного периода будет неэффективным и в целом опасным. При ограниченных ресурсах сил и времени расходовать их нерационально — значит увеличивать существующую научную и технологическую брешь с конкурирующей стороной с неблагоприятными последствиями для безопасности. По существу, из предшествующих работ авторов следует, что с точки зрения ряда требований альтернативы сетевым системам подводного наблюдения сейчас нет, в том числе — с точки зрения экономической стороны выбора решений. Однако создавать такие сетевые системы подводного наблюдения необходимо с учетом возможного противодействия им и методов их защиты, чему посвящена настоящая работа. Сделать это — означает принять современный технологический вызов. Принимать его необходимо. Что же касается собственно аспектов противодействия указанным системам и методов их защиты, можно сделать следующие выводы:

— бороться с распределенными сетевыми системами подводного наблюдения необходимо как с целостными образованиями с использованием совокупности мер по противодействию сетям и с учетом специфики океанической среды и распространения в ней акустических сигналов;

— борьба с сетевыми системами подводного наблюдения путем физической нейтрализации их элементов или локального подавления помехой неэффективна. Неэффективно применение приборов гидроакустического противодействия существующего типа;

— для защиты собственных сетевых систем подводного наблюдения необходимо предусмотреть в их составе соответствующие подсистемы, реализующие набор приемов, описанных в данной статье.

References

1. *Kovalenko V. V., Korchak V. Yu., Chulkov V. L.* Concept and Key Technologies of Underwater Surveillance Systems in Networked Centric Warfare. *Fundam. prikl. gidrofiz.* 2011, 4, 3, 49—64 (in Russian).
2. *Kovalenko V. V., Korchak V. Yu., Khil'ko A. I., Chulkov V. L.* Underwater Network-centric Surveillance Requirements. *Fundam. prikl. gidrofiz.* 2014, 7, 2, 22—26 (in Russian).
3. *Kovalenko V. V., Luchinin A. G., Mareev E. A., Malekhanov A. I., Khil'ko A. I.* Underwater acoustics surveillance systems. Structural and physical principles. Barriers, Zones, Multi-static. *Proceedings of 12 All-Russian conference «Applied Technologies for Hydro-acoustics and Hydro-physics». St.-Petersburg,* 2014, 25—29 (in Russian).
4. *Yenumula B. Reddy.* Security Issues in Wireless Sensor Networks. *SENSORCOM,* 2011
5. *Krasil'nikov R. V.* Anti-Unmanned Vehicles Warfare. Asymmetrical reply 21 century threats. *St.-Petersburg, Info-da,* 2013 (in Russian).
6. *Dong Yangze, Liu Pingxiang* Underwater Networked Acoustic Warfare — Concepts and Key Technologies. *The 9-th Pacific Acoustic Conference, Seoul, Korea,* June 26—28, 2006.
7. *Grund M., Freitag L., Preisig J., Ball K.* The PLUSNet underwater communications system: Acoustic telemetry for undersea surveillance. *Proc. MTS/IEEE Oceans 2006.* Boston, MA, USA: IEEE, 2006.
8. *Dong Yangze, Hefeng Dong, Gangqiang Zhang.* Study on Denial of Service against Underwater Acoustic Networks. *Journal of Communications.* 2014, 9, 2.

Статья поступила в редакцию 06.05.2015 г.