УДК 621.324

к.т.н. Миночкин А.И. (ВИТИ НТУУ “КПИ”)
д.т.н. Романюк В.А. (ВИТИ НТУУ “КПИ”)

БЕЗОПАСНОСТЬ МОБИЛЬНЫХ РАДИОСЕТЕЙ

Рассматривается динамичная самоорганизующаяся архитектура построения мобильных радиосетей (МР) или MANET (Mobile Ad-Hoc Networks), предполагающая отсутствие фиксированной сетевой инфраструктуры (базовых станций) и централизованного управления [1]. Все узлы (хосты) сети мобильны и обмениваются информацией непосредственно между собой или применяют ретрансляцию передаваемых пакетов. Под узлом сети понимается радиотерминал (или переносной компьютер, оснащенный радиомодемом), реализующий функции маршрутизатора.

Возросший в последние годы повышенный научный интерес к исследованию МР объясняется появлением недорогих беспроводных сетевых решений (стандарт IEEE 802.11, технологии HiperLAN/2, Bluetooth). Классическими примерами МР являются сети радиосвязи тактического звена управления [2] и сети радиосвязи, обеспечивающие национальную безопасность в кризисных ситуациях. Так перспективная архитектура сетей связи тактического уровня будет представлять собою совокупность трехуровневой иерархии мобильных радиосетей. Другие сценарии применения МР включают: персональные сети для дома и офиса, сенсорные сети, конференции, виртуальные классы и т. п.

МР характеризуются: высокой динамикой топологии, значительной размерностью (сотни и тысячи узлов), низкой пропускной способностью радиоканалов (по сравнению со стационарными сетями), неоднородностью узлов (по мобильности, ресурсам мощности и производительности), ограниченной физической безопасностью и др.

Одной из основных задач управления МР является обеспечение ее безопасности [3]. Целью статьи является анализ основных аспектов безопасности: уязвимость МР, потенциальные атаки противника [4-6] и оценка их угроз, необходимые сервисы (определяют характеристики требований) безопасности возможные механизмы их реализации.

1. Уязвимость мобильных радиосетей

Уязвимость МР по сравнению со стационарными сетями определяется особенностями ее архитектуры и используемыми протоколами функционирования [6].

1. Ограниченность физической безопасности радиоканала. Широковещательная природа радиоканала позволяет противнику ставить активные и пассивные помехи, осуществлять прослушивание передач узлов, анализировать сетевой трафик и вскрывать существующую систему управления войсками.

2. Узел может быть захвачен на поле боя противником или скомпрометирован.

3. Динамичная топология и коллективная работа узлов предполагают уязвимость функционирования протоколов канального, сетевого и других уровней, а также методов управления топологией, радиоресурсом и т.д.

4. Ограниченность ресурсов элементов сети (емкость батареи, объем памяти, производительность процессора узла; пропускная способность радиоканала и др.).

В настоящее время для стационарных сетей предложен ряд механизмов обеспечения безопасности. Однако они не в полной мере могут быть применены для МР. Во-первых, проводные каналы относительно защищены от прослушивания, постановки активных помех и др. Во-вторых, протоколы маршрутизации в МР носят коллективный характер и особенности реализации (например, зондовая маршрутизация [7]), поэтому возможны атаки типа “подмена”, “отказ в обслуживании” и др. [6]. В-третьих, отсутствие фиксированной инфраструктуры и централизованного управления, непредсказуемость сетевой топологии и мобильность узлов вызывают трудности распределения ключей, реализации систем обнаружения вторжений и т.д. В-четвертых, ограниченность ресурса радиотерминала и

ограниченность производительности радиоканала требуют разработку методов безопасности меньшей вычислительной и связной сложности. В заключение, сервисы безопасности должны функционировать в условиях: наличия ошибок в каналах, значительной размерности МР, возможного разделения МР на отдельные подсети, подключения новых и выхода из сети части абонентов.

Существующие беспроводные протоколы реализуют централизованные схемы обеспечения безопасности и эквивалентны механизмам безопасности проводных сетей [5]. Например, протокол 802.11b обеспечивают контроль доступа на канальном уровне и механизмы шифрования Wired Equivalent Privacy (WEP). WEP защищает только пакет данных, но не защищает заголовки физического уровня, так что другие узлы могут просматривать данные, необходимые для управления сетью. Для шифрования данных стандарт использует алгоритм RC4 (потоковый шифр) с 40, 64 или 128-битным разделяемым ключом. На смену ему предусмотрено использование WPA (Wi-Fi Protected Access), который предусматривает не только шифрование с динамически изменяемыми ключами, но и аутентификацию пользователей. Однако данные централизованные решения не приемлемы в МР.

2. Классификация атак и оценка их угроз

По аналогии с проводными сетями атаки в зависимости от характера действий противника делятся на активные и пассивные (рис. 1). Пассивные атаки осуществляются путем несанкционированного прослушивания радиоэфира и анализа сетевого трафика с целью вскрытия топологии сети, способов ее маршрутизации и адресации и др. В этом случае атакующая сторона не нарушает нормальную работу протоколов информационного обмена. Обнаружить пассивные атаки в беспроводной среде обычно невозможно и соответственно защититься от них довольно сложно.

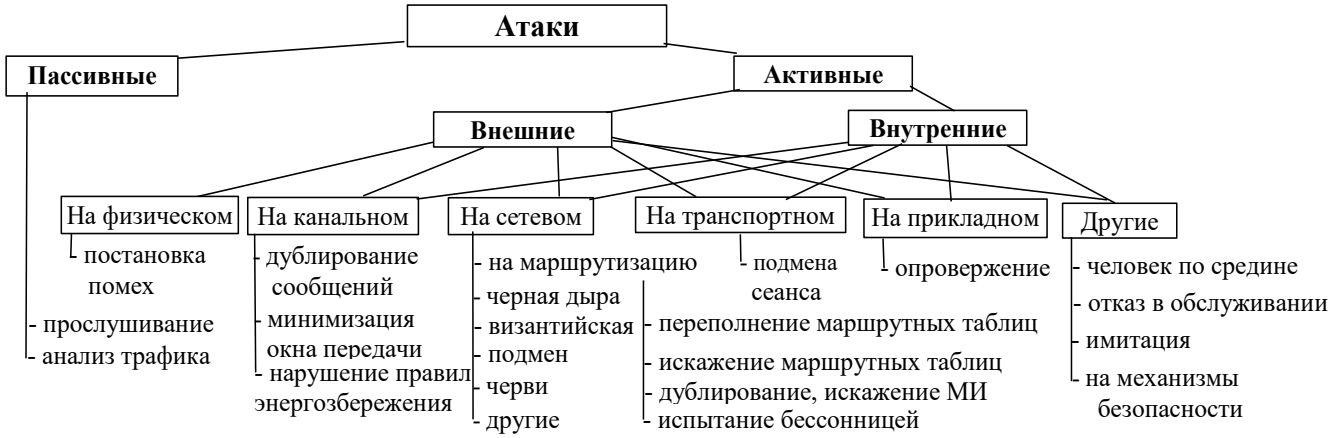

Рис. 1. Классификация атак

Пассивные атаки происходят без воздействия на процесс передачи информации, в то время как активные атаки включают преобразование, модификацию и/или введение ложной информации (в том числе и управляющей). Результат действий активных атак может варьироваться от снижения производительности сети до полной дезорганизации ее работы. Главное отличие активных атак от пассивных заключается в том, что они могут быть обнаружены. В свою очередь активные атаки делятся: на внешние и внутренние (при наличии скомпрометированных или захваченных узлов сети).

Практически все типы активных атак осуществляемых в проводных сетях возможны и в МР, например, подмена сеанса (hijacking), человек посредине (man-in-the-middle), навязывание ложного маршрута, повтор, разрушение маршрутов, отказ в обслуживании (DoS, Denial of Service), опровержение (repudation), имитация (impersonation), затопление (SYN Flooding) и др. [4]. Хотя МР обычно изолирована от общей сети (Интернет), в тоже время атакующий может использовать ее уязвимые стороны. Реализация атак возможна на всех уровнях эталонной модели взаимодействия открытых систем (ЭМ ВОС).

На физическом уровне противник может осуществлять постановку помех.

На канальном уровне возможны атаки: “повтор” (дублирование захваченных пакетов с целью наложения на передаваемые пакеты или создания ложного трафика), направленные на нарушение правил функционирования протоколов канального уровня. Например, использование децентрализованного канального протокола IEEE 802.11 DCF (множественный доступ с контролем несущей) предусматривает случайный розыгрыш окна CW (Contention Windows) начала передачи сообщения. Злоумышленник может воспользоваться этим и, назначая минимальное значение CW, получать первым доступ к каналу. Это приведет к значительному снижению производительности в зоне радиопокрытия противника. Кроме этого, противник может нарушить скоординированную работу энергосберегающих протоколов [8], что приведет к скорейшему выходу батарей из строя.

На сетевом уровне активные атаки на направлены на протоколы маршрутизации [9]. Цель – частичная или полная дезорганизация работы МР путем ввода в сеть повторной (устаревшей) или ложной (измененной) маршрутной информации (МИ). Например, атака типа “отказ в обслуживании” может быть легко реализована модификацией одного или нескольких полей маршрутного сообщения (зонда): адреса отправителя (spoofing), числа ретрансляций, номера сообщения и самого маршрута передачи. Результатами активных атак могут быть: перенаправление маршрутов (и, соответственно, трафика), зацикливание маршрутов, создание перегрузки в узлах сети, переполнение маршрутных таблиц, имитация разделения сети на отдельные подсети, увеличение времени доставки сообщений и т. д.

Приведем примеры некоторых активных атак, которые могут быть осуществлены в МР (рис. 1).

“Черная дыра”. В этом случае противник, используя имеющийся протокол маршрутизации, объявляет себя узлом в кратчайшем пути к адресату и переправляет весь трафик на себя.

“Переполнение маршрутной таблицы”. Противник стремится создать маршруты к несуществующим узлам. Цель атаки заключается в создании маршрутов, которые бы предотвратили создание новых маршрутов путем переполнения таблицы маршрутизации.

“Испытание бессонницей”. Атака характерна для МР и направлена на скорейший разряд батарей узлов. Противник может нарушить функционирование энергосберегающих протоколов различных уровней ЭМ ВОС. Кроме того, генерируя ложный информационный и/или служебный трафик (например, генерируя зонды-запросы на построение маршрута к несуществующим узлам) неприятель заставляет узлы расходовать свою энергию батарей.

“Обнаружение местоположения”. Противник, используя зондовую маршрутизацию, рассылает зонды-запросы [7]. На основе анализа содержимого зондов-ответов он пытается узнать информация о местоположении узлов или раскрыть структуру сети.

“Отказ в обслуживании”. Атака направлена на занятие ресурса сети (связного, вычислительного) и может быть реализована на любом уровне ЭМ ВОС: на физическом (постановка помех), на канальном (повторная передача), на сетевом (перенаправление маршрутов) и др. Она также может быть направлена на протоколы управления ключами.

3. Сервисы безопасности и механизмы ее обеспечения

Сервисы безопасности должны учитывать особенности МР и обеспечиваться теми или иными механизмами безопасности с целью защиты от определенного множества атак. Сервисы безопасности обычно включают следующие основные понятия [4]:

- секретность (confidentiality) – невозможность ознакомления противником со смысловым содержанием передаваемого сообщения;
- подлинность (аутентификация, authentication) – уверенность в том, что данные отправлены именно тем, от чьего имени они получены;
- целостность (integrity) – уверенность в том, что принятые данные не были изменены по пути от отправителя к получателю;

- контроль доступа (access control) – предотвращение доступа пользователя к объекту (ресурсу) без соответствующих полномочий;

- неопровержимость (non-repudation) – механизм, гарантирующий невозможность отказа от факта получения или отправления сообщения;

- доступность (availability) – свойство ресурса системы, заключающееся в возможности его использования по требованию пользователя, имеющего соответствующие полномочия, несмотря на возможные атаки.

В табл. 1 показаны механизмы реализации указанных сервисов. Защита от внешних атак включает шифрование информации, использование цифровой подписи и обеспечение других сервисов безопасности. Так цифровая подпись позволяет проверить подлинность, целостность сообщения, а также обеспечить его неопровержимость (обеспечивает защиту от атак типа отказ, подмена и модификация передаваемых данных). Для обнаружения дубликатов пакетов и соблюдения необходимого порядка их поступления целесообразно использовать в формате пакета временные метки и порядковый номер пакета. Для защиты от внутренних атак предполагается использовать систему обнаружения вторжений.

Табл. 1

Сервисы безопасности	**Механизмы реализации**
Секретность	Шифрование
Подлинность	Цифровая подпись
Целостность	Шифрование, хэш-функция
Контроль доступа (идентификация)	Блок идентификации абонента, протоколы идентификации узлов
Неопровержимость	Цифровая подпись
Доступность	Средства физической защиты, использование робастых протоколов

Для обеспечения сервисов безопасности могут применяться симметричная и/или асимметричная криптосистема. Симметричная криптосистема предполагает наличие общего секретного ключа и обеспечивает сервисы секретности, целостности и подлинности. Ее недостатком является возможность дешифрования всех перехваченных сообщений при компрометации ключа. Асимметричная криптосистема предполагает наличия у каждого узла пары ключей: открытого и закрытого. Основываясь на данной паре ключей, могут быть обеспечены сервисы аутентификации, целостности и неопровержимости.

С точки зрения вычислительной сложности предпочтительна симметричная криптосистема. Поэтому обычно используют гибридные схемы: сеансовый симметричный ключ для шифрования сообщений, а асимметричный закрытый ключ используется для шифрования сеансового ключа (протоколы PGP [4], WAP [5]).

Отдельной проблемой в МР (в условиях отсутствия фиксированной инфраструктуры) является управление ключами (п. 3.6): для симметричных криптосистем необходим закрытый канал, для асимметричных – необходимость “третьей стороны” для сертификации ключей, возможность атаки “человек по середине”.

3.1. Контроль доступа абонентов в сеть, протоколы идентификации узлов

Контроль доступа абонентов в сеть осуществляется введением в радиотерминал блока (модуля) идентификации и аутентификации лиц, запрашивающих доступ к системе. Данный блок может быть реализован в виде интеллектуальной карты (содержащей микропроцессор и необходимые криптографические протоколы, алгоритмы), а также может быть дополнен использованием PIN-кода, пароля или биометрии. Достоинством карты является возможность смены владельца радиотерминала, недостатком – возможность захвата противником. Контроль доступа абонентов в сеть (авторизация) может осуществляться периодически и/или по мере передачи секретной информации.

В сети контроль доступа должен включать протоколы идентификации узлов и управления группами узлов, например, при кластеризации сети необходимо выделение главных

узлов зон. В стационарных и беспроводных сетях обычно доступ определяется его IP-адресом. В МР IP-адрес динамичен (например, при иерархической организации сети) и поэтому для идентификации узла его формат необходимо дополнять отрытым ключом [10].

3.2. Защита от атак на физическом уровне ЭМ ВОС

1. Значительное уменьшение возможности противника по обнаружению и прослушивания передач МР на физическом уровне может быть достигнуто следующими способами: применение технологии расширения спектра сигнала, направленных антенн, оптимизация мощности передачи узлов (при управлении топологией сети [11]).

2. Разделение информации на части, их шифрование и передача по нескольким независимым маршрутам. Для этого необходимо предусмотреть в сетевом программном обеспечении узлов наличие многопутевого метода маршрутизации [12]. Данное решение неприемлемо при непосредственной близости отправителя и получателя. В этом случае многопутевую маршрутизацию можно сочетать с независимыми радиоканалами, полученными с помощью направленных антенн. Недостаток данного подхода – значительные затраты ресурсов сети для построения и поддержания многопутевых маршрутов.

3. Защита от анализа трафика противником возможно за счет шифрования как информационной, так и служебной части пакета (при передаче пакета открытым остается только адрес текущего ретранслятора).

3.3. Защита протоколов канального уровня

Зависит от использования конкретного протокола канального уровня [13]. Для уменьшения влияния атак данного уровня необходимо предусмотреть смену канальных протоколов или использование адаптивных протоколов с разной степенью коллективности принятия решений на занятие радиоресурса. Например, при использовании протокола множественного доступа с контролем несущей и обнаружении атак (ложный трафик, захват временного интервала передачи) целесообразно перейти на протокол не кооперированной работы, например, типа ALOHA.

3.4. Защита протоколов маршрутизации

В существующих протоколах маршрутизации сети Интернет используются простейшие механизмы обеспечения безопасности [4]. Так в протоколе RIP (Routing Information Protocol) аутентификация производится посредством незащищенного пароля из 16 бит. Протокол OSPF (Open Shortest Path First) проверяет маршрутную информацию, используя 16 битовую контрольную сумму (дополнительно может использоваться 64-битовое поле аутентификации). В последних версиях RIP-2 и OSPF v.2 для аутентификации используются хэш-функция MD-5 (Message Digest). Однако данное решение необходимо интегрировать с существующими механизмами управления ключами. Перспективным направлением обеспечения безопасности маршрутизации признано использование протокола безопасности IPSec (Internet Protocol Security) [4]. Однако данный протокол безопасности (как и протоколы маршрутизации в Интернет) ориентированы на использование в статичных сетях. Например, протокол IPSec решает задачи безопасности между двумя входами в сеть при существующем маршруте. Т.е. непосредственное его применение в МР невозможно. Кроме того, в условиях высокой динамики топологии МР предпочтительно использование зондовой или гибридной маршрутизации, которая характеризуется своими особенностями построения и поддержания маршрутов по сравнению с таблично-ориентированными протоколами [7].

Определим основные требования к безопасной маршрутизации в МР как невозможность противником: фальсифицировать адрес отправителя МИ, внедрять в сеть ложную МИ, изменять МИ в процессе ее ретрансляции, формировать маршрутные циклы, перенаправлять маршрут, определять сетевую топологию из МИ. Неавторизованные узлы должны быть исключены из процесса вычисления и построения маршрутов. Защита от активных атак на

протоколы маршрутизации в МР должна предусматривать аутентификацию и целостность маршрутной информации, а защита от анализа трафика ее шифрование.

3.5. Система обнаружения вторжений (IDS).

Возможным способом защиты от внутренних атак является применение систем обнаружения вторжения IDS (Intrusion Detection System) [6, 14]. IDS могут быть классифицированы:

по способу обнаружения атаки – обнаружение злоупотреблений (основано на правилах обнаруживающих известные атаки по содержащимся в базе данных сигнатурам) и обнаружение аномального поведения (за определенный период времени);

по объекту мониторинга – обнаружение атак, направленных на всю сеть, отдельный ее сегмент (характерно для проводных сетей) или на конкретный узел сети;

по реакции на атаку – пассивные (регистрируют атаку и сообщают о ее наличии) и активные (кроме регистрации и оповещения препятствуют взломщику);

по принятию решений – локальные и кооперированные (решение об атаке принимается группой узлов).

Системы обнаружения вторжений, созданные для проводных сетей не эффективны или не применимы в МР. Например, сетевые IDS анализируют трафик реального времени на сегменте сети (совокупности коммутаторов, маршрутизаторов или шлюзов), в то время как трафик в МР по своей природе не может быть сконцентрирован в одной точке (в зоне радиосвязности). Необходимость анализа реального трафика требует значительной производительности компьютера, что входит в противоречие с имеющимися ресурсами узлов МР. Кроме этого возможность компрометации узлов (узел не может полностью доверять своему соседу) и их мобильность создают дополнительные трудности в обнаружении различий между аномальным и нормальным функционированием сети.

Поэтому IDS должна быть реализована на каждом узле независимо – каждый узел оценивает поведение своих соседей (с возможностью запроса соседа о его действиях и поведении, а также информировании об аномальных действиях определенных узлов), анализирует их трафик и принимает решение самостоятельно. Общий подход к анализу поведения соседнего узла заключается в реализации принципа “сторожевой собаки”. При этом каждый узел может оценивать поведение своего соседа по определенным параметрам: частота сброса пакетов; частота перестроения или потери маршрута; качество маршрутов (число ретрансляций, соответствие типу трафика и т.д.), мобильность, используемые протоколы канального и сетевого уровней и на основании данной информации вычисляет величину, характеризующую степень доверия к нему. Окончательное решение о компрометации определенного узла может быть принято после согласования своей степени доверия с другими узлами (т.е. кооперированная IDS).

Реализованы IDS могут быть на основе применения технологий искусственного интеллекта (экспертные системы, нечеткие множества, нейросети и др.). Один из перспективных подходов построению комплексных систем защиты информации (СЗИ), позволяющим учесть особенности функционирования МР, является *технология интеллектуальных многоагентных систем* [15]. Этот подход позволяет по сравнению с традиционными методами существенно повысить эффективность защиты информации, в том числе ее адекватность, отказоустойчивость, устойчивость к деструктивным действиям, универсальность, гибкость и т.д.

Компоненты многоагентной СЗИ (агенты защиты) представляют собой интеллектуальные автономные программы, реализующие определенные функции защиты с целью обеспечения требуемого класса защищенности. Они позволяют реализовать комплексную надстройку над механизмами безопасности используемых сетевых программных средств,

операционных систем и приложений, повышая защищенность системы до требуемого уровня.

Предполагается, что агенты распределены по узлам защищаемой сети, специализированы по типам решаемых задач и взаимодействуют друг с другом с целью обмена информацией и принятия согласованных решений. Важно подчеркнуть, что в явном виде отсутствует "центр управления" семейством агентов – в зависимости от сложившейся ситуации ведущим может становиться любой из агентов, специализирующихся на задачах управления. В случае необходимости агенты могут клонироваться и прекращать свое функционирование. В зависимости от ситуации (вида и количества атак на МР, наличия вычислительных ресурсов для выполнения функций защиты) может генерироваться несколько экземпляров агентов каждого класса. Они адаптируются к реконфигурации сети, изменению трафика и новым видам атак, используя накопленный опыт [15]. Выделяются следующие базовые агенты: агенты восприятия, агенты обнаружения вторжения, агенты разграничения доступа, агенты идентификации и аутентификации, агенты подавления атакующего, агенты оценки повреждений и восстановления целостности данных, агенты криптографической защиты, агенты обучения, мета-агенты.

Реализация многоагентных СЗИ потребует значительных вычислительных мощностей и поэтому их реализация возможна в мобильных базовых станциях [2].

3.6. Управление ключами

Управление ключами играет фундаментальную роль в криптографии, являясь основой криптографических методов. Управлением ключами предполагает их распределение, аутентификацию, обновление и регламентацию порядка использования. Необходимость обновления ключей (сертификатов) определяется возможностью компрометации узлов и самого центра сертификации [4-6].

В стационарной сети Интернет используется централизованный центр сертификации в рамках инфраструктуры открытых ключей [4]. Централизованное управление не может быть применено в МР из-за низкой живучести, возможной перегрузки, абоненты МР могут выключать радиотерминалы или быстро перемещаться. Кроме этого к системе распределения ключей в МР предъявляются следующие основные требования: поддержка значительного количества пользователей – порядка 1000, вычислительная эффективность, ограниченный служебный трафик, надежная доставка управляющей информации и др. Возможным решением может стать распределение функций центра сертификации среди некоторой части или всех узлов.

1. Кооперированный и распределенный центр сертификации [16]. С помощью некоторой (k, n) пороговой схемы (например, схема разделения секрета Памира $k<n$) распределяется секретный ключ. Кроме того предполагается наличие протокола, позволяющего коалиции из K пользователей производить распределенную подпись, не раскрывая при этом секретного ключа. Недостаток данного решения – необходимость постоянной связи с узлами сертификации и их аутентификация (для обеспечения устойчивости к DoS атакам).

2. Иерархия центров сертификации (в соответствии с иерархией построения системы управления сетью): беспилотный летательный аппарат – мобильная базовая станция – мобильный абонент с передачей функций управления друг другу [17].

3. Самоорганизующееся управление открытыми ключами, основанное на протоколе PGP (Pretty Good Privacy) [18]. Особенностью PGP является распределенный подход к распределению ключами – поддерживается "сеть доверия". Каждый пользователь сам создает и распространяет свой открытый ключ. Пользователи подписывают ключи друг друга, создавая взаимосвязанное общество PGP. Для этого каждый пользователь поддерживает локальную сертификационную базу, хранимую в виде трастового графа отношений между пользователями. Когда пользователь u желает получить открытый ключ пользователя v, он ищет направленный путь в трастовом графе и соединяет локальную сертификационную базу

обоих пользователей и пытаться найти соответствующий сертификат из скрепленной базы. Недостатком данного решения является отсутствие гарантии отзыва скомпрометированных ключей.

Таким образом, сервисы безопасности МР в основном аналогичны сетям общего пользования. Защита от внешних атак обеспечивается реализацией механизмов безопасности (шифрование информации, цифровой подписи и др.), защита от внутренних атак – применением систем обнаружения вторжений. Однако обеспечение механизмов безопасности является более сложной проблемой по сравнению со стационарными сетями связи из-за необходимости построения эффективной распределенной системы управления ключами и децентрализованной системы обнаружения вторжений. Рассмотренные механизмы обеспечения безопасности в МР могут найти свое применение в тактических сетях связи.

ЛИТЕРАТУРА

1. *Романюк В.А.* Мобильные радиосети – перспективы беспроводных технологий // Сети и телекоммуникации. – 2003. – № 12. – С. 62 – 68.

2. *Міночкін А.І., Романюк В.А.* Архітектура перспективної мобільної компоненти тактичних мереж зв'язку збройних сил України // Збірник наукових праць № 5. – К.: ВІТІ НТУУ "КПІ". – 2004.

3. *Міночкін А.І., Романюк В.А., Скрипник Л.В.* Управління мобільними радіомережами військового призначення – проблеми та шляхи рішення // Збірник наукових праць № 4. – К.: ВІТІ НТУУ "КПІ". – 2003. – С. 78 – 91.

4. *Блек У.* Интернет: протоколы безопасности. – СПб.: Питер, 2001. – 288 с.

5. *Максим М., Полино Д.* Безопасность беспроводных сетей. – М.: ДМК Пресс, 2004. – 288 с.

6. *Chen X., Huang X., Du D.-Z.* A Survey of Wireless Security in Mobile Ad Hoc Networks: Chalenges and Available // Ad Hoc Wireless Networking, 2003. – pp. 319 – 364.

7. *Миночкин А. И., Романюк В.А.* Протоколы маршрутизации в мобильных радиосетях // Зв'язок. – 2001. – № 1. – С. 31 – 36.

8. *Миночкин А.И., Романюк В.А.* Управление энергоресурсом мобильных радиосетей // Зв'язок. – 2004. – № 8. – С. – .

9. *Романюк В.А.* Безпека протоколів маршрутизації в автоматизованих мережах радіозв'язку // Труди Академії № 37. – К.: НАОУ. – 2002. – С. 174 – 178.

10. *Sarela M., Nikander P.* Applying Host Identity Protocol to Tactical Networks // In Proceedings of MILCOM'04, 2004.

11. *Миночкин А.И., Романюк В.А.* Управление топологией мобильной радиосети // Зв'язок. – 2003. – № 2. – С. 28 – 33.

12. *Миночкин А.И., Романюк В.А.* Многопутевая маршрутизация в мобильных радиосетях // Зв'язок. – 2004. – № 6.

13. *Миночкин А.И., Романюк В.А.* Методы множественного доступа в мобильных радиосетях // Зв'язок. – 2004. – № 2.

14. *Zhang Y., Lee W.* Intrusion Detection in Wireless Ad-Hoc Networks // In Proceedings ACM/IEEE MOBICOM, 2000. – pp. 275 – 283.

15. *Міночкін А.І.* Розподілена система захисту інформації в мобільних радіомережах // Збірник наукових праць № 2. – К.: ВІТІ НТУУ "КПІ". – 2003.

16. *Zhou L., Haas Z.J.* Securing Ad Hoc Networks // IEEE Networks Magazine, vol. 13, no. 6, 1999. – pp. 24 – 30.

17. *Kong J., Luo H., Xu K., Gu D.-L., Gerla M.* Adaptive Security for Multilevel Ad-hoc Networks // Wireless Communications and Mobile Computing, 2002. – pp. 533 – 547.

18. *Hubaux J.-P., Buttyan L., Capkun S.* The Quest for Security in Mobile Ad Hoc Networks // In Proceedings MOBIHOC'01, 2001.

19. Chan A. Distributed Symmetric Key Management for Mobile Ad hoc Networks // In Proceedings INFOCOM'04, 2004.

20. Bercher M., Hof H.-J., Kraft D. A Cluster-Based Security Architecture for Ad Hoc Networks // In Proceedings INFOCOM'04, 2004.