

УДК: 621.325 : 621.391

С.В. Малахов, А.Г. Снисаренко, С.Г. Рассомахин, Н.Ф. Линник, В.Н. Шлокин

*Объединенный научно-исследовательский институт Вооруженных Сил, Харьков*

## ТРАНСЦЕНДЕНТНАЯ РЕАЛИЗАЦИЯ ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТЬЮ ПЕРСПЕКТИВНОГО РАКЕТНОГО КОМПЛЕКСА НА ОСНОВЕ ПРИНЦИПОВ WMN-ТЕХНОЛОГИИ

*Предложен вариант адаптации технологии Mesh-сетей для решения задачи синтеза мультисервисной телекоммуникационной системы перспективного ракетного комплекса. Сделан вывод о том, что в условиях значительной гетерогенности сетевого клиентского оборудования использование WMN-технологии позволяет осуществить конвергенцию принципов иерархического и распределенного управления коммуникационным оснащением и канальным ресурсом сети.*

*децентрализованное управление, мультисервисная сеть, роутер, Mesh-сеть*

### Введение

Новационные решения, рождающиеся на стыке электросвязи и микропроцессорной техники, являются постоянным катализатором разработок в области создания принципиально новых образцов военной техники. Внедрение передовых технологий в автоматизированные системы управления и связи в значительной степени повлияло как на сами эти системы, так и на способы ведения боевых действий. Примером данной тенденции служит активное использование новых форм и способов обработки и обмена информацией в современных образцах автоматизированных систем управления и связи технически развитых стран мира (FBCB<sup>2</sup>, IBCS и EPLRS - США, "Топаз-В" – Россия и т.д.) [1 – 4].

Процесс разработки перспективного ракетного комплекса (ПРК) инициировал работы, связанные с анализом и выбором принципов построения основных систем комплекса. При этом одним из важнейших направлений является разработка предложений по формированию «облика» его информационно-телекоммуникационной системы. Изначально предполагается, что данная система представляет собой часть интегрированной автоматизированной системы управления ПРК и должна обеспечить достижение высоких вероятностно-временных характеристик разрабатываемого телекоммуникационного оснащения комплекса. Ожидается, что принятие научно-обоснованных решений, касающихся вопросов создания единой телекоммуникационной среды, и применение эффективных внутрисетевых переносчиков информации [5 – 7] позволит реализовать функционирование системы управления ПРК в масштабе времени, близком к реальному, обеспечивая при этом выполнение целого ряда дополнительных мультисервисных функций.

**Анализ литературы.** Известно, что традиционным вариантом развертывания современных ра-

диосетей связи и обмена информацией военного назначения является такой, при котором все абоненты сети связываются не напрямую, а посредством базовой (центральной) станции (БС) [6 – 9]. Используемый при этом протокол обслуживания РМР (Point-to-Multipoint Protocol – протокол "точка-многоточие") [8, 10] зарекомендовал себя в качестве простого и надежного решения в большинстве военных систем радиосвязи и передачи данных (высокоскоростная широкополосная мультимедийная система пакетной радиосвязи "Топаз-В"). Однако для такого варианта реализации сетевой структуры характерен ряд существенных недостатков [6 – 9]. Главные из них – наличие узловых БС, что ухудшает мобильность всей системы и накладывает определенные ограничения на параметры ее размещения, и относительно низкая структурная устойчивость сети, обусловленная трансляцией основной части трафика непосредственно через БС.

**Цель статьи** – разработка предложений по применению принципов имманентных WMN-технологии (Wireless Mesh Networks) [7] в телекоммуникационной системе ПРК. При этом, с точки зрения практической реализации этой системы, WMN рассматривается в качестве альтернативы РМР-сетям.

В результате анализа особенностей функционирования WMN внимание акцентируется на возможностях технической реализации принципов децентрализованного управления телекоммуникационной системой ПРК при распределенной физической реализации ее топологии.

### Основной материал

В технической литературе термин WMN (или Mesh-сети) трактуется как беспроводные сети, образуемые из связанных равноправных узлов [7]. При этом отличительной чертой Mesh-структуры является то, что она представляет собой распределенную

систему, в которой каждый из образующих ее узлов обладает одинаковыми или заданными правами и функциональными возможностями.

На практике WMN-технология является инструментом построения широкополосных сетей передачи данных, в которых информация может передаваться по цепи из нескольких узлов, чем нивелируются трудности, обусловленные отсутствием прямой связи между абонентами. Таким образом, обеспечивается поддержка множества альтернативных маршрутов от отправителя до получателя информации, причем их количество увеличивается по мере добавления в сеть новых узлов. Однако, несмотря на то, что в WMN все узлы формально равноправны, в ее структуре практически всегда присутствует, как минимум, один узел, посредством которого реализуется взаимодействие Mesh-сети с внешним окружением. Традиционно на этот узел возлагается и часть функций связанных с координацией управления непосредственно Mesh-сетью. При этом функции управления доступом реализуются либо на основе механизма распределенного управления, либо централизованным способом под управлением базового узла (БУ), а в случае необходимости возможна и их комбинация [7]. Таким образом, WMN описывает рассредоточенную сетевую структуру (Mesh-Scatternet), в которой все БС замещены магистральными узлами – Mesh-маршрутизаторами (Mesh-роутерами), посредством которых организуется беспроводная транспортная Mesh-сеть и реализуются функции доступа к любым внешним сетям передачи информации и информационным ресурсам.

В рассматриваемом варианте реализации телекоммуникационной системы ПРК (рис.1) использование принципов, свойственных WMN-технологии, позволит органам управления более высокого уровня в значительной степени абстрагироваться от процессов, связанных с организацией и мониторингом физических каналов передачи данных в подчиненных звеньях управления. Это будет способствовать улучшению ситуационной осведомленности номеров дежурных сил и, соответственно, позволит им в большей степени сконцентрироваться на вопросах применения комплекса по назначению.

Система магистральных роутеров 1-2-го ранга, образующих транспортную Mesh-сеть доступа ПРК и выполняющих функцию шлюзов (рис. 1), совместно с пунктами радиодоступа полевой опорной сети связи [11], обеспечит интеграцию телекоммуникационной системы ПРК с любыми внешними информационными ресурсами.

Радиосети нижнего звена управления, являясь клиентской частью WMN, должны самостоятельно осуществлять детерминированный выбор каналов передачи данных адекватно помеховой обстановке, складывающейся в позиционном районе. При этом

процесс активации того или иного канала между элементами клиентской радиосети является прерогативой аппаратуры приема-передачи данных (Mesh-роутеров), интегрированной в состав оборудования узлов клиентской Mesh-сети, и осуществляется на основе измерения параметров принимаемых сигналов. Учитывая то, что в WMN передача данных реализуется посредством промежуточных узлов [7], а радиообмен осуществляется с пониженными уровнями излучаемой мощности, можно говорить о повышении скрытности функционирования телекоммуникационной сети ПРК.

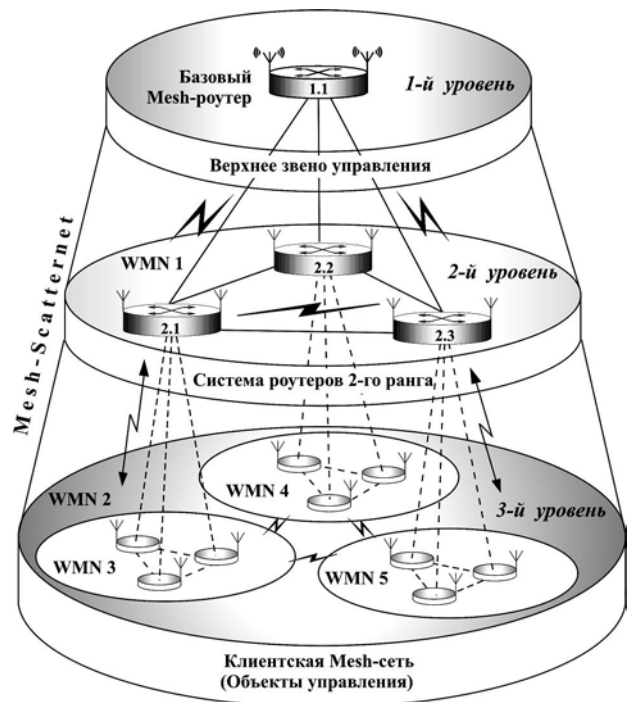


Рис. 1. Вариант организации WMN ПРК

Важно подчеркнуть, что в рассматриваемом варианте реализации мультисервисной [12] телекоммуникационной системы (рис. 1), в ее клиентской части (3-й уровень Mesh-Scatternet ПРК, т.е. WMN 2-5) предполагается использование только одного интерфейса радиообмена, вследствие чего программно-аппаратная реализация коммуникационного оборудования объектов управления, по сравнению с оборудованием органов управления, выполняется в упрощенном варианте. При этом WMN 2 представляет собой реализацию варианта взаимодействия терминалов, представленных в различных сегментах (пикосетях) клиентской части сети ПРК, без участия Mesh-роутеров вышестоящих звеньев управления. Таким образом, WMN 2 является реализацией процесса ситуативного расширения сетевого окружения за счет объединения нескольких пикосетей ПРК на самом нижнем уровне иерархии всей системы (в отличие от решений принятых, например, в системе пакетной связи "Топаз-В"). По-

сколькx каждая клиентская сеть для обмена данными между своими элементами в каждый момент времени использует уникальную сигнальную конструкцию [5], то любой терминал, одновременно ассоциирующийся в двух и более пикосетях, должен получить информацию об изменении соответствующих настроек для каждой из этих сетей. При этом каждый узел WMN хранит список данных обо всех своих «соседях» (удаленность - порядок соседства, секторы **max** диаграммы направленности антенн, мощность передатчика для поддержания устойчивой связи, задержки распространения сигнала и т.д.) и транслирует его в сеть с заданной периодичностью. В общем случае, управление сетью происходит на основании данных получаемых от каждого из узлов WMN [7].

Вариант взаимодействия в рамках WMN 2 является дублирующим и повышает устойчивость телекоммуникационной системы к негативным воздействиям относительно ее узлов и каналов передачи данных. Осуществление информационного взаимодействия в рамках WMN 2 без привлечения коммуникационного оборудования вышестоящих уровней позволяет представить структуру телекоммуникационной системы ПРК (рис. 1) в упрощенном виде (рис. 2).

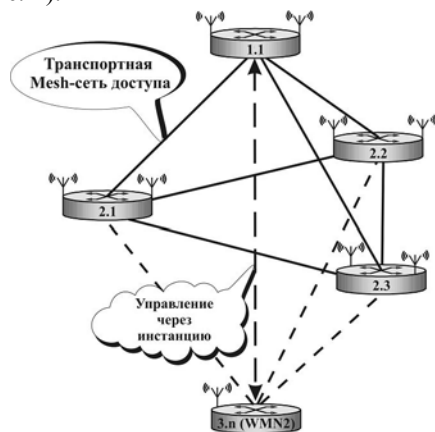


Рис. 2. Упрощенная схема WMN

При этом, введенное на рис. 2 обозначение элемента схемы – 3.n (WMN2) следует читать, как: n-й терминал 3-го уровня Mesh-сети ПРК, входящий в состав WMN2 (рис. 1).

Фактически же элемент 3.n (WMN2) – это один из объектов управления.

Известно, что при использовании WMN-технологии задача распределения канальных ресурсов решается **централизованным** и **распределенным** способами [7]. В свою очередь, децентрализованное распределение может координироваться с узла Mesh-сети, назначенного в качестве базового (базовый роутер 1-го ранга, рис. 1), и быть некоординированным. При этом децентрализованное управление коммуникационным оборудованием

подразумевает, что распределение канального ресурса происходит в пределах одной группы соседних узлов (пикосети WMN 3-5, рис. 1).

При реализации **координированного децентрализованного распределения** канальных ресурсов все узлы WMN обмениваются между собой так называемыми DSCH-сообщениями (distributed scheduling), представляющими собой формализованную форму запроса/ответа на предоставление канального ресурса соседнего узла (временного интервала в субкадре данных). Механизм координации заключается в том, что период выдачи таких сообщений каждым терминалом WMN ПРК определен и известен соседним узлам сети. Координированные DSCH-сообщения передаются в субкадрах управления очередностью доступа в оговоренных сетевым дескриптором интервалах.

Некоординированные DSCH-сообщения передаются в субкадре данных (например, в случае изменения структуры развернутой сети в аварийном режиме - WMN2, рис. 1).

**Централизованное** распределение канальных ресурсов подразумевает древовидную реализацию топологии Mesh-сети с БУ в вершине (базовый роутер 1.1, рис. 1, 2). Реализуется посредством использования двух типов сообщений, размещаемых в начале каждого субкадра управления графиком доступа к телекоммуникационной сети ПРК: 1 – централизованного конфигурирования; 2 – централизованного планирования.

Сообщения **централизованного конфигурирования** формируются БУ (1-й уровень иерархии управления, рис. 1) и транслируются по сети для информирования всех узлов о текущем состоянии. Они должны содержать следующую информацию:

- число доступных логических каналов;
- перечень активированных узлов Mesh-сети ПРК с указанием числа дочерних узлов для каждого из них (ранга соседства);
- профили восходящих/нисходящих пакетов для каждого дочернего узла.

Сообщения **централизованного планирования** необходимы для определения узлами WMN (рис. 1) потребности в трафике для своих дочерних (соседних) узлов с последующей переадресацией этих данных вышестоящему узлу, вплоть до БУ. После обобщения полученной информации базовый узел ретранслирует сообщения централизованного планирования, информируя, таким образом, каждый узел WMN ПРК о выделенной ему полосе пропускания в восходящем и нисходящем направлениях. Располагая этими данными, каждый узел самостоятельно запрашивает (назначает) расположение пакетов в субкадре данных для своих соседних узлов посредством сообщений **децентрализованного планирования** (DSCH).

Для повышения структурной устойчивости Mesh-сети ПРК необходимо предусмотреть возможность эмуляции части функций базового узла на одном из элементов WMN1 (рис. 1). С этой целью на вычислительных средствах базового и дублирующего узлов устанавливается программно-математическое обеспечение (ПМО), выполняющее функции ядра WMN (рис. 3). Репликация текущих эксплуатационных настроек ядра сети на вычислительных средствах дублирующего узла, при необходимости, позволит оперативно сконфигурировать все сетевые параметры Mesh-сети ПРК («Система аварийной реконфигурации», рис. 3).



Рис. 3. Состав ПМО ядра WMN ПРК

Ядро WMN включает в себя систему мониторинга и управления сетью, систему управления контентом, а также систему управления удаленным доступом. Кроме того, в зависимости от набора сервисов [12], в ядро сети могут быть включены программные платформы различных дополнительных услуг: система управления сетью VoIP; система видеоконференцсвязи и т.д. (на рис.3 – затенены). Перечень подобных функций требует дополнительного обсуждения и не является в контексте излагаемого материала предметом детального рассмотрения.

Отличие ПМО дублирующего узла от его оригинала заключается в ограничении некоторых функций ядра сети, что обусловлено различиями в техническом оснащении пунктов управления нижестоящего уровня и разнице наряда размещаемых на них дежурных смен. Перевод функций управления от базового узла к дублирующему осуществляется посредством системы санкционирования полномо-

чий. Таким образом, функции сетевого взаимодействия и распределения канальных ресурсов системы реализуются посредством перехода от штатного **централизованного** к **децентрализованному координированному** способу управления [7], осуществляемого с резервного базового узла 2-го ранга Mesh-сети ПРК (рис. 1). При этом функции мониторинга WMN осуществляются дублирующим комплектом «Терминала технической поддержки» (рис. 4). Технической основой для организации данного рабочего места может служить один из терминалов звена управления нижестоящего уровня («Терминалы звена управления», рис. 4). На остальных магистральных узлах сети ПРК выполнение данных функций не предусматривается.

В представленном на рис. 3 варианте имплементации ядра WMN обозначено присутствие беспроводного и проводного магистральных роутеров узла 1-го ранга. Приведенные общепринятые сокращения (MGW – цифровая система абонентского радиодоступа, ATM – технология асинхронного режима передачи, MPLS – технология многопротокольной коммутации пакетов, VoIP – технология передачи речевой информации) [11, 12] иллюстрируют поддерживаемые технические возможности коммуникационного оборудования телекоммуникационной сети ПРК.

Наличие на двух узлах (пунктах управления разных уровней) телекоммуникационной сети ПРК программных комплектов ядра

WMN позволит, при необходимости, провести оперативное реконфигурирование и восстановление функций системы. В случае выхода из строя двух указанных узлов (1.1, 2.1, рис. 1, 2) организацию сетевого взаимодействия и распределение канального ресурса, в рамках сложившейся конфигурации системы, предполагается выполнить переходом к **децентрализованному некоординированному** способу управления [7]. Данная ситуация характерна также и для случая выхода из строя узлов (роутеров) 2-го ранга без перехвата функций управления их клиентской сетью базовым роутером верхнего звена управления (т.е. без активации режима управления через инстанцию, рис. 2).

Таким образом, по мере выхода из строя базовых узлов WMN процесс управления коммуникационным оборудованием и канальным ресурсом сети претерпевает следующую эволюцию в использовании различных способов управления: централизо-

ванное → децентрализованное координированное → децентрализованное некоординированное. При этом в ходе восстановления утраченных функций базовыми узлами системы возможен и обратный процесс.

Рассмотрим основные инструменты защиты сетевого трафика WMN. С целью ограничения доступа к ресурсам Mesh-сети необходимо предусмотреть комплекс специальных технических мер. При этом,

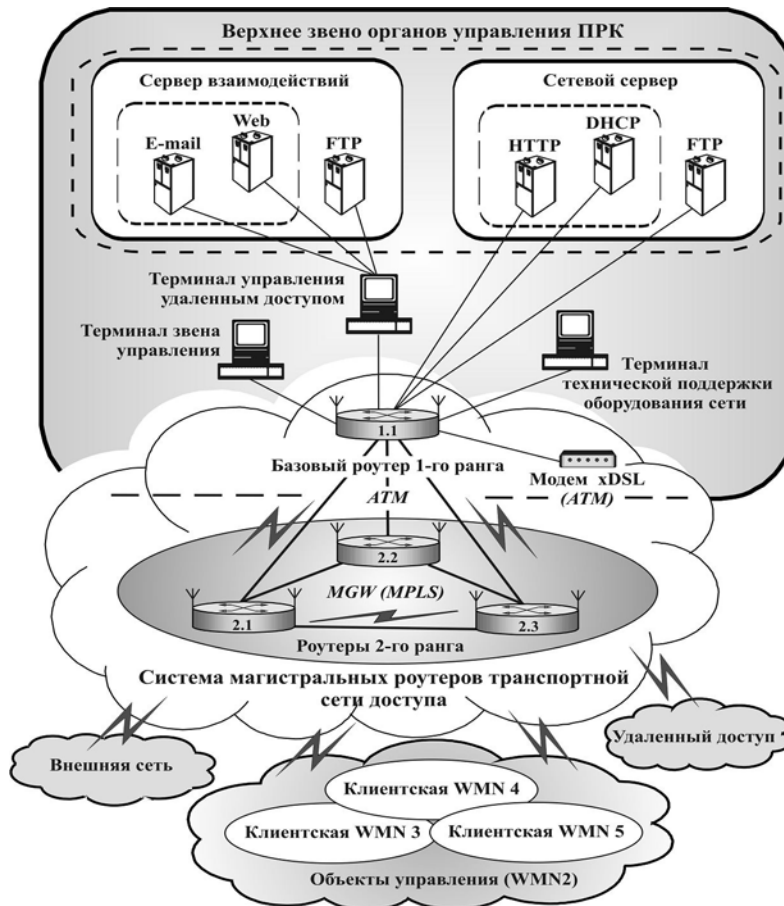


Рис. 4. Структура базового узла

эффективным способом обеспечения безопасности как проводной, так и беспроводной реализации сети, является использование следующих технических мер [6 – 8, 10, 13]:

1) применение идентификаторов (SSID) роутеров. Вводится с целью предоставления отдельным группам пользователей WMN возможности взаимодействия с назначенными точками доступа AP (Access Point). Используется для защиты от несанкционированного проникновения в сеть, если рассматривать SSID как пароль;

2) списки доступа по MAC-адресам. При этом в роутерах, интегрированных в состав оборудования органов управления, создается реестр MAC-адресов сетевых адаптеров развернутой Mesh-Scatternet, имеющих право доступа к ней. Учитывая значительную гетерогенность абонентского оборудования

телекоммуникационной сети, указанный реестр необходимо периодически пополнять и реплицировать на все магистральные роутеры (выполняется с БУ). Данная мера может служить достаточно надежной защитой при условии, если в сетевых адаптерах абонентского оборудования, на этапе ввода в эксплуатацию, аппаратно заблокировать функцию изменения своих MAC-адресов;

3) шифрование трафика с использованием стеганографических методов и потоковых шифров с переменной длиной ключа, где пользователем задается лишь часть пароля (вектор инициализации). При этом необходимо предусмотреть возможность смены ключей, однако, сменив пароль на одном роутере, необходимо уведомить об этом все терминалы WMN (образующих одну пикосеть). В этом случае необходимо принять организационно-технические меры, направленные на обеспечение скрытия ключевой информации, хранимой абонентскими устройствами WMN. Использование данных мер обеспечивается сеансовая стойкость (криптозащита на уровне временной стойкости);

4) использование протоколов, обеспечивающих как шифрование, так и аутентификацию. При этом с целью повышения стойкости шифрования также необходимо предусмотреть возможность смены сеансовых ключей (RSA, DES).

Рассмотрим последовательность действий, обязательных при настройке безопасной работы WMN. В общем случае необходимо выполнить два этапа: организация AP и настройка коммуникационного оборудования.

Конфигурирование магистральных роутеров пунктов управления (рис. 1, 2) потребует установки следующих основных параметров: системное время, пароль администратора WMN (при осуществлении централизованного управления сетью с одного из базовых узлов), трансляция SSID [10], DHCP-сервер, установка паролей.

Для исключения конфликтов с функцией автоматического назначения WMN-адресов на БУ верхнего звена управления необходимо активировать только один DHCP-сервер (рис. 3).

После обеспечения требуемого уровня аутентификации абонентов сети необходимо провести операции, связанные с криптозащитой (настройкой шифрования) трафика.

С целью повышения степени защиты WMN для каждого магистрального роутера должен быть сформирован список MAC-адресов его окружения и абонентских терминалов клиентской части радиосети (имя терминала, MAC-адрес, тип подключения). При этом важно убедиться, что MAC-адрес автоматизированного рабочего места (один из базовых узлов 1-2-го ранга, рис. 1, 2), с которого настраиваются роутеры транспортной сети доступа, имеется в реестре «Системы санкционирования полномочий» ядра системы (рис. 3). В общем случае осуществить функцию фильтрации радиодоступа можно не только по MAC-адресам, но и WMN-адресам, портам и протоколам. Поэтому, при необходимости, можно реализовать многоступенчатую схему санкционирования доступа (функция «Системы санкционирования полномочий»), рис. 3).

Последний этап – санкционирование доступа к настройкам магистральных роутеров пунктов управления (рис. 2) и терминалов сети и организация альтернативного варианта управления коммуникационным оборудованием WMN. Для этого необходимо установить диапазон статических WMN-адресов, с которых производится настройка магистральных роутеров. Желательно, чтобы это были только два специализированных терминала, доступ к которым находится под особым контролем (основной и резервный базовые узлы сети). Соответственно, при организации дублирующих схем управления Mesh-сетью ПРК, функции администрирования управления коммуникационным оборудованием и каналным ресурсом сети логично возложить на резервный БУ нижестоящего звена управления Mesh-Scatternet.

Предполагается, что при активации в сети ПРК новых узлов их динамические WMN-адреса автоматически назначаются “активным” DHCP-сервером базового узла системы (рис. 4). Статические же адреса предлагается закрепить за магистральными роутерами транспортной Mesh-сети доступа (рис. 2). Такое разделение обусловлено тем, что использование статической адресации имеет смысл в случае запуска на узле какого-либо сетевого сервиса. А с учетом того, что все магистральные роутеры интегрируются в состав оборудования пунктов управления, такое распределение является вполне логичным. При этом для магистральных роутеров возможно два варианта обращений: от абонентов внешних сетей и от терминалов WMN (рис. 3, 4). С целью придания коммуникационным возможностям сети мультисервисных функций [12] для пунктов управления необходимо предусмотреть возможность подключения к их оборудованию различной периферии, а также обеспечить осуществление доступа к внешним информационным ресурсам посредством известных сетей – CDMA, GSM, Wi-Fi, WiMAX [1, 6 – 9, 11].

Таким образом, с организационной точки зрения, использование в терминальном оборудовании органов управления ПРК возможностей статической адресации обеспечит достижение транспарентности коммуникационных сервисов органов управления, ассоциированных в различных информационных системах, что в значительной мере разрешит трудности в организации оперативного взаимодействия при выполнении миротворческих задач [11, 14].

Одновременно решаются следующие технические задачи: поддержка функционирования интегрированной распределенной корпоративной сети (VPN – Virtual Private Network) ПРК; осуществление функции удаленного доступа; организация на пунктах управления FTP/ HTTP-серверов (обеспечение поддержки видеоконференцсвязи, VoIP, обмена e-mail и др.). При наличии встроенного детектора движения возможна реализация варианта охранной системы с видеонаблюдением.

В случае возникновения в коммуникационном оборудовании БУ аварийной ситуации, и как следствие, недоступности его FTP-сервера, необходимо предусмотреть проводной модем с серверным программным обеспечением (рис. 4).

Соответственно, на дублирующем узле устанавливается аналогичный модем и клиентская часть программы, что обеспечит выполнение функций доступа к аварийному терминалу (серверу), настройку системы и автоматическое возобновление обмена трафиком с FTP-сервером базового узла без выполнения перезагрузки ядра системы на ее БУ.

С целью обеспечения доступа к информационным ресурсам внешних сетей и осуществления взаимодействия с их абонентами, в составе серверной части ядра системы (базового узла ПРК), организуется сервер взаимодействий (рис. 4).

При выходе из строя БУ (децентрализованное координированное управление) функции управления удаленным доступом осуществляются с любого из оставшихся магистральных узлов (пунктов управления), но с ограничением некоторых сервисов (обведены пунктиром - «Сервер взаимодействий», рис. 4).

В общем случае, различия в составе серверной части ПМО устанавливаемом на всех пунктах управления ПРК, заключаются в ограничении части функций управления Mesh-сетью (HTTP/DHCP-серверы) и осуществления удаленного доступа (E-mail, Web) (на рис. 4, выделены пунктиром).

## Выводы

Основной недостаток централизованного способа управления коммуникационным оборудованием и каналными ресурсами вытекает из самого принципа централизованности.

Единый центр управления – базовый узел – должен быть надежно защищен от сбоев, а его каналы связи и передачи данных с периферийными коммутаторами необходимо резервировать, что влечет за собой дополнительные затраты.

Кроме того, в результате направленного воздействия по базовому узлу системы, результатом которого является его нейтрализация, вся схема организации взаимодействия претерпевает значительные изменения, что делает невозможным выполнение некоторых функций, ограничивает интенсивность обмена трафиком и снижает оперативность принятия решений.

Напротив, построение распределенной сети, реализованной с использованием принципов WMN-технологии, имеет ряд неоспоримых преимуществ. К главным из них следует отнести гибкость, масштабируемость, высокую структурную устойчивость и способность динамического перераспределения нагрузки в сети.

Кроме того, ее использование позволяет интегрировать для конечного пользователя широкий спектр телекоммуникационных услуг, причем как фиксированной, так и мобильной связи.

К недостаткам, обусловленным использованием WMN, можно отнести тот факт, что протоколы маршрутизации Mesh-сетей весьма специфичны, а их разработка – непростая инженерная задача с различными критериями и множеством параметров. Протокол должен гарантировать надежную доставку сообщений в случае потери канала связи и одновременно распределять информационную нагрузку, то есть не ухудшать производительность всей сети при ее расширении.

Все это усложняется маршрутизацией для многоадресных приложений и применением в сети узлов с поддержкой нескольких интерфейсов (узлы транспортной сети доступа).

Однако можно предположить, что объединение функций маршрутизации и MAC позволит добиться определенных улучшений как собственно протокола маршрутизации, так и суммарных характеристик WMN.

Таким образом, использование технологии Mesh-сетей может обеспечить устойчивое конфигурирование сетевого коммуникационного оборудования и позволит достичь высокой степени скрытности и структурной стойкости телекоммуникационной системы перспективного ракетного комплекса.

## Список литературы

1. Аганов А. Модернизация танков М1 “Абрамс” и боевых машин пехоты М2 “Брэдли” в США // *Зарубежное военное обозрение*. – 2002. – № 9. – С. 24-29.
2. Азаров Г.И. Направления развития средств и систем военной связи // *Военная мысль*. – 2003. – № 4. – С. 41-44.
3. Харченко Н. Современное состояние и перспективы развития радиостанций зарубежных государств // *Зарубежное военное обозрение*. – 2003. – № 6. – С. 22-30.
4. Донсков Ю.Е., Ботнев А.К. Системы связи и передачи данных армии США: состояние и перспективы развития // *Военная мысль*. – 2005. – № 7. – С. 42-48.
5. Сорока Л.С. Основы теории минимально-избыточных сигналов. Математические методы и средства обработки: Монография. – Х.: МОУ, ОНИИ ВС, 2005. – 280 с.
6. Григорьев В.А., Лагутенко О.И., Распаев Ю.А. Сети и системы радиодоступа. – М.: Эко-Трендз, 2005. – 384 с.
7. Шахнович И.В. Современные технологии беспроводной связи. Издание второе, исправленное и дополненное. – М.: Техносфера, 2006. – 288 с.
8. Карташевский В.Г., Семенов С.Н., Фирстова Т.В. Сети подвижной связи. – М.: Изд-во Эко-Трендз, 2001. – 299 с.
9. Наритник Т.М., Почерняев В.М., Уткін Ю.В. Радіорелейні та тропосферні системи передачі: Навчальний посібник. – 2007. – 312 с.
10. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2001. – 672 с.
11. Рудик В.В. Актуальні проблеми та напрями розвитку системи зв'язку Збройних Сил України як складової частини системи управління військами (силами) // *Наука і оборона*. – 2005. – № 2. – С. 22-28.
12. Телекоммуникационные системы и сети: Учебн. пос. В 3-х т. Т. 3. Мультисервисные сети / В.В. Величко, Е.А. Субботин, В.П. Шувалов, А.Ф. Ярославцев; под ред. В.П. Шувалова. – М.: Горячая линия–Телеком, 2005. – 592 с.
13. Столингс В. Криптография и защита сетей: принципы и практика, 2-е изд.: Пер. с англ. – М.: Изд. дом “Вильямс”, 2001. – 672 с.
14. Семеріч Ю.П. Забезпечення зв'язку в миротворчих операціях // *Наука і оборона*. – 2004. – № 1. – С. 33-37.

Поступила в редколлегию 3.04.2007

**Рецензент:** д-р техн. наук, старший научный сотрудник В.И. Антюфеев, Объединенный научно-исследовательский институт Вооруженных Сил, Харьков.