THE APPROACH FOR SELECTION OF A ROUTING METRIC IN SPECIAL-PURPOSE WIRELESS NETWORKS UNDER THE INFLUENCE OF RADIO-ELECTRONIC INVESTIGATION

Snegurov A.V., Chakryan V.K., Mamedov A.A.
Kharkiv National University of Radioelectronics
Department of Telecommunication Systems
14, Lenina Ave., Kharkiv, 61166, Ukraine
Ph.: (057) 7021320, e-mail: tkc@kture.kharkov.ua

Abstract — The present paper concerns the approach for selection of a routing metric in special-purpose wireless networks under the influence of radio-electronic investigation (REI). In this approach the routing metric considers both the quality of service (QoS) requirements and security requirements from REI. The index of information security risk of the route is added in the metric calculation function. This index depends on the information security risk of the network routing elements. The ways of index calculation are proposed.

ПОДХОД К ВЫБОРУ МЕТРИКИ МАРШРУТИЗАЦИИ В БЕСПРОВОДНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ В УСЛОВИЯХ ДЕЙСТВИЯ СРЕДСТВ РАДИОЭЛЕКТРОННОЙ РАЗВЕДКИ

Снегуров А.В., Чакрян В. Х., Мамедов А. А.
Харьковский национальный университет радиоэлектроники
кафедра Телекоммуникационных систем
пр. Ленина, 14, Харьков, 61166, Украина
тел.: (057) 7021320, e-mail: tkc@kture.kharkov.ua

Аннотация — В работе предложен подход к маршрутизации в телекоммуникационных сетях специального назначения (ТКС СН), функционирующих в условиях действия средств радиоэлектронной разведки (РЭР). Предлагается метрика маршрутизации, учитывающая как требования к качеству сервиса (Quality of Service, QoS) так и требования к защищенности от РЭР. В функцию, учитывающую вес маршрута вводится такой показатель, как риск информационной безопасности маршрута, зависящий от риска информационной безопасности узлов ТКС СН. Предлагаются способы расчета данного показателя.

I. Введение

Беспроводные телекоммуникационные сети специального назначения (ТКС СН) в ближайшем будущем выведут системы управления войсками и оружием на качественно новый уровень. Внедрение таких ТКС СН позволит реализовать так называемую концепцию сетецентрической войны, элементы которой были апробированы армией США в боевых действиях в Ираке и Афганистане. Объединение с использованием ТКС СН в единую информационную сеть средств разведки, органов управления и средств огневого поражения, радиоэлектронного и электромагнитного подавления обеспечит опережение противника в принятии решения и опережающий вывод из строя ключевых элементов его инфраструктуры.

Данные ТКС СН могут строиться как на основе сетей с фиксированной инфраструктурой, так и на основе сетей с динамически меняющейся сетевой инфраструктурой. Примером реализации мобильных адаптивных сетей является перспективная система радиосвязи для вооруженных сил США, разрабатываемая по программе JTRS. Технологии сетей с фиксированной инфраструктурой отрабатываются на стандартах 802.11, 802.16.

Особенностью применения ТКС СН является возможность их функционирования в условиях целенаправленного информационного противодействия. При этом по узлам и каналам связи ТКС СН могут применяться средства радиоэлектронной разведки и радиоэлектронного подавления (киберразведки и кибернападения).

При этом использование средств информационного противодействия может привести к совершенно обратным результатам применения ТКС СН. Так, например, использование средств радиоэлектронной разведки (РЭР) позволяет путем выявления и обработки информации о ТКС СН вскрывать группировку войск, намерения командования и т.д. При этом применение современных средств защиты, например, криптографических средств защиты информации, не позволяет в полном объеме противодействовать РЭР. Это обусловлено тем, что выявление излучений узлов ТКС СН, определение параметров сигналов, тонкий анализ данных сигналов, пеленгация и определение координат узлов ТКС СН уже дает существенный объем информации для разведорганов противника.

В этих условиях остается актуальной задача проведения исследований в направлении обеспечения информационной безопасности (ИБ) ТКС СН. Одним из путей решения данной задачи является разработка и использование алгоритмов маршрутизации, учитывающих требования к информационной безопасности. В данном исследовании предлагается подход к формированию метрик маршрутизации, учитывающих требования к качеству сервиса (Quality of Service, QoS) и защищенности от РЭР.

II. Подход к выбору метрики маршрутизации

С позиции теории массового обслуживания каждый тракт передачи ТКС рассматривается, как правило, в виде модели M/M/1. При этом поток, который посту-

2013 23rd Int. Crimean Conference "Microwave & Telecommunication Technology" (CriMiCo'2013). 9—13 September, Sevastopol, Crimea, Ukraine
 ISBN: 978-966-335-395-1. IEEE Catalog Number: CFP13788

пает в сеть, считается пуассоновским, длины пакетов рассматриваются независимыми и распределенными по показательному закону. Одним из основных моментов является принятие «гипотезы про независимость», которая предусматривает, что при объединении нескольких потоков в тракте передачи сохраняется независимость между интервалами поступления и длинами пакетов. Решение задачи маршрутизации при этом можно свести к нахождению целевой функции [1]:

$$D_0 = \min_{\lambda} \sum_{(i,j)} D_{ij}(\lambda_{ij}). \quad (1)$$

где $D_{ij}(\lambda_{ij})$ — функция, которая характеризует вес маршрута. В качестве данной функции, учитывающей требования QoS и ИБ, можно выбрать соотношение:

$$D_{ij}(\lambda_{ij}) = a^{R_{ij}^m}\left(\frac{\lambda_{ij}}{\phi_{ij}-\lambda_{ij}} + \tau_{ij}^n \lambda_{ij}\right), \quad (2)$$

где λ_{ij} — информационный поток [1/с] в тракте передачи (ji); ϕ_{ij} — пропускная способность тракта (ji) [1/с]; τ_{ij}^n — задержка распространения пакетов [с], $R_{ij}^m \in [0,1]$ — риск ИБ маршрута, который можно определить на основе риска ИБ узлов ТКС СН через выражение:

$$R_{ij}^m = 1 - \prod_{Z=1}^{Z^m}\left(1 - R_z^m\right), \quad (3)$$

где Z^m — множество узлов ТКС СН, которые входят в m-й тракт передачи информации.

Риск информационной безопасности узлов ТКС СН является функцией следующих показателей:

$$R_z = f(P_{усp_k}^z, P_{уязв_k}^z), \quad (4)$$

где $P_{усp_k}^z$ — вероятность использования k-го комплекса РЭР на z-й узел ТКС СН; $P_{уязв_k}^z$ — вероятность разведки z-го узла ТКС СН k-м комплексом РЭР. Данные показатели должны определяться на основе прогноза возможных координат средств комплекса РЭР.

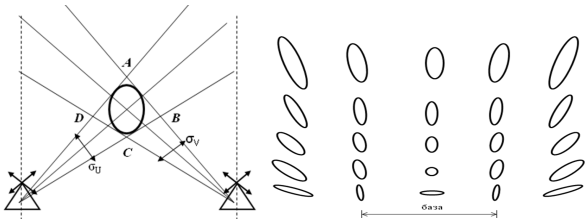
Вероятность $P_{уязв_k}^z$ может включать в себя такие показатели, как вероятность локализации (определения координат с заданной точностью) узла ТКС СН комплексом РЭР и вероятность перехвата сигнала узла ТКС СН приемниками комплекса РЭР.

Точность определения координат узлов ТКС СН наиболее полно характеризуется эллипсом и полем ошибок (рис. 1).

Если местоположение узла ТКС СН определяется на плоскости, то двумерная плотность распределения вероятности ошибок определения его координат пеленгационным способом определяется из выражения [2]:

$$\varphi(U,V) = \frac{1}{2\pi\,\sigma_U\sigma_V} e^{-\frac{1}{2}\left[\frac{U^2}{\sigma_U^2}+\frac{V^2}{\sigma_V^2}\right]},$$

где U и V — случайные ошибки линий положения, описываемые нормальным законом распределения; σ_U и σ_V — среднеквадратические ошибки линий положения (пеленгов).



а) б)

Рис. 1. Эллипс и поле ошибок определения координат узлов ТКС СН пеленгационным способом.

Fig. 1. The ellipse and errating band of sites coordinates determination of special-purpose wireless networks by means a direction-finding method

Вероятность того, что ТКС СН находится в пределах эллипса ошибок определяется из выражения:

$$P(x) = \iint_{S(\lambda)} \varphi(U,V)\,dU\,dV, \quad (5)$$

где $S(\lambda)$ — область, ограниченная эллипсом ошибок.

Из представленных выражений и рисунка видно, что знание противником координат узлов ТКС СН зависит от ряда факторов, к которым относятся их ориентация и удаление от пеленгаторной сети, СКО определения пеленгов в пеленгаторах и т.д.

Вероятность несанкционированного приема (перехвата) сигнала РЭС ТКС СН средствами РЭР можно оценить с использованием такого показателя, как вероятность ошибки приема каждого отдельного символа цифрового сигнала ТКС *Рош* [3]:

$$P_{ош} = \frac{1}{2}\left[1 - \Phi\left(\sqrt{\frac{Q_c}{N}(1-\rho_s)}\right)\right], \quad (6)$$

где $Q_c = P_c$, *тс* — энергия символа; P_c — мощность сигнала на входе разведприемника, T_c — длительность символа; *N* — спектральная плотность мощности шума; $\rho_s \in [-1;1]$ — коэффициент взаимной корреляции между сигналами, которые соответствуют передаче символов «1» и «0». Параметр P_c зависит от энергетических характеристик и удаленности узла ТКС СН, ориентации его антенной системы относительно средства РЭР, условий распространения радиоволн и т.д.

III. Заключение

Вышесказанное означает, что каждый узел ТКС СН имеет различную степень защищенности от средств РЭР (разный риск ИБ узла). Использование предложенного подхода позволяет выбирать более безопасный маршрут передачи информации с точки зрения защищенности от средств РЭР и учесть требования к качеству сервиса (QoS).

IV. References

[1] Gallager R.G. A minimum delay routing algorithm using distributed computation. *IEEE Trans. on communications*, 1975. vol. 25, No 1, pp.73-85.

[2] Sajbel' A.G. *Osnovy teorii tochnosti radiotehnicheskih metodov mestoopredelenija* [Basis of theory of precision of radiotechnical positioning methods]. Moscow, Oborongiz, 1958. 56 p.

[3] Cvetnov V.V., Demin V.O., Kuprijanov A.I. *Radiojelektronnaja bor'ba: radiorazvedka i radioprotivodejstvie* [Radioelectronic struggle: radioprospecting countermeasure]. Moscow, Izd-vo MAI, 1998. 248 p.