СИСТЕМА РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ В СЕНСОРНЫХ СЕТЯХ С ИСПОЛЬЗОВАНИЕМ КОМБИНАТОРНЫХ БЛОК-СХЕМ

М.А. Алисеенко, С.Б. Саломатин

Рассматривается распределенная сенсорная сеть, в которой N сенсорных узлов случайным образом разбросаны по территории. Сенсорные узлы взаимодействуют друг с другом и требуют парных ключей для защиты своей связи. Каждый датчик имеет связку из K ключей, которая хранится в его ПЗУ перед развертыванием. При этом пара сенсорных узлов должна иметь пул общих ключей в своей цепочке ключей.

Проблема состоит в том, чтобы выбрать размер цепочки для ключей и размер пула ключей, чтобы каждая пара узлов могла установить ключ сеанса напрямую или через путь с высокой вероятностью [1].

Математической основой системы является сбалансированные блок-схемы (BIBD), представленные множеством взаимных ортогональных латинских квадратов [2].

Алгоритм системы распределения ключей включает в себя следующие действия. Нахождение степень простого числа n, удовлетворяющего квадратичному соотношению, соответствующему размеру сети N. Формирование $(n-1)$ полного набора взаимных ортогональных латинских квадратов (MOLS) порядка n. Построение аффинной плоскости порядка n по MOLS. Построение проективной плоскости порядка n по аффинной плоскости.

Для симметричных блок-схем справедливо, что любая пара блоков разделяет ровно один объект. Таким образом, вероятность совместного использования ключа между любой парой узлов равна 1, поэтому средняя длина пути к ключу равна 1.

Комбинаторный подход увеличивает вероятность того, что пара сенсорных узлов будет иметь общий ключ, и уменьшает длину ключевого пути.

Литература

1. Song, Y., Wool A., Yener B. Combinatorial Design of Multi-Ring Networks with Combined Routing and Flow Control. Computer Networks. 2003. Vol. 3 (3). P. 247–267.

2. Colbourn, C.J., Dinitz J.H. The CRC Handbook of Combinatorial Designs. CRC Press, 1996. 753 p.