МНОГОПУТЕВОЕ РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ В СЕНСОРНОЙ СТОХАСТИЧЕСКОЙ СЕТИ

С.Б. Саломатин, А.П. Турлай

В сенсорных сетях распределение ключей обычно сочетается с начальным установлением связи, чтобы настроить безопасную коммуникационную инфраструктуру из набора развернутых сенсорных узлов [1].

Один их подходов решения задачи распределения секретных ключей предполагает использовать случайную маршрутизацию сетевой структуры.

Модель распределения ключей. В сенсорных сетях распределение ключей обычно сочетается с начальным установлением связи, чтобы настроить безопасную коммуникационную инфраструктуру из набора развернутых сенсорных узлов. В процессе настройке, узлы предварительно инициализируются секретной информацией. После настройки сети известно местоположение узлов. Предположим, что можно обмениваться достаточной маршрутной информацией, так что A знает все непересекающиеся пути к B, созданные во время начальной установки ключа.

Модель динамической стохастической сенсорной сети [2]. В модели сенсорной сети, каждый узел обновляет скалярное состояние. Узел является последовательным, если для формирования управляющего действия используется только относительный обмен информацией с соседями. Узел является лидером, если, помимо относительного обмена информацией с соседями, он также имеет доступ к собственному состоянию. Проблема идентификации лидеров сети, сводится к решению задачи минимизации среднеквадратического отклонения.

Алгоритм многопутевого ключа состоит в том, чтобы координировать обновление ключа по нескольким независимым путям, определяемыми случайно расположенными лидерами сети. Секретность ключа защищена всеми случайными значениями путей.

Литература

1. Chan H., Perrig A., Song D. Key distribution techniques for sensor networks. Norwell, MA, USA: Kluwer Academic Publishers, 2004.

2. Саломатин С.Б., Алексеенко А.Э., Турлай А.П. Сетевое кодирование кодом Рида-Соломона с учетом лидеров стохастической сети // Кодирование и цифровая обработка сигналов в инфокоммуникациях: материалы международной научно-практической конференции, Минск, 19 апреля 2021 г. С. 23–27.