ОБЕСПЕЧЕНИЕ НАДЕЖНОСТИ ДАННЫХ ДЛЯ МНОГОРЕЖИМНЫХ ДАТЧИКОВ В БЕСПРОВОДНОЙ СЕТИ

С.И. Сиротко, С.В. Юзефович

По мере распространения беспроводных технологий для все более широкого круга применений становится актуальной разработка оконечных устройств различного назначения — сравнительно простых и недорогих, но достаточно функциональных и эффективных. В частности, требования к беспроводным датчикам нередко могут быть противоречивы: поддержка различных типов чувствительных элементов и режимов работы, при этом унификация управления и экономичность. Это предполагает наличие достаточно емкой памяти данных и параметров, а также использование специального протокола обмена, причем устройство подвержено сбоям из -за внешних факторов, а канал связи — помехам и искажениям. Следовательно, необходимо обеспечивать надежность и безошибочность хранимых и передаваемых данных, включая и их восстановление.

Методы, использующие контрольные суммы и помехозащищенные коды, обеспечивают достаточную надежность и безусловно целесообразны, но они реализуются на нижних уровнях иерархии программных средств и не распространяется на логическую корректность данных. Целостность и одновременно правильность обработки могут быть достигнуты объединением данных с описанием их формата и структуры; примером может служить XML. Однако работа с такими форматами достаточно затратна.

Для простых устройств с ограниченными ресурсами эффективно самодокументирование данных в более простой форме: представление их структурами, состоящими из обязательного дескриптора и некоторого (возможно, нулевого) количества однотипных элементов данных, причем дескриптор несет исчерпывающие сведения о всей структуре. Такая форма универсальна, сочетаема с объектными моделями и позволяет корректно интерпретировать каждую отдельно взятую структуру. Ошибки элементов данных ограничиваются пределами структуры, а ошибка в дескрипторе или неверная выборка дескриптора приводят к нарушению связности списка структур и тоже могут быть локализованы (восстановление списка будет требовать дополнительных внешних средств).

Защита передаваемой информации от несанкционированного перехвата и/или искажения рассматривается как задача следующего этапа разработки.