УДК 621.391.037.372

СРАВНЕНИЕ АЛГОРИТМОВ НАДЕЖНОЙ ПЕРЕДАЧИ ПАКЕТОВ ДЛЯ СЕНСОРНЫХ СЕТЕЙ

Е. М. Линский,
науч. сотрудник
Г. С. Евсеев,
канд. техн. наук, доцент
Санкт-Петербургский государственный университет аэрокосмического приборостроения

Сенсорная сеть состоит из устройств с ограниченными ресурсами. Часто сенсорная сеть развертывается в неконтролируемом окружении, что приводит к низкой физической защищенности отдельных узлов, т. е. узлы могут быть захвачены злоумышленником. Основным источником ненадежности при передаче пакетов в сенсорной сети являются компрометированные узлы, удаляющие пересылаемые через них пакеты. Статья посвящена сравнению алгоритмов надежной передачи для сенсорной сети, которые противодействуют этой атаке.

A sensor network consists of devices with limited resources. There are scenarios, where a sensor network is deployed in a hostile environment. This leads to low physical security of sensors, i. e. sensors could be captured by adversaries. The main source of unreliability in packet forwarding protocol is compromised nodes that drop forwarded packets. This paper compare reliable packet forwarding protocols that act against this attack.

Введение

Сенсорная сеть состоит из множества сенсоров, случайным образом распределенных по исследуемой поверхности, и базовой станции. Сенсор — это автономное беспроводное устройство с ограниченными ресурсами. Задачей сенсора является сбор информации и ее передача базовой станции. Ресурс источника питания сенсора обычно ограничен, что фактически определяет время жизни сенсора, тесно связан с его вычислительными возможностями и влияет на мощность передатчика. Сфера применения сенсорных сетей довольно обширна: мониторинг окружающей среды, раннее диагностирование поломок устройств в промышленности, управление дорожным движением, контроль за безопасностью объектов.

Сенсорная сеть часто разворачивается в неконтролируемом окружении. Поэтому сенсор может быть захвачен и его программное обеспечение может быть заменено. Такой сенсор называется компрометированным узлом или атакующим. Действия атакующих направлены на нарушение работы основных протоколов сенсорной сети, в том числе и протокола передачи пакетов. Основной атакой, влияющей на надежность передачи, является атака, в рамках которой компрометированный узел выборочно удаляет передаваемые через него пакеты [1]. Компрометированный узел не может удалить все передаваемые через него пакеты, так как в этом случае он будет обнаружен.

В работах [2–4] были рассмотрены алгоритмы передачи для сенсорной сети, которые предназначены для противодействия описанной атаке. Общая идея этих алгоритмов состоит в том, что для передачи используются несколько независимых маршрутов. Предложенные алгоритмы можно разделить на две группы: неадаптивные [3, 4] и адаптивные [2]. Неадаптивный алгоритм в отличие от адаптивного не использует информацию о качестве маршрутов (вероятность ошибки, энергопотребление и т. д.) и не меняет своих параметров в зависимости от этих характеристик. Можно выделить два основных неадаптивных алгоритма: алгоритм случайной передачи (СП) [4] и алгоритм избыточной передачи (ИП) [3]. В алгоритме СП отправитель случайным образом выбирает один из маршрутов и посылает по нему пакет. В алгоритме ИП по всем маршрутам направляется по одной копии исходного пакета. Алгоритм адаптивной избыточной передачи (АИП) [2] является усовершенствованием алгоритма избыточной передачи. На основе информации о качестве маршрутов для каждого из маршрутов определяется количество копий, которое должно быть по нему послано.

Целью данной работы является численное сравнение адаптивных и неадаптивных алгоритмов.

Сравнение алгоритмов

Качество алгоритма передачи оценивается по двум характеристикам: вероятности ошибки передачи и энергозатратам при передаче. Вероятность ошибки при передаче — это вероятность того, что до получателя не дойдет ни одна копия пакета. Сравнение проводится следующим образом: вычисляются энергозатраты алгоритмов при одинаковой вероятности ошибки. Для алгоритмов СП и ИП предполагается, что передача осуществляется n раз.

Вначале рассмотрим ситуацию с двумя маршрутами. Пусть имеется два независимых маршрута с характеристиками $\{p_1, E_1\}$ и $\{p_2, E_2\}$, где $p_i \in [0; 0{,}5)$ — вероятность потери пакета на маршруте i, а E_i — энергопотребление при передаче одного пакета по маршруту i. Задана вероятность ошибки при передаче p, требуется определить количество энергии, затраченное на передачу однопакетного сообщения каждым из алгоритмов.

Ниже представлены системы ограничений для каждого из алгоритмов. В методах СП и ИП для достижения необходимой вероятности ошибки требуется выполнить передачу n раз, и, соответственно, формулы имеют вид

$$\begin{cases}(0{,}5p_1 + 0{,}5p_2)^n \le p \\ E = 0{,}5n(E_1 + E_2) \to \min\end{cases};$$

$$\begin{cases}(p_1 p_2)^n \le p \\ E = n(E_1 + E_2) \to \min\end{cases}.$$

В алгоритме АИП по первому маршруту посылается n_1 копий пакета, а по второму — n_2 копий. Величины n_1 и n_2 определяются решением целочисленной оптимизационной задачи

$$\begin{cases}p_1^{n_1} p_2^{n_2} \le p \\ E = n_1 E_1 + n_2 E_2 \to \min\end{cases}.$$

Для сравнения требуется рассмотреть три случая:

1) оба маршрута имеют одинаковые характеристики;

2) один маршрут лучше другого хотя бы по одному из параметров;

3) маршруты являются несравнимыми, т. е. у одного маршрута ниже вероятность ошибки, а у другого — ниже затраты энергии на передачу одного пакета.

Пусть $k \ge 1$ и $s \ge 1$ — некоторые коэффициенты. Рассмотрим маршруты со следующими характеристиками: $\{p_1 = p_0, E_1 = sE_0\}$ и $\{p_2 = kp_0, E_2 = E_0\}$.

Тогда системы ограничений могут быть переписаны в следующем виде.

Для алгоритма СП система имеет вид

$$\begin{cases}(0{,}5p_0(1+k))^n \le p \\ E = 0{,}5nE_0(s+1) \to \min\end{cases},$$

откуда E может быть вычислено как

$$E_{\text{I}} = \frac{\log(p)E_0(s+1)}{2\log(0{,}5p_0(1+k))}.$$

Для алгоритма ИП система имеет вид

$$\begin{cases}(kp_0^2)^n \le p \\ E = nE_0(s+1) \to \min\end{cases};$$

из этой системы следует, что затраты энергии выражаются формулой

$$E_{\text{II}} = \frac{\log(p)E_0(s+1)}{\log(kp_0^2)}.$$

Для алгоритма АИП система принимает вид

$$\begin{cases}p_0^{n_1}(kp_0)^{n_2} \le p \\ E = E_0(n_1 s + n_2) \to \min\end{cases}.$$

Ограничение для алгоритма АИП может быть переписано в виде линейной функции:

$$n_1 \frac{\log(p_0)}{\log(p)} + n_2 \frac{\log(kp_0)}{\log(p)} \ge 1.$$

Тогда решением системы является одна из двух точек: $(n_1 > 0, n_2 = 0)$ либо $(n_1 = 0, n_2 > 0)$.

Таким образом, энергозатраты для данного маршрута равны

$$E_{\text{III}} = \min\left(sE_0\frac{\log(p)}{\log(p_0)}, E_0\frac{\log(p)}{\log(kp_0}\right).$$

Можно сказать, что в случае двух маршрутов алгоритм АИП всегда ведет передачу только по одному из них.

Простыми выкладками можно показать, что в первом случае (маршруты имеют одинаковые характеристики) алгоритмы обеспечивают одинаковый расход энергии. А в двух других случаях выполняется соотношение

$$E_{\text{I}} \ge E_{\text{II}} \ge E_{\text{III}}.$$

Очевидно, что наиболее предпочтительным является алгоритм адаптивной передачи, так как он обеспечивает минимальный расход энергии.

Теперь рассмотрим случай N маршрутов. Пусть имеется N маршрутов с вероятностями ошибки $\{p_i\}_{i\in[1,N]}$ и энергозатратами $\{E_i\}_{i\in[1,N]}$ и задана требуемая вероятность ошибки передачи p. Ниже приведены системы ограничений для алгоритмов СП, ИП и АИП.

Система для алгоритма СП имеет вид

$$\begin{cases} \left(\frac{1}{N} \sum_{i=1}^{N} p_i \right)^n \le p \\ E = \frac{n}{N} \sum_{i=1}^{N} E_i \to \min \end{cases};$$

из этой системы может быть получено выражение для энергозатрат при передаче одного пакета

$$E_{\text{I}} = \frac{\log(p)}{N \log\left(\frac{1}{N} \sum_{i=1}^{N} p_i \right)} \sum_{i=1}^{N} E_i.$$

Система ограничений для алгоритма ИП имеет вид

$$\begin{cases} \left(\prod_{i=1}^{N} p_i \right)^n \le p \\ E = n \sum_{i=1}^{N} E_i \to \min \end{cases},$$

откуда может быть получена формула для энергозатрат

$$E_{\text{II}} = \frac{\log(p)}{\log\left(\prod_{i=1}^{N} p_i \right)} \sum_{i=1}^{N} E_i.$$

Для алгоритма АИП система ограничений принимает вид

$$\begin{cases} \prod_{i=1}^{N} p_i^{n_i} \le p \\ E_{\text{III}} = \sum_{i=1}^{N} E_i n_i \to \min \end{cases}.$$

Эта система определяет задачу целочисленного линейного программирования. Получить конечное выражение для энергозатрат E_{III}, как это было сделано для случая двух маршрутов, не представляется возможным. Сравнение энергозатрат E_{I}, E_{II} и E_{III} будет проведено с помощью моделирования.

При моделировании использовались следующие параметры.

1. Требуемая вероятность ошибки при передаче $p = 10^{-3}$.

2. Вероятность потери пакета на маршруте p_i генерировалась как случайное число, равномерно распределенное в интервале $p < p_i \le 0{,}49$. Маршруты с большей вероятностью ошибки считаются непригодными для использования.

3. Энергозатраты на маршруте — величина E_i генерировалась как случайное число в интервале $0 < E_i \le 100$.

4. Для того чтобы протестировать алгоритмы на более сложных примерах, после генерации параметры маршрутов сортировались таким образом, чтобы маршрутам с минимальной вероятностью ошибки соответствовали максимальные временные и энергетические затраты.

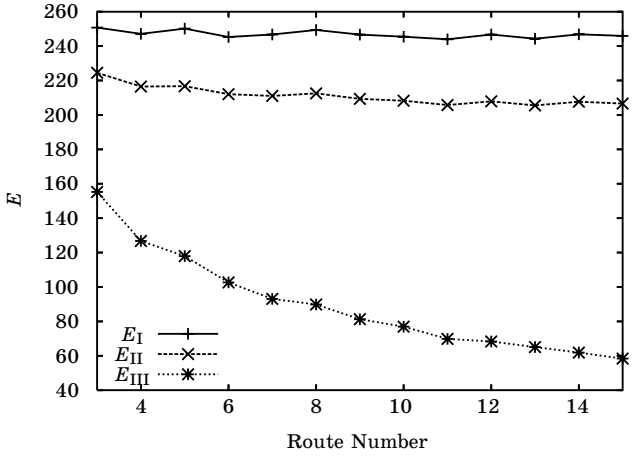
5. В соответствии с размером рассматриваемых сетей используется от 3-х до 15 маршрутов.

6. Решение оптимизационной задачи для алгоритма АИП проводилось с помощью метода ветвей и границ.

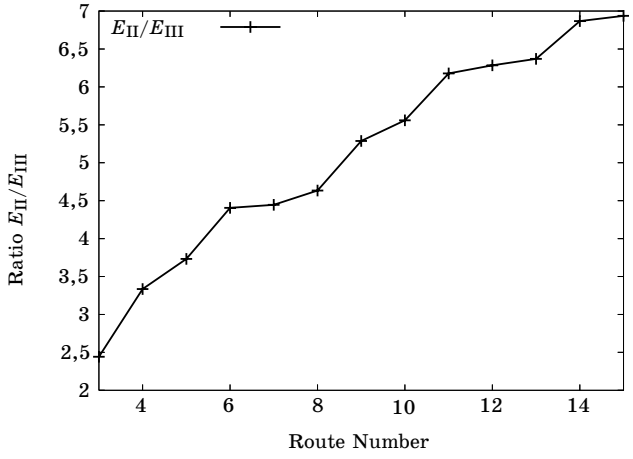
На рис. 1 представлены графики энергозатрат для алгоритмов СП (E_{I}), ИП (E_{II}) и АИП (E_{III}) в зависимости от числа используемых маршрутов.

Из графиков видно, что алгоритм АИП характеризуется наименьшими энергозатратами. На рис. 2 показано отношение энергозатрат алгоритмов ИП и АИП.

Из графика видно, что с увеличением числа маршрутов выигрыш алгоритма АИП увеличивается.



■ ***Рис. 1.*** *Энергозатраты при передаче для алгоритмов СП (E_{I}), ИП (E_{II}) и АИП (E_{III})*



■ ***Рис. 2.*** *Отношение энергозатрат при передаче для алгоритмов ИП и АИП*

Качественное объяснение полученного выигрыша может быть дано следующим образом. В алгоритмах СП и ИП не используется информация о характеристиках маршрутов, т. е. они полагаются равноценными. Поэтому выигрыш адаптивный алгоритм должен давать тем больший, чем менее равноценными данные маршруты являются.

В отличие от неадаптивных алгоритмов, для которых передача ведется по всем имеющимся маршрутам, адаптивный алгоритм на основе решения оптимизационной задачи выбирает подмножество маршрутов и передает только по ним.

Выводы

В данной статье проведено сравнение протоколов надежной передачи для сенсорной сети. Были рассмотрены протоколы случайной, избыточной и адаптивной избыточной передачи. При одинаковой вероятности ошибки передачи сравнивались суммарные энергозатраты, так как эта характеристика является особо важной для сенсорной сети. Сравнение показало, что предложенный алгоритм превосходит существующие аналоги. Преимущество алгоритма обусловлено тем, что в отличие от существующих алгоритмов он использует информацию о характеристиках маршрутов.

Литература

1. **Karlof C., Wagner D.** Secure routing in wireless sensor networks: Attacks and countermeasures // First IEEE International Workshop on Sensor Network Protocols and Applications. 2002. P. 113–127.
2. **Linsky E., Evseev G. S.** Reliable packet transmission for sensor networks // Proc. of XI international symposium on problems of redundancy in information and control systems. 2007. P. 284–288.
3. **Deng J., Han R., Mishra S.** Intrusion-tolerant routing for wireless sensor networks // Elsevier Journal on Computer Communications, Special Issue on Dependable Wireless Sensor Networks. 2005. P. 146–156.
4. **Wood D., Fang L., Stankovic J. A., He T.** SIGF: A family of configurable, secure routing protocols for wireless sensor networks // ACM SASN. 2006. P. 35–48.