文章编号: 1001-0920 (2016) 03-0435-06 DOI: 10.13195/j.kzyjc.2015.0097

一种信任和能量意识的WSN补救路由算法

胡蓉华[1,2], 董晓梅[1], 王大玲[1]

(1. 东北大学 信息科学与工程学院，沈阳 110004；2. 长江大学 计算机科学学院，湖北 荆州 434023)

摘 要: 在ARRIVE算法的基础上, 提出一种信任和能量意识的补救路由算法(TeaRR). 在选择下一跳节点时, TeaRR综合考虑候选节点的信任值和剩余能量, 选择信任值和剩余能量最优的节点转发数据. 为了防御链路不稳定和On-Off攻击造成的丢包问题, TeaRR采用发送节点主动推荐和邻居节点被动参与相结合的补救策略, 快速恢复对可能丢失包的转发. 实验结果表明, TeaRR更加适用于延时敏感的应用, 可在接收率与能耗间平衡.

关键词: 无线传感器网络；路由；信任；能量意识；补救；On-Off攻击

中图分类号: TP309 **文献标志码:** A

A trust and energy aware remedy routing algorithm for wireless sensor networks

HU Rong-hua[1,2], *DONG Xiao-mei*[1], *WANG Da-ling*[1]

(1. College of Information Science and Engineering，Northeastern University，Shenyang 110004，China；2. School of Computer Science，Yangtze University，Jingzhou 434023，China. Correspondent：DONG Xiao-mei，E-mail: dongxiaomei@ise.neu.edu.cn)

Abstract: The trust and energy aware remedy routing(TeaRR) algorithm is proposed to enhance the original ARRIVE algorithm. Considering nodes' trust and remaining energy synthetically, the TeaRR algorithm selects the nodes with the optimal trust value and remaining energy as next-hop nodes. To overcome the packet lost problem caused by the variability of link quality and the On-Off attacks, TeaRR adopts a rescue scheme, which combines sending nodes' active recommendation with neighbor nodes' passive participation, to quickly resume forwarding the possible lost packets. Experimental results show that the TeaRR algorithm is more suitable for delay-sensitive applications, and can provide a trade-off between the packet delivery ratio and the energy cost.

Keywords: wireless sensor network；routing；trust；energy awareness；remedy；On-Off attack

0 引 言

在无线传感器网络(WSN)中, On-Off转发攻击是一种影响路由传输质量且较隐蔽的攻击, 恶意节点利用无线链路质量的不稳定性, 交替性地丢包和转发包. 由于在很多延时敏感的应用中, 安全及时地将采集的数据传输至基站非常关键, 当遭受到On-Off转发攻击时, 需要一种有效的补救转发策略, 将数据包及时可靠地传输至基站. 本文将带有中间节点参与补救转发策略的路由称为补救路由, 以区分从源节点重传被丢包的路由方法.

信任路由是现有应对On-Off转发攻击的主流方法, 选择高信任值的节点转发数据包, 提高安全性和包的接收率. 然而很多基于信任机制的路由算法都存在一定的不足: 1) 路由建立需要广播认证的支持, 通信开销较大且路径建立的延时长; 2) 没有考虑节点间链路质量不稳定的特性, 缺乏有效的应对丢包的补救策略, 包的接收率较低或包的路由延时较长; 3) 下一跳节点的选择未考虑节点的能量, 使得高信任节点执行过多的转发任务而能量过早耗尽, 进而影响网络的连通性和生命周期.

为了克服已有工作的不足, 本文针对WSN中节点间链路质量不稳定性和可能遭受On-Off攻击而造成丢包的问题, 提出一种基于本地信息信任和能量意识的补救路由算法TeaRR (trust- and energy-aware

收稿日期: 2015-01-22；**修回日期:** 2015-08-24.

基金项目: 国家自然科学基金项目(60873199).

作者简介: 胡蓉华(1985−), 男, 讲师, 博士, 从事信息安全技术的研究；王大玲(1962−), 女, 教授, 博士生导师, 从事信息安全、数据挖掘等研究.

remedy routing), 其基本思想是: 1) 采用本地 (局部) 信息选择下一跳转发节点, 克服全局选择模式中通信开销大和建立延时长等缺点; 2) 采用发送节点主动推荐和邻居节点被动参与的策略, 实现对丢包的快速有效补救转发, 减少路由转发延时; 3) 考虑节点的信任值和剩余能量, 保证安全的同时实现节点间的能量均衡, 避免已有工作中仅考虑节点信任值而导致的高信任节点过早失效问题. 具体地, 基于节点的信任值和剩余能量, 节点不仅选择路由评价指标最优的节点作为下一跳主转发节点, 同时推荐候选的补救转发节点以一定概率参与补救转发, 改善了已有工作中无补救方法导致的低接收率和长延时问题, 或以预设置的较小概率参与补救转发而导致的低补救效率问题. 利用无线传输的广播特性, 当候选的补救转发节点察觉到主转发节点可能丢包后, 综合考虑推荐补救概率、自己的信任记录和剩余能量, 以一定概率转发可能被丢弃的包. 在相同条件下, 将 TeaRR 与两种典型的信任路由算法 ARRIVE[1]和 ATSR[2]进行仿真对比, 结果表明, TeaRR 在端到端的延时方面优于 ARRIVE 和 ATSR, 可在接收率和能耗间平衡.

1 信任路由

信任机制是 WSN 中一种有效的内部防御机制[3-4]. 基于信任机制的安全路由协议主要用于应对内部攻击, 利用无线传输的广播特性, 节点采用监听策略观察邻近节点的行为; 通过观察到的历史行为计算节点的信任值, 选择信任值高的节点或路径转发数据. 目前已有的基于信任机制的路由协议可分为全局选择模式 G-Scheme[5-7]和本地选择模式 L-Scheme[1-2,8]两类.

G-Scheme 需要在投递数据包前建立到达目的节点的整条路径, 可以在全局上保证较好的路由质量, 但通信开销较大且路由建立延时相对较长. 文献 [5] 提出了一种信任意识的路由协议 (TARP), 利用节点过去的路由行为和链路质量确定路由路径. 文献 [6] 设计并实现了一个信任意识的路由框架 (TARF), 提供可信且能量有效的路由. 文献 [7] 提出了一种信任意识的安全路由框架 (TSRF), 选择满足一定安全等级的最优可信路径. 这些协议都没有考虑可靠传输的问题, 当丢包比较严重时, 更换下一跳节点[5-6]或重新选择整条路径[7], 延时较长或维护开销较大.

L-Scheme 仅依赖本地路由评价信息选择最优的下一跳节点, 通信开销较小, 无路径建立延时. 文献 [1] 提出了一种基于信誉的概率路由算法 ARRIVE, 利用 WSN 节点密度高和固有的广播特性实现可靠的路由, 通过主动参与策略对可能丢弃的包补救转发. 当节点 A 观察到节点 B 没有将接收到的包转发时, 节点 A 将以较小概率负责转发. ARRIVE 的不足之处在于: 1) 下一跳节点的选择未考虑节点能量; 2) 在父节点和兄弟节点间选择时, 未考虑节点的信任值, 带来额外的传输延时和开销; 3) 仅采用主动参与策略, 不同链路质量下参与补救的概率一样, 补救效率有待提高. 文献 [2] 提出了一个基于信任和能量意识的路由协议 ATSR, 评价节点的位置、信任值和能量, 拥有最大路由评价量的节点被选择作为下一跳节点, 然而 ATSR 没有考虑延时和可靠传输的问题. 文献 [8] 提出了能量意识的信任模式 PRS 用于传感器节点的选择, 虽然提及选择一个或多个高信任值节点协作, 但具体如何协作没有讨论.

由于 WSN 中可能部署成百上千个节点, 从自适应能力、可扩展性和代价开销考虑, L-Scheme 比 G-Scheme 更具有优势, 本文路由算法 TeaRR 采用本地选择模式.

2 信任和能量意识的补救路由算法

2.1 网络模型与相关定义

本文考虑由一个基站和 N 个传感器节点组成的静态 WSN. 基站是一个功能强大的安全节点, 拥有更多资源. 网络采用了类似 LEAP+[9]的方式完成了安全初始化操作, 邻居节点间的安全通信链路已经建立. 为了节省能量, 网络采用类似文献 [10] 的节能策略, 节点轮换承担路由转发任务, 同时保证网络的连通性. 负责路由转发的节点一直处于监听状态, 其余节点处于休眠状态. 由于本文工作的重点是基于已有的信任机制设计一种有效的补救路由算法, 假设网络中存在一个安全有效的信任机制[3-4], 节点周期性地广播自己的剩余能量[2], 每个节点可以记录其邻居节点的信誉值和剩余能量.

本文主要考虑 On-Off 转发攻击, 它利用 WSN 节点间链路质量的不稳定性, 对接收到的包随机或有选择地丢弃. 正常节点很难判断丢包是由于链路质量差造成的, 还是转发节点故意丢弃的. 为了便于介绍本文的路由算法 TeaRR, 现作如下定义[1-2].

定义 1 (事件) 一个事件可以是一个单一的传感器读数, 几个邻居节点的融合结果或者任何其他感兴趣的信息. 事件由唯一的 [源 ID, 事件 ID] 对标识.

定义 2 (层次) 每个节点拥有唯一的层次号, 表示距离基站的跳距. 基站的层次为 0, 所有可以接收到基站消息的节点的层次为 1. 所有可以监听到层次 1 的节点且层次不小于 2 的节点为第 2 层次节点, 依此类推. 采用类似文献 [1,11] 的方法, 每个节点可获得自己及邻居节点的层次.

定义 3 (父亲节点集) 节点 i 的父亲节点集是在

i的通信范围内并且层次比i更接近基站的所有节点.

定义 4(兄弟节点集)　节点i的兄弟节点集是在i的通信范围内并且层次与i相同的所有节点.

定义 5(剩余能量)　节点i记录的关于节点j的剩余能量为$e_i(j)=V^j_{\text{now}}/V^j_{\text{initial}}$, V^j_{now}和V^j_{initial}分别为节点j的剩余能量容量和初始能量容量.

定义 6(信任值)　节点i记录的关于节点j的信任值$r_i(j)$由beta分布函数计算[12-13]为

$$r_i(j)=\frac{R^{j\uparrow i}+1}{S^{i\to j}+2}. \tag{1}$$

其中: $S^{i\to j}$为节点i发送给节点j的包的个数, $R^{j\uparrow i}$为节点i监听到节点j协作转发自己所投递包的个数.

定义 7(路由评价量)　节点i计算的关于节点j的路由评价量为

$$T_i(j)=\alpha\times r_i(j)+\beta\times e_i(j),$$

其中α和β为平衡因子, $\alpha+\beta=1$, 用于在信任值和剩余能量间平衡, 一般而言, 出于安全考虑$\alpha>\beta$.

本文使用的相关符号及其含义如表 1 所示.

表 1　符号及其含义

符　号	含　义
$r_i(j)$	节点i记录的关于节点j的信任值
$e_i(j)$	节点i记录的关于节点j的剩余能量
$T_i(j)$	节点i计算的关于节点j的路由评价量
$P_i=\{p^i_1,p^i_2,\cdots,p^i_m\}$	节点i的父节点集合
$p^i_{gp}\in P_i$	P_i中路由评价量最大的节点
$\text{avg}T^i_P$	P_i中平均路由评价量
$S_i=\{s^i_1,s^i_2,\cdots,s^i_n\}$	节点i的兄弟节点集合
$s^i_{gs}\in S_i$	S_i中路由评价量最大的节点
f^i_0	节点i选择的主转发节点
f^i_1	节点i选择的补救转发节点

2.2　TeaRR 算法

TeaRR算法包括3部分: 主转发节点的选择、候选补救转发节点的选择及补救转发概率的确定、补救转发.

2.2.1　主转发节点的选择

在父节点和兄弟节点间选择下一跳时, 综合考虑这些节点的信任值和剩余能量, 选择一个路由评价量最优的父节点或兄弟节点作为主转发节点, 以克服ARRIVE随机选择可能导致的额外开销.

每个节点记录的状态信息包含: 1) 自己所在的层次; 2) 每个父节点的信任值和剩余能量; 3) 每个兄弟节点的信任值和剩余能量. 对于任意节点i, 选择主转发节点f^i_0的流程如下.

Step 1: 计算父节点集合P_i中路由评价量的最大值为

$$T_i(p^i_{gp})=\max T_i(p^i_j),\ p^i_j\in P_i, \tag{2}$$

其中路由评价量的计算方法如定义 7 所示. 当信任值和剩余能量不一致, 即某一个节点的信任值相对较高而剩余能量相对较低, 另一个节点的信任值相对较低而剩余能量相对较高, 且两者的路由评价量相等时, 出于安全原则考虑, 选择信任值高的节点.

Step 2: 按照安全原则, 计算兄弟节点集合S_i中路由评价量的最大值为

$$T_i(s^i_{gs})=\max T_i(s^i_j),\ s^i_j\in S_i. \tag{3}$$

Step 3: 如果$T_i(p^i_{gp})>T_i(s^i_{gs})$, 则选择父节点$p^i_{gp}$为$f^i_0$, 否则计算$P_i$的平均路由评价量为

$$\text{avg}T^i_P=\frac{1}{m}\sum_{j=1}^{m}T_i(p^i_j). \tag{4}$$

Step 4: 如果下式成立:

$$\text{avg}T^i_P\times T_i(s^i_{gs})>T_i(p^i_{gp}), \tag{5}$$

则选择兄弟节点s^i_{gs}为f^i_0, 否则选择父节点p^i_{gp}为f^i_0.

2.2.2　候选补救转发节点的选择及补救转发概率的确定

推荐节点(发送节点)依据路由评价量推荐一个可靠的节点作为候选补救转发节点, 优先考虑路由评价量高的节点作为补救转发节点, 以提高路由的可靠性和补救模式的效率; 依据故意丢包的概率Pr_{del}和包的优先级(重要程度)计算补救转发概率, Pr_{del}越大, 包的优先级越高, 补救转发概率应该越大.

对于任意发送节点i, 选择候选补救节点f^i_1的方法与选择f^i_0的方法类似, 选择路由评价量最高的节点(f^i_0除外)作为补救转发节点.

为了提高补救的效率, 可依据Pr_{del}推荐补救转发概率fwdPr. 如图 1 所示, 假设节点A选择节点B将数据包投递至节点D, 节点C为补救转发节点. 当C监听到B没有转发数据包时, 以一定补救概率参与补救转发. 设每条链路的平均质量均为avgLq, 则B成功接收到A发送的包的概率为avgLq, 即正常情况下B转发包的可能性为avgLq; B为非恶意节点时, C未监听到B转发数据包的概率为$1-\text{avgLq}^2$, 则C由式(6)估计B故意丢包的概率为

$$\text{Pr}_{\text{del}}=\text{avgLq}-(1-\text{avgLq}^2). \tag{6}$$

显然, Pr_{del}越大, fwdPr也应该越大. 有

$$\text{fwdPr}_i=\begin{cases}\gamma\times[\text{avgLq}_i-(1-\text{avgLq}_i^2)]+1-\gamma,\\ \qquad f^i_1\in\text{nbr}(f^i_0);\\ \{\gamma\times[\text{avgLq}_i-(1-\text{avgLq}_i^2)]+1-\gamma\}\times\\ (1-\text{avgLq}_i^2),\ f^i_1\notin\text{nbr}(f^i_0).\end{cases} \tag{7}$$

其中: $\text{nbr}(f^i_0)$为f^i_0的邻居节点集合; $\gamma(0\leqslant\gamma\leqslant1)$为调节因子, γ取值越大, 表示fwdPr越依赖Pr_{del}, 反

之 fwdPr 对 $\mathrm{Pr_{del}}$ 依赖程度越低.

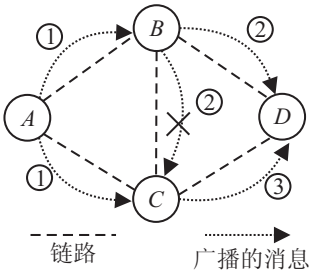

图 1 故意丢包概率计算

γ 的取值可依据包的优先级设置. 包的优先级越高, γ 应该越小, 节点参与补救转发的概率越大, 网络消耗的能耗可能越多. 例如在图 1 中, 如果 $\gamma = 0$, 则当 B 实际转发了 A 投递的数据包而 C 没有监听到时, C 将以概率1参与补救转发, 会增加一定的能耗开销. 节点在发送数据包时, 采用捎带方式将选择的推荐节点和对应概率嵌入在包中.

2.2.3 补救转发

依据对推荐节点的信任记录、推荐节点给出的转发概率和自己的剩余能量, 候选转发节点决定是否对可能丢弃的包进行补救转发. 推荐节点越可信、给出的转发概率越大以及自己有足够的剩余能量, 则参与补救转发的可能性越大.

同文献 [1-2, 5-6] 一样, 假设有一个预定义的可协作信任阈值 Thr_g, 当节点的信任值不小于该值时, 该节点为可协作节点. 当节点察觉到数据包可能被丢弃后, 参与补救转发遵循以下原则:

1) 当 $f_1^i \in \mathrm{nbr}(f_0^i)$ 时, 如果

$$r_{f_1^i}(i) \geqslant \mathrm{Thr}_g,\ r_{f_1^i}(f_0^i) \geqslant \mathrm{Thr}_g,$$

则 f_1^i 按照 i 的推荐概率参与补救转发, 否则, f_1^i 不参与补救转发.

2) 当 $f_1^i \notin \mathrm{nbr}(f_0^i)$ 时, 如果 $r_{f_1^i}(i) \geqslant \mathrm{Thr}_g$, 则 f_1^i 按照 i 的推荐概率参与补救转发, 否则, f_1^i 不参与补救转发. 注意到, 当 i 不知道 f_0^i 的邻居信息时, 可周期性地将 avgLq_i 以捎带方式嵌入在发送的包中, 其 fwdPr_i 可按照假设 $f_1^i \in \mathrm{nbr}(f_0^i)$ 的条件计算. f_1^i 接收到 i 发送的数据包后自己可以判断是否为 f_0^i 的邻居节点, 如果 $f_1^i \notin \mathrm{nbr}(f_0^i)$, 则可以依据 $\mathrm{fwdPr}_i \times (1 - \mathrm{avgLq}_i^2)$ 的概率参与补救转发.

2.3 对比分析

本文方法与其他基于信任的路由方法比较如表 2 所示. 由表 2 可见, 本文方法与已有的典型方法相比主要不同之处在于选择模式和补救策略上.

从整体上, 出于自适应性、可扩展性和代价开销等方面的考虑, 本地模式比全局模式更具有优势, 因此本文方法也采用了本地选择模式. 在具体选择下一跳转发节点的方法上, TeaRR 在父节点与兄弟节点中选择时考虑了平均路由评价量, 与 ARRIVE 的随机选择相比, 会选择出表现更好的节点, 因此在延时和通信开销方面表现更优. 与 ATSR 简单考虑节点与基站的距离来计算路由评价量相比, TeaRR 不仅考虑了距离 (即节点距离基站的层次), 而且考虑了实际的链路状况 (即平均路由评价量), 考虑更加全面. 同时获得节点的层次比取得节点与基站的距离更加容易, 不需要定位设备和安全的定位算法[14-15]支持, 辅助的通信开销和硬件代价也更小.

在补救策略上, TeaRR 依靠发送节点选择出优秀的候选补救转发节点, 并依据当前链路的平均质量和包的优先级给出补救转发概率, 与 ARRIVE 预设置某一较小的补救概率相比, 更加合理且有效. 与 TARF 或 TSRF 仅在转发节点表现很差或信任值波动较大时才重新选择转发节点或重新建立路径相比, 更加及时和有效.

3 仿真实验

为分析本文所提出的 TeaRR 协议的性能, 使用 Castalia 构建了 TeaRR、ARRIVE 和 ATSR 三种协议的仿真模型, 并进行了仿真实验. 其中, ARRIVE 是一种基于信任的概率路由方法, 在父节点和兄弟节点中随机选择一个可信节点作为下一跳节点, 邻居节点察觉到可能丢包时以较小的概率补救转发; ATSR 是一种基于信任和能量意识的路由方法, 拥有最大路由评价量的节点被选择作为下一跳节点, 无补救策略.

实验参数设置如下: 100 个传感器节点以 10×10 格的形式部署在 450 m×450 m 的区域, 基站位于部署区域的中心, 节点的通信半径为 72 m, $\alpha = 0.7$, $\gamma = 0.5$, $\mathrm{Thr}_g = 0.2$, 节点发射和接收能耗分别为 $e_{tx} = 1.625\,\mu$J/byte, $e_{rx} = 1.25\,\mu$J/byte,节点的初始能量容量为 10 J. 网络中节点间的初始信任关系已经建立. 对于任意邻居节点对 i 和 j, $S^{i\to j} = 100$, 当 avgLq = 0.9 时, $R^{j\uparrow i} = 100 \times \mathrm{avgLq}^2 = 81$; 当 avgLq = 0.95 时, $R^{j\uparrow i} = 90$. 坐标为 (200, 0) 的事件源节点每秒产生 1 个数据包, 共产生 600 个数据包, 包的负载为 100 字节, TeaRR 和 ARRIVE 的额外开销分别为 6 字节和 4 字节; 坐标为 (150, 50)、(150, 100)、(150, 150) 的节点为 On-Off 攻击节点, 以 0.6 的概率转发接收到的数据包; ARRIVE 中的投递概率初始值设置为 0.7. 每组实验进行 100 次模拟, 所有结果由 100 次实验结果取平均值后得到.

在仿真实验中, TeaRR 的部分实现过程如下:

1) TeaRR 路由选择过程. ① 按式 (4) 计算父节点的平均路由评价量; ② 按式 (5) 从父节点和兄弟节点中选择最优的节点作为主转发节点; ③ 按照类似

② 的方法, 在父节点和兄弟节点中选择主转发节点最优的邻居节点作为补救转发节点, 并依据 avgLq 和 γ, 按式 (7) 计算补救转发概率 fwdPr.

2) 候选节点监听补救转发过程. 某节点在得知自己为补救转发节点后, 设置一计时器, 并监听主转发节点是否投递相应的数据包. 若在计时器结束时仍然没有监听到主转发节点投递对应的数据包, 则按照补救转发概率执行补救转发任务.

3) 接收率统计. 由基站统计成功接收到的总的数据包个数.

4) 端到端延时统计. 每转发一跳, 延时增加一个单位.

5) 能耗统计. 节点发送、接收或监听到包后, 依据包的字节大小和实验参数设置的发送/接收能耗, 计算相应的能耗.

实验结果如图 2 ~ 图 4 所示, 其中“*-no”表示无攻击的情况; “ATSR-Re”表示采用 ATSR 重传补救策略, 即当投递节点观察到下一跳未转发数据包时, 重新选择下一跳发送; “TeaRR-Const”表示采用 TeaRR 模式时, 补救转发概率 fwdPr = 1, 即 $\gamma = 0$.

由图 2 可见, TeaRR-Const 在接收率方面表现最好, TeaRR 和 ATSR-Re 相当, 它们的接收率明显高于 ARRIVE 和 ATSR. 由图 3 可见, TeaRR、TeaRR-Const 在端到端的延时方面都要明显优于 ARRIVE、ATSR 和 ATSR-Re, 其中 TeaRR-Const 略优于 TeaRR. 由图 4 可见, ATSR 平均能耗表现最好, 在存在攻击的情况下, TeaRR、TeaRR-Const 和 ATSR-Re 能耗相当, 在正常情况下, TeaRR-Const 的能耗高于 TeaRR 和 ATSR-Re, TeaRR 的能耗略高于 ATSR-Re. 本文方法与相关工作的对比如表 2 所示.

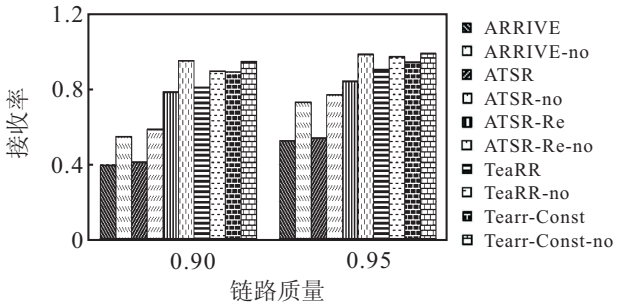

图 2　数据包投递率比较

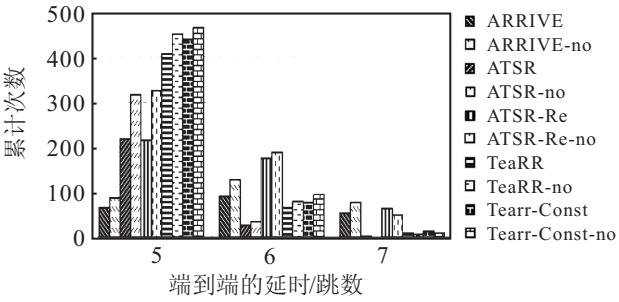

图 3　avg$Lq = 0.9$ 时端到端的延时分布比较

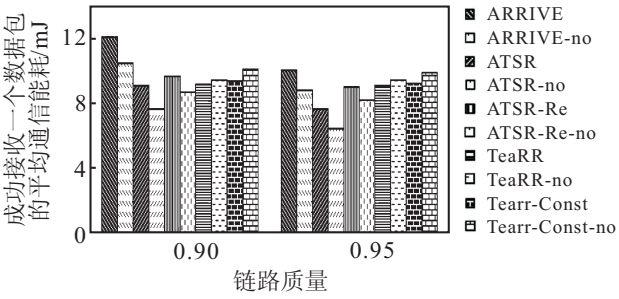

图 4　能耗对比

表 2　本文方法与相关工作对比

方 法	信任因素	能耗因素	选择模式	补救策略
TARP[5]	√	×	全局选择: 从基站的邻居节点开始, 依据节点的信誉值和链路质量来确定有效的路径	无明确说明
TARF[6]	√	√	全局选择：从基站的邻居节点开始, 基于信任等级和能量代价, 节点从邻居节点中选择最优的下一跳节点	如果当前的下一跳节点执行接收和投递数据包任务表现很差时重新选择下一跳节点
TSRF[7]	√	√	全局选择: 从源节点开始, 在路径选择中加入路径信任阈值, 路径信任值大于信任阈值的节点为侯选转发节点, 直到找到一条最优的路径	当发现转发节点的信任值波动超过给定阈值时, 从源节点开始重新建立路径
ATSR[2]	√	√	本地选择：下一跳的选择同时考虑节点与基站的距离, 拥有最大路由评价量的节点被选择作为下一跳节点	无明确说明
ARRIVE[1]	√	×	本地选择：在父节点和兄弟节点中随机选择一个可信节点作为下一跳节点	邻居节点主动参与补救, 察觉到可能丢包时以较小概率补救转发, 补救效率依赖选取的补救概率
本文方法	√	√	本地选择：选择一个路由评价量最优的父节点或兄弟节点作为主转发节点；在父节点与兄弟节点间选择时考虑了平均路由评价量	发送节点主动推荐和邻居节点被动参与, 察觉到可能丢包时被选中的补救转发节点依据推荐的补救转发概率补救转发, 补救转发概率考虑了当前链路的平均质量和包的优先级

综上所述, 当同时考虑接收率和能耗时, ATSR-Re 和 TeaRR 是较好的选择; 如果再考虑延时, 则 TeaRR 是较好的选择; 进一步考虑网络包的优先级, 对于优先级高的网络包, TeaRR-Const 是较好的选择. 即 TeaRR 可在接收率和能耗间平衡, 对于优先级较高的包, 为了保证较高的包的接收率, 可以将 γ 设置为相对较小的值; 对于优先级较低的包, 在保证一定水平的包接收率的情况下, 为了减少补救转发产生的能耗开销, 可以将 γ 设置为相对较大的值.

4 结 论

本文提出了一种信任和能量意识的补救路由算法 TeaRR, 通过采用发送节点主动推荐和邻居节点被动参与的策略, 实现了对丢包的快速有效补救转发, 减少了路由转发延时, 可有效防御由于链路不稳定和 On-Off 转发攻击造成的丢包问题. 通过考虑估计的故意丢包概率和包的优先级, 给出了针对不同的应用需求推荐相应的补救转发概率的方法. 通过仿真对比实验, 表明了 TeaRR 更适用于延时敏感的应用, 可在接收率和能耗间平衡.

参考文献(References)

[1] Karlof C, Li Y P, Polastre J. ARRIVE: Algorithm for robust routing in volatile environments[R]. California: University of California at Berkeley, 2003: 1-11.

[2] Zahariadis T, Leligou H C, Voliotis S, et al. Energy-aware secure routing for large wireless sensor netoworks[J]. WSEAS Trans on Communications, 2009, 8(9): 981-991.

[3] Khalid O, Khan S U, Madani S A, et al. Comparative study of trust and reputation systems for wireless sensor networks[J]. Security and Communication Networks, 2013, 6(6): 669-688.

[4] Han G J, Jiang J F, Shu L, et al. Management and applications of trust in wireless sensor networks: A survey[J]. J of Computer and System Sciences, 2014, 80(3): 602-617.

[5] Rezgui A, Eltoweissy M. TARP: A trust-aware routing protocol for sensor-actuator networks[C]. IEEE Int Conf On Mobile Adhoc and Sensor Systems. Pisa: IEEE, 2007: 1-9.

[6] Zhan G X, Shi W S, Deng J L. Design and implementation of TARF: A trust-aware routing framework for WSNs[J]. IEEE Trans on Dependable and Secure Computing, 2012, 9(2): 184-197.

[7] Duan J Q, Yang D, Zhu H Q, et al. TSRF: A trust-aware secure routing framework in wireless sensor networks[J]. Int J of Distributed Sensor Networks, 2014(2014): 1-14.

[8] Han G J, Shu L, Ma J H, et al. Power-aware and reliable sensor selection based on trust for wireless sensor networks[J]. J of Communications, 2010, 5(1): 23-30.

[9] Zhu S C, Setia S, Jajodia S. LEAP+: Efficient security mechanisms for large-scale distributed sensor networks[J]. ACM Trans on Sensor Networks, 2006, 2(4): 500-528.

[10] Xu Y, Heidemann J, Estrin D. Geography-informed energy conservation for ad hoc routing[C]. Proc of the Annual Int Conf on Mobile Computing and Networking. Rome: ACM, 2001: 70-84.

[11] Han K H, Ko Y B, Kim J H. A novel gradient approach for efficient data dissemination in wireless sensor networks[C]. IEEE 60th Vehicular Technology Conf. Log Angeles: IEEE, 2004: 2979-2983.

[12] Josang A, Ismail R. The beta reputation system[C]. Proc of the 15th Bled Conf Electronic Commerce. Bled: Slovenia, 2002: 1-14.

[13] Ganeriwal S, Balzano L K, Srivastava M B. Reputation-based framework for high integrity sensor networks[J]. ACM Trans on Sensor Networks, 2008, 4(3): 1-37.

[14] Zhang Y C, Liu W, Fang Y G. Secure localization in wireless sensor networks[C]. Proc of the IEEE Military Communications Conf. New Jersey: IEEE, 2005: 1-7.

[15] Liu D G, Ning P, Du W L. Attack-resistant location estimation in sensor networks[C]. Proc of the 4th Int Symposium on Information Processing in Sensor Networks. New Jersey: IEEE, 2005: 99-106.

(责任编辑：郑晓蕾)