基于能量优化的无线传感器网络安全路由算法

周贤伟,覃伯平
(北京科技大学信息工程学院,北京 100083)

摘 要: 针对无线传感器网络路由面临安全威胁和节点能量有限的不足,提出一种基于能量优化的安全路由算法(EOSR). 该算法把优化能量、提高路由安全性和缩短传输时延同时作为设计目标,采用多目标决策,在保证安全性和快速传输的同时,让能量储备较多的节点承担较多的数据转发任务,可获得最优路由和延长网络生命期. 通过预置公私密钥对,有效地提高了路由的安全性. 给出了该算法中路由发现、路由选择和路由删除的具体步骤,通过仿真实验证明该算法的有效性.

关键词: 无线传感器网络; 网络安全; 路由算法; 能量优化; 多目标决策
中图分类号: TP393.08 **文献标识码**: A **文章编号**: 0372-2112 (2007) 01-0054-04

Secure Routing Algorithm Based on Energy Optimization for Wireless Sensor Networks

ZHOU Xian-wei, QIN Bo-ping
(School of Information Engineering, University Science and Technology of Beijing, Beijing 100083, China)

Abstract: To the problems of threat to routing security and limited energy of the nodes in sensor network, this paper presents a secure routing algorithm based on energy optimization (EOSR). The algorithms takes energy optimization, improvements of secure routing, and shorten of transmission delay as its design targets. With the multi-pile policy nodes with more energy storages will undertake more tasks of data switching, which can obtain optimal routing and prolong network lifetime. Security of routing is also efficiently improved through pre-distribution of public and private key pair. Detailed process of routing finding, routing choosing and routing deleting are given in this paper. The affectivity of this algorithm is proved with emulative experiment.

Key words: wireless sensor networks; network security; routing algorithm; energy optimization; multi-pile policy

1 引言

无线传感器网络是由一组能量有限的传感器节点通过无线介质自组织构成,不需要固定网络支持,具有快速展开,抗毁性强等优势的无线网络[1]. 它是一种特殊的无线 Ad Hoc 网络,有节点能量有限、无全局标识、节点数量大且密集、数据冗余大的特点[2,3]. 其节点不仅有信息感知和数据通信的能力,还需兼备路由器的功能,因此,包括 Ad Hoc 网络在内的传统网络路由技术都无法直接应用到无线传感器网络中.

针对无线传感器网络中数据传送的特点,已经提出许多新的较为合适有效的路由技术. 就路由算法而言,按实现方法划分,有洪泛式路由(如 Gossiping)、以数据为中心的路由(如 Directed Diffusion)、层次式路由(如 LEACH)、基于位置信息的路由(如 GPSR)等[4~7]. 但是,这些针对无线传感器网络提出的路由算法,只对节点有限的性能和网络特性的应用进行了尽可能的完善,却没有考虑安全问题.

考虑无线传感器网络的特性,它将面临比传统网络更多的威胁[8]. 针对路由将面临如虚假路由信息、选择性转发、Sybil 攻击和 HELLO flood 攻击、确认欺骗、sinkhole 攻击和 Wormholes 攻击等[9],已提出了一些安全路由协议,如基于 Dimeter 协议的安全路由 DSR[10],容侵路由 INTRSN[11]等. 这些安全路由协议一般采用链路层加密和认证、多路径路由、身份认证、双向连接认证和认证广播等机制来有效抵御有关攻击. 但是这些安全路由协议并没把节点能耗作为设计目标.

本文把能量优化、路由安全性和传输时延同时作为路由算法设计目标,提出一种能量优化的安全路由算法(EOSR). 通过预置公私密钥对来增加安全机制,采用让能量储备较多的节点承担较多的数据转发任务,以延长能量储备较少的节点的生存时间,进而延长整个网络的生命周期.

本文的其余部分组织如下:第 2 节介绍所提路由算法的网络模型;第 3 节描述安全路由算法的具体过程;第 4 节通过实验验证算法的有效性;全文总结在第 5 节中给出.

收稿日期:2006-01-19; 修回日期:2006-05-11
基金项目:国家自然科学基金(No. 60573050);北京市优秀人才培养专项基金(No. 20042D0500103)

2　网络模型

假设无线传感器网络的节点是随机而稠密地分布在一个区域内,每个节点在网中有唯一地址标识符,并且其发射功率为固定值,但是不同节点可能有不同的发射功率.

为便于表述,作如下记号和定义:

V_i 表示地址标识符为 i 的节点;$V=\{V_i \mid V_i$ 表示地址标识符为 i 的节点$\}$,则 V 为有限集合,其元素个数为网络节点数 n;$W=\{w_{ij} \mid w_{ij}$ 为 V_i 到 V_j 的无线链路边$\}$;E_i 为 V_i 的现存能量;$e_{\text{out},i}$ 为 V_i 发送单位数据所需能量;$e_{\text{com},i}$ 为节点 V_i 解密(加密)计算单位数据所需能量.

定义 1:设节点 V_i 的传播半径为 R_i,如果物理距离 $|V_j - V_i| \le R_i$,则称 V_j 为 V_i 的邻居节点. 记 $N_i=\{V_j \mid V_j \in V$,且 $|V_j - V_i| \le R_i\}$.

定义 2:在无线传感器网络中,当网络中存活节点的数量所占比例低于某一门限值的时候,则认为其寿命已经到期[12].

定义 3:数据从源节点传输到目的节点所用的时间称为传输时延;所有数据包传输时延的平均值称为平均时延. 在上述假设下,同一数据包的传输时延仅与数据传输所经历节点数目相关.

根据上述定义和假设,源节点 S 向目的节点 D 发送数据时,无线传感器网络可以抽象为一个有向图 $G(V,W)$.

设 $P=\{P_k \mid P_k$ 表示所有 S 到 D 的路径$\}$,M_k 表示路径 P_k 所包含节点的数目.

f_{ij} 为 V_i 发送到 V_j 的数据流,因此,节点 V_i 发送的数据流总和为

$$F_i=\sum_{j\in N_i} f_{ij} \tag{1}$$

由于对所有路由信息采取加密和数字签名算法,节点 V_i 在转发和接收数据包时,需经数字签名或解密,从而节点 V_i 的生存时间为:

$$T_i=\frac{E_i}{(e_{\text{out},i}+e_{\text{com},i})F_i}=\frac{E_i}{(e_{\text{out},i}+e_{\text{com},i})\sum_{j\in N_i} f_{ij}} \tag{2}$$

因此,节点 V_i 的生存时间 T_i 将直接影响到网络的生命期.

3　算法描述

为解决计算开销和提高路由的安全性,在节点部署之前,一般把密钥预先配置在节点中. 这里采用 Du W 等人提出的成对密钥预置方案(Pairwise key pre-distribution scheme)[13],邻居节点相互拥有的成对密钥分别为公钥和私钥.

由于节点能量的消耗和不安全因素等,无线传感器网络路由具有较大的动态性,如中间节点的现存能量不能完成一次数据转发任务时,该路径失效,当有效路径数目小于某一阈值时,就触发新的路由发现过程.

3.1　路由发现

当源节点 S 需要向目的节点 D 进行通信时,节点 S 开始路由发现过程,其步骤如下:

第一:S 构造一个路由请求消息包(RREQ),向邻居节点进行广播.

RREQ = (Kps[time,S,D],random,Hopcount,Emin,Path)

其中 time 表示发包时间戳序列号,S、D 分别表示源节点和目的节点的标识符,Kps[S,D]表示用 S 的私钥 Kps 对 time、S 和 D 进行加密,random 表示节点 S 产生的随机数,Hopcount 表示转发跳数,Emin 表示消息所经路径各节点最小现存能量(这里 Emin = Es),Path 表示消息所经历的路径.

第二:中间结点转发路由请求消息.

中间节点 V_i 收到路由请求消息后,首先用自身拥有的公钥 Kus 解密,然后查看时间戳 time 是否过期,如果大于预定阈值(过期),则丢弃该消息,否则进一步查看是否被转发过;如果该消息被转发过则丢弃该消息,否则中间节点 V_i 把自身的地址标识符 i 加入 Path 域,同时把 Hopcount 加 1,Emin = min{接受消息中的 Emin,Ei},用 V_i 的私钥 Kpi 加密 time、S 和 D 后转发该路由请求消息.

第三:目的节点收到路由请求消息后,在限定的时间内,目的节点会收到 S 到 D 的不同路径的路由请求信息,建立可行路径集合 Pathset(S,D),构造一个路由应答消息(RREP),按照原路向回转发. 路由应答消息(RREP)格式如下:

RREP = { Kpd[time,S,D],random,Hopcount,Emin,Path,Pathset(S,D)}

第四:确认路由应答信息. 和转发路由请求消息一样,中间节点 V_i 转发的路由应答消息到达源节点 S 后,经拥有的公钥 Kui 解密,核实 random,构建可行路由集合 P = Pathset(S,D),路由发现结束,触发路由选择过程.

3.2　路由选择

根据网络模型,一方面,为使得整个网络生命期延长,关键在于作路由选择时,让现存能量较多的节点承担较多的数据转发和计算任务,也就是使得生存时间最小的节点的生存时间达到最大为最优路由,即 $\min T_i \to \max$.

另一方面,为提高网络性能,要求传输时延尽量最小. 按照网络模型假设,节点是稠密随机分布在区域内,可以认为是均匀分布的. 因此,传输时延小,相当于所选择最优路由的跳数少,即 $M_k \to \min$.

则路由选择问题转化为多目标决策问题,即

求解最佳路由 P_k,使 $\max(\min T_i)$、$\min M_k$ 的约束条件为

$$\begin{cases} f_{ij}\ge 0,\ \forall V_i\in P_k,\ \forall V_j\in N_i \\ 1\le M_k\le n \\ E_i\ge 0,\ \forall V_i\in P_k \end{cases} \tag{3}$$

这是非线性两目标决策问题,具体步骤为:

第一:先解 $\min M_k$. 根据路由发现阶段构成的可行路径集合 P,求出路径的最短跳数 m 和最大跳数 M. 构造满意度函数

$$y=\cos\left[\frac{\pi(x-m)}{2(M-m)}\right] \tag{4}$$

这里 x 是路径的跳数,y 指网络性能满意度.

第二:再解 $\max(\min T_i)$. 对于已构成的可行路径集合 P,

设 $w_{ij} = \min T_i$,则问题转化为在有向加权子图 $G_p(V_p, W_p)$ 中可求出满足 $\max(\min T_i)$ 条件的路径即可. 也就是求出满足 $w_{ij} = \max\{w_{ik}, w_{il}, \cdots\}$ 的最佳路径 $P_{k-T} \in P$,即: $P_{k-T} = (V_s, \cdots, V_i, V_j, \cdots, V_D)$,设其跳数为 X_{k-T}.

第三:判断满意路径. 把 X_{k-T} 代入式(4),求出的满意度如果符合要求,则 P_{k-T} 即为所选最优路由;否则在集合 $P - \{P_{k-T}\}$ 中重复第二、三步,直到满足要求为止.

3.3 路由删除

当某一节点 V_i 由于能量问题,或受到攻击等因素发生异常,它将向源节点发送请求退出的报警包,源节点收到 V_i 的报警信息后,以广播形式发送 RD(Routing Delete)包,发起路由删除过程,把含有节点 V_i 的路由全部删除.

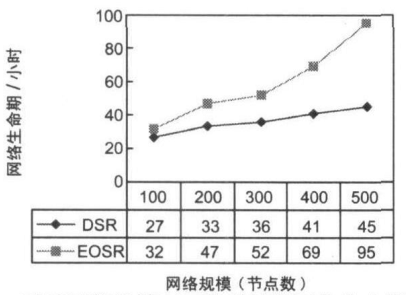
3.4 算法分析

由于算法把能量优化、安全性和传输时延同时作为设计目标,避免在已设计好的路由算法上再次增加某些性能,降低了设计成本;通过在节点部署前预置加公私密钥对,增加了算法的安全性;算法进行路由选择时,以最少转发跳数作为选择条件,缩短了数据传输时延;采用让能量储备较多的节点承担较多的数据转发任务,以延长能量储备较少的节点的生存时间,进而延长了整个网络的生命期. 因此,算法具有安全性,并降低了设计成本、缩短传输时延和延长网络生命期.

4 模拟结果

用仿真分析的方法来对安全路由算法进行性能评估,由于已增加安全机制,算法本身具备安全性,现主要分析传输时延和网络生命期. 仿真工具采用 NS2 平台,通过与 DSR 算法在不同环境下的比较来验证 EOSR 算法的有效性.

仿真环境中,节点位置随机分布在 500m ×500m 的矩形区域内,通信带宽是 1Mkbs,MAC 层采用 802.11 协议,节点传输半径 R_i = 10m,每个节点的初始能量为 1000J,采用通用的 CENT 公司 RSA 芯片来预置密钥对,选取 RSA 中的 e 值为 3,网络生命期的门限值选取为 10. 在同一矩形区域内,网络规模分别为节点数 n = 100,200,300,400,500 时,对 EOSR 算法和 DSR 算法的网络生命期作比较,结果如图 1 所示.

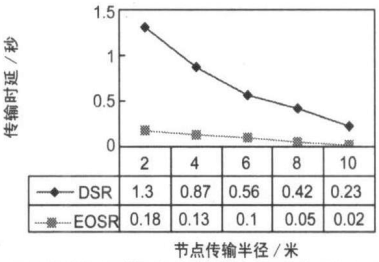


	100	200	300	400	500
DSR	27	33	36	41	45
EOSR	32	47	52	69	95

图 1 不同网络规模下三种算法的网络生命期比较

从图 1 可以看出,网络规模增大时,可选路由数目增多,两种算法的网络生命期呈递增的趋势. 由于 DSR 算法仅考虑安全性,而没把节点能耗作为设计目标,其网络生命期增加不大;EOSR 算法在此实验中,当网络规模节点数达 500 个的时候,其网络生命期已近 100 小时,说明随着网络规模的增大,它能延长网络生命期的性能越明显.

在上述同样的网络环境下,设网络规模节点数为 n = 200,当传输半径为 2m、4m、6m、8m、10m 时,对 EOSR 和 DSR 算法的传输时延作比较,结果如图 2 所示.



	2	4	6	8	10
DSR	1.3	0.87	0.56	0.42	0.23
EOSR	0.18	0.13	0.1	0.05	0.02

图 2 不同网络规模下三种算法的传输时延期比较

从图 2 中可以看出,节点传输半径增大时,传输所需的跳数减少,数据包传输时间将减少,则两种算法的传输时延呈递减的趋势. 由于 DSR 算法没有考虑最少跳数最为最优,其传输时延明显最长;EOSR 算法的波动不大,平均时延不超过 0.15 秒,而 DSR 算法的平均时延达到 0.5 秒以上,最高达 1.3 秒,说明 EOSR 算法对缩短传输时延有明显效果.

5 结论

无线传感器网络路由面临的特殊威胁和节点资源受限的特点,使得安全路由算法的研究成为热点. 本文把能量优化、安全性、传输时延同时作为设计目标,提出了一种安全路由算法. 该算法具有设计简单、针对性强和安全性高等特点;和相关算法相比,降低了设计成本,缩短了传输时延并延长了网络生命期.

但是,该算法在触发路由发现时,引入预定阈值来与有效路径数目比较,以判断路由发现时机,精确性不够,还须做进一步的改进和完善. 在以后的工作中,将根据无线传感器网络的具体应用环境,把信息的采集、处理、传输和安全性融为一体,设计出高效适用的安全路由算法.

参考文献:

[1] I F Akyildiz, W Su, Sankarasubramaniam Y, et al. Wireless sensor networks: a survey [J]. Computer Networks, 2002, 38(4): 393 - 422.

[2] B Krishnamachari. Impact of data aggregation in wireless sensor networks [A]. Proceeding of the International Workshop of Distributed Event Based Systems [C]. Los Alamitos: IEEE Computer Press, 2002. 1 - 11.

[3] 李建中,李金宝,石胜飞. 无线传感器网络及其数据管理的概念、问题与进展 [J]. 软件学报, 2003, 14(10): 1717 - 1727.
J Z Li, J BLi, S F Shi. Concepts, issues and advance of sensor networks and data management of sensor networks [J]. Journal of Software, 2003, 14(10): 1717 - 1727. (in Chinese)

[4] S Hedetniemi, A Liestman. A survey of gossiping and broadcasting in communication networks [J]. Networks, 1998, 18

(4) :319 - 349.

[5] Chalemek Intanagonwiwat, ramesh Govindan, Deborah Estrin, et al. Directed diffusion for wireless sensor networking[J]. IEEE/ACM transactions on networking, 2003, 11(1) :1 - 16.

[6] W R Heinzelman, A Chandrakasan, H Balakrishnan. An application-specific protocol architecture for wireless microsensor networks[J]. IEEE Transactions on Wireless Communications, 2002, 1(4) :660 - 670.

[7] K Brad, H T Kung. GPSR: Greedy perimeter stateless routing for wireless networks[A]. Proceeding of the 6th Annual International Conference on Mobil Computing (MobiCom '2000) [C]. Boston, MA, USA, 2000. 243 - 254.

[8] Haowen Chan, A Perrig. Security and privacy in sensor networks[J]. Computer, 2003, 36(10) :103 - 105.

[9] C Karlof, D Wagner. Secure routing in wireless sensor networks: attacks and countermeasures[J]. Ad Hoc Networks, 2003, 1(3) :293 - 315.

[10] Changqing Yin, Shaoyin Huang, Pengcheng Su, et al. Secure routing for large-scale wireless sensor networks[A]. Proceedings of the 2003 International Conference on Communication Technology (ICCT '2003) [C]. Beijing, China, 2003. 1282 - 1286.

[11] J Deng, R Han, S Mlshra. INTRSN: Intrusion-tolerant routing in wireless sensor networks[A]. Proceedings of the 23rd IEEE International Conference on Distributed Computing Systems (ICDCS '2003) [C]. Providence, RI, 2003. 65 - 71.

[12] Marco Zuniga, Bhaskar Krishnamachari. Integrating future large scale sensor networks with the Internet[R]. USC Computer Science Technical Report, 2003. 03 - 792.

[13] W Du, J Deng, Y S Han, P K Varshney. A pairwise key predistribution scheme for wireless sensor networks[A]. Proceeding of the 10th ACM Conference on Computer and Communications Security (CCS '2003) [C]. Washington, DC, USA, 2003. 42 - 51.

作者简介:

周贤伟　男, 1963 年生于四川成都, 北京科技大学信息工程学院教授、博士生导师, 主要研究领域为网络安全、移动通信、无线传感器网络. E-mail: xwzhouli @sina. com

覃伯平　男, 1971 年生于四川江安, 2002 年毕业于北京航空航天大学, 获硕士学位, 现于北京科技大学信息工程学院攻读博士学位, 主要研究方向包括网络安全、无线传感器网络及路由协议. E-mail: qinbp @163. com