圆分布双跳无线传感器网络网络配置及拓扑发现修复算法与仿真*)

张金荣[1] 曹长修[1] 唐贤伦[2]

(重庆大学自动化学院 重庆 400030)[1] (重庆邮电大学自动化学院 重庆 400065))[2]

摘 要 无线传感器网络在从战场到环境监测的许多领域都表现得越来越重要。本文首先给出了一类圆分布双跳无线传感器网络，并提出其安全性要求和模型。对于其面临的威胁，在权衡网络资源局限性的基础上，提出了相应解决方案，包括拓扑发现算法、网络配置协议和网络修复算法(TDNSR)。仿真结果表明：和SPIN算法相比，TDNSR能迅速实现网络拓扑发现和配置并修复，能有效减少资源开销。

关键词 无线传感器网络，网络配置，拓扑发现，网络安全，能量有效性

Algorithm and Simulation of Network Setup and Topology Discovery for Circle-distributed 2-hops WSN

ZHONG Jin-rong[1] CAO Chang-xiu[1] TANG Xian-lun[2]

(College of Automation, Chongqing University, Chongqing 400030, China)[1]

(College of Automation, Chongqing University of Posts and Telecommunications, Chongqing 400065, China)[2]

Abstract Wireless sensor networks (WSN) have been identified as being useful in a variety of domains from the battlefield to environmental monitoring. We motivate the security problems that sensor networks face by developing a scenario representative of a circle-distributed 2-hops network model. Threats are identified to this model and a new lightweight security solution, comprised of the topology discovery and network set protocol and the network repair protocol (TDNSR), is proposed which operates in the base station while the resource constraints of sensor networks are traded off. Simulation results show that the proposed algorithm can rapidly setup and repair the network to meet with the request of security, while the cost, in terms of energy consumption, is decreased efficiently.

Keywords Wireless sensor network, Network setup, Topology discovery, Energy-efficient security

近年来，随着无线通信、集成电路、嵌入式计算及微机电系统等技术的飞速发展和日益成熟，具有感知能力、计算能力和通信能力的微型无线传感器开始在世界范围内出现[1,2]。这些传感器具有低成本、低功耗、多功能等特点和无线通信、数据采集、信息处理、协同合作等功能。由这些微型传感器节点构成的传感器网络，能够协作地实时监测、感知和采集网络分布区域内的各种环境或监测对象的信息，并对这些数据进行处理，被广泛应用于军事斗争、国家安全、环境监测、交通管理、医疗卫生、制造业和反恐抗灾等领域。

传感器网络的许多应用(如军事目标的监测和跟踪等)在很大程度上取决于网络的安全运行[3,4]，一旦传感器网络受到攻击或破坏，将可能导致灾难性的后果。如何在节点计算速度、电源能量、通信能力和存储空间非常有限[5,6]的情况下，通过设计安全机制，提供机密性保护和身份认证功能，防止各种恶意攻击，为传感器网络创造一个相对安全的工作环境，是一个关系到传感器网络能否真正走向实用的关键性问题[7,8]。

虽然传感器网络的研究始于20世纪90年代末期，但由于传感器网络还未被真正地模型化和量化，无线传感器网络安全方案还处于理论研究阶段，研究成果离实际应用和形成普遍接受的标准还相差甚远[9,10]。

现有对无线传感器网络的安全协议的研究基本上是在分层、分簇、多对多或多对一模式上进行的，这种试图提出一种普适解决方案的研究方法在有些情况下并不适用。例如，在需要临时采取安全保卫的场合，现有的拓扑发现和网络配置方法虽然也能正常工作，但需时较长，反应较慢。因为在这种只需要节点和基站一对一通信的情况下，我们需要一种更简单有效的方法而不是规模较大的普适方法。

本文首先给出了一种以基站为中心的圆分布双跳无线传感器网络一对一通信模型；然后，在该模型的基础上，权衡资源限制，提出相应的安全需求和解决方案，给出网络配置、拓扑发现和网络修复协议和算法；最后对算法进行了计算机仿真。

1 安全需求

一种比较完善的无线传感器网络安全解决方案应当具备如下基本特征[5,9]：

(1) 机密性：传感器网络不应当向其他网络泄漏任何敏感的信息，且因密钥泄漏造成的影响应当尽可能控制在一个小的范围内，从而使得一个密钥的泄露不至于影响整个网络的安全。

(2) 真实性：节点身份认证或数据源认证在传感器网络的许多应用中是非常重要的。在传感器网络中，攻击者极易向网络注入信息，接收者只有通过数据源认证才能确信消息

*)重庆市科委自然科学基金资助项目(CSTC2006BB2430)和重庆市教委科学技术研究项目(KJ050508)。张金荣 博士研究生，助理研究员，研究方向为传感器网络与通信、控制理论与工程、光机结构设计。

是从正确的节点处发送过来的。

(3) 完整性:在通信过程中,数据完整性能够保证接收者收到的信息在传输过程中没有被攻击者篡改或替换。

(4) 新鲜性:为防止攻击者进行任何形式的重放攻击,我们必须保证每条消息是新鲜的。简单地说,新鲜性是指发送方传给接收者的数据是在最近时间内生成的最新数据。

(5) 扩展性:传感器网络的可扩展性表现在传感器数量、网络覆盖区域、生命周期、时间延迟、感知精度等方面的可扩展极限。因此,给定传感器网络的可扩展性级别,安全解决方案必须提供支持该可扩展性级别的安全机制和算法,来使传感器网络保持良好的工作状态。

(6) 可用性:传感器网络的安全解决方案所提供的各种服务能够被授权用户使用,并能够有效防止非法攻击者企图中断传感器网络服务的恶意攻击。同时,安全性设计方案不应当限制网络的可用性。

2 拓扑模型

我们的模型中网络是动态配置的,而非拓扑预知或网络预置。其应用场合是需要数据向中心控制器或基站汇聚由基站进行数据融合的情况。它面临的问题主要有:(a)被动信息收集;(b)节点陷落;(c)伪装节点;(d)加入节点。

因此,要考虑的安全问题包括鉴证、完整性、机密性、认可、反重放和反交通分析。接受一条信息需要毫不含糊地确认该信息来自明确的源,在传输过程中没有被改变,该信息不是以前信息的重放,并且,通信需要保密以使窃听者不能截取、研究、分析并图谋设计发现传感器网络目的的方法。同时,还要考虑资源配置,权衡安全水平与资源之间的限制关系。

在我们的模型中做了如下假定:(1)基站鲁棒性强,具有所需的处理器速度、存储能力和电力支持以满足加密和路由需求,位于固定的安全位置且能连续工作。也就是说,基站处于一个可信任的计算环境。对各个节点则无此要求;(2)密钥管理的重分配机制是非必需的,因为基站掌管所有节点的密钥,如假定(1),它是安全的;(3)通信模式是一对一,而非一对多或多对一,因为每一个信息都有特定的目的地——虽然在路由层和 MAC 层信息是广播的。这样,所有通信可以实现端对端加密,能有效降低交通分析威胁;(4)每个传感器直接或间接同基站通信,基站融合各个传感器的数据,同时,基站需要确认传感器节点的真实性、通信的完整性、信息非以前信息的重放。

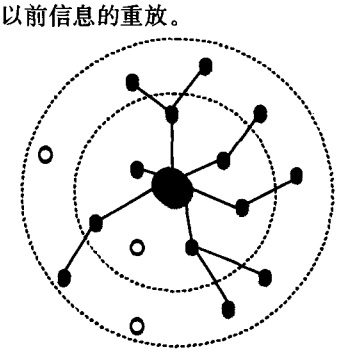

图 1 拓扑模型

图 1 给出了符合这些假定的一种圆分布双跳拓扑模型。若以圆分布于基站周围的节点距离基站较远(非邻接节点),需要经过距离基站较近的节点(邻接节点)作为中间节点传送数据。对该类传感器网络,我们的路由协议为每个节点配置一个 64-bit 的密钥和一个公共密钥 KBS,这两种密钥都与基站共享。

3 报文格式

通信报文包含前缀、头部和正文三部分。倘若通信是由基站向节点发起,前缀可以为空,否则它包含发送者的地址;头部包含接收者地址、时间印和命令类型,并用接收节点的密钥 K_N 加密;正文部分是基站和目的节点之间的交换数据,并用目的节点的密钥 K_D 进行加密。注意,这里接收节点和目的节点可能不是同一个节点,因为我们讨论的是双跳模型,目的节点如果不是基站的邻接节点,需要邻接的中间节点中继。对基站而言,此时的接收节点是中间节点。图 2 给出了这种通信格式。

图 2 中,Addr_1 是发送节点的地址。若通信是由基站流向节点,Addr_1 可以为空,反之,Addr_1 不为空可以使基站直接迅速地选择相应的密钥解密信息,而不用一个一个试用直到找到发送者的正确密钥;当通信流是由基站到节点时 Addr_2 表示目的节点的地址,反之表示发送者的地址;DTG 是时间印,用来预防重放攻击;COMMAND 描述了发给接收者的信息类型。这种用基站密钥和节点密钥双加密的方式增强了网络的鲁棒性,即使某个节点陷落,密钥暴露,网络亦能正常工作[7-9]。

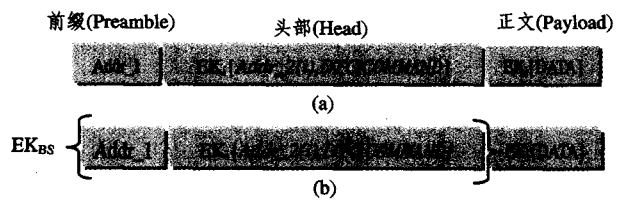

图 2 (a) 基站发向节点报文,(b)节点发向基站报文

4 拓扑发现和网络配置算法

基站配置唯一识别码和主密钥 K_{BS},并存储每一个节点的对称加密密钥。相应地,节点配置自己的唯一密钥 K_N,并共享基站密钥 K_{BS}。为安全起见,节点获得密钥并不通过无线方式,而是通过程序预配置。在网络的初始阶段,基站自适应学习网络拓扑,生成并优化路由表,提供和非邻接节点安全通信的机制。

4.1 拓扑发现

首先,基站向每一个节点 i 发送链接请求 HELLO。节点 i 用其密钥解密该信息的头部,成功则意味着该信息是发向自己的,随即向基站发送应答 HELLO-REPLY。基站用 K_{BS} 解密前缀,从 Addr_2 获得节点 i 的地址,从而得到该节点的密钥并解密该应答的信息头。如果信息头包含有效 DTG 和 HELLO-REPLY 命令,则该节点是基站的邻接节点,将其加入路由表,那些没有应答的节点则被认为是需要双跳的非邻接节点。

对非邻接节点 j,基站通过每一个邻接节点 i 向其发送 HELLO-RELAY。为完成这步操作,基站将发向节点 j 的信息头部和信息正文放在发给节点 i 的中继信息的正文中,并用节点 j 的密钥 K_j 加密,中继信息头部用节点 i 的密钥 K_i 加密。节点 i 收到含有中继命令 RELAY 的中继信息后,加入前缀并转发给节点 j。节点 j 收到的信息头部含有链接请

求 HELLO-RELAY，信息正文含有节点 j 所用的用以通过节点 i 向基站返回信息的机制(记为 Ψ)。Ψ 是含有用 K_i 加密了的中继命令 RELAY 的信息头部。为了应答 HELLO-RELAY，节点 j 构建 HELLO-REPLY，将其用 K_j 加密放进正文中。Addr_2(j)和 Ψ 组成前缀装配进正文中发送。返回时，i 将收到的 j 发送的报文解密，查看头部，制作前缀，将 $EK_{BS}(i)$加入正文中，传回基站。一旦基站发现哪些节点和它相邻，哪些节点可通过相邻节点路由可达，则建立并优化路由表。优化的目的是尽量均衡中间节点的负载，不至使某些中间节点负载过大而另外某些中间节点没有负载。若用 Ψ 表示 EK_i{addr_2(i)，Γ，RELAY}，Γ 表示 EK_i{data}，下面列出了上面提到的六类报文格式：

① HELLO：〈Addr_1；EK_i｛addr_2(i)，DTG，HELLO｝；Γ〉

② HELLO-REPLY：〈EK_{BS}{addr_2(i)；EK_i{addr_2(i)，DTG，HELLO-REPLY}｝；Γ〉

③ HELLO-RELAY：〈addr_1；Ψ；EK_j{addr_2(j)，DTG，HELLO；Ψ}〉

④ HELLO- RELAY-REPLY：〈addr_1；Ψ；EK_j{addr_2(j)，DTG，HELLO}；Ψ}〉

⑤ HELLO-RELAYED：〈EK_{BS}{addr_2(j)；Ψ}；EK_j{addr_2(j)，DTG，HELLO-REPLY}〉

⑥ HELLO-RELAYED-REPLY：〈EK_{BS}{addr_2(j)；EK_j{addr_(j)，DTG，HELLO-REPLY}；EK_{BS}{j}〉

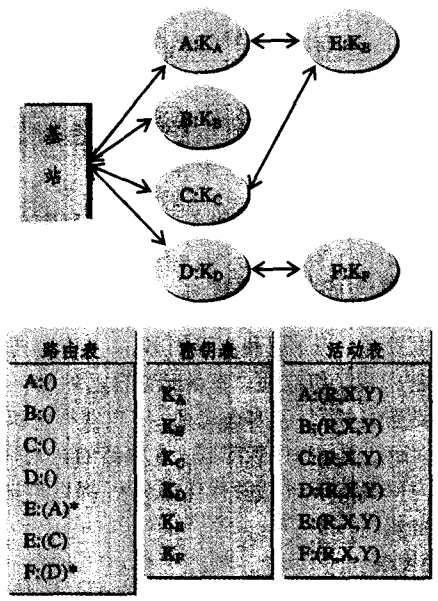

图 3　网络拓扑实例

下面给出了该拓扑发现算法：

```
//secure topology discovery and network setup protocol
//Note: the DTG is only verified by the final destination
//because it is null for intermediate nodes
//BS : the base station, C : the collection of all nodes
Route table ←Φ
Temp route table←Φ
For each i∈C do
    BS→i: HELLO //BS sends HELLO to j node
    If (i→BS: HELLO-REPLY) then //if i is an adjacent node
        Route table=Route table+i
        C=C−i
    Endif
Endfor
//now C contains all the non-adjacent nodes
//Route table contains all the adjacent nodes
For each j∈C do
    For each i∈Route table
        BS→i: HELLO-RELAY
        i→j: HELLO-RELAYED
        if(j→i: HELLO-RELAYED-REPLY) and
         (i→BS: HELLO- RELAY-REPLY)then
            Temp route table= Temp route table+i
        Endif
    Endfor
Endfor
OptimizeRoute()
    Route table=Route table+Temp route table
```

基于维护和修复网络的目的，基站需要维护三种表：(1)路由表维护可达节点的主路由(*)和可替换路由，A()表示 A 是基站的邻接节点，A(B)表示 A 节点是非邻接节点，要通过 B 邻接节点中转；(2)密钥表维护各个节点和基站共享的密钥；(3)活动表包含由节点发给基站信息的最近时间信息(DTG)，该节点发给基站遭破坏信息的计数 X，以及其它节点通过该节点转发给基站的信息遭破坏的计数 Y。X 和 Y 是用来判断节点行为异常的依据。这三种表和其它符号一起用来进行网络配置和拓扑发现。图 3 所示为一实例。

4.2　插入新节点

向现存网络插入一个新节点比较容易。如要加入节点 R，首先将 R 的标识符和密钥 KeyR 载入基站，其时钟同步到现有网络；接着基站重复网络发现算法，明确地寻找新加入的节点。一旦节点 R 被发现，基站更新路由表。

4.3　异常节点处理

异常节点是那些不能按要求工作的节点。及时发现并孤立异常节点，尤其是中间节点，对网络能否进行下一步工作很重要。节点的异常行为常常有：(1)能源耗尽；(2)物理损坏；(3)节点被捕获，信息转送前被修改；(4)依赖于中间节点的节点由于中间节点，产生前两项异常；(5)依赖于中间节点的节点因为中间节点被捕获。异常节点发现修复算法描述如下：

step1　对所有节点 j，若 T-DTG>Δ，当 j 为邻接节点时则转(2)，为非邻接节点时转(3)；若所有节点 j 的"T-DTG>Δ"条件检查完毕，转(7)；

step2　基站向 j 发送查询 REQUEST-QUERY，若没有在规定时间 t 内收到查询应答 REQUEST-ANSWER，则该节点的失败计数 Y=Y+1，转(1)；

step3　基站向 j 的主中间节点 $N_{primary}$ 发送 REQUEST-QUERY。若收到 $N_{primary}$ 应答 REQUEST-ANSWER，转(4)，否则转(5)；

step4　基站通过 $N_{primary}$ 向 j 发送 RELAY-REQUEST-QUERY。若收到 j 的 RELAY-REQUEST-ANSWER，转(1)，否则转(6)；

step5：基站通过其它(若存在)中间节点 $N_{alternative}$ 向 j 发送 RELAY-REQUEST-QUERY，若收到 j 的 RELAY-REQUEST-ANSWER，基站向 j 发送更新路由指令 UPDATE 并为 $N_{primary}$ 的 Y 增加计数；若未收到 j 的 RELAY-REQUEST-ANSWER，基站从路由表中删除 j。转(1)；

step6　基站通过其它(若存在)中间节点 $N_{alternative}$ 向 j 发送 RELAY-REQUEST-QUERY，若收到 j 的 RELAY-REQUEST-ANSWER，基站向 j 发送更新路由指令 UPDATE；若未收到 j 的 RELAY-REQUEST-ANSWER，基站从路由表中删除 j，转(1)；

step7　对所有节点 j 检查其活动表中的 X 计数，若 X 大于阈值，转(8)；若所有节点检查完毕，转(9)；

step8　若 j 是邻接节点，将 j 从路由表中删除，对所有以 j

为主邻接节点的非邻接节点 k，基站通过可替换中间节点向 k 发送路由更新命令；若 j 是非邻接节点，基站通过可替换路由向 j 发送查询命令，若收不到应答，将 j 从路由表中删除，转(7)

step9 对路由表中的每个节点 j，检查其 Y 计数。若 Y 大于阈值，将 j 从路由表中删除。若所有节点检查完毕，转(10)；

step10 退出。

在上面的算法中，T 是现在的时间，Δ 是设定的节点不活动持续时间阈值。

4.4 数据加密

我们使用 CFB(Cipher Feedback)模式对数据进行 64-bit DES 加密。选择 DES 是因为它是一种广泛应用的标准加密算法，对它的破解只有暴力破解法，而这很难。另外，文献[11]认为，应用 DES 可以很好地优化能量使用，这对传感器网络来说很重要。

5 仿真结果

仿真工具采用 NS(network simulator)。所有协议在路由层实现。节点数量 80 个，随机分布在以基站为中心半径 25m 的圆内。生成 100 个密钥存在基站内(第一个作为基站密钥，80 个作为各节点密钥，另外 19 个为加入新节点预留)，基站密钥和节点密钥同时存在节点内。表 1 给出了部分重要的仿真参数。仿真结果给出了节点发射、接收和 CPU 三部分的能量消耗，如图 4 所示。

结果显示，拓扑发现和网络配置完成用时 37.5s，耗能 33.5mJ。其中网络配置占用了大部分时间。另外，在节点总数不变的情况下，我们发现：越多的节点分布于内圆，拓扑发现和网络配置用时越少，能耗越低。为了观察网络修复情况，我们分别令 $\Delta=15$，$X=5$，$Y=5$。每隔 4 秒，节点向基站发送信息以更新基站内各节点的 X 和 Y 计数，20 秒后令邻接和非邻接节点各有 6 个成为非活动节点，此时执行网络修复算法。结果显示，经过大约 7.8s 左右，网络修复完成，耗能 7.3mJ。

表 1 仿真参数

项目	值
每个节点能量/J	36
数据传输率/Kbps	19.2
报文长度/Bytes	48
数据发送时电流/mA	5.0
数据接收时电流/mA	4.2
节点电压/V	1.5
内圆半径/m	10
外圆半径/m	25

仿真中我们把 TDNSR 和著名的 SPINS[11] 协议（包括 SNEP 和 μTESLA 两部分，前者提供加密、数据鉴证、数据时效性和完整性，后者提供数据广播鉴证）做了对比。TDNSR 和 SPINS 相比有如下优点：SPINS 的路由类似非广播路由机制，易受交通分析攻击，TDNSR 一对一通信端对端加密，可有效防止交通分析；SPINS 协议复杂，适合大规模、分层、分簇网络，普适性好，TDNSR 协议简单，针对性强；因此，在我们的模型中，使用 TDNSR 比使用 SPINS 更节省能耗，网络反应更迅捷有效。

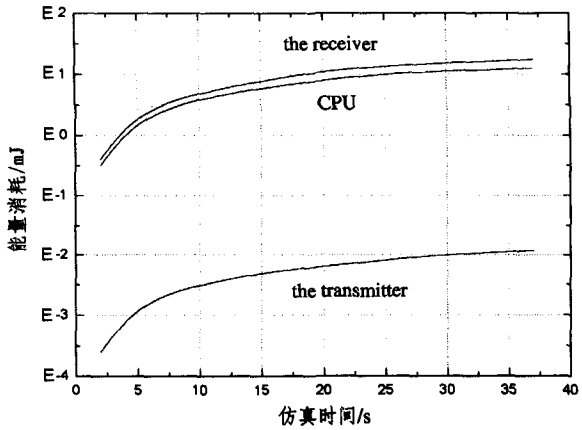

图 4 能耗仿真结果

结束语 纵观以上分析，本文给出的算法有如下特点：(1)通信过程端对端加密，节点解密它侦听到的信息只需很小的开销。节点在解密前 64 位信息(接收信息节点的地址)后，就可判定该信息是否指向自己，若是则继续，否则丢弃；(2)鉴证过程通过使用在基站和节点间共享节点密钥得到，数据完整性通过加密算法得到维护；(3)反重放攻击通过在信息中加入 DTG 获得；(4)协议简单，针对性强；(5)更节省能耗，网络反应更迅捷有效。

参 考 文 献

[1] 王东，张金荣，魏延，等. 利用 ZigBee 技术构建无线传感器网络[J]. 重庆大学学报(自科版)，2006，29(8)：95-97

[2] Zhang Jinrong, Wang Dong, Zhuang Ling, et al. A method of energy estimation for wireless sensors networks [A]// Proceedings of The Intenational symposium on computer Science and technology [C]. Ningbo, China: ASP, 2007:928-931

[3] 郑增威，吴朝晖，林怀忠，等. 可靠传感网聚类路由算法研究[J]. 浙江大学学报(自科版)，2005，10：38-40

[4] Perrig A, Stankovic J, Wagner D. Security in Wireless Sensor Networks [J]. Communications of the ACM, 2004, 47(6): 53-57

[5] Lu K, Qian Y, Hu J. A framework for distributed key management schemes in heterogeneous wireless sensor networks [A]// Proceedings of IPCCC 2006 [C]. Phoenix, USA: IEEE, 2006: 513-519

[6] Shih E, Cho S, et al. Design consideration for energy efficient radios in wireless microsensor networks [J]. Journal of VLSI Signal Processing, 2004: 37(1):77-94

[7] Chan H, Perrig A, Song D. Random key predistribution schemes for sensor networks [A] // Proceedings of IEEE 2003 Symposium on Research in Security and Privacy. IEEE Computer Society [C]. Berkeley, CA: IEEE, 2003: 197- 213

[8] Ashraf W, Stephan O, Larry W, et al. Scalable Cryptographic Key Management in Wireless Sensor Networks [A]// Proceedings of the 24th International Conference on Distributed Computing Systems Workshops [C]. Tokyo: IEEE Computer Society, 2004: 796 - 802

[9] 郎为民，程文青，杨宗凯，等. 一种基于无线传感器网络的密钥管理方案[J]. 计算机科学，2005，32 (4)：147- 154

[10] Wang Dong, Zhang Jin-rong, Cao Chang-xiu. The estimating calculation and distributing regularity of wireless sensors [A]// Proceedings of The International Conference on Mechanical Transmissions [C]. Chongqing, China: Science Press, 2006, 2: 1532-1535

[11] Adrian P, Robert S, Tygar J D, et al. SPINS: Security Protocols for Sensor Networks [J]. Wireless Networks, 2002, 8: 521-534