doi: 10.3969/j.issn.1006-1576.2010.12.014

基于虚拟 Steiner 树的无线传感器网络安全组播路由协议

赵建平[1]，赵建辉[2]，王玮[1]，刘晓阳[1]
（1. 中国卫星海上测控部 技术部，江苏 江阴 214431；2. 中国卫星海上测控部 远望二号测量船，江苏 江阴 214431）

摘要：针对如传统的安全路由协议不适用于组播通信的问题，提出一种基于虚拟 Steiner 树的安全组播路由协议。采用随机密钥预分布模型对无线传感器网络中的节点进行密钥预置，结合组播树的生成算法，对基于虚拟 Steiner 树的安全组播路由协议进行安全性分析。结果表明，该协议能使每一个节点与其邻居节点间共享一个对称密钥，阻止非法节点参与路由过程，达到建立安全组播树的目的。

关键词：无线传感器网络；组播；安全路由
中图分类号：TP391.01; TP393.08　　**文献标识码**：A

Virtual-Steiner-Tree-Based Secure Multicast Routing Protocol in Wireless Sensor Networks

Zhao Jianping[1], Zhao Jianhui[2], Wang Wei[1], Liu Xiaoyang[1]
(1. Technology Department, Satellite Marine Tracking & Control Department of China, Jiangyin 214431, China;
2. Yuan Wang Tracking Ship II, Satellite Marine Tracking & Control Department of China, Jiangyin 214431, China)

Abstract: Proposes a virtual-Steiner-tree-based secure multicast routing Protocol in wireless sensor networks for the traditional Secure Multicast Routing Protocol not applying to multicast communications. Basic Random Key Scheme model has been proposed to distribute key among nodes of wireless sensor networks, and the security of this protocol has been analyzed by the multicast tree generation algorithm. The results show that the protocol enables each node share a symmetric key with its neighbor nodes, to stop the false nodes involved in the routing process for the purpose of establishing a secure multicast tree.

Keywords: wireless sensor networks; multicast; secure routing

0 引言

由于无线传感器网络用于通信的能量开销大于用于数据计算的能量开销[1]，因此，组播在无线传感器网络“一对多”场景中的应用可以大幅减少传感器节点的能量消耗，从而延长传感器节点的失效时间。所以，组播是无线传感器网络中重要的通信方式，特别对传感器网络中的组群形态[2]，组播路由是无线传感器网络研究的重点问题。无线传感器网络面临比传统网络更多的威胁[3]。针对路由面临的如虚假路由信息、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[4]，已提出了一些安全路由协议，如基于 Dimeter 协议的安全路由 DSR[5]，容侵路由 INTRSN[6]等，但这些路由协议都不适用于组播通信。故采用随机密钥预分布模型对无线传感器网络中的节点进行密钥预置，并结合组播树的生成算法，设计了一种基于虚拟 Steiner 树的安全组播路由协议，并对其进行了安全性分析。

1 随机密钥预分配与拓扑建立

密钥管理技术是解决安全问题的关键技术，尤其是加密和密钥更新技术。在设计路由协议时，对路由信息实时加密和签名认证，可增强路由的安全性。为解决无线传感器网络的通信开销，在节点部署之前，一般采用将密钥预先配置在节点中，通过预存的秘密信息来计算会话密钥，由于节点存储和能量的限制，预配置密钥管理方案必须考虑节省存储空间和减少通信开销。故采用随机密钥预分配方案[7]对传感器节点进行密钥预置。

随机密钥预分配方案是由 Eschenauer 和 Gligor 首先提出的，其基本思想是存在一个比较大的密钥池，每一个节点都拥有密钥池中的一部分密钥，只要节点之间拥有一对相同的密钥就可以建立安全链路。该方案利用任意两节点间共享密钥的可能性，利用简单的共享密钥发现协议，来实现密钥的分发、撤销以及节点密钥的更新。

当检测到一个节点被俘获时，控制节点广播被俘节点所有密钥的标识符，其他节点收到信息后删除自己密钥环中含有相同标识符对应的密钥，一旦密钥从密钥环上删除，与被删除的密钥相关的链接将会消失，受影响的节点需要重新启动共享密钥发现，以及路径密钥的建立。该方案的优点是计算复

收稿日期：2010-06-21；修回日期：2010-08-20
作者简介：赵建平（1974-），女，福建人，硕士，工程师，从事软件工程及计算机应用研究。

杂度比较低，网络具有一定的扩展能力，实现简单。缺点是对部分节点被俘获的抵抗性太差，敌人可以通过交换的标识符分析出网络的安全连接，攻破少数的节点而获取较大份额的密钥，从而影响其他节点间的通信。

2 虚拟 Steiner 树的建立

实现组播路由最普遍的方法是构造源节点到组播节点的树形路由结构，信息可以沿着这棵树决定的路径进行发送，减少了信息传递的延时，信息的复制仅在树的分支处进行，可以节省网络带宽资源，降低网络负载。文献[8]中提出了一种虚拟 Steiner 树的生成算法。

2.1 虚拟 Steiner 树生成算法思想

1) 节点集 S 放置在二维空间 G 中。节点 Vi 是属于集合 S 中节点，Vi 的坐标表示为 (X_i,Y_i)，该协议中，节点可以通过 GPS 或其他独立的定位系统准确地知道自己的坐标即位置信息，这个坐标就是它的网络标识符和地址。

2) 在一个欧几里德平面内，如果只有 3 个节点，即一个源节点和 2 个组播节点，那么这 3 个节点的 Steiner 点能被有效地计算出来[8]。故可基于这种思想来建立的高效启发式 Steiner 树。

3) 对于给定的目的节点组 (u,v) 和源节点 s，缩率表示为 $RR(s,u,v)$：

$$RR(s,u,v)=1-\frac{d(s,t)+d(t,u)+d(t,v)}{d(s,u)+d(s,v)} \tag{1}$$

其中，t 是节点组 $\{s,u,v\}$ 的 Steiner 节点。

2.2 虚拟 Steiner 树生成算法描述

对于一个给定的组播节点集合，初始时源节点视所有组播节点为活动的，即组播树没有覆盖任何组播节点。在每次循环中，确定一个最大缩率值的组，然后分别把该组 Steiner 节点和组播节点的连接加入到 Steiner 树，Steiner 节点被激活。循环过程中，如果 Steiner 节点和组播节点组中的某一点重合，则连接另一点和 Steiner 节点，加入 Steiner 树，该重合组播节点被激活。如果 Steiner 节点和源节点重合，则源节点和两组播节点的连线都被加入 Steiner 树中。

以图 1 为例说明算法的过程。第一次循环中，组 (u,v) 被检测到，所以它的 Steiner 节点和组播节点的连线 $\overline{wu}$ 和 $\overline{wv}$ 被连进了 Steiner 树。u、v 节点变灰，w 被激活加入到组播节点集合当中。第二次循环中 (w,d) 被检测到，Steiner 节点为 q。第三次检测到 (q,c)，Steiner 节点和节点 c 重合，所以 $\overline{qc}$ 被加入 Steiner 树，c 点被激活。第四次检测到 (c,c)，Steiner 点与 S 点重合，$\overline{sc}$ 被加入 Steiner 树。整个 Steiner 树就建立起来了。目的节点序列如图 2。

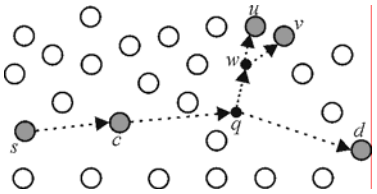

图 1 虚拟 Steiner 树的建立

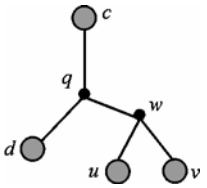

图 2 目的节点序列

在整个 Steiner 树中，Steiner 节点可能并不是真实的传感器节点，而是虚拟的 Steiner 节点（如 q 节点和 w 节点），所以整个 Steiner 树被称为虚拟 Steiner 树。

3 基于虚拟 Steiner 树的安全组播路由协议

该安全组播路由协议主要思想是：以虚拟 Steiner 树为基础，结合基本的随机密钥预分布模型对无线传感器网络中的节点进行密钥预置，通过邻居节点的认证，协商对称会话密钥，在建立组播路由树的过程中对所有的路由消息进行逐跳加密和认证，以实现匿名性和防止攻击者对路由协议的破坏。

3.1 网络模型

假设无线传感器网络的节点 Vi 是随机而稠密地分布在一个二维空间中内，Vi 的坐标表示为 (X_i,Y_i)，该协议中节点可以通过 GPS 或其他独立的定位系统准确地知道自己的坐标即位置信息，这个坐标就是它唯一的网络标识符和地址，所以该协议中不用另行考虑节点的定位问题，所有节点的地位平等，即发射功率、通信半径一致且为固定值，但是基站拥有足够大能量且安全可靠。

采用随机密钥预分配方案对网络中所有的合法节点 Vi 进行密钥预置，为了保证节点之间数据交换的安全性，设定节点之间至少存有一个相同的密钥才可以实施通信，要求所有传输信息都采用对称密钥加密来防止窃听。

3.2　路由协议的描述

本路由协议包括组播树建立和组播树维护 2 个过程。

3.2.1　组播树的建立

组播树的建立分为以下几个步骤：

1) 网络中的每个节点根据随机密钥预配置方案与其邻居节点建立安全连接，并把与之建立了安全连接的邻居节点存储在自己的安全邻居表内。

2) 当一个组播源节点有数据需要发送给它的组成员时，先建立虚拟 Steiner 树 T，源节点把树中的组播节点按照在虚拟 Steiner 树中的生成顺序构成一个二叉树结构的目的节点序列，最先被检测到的目的节点放在序列的最后。组播源节点把这个目的节点序列存储在自己的内存中。如图 1 的虚拟 Steiner 树，目的节点序列如图 2，其中 q 和 w 是虚拟 Steiner 节点。

3) 针对目的节点序列，源节点把目的节点序列中的第一个节点（图 2 中的节点 c）作为目的节点。源节点首先检查目的节点是否在自己的安全邻居表中。若在，源节点把构造的路由申请消息（*RREQ*）直接发给目的节点建立路由连接；若不在，源节点把 *RREQ* 发往安全邻居表中的所有邻居节点。

$RREQ = \{K_{si}[time, s, c], nonce, random, Hop, Path\}$，

其中，time 和 nonce 分别表示发包时间戳和序列号，s 和 c 分别表示源节点和目的节点的标识符，$K_{si}[time, s, c]$ 表示用源节点与安全邻居节点共同存储的对称密钥 K_{si} 对 time、s 和 c 进行加密，random 表示源节点产生的随机数，Hop 表示转发跳数，Path 表示 *RREQ* 所经历的路径。

4) 中间节点 V_i 收到 *RREQ* 后，用对称密钥 K_{si} 解密该请求包；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 vi 加入 Path 域，并且把 Hop 加 1。然后，用 V_i 与安全邻居节点共同存储的对称密钥加密 time、s 和 c 后向安全邻居节点转发该路由请求消息。

5) 在限定的时间内，目的节点会收到来自不同路径的 s 到 c 的 *RREQ*，然后建立可行路径集合 $Path(s,c)$，构造一个路由应答消息（*RREP*），按照不同路径向原路回发。*RREP* 包的格式如下：$RREP = \{K_{ij}[time, s, c], nonce, random, Hop, Path(s,c)\}$。

6) 经过中间节点 V_i 的转发，*RREP* 到达源节点 s，解密后核实 nonce 和 random，于是 s 到 c 构建了可行的路由路径集合 $P=Path(s,c)$。

7) 根据上述步骤构成的可行的路由路径集合 P，源节点 s 选择转发跳数最小（即 Hop 值最小）的路由路径 $P_{\min}$ 作为组播树的分支连入组播树。

8) 当源节点 s 和目的节点 c 之间的路由路径建立后，以目的节点 c 为源节点，以节点 c 的孩子节点 q 为目的节点，重复 3)～7) 的路由建立过程，把所得到的转发跳数最小的路由路径集合$\{P_{\min}\}$按目的节点序列所构造的二叉树结构依次连入组播树。

通过上述步骤，就在源节点和组播节点之间建立了安全的组播树。

组播树建立过程中，存在 2 种特殊情况：

1) 当源节点有 2 个孩子节点时，需要复制数据包，以不同的孩子节点为目的节点进行两次路由路径建立过程。

2) 当目的节点不是真实的传感器节点，而是虚拟 Steiner 点时，只要找到能覆盖该虚拟 Steiner 点的传感器节点即可。

3.2.2　组播树的维护

3.2.2.1　组播节点的加入

当有新的组播节点要加入组播树时，组播源节点先从目的节点序列中找出距离新的组播节点最近的目的节点，然后以这个目的节点为源节点，新的组播节点为目的节点启动路由建立过程。路由路径建立后把此分支加入组播树即可。

3.2.2.2　组播节点的删除

当组播节点要退出组播组时，如果是叶子节点，此节点就向它的上游节点发送一个退出请求包，上游节点把退出请求包逐跳向上转发，目的节点序列中此节点的父节点收到退出请求包后，就把此路由路径从组播树中删除；如果不是叶子节点，此节点向它的上游节点和下游节点都发送退出请求包，请求包中包含此节点的上游节点和下游节点的坐标，然后以上游节点为源节点，下游节点为目的节点启动路由建立过程。

4　协议的安全性分析

安全协议提供的安全服务可从以下方面考虑：

（下转第 68 页）

高水平状态指示仪的显示效果。

参考文献：

[1] 张强，元洪波，赵利杰. 某型机载信息显示设备检查系统[J]. 兵工自动化, 2010, 29(3): 60−62.

[2] Herman, R. Using the cockpit display to improve on-aircraft maintenance[D]. Orlando: The International Society for Optical Engineering, 2006: 204−210.

[3] 张波，张焕春，经亚枝. 基于 DSP 和 FPGA 的座舱图形显示系统关键技术研究[J]. 信息与控制，2003, 32(6): 548−552.

[4] 李开宇. 用 FPGA 实现机载全姿态指示仪图形硬件填充[J]. 计算机辅助设计与图形学学报，2004, 16(2): 248−251.

[5] 胡小龙，周俊明，夏显忠. 飞机座舱图形显示加速系统设计及 FPGA 实现[J]. 中南大学学报：自然科学版，2008, 39(5): 1042−1048.

[6] 朱耀东. 飞机座舱综合图形显示系统关键技术研究[D]. 南京：南京航空航天大学, 2003.

[7] James D. Foley. 计算机图形学导论. 北京：机械工业出版社, 2004: 48−56.

[8] 江修，张焕春，经亚枝. 直线生成算法在飞机座舱全罗盘画面绘制中的应用[J]. 计算机辅助设计与图形学学报, 2003, 15(11): 1448−1451.

[9] 杨蕾，赵慕奇，冯晨. 飞机座舱显示系统的反走样技术研究[J]. 液晶与显示, 2006, 21(6): 686−691.

****

（上接第 51 页）

1) 能够有效防御 Dos 攻击。该协议利用对称密钥对所有路由信息进行逐跳加密和认证，恶意节点的 Dos 攻击包会在刚刚进入网络的时候就被丢弃。

2) 防御修改攻击。在该协议中，由于目的节点需要回复 *RREP* 到源节点，如果路由消息被修改 *RREP* 就不可能到达源节点，路由路径就无法建立，所以可以检测恶意节点通过修改破坏消息的完整性。

3) 防御虚假路由信息。该协议中任意 2 个可相互通信的节点之间都共享会话密钥，通过该密钥可以认证彼此身份，路由消息中用共享的会话密钥对源节点和目的节点进行了加密，所以可以检测出恶意节点虚假的路由信息。

4) 防御传输分析。路由消息在传播中均被加密保护，可以在一定程度上提供匿名性，防止攻击者进行传输分析，跟踪特定节点的行为。

5) 防御 Wormholes 攻击。该协议中节点通过 GPS 或某些定位装置知道自己精确的位置信息，可抵御 Wormholes 攻击。

6) 防御重放攻击。由于在路由信息交换中增加了时间戳和产生随机数时间的一致性判别，该协议能够防御重放攻击。

5 结束语

该协议利用随机密钥预分配方案在传感器节点中预置密钥，使得每一个节点与其邻居节点之间共享一个对称密钥，在组播路由树的建立过程中采用对称密钥算法进行逐跳加密和认证，可以阻止非法节点参与路由过程，达到建立安全组播树的目的。

参考文献：

[1] Ettus M.. System Capacity, Latency and Power Consumption in Multihop-routed SS-CDMA Wireless Networks[C]. In: Radio and Wireless Conference. Colorado, 1998: 55−58.

[2] De Castro L N. Immune cognition, micro-evolution, and a personal account on immune engineering[J]. SEED Journal, 2003, 3(3): 134−155.

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

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

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

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

[7] Laurent Eschenauer, Virgil D. Gligor. A key management scheme for distributed sensor networks[C]. Washington D.C.,USA: Proceedings of the 9th ACM Conference on Computer and Communication Security, 2002: 41−47.

[8] Shibo Wu, K. Selcuk Candan. GMP: Distributed Geographic Multicast Routing in Wireless Sensor Networks[C]. Lisboa, Portugal: Proceedings of the 26th IEEE International Conference on Distributed Computing Systems (ICDCS'06), 2006.