Steiner-Based Hierarchical Secure Multicast Protocol for Wireless Sensor Network*

*FAN Rong, PAN Xuezeng, FU Jianqing, PING Lingdi**

(1. *College of Computer Science, Zhejiang University, Hangzhou* 310029, *China*)

Abstract: By applying multicast technology, the energy consumption can be significantly reduced, and the life time of nodes can be extended in query-based wireless sensor networks. The multicast protocol for large-scale wireless sensor networks from existing literature is usually low performance and low safety. For this reason, a steiner-based hierarchical secure multicast protocol for wireless sensor network is proposed. The main idea of proposed protocol is based on steiner tree and cluster topology. Multicast efficiency can be improved since high-efficiency of steiner tree and high-scalability of clustering are combined. Besides, the energy consumption of nodes can be balanced, and the life time of network can be extended. Furthermore, the protocol adopts secure communication mechanism to prevent from varies network attacks and ensure the data security, integrity and verifiability. Based on the analysis and simulation results, it is shown that the proposed protocol is suitable for large-scale wireless sensor networks.

Key words: wireless sensor network; steiner tree; cluster; secure multicast

EEACC: 6150P **doi**: 10.3969/j.issn.1004-1699.2011.04.025

基于 Steiner 树的层次型无线传感器网络安全组播协议*

范 容, 潘雪增, 傅建庆, 平玲娣*

(浙江大学计算机科学与技术学院, 杭州 310029)

摘 要: 在基于查询的无线传感器网络中, 组播技术的应用可大幅减少传感器节点的能量消耗, 延长节点寿命。针对大型无线传感器网络组播协议性能不高, 且易遭受攻击等问题, 提出了基于 Steiner 树的层次型无线传感器网络安全组播协议。该协议主要运用 Steiner 树与分簇网络的思想, 将 Steiner 树的高效性与簇的高扩展性相结合, 提高了无线传感器网络组播效率, 均衡了网络能量消耗, 延长了网络生命周期, 并在此基础上加入安全通信机制, 以抵御各种网络攻击并确保组播数据的安全性、完整性与可验证性。最后通过理论证明及模拟实验表明本协议适用于大规模无线传感器网络, 具有较低能耗及较高安全性。

关键词: 无线传感器网络; Steiner 树; 簇; 安全组播

中图分类号: TP393 **文献标识码**: A **文章编号**: 1004-1699(2011)04-0601-08

无线传感器网络(Wireless Sensor Network, WSN)是由一组具有路由功能的廉价微型传感器节点所组成, 并依靠无线通信技术形成一个多跳、自治的系统[1]。传感器网络被广泛应用于军事、环境监测、城市交通、智能家居等领域[2-3]。在可预见的未来, 随着与传感器网络相关的硬件技术与软件技术的不断发展, 无线传感器网络必将深入到人类生活的方方面面。

目前研究表明, 无线传感器网络用于通信的能量开销要远大于用于数据计算的能量开销[4]。为了能够尽可能延长传感器节点获取与发送感知数据的时间, 用户应采用按需的方式来询问他所需要的信息, 例如在海洋环境监测中, 监测海水化学指标的传感器节点大部分时间处于休眠状态, 只有当有查询到来的时候才开始检测周围环境并报告数据, 或者由信息收集者发送设置命令以满足不同的应用场景。因此当发送类似数据时, 通过组播的方式可以大幅降低传感器节点的能量消耗, 从而延长其失效时间[5]。

针对组播通信效率与安全性的问题, 本文提出了一个基于 Steiner 树的层次型安全组播协议。该协议通过引入 Steiner 组播树和层次型网络拓扑的思想来构建高效的组播网络, 并在此基础上应用安全通信机制来保证通信数据的安全性、完整性与可验证性, 抵御诸如重放攻击、路由篡改等网络攻击。

项目来源: 国家 863 计划项目(2008AA01A323); 浙江省科技计划项目(2010C31003)

收稿日期: 2010-09-01 **修改日期**: 2010-11-05

本文安排如下,第 1 节简述无线传感器网络安全组播协议的相关工作;第 2 节提出基于 Steiner 树的层次型无线传感器网络安全组播协议,包含系统模型、组播路由建立以及维护机制和组播数据包安全分发协议;第 3 节通过理论分析证明了该组播协议的安全性;第 4 节通过实验分析了该组播协议在能耗方面的表现;第 5 节是本文的结论。

1 传感器网络安全组播协议相关工作

目前,对于无线传感器网络组播协议的研究已经取得诸多成果,主要分为如下 3 类:(1)基于树的组播路由协议,有 EMRS[6]、VLM[2,7]和 DPTB[8]等协议;(2)基于能量的组播,有 BAM[9]、DPAM[10]等协议;(3)基于组群区域的组播,有 GeoCast[11]、Team Multicast[12]和 Spatiotemporal Multicast[13]等协议。同时文献[14]提出一种基于虚拟 Steiner 树的无线传感器网络组播随机路由协议,虽然此协议可以不维护路由信息并提高了组播效率,但每次发起组播任务都需要启动路由建立机制,不适合于数据发送比较频繁的网络中,并且以上这些组播协议都没有考虑安全因素,无法在“敌对环境”中保证通信的安全。

此外,在无线传感器网络安全组播协议方面,文献[15]提出一种基于分簇的无线传感器网络安全组播协议,通过引入 HiM-TORA 树型组播寻路机制和 TESLA 密钥链等机制有效地抵御了对组播路由的各种攻击。在文献[16-17]中,作者在层次型组播路由协议中直接运用 TESLA 密钥链的扩展方案,提高了系统灵活性增强了组播效率。再者文献[18]提出一种基于定向扩散路由协议的安全组播机制来确保组播数据的可验证性,但是定向扩散路由建立时需要一个兴趣扩散的洪泛传播,能量开销和时间延迟都比较大。在最近 2009 年所发表的文献中,文献[19]提出一种能抵御来自内部攻击的多跳组播路由(BSMR),但其方案采用非对称密钥加密,节点验证需要耗费较多能量,不适合通信频繁的网络;文献[20]提出一种将所有节点按照地理位置进行分隔成组的安全组播路由协议(GPLD),虽然提高了系统灵活性,但此协议只依靠节点的地理位置进行分组,并未考虑到节点的分布密度等情况,使得形成的组播组并不是最优结果。

2 提出的安全组播协议

2.1 系统模型

2.1.1 网络模型

传感器节点随机布置在一个二维空间 $V=(G,E)$ 中,其中 G 包含源节点 S 与感知节点 n_i,E 为通信链接。如在空间 V 中如存在一对节点 $(a,b)\in E$,那么表示节点 a 与节点 b 可直接通信,即节点 b 在节点 a 的无线电通信覆盖范围内。

同时网络中任意传感器节点都包含一个预置的全局标识 ID_i,并可通过全球定位系统(GPS)或者其他定位系统准确地获取其所处位置信息,在本模型中表示为坐标 (x_i,y_i),并以此作为 PID_i。无论源节点还是传感器节点 n_i 都维持一张状态信息表,如表 1 所示。感知节点据此来获得其周边网络拓扑结构,同时源节点记录所有节点的状态信息表。节点状态信息表中每个参数的具体含义如表 2 所示。此外网络模型还规定簇头节点的所有成员节点都在其无线电覆盖范围,即簇头节点与其成员节点之间只有一跳的网络间隔,而且此无线传感器网络已具有基于地理位置的基础路由协议和时间同步协议。

表 1 节点状态信息表

ID	PID	ClusterHead Flag	Height Value	Membership Flag	Father Node	Child Node
Node23	(18,45)	1	2	1	(13,33)	(20,53)

表 2 节点状态信息表参数说明

参数	参数说明
ID	全局标识
PID	位置标识
ClusterHead Flag	簇头标识 1 为簇头节点,0 为成员节点,其他值表示还未加入网络
Height Value	树高值 表示簇头所在 Steiner 树中的高度,0 为源节点,∞ 表示其不在 Steiner 树中
Membership Flag	成员结点标识 0 为簇内没有成员节点,1 为有成员节点
Father Node	父节点标识 如果是簇头节点,即为其 Steiner 树中的父节点;如果是成员节点,即为其簇头
Child Node	子节点标识 如是簇头节点,即为其 Steiner 树中的下一跳节点;如是成员节点,那么子节点为空

2.1.2　安全模型

在本文中设定源节点为可信节点,且不会被任何入侵者所俘获。入侵者除非俘获传感器节点本身,否则无法从源节点处获取网内任一传感器节点的密钥。在已有的无线传感器网络安全组播协议中,其中以 Roberto Di Pietro 等人提出的基于定向扩散的安全组播机制[18]最为典型。在本文中规定密钥树结构共分为 3 个层次:Steiner 子树密钥、簇密钥与节点密钥。

2.1.3　威胁模型

在本文中假设无线传感器网络是被部署在敌对环境中,入侵者不仅可以窃听所有网络内部通信,还可以俘获部分节点并从中获取感知数据或秘密信息。此外,本文还假设在一定时间限定内,源节点能够检测并屏蔽那些被入侵者所妥协的传感器节点,并且任何新节点在完成注册和获取密钥前不会被妥协。需要特别指出的是,任意妥协节点在被探测到之前,没有任何密钥方案能够防止入侵者获取被妥协节点上的秘密信息,例如:节点密钥、簇密钥等。

2.2　基于 Steiner 树的组播路由建立与维护

2.2.1　节点信息收集

当完成节点部署工作后,传感器节点需要依靠其 GPS 或者其他定位系统获得位置信息,并通过基于地理位置的基础路由协议发送此信息给源节点 S。由于传感器节点的特殊性,除特殊情况下,如找不到相邻节点或者节点能量即将消耗殆尽时才会调整发射功率,改变无线电信号发射功率来保证通信质量,其他情况下无线电信号覆盖范围大致一定。因此节点无需发送有关无线电覆盖范围的参数给源节点,并且源节点在生成层次型 Steiner 树时将所有节点按统一的信号覆盖范围来处理。当网络稳定后,源节点将收到的节点注册信息存入数据库中以备下一步进行规划生成层次型 Steiner 树。

2.2.2　层次型 Steiner 树生成

在无线传感器网络中,建立一棵以源节点为根,覆盖所有目的节点的费用最小生成树的问题在数学上归结为 Steiner 树问题,这是一个 NP 完全问题,其最优解不可能在多项式时间内完成,所以现在的算法都是近似的启发式算法,目的是为了降低算法难度,并且在性能上逼近理论算法。

在本方案中,源节点 S 在收集完节点注册信息后开始构造层次型 Steiner 树。源节点 S 采用与文献[21]相类似的 Steiner 树生成方法来构建层次型 Steiner 树,但与文献[21]不同的是当一个节点加入 Steiner 树成为簇头节点后,在其无线电覆盖范围内的未归类节点立即标记为它的成员节点,并且这些节点不再参与到余下的 Steiner 树的生成过程中。具体算法描述如图 1 所示。以图 2 为例,源节点 S 出发首先将其无线电覆盖范围内的节点:n1、n2、n3 标记为成员节点,然后寻找到最近非归类节点 n6,并建立虚拟连接,同时也将 n6 通信半径内的节点(n12、n13)标记为其成员节点;接着以源节点 S 和簇头 n6 为集合,寻找最近的未归类节点,并建立虚拟连接,最后遍历所有节点完成 Steiner 树的建立。

```
1  Create_Steiner()
2  {
3    //执行以下程序段直到所有节点都完成标记
4    while(Find_Unattached_Node())
5    {
6      //寻找当前簇头节点周围一跳内的节点
7      membership_node_array=Find_Membership_Node(current_node);
8      //将寻找到的节点标记为此簇头的成员节点
9      Set_Membership_Node(membership_node_array, current_node);
10     //寻找离当前簇头节点最近的未标记节点
11     temp_node=Find_Closest_Node(node_array, current_node);
12     //设置当前簇头节点的子节点和最近未标记节点的父节点
13     Set_Cluster_Head_Node(current_node, temp_node)
14     //将最近未标记节点设置为当前簇头节点
15     current_node=temp_node;
16   }
17 }
```

图 1　层次型 Steiner 树生成算法描述

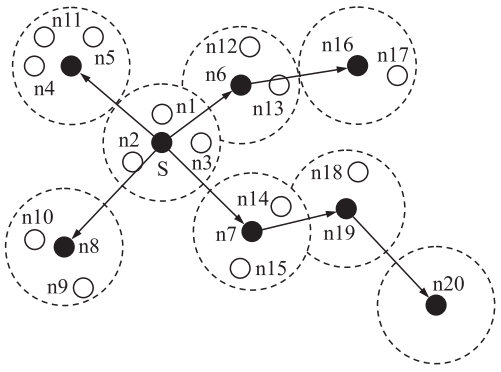

图 2　Steiner 树构建图

为了提高组播效率,组播包中通常含有所需接收者的信息,而单个组播包的大小也直接限制接收者的个数,所以为了尽可能发挥每次发送组播数据的效率,在此以组播包头部所能包含的接收者个数为参数来分割 Steiner 树以形成 Steiner 子树,即组播组或者簇组。也就是说源节点 S 按照本网络系统规定的组播包头部最多能容纳目的地址个数来分割层次型 Steiner 树,例如每个组播包头部至多能包含 4 个接收者信息,那么每棵 Steiner 子树中包含的簇头节点就不能超过 4 个。本方案运用递归算法分割 Steiner 树,将无线传感器网络所在二维空间 V 中的 Steiner 树进行分割,任一子树的簇头节点(Steiner 树节点)个数不能超过组播包头的限制。源节点 S

首先任意选择一个 Height Value 值最大的簇头,并从此簇头出发逆向形成 Steiner 子树,其规则是:将任何节点(除子树的根节点以外)加入 Steiner 子树,必须将其所含树子节点都加入子树。以图 3 为例(已去除所有成员节点,括号内为其 Height Value),此处假设组播包头至多能包含 4 个接收者信息,选择 Height Value 最大的节点 n39,并从节点 n39 出发,依次将 n33、n31、n25 划归为一棵子树(图中以.1.标出),其中由于 n25 为子树根节点,所以其树子节点 n29 不必加入此 Steiner 子树,并且其仍可成为其他 Steiner 子树的节点。以此类推图 2 中的 Steiner 树被分为 4 棵子树。

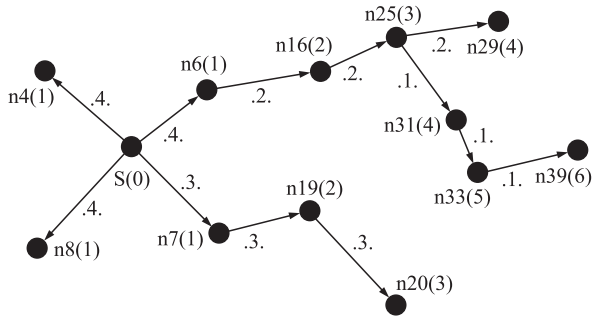

图 3 Steiner 子树构建图

2.2.3 层次型 Steiner 树发布

在完成 Steiner 树的生成与分割后,就需将簇组(Steiner 子树)拓扑结构进行广播,让网络中每个节点都了解其角色与网络拓扑结构。由于节点状态信息表中包含节点周边网络的拓扑结构,传感器节点可通过此表来获取组播路由;并且由于基于 Steiner 层次型组播路由的特性,成员节点很容易找到距离为单跳的簇头节点,并加入簇。

2.2.4 数据发送

无线传感器网络对于传感数据的请求大多是基于地理位置信息的,无地理位置信息的感知数据是毫无意义的。当源节点想要发送任何请求时,它先确定需要组播的区域,即地理范围。然后以 Steiner 子树为单位通过单播的形式发送组播数据。当组播包到达特定 Steiner 子树后,簇头节点将组播包按照簇头 Height Value 从小到大的排序在 Steiner 子树中进行转发,并分析包头内容,如发现其为组播对象,那么将组播内容在本簇内广播。

2.2.5 路由维护

(1)节点加入 对于传感器网络新节点的加入,首先此新加入的节点发送注册信息给源节点 S,源节点 S 将其注册后按照现有的网络拓扑结构给此新的节点分配角色。如果是成员节点,那么此节点在得到源节点 S 的回复后就发送“Join”消息给相应簇头;如果无法成为任何簇头节点的成员节点,源节点 S 就标记此节点为簇头节点,并寻找适合的 Steiner 子树加入;再者如无法加入任何 Steiner 子树,源节点 S 就将其分配新的 Steiner 子树。

(2)节点失效 对于成员节点的失效,任一簇头当其 Membership Flag 等于 1 时,需要周期性检查其成员节点,来发现其中离开或者由于电池耗尽而消亡的成员节点;对于簇头节点的失效,一般会由 Steiner 子树中的其他节点发现并报告给源节点 S,并按照子树的拓扑结构删除此节点并重新建立虚拟链接,对于其成员节点按照新加入节点处理。

2.3 基于 Steiner 树的安全组播协议

在目前已有的无线传感器网络安全组播协议中,Roberto Di Pietro 等人提出的基于定向扩散的安全组播机制[18]采用层次型密钥树结构来达到较高的安全性。但由于定向扩散的兴趣发布是基于洪泛方式进行,并且需要经过梯度建立与加强的过程,能量消耗与时间延迟都比较大,而且对于前文所提出的基于 Steiner 树的层次型组播机制也需另外设计新的安全协议,无法照搬文献[18]中所提出的方案。基于以上论述本文在参考了文献[18]中层次型密钥树结构的思想后,结合 Steiner 树的特征结构提出一种高效的基于 Steiner 树的层次型安全组播协议。在表 3 中列举了本协议所需参数,其详细描述如下。

表 3 安全协议参数说明

参数	参数说明
ID_i	节点全局预置标识
PID_i	节点位置标识
R_i	节点状态信息,详见表 1
SK_i	节点预置的密钥
TK_m	Steiner 子树密钥
CK_n	簇的广播密钥
$H(.)$	散列函数,例如:$SHA-1$
$H^k(.)$	进行 k 次散列函数操作
$E(K,M)$	使用密钥 K 将消息 M 进行加密
||	字符串连接
$\oplus$	异或操作

2.3.1 信息收集与节点验证阶段

在源节点 S 收集节点位置信息时,任一需要加入网络的传感器节点必须通过源节点的验证才能加

入通信网络,成为注册节点。本方案中,源节点 S 通过验证预置在各个传感器节点上的密钥来验证其身份合法性,其协议过程描述如下:

首先,各个传感器节点计算并存储 $A_i=H(\mathrm{SK}_i||T_{\mathrm{reg}})$,并发送如下信息给源节点:

$$n_i\rightarrow S:\mathrm{ID}_i,\mathrm{PID}_i,T_{\mathrm{reg}},H(\mathrm{ID}_i||\mathrm{PID}_i||\mathrm{SK}_i||T_{\mathrm{reg}})$$

其中 T_{reg} 为节点发送节点注册消息时的时间戳。当源节点收到此注册消息后,首先通过本地时间与 T_{reg} 之间的差值来确定是否进行下一步验证,以抵御重放攻击:$T^*-T_{\mathrm{reg}}\leqslant\Delta T$,其中 T^* 表示源节点接收到此注册消息时的时间戳。如果此消息通过时间戳验证,源节点从数据库中读取对应于 ID_i 的密钥 SK_i^*,计算 $H(\mathrm{ID}_i||\mathrm{PID}_i||\mathrm{SK}_i^*||T_{\mathrm{reg}})$,并对比接收到的哈希(Hash)值 $H(\mathrm{ID}_i||\mathrm{PID}_i||\mathrm{SK}_i||T_{\mathrm{reg}})$。如果相等,源节点接受此传感器节点的注册请求并将其 PID_i 写入节点状态信息表中,同时计算与存储对应的 A_i;反之则忽略此注册信息。

2.3.2　层次型 Steiner 树发布阶段

基于§2.2 所提出的组播路由生成方案,源节点 S 首先计算生成 Steiner 组播树并完成 Steiner 子树的分割。接着源节点为每棵 Steiner 子树(组播组)生成用于组播数据加解密的密钥 TK_m 以及每个簇用于组播数据簇内广播的密钥 CK_n。然后源节点发送相应参数给簇头节点或者成员节点。如果注册节点是簇头节点,则计算:

$$\begin{cases}B_i=\mathrm{TK}_m\oplus H(A_i||T_s)\\C_i=\mathrm{CK}_n\oplus H(\mathrm{SK}_i||T_s)\\D_i=H(\mathrm{PID}_i||\mathrm{TK}_m||\mathrm{CK}_n||R_i||T_s)\end{cases}$$

其中 T_s 为源节点发送此消息时的时间戳,然后源节点发送如下信息给簇头节点:

$$S\rightarrow n_i:\mathrm{PID}_i,R_i,B_i,C_i,D_i,T_s$$

如果注册节点是成员节点,则只需计算:

$$\begin{cases}C_i=\mathrm{CK}_n\oplus H(\mathrm{SK}_i||T_s)\\D_i=H(\mathrm{PID}_i||\mathrm{CK}_n||R_i||T_s)\end{cases}$$

接着源节点发送如下消息给成员节点:

$$S\rightarrow n_i:\mathrm{PID}_i,R_i,C_i,D_i,T_s$$

在节点接收到此信息后也同§2.3.1 中所述进行时间戳的验证,然后计算 $C_i\oplus H(\mathrm{SK}_i,T_s)$ 来获得本簇的广播密钥 CK_n。同时,如果是簇头节点,则还需计算 $B_i\oplus H(A_i||T_s)$ 来获得 Steiner 子树的密钥 TK_m。最后传感器节点重新计算 D_i^*,并对比收到消息中的 D_i,以确定是否发送自源节点并确保所接收数据的完整性。并且由于节点收到了节点状态信息 R_i,它即可了解其周边的网络拓扑结构。

2.3.3　数据发送阶段

源节点 S 将组播数据以单播方式发送,以此实现减少发送冗余的组播数据,其网络协议描述如下:

$$S\rightarrow n_i:\mathrm{HEAD},E(H^k(\mathrm{TK}_m),M),T_s,H(\mathrm{HEAD}||M||T_s)$$

其中 T_s 表示源节点发送此组播消息时的时间戳;HEAD 表示组播包头,里面包含了组播对象,即某一特定 Steiner 子树中的簇头节点。当此 Steiner 子树中的 Height Value 最小的簇头节点在接收到此组播数据包后按照节点信息中的 Child Node 转发此数据包,直到有簇头节点无任何子节点可进行转发。此外,$H^k(\mathrm{TK}_m)$ 表示此 Steiner 子树第 k 次收到组播包,并且以 TK_m 的第 k 次散列函数运算结果作为密钥对组播消息 M 进行加密。接着每个簇头解密组播消息 M 并通过散列值来验证其完整性。最后簇头节点重新计算相应的广播包,以发送给簇内成员节点:

$$\mathrm{CH}_j\rightarrow n^*:E(H^k(\mathrm{CK}_n),M),T_{\mathrm{CH}},H(M||T_{\mathrm{CH}})$$

其中 T_{CH} 表示簇头节点发送此组播消息时的时间戳,并且 $H^k(\mathrm{CK}_n)$ 为 CK_n 第 k 次散列函数运算结果。此处需要特别说明的是,TK_m 与 CK_n 使用次数是有限制的,也就是说当 k 达到一定数值(例如:20 次)后子树密钥与簇密钥就会失效需要系统重新更新密钥。

2.3.4　路由以及密钥更新

路由以及密钥更新的安全机制主要是通过存储在各个节点的密钥 SK_i 和 A_i 来完成,当需要更新密钥时,源节点 S 重新生成相应的组播密钥 TK_m 以及簇的广播密钥 CK_n,并发送与§2.3.2 中一样的消息包给相应节点。当需要更新路由时,源节点发送如下信息给传感器节点,并且节点以此来更新其状态信息表:

$$S\rightarrow n_i:\mathrm{PID}_i,R_i,T_s,H(\mathrm{PID}_i,R_i,T_s,A_i)$$

3　安全性分析

3.1　数据安全性

数据安全包括数据的完整性、新鲜性、保密性以及可验证性。在基于 Steiner 树的层次型安全组播协议中发送的所有信息都使用了散列函数,保证了数据的完整性;同时由于此散列值包含了密钥,接收消息的节点可通过验证消息发送方的身份来达到数据的可验证性;并且在发送消息时都加入了时间戳,保证了消息的新鲜性并可抵御重放攻击;最后发送密钥与组播消息时都用相应的密钥进行加密,保证了数据的保密性。

3.2　伪造节点注册

外部攻击者可通过发送注册信息来获得加入无

线传感器网络的权限,从而骗取密钥进而发动网络攻击,但由于节点注册需要发送预置的全局标识与携带有密钥的散列值,攻击者即使截取注册信息也无法获得密钥,这样也就无从发动攻击。另一方面,无线传感器网络中的节点是随机分布在被测环境中,较容易被攻击者俘获,密钥就有泄漏的危险,但由于节点上存储的是节点密钥,所以整个网络的密钥并没有暴露,同时源节点还可通过对于感知数据的分析来判断节点是否被俘获。

3.3 篡改节点信息

虽然节点状态信息并没有加密传输,但带有节点密钥的散列值却可保证数据的完整性与可验证性。节点可验证状态信息表是否是发送自源节点,并可获取其中的密钥。一旦攻击者篡改或伪造节点信息,立刻就会被传感器节点所发现。

3.4 伪造路由信息

由于传感器节点在注册后也有被俘获的危险,所以传感器节点的密钥与相应的子树密钥、簇密钥也可能被攻击者获知。虽然攻击者可任意发出伪造路由消息,但是各个节点的状态信息表是由带有节点密钥的散列值来保证其完整性,里面包含了其父节点与子节点的信息,攻击者发送的伪造路由信息会立即被其他节点发现。

3.5 Wormhole 与 Sybil 攻击

由于路由是由源节点 S 统一计算生成,节点可验证路由信息,攻击者无法改变任一节点的路由信息,也就无法完成 Wormhole 攻击;对于 Sybil 攻击,由于对于任意节点来说它只能在源节点注册一次,无法进行重复注册,所以无法伪造多个身份进行 Sybil 攻击。

3.6 节点妥协

在敌对环境中,节点往往会被攻击者给俘获,并成为其“傀儡”,攻击者可获取存储在俘获节点上的密钥,对无线传感器网络构成了很大的威胁。但由于本方案中采用了层次型密钥树,使得安全性得以大幅提高:虽然可获取被妥协节点的密钥 SK_i,但由于无法获取其他节点的密钥 SK_i,也就无法假冒成为源节点为各个节点更新密钥;虽然攻击者可能通过多次俘获节点,来俘获簇头节点进而获取 Steiner 子树密钥 TK_m,但一方面由于没有获取其他簇的簇密钥 CK_n,也就无法假冒成为其他簇头发送组播信息。另一方面虽然可假冒源节点在子树范围内发送组播数据,但源节点与感知节点的通信是一对一加密进行的,源节点很容易发现被篡改的感知数据,进而定位可能有问题的子树,这样可将其危害尽可能降低,控制在单棵子树内部。

3.7 拒绝服务攻击

拒绝服务(Denial of Service,DoS) 攻击时,攻击者通过欺骗伪装或者其他手段,使提供服务资源的主机出现错误或者资源耗尽。在本文所提出的安全组播协议中,源节点 S 只需要简单的散列函数操作以及对称密钥加密即可完成包括:节点注册,拓扑发布,数据组播等工作,其计算负载少,能量消耗小,完全可以抵御 DoS 攻击。并且由 2.3 节点可以得出,对于任一传感器节点(以簇头节点为例)而言,完成节点注册,拓扑发布,数据组播三个过程共只需要 3 次通信(成员节点)或者 4 次通信(簇头节点),9 次散列函数操作(其中两次为子树密钥以及簇密钥更新操作)和 2 次对称密钥加解密。由此可见无论是通信负载还是计算负载都非常小,非常适合于无线传感器网络。同时源节点可运用 Client Puzzles 机制[23],加入 Puzzle 值使得哈希值头部特定位值为 0,以进一步抵御 DoS 攻击。

4 实验及结果分析

本文提出的基于 Steiner 树的层次型安全组播路由是一种由源节点发起的组播协议。在本节中,基于 Steiner 树的层次型安全组播协议将和其他 2 种最新的安全组播协议:BSMR[19],和 GPLD[20] 比较能量利用效率。在仿真环境中,本文采用由文献[24-25]中提出的实验模型及其参数,实验主要将 4 种目的地位置参数:组播分散角度(AOD)、组播目的数、组播范围和节点密度作为模型化参数;其他默认的参数设置如下:节点的通信半径为 50 m,节点随机分布在占地面积为 500 m×500 m 的范围内,且一个组播包头共可以包含 5 个组播对象,供电电压为 3 V,数据包传输率为 250 kbit/s,数据包的有效载荷为 20 byte,并且默认带有获取节点位置信息的设备。

如图 4 ~ 图 7 所示,4 副图分别表示了 4 种不同的目的位置参数对于组播表现性能的影响。从图 4 中可以发现,本文所提方案在组播分散角度不大的时候与 GPLD 方案能量消耗相差不大,这是由于基于 Steiner 树的层次型安全组播路由需要收集节点信息

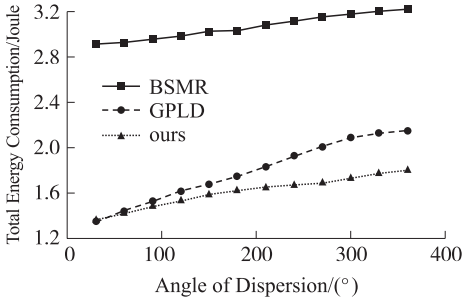

图 4 组播分散角度对于能量消耗的影响

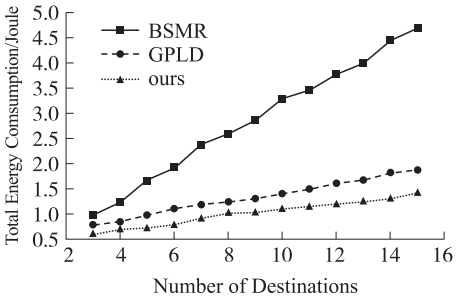

图 5　组播目的数对于能量消耗的影响

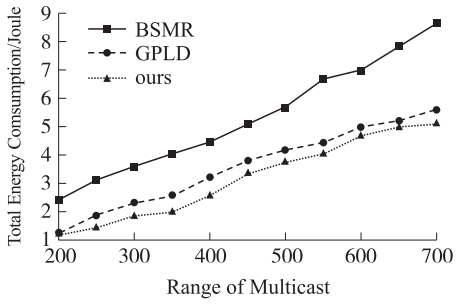

图 6　组播范围对于能量消耗的影响

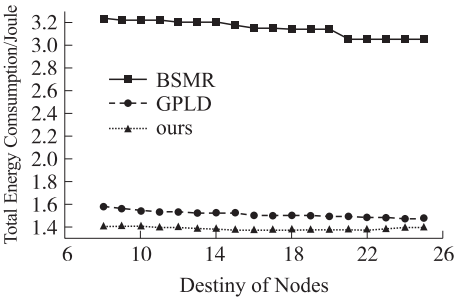

图 7　节点密度对于组播能量消耗的影响

并且注册,这些需要耗费一定能量,而随着组播分散角度的不断扩大,基于 Steiner 树的层次型安全组播路由的 Steiner 子树与层次型拓扑结构的优势就愈加明显,其性能比 GPLD 方案要来得好;而 BSMR 方案由于采用了非对称密钥加密方案,其能量消耗比较大。不过由于采用了节点信息收集等工作,在一定程度上破坏了传感器网络的自组织性,提高了方案实现的自然环境要求。从图 5 中可以发现,相比 GPLD 方案,基于 Steiner 树的层次型安全组播路由具有网络架构上的优势:每个组播包里面包括了一个 Steiner 子树的几个或者全部簇头,而源节点只需要单播此组播包即可完成特定区域的组播任务,效率较高。从图 6 中可以发现,随着组播范围的加大基于 Steiner 树的层次型安全组播路由能量消耗好于 GPLD 路由。从图 7 中可以发现,随着节点密度的加大,由于本文所提方案和 GPLD 都采用本地广播组播数据的机制,所以两者的能量利用效率大体相当,变化不大。基于以上实验结果可以发现,基于 Steiner 树的层次型组播路由机制在采用安全机制后其能量利用效率优于 GPLD 和 BSMR 两个方案。

5　结束语

本文提出基于 Steiner 树的层次型安全组播协议通过收集节点位置信息来生成层次型 Steiner 树,并以此提高组播通信效率,同时在节点信息收集阶段、Steiner 树发布阶段与组播数据发送阶段采用带有密钥的散列值和对称密钥加密机制来保证通信的安全性与通信数据的完整性。在实验对比中,其能量利用效率比较之 2009 年提出的两个安全路由协议方案[19-20]都好。因此基于 Steiner 树的层次型安全组播路由是一种较安全的,能量利用率较高的无线传感器网络安全组播协议,比较适合于有较高安全需求,大型的且数据发送频繁的无线传感器网络中。在未来的工作中,我们需要着重解决组播包头大小与整个数据包大小之间的权衡问题,设计出既尽可能多包含组播对象又同时发送较少数据的方案。

参考文献:

[1] 孙利民. 无线传感器网络[M]. 1 版. 北京:清华大学出版社, 2005.

[2] Cerpa A, et al. Habitat Monitoring: Application Driver for Wireless Communications Technology [C]//2001 ACM SIGCOMM Workshop on Data Communications. Latin America and the Caribbean, CostaRica, April, 2001.

[3] Rabaey J, et al. PicoRadio: Ad-Hoc Wireless Network of Ubiquitous Low-Energy Sensor/Monitor Nodes [C]//Proceedings of IEEE Computer Society Annual Workshop on VLSI (WVLSI'00), Orlando, Florida, April, 2000.

[4] Ettus M. System Capacity, Latency, and Power Consumption in Multihop-Routed SS-CDMA Wireless Networks [C]//Proceeding of the International Radio and Wireless Conference. Colorado, 1998:55-58.

[5] 宋震,周贤伟,林亮. 链路可靠的无线传感器网络组播路由协议[J]. 电子学报,2008,36(1):64-69.

[6] Niwat Thepvilojanapong, Yoshito TOBE, Kaoru SEZAKI. An Efficient Multicast Routing Protocol for Wireless Sensor Networks [C]//IEIC Technical Report, 2005, 104(690):419-422.

[7] Anmol Sheth, Brain Shucker, Richard Han. VLM^2: A Very Lightweight Mobile Multicast System For Wireless Sensor Networks [C]//Proceedings of the IEEE Globecom, 1998, 2:1036-1042.

[8] Zhang Wensheng, Cao Guohong, Tom La Porta. Dynamic Proxy Tree-Based Data Dissemination Schemes for Wireless Sensor Networks[J]. Wireless Networks, 2007, 13(5):583-595.

[9] Okura A, Ihara T, Miura A. BAM: Branch Aggregation Multicast for Wireless Sensor Networks [C]//IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, 2005, 10, 363:7-7.

[10] Sagink Bhattacharya, Hyung Kim, Shashi Prabh, et al. Energy-Conserving Data Placement and Asynchronous Multicast in Wireless Sensor

Networks[C]//MobiSys'03:Proceedings of the 1st International Conference on Mobile Systems,Applications and Services,2003:173-185.

[11] Ko Yong-Bea,Nitin H Vaidya. Ceocasting in Mobile Ad Hoc Networks:Location-Based Multicast Algorithms [C]//Proceedings of the Second IEEE Workshop on Mobile Computer Systems and Applications. Washington:IEEE Computer Society,1999:101-110.

[12] Mario Gerla, Yunjung Yi. Team Communication among Autonomous Sensor Swarms[C]//SIGMOD Rec,2004,33(1):20-25.

[13] Hugng Qing,Lu Chenyang,Gru Ia-Catalin Roman. Mobicast:Just-In-Time Multicast for Sensor Networks Under Spatiotemporal Constraints[C]//Proc IPSN California,2003:442-457.

[14] 王建萍,贾东耀,周贤伟. 基于虚拟 Steiner 树的无线传感器网络组播随机路由协议研究[J]. 传感技术学报,2008,21(11):1896-1899.

[15] 程娅荔,何波. 基于分簇的无线传感器网络安全组播路由协议[J]. 微计算机信息,2007(30):75-77.

[16] Jin Jing,Qin Zhiguang,Xiong Hu,et al. DCSMS:A Mobicast-Based Dynamic Clustering Secure Mobile Multicast Scheme for Large-Scale Sensornets [C]//International Conference on Frontier of Computer Science and Technology,2009:722-727.

[17] Tian Jire,Wang Guiling,Yan Tan,et al. A Power-Efficient Scheme for Securing Multicast in Hierarchical Sensor Networks[C]//Proceedings of 18th Internatonal Conference on Computer Communications and Networks,2009:1-6.

[18] Roberto Di Pietro,Luigi V. Mancini,Yee Wei Law,et al. LKHW:A Directed Diffusion-Based Secure Multicast Scheme for Wireless Sensor Networks[C]//Parallel Processing Workshops,International Conference on IEEE Computer Society Los Alamitos,CA,USA,2003:397.

[19] Reza Curtmola,Cristina Nita-Rotaru. BSMR:Byzantine-Resilient Secure Multicast Routing in Multi-hop Wireless Networks[C]//4th Annual IEEE Communications Society Conference on Sensor,Mesh and Ad Hoc Communications and Networks,2007:263 -272.

[20] Ren Kui,Lou Wenjing,Zhu Bo,et al. Secure and Efficient Multicast in Wireless Sensor Networks Allowing Ad hoc Group Formation[J]. IEEE Transactions on Vehicular Tcehnology,2009,58(4).

[21] Zhang Wesnsheng, Cao Guohong, Tom La Porta. Dynamic Proxy Tree-Based Data Dissemination Schemes for Wireless Sensor Networks[J]. Wireless Networks,Volume,13(5):583-589.

[22] Wong C K,Gouda M,Lam S S. Secure Droup Communications Using Key Graphs [J]. IEEE/ACM Transactions on Networking (TON),2000,8(1):16-30.

[23] Tuomas Aura, Pekka Nikander, Jussipekka Leiwo. DOS-Resistant Authentication with Client Puzzles[J]. Security Protocols, Lecture Notes in Computer Science,2133,2001:170-177.

[24] Xu J H,Peric Band,Vojcic B. Energy-Aware and Link-Adaptive Routing Metrics for Ultra Wideband Sensor Networks[C]//2005 Networking with Ultra Wide Band and Workshop on Ultra Wide Band for Sensor Networks,July,2005:1-8.

[25] Zhao E,Yi B L,Li H Y,et al. Transmission Range Adjustment in WSNs Based on Dynamic Programming Algorithm[C]//2006 International Conference on Wireless Communications, Networking and Mobile Computing,2006:1-4.

范 容(1981-),男,博士研究生,主要研究方向为无线传感器网络安全,rong. fan. cn@ gmail. com;

平玲娣(1946-),女,教授,博导,主要研究方向为网络数据库安全技术、下一代网络通讯与移动计算、面向 SOC 专用集成电路软硬件设计、电子商务多媒体计算机技术,数字电视系统,ldping@ cs. zju. edu. cn。