·计算机工程与应用·

SEC-Tree的安全WSNS路由协议

刘 丹[1]，刘 伟[1]，左朝树[2]，刘 凯[1]

(1. 电子科技大学计算机科学与工程学院 成都 610054; 2. 现代通信国家重点实验室 成都 610040)

【摘要】针对无线传感器网络(WSNs)的广泛应用及其对低能耗、高安全性迫切需求，提出SEC-Tree拓扑结构。以Sec-Tree为基础，设计了多层多路径路由协议，给出了一个自适应多路径路由算法。提出一种PSK生成算法，并将PSK应用于Sec-Tree初始化及路由维护中，实现了基于局部化的加密和鉴别技术，使该协议具有良好的安全特征、抗攻击能力和多跳、多路径路由的可靠特征。分析表明该路由协议具有高效安全的良好特性。

关 键 词 多路径路由; 安全路由协议; 拓扑结构; 无线传感器网络

中图分类号 TP393.02 文献标识码 A

Security WSNs Routing Protocol Based on SEC-Tree

LIU Dan[1], LIU Wei[1], ZUO Chao-shu[2], and LIU Kai[1]

(1. School of Computer Science and Engineering, University of Electronic Science and Technology of China Chengdu 610054;
2. National Laboratory for Modern Communications Chengdu 610040)

Abstract To cope with the emerging massive application of wireless sensor networks (WSNs) and its urgent attribute demands in low-energy consumption and high-security, a security and energy considering tree (SEC-Tree) topologized structure is proposed. Based on SEC-Tree, a multi-layer and multi-path routing protocol and a self-adaptation multi-path routing algorithm are presented. By applying pairwise shared key (PSK) in SEC-Tree initialization and route maintenance, a localized technology in encryptation and identification is brought forward to ensure the protocol high security, anti-attackability, and reliability in multi-hop and multi-path route. Theoretical analysis indicates the high efficiency and security of the routing protocol.

Key words multi-path routing; security routing protocol; topological stracture; wireless sensor networks

由于WSNs网络能量资源易受限，且易受外界干扰和攻击，设计高效且安全的WSNs网络路由协议成为研究热点。目前WSNs路由协议大致分为基于层次的路由协议[1-4]、以数据为中心的路由协议[5-7]以及基于地理位置的路由协议[8-9]。

本文在传统层次路由协议基础上设计的高效安全的路由机制－SEC-Tree路由协议，克服了传统层次路由协议[1]采用单跳通信、扩展性差、不适合大规模网络的缺点，并引入了身份鉴别机制，具有高效安全的特征。

1 PSK密钥生成算法

为防止各类攻击，提出PSK密钥在WSNs路由邻接节点对间进行信息加密传送，该密钥的生成基于节点对间相互身份鉴别，以提高网络安全性。

1) 在网络初始化时由可信任的接收中心(sink)生成主密钥k^m，并配置给各个传感器节点。节点i根据主密钥生成自己的对称密钥$k_i = f_{k^m}(i)$，其中f_k是伪随机函数[10]。

2) 节点对(I, j)在路由初始化时进行双向身份鉴别。(1) 节点i给节点j发送请求身份鉴别消息包，其中包含自己的i_d和消息认证码$\{i, \mathrm{MAC}(k_i, i)\}$；(2) j收到i的消息后，根据i计算出k_i，并用其解密，完成对i鉴别功能，鉴别成功则进入下一步，否则算法结束；(3) j给i发送确认信息，其中包含自己的i_d和消息认证码$\{j, \mathrm{MAC}(k_j, j)\}$；(4) i收到j的应答信息后，根据j计算出k_j，并用其解密，完成对j鉴别功能，鉴别成功则进入下一步，否则算法结束。

收稿日期：2007－09－07；修回日期：2008－05－21
基金项目：现代通信国家重点实验室基金(060C11)
作者简介：刘 丹(1969－)，男，博士，副教授，主要从事计算机应用方面的研究.

3) 节点对(i, j)各自生成i、j间的PSK密钥：$k_{ij}=f_{k_j}(i)$。

4) 各节点保留自己的密钥和PSK密钥，清除其他密钥，对于i，保留密钥k_i和k_{ij}。

2 SEC-Tree安全路由协议

SEC-Tree对分层路由机制进行改进，将节点到簇头的数据交付修改为多跳交付机制，以减小数据传递的能耗，适应大规模WSN$_S$应用需求。同时，针对SEC-Tree的特性，设计自适应多路径安全路由策略，增强路由协议的抗攻击能力与容错能力，提高可靠性。

2.1 SEC-Tree拓扑形成算法

ECM算法基于能量约束以实现SEC-Tree初始化，形成多跳路由基本拓扑。

(1) 基本概念和定义

最大额定发射功率p_m：在SEC-Tree初始化过程及路由稳定运行阶段，所有节点的最大发射功率。

邻节点：某节点α以p_m发射消息所能覆盖的节点为其邻节点。

树T_v^l：l为树的级数，表示树中节点所经过的合并次数；v为该树的根节点。

边缘节点：树T中的节点α具有不属于该树的邻节点，则α为该树的边缘节点。

边缘中心节点：树T的边缘节点中，与树内其他节点的平均距离最小的节点。

直接可达性R_{ij}：当节点i能直接交付数据到节点j，则R_{ij}=1，否则R_{ij}=0。

距离D_{ij}：两节间往返时间为距离度量，即$d_{ij}=d_{ij\text{-RTT}}$。

(2) SEC-Tree形成算法

SEC-Tree初始化过程形成一个相对稳定的路由拓扑。该过程中各节点进行消息交互的同时相互认证、建立PSK、删除主密钥和其他节点密钥、进行结构初始化。

(3) 节点合并

初始化时，各节点广播身份鉴别消息包。节点a收到各个节点的鉴别消息包后，计算与各个节点的通信能耗，发现通信代价最小的邻居b。向b发送身份确认包，算法建立PSK密钥后，相互发起合并请求。若节点a与b相互收到对方的合并请求，则达成合并协议，形成子树T_{ab}^1，如果请求节点收到合并目标的拒绝消息，那么该节点继续在剩余邻居节点中计算新的最小能耗合并对象。

(4) 树合并及树根节点形成

两个节点合并成一个一级树，两个一级树合并为一个二级树，依次类推，当网络中所有节点都包含于同一棵子树时，停止递归过程，形成如图1所示SEC-Tree。

两个节点合并成1个一级树，选这两个节点作为该树的双根；两个$l(l\geqslant 1)$级树T_i^l和T_j^l欲合并成$l+1$级树时，确定这两个l级树的双根节点(i_1, i_2)和(j_1, j_2)，其中(i_1, i_2)为T_i^l的所有节点中与T_j^l的边缘中心节点j间通信能耗最小的两个节点；(j_1, j_2)为T_j^l的所有节点中与T_i^l的边缘中心节点i间通信能耗最小的两个节点。根节点确定后，将T_i^l和T_j^l重新表示为$T_{i1,i2}^l$和$T_{j1,j2}^l$，这两棵l级树合并形成了1棵$l+1$级树T_v^{l+1}，其中v表示虚根节点，在T_v^{l+1}和其他$l+1$级树合并时，再形成实际的双根节点。可见，SEC-Tree中各级子树具有双根特征。

(5) 基于树结构的节点地址分配

根据该树的合并过程，为每个节点α分配唯一的网络地址$\alpha_{n-1}, \alpha_{n-2},\cdots, \alpha_0$，其中$n$为该树的级数，$\alpha_i$表示该节点的第$i$位。该地址由低位到高位形成，以图1为例，节点$a$与$b$合并时，令$a_0$=0，$b_0$=1；节点$c$与$d$合并时，令$c_0$=0，$d_0$=1；设$T_{ab}^1$和$T_{cd}^1$合并形成二级树，为树$T_{ab}^1$和$T_{cd}^1$分配一级地址0和1。对于节点$x\in T_{ab}^1$，令$x_1$=0；对于节点$x\in T_{cd}^1$，令$x_1$=1。当该二级树进一步产生合并行为时，设选择了$a$和$c$为根，表示为$T_{ac}^2$。按照该方法不断递归，当一棵完整的SEC-Tree形成时，各节点的地址也分配完成。

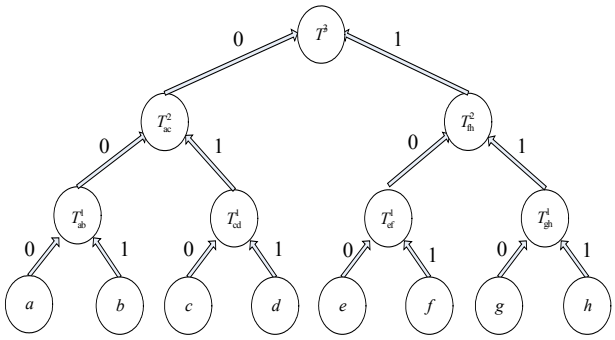

图1 SEC-Tree的形成

2.2 SEC-Tree路由表

SEC-Tree合并完成后，形成n级树(树的最高级数是n)。在形成SEC-Tree过程中，同时形成各节点的路由表。每个节点α的路由表包含$n-1$项，每项包含两个下一跳节点，表示为$R_\alpha^l=(l,\beta_1^l,\beta_2^l)$，其中$(0\leqslant l\leqslant n-1)$，$\beta_1^l$和$\beta_2^l$表示$l$层路由项的下一跳节点，它们是在两个$l$级子树合并过程中，不包含$\alpha$的那棵$l$级子树的两个根节点。由于对每一层路由项

维护了两个下一跳节点，保证了路由的灵活与可靠。

1个l级子树包含2^l个节点，在参予合并成l+1级子树时，确定出其l层路由项，在更新自身路由表时，将路由更新信息传播给子树中的所有其他节点。当SEC-Tree的规模较大时，不是所有节点都具有边缘节点的特征，各节点收到路由表更新信息后，测试相应的下一跳节点是否可达，若可达则更新路由表，否则保持下一跳节点为空。

为适应WSN具有网络拓扑结构不稳定及易受攻击的特征，保证路由的安全有效，路由表中同时维护各下一跳节点的可达性和距离指标，即在节点a的路由表中，对其下一跳节点b，维护R_{ab}、D_{ab}。

图1中，a节点路由表的建立过程为：a首先与b合并形成T_{ab}^1；接着T_{ab}^1和T_{cd}^1合并形成二级树T_{ac}^2；最后T_{ac}^2与T_{fh}^2合并，形成树T^3并完成SEC-Tree合并过程。根据上述路由表建立算法，节点a按照自身所在子树级数由高到低的顺序，依次将各级子树在形成时所利用的根节点加入到路由表中，如表1所示。设图1中节点d不能直接连接到节点f或h，此时，节点d的二级路由表为空。

表1　节点a路由表

级数l	下一跳	可达性	距离
2	f(101),h(111)	R_{af},R_{ah}	D_{af},D_{ah}
1	c(010),d(011)	R_{ac},R_{ad}	D_{ac},D_{ad}
0	b(001)	R_{ab}	D_{ab}

表2　节点d路由表

级数l	下一跳	可达性	距离
2			
1	a(000),b(001)	R_{da},R_{db}	D_{da},D_{db}
0	c(010)	R_{ac}	D_{dc}

2.3　SEC-Tree路由表的维护

各节点基于PSK密钥加密，周期性发送探测包到其各级下一跳节点，拾取各下一跳节点的可达性和时延指标，以保证路由的安全有效。节点i发送一个探测数据包P_i:$(\mathrm{msg})_{k_{ij}}$给节点j，节点i在预定时间范围内收到P_{ackj}并验证通过，R_{ij}=1，在收到响应包的同时更新D_{ij}，否则R_{ij}=0，表示节点j不可达。随时间变化，WSN的拓扑发生较大变化后，需要重建拓扑。在实现中，对于l级根节点i，若其路由表中有1/3的节点失效，则重建本l级子树的SEC-Tree拓扑。

2.4　自适应多路径路由算法

设节点a地址A_a= $A_a^{n-1}\,|\,A_a^{n-2}\,|\cdots|\,A_a^0$，节点$b$地址$A_b$= $A_b^{n-1}\,|\,A_b^{n-2}\,|\cdots|\,A_b^0$，其中$n$为SEC-Tree的最高级数。当$a$向$b$传递数据时，提出以下自适应多跳路由算法步骤：

(1) 令l=n−1。

(2) 若$A_a^l \neq A_b^l$时，转3，否则l=l−1，重新开始步骤(2)。

(3) 查询a路由表中l级的表项$R_\alpha^l=(l,\beta_1^l,\beta_2^l)$；若$\beta_1^l$或$\beta_2^l$不为空，转步骤(5)。

(4) 若$R_{a\beta_1}$=$R_{a\beta_1}$=0，即β_1^l或β_2^l都为空，则l=l−1，转步骤(3)。

(5) 若$R_{a\beta_1}$=1、$R_{a\beta_1}$=0，则选择β_1^l为下一跳节点；若$R_{a\beta_1}$=0、$R_{a\beta_1}$=1，则选择β_2^l为下一跳节点，转步骤(7)。

(6) 若$R_{a\beta_1}$=$R_{a\beta_1}$=1，选择距离小的节点为下一跳节点。

(7) 数据交付至下一跳节点，下一跳节点重复本算法交付数据，算法结束。

例：节点d准备向h传递数据。由图1的拓扑结构，节点d和h的地址分别为R_d=011和R_h=111。从最高地址位依次比较，因$A_d^2 \neq A_h^2$，根据表2，查找到节点d的二级路由表项$R_d^2=(2,,)$。继续查表2，找到节点d的一级路由表项$R_d^1=(1,a,b)$，按照多跳路由算法，选a为下一跳节点，将消息直接传递给节点a。节点a重复该算法，$A_a^2 \neq A_h^2$，查找到节点a的二级路由表项$R_a^2=(2,f,h)$，按照多跳路由算法，选h为下一跳节点，交付完成。

3　性能分析

3.1　路由效率及可靠性

路由采用多级、每级双下一跳节点的机制，增加了路由的伸缩性，某些中间节点受到攻击而暂时不能提供路由服务，也不影响路由可靠性。

定义1　路由可达概率E_{num}从源节点到目的节点是间接可达的概率，num表示该路径中每一跳可以选择的路由节点数。

对于一个规模为n级SEC-Tree的WSN，总节点数为2^n，节点地址宽度为n，任意两节点间的最大物理跳数N_m≤n。对于路由表中出现空项，其一是因为距离原因而不可达，其二是由于节点受到攻击而不能正常工作。距离因素不是本算法需要考虑的范畴，忽略该因素。设节点能正常工作的概率为p，则节点i的路由表包含n项共$2n$个下一跳节点，其中有效节点数为$2np$。对于每个节点，只要在其可供选择的$2np$个下一跳节点中有一个可正常路由，则其可以将数据交付到下一跳，则该跳路由是可达的，当某路由中的所有跳都是可达的，则该路由是可靠的。因此规模为2^n的WSN的可达性为：

$$E=\left[\frac{2np!}{i!(2np-i)!}p^{i}(1-p)\right]^{n} \tag{1}$$

相对于普通多跳路由机制，其每跳只有一个节点可供选择，有 $E_1^n=p^n$ 。

两者可达性之比为：

$$\frac{E_{2np}^n}{E_1^n}=\left[\frac{2np!}{i!(2np-i)!}p^{i-1}(1-p)\right]^{n} \tag{2}$$

当p=0.8，n=3，$2np$≈5，则有 E_5^n =0.999，而 E_1^n =0.512。可见，在不需要更新路由表的情况下，该方法的可达性相对于单路由维护机制的可达性有极大提高。

3.2 安全性

设攻击者捕获一个节点需要的最小时间为$T_{\min}$，SEC-Tree的初始化时间T_{est}通常为几秒，可假设T_{est}<$T_{\min}$。当经过$T_{\min}$后，没有任何一个节点保留主密钥k^m。即使一个攻击者在$T_{\min}$后捕获一个节点，该节点已经完成密钥分配及生成过程，攻击者不能获得其他节点的密钥信息和主密钥，有效防止了攻击者进一步扩散攻击。

由于SEC-Tree形成是基于能量距离的，自然就避免了黑洞攻击(black-hole attack)。由于路由的灵活性，该路由协议能够使一个有效节点绕过wormhole攻击、jamming攻击和一些抑制网络流量的攻击。

SEC-Tree形成算法完全确定了网络拓扑，可防止恶意节点实施路由环、基于路由的DOS、hello flood等攻击；由于恶意节点不容易加入到路由拓扑中，可有效抑制选择性转发攻击的发生；基于鉴别机制的SEC-Tree形成算法可有效防止sybil节点进入网络；同时，在路由维护过程中采用双向身份鉴别机制，能有效抑制虚假路由信息的攻击、sinkhole攻击等。

对于内部攻击，一个节点在路由表中维护的是各级下一跳节点的信息，当一个已经被攻击的节点只能骗取该节点上各级下一跳节点的信任，其扩展带有一定局部性，可以延缓攻击扩展速度。

4 结 束 语

本文首先提出SEC-Tree拓扑形成算法，并基于该拓扑构建了多层结构的路由表。进而提出自适应多路径路由机制及相应的路由算法，更好地控制节点通讯能耗，提高路由的可靠性和灵活性。为提高WSNs的安全性，设计了一种PSK密钥生成算法，在SEC-Tree拓扑形成过程和路由表的维护过程中，基于PSK实现身份鉴别。最后通过理论分析证明路由协议的高效能、高可靠性和安全性。

参 考 文 献

[1] HEINZELMAN W, CHANDRAKASAN A, BALAKRISHNAN H. Energy-efficient communication protocol for wireless microsensor networks[C]//Proc of the 33rd Annual Hawaii Int'l Conf on System Sciences. Maui: IEEE Computer Society, 2000: 3005-3014.

[2] MANJESHWAR A, AGRAWAL D P. Teen: a protocol for enhanced efficiency in wireless sensor networks[C]//Int'l Proc of the 15th Parallel and Distributed Processing Symp. San Francisco: IEEE Computer Society, 2001: 2009-2015.

[3] MANJESHWAR A, AGRAWAL D P. Apteen: a hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks[C]// Proceedings of International, Parallel and Distributed Processing Symposium. [S.l.]: [s.n.], 2002:195-202.

[4] LINDSEY S, RAGHAVENDRA C S. PEGASIS: Power-efficient gathering in sensor information systems[C]// Proc of the IEEE aerospace conf. Montana: IEEE Aerospace and Electronic Systems Society, 2002: 1125-1130.

[5] KULIK J, HEINZELMAN W R. Negotiation based protocols for disseminating information in wireless sensor networks[J]. Wireless Networks，2002，8(23): 169-185.

[6] INTANAGONWIWAT C, GOVINDAN R, ESTRIN D. Directed diffusion: a scalable and robust communication paradigm for sensor networks[C]//Proc 6th Int'l Conf on Mobile Computing and Networks (ACM Mobicom). Boston, MA: [s.n.], 2000: 56-67.

[7] BRAGINSKY D, ESTRIN D. Rumor routing algorthim for sensor networks[C]//WSNA'02: Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications. [S.l.]: ACM Press, 2002: 22-31.

[8] YU Y，ESTRIN D， GOVINDAN R. Geographical and energy-aware routing: A recursive data dissemination protocol for wireless sensor networks[C]//UCLA-CSD TR-01-0023. Los Angeles: [s.n.] 2001: 1-11.

[9] XU Y, HEIDERMANN J. Geography-informed energy conservation for ad hoc routing[C]//Proc of the 7th annual ACM/IEEE Int'l Conf on Mobile Computing and Networking. Rome: ACM Press, 2001: 70-84.

[10] GOLDREICH O, GOLDWASSER S,. MICALI S. How to construct random functions[J]. Journal of the ACM，1986, 33(4): 210-217.

编 辑 熊思亮