一种无线传感器网络的组密钥管理方案研究

章志明[1],邓建刚[3],彭雅丽[1],余 敏[2]
ZHANG Zhi-ming[1],DENG Jian-gang[3],PENG Ya-li[1],YU Min[2]

1.江西师范大学 软件学院,南昌 330022
2.江西师范大学 计算机信息工程学院,南昌 330022
3.江西师范大学 科技处,南昌 330022
1.College of Software,Jiangxi Normal University,Nanchang 330022,China
2.College of Computer Information Technology,Jiangxi Normal University,Nanchang 330022,China
3.Science and Technology Research Place,Jiangxi Normal University,Nanchang 330022,China
E-mail:zzm_9650@163.com

ZHANG Zhi-ming,DENG Jian-gang,PENG Ya-li,et al.Group key management scheme research of wireless sensor networks.Computer Engineering and Applications,2009,45(29):91-93.

Abstract: To support secure group communications in resource constrained wireless sensor networks,and consider the security requirement of forward security,backward security and integrality that group key management must meet,a security and efficient group key management scheme which only uses elliptic curve cryptosystems and XOR is proposed.Compared with previous group key management schemes for wireless sensor networks,this scheme provides more efficiency and is more suitable for wireless sensor networks.
Key words: wireless sensor network;group key;forward security;backward security

摘 要:为了在有限资源的无线传感器网络上能安全进行群组通讯,同时考虑到组密钥管理必须满足前向安全性、后向安全性和完整性的安全需求,使用椭圆曲线密码体制的部分步骤和异或运算提出了一种安全有效的组密钥管理方案。与目前现有的群组密钥相比,方案不仅具有较好的效率,并且更适合于无线传感器网络。
关键词:无线传感器网络;组密钥管理;前向安全性;后向安全性
DOI:10.3778/j.issn.1002-8331.2009.29.026 **文章编号**:1002-8331(2009)29-0091-03 **文献标识码**:A **中图分类号**:TP212

1 引言

无线传感器网络(Wireless Sensor Network,WSN)是由许多低成本的传感器(sensor node)组成,每一个传感器都含有有限的计算能力,有限的能源与存储空间。传感器最主要是利用网络环境来收集信息,在该位置进行处理,最后把处理结果传送给基站。现在许多无线传感器网络的应用,如森林火灾检测、生态环境监控、野生动物跟踪监控等,都是建立在群组式通讯的模式之上,基站必须安全地传送信息到一组数量众多,负责处理与收集信息的传感器,因此,建立一个用以加密群组通讯的组密钥,保障传感器网络的安全运行是传感器网络得以更广泛应用的基础之一。但是,与传统的网络不同,传感器网络本身的特点决定了其安全研究的复杂性和独特性,如传感器节点大规模地分布在未保护或敌对环境中,节点容易被捕获而泄漏敏感信息;昂贵的安全机制(如公钥密钥)不能适用于资源受限的传感器网络;无线多跳通信的特性使得窃听、干扰等攻击更加容易;另外,传感器节点的低成本也使得节点被捕获后容易泄露密钥,从而导致整个网络的安全受到威胁。

国内外许多学者对于如何保护无线传感器网络上的群组通讯安全做了深入的研究工作[1-5]。大多数有关无线传感器网络组密钥管理的文献大多数采用了树型密钥管理方案,例如文献[3-5],密钥树结构使得密钥更新时的通信复杂性相比其他方案有一定的优势,但仍然使用了模和指数型等高成本的运算方式,不太适合无线传感器网络。仅使用椭圆曲线密码体制的部分步骤和异或运算,提出了一种具安全有效的组密钥管理方案,并可满足前向和后向安全性,且椭圆曲线密码体制的部分步骤是在基站进行处理,大大减少了网络的计算量,且当群组数目改变时,每一个节点更新组密钥时所花费的运算成本独立于群组大小。与目前现有的群组密钥管理方案相比,提出的方

基金项目:国家重点基础研究发展规划(973)(the National Grand Fundamental Research 973 Program of China under Grant No.2007CB316505,No.2006CB303000);国家自然科学基金(the National Natural Science Foundation of China under Grant No.60363002);科技型中小企业技术创新基金项目(No.07C26213600564);江西省科技支撑计划资助。
作者简介:章志明(1978-),男,讲师,主要研究方向:网络信息安全、无线传感器网络;邓建刚(1977-),男,硕士生,主要研究方向:信息安全、网络计算技术;彭雅丽(1983-),女,硕士,主要研究方向:网络信息安全、电子商务安全;余敏(1964-),女,博士,教授,主要研究方向:网络信息安全,分布式系统与移动计算技术,无线传感器网络。
收稿日期:2008-05-29 **修回日期**:2008-08-19

案,不仅具有较好的效率,并且更适合于无线传感器网络。

2 WSN 组密钥管理的安全需求

把无线传感器网络当作是一种分层的无线传感器网络,称作为分簇无线传感器网络,每簇由簇头节点和普通节点组成。WSN 组密钥管理分为系统初始化、组密钥(group key)生成和组密钥更新三个步骤。组密钥是网络内所有成员节点以及基站的共享密钥,被用来对组播报文进行加密和解密等操作。无线传感器网络的组密钥管理必须至少满足以下的安全需求:

(1)前向安全性和后向安全性:由于无线传感器的移动性和脆弱性,组成员可能会发生改变,例如:成员的离开、成员的加入和成员被俘虏等。这样当有成员改变时方案必须保证离开和被俘虏的成员无法再利用它所知的组密钥解密后来的组报文或生成有效的加密报文,称为前向安全性,同样当有新的成员加入,它获得组密钥不能解密以前的组报文,称为后向安全性。

(2)完整性:保证信息的完整性不被破坏。

(3)健壮性:是指网络中少数节点的失效(例如被敌方控制)不会使得整个网络瘫痪。

3 分簇无线传感器网络的组密钥管理方案

3.1 网络模型

按文献[1-2]的思想把网络当作是一种分层的无线传感器网络,网络结构如图 1 所示,网络分为三层:基站(base station)、簇头节点、普通节点。

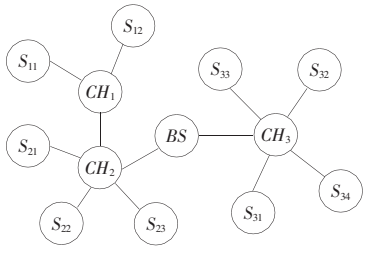

图 1 分簇无线传感器网络模型

(1)基站:基站是整个无线传感器网络与外界网络的接口,将接收来自无线传感器网络中节点发送过来的所有数据,基站一般作为无线传感器网络的控制中心,部署在可控制的环境下不会被敌人俘获,而且处理能力、内存及无线发射功率都不受限制。

(2)簇头节点:簇头节点不仅负责对簇内数据进行预处理,而且负责簇内的组密钥管理。出于安全性和资源消耗的原因,簇头节点周期地从普通节点中产生。

(3)普通节点:普通节点只需采集周围环境的数据并发往簇头节点或基站,由于节点的移动性,它们可能离开一个簇进入另一个簇。

簇头节点和普通节点都可能会被俘虏,一但被俘虏,这个节点上的所有信息将被泄露,一个被俘虏的节点能够被它的邻居节点发现。

3.2 符号说明

BS:基站

CH_i:簇头节点 i

S_{ij}:在第 i 簇的普通节点 j

$\oplus$:表示异或运算

$K_{Sij,BS}$:第 i 簇的普通节点 j 和基站预先分配的共享对称密钥

$K_{CHi,BS}$:第 i 簇的簇头节点 i 和基站预先分配的共享对称密钥

$K_{Sij,CHi}$:第 i 簇的普通节点 j 和第 i 簇的簇头节点 i 的共享对称密钥

K_g:组密钥

3.3 系统初始化

假定网络中的传感器数量为 n,被分成 m 个簇。每个普通节点都预先分配一个与基站共享的密钥 $K_{Sij,BS}$,每个簇头节点都预先分配一个与基站共享的密钥 $K_{CHi,BS}$。

3.3.1 产生簇头节点与簇内每个节点共享密钥

基站分别使用基站与簇头和基站与簇内每个节点共享的密钥 $K_{CHi,BS}$ 和 $K_{Sij,BS}$,加密簇头节点与簇内每个节点共享的密钥 $K_{Sij,CHi}$,分别传送给簇头节点和簇内节点:

$\forall 0\leqslant i\leqslant m, \forall 0\leqslant j\leqslant n_i, BS\rightarrow CH_i: \mathrm{E}K_{CHi,BS}(K_{Sij,CHi})$

$BS\rightarrow S_{ij}: \mathrm{E}K_{Sij,BS}(K_{Sij,CHi})$

其中(m 表示网络被分成 m 个簇,n_i 表示第 i 簇节点数),这样每个普通节点都与它所在簇的簇头节点共享一密钥 $K_{Sij,CHi}$。

3.3.2 分配安全信息

为了产生组密钥,基站将分别为每个簇头节点和普通节点通过下面几个步骤产生一些安全信息:

(1)基站在有限域 $GF(p)$ 上选择一椭圆曲线 $\mathrm{E}: y^2=x^3+ax+b, p>3$,其中 $a,b\in GF(p)$ 并且在 $GF(p)$ 中满足 $4a^3+27b^2\neq 0 \pmod p$,椭圆曲线密码的相关数学背景及其原理这里不过多阐述,有关这方面的更详细的叙述见文献[6-7]。

(2)基站分别为每个簇在 $\mathrm{E}(GF(p))$ 上选一个点 $G_i=(X_i, Y_i)$,同时选择两个随机数 S, W。

(3)基站用与每个簇的簇头节点共享的密钥 $K_{CHi,BS}$ 加密一个安全信息 $X_i\oplus W$ 传送给每个簇的簇头节点 CH_i:$\forall 0\leqslant i\leqslant m$, $BS\rightarrow CH_i: \mathrm{E}K_{CHi,BS}(X_i\oplus W)$。

(4)基站用与第 i 簇的每个节点共享的密钥 $K_{Sij,BS}$ 加密一个安全信息 $Y_i\oplus S$ 传送给第 i 簇每个节点 S_{ij}:$\forall 0\leqslant i\leqslant m, \forall 0\leqslant j\leqslant n_i, BS\rightarrow S_{ij}: \mathrm{E}K_{Sij,BS}(Y_i\oplus S)$。

3.4 组密钥的建立

(1)基站选择一个随机数 R,计算组密钥 $K_g=S\oplus R$,然后发送 $W\oplus R$ 给所有的簇头节点 CH_i:$\forall 0\leqslant i\leqslant m, BS\rightarrow CH_i: \mathrm{E}K_{CHi,BS}(W\oplus R)$。

(2)每个簇头节点用它原来的安全信息 $X_i\oplus W$ 与接收到 $W\oplus R$ 信息进行异或运算,得到信息 $SI=X_i\oplus W\oplus W\oplus R=X_i\oplus R$,然后把 SI 发送给本簇的所有节点:

$\forall 0\leqslant i\leqslant m, \forall 0\leqslant j\leqslant n_i, CH_i\rightarrow S_{ij}: \mathrm{E}K_{Sij,CHi}(X_i\oplus R)$

(3)本簇的所有节点用它原来得到的安全信息 $Y_i\oplus S$ 与接收到的 $X_i\oplus R$ 信息以及自己点 $G_i=(X_i,Y_i)$ 的 X_i, Y_i 进行异或运算,得到组密钥 K_g:

$K_g=(Y_i\oplus S)\oplus(X_i\oplus R)\oplus(X_i,\oplus Y_i)=S\oplus R$

经过上面几步,所有合法的成员将得到一个与基站共享的组密钥 K_g。

3.5 簇组成员的改变

3.5.1 簇组成员的离开

在无线传感器网络中,当节点离开网络时,为了保证前向安全性,簇头节点需要立即把这个节点从本簇删除,并且更新组密钥(Group Key)K_g,使离开的节点不知道新的组密钥 K_g'。

假设第 i 簇的一个节点 j 要离开网络,更新组密钥(Group Key) K_g 步骤如下:

(1)基站为第 i 簇在 E($GF(p)$)上重新选一个新的点 $G_i'=(X_i',Y_i')$。

(2)基站用与第 i 簇簇头节点共享的密钥 $K_{CHi,BS}$ 加密一个安全信息 $X_i'\oplus W$ 传送给簇头节点 CH_i:$BS\rightarrow CH_i$:$EK_{CHi,BS}(X_i'\oplus W)$。

(3)基站用与第 i 簇每个普通节点共享的密钥 $K_{Sij,BS}$ 加密一个安全信息 $Y_i'\oplus S$ 传送给第 i 簇除节点 j 外的其他普通节点 S_{ik}:$\forall 0\leqslant k\leqslant n_i,k\neq j$,$BS\rightarrow S_{ik}$:$EK_{Sk,BS}(Y_i'\oplus S)$。

(4)更新完第 i 簇的安全信息后基站选择一个新的随机数 R',计算新的组密钥 $K_g'=S\oplus R'$,然后重新执行 3.4 节的组密钥生成步骤,使所有合法的节点产生新的组密钥 K_g'。

3.5.2 簇组成员的加入

在无线传感器网络中,当有新的节点加入网络时,为了保证后向安全性,需要立即更新组密钥(Group Key)K_g,使新加入的节点得到的组密钥 K_g'不能解密以前的组报文。假设有一个节点 j 加入到第 i 簇,更新组密钥(Group Key)K_g 步骤如下:

(1)基站为节点 j 分配一个与基站共享的密钥 $K_{Sij,BS}$,然后分别发送如下信息给节点 j 和第 i 簇的簇头节点 CH_i:

$BS\rightarrow CH_i$:$EK_{CHi,BS}(K_{Sij,CHi})$,$BS\rightarrow S_{ij}$:$EK_{Sij,BS}(K_{Sij,CHi})$

(2)基站为第 i 簇在 E($GF(p)$)上重新选一个新的点 $G_i'=(X_i',Y_i')$。

(3)基站用与第 i 簇的簇头节点共享的密钥 $K_{CHi,BS}$ 加密一个安全信息 $X_i'\oplus W$ 传送给簇头节点 CH_i:$BS\rightarrow CH_i$:$EK_{CHi,BS}(X_i'\oplus W)$。

(4)基站用与第 i 簇每个普通节点共享的密钥 $K_{Sij,BS}$ 加密一个安全信息 $Y_i'\oplus S$ 传送给第 i 簇(包括新加入)的所有节点 S_{ik}:$\forall 0\leqslant k\leqslant n_i$,$BS\rightarrow S_{ik}$:$EK_{Sk,BS}(Y_i'\oplus S)$。

(5)更新完第 i 簇的安全信息后基站选择一个新的随机数 R',并计算新的组密钥 $K_g'=S\oplus R'$,然后重新执行 3.4 节的组密钥生成步骤,使所有合法的节点产生新的组密钥 K_g'。

4 安全性与效率分析

4.1 安全性分析

在方案中,基站与每个节点共享的对称密钥 $K_{Sij,BS}$ 是预先分配的,所以攻击者不可能获得密钥,并且对称密钥是互不相同的,当一个节点被俘虏后,不会影响其他节点的安全,更影响不到全网的安全。簇头节点与簇内节点共享的对称密钥 $K_{Sij,CHi}$ 是通过 $K_{Sij,BS}$ 加密传送给簇内节点,由于攻击者不可能获得 $K_{Sij,BS}$,所以也不能获得 $K_{Sij,CHi}$。攻击者不可能获得当前的组密钥,因为用于产生组密钥的安全信息 $X_i\oplus W$ 和 $Y_i\oplus S$ 是被加密传送给所有合法的传感器节点。组密钥管理方案完全满足前向安全性和后向安全性。当有节点离开(被俘虏)时,因为及时更新了组密钥(Group Key)K_g,这样离开(被俘虏)的节点就不可能用旧的组密钥解密后来的组报文或生成有效的加密报文。同样当有新的节点加入时,它获得组密钥不能解密以前的组报文,从而保证了后向安全性。即使攻击者控制了一个节点,也不可能获得其他节点的密钥和其他节点的任何安全信息,仍可避免整个群组被进一步控制,所以该密钥管理方案具有很好的健壮性和安全性。

4.2 效率分析

假设网络中的节点数目为 N,S 表示每簇平均节点的数目,d 表示树的高度为 d(根节点为第一层),下面将从存储复杂性、计算复杂性和通信复杂性对提出的方案与基于密钥树的方案进行比较。

(1)存储复杂性:在密钥树中,基站存储密钥量的复杂度为 $O(N)$,簇头节点的密钥量存储复杂度为 $O(S)$,普通节点存储密钥量的复杂度为 $O(\log_2(S))$。方案中,基站与每个节点都预先分配一个共享密钥,存储密钥量的复杂度为 $O(N)$,簇头节点需要存储与基站共享的密钥、组密钥以及与本组各成员分别共享的密钥对,它所存储的密钥量为 $O(S)$,普通节点只需存储一个与基站共享的密钥、与簇头节点共享的密钥以及一个组密钥,所以单个节点的密钥存储复杂度仅为 O(1),因此,新方案的存储复杂性明显优于基于密钥树方案。

(2)计算复杂性:在密钥树的组密钥管理方案中,当加入新节点时,簇头节点需要更新新节点所在子树(从叶子节点到根节点)的密钥,计算复杂度为 $O(\log_2(S))$;当从密钥树中删除某节点时,簇头节点需要更新被删除节点所共享的所有密钥,其密钥更新的计算复杂度为 $O(\log_2(S))$,当网络的节点数目增加时,簇头节点的计算复杂度也会呈对数级增长。并且每个传感器节点需要执行许多模指数运算来计算更新簇密钥和组密钥,这种模指数运算的离散对数计算对于传感器节点而言仍然不是很适合,会很快消耗节点电能。而方案只仅使用对称加密算法和异或运算来产生和更新组密钥,虽然方案用到了椭圆曲线密码体制的部分步骤,但只是用于产生一个安全信息,并且是在基站中完成的并不占用节点资源。对于簇头节点而言,当有节点加入或离开它仅需计算一个用于更新组密钥的安全信息,其计算复杂度为 O(1),而普通节点的计算复杂度也仅为 O(1),因此,新方案明显优于旧方案。

(3)通信复杂性:在密钥树的组密钥管理方案中,当加入新节点时,需要更新新节点所在子树(从叶子节点到根节点)的密钥,通信量为 $O(d\log_d N-d)$;当从密钥树中删除某节点时,需要更新被删除节点所共享的所有密钥,其密钥更新的通信量为 $O(d\log_d N-1)$。而在该方案中,删除和增加节点的通信量为 $O(N)$,可见,新方案在通信时的通信量要略高于旧方案,但计算复杂度要优于旧方案。

5 结束语

使用对称加密算法和异或运算提出了一种安全有效的组密钥管理方案,并可满足前向和后向安全性,健壮性以及可扩展性等安全需求。通过性能分析,与目前主要使用密钥树型管理结构相比,方案在增加适量通信复杂性的同时,有效降低了存储复杂性和计算复杂性,并且当群组数目改变时,每一个节点更新组密钥时所花费的运算成本独立于群组大小。与目前现有的群组密钥管理方案相比,提出的方案,不仅具有较好的效率,并且更适合于无线传感器网络。下一步的工作,将使用无线传感器网络测试平台 TinyOS 和 TingPK[8],对提出的方案进行更深入的算法复杂性研究,从理论和应用角度,得到更详细的结果。

参考文献:

[1] Arisha K A,Youssef M A,Younis M F.Energy-aware TDMA based MAC for sensor networks[C]//Procof IEEE Workshop on IMPACCT1. Los Alamitos,CA:IEEE Computer Society Press,2002:372-382.

(下转 149 页)