

无线传感器网络里密钥分配算法分析

翟朔¹,何梦云²

(1. 中国矿业大学 计算机学院, 江苏 徐州 221116;

2. 中国矿业大学 管理学院, 江苏 徐州 221116)

摘要:基于无线传感器网络现有的安全问题,给出了传感器网络里现有的一些常用密钥分配算法:随机密钥预分配方案、 q -composite、对称密钥、新颖随机密钥算法。在此基础上,对这些算法的抵抗俘获、网络连通性、可扩展性和内存开销的特性进行分析,指出它们存在的问题。新颖密钥分配算法具有网络连通性好、存贮开销小和抗俘获能力强等优点,但是该算法也存在缺点:建立密钥的过程、消息是明文传送的,容易遭到偷听攻击。提出在建立密钥阶段通过共享密钥加密节点之间的通信,建立密钥后该共享密钥自动擦除。

关键词:随机图理论;对称密钥;二元多项式;双向函数

中图分类号:TP301.6

文献标识码:A

文章编号:1673-629X(2010)08-0142-04

Key Distribution Algorithm Analysis in Wireless Sensor Network

ZHAI Shuo¹, HE Meng-yun²

(1. College of Computer Science, China University of Mine and Technology, Xuzhou 221116, China;

2. School of Management, China University of Mine and Technology, Xuzhou 221116, China)

Abstract:Based on the existing security problems in wireless sensor networks, present some of the existing key distribution algorithms in wireless sensor networks: a random key pre-distribution scheme, q -composite, symmetric key, new random key algorithm. On this basis, analyse the characteristics of the capture of resistance, network connectivity, scalability and memory overhead of these algorithms, and point out their problems. The novel random key algorithm has advantage in good network connectivity, small memory overhead and enhanced resistance against capture, but it also has disadvantage: message is transferred with plaintext in the process to establish key, so it is easy to eavesdrop attack. Propose that make use of share key to encrypt the communication of nodes in the process to establish key, then the share key is automatically erased.

Key words: random graph theory; symmetric key; bivariate polynomial; bidirectional key function

0 引言

电子和计算机技术的新发展为传感器网络的发展铺平了道路^[1,2]。传感器网络通常由超小型大量的自治设备组成。每个设备叫做一个传感器节点或者传感器,是电池配备集成的传感器,具有数据处理和短距离的无线通信能力。在典型的应用情况下,传感器节点随机地散布在部署区域,在没有任何固定的和可信的基础设施的情况下收集传感器数据。结果,方案的类型取决于一个可信的服务的关键协议,在两个节点之间是不适合传感器网络的,如 Kerberos。

传感器网络正被广泛地应用,包括军事侦查和跟踪、环境检测、病人检测和追踪、智能环境等^[3-5]。当传感器网络被实施在敌方环境里时,安全变得尤为重要,因为它们是比较脆弱的,且容易受到各种恶意的攻击^[6,7],例如,偷听、冒充、业务分析、节点俘获等。因此,在传感器节点之间保护通信以便使信息机密和完整是重要的。作为基本安全服务原则的其中之一,成对密钥的建立保证了传感器节点之间的通信安全。然而,由于传感器节点资源的限制,对它们来说使用传统的成对密钥的建立是不可行的,例如公钥密码和密钥分发中心。

1 相关理论

1.1 预分配密钥方案

一种朴素的解决方案是所有的节点带有一个主密钥 K , 如图 1 所示。

收稿日期:2009-12-11;修回日期:2010-03-23

基金项目:东南大学移动通信国家重点实验室开放研究基金资助项目(W200817)

作者简介:翟朔(1988-),女,河南永城人,研究方向为计算机信息安全;导师:毕方明,讲师,研究方向为信息安全。

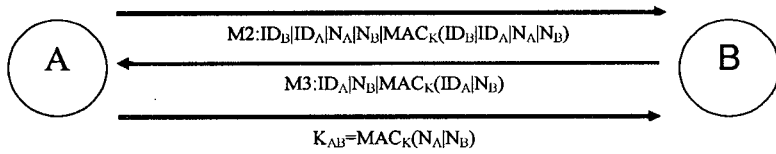


图1 主密钥分配方案

任意两个节点利用它完成密钥协商并获得一个新的成对密钥。该方案不能显示合适的网络恢复力:一旦一个节点被危害,整个网络的通信将受到危害。

另外一个预分配方案是让每一个节点带 $N-1$ 个秘密成对密钥,如图2所示。

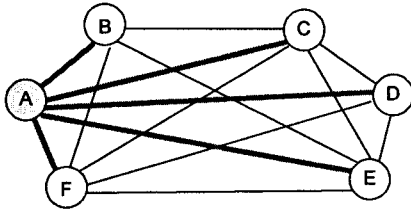


图2 任意两节点之间密钥不同

这个方案的抗毁性是比较完美的,因为一个危害的节点不影响其他节点之间的通信安全。然而,对于 N 很大来说,这种方案对于存储有限的传感器来说是不实际的。而且,增加一个新节点到现有的传感器网络是很困难的,因为现有的节点没有新节点的密钥。

1.2 随机密钥预分配方案

Eschenauer 等^[8]人提出了一个随机密钥预分配方案。在他们的方案里,在节点部署之前,随机地从一个密钥池里选择对称密钥的子密钥分发给每一个传感器节点。部署之后,每一个传感器与邻居节点交换它存储的密钥。如果两个邻居有共同的密钥,它们就是安全连接。这个共同密钥被用于加密它们之间的通信。万一两个邻居节点没有共同密钥,如果它们可以找到一个共同的中间节点,仍然可以建立一个成对路径密钥;否则,这两个节点被看做是无连接的。根据随机图理论,如果任意个节点共享至少一个共同密钥的概率达到一个关键值时,那么整个网络接近是一个连接的网络。

1.3 q-composite 预分配密钥方案

Chan 等^[9]人提出了一个 q-composite 方案来改进网络抗毁性攻击。网络抗毁性在这里定义为:当一些节点被俘获或危害之后,在没有被危害的节点之间的通信有多少被危害,这是对预分配密钥方案安全属性的主要度量。Chan 方案要求两个节点共享至少 q 个共同的密钥来建立安全的连接。当被危害的节点总数比较小时,随着 q 值的增加,网络抗节点俘获攻击的能力不断得到改善。总之,攻击者需要俘获更多的节点以达到危害同样数量的没有被俘获的节点之间的通

信。

上述两个方案都是随机密钥预分配方案,这种防范有一些局限性。首先它们不能保证整个网络的连通性。一个节点如果和它的邻居节点没有共同密钥,则有可能

从网络中脱离。虽然增加预载入密钥的数量可以改善网络的连通性,但是它也增加了存储开销和降低了抗毁性。这些方案的另一个弱点是通信开销。在网络初始化阶段,每个节点需要和邻居节点交换密钥信息,这引入了通信开销和冲突。同时,路径密钥建立过程是复杂的、耗能的操作,它不仅降低了建立密钥的安全登记,而且导致额外的通信开销。

1.4 对称密钥生成方案

Blom^[10]提出了一种在组里任意两成员间建立一个成对密钥的机制(见图3)。首先, $(\lambda-1) \times n$ 和 $(\lambda-1) \times (\lambda-1)$ 对称矩阵 D 被创建,这里 n 是组的大小,对于危害机密 λ 是预期临界点。每个成员存储一个来自矩阵 A ($A = G^T * D^T$) 的行向量和对应的来自矩阵 G 的列向量。

$$\begin{aligned}
 G &= \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ a_{21} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots \\ a_{(\lambda-1)1} & \cdots & a_{(\lambda-1)n} \end{bmatrix} \\
 D &= \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1(\lambda-1)} \\ b_{21} & b_{22} & \cdots & b_{2(\lambda-1)} \\ \vdots & \vdots & \vdots & \vdots \\ b_{(\lambda-1)1} & b_{(\lambda-1)2} & \cdots & b_{(\lambda-1)(\lambda-1)} \end{bmatrix} \\
 A &= G^T * D^T \\
 K_{ij} &= A(i) \times G(j) = G^T(i) \times D \times G(j) \\
 K_{ji} &= A(j) \times G(i) = G^T(j) \times D \times G(i) \\
 &\text{因为 } D \text{ 是对称矩阵} \\
 &\text{所以 } K_{ij} = K_{ji}
 \end{aligned}$$

图3 对称密钥产生

根据对称矩阵的性质,任何两个成员在他们俩之间通过预载入的行向量乘以伙伴的列向量可以计算一个唯一的密钥。

实际上 Blom 的机制是 λ 度二元多项式密钥预分配方案的特殊情况。二元多项式密钥预分配方案由 Blundo 等人^[11]提出。多项式密钥方案使用一个 λ 度二元对称多项式 $f(x, y)$ 在两通信节点之间产生一个成对密钥。在部署之前每个节点估计一个 $f(x, y)$, 这里 $x = i$, i 是一个特定节点的 id 。假定部署之后节点 a 和节点 b 想通信,节点 a 存储 $f(a, y)$ 和节点 b 存储 $f(b, y)$ 。他们首先交换他们的 Id , 然后,节点 a 计算

$f(a, y), y = b$, 节点 b 计算 $f(b, y), y = a$ 。因为 $f(x, y)$ 是一个二元对称多项式, 所以 $f(a, b) = f(b, a)$ 。因此节点 a 和节点 b 能建立一个唯一的成对密钥。前面提到多项式密钥预分配方案仅在受危害的成员不多余 λ 时是安全的。由于 λ 度二元多项式的这个特性, 当危害的成员多余 λ 时, 敌手能获得多项式的所有系数。为了改善抗毁性, 通过把单密钥空间分离成多密钥空间, 用随机密钥预分配过程为每一个传感器节点选择一个密钥空间。Du 的方案在抗毁性方面优于上述方案, 但它仍不能保证整个网络的连通性。

2 一个新颖的随机密钥算法

算法描述见图 4^[12]。

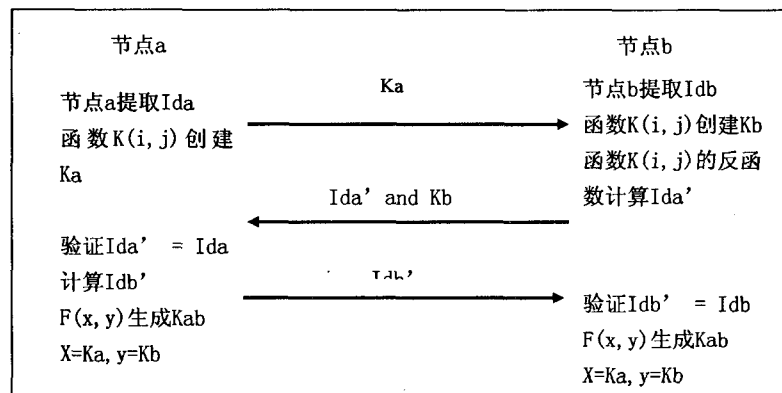


图 4 新颖密钥分配算法

步骤 1: 部署传感器节点之后, 在初始化阶段, 每个节点分发一个基本的密钥、双向函数 $K(i, j)$ 和单向函数 $f(x, y)$ 。一个密钥池矩阵 G (见图 5) 被基本密钥创建, 双向密钥函数 $K(i, j)$ (见图 4), 这里 $i, j < n, n < 100, x, y \in G$ 。矩阵的密钥在通信里生成, 但是它们在初始步骤里不被存储。

$k(1,1)$	$k(1,2)$	$k(1,3)$	$k(1,4)$	\cdots	$k(1,j)$	$k(1,n)$
$k(2,1)$	$k(2,2)$	$k(2,3)$	$k(2,4)$	\cdots	$k(2,j)$	$k(2,n)$
$k(3,1)$	$k(3,2)$	$k(3,3)$	$k(3,4)$	\cdots	$k(3,j)$	$k(3,n)$
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots
$k(i,1)$	$k(i,2)$	$k(i,3)$	$k(i,4)$	\cdots	$k(i,j)$	$k(i,n)$
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots
$k(n,1)$	$k(n,2)$	$k(n,3)$	$k(n,4)$	\cdots	$k(n,j)$	$k(n,n)$

图 5 密钥池矩阵

步骤 2: 假设节点 a 和节点 b 彼此传输数据。首先, 十进制数 Ida 被节点 a 随即生成。在这个十进制数里, 前两个数字等于矩阵 G 里对应密钥的横坐标 i 值, 后两个数字等于密钥纵坐标 j 值。密钥 Ka 被双向函数 $K(i, j)$ 创建和传播。

步骤 3: 当节点 b 收到密钥 Ka, Ida 值时, Ida 对应于通过反函数 $K(i, j)$ 评价的密钥 Ka 。节点 b 发送

Ida' 和 Kb (Kb 由节点 b 随机生成)。

步骤 4: 节点 a 收到由节点 b 发送的 Ida' 后, 如果 $Ida = Ida'$, 则证明节点 b 对于 a 来说是安全的, 然后与密钥 Kb 对应的 Idb' 值由 $K(i, j)$ 的反函数评价。节点 a 传输 Idb' 给节点 b 。最后, 节点 a 用单向函数 $f(x, y)$ 生成密钥 Kab , 这里 $x = Ka, y = Kb, Kab$ 将被用于加密节点 a 和节点 b 之间的通信数据。

步骤 5: 节点 b 收到 Idb' 值后, 它判断 Idb' 是否等于 Idb , 这里 Idb 与它自己随机创建的 Kb 对应。如果相等, 将确保节点 a 对于节点 b 来说是安全的。密钥 Kab 由 Ka 和 Kb 通过单向函数 $f(x, y)$ 生成, 然后用 Kab 解密来自节点 a 的数据。最后, 从节点 a 到节点 b 的数据传输结束。

3 安全分析和性能评价

3.1 网络安全分析

(1) 在无线传感器网络里, 对节点的安全有很高的要求, 因为它们通常被部署在未知区域或者敌对区域 (用于军事事务), 因此, 一些传感器在运行时期可能被俘获。在现有的密钥预分配方案里, 成对通信密钥直接被从预载入的密钥中挑选出来。在网络初始化阶段之后, 如果一个传感器节点被俘获, 那么它所存储的所有

密钥就会被危害, 敌方可能复制一些恶意节点, 把它们放到网络里来实现一些攻击, 例如, 偷听、拒绝服务等。然而, 在新颖算法里, 由于通信内容没有经过加密处理, 故只需要拦截节点之间的通信内容 (Ka 和 Kb) 就可以得到 Kab , 从而导致节点之间的通信不再安全。

(2) 与其它算法比较, 新颖算法在抗毁性方面优于其它算法。节点俘获攻击是传感器网络里最严重的威胁, 因为通过这种攻击秘密信息 (例如通信密钥、关键数据、其它宝贵信息) 将被危害。在随机密钥预分配方案里, 在网络运行阶段, 不同的成对传感器节点可能有相同的成对密钥。因为每一个传感器节点存储一个来自同一个密钥池的密钥子集, 如果敌方俘获一定数量的节点, 那么密钥池的大部分将会被敌方危害。在新颖算法里, 密钥 Kab 是由单向函数生成, 尤其是随机的, 所以攻击节点不能俘获。

在 q -composite 方案里, 虽然通过要求两个节点共享至少 $q (q > 1)$ 个相同密钥来建立安全连接, 但是它仅当俘获节点的数量少于一个关键值时, 才能运转。但是关键值一旦被超过, 整个网络就会不安全。

在低安全要求下 (非军事领域), 两个通信节点仅需要发送由他们自己生成的密钥 ID 给彼此, 然后建立

密钥 K_{ab} 。当以这种方式相互通信时,在通信部分开销将被节省。

3.2 网络连通性

随机密钥预分配方案不能保证任何两个传感器节点直接建立成对密钥。因为两个节点可能没有共享密钥。基于概率理论,如果没有路径密钥被建立,则一些传感器或者部分网络可能仍然脱离该网络。但是在新颖算法里,每个邻居仅通过一跳能相互通信。因为每一个部署的节点对应密钥池、双向函数 $K(i, j)$ 和单向函数 $f(x, y)$, 因此它能保证网络连通性。

3.3 存储开销

由于传感器有限的存储容量,所以它们不可能分配大的密钥池。然而,在预分配方案里,它必须被预分配一个大的密钥池,于是它将占用大量的存储容量。如果使密钥池变小,它将很容易被攻击节点俘获。在部署之前, q -composite 方案分配一个大的密钥池,每一个传感器节点从大密钥池收到一个随机的密钥子集。它不仅存储开销大,而且,不能保证任何两个节点建立安全连接,于是,这种方案的网络连接能力很弱。

新颖算法仅存储基本的密钥和两个函数;然而,密钥池在节点上不存储。节点的存储开销将尽可能地节省。由于存储的节省,一个传感器网络的连通性将变好。当扩大网络时,仅增加 n 值,而不会增加存储开销。在现有的方案里,密钥池的大小随网络的扩大而变大。

3.4 网络大小分析

在密钥预分配方案里,假设 64 位万能密钥被使用,一个有 1000 个节点的网络将需要 8k 位密钥存储空间,增加各种源密钥,它将极大地谋取存储空间。在现有的方案里,很容易知道,当密钥池大小增加时,网络的大小是线性增加的。相反,仅有一个基本密钥和两个函数被存储在每个节点上。当扩大网络时,存储开销不变。

4 结束语

在存储、能量和传输有限的传感器里,网络的安全越来越受到关注。

基于上述问题和现有方法,新颖的随机密钥算法首先要求两个节点间认证地提高了抗毁性和复制攻击;

第二,在发送和接收节点里,使用的加密和解密密钥是由他们自己创建的,他们将有相同的密钥;

第三,修改了密钥的存储方法:在节点上,仅存储基本密钥和两个用于创建密钥的函数,用这种方法,被密钥池占用的内存将降到最小。

但是该密钥分配算法也存在一个缺点:在通信密钥建立阶段,节点之间的通信没有加密,存在偷听攻击。

为了解决上面的问题,可以考虑采取在密钥建立阶段(时间 T)用一个共同密钥加密节点之间的通信,获得通信密钥之后销毁这个密钥,以防止俘获攻击。

参考文献:

- [1] 余平,王汝传,孙力娟.基于无线传感器网络的普适计算模型研究[J].计算机技术与发展,2006,16(4):1-3.
- [2] 颜振亚,郑宝玉.无线传感器网络[J].计算机工程与应用,2005(15):20-23.
- [3] 郑彦,王汝传,高冉,等.无线传感器网络中密钥管理机制约束因素研究[J].计算机技术与发展,2006,16(10):118-121.
- [4] 任丰原,黄海宁,林闯.无线传感器网络[J].软件学报,2003,14(7):1282-1290.
- [5] 郎为民,杨宗凯,吴世忠,等.无线传感器网络安全研究[J].计算机科学,2005,32(5):54-58.
- [6] 郎为民,杨宗凯,吴世忠,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):147-148.
- [7] 陆克中,黄刘生,万颖渝,等.无线传感器网络中传感器节点的布置[J].小型微型计算机系统,2006(11):1000-1002.
- [8] Eschenauer L, Gligor V D. A key-management scheme for distributed sensor networks[C]//Proceedings of the 9th ACM Conference on Computer and Communications Security. New York: ACM, 2002.
- [9] Chan H, Perrig A, Song D. Random key pre-distribution schemes for sensor networks[C]//IEEE Symposium on Security and Privacy. Washington: IEEE Computer Society, 2003.
- [10] Blom R. An optimal class of symmetric key generation systems [C]//Proceedings of EUROCRYPT 84. New York: Springer-Verlag, 1985.
- [11] Blundo C, Santis A D, Herzberg A, et al. Perfectly-secure key distribution for dynamic conferences[J]. Lecture Notes in Computer Science, 1993(740):471-486.
- [12] Jiang Chao, Ren Xiuli. A Novel Random Key Algorithm in Wireless Sensor Networks[C]//2008 IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application. Washington: IEEE Computer Society, 2008.

