

一种 WSN 簇头更换过程中的信息转移方法

苑津莎,张路路,赵 曼

(华北电力大学 电子与通信工程系,河北 保定 071003)

摘 要: 提出簇 ID 的概念,在此基础上提出了一种簇头更换过程中将路由信息、密钥信息转移到下一个簇头节点的方法. 利用簇 ID 通信时,可以直接发送数据包给下一跳节点内的簇 ID,避免了查询簇头的繁琐过程,使簇头转移过程简化. 根据现有簇头与簇头之间的簇间密钥,应用 Diffie-Hellman 算法生成新簇头节点间密钥,最后运用 BAN 逻辑的形式化分析方法,对该协议的安全性进行了证明.

关键词: 无线传感器网络;密钥管理;簇 ID;簇间密钥;Diffie-Hellman;BAN 逻辑

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2016)05-0147-06

A Method of Information Transfer in the Process of WSN Cluster Head Replacement

YUAN Jin-sha, ZHANG Lu-lu, ZHAO Man

(Department of Electronic and Communication Engineering, North China
Electric Power University, Baoding 071003, China)

Abstract: In this paper, the concept of cluster ID is put forward, and a new method is put forward based on which the routing information and key information are transferred to the next cluster head in the replacement process. When the cluster ID is used, the data packets can be sent directly to the cluster ID in the next hop node, which can avoid the complicated process of the cluster head. According to the existing cluster key and application of Diffie Hellman algorithm generated key between the new cluster head nodes. Finally, we use formalization of BAN logic analysis method, the security of the protocol is proved.

Key words: Wireless sensor network; key management; cluster ID; cluster key; Diffie-Hellman; BANlogic

1 引言

无线传感器网络 (wirelessSenser networks, WSN)是由若干个智能传感节点自组织构成的网络^[1],广泛应用于环境监测、交通控制、医疗、军事等众多领域. WSN 节点大多部署在无人看管、难以触及且容易受损失效的环境中,所以保证其安全性就尤为重要. 密钥协商认证在密码安全领域中尤为重要,它是指存在中间人攻击、主动攻击或其他攻击时,双方能以某种方式产生一个秘密值而得到相互之间的认证,进而安全的通信.

文献[2]提出的目前应用广泛的分簇结构,采用网络密钥加密簇头信息并广播,其他节点记录簇头

信息,根据信号强度加入某簇,并且以周期性重新建立簇的方式产生新的簇头. 但论文中并未讨论重建簇头后的路由问题.

文献[3]中通过综合考虑节点的剩余能量和地理位置信息提出了一种优化簇头选举机制方案,均衡了网络内的能量负载. 但每轮重新选择簇头过程十分繁琐,未能考虑簇头更换之后路由信息的转移.

本文在假设密钥管理初始化已完成,在簇头节点需要更换时对存储的路由、密钥信息进行转移,并且把该簇头节点与其他簇头节点之间建立的密钥一并转移到下一个簇头节点,方便下一簇头节点与其他节点之间建立密钥,在通信过程中使用簇 ID 号,可以简化密钥建立过程,节省能量,提高效率.

2 无线传感器网络模型

2.1 无线传感器网络

不失一般性假设有 N 个正常传感器节点部署在区域内,组成一个无线传感器网络,并且这些节点有以下共同性质:(1)一个基站;(2)每个节点都有唯一识别自身的 ID 号、与基站之间唯一的密钥、Diffie-HeHman 算法中的参数 g,n ;(3)无线传感器网络以一定方式形成簇^[4],以分簇的形式存在。

无线传感器网络中节点位置被随机分配在区域内,部署之后根据某种方式形成簇型结构,一些节点选为簇头,之后簇内节点轮流为簇头.簇内节点感知信息传送给簇头,簇头再直接发送给基站或经过中间节点发送到基站.图 1 为无线传感器网络数据传输过程模型示意图.簇 1 内的节点向簇头 1 发送数据,簇 1 内的簇头 A 向簇 2 内簇头 B 发送数据包,簇头 B 再把数据包发送给基站。

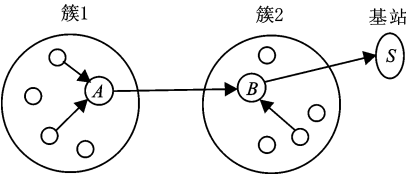


图 1 无线传感器网络模型

2.2 簇内密钥

通常分簇密钥有两种情况,簇内共用同一密钥或簇内任意两节点都有唯一密钥.下面逐一介绍这两种情况。

2.2.1 簇内共用同一密钥 K_i

若网络规模不大,要求安全性不太高通常簇内共用同一密钥^[5],网络部署阶段簇形成时,基站为每一簇分配一个不同的密钥,簇内节点使用这个密钥把感知到的信息发送给簇头节点.一个阶段之后,簇内密钥会更新,删除之前的密钥。

2.2.2 簇内每一节点都与簇头有唯一密钥

当网络规模比较大,要求安全性比较高时,簇内使用同一密钥极容易被恶意节点攻击从而使网络破坏.因此有些传感器网络簇内每个节点都有与簇头节点的不同的密钥^[6].在网络部署安全阶段时,节点与簇头建立密钥,簇头内存储着簇内每一节点的 ID 号以及密钥信息.簇头更新时,新簇头利用 Diffie-Hellman 算法建立与簇内每一节点的新密钥。

3 Diffie-Hellman 算法

Diffie-Hellman^[7]是实现密钥交换的一种算法,

需要 $A、B$ 双方同意使用 g 和 n 两个值,也就是说 g 和 n 这两个数值是相对公开的,在本文的传感器网络节点中可预先存储.另外有两个私密数据 x,y ,其中 A 方只知道 x , B 方只知道 y . mod 是求余运算,假设最后生成的交换密钥的值为 K . 算法实现过程如图 2 所示。

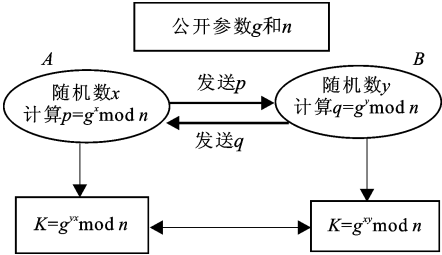


图 2 Diffie-Hellman 算法实现过程

步骤 1:每个节点内存在两个参数,素数 g 和整数 n,n 是 g 的一个原根。

步骤 2:假设节点 A 和节点 B 需要建立一个密钥,节点 A 生成一个随机数 $x < g$,并计算 $p, p = g^x \text{mod } n$,节点 A 保密存储 x ,而公开将 p 发送给节点 B . 类似地,节点 B 同样生成一个随机数 $y < g$ 并计算 $q = g^y \text{mod } n$,节点 B 保密存储 y . 而公开将 q 发送给节点 A 。

步骤 3:节点 A 以 $K_{AB} = q^x \text{mod } n$ 产生共享密钥. 同样,节点 B 产生共享密钥 $K_{BA} = p^y \text{mod } n$. 由 $K_{AB} = q^x \text{mod } n = (g^y \text{mod } n)^x \text{mod } n = g^{xy} \text{mod } n = g^{xy} \text{mod } n = (g^x)^y \text{mod } n = (g^x \text{mod } n)^y \text{mod } n = p^y \text{mod } n = K_{BA}$ 。

因此双方能够得到相同的共享密钥. 由于计算以素数为模的指数相对容易,而计算离散对数较难,因此用 Diffie-Hellman 算法计算配对密钥能保证密钥的安全性。

Diffie-Hellman 算法过程本身存在不能防御中间人攻击的问题,所以在无线传感器网络中无法得到应用. 本文应用该算法时,对发送过程中的 $p、q$ 加密,使其能够抵抗中间人攻击,以保障双方能相互认证从而安全的进行通信。

4 簇头更换时密钥管理

4.1 簇 ID

本文引入簇 ID 概念,使簇头之间通信更便捷,簇 ID 是指簇内每一个节点除了有自己唯一的 ID 号之外,每一簇也有一个唯一的 ID 号,簇内节点担当簇头时与簇外节点通信时使用此 ID 号,若一簇中共

步骤 9:簇头 C 用 K_{12} 解密接收到的信息,并返回确认值.

步骤 10:簇头 C 生成新簇间密钥 $K_{12}' = g^{zy} \bmod n$,簇头 B 节点生成新簇间密钥 $K_{21}' = g^{yx} \bmod n$.由 Diffie-Hellman 算法可知 K_{12}' 与 K_{21}' 应该相等.

步骤 11:簇头 B 、簇头 C 测试建立的新密钥成功之后,用新密钥替换原密钥 K_{12} .

步骤 12:转向步骤 5,直至所有相关节点密钥生成完成后结束.

4.3 簇头转移过程中具体数据传送操作过程

步骤 1:簇 1 内簇头节点 A 更换为簇 1 内节点 C .节点 A 通知节点 C 准备更换为簇头并接收相关信息,假设用 M_1 表示发送通知消息, N_1 为节点 A 产生的随机数.

$A \rightarrow C$:

ID _A	ID _C	$E_{K_{AC}}(M_1, N_1)$	$MAC(M_1 N_1)$
-----------------	-----------------	------------------------	-------------------

步骤 2:节点 C 回复确认信息,假设用 ACK_1 表示应答消息, N_2 表示节点 C 产生的随机数.

$C \rightarrow A$:

ID _C	ID _A	$E_{K_{AC}}(ACK_1, N_2)$	$MAC(ACK_1 N_2)$
-----------------	-----------------	--------------------------	---------------------

步骤 3:节点 A 用节点 A 和节点 C 之间的密钥 K_{AC} 将路由表信息加密,传送给节点 C .假设发送路由表信息用 M_2 表示. N_3 表示节点 A 产生的随机数.

$A \rightarrow C$:

ID _A	ID _C	$E_{K_{AC}}(M_2, N_3)$	$MAC(M_2 N_3)$
-----------------	-----------------	------------------------	-------------------

步骤 4:节点 C 用 K_{AC} 解密接到的信息,存入节点 C 的路由表中,返回成功接收确认.假设应答消息用表示 ACK_2 . N_4 表示节点 C 产生的随机数.

$C \rightarrow A$:

ID _C	ID _A	$E_{K_{AC}}(ACK_2, N_4)$	$MAC(ACK_2 N_4)$
-----------------	-----------------	--------------------------	---------------------

步骤 5:节点 A 在路由表中查找转发信息相关簇头,假设得到节点 B ,簇头节点 A 把簇间密钥 K_{12} 利用簇内节点 A 和 C 之间的密钥 K_{AC} 加密发送给 C . N_5 表示节点 A 产生的随机数.

$A \rightarrow C$:

ID _A	ID _C	$E_{K_{AC}}(K_{12}, N_5)$	$MAC(K_{12} N_5)$
-----------------	-----------------	---------------------------	----------------------

步骤 6:节点 C 回复确认消息给簇头节点 A . N_6 表示节点 C 产生的随机数.

$C \rightarrow A$:

ID _C	ID _A	$E_{K_{AC}}(ACK_3, N_6)$	$MAC(ACK_3 N_6)$
-----------------	-----------------	--------------------------	---------------------

步骤 7:节点 C 更新簇 1 内簇头与簇 2 内簇头之间的簇间密钥 K_{12} ,节点 C 生成随机数 z ,并计算 $p = g^z \bmod n$,用临时簇间密钥 K_{12} 加密 p ,并发送给簇头节点 B 所在簇的簇 ID,即 $IDD2$. N_7 为节点 C 产生的随机数.

$C \rightarrow B$:

IDD1	IDD2	$E_{K_{12}}(p, N_7)$	$MAC(p N_7)$
------	------	----------------------	-----------------

步骤 8:簇头 B 用 K_{12} 解密接收到的信息,并返回确认值.簇头节点 B 也生成随机数 y ,计算 $q = g^y \bmod n$,用簇间密钥 K_{12} 加密 q ,并发送给节点 C 所在簇的簇 ID,即 $IDD1$. N_8 为节点 B 产生的随机数.

$B \rightarrow C$:

IDD2	IDD1	$E_{K_{12}}(ACK_4, q, N_8)$	$MAC(ACK_4 q N_8)$
------	------	-----------------------------	--------------------------

步骤 9:簇头 C 用 K_{12} 解密接收到的信息,并返回确认值. N_9 为节点 C 产生的随机数.

$C \rightarrow B$:

IDD1	IDD2	$E_{K_{12}}(ACK_5, N_9)$	$MAC(ACK_5 N_9)$
------	------	--------------------------	---------------------

步骤 10:簇头 C 生成新簇间密钥 $K_{12}' = g^{zy} \bmod n$,簇头 B 节点生成新簇间密钥 $K_{21}' = g^{yx} \bmod n$.

步骤 11:簇头 B 、簇头 C 之间测试建立的新密钥成功之后,删除临时密钥 K_{12} .

测试新密钥过程^[8],簇头 B 发送一个用新密钥加密的测试数据包给簇头 C ,簇头 C 能解密此测试包则表示新密钥建立成功,同时给簇头 B 发送一个确认值.簇头 B 、簇头 C 之间测试建立的新密钥成功之后,删除临时密钥 K_{12} .否则,丢弃数据包.

步骤 12:转向步骤 5,直至所有相关节点密钥生成完成后结束.

簇内密钥更新方法,簇内使用同一密钥此时不用处理,网络会在相隔一定时间内对簇内使用同一密钥进行更新处理.若簇内使用不同密钥,由网络部署阶段假设任意两节点之间都存在密钥,对此不做处理.

5 协议的安全性能分析

一个协议是否安全,需要特殊的协议分析方法对协议安全进行证明. BAN 是一种基于信念的逻

辑证明方法,是在抽象的层次上证明协议的安全性。本协议用 BAN 逻辑证明其安全性。

5.1 BAN 逻辑

本协议用到的推理规则^[9]如表 2 所示。

表 2 推理规则

符号	含义
$P \models X$	表示 P 相信 X
$P \triangleleft X$	表示 P 收到过 X
$P \mid \Rightarrow X$	表示 P 对 X 有管辖权
$P \mid \sim X$	表示 P 产生过 X
$P \overset{K}{\leftrightarrow} Q$	P 和 Q 共享以密钥
$\#(X)$	表示 X 是新鲜的
$\{X\}_K$	表示用密钥 K 加 X 后得到的密文

BAN 逻辑有 19 种逻辑规则^[10],逻辑规则表达式如表 3 所示。

表 3 逻辑规则表达式

规则	表达式
新鲜性规则	$\frac{P \models \#(X)}{P \models \#(\alpha^X)}$
临时值验证规则	$\frac{P \models \#(X), P \models Q \mid \sim X}{P \models Q \models X}$
仲裁规则	$\frac{P \models Q \mid \Rightarrow X, P \models Q \models X}{P \models X}$
消息含义规则	$\frac{P \mid \Rightarrow Q \overset{K}{\leftrightarrow} P, P \triangleleft \{X\}_K}{P \models Q \mid \sim X}$
会话密钥规则	$\frac{A \models \#(K), A \models B \models X}{A \models A \overset{K}{\leftrightarrow} B}$
接收消息规则	$\frac{P \models P \overset{K}{\leftrightarrow} Q, P \triangleleft \{X\}_K}{P \models Q \overset{K}{\leftrightarrow} P}$
秘密与密钥规则	$\frac{P \models R \overset{K}{\leftrightarrow} R'}{P \models R' \overset{K}{\leftrightarrow} R}$
信念规则	$\frac{P \models (X, Y) \quad P \models Q \models (X, Y)}{P \models X \quad P \models Q \models X}$

5.2 假设条件以及协议理想化模型

本协议中涉及三个簇头 A 、 B 、 C 。 A 和 C 处在同一簇内,簇头 B 在另一簇内。 A 与 B 之间在初始化时已共享一个簇密钥 K_{12} 。协议要证明节点 B 与节点 C 新建立的密钥 K'_{12} 是保密的。理想模型如下所示。

a: $A \rightarrow C: \{K_{12}\}$;

b: $C \rightarrow B: \{g^z\}K_{12}$;

c: $B \rightarrow C: \{g^y\}K_{12}$ 。

假设: $C \models B \mid \Rightarrow g^y, C \models B \models g^y,$

$B \models C \mid \Rightarrow g^z \quad B \models B \overset{K_{12}}{\leftrightarrow} C,$

$C \models C \overset{K_{12}}{\leftrightarrow} B, B \models C \models g^z$

协议证明目标: $C \models C \overset{K_{12'}}{\leftrightarrow} B, B \models B \overset{K_{21'}}{\leftrightarrow} C,$
 $C \models B \models C \overset{K_{12'}}{\leftrightarrow} B, B \models C \models B \overset{K_{21'}}{\leftrightarrow} C.$

5.3 证明协议安全性

理想模型 b 可知 $B \triangleleft (g^z)K_{12}$, 由假设 $B \models B \overset{K_{12}}{\leftrightarrow} C$, 根据接收消息规则 $\frac{P \models P \overset{K}{\leftrightarrow} Q, P \triangleleft \{X\}_K}{P \triangleleft X}$ 可得:

$$B \triangleleft (g^z) \quad (1)$$

由 $B \models B \overset{K_{12}}{\leftrightarrow} C$ 和 $B \triangleleft (g^z)K_{12}$, 根据消含义规则 $\frac{P \models Q \overset{K}{\leftrightarrow} P, P \triangleleft \{X\}_K}{P \models Q \mid \sim X}$, 可得:

$$B \models C \mid \sim g^z \quad (2)$$

由 $B \models \#(y)$, 根据新鲜性规则 $\frac{P \models \#(X)}{P \models \#(\alpha^X)}$, 可得:

$$B \models \#(g^y) \quad (3)$$

根据由 (2) 和 (3), 以用临时值验证规则 $\frac{P \models \#(X), P \models Q \mid \sim X}{P \models Q \models X}$ 可得:

$$B \models C \models (g^z) \quad (4)$$

根据式 (4) 和信念规则 2: $\frac{P \models (X, Y)}{P \models X}$, 可得:

$$B \models C \models z \quad (5)$$

根据式 (4) 和假设 $B \models C \mid \Rightarrow g^z$, 以及仲裁规则 $\frac{P \models Q \mid \Rightarrow X, P \models Q \models X}{P \models X}$ 可得:

$$B \models g^z \quad (6)$$

同理可得:

$$C \models g^y \quad (7)$$

理想协议中簇头 B 接收到 g^z , 簇头计算密钥 $K_{12'} = (g^y)^z$ (8)

由 $C \triangleleft g^y, C \models \#(z)$, 根据新鲜性规则: $\frac{P \models \#(X)}{P \models \#(\alpha^X)}$, 可得:

$$C \models \#(K_{12'}) \quad (9)$$

假设 $C \models B \models g^y$, 在式 (9) 的基础上, 根据会话密钥规则 $\frac{A \models \#(K), A \models B \models X}{A \models A \overset{K}{\leftrightarrow} B}$, 可得

$$C \models C \overset{K_{12}}{\leftrightarrow} B \quad (10)$$

根据协议自身具有的对称结构, 得出 C 相信 B 一定同样能得到相同的信仰, 即:

$$C \models B \models C \overset{K_{12'}}{\leftrightarrow} B \quad (11)$$

同理可以证出,

$$B \models B \overset{K_{21'}}{\leftrightarrow} C \quad (12)$$

$$B|\equiv C|\equiv B\overset{K_{12'}}{\leftrightarrow}C$$

(13)

式(10)~(13)是通过 BAN 逻辑推理证明出安全性目标.簇头 A 更换为 C 时,将信息转移到下一簇头,新簇头与临近节点建立新密钥时,在基于信念逻辑推理上证明出簇头 C 和簇头 B 相信建立的新密钥是可信的,其他节点不知晓该密钥.

5.4 协议安全性分析

(1)保密性,假设存在恶意节点 D,接收到节点 C 和 B 之间发送的数据包,截获数据包后,由于传送数据过程中都经过加密,所以恶意节点无法解密数据.保证网络数据传送的保密性.(2)防止重放攻击,恶意节点 D 接收到节点 C 的数据包,伪装成节点 C 发送原数据包给节点 B,节点 B 收到数据包之后解密信息,得知是已发送过的数据包后直接丢弃,并通知监测节点去查询该恶意节点,防重放攻击.(3)防更改,协议中设置随机数的消息摘要,修改发送消息后会被立即发现.(4)新鲜性,协议中 C 节点与 B 节点利用临时密钥 K_{12} 建立新簇密钥之后立刻更新簇密钥.保证簇密钥的新鲜性.

6 结束语

本文提出一种簇头更换过程中的密钥管理方案.针对现有两种网络簇内密钥管理方案,论述了本方法的实施步骤.最后用 BAN 逻辑证明了本协议中簇头更换过程中新建立的密钥安全性.

参考文献:

[1] 李琳,王汝传,姜波,等.无线传感器网络层簇式密钥管理方案的研究[J].电子与信息学报,2006,12(28):2394-2397.

[2] 吴明,潘继强.一种分层式无线传感器网络密钥分配

管理方案[J].计算机与数字工程,2014,42(8):1459-1463.

[3] 周琴,李腊元,程真.一种基于分簇的无线传感器网络动态密钥分发协议[J].传感技术学报,2009,22(7):1002-1006.

[4] Wang Kai, Liu Yulin, Wan Qun, et al. Compressed Sensing of Wireless Sensor Networks Data with Missed Measurements[J]. Chinese Journal of Electronics, 2015, 24(2):388-392.

[5] 薛兵兵.基于无线传感网络的混合密钥管理机制研究[D].黑龙江:黑龙江大学,2012.

[6] 吴尊雷.无线传感器网络组密钥管理方案研究[D].杭州:杭州电子科技大学,2014.

[7] 陈锋,徐正全,徐彦彦.一种利用 Diffie-Hellman 密钥协商改进的 Kerberos 协议[J].计算机应用,2007,27(增刊2):116-117.

[8] Neng-Chung Wang, Yung-Kuei Chiang, Chih-Hung Hsieh. A Path-Based Approach for Data Aggregation in Grid-Based Wireless Sensor Networks[J]. Journal of Electronic Science and Technology, 2014, 12(3):313-317.

[9] 杨世平.安全协议及其 BAN 逻辑分析研究[D].贵阳:贵州大学,2007.

[10] 冯登国,范红.安全协议形式化分析理论与方法研究综述[J].中国科学院研究生院报,2003,20(4):389-406.

作者简介:

苑津莎 男,(1957-),教授,博士生导师.研究方向为智能信息处理、电磁场理论及应用.

张路路(通讯作者) 女,(1990-),硕士研究生.研究方向为智能信息处理. E-mail:lulu15075208311@126.com.

赵 曼 女,(1990-),硕士研究生.研究方向为智能信息处理.

(上接第 146 页)

作者简介:

杜高明 男,(1977-),副教授,硕士生导师.研究方向为多核集成电路体系结构、片上网络集成电路体系结构.

E-mail:duyaoming@hfut.edu.cn.

曹舒婷 女,(1991-),硕士生.研究方向为 SoC 设计、片上网络集成电路体系结构.

张多利 男,(1976-),教授,硕士生导师.研究方向为多核处理器体系结构与设计方法、多媒体专用集成电路设计实现等.