基于群密钥协商的无线传感器网络签名协议

于斌斌[1,2],武欣雨[1],初剑峰[1],胡 亮[1]

(1.吉林大学 计算机科学与技术学院,长春 130012;2.北华大学 信息技术与传媒学院,吉林省 吉林市 132013)

摘 要:为确保信息在无线传感器网络安全传输,提出了一个新的基于群密钥的安全协议。通过离散对数和哈希链的使用,可确保信息不被攻击者伪造或窃取。同时,考虑到无线传感器网络是由大量能量有限的节点构成,其计算能力不高,生存周期较短的特性,为节省传感器电池能量,降低能源的消耗,在初始化阶段传感器节点发送数据前通过服务器来完成群密钥协商。经过实验和理论分析,所提出协议的安全和效率整体上优于其他协议。

关键词:计算机系统结构;无线传感器网络;群密钥;哈希链;离散对数;数字签名

中图分类号:TP393 **文献标志码**:A **文章编号**:1671-5497(2017)03-0924-06

DOI:10.13229/j.cnki.jdxbgxb201703032

Signature protocol for wireless sensor network based on group key agreement

YU Bin-bin[1,2], WU Xin-yu[1], CHU Jian-feng[1], HU Liang[1]

(1. *College of Computer Science and Technology, Jilin University, Changchun* 130012, *China*; 2. *College of Information Technology and Media, Beihua University, Jilin* 132013, *China*)

Abstract: In order to guarantee the security of event update messages in transmission, a novel protocol is proposed based on the group key agreement. With the utilization of hash-chain keys and discrete logarithm, the attackers and malicious sensor nodes could not forge or modify the messages. Simultaneously, as the wireless sensor network is composed of massive low-energy sensor nodes with limited computing capacity and short life period, it is vital to save the battery energy and reduce the consumption. Therefore, in the initialization phase, namely before message transmission, the key agreement is completed with help of the server. Theoretical analysis and experiment verify that the proposed protocol is better than other protocols both in security and efficiency.

Key words: computer system organization; wireless sensor network; group key agreement; hash-chain; discrete logarithm; digital signature

收稿日期:2016-09-21.

基金项目:欧盟FP7国际合作项目(FP7-PEOPLE-2011-IRSES);国家科技支撑计划项目(2014BAH02F03).

作者简介:于斌斌(1984-),男,博士研究生.研究方向:网络安全.E-mail:22342690@qq.com

通信作者:初剑峰(1978-),男,副教授.研究方向:协议安全.E-mail:chujf@jlu.edu.cn

0 引　言

在无线传感器网络[1,2]中，传感器节点的能量由能量有限的电池提供，因此，网络中数据的传输和转发应尽量节省能量，传感器节点将采集的数据通过合适的路由发现算法建立从数据源到服务器，即汇聚节点的转发路径，使多个独立的节点相互协作形成一个多跳的数据传输网络。当前已存在的路由协议有平面路由协议，如基于协商的以数据为中心的 SPIN 自适应路由协议[3]；层次化路由协议，如依据现有电量和距离来完成分组的 LEACH 路由协议[4]；基于地理位置的路由协议，如分节点为激活和睡眠状态的基于位置的自适应保真度的 GAF 路由协议[5]，以及通过能量感知和地理信息支持选择最短路径的 GEAR 路由协议[6]。通过路由协议数据完成在无线传感器网络的转发并最后汇聚到汇聚节点上。随着无线传感器网络得到越来越多的关注和实际应用，如何保证数据在传输和转发过程中的真实性和完整性成为重要的安全问题。

2012 年，He 等[7]提出了一个基于身份验证方案的签名协议。该协议应用哈希函数和公钥密码体制来完成数字签名，消息以哈希树的形式在网络中层层传播。每一个认证节点都会分配其私钥并计算得到公钥，通过哈希函数和私钥为每一次转发进行签名。而在验证阶段，该协议则是通过双线性配对[8]的方法来确保消息传播的完整性和正确性。然而，在 2013 年，该协议被指出其尚存在安全方面的不足。攻击者在消息传输过程中，可以通过窃听的方式轻易获取并覆盖传感器节点的密钥，进而模仿合法用户来发送或转发消息，因此攻击者可以发动能量消耗攻击。而由于无线传感器网络中其他节点并不知情，该虚假消息也能够通过验证并被接收，给数据传递造成了极大风险。其次，由于在验证过程中使用了多次双线性对，节点将进行多次基于幂和函数的计算，故其计算量相对较大，效率也并不高。

接着，He 等[9]基于 Barreto 等人的认证方法提出了一个改进的签名方案，然而，与前一方案相同的是，该协议也无法完全保护密钥和抵抗能量消耗攻击，并也需要完成大量双线性对的计算来保证签名验证的准确性。

2013 年，Sahingoz 等[10]提出了一个多级的动态密钥协议，该协议基于非对称密钥的协商和椭圆曲线密码。传感器节点使用其私钥和公钥，与每一个邻居节点都进行协商来完成对数据的签名和验证。由于椭圆曲线群上离散对数问题计算的困难性，攻击者没有有效的办法来获取密钥并伪造消息。然而，因为每两个转发节点在传输过程中都要完成一次协商，该协议拥有很大的计算量，所以会对节点的能量造成巨大的损耗，故会减少电池的使用时间。

2015 年，Lin[11]提出了一个基于位置的密钥隔离签名协议。在该协议中，每一个节点拥有两个私钥，一个是短的由节点自身生成的私钥，而另一个是相对较长的存储在协助器里的私钥。我们设定协助器是一个安全性较高的独立外围设备，协议的安全性基于时间片更新和离散对数。在协助器的帮助下，传感器节点能周期性地在公钥保持不变的基础上更新其私钥。这样，在不同时间周期内，传感器节点将使用不同的私钥来进行数字签名。所以即使攻击者或恶意节点掌握之前时间片的私钥，它们也无法由其推断出当前时间片的私钥。同时，由于该协议对椭圆曲线密钥的使用，除密钥生成节点，其他节点或攻击者很难从发布的参数中逆运算得到相应的私钥，其难度等同于解决椭圆曲线离散对数问题[12,13]。而基于双线性对的验证算法更是确保信息是由相应的发送节点发出的，并在传输过程中没有被恶意的中间节点或攻击者伪造或篡改。然而，由于该算法还是需要进行双线性配对，依旧会产生很大的开销，需要大量的计算时间和高昂的代价。

针对以往研究中存在的问题和不足，本文基于哈希链和离散对数提出了一个新的协议。协议不使用造成高计算量的双线性对，而由服务器在初始化阶段，即传感器节点发送任何数据之前完成共享密钥的生成。所以所提协议在保证无线传感器网络安全同时延长了网络的使用周期。

1 协议介绍

1.1 设计原则

(1)由于无线传感器网络是由大量传感器节点经播撒或随意放置而成的分布式多跳自组织网络，其通信是不固定的。传感器节点的位置不能预先确定，节点之间的相互邻居关系也不预知。因此为保证传感器网络中的任意传感器节点都能相互通信，本协议采用了群密钥协商方案。由服务器，即汇聚节点预先在初始化阶段进行多方协

商生成一个所有传感器节点都可共享的群密钥。进而,汇聚节点可将该群密钥分发给各个节点。

(2)鉴于在无线传感器网络中,传感器节点可被俘获,恶意节点可以伪造或篡改合法信息,我们需要对传输的信息进行数字签名。在本协议中,签名和验证基于哈希函数链和离散对数。初始化阶段,应用哈希函数对密钥进行哈希函数链的操作,这样,在每一轮消息传输中,都将采用不同的密钥。这种基于哈希函数链不断动态变化的特性使攻击者不易捕获密钥,一定程度上保护了信息。同时,由于计算离散对数问题的困难性,攻击者没有合理有效的方法得到其他节点的私钥,因此攻击者无法伪造合法的有效信息且无法成功通过验证。在实际应用中,基于网络应用场景的不同,客户还可以根据需要选择是否进行加密。

(3)由于传感器节点的计算能力不强,电源能量有限,无线传感器网络的生存周期较短,因此,为了尽量节省能源,本协议在数据传输前使用汇聚节点来完成初始化阶段中群密钥和中间值的生成,各个传感器节点无须再进行额外的协商和开销,不会造成电池的损耗。且在对节点进行签名时,将使用针对接收节点而做的签名来生成针对汇聚节点的签名,因此可以减少第二个签名所需的计算量,降低电源能量的消耗,延长网络周期。

1.2 协议提出

本文所提出的安全协议共有3个阶段:初始化阶段,签名阶段和验证阶段。初始化阶段是在传感器节点发送消息之前完成的,因此并不耗电。签名阶段和验证阶段是为了保证信息在传输过程中不被攻击者篡改,因此这两个阶段是在传感器节点发送消息之后进行的,所以需要考虑其对电池能源的损耗。本文所需符号说明见表1。

表1 所需符号说明

Table 1 Explanation of notations

n	当前节点数量
ID_i	标识每个节点的编号
K_i^r	第 i 个节点在第 r 轮生成的一次性签名
M_i^r	第 i 个节点在第 r 轮发送的消息
K_g	群密钥
$H(x)$	哈希函数操作
Δi	初始化时所做签名
δ_i^r	由 K_i^r 所完成的签名
C_i^r	由 K_g 所完成的签名
KU_i	群密钥生成中由除第 i 个节点外的其余节点生成

1.2.1 初始化阶段

(1)哈希链的初始化

传感器节点 i 随机选择1个数 x_i 并计算一系列的一次性签名密钥 $K_i^n = H(x_i)$;$K_i^{r-1} = H(K_i^r)$,图1展示了具体的哈希链生成过程。

$$x_i \xrightarrow{H(x_i)} K_i^n \xrightarrow{H(K_i^n)} K_i^{n-1} \cdots \xrightarrow{H(K_i^1)} K_i^0$$

图1 哈希链的生成

Fig. 1 Hash-chain key generation

(2)群密钥的初始化

假设无线传感器网络中共有 n 个节点,由汇聚节点预先生成整个传感器网络的群共享密钥 $K_g = g^{x_1 x_2 \cdots x_n} \bmod n$,其中 g 是循环加法群的生成元。汇聚节点将生成的群密钥 K_g 广播给无线传感器网络中的各个节点。

(3)中间值 KU_i 的初始化

在群密钥生成过程中,汇聚节点同时也会为每个节点生成一个中间值 KU_i,该中间值由除了节点 i 外的所有节点协商而成,并分发给相应节点。如第1个节点会得到 $KU_1 = g^{x_2 x_3 \cdots x_n}$,第2个节点会得到 $KU_2 = g^{x_1 x_3 x_4 \cdots x_n}$,…,第 n 个节点将会得到 $KU_n = g^{x_1 x_2 x_3 \cdots x_{n-1}}$。$KU_i$ 将被用于转发节点的验证过程,以确定消息转发的正确性。

(4)初始签名 Δi 的初始化

使用群密钥 K_g、第一个一次性签名 K_i^0 以及身份标识 ID_i 计算 Δi 得 $i = H(K_i^0 \mid K_g \mid \mathrm{ID}_i)$。

1.2.2 签名阶段

本协议中,消息的传递与转发依据adhoc网络的路由发现算法,发送消息的传感器节点 i 对消息进行签名如下。

(1)在第1轮消息传递过程中,传感器节点 i 首先用 K_g 做一个签名 $C_i^1 = H(K_g \mid M_i^1 \mid i \mid \mathrm{ID}_i)$ 并将它保存起来。进而,节点 i 用这个已知的签名和 K_i^1 继续生成一个新的签名 $\delta_i^1 = H(C_i^1 \mid K_i^1)$。节点 i 将 $C_i^1 = H(K_g \mid M_i^1 \mid i \mid \mathrm{ID}_i)$,$\delta_i^1 = H(C_i^1 \mid K_i^1)$,$\triangle i$,$K_i^0$ 发给下一层节点。

(2)在第 r 轮的消息传递过程中,传感器节点 i 用 K_g 完成第一个签名 $C_i^r = H(K_g \mid M_i^r \mid \mathrm{ID}_i)$ 并将它保存起来。进而,节点 i 用这个已知的签名和 K_i^r 继续生成一个新的签名 $\delta_i^r = H(C_i^r \mid K_i^r)$。节点 i 将 $C_i^r = H(K_g \mid M_i^r \mid \mathrm{ID}_i)$,$\delta_i^r = H(C_i^r \mid K_i^r)$,$K_i^{r-1}$,$M_i^{r-1}$ 发给下一层节点。

下述等式展示了传感器节点 i 所发送的经过签名的消息:

$$\begin{cases} C_i^1 = H(K_g \mid M_i^1 \mid i \mid \mathrm{ID}_i) \\ C_i^r = H(K_g \mid M_i^r \mid \mathrm{ID}_i) \end{cases}$$

$$\begin{cases} \delta_i^1 = H(C_i^1 \mid K_i^1), i, K_i^0 \\ \delta_i^r = H(C_i^r \mid K_i^r), K_i^{r-1}, M_i^{r-1} \end{cases}$$

1.2.3　验证阶段

当转发节点或汇聚节点接收到发送的消息时，需要对其进行验证，判断其合法性。转发节点和汇聚节点所要完成的工作如下：

(1)转发节点 j 接收消息

①转发节点 j 用自己的私钥 x_j 和中间值 KU_j 计算 $KU^{x_j} \bmod n$。根据离散对数知识可知计算得到的值应等于群密钥 $K_g = g^{x_1 x_2 \cdots x_n} \bmod n$ 的值。

②在第 1 轮消息传递过程中，接收节点 j 计算 $H(K_g \mid K_i^0 \mid \mathrm{ID}_i)$ 来判断其是否与 Δi 相等。如果等式成立，则我们认为消息合法。

③在第 r 轮的消息传递过程中，接收节点 j 只需计算 $H(K_g \mid M_i^{r-1} \mid i \mid \mathrm{ID}_i)$，并通过验证其是否与 C_i^{r-1} 相等来验证消息的完整性和正确性。

(2)汇聚节点接收消息

①如果消息已发送到汇聚节点，即服务器上，则在第 1 轮消息传递过程中，汇聚节点计算 $H(K_g \mid K_i^0 \mid \mathrm{ID}_i)$，如果计算得到的值与 Δi 相等，则 K_i^0 可以确认为合法的。

②在第 r 轮的消息传递过程中，汇聚节点首先验证 $K_i^{r-2} = H(K_i^{r-1})$ 是否成立，以保证签名密钥 K_i^{r-2} 的真实性，其中 $r = 2,3,4,\cdots,n$，且 K_i^{r-2} 在第 $(r-1)$ 轮中已被获得，故已知。如果等式成立，汇聚节点继续计算哈希函数值 $H(C_i^{r-1} \mid K_i^{r-1})$ 并判断它是否与接收到的 δ_i^{r-1} 相等。如果验证成功，汇聚节点则认为消息没有被攻击者篡改。

图 2 详细地展现了上述的签名验证传输过程，对协议进行了具体的解释。

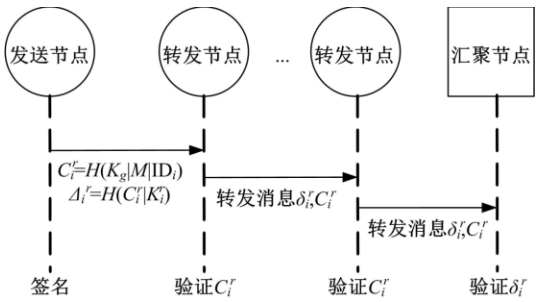

图 2　消息传输

Fig. 2　Message transmission

2　安全和效率分析

2.1　安全性分析

本协议中，每个传感器节点都会选择一个随机数作为自己的私钥，根据离散对数，汇聚节点可以生成一个群共享的会话密钥 $K_g = g^{x1x2\cdots xn} \bmod n$，接收节点可根据私钥，中间值和共享的群密钥来判断消息的发出者是否正确，即是否由其他节点伪造。同时，针对无线传感器网络密钥的易俘获性，本文采取用哈希函数链对密钥保护的方法，使其在每轮的消息传递过程中不断变化。并且由于哈希函数的单向性和强抗碰撞性，无法从哈希函数值逆向得到被签名的内容，且在计算上找到两个拥有相同的哈希值的不同消息是不可行的。本文用前一轮的哈希链密钥来验证当前轮消息的合法性。而且，由于离散对数问题计算的困难性和复杂性，一个传感器节点无法得到其他节点的私钥，所以经过签名的哈希值得到了进一步保护。因此攻击者不能发动伪造攻击或篡改消息。

即使攻击者可以拦截或伪造公共信息如 $K_i^{r-1}, M_i^{r-1}, \mathrm{ID}_i$，由于私钥的不易获得性，攻击者没有有效的办法来伪造 K_g，所以攻击者无法成功通过验证。因此，假设最坏情况攻击者成功捕获拦截到了 K_i^{r-1}，并修改其为 $K_i^{r-1}{}'$，同时攻击者向接收节点或汇聚节点发送其自己伪造或篡改的消息 $M_i^{r-1}{}'$。然而，攻击者还是无法生成一个合法有效的哈希值 $H(K_g \mid M_i^{r-1}{}' \mid i \mid \mathrm{ID}_i)$，使其等于 C_i^{r-1}，所以攻击节点所伪造修改的消息无法被转发节点验证接收，即可以防止恶意的中间节点伪造消息发动能量消耗攻击。而对汇聚节点，也是同样的情况，攻击者所伪造的哈希值 $H(C_i^{r-1}{}' \mid K_i^{r-1}{}')$ 仍然不等于 δ_i^{r-1}，故汇聚节点也不会验证通过，所以即使发送节点就是恶意的，汇聚节点也可以通过验证阻止其发动能量消耗攻击。因为攻击者只能通过传感器节点的公钥 $g^x \bmod n$ 来获得 x_i，而其计算的难度等同于解决 DL 问题。攻击者无法重新用其伪造或篡改的信息得到正确的签名信息，故无法成功通过接收节点或汇聚节点的验证，所以攻击者无法发动有效攻击，确保了无线传感器网络传输的安全性。

2.2　效率分析

为了更好地说明本文提出的协议的效率，将本协议与之前的部分协议进行了比较，表 2 展示了比较结果。假设忽略一次性操作，hash 代表哈

希函数操作,K 代表传感器节点的密钥,bp 代表双线性配对操作。

(1)初始化阶段效率

在本协议里,由于无线传感器网络中可共享的群密钥 K_g 是由汇聚节点服务器预先生成的,所以尽管产生 K_g 需要进行协商并产生中间值,这个过程也不会造成传感器节点电池的损耗和能源的消耗。同时,因为在生成分配群密钥的过程中对离散对数的计算是由服务器进行的,所以也不存在计算量超过传感器有限计算能力的情况。所以,本文不对初始化阶段效率进行比较。

(2)签名阶段效率

在之前所介绍的相关方案中,无论是 He 等[9]、Sahingoz 等[10]还是 Lin[11]提出的方案,都和本协议一样需要在签名阶段使用哈希函数。在本文协议中,只需在每个节点最初发送消息之前对哈希函数链进行一次必要的初始化,之后只需使用所得到的哈希链的值。而且,尽管在本文协议中,每当有一个消息需要被发送时,发送节点都需要做两次签名。但是,节点在生成第一个签名 $H(K_g \mid M_i^r \mid \mathrm{ID}_i)$ 后,会将其保存为 C_i^r,继而用这个已得到的签名生成下一个签名 $\delta_i^r = H(C_i^r \mid K_i^r)$,所以并不会产生额外的操作和多余的计算。并且,在本文协议中,只有发送节点需要完成对信息的签名。然而,对于 Sahingoz 等人的方案,任意两个节点在转发消息时都要进行一次密钥的协商,这会造成较大的开销。另外对于内存占用,由于 Lin 的方案中每个节点将保存两个私钥,因此需要一个额外的位置。

(3)验证阶段效率

在本协议中,接收节点和服务器需要对发送节点发送的消息进行验证,由于服务器的验证并不会减少网络的能量,本文艺事业只考虑接收节点的验证。而该验证只需基于哈希链和离散对数,并不需要进行双线性配对。但何道静等人、Sahingoz 等人的协议在验证阶段需要额外的两次双线性对操作,Lin 方案的验证则需要四次双线性对的计算。因此,本文协议更满足无线传感器网络能源和计算有限的特性,减少了冗余的计算,降低了传感器电池的损耗。

表 2 与其他协议的比较

Table 2 Comparisons with other protocols

协议	内存占用	签名阶段计算开销	验证阶段计算开销	密钥生成和协商开销	发送节点为恶意节点时	中间节点为恶意节点时
何道静的协议	$n$hash	2hash	2bp+1hash	n	不安全	不安全
Ozgur 的协议	$n$hash	2hash	2bp+1hash	c_n^2	安全	安全
Lin 的协议	$n$hash+nK	2hash	4bp+1hash	n	安全	安全
本文协议	$n$hash+1K	2hash	1hash	n	安全	安全

3 结束语

针对当前无线传感器网络存在的安全问题,提出了一个新颖的签名协议。本协议基于离散对数问题的不易解决性来实现签名并完成对传送数据的保护,同时通过对哈希函数链的使用来确保密钥无法轻易地被攻击者所获得。因此,攻击者无法在转发过程中伪造或篡改合法信息,保证了数据的真实性和完整性。考虑到在无线传感器网络中,传感器节点是由电池来提供能量的,因此为了使本安全协议消耗尽量少的能源,本文利用汇聚节点,即服务器来进行协商完成群密钥的生成,因此减少了传感器节点冗余的计算量,延长了无线传感器网络的生存周期。通过分析和比较可知,本协议同时拥有较强的安全性和较高的效率。

参考文献:

[1] Mohsen A, Aljoby W, Alenezi K. A robust harmony search algorithm based Markov model for node deployment in hybrid wireless sensor networks[J]. International Journal of GEOMATE, 2016, 27(11): 2747-2754.

[2] Zhang W, Liu Y, Das S, et al. A watermark based authentication supportive approach[J]. Pervasive and Mobile Computing, 2008, 4(5): 658-680.

[3] Yuan Arak Sac, Fang Hsiang-Ting, Wu Quincy. Open flow based hybrid routing in wireless sensor networks[C]// 9th IEEE International Conference on Intelligent Sensors, Singapore, 2014: 21-24.

[4] Ma Z F, Li G M, Gong Q. Improvement on LEACH-C protocol of wireless sensor network[J]. International Journal of Future Generation Commu-

nication and Networking, 2016, 9(2): 183-192.

[5] Qi Xiao-gang, Qiu Chen-xi. An improvement of gaf for lifetime elongation inwireless sensor networks [C] // 5th International Conference on Wireless Communications, Beijing, China, 2009: 14-21.

[6] Shen Yi-ming, Wu Qiong, Wang Xiao-peng. Wireless sensor network energy-efficient routing techniques based on improved gear[C] // IEEE International Conference on Network Infrastructure and Digital Content, Beijing, China, 2009: 114-117.

[7] He D, Chen C, Chan S. SDRP: A secure and efficient reprogramming protocol for wireless sensor networks[J]. IEEE Trans Ind Electron, 2012, 59 (11): 4155-4163.

[8] Du Hong-zhen. Efficient certificateless signcryption from bilinear pairings[J]. International Journal of Security and ITS, 2016, 10(4): 303-316.

[9] He D, Chen C, Chan S, et al. Security analysis and improvement of a secure and distributed reprogramming protocol for wireless sensor networks [J]. IEEE Transactions on Industrial Electronics, 2013, 60 (11): 5348-5354.

[10] Sahingoz O K. Large scale wireless sensor networks with multi-level dynamic key management scheme [J]. Journal of Systems Architecture, 2013, 59(9): 801-807.

[11] Lin Han-yu. Location-based data encryption for wireless sensor network using dynamic keys [J]. Wireless Networks, 2015, 21(8): 2649-2656.

[12] Craig Prather J, Bolt Michael, Harrell Haley, et al. Antenna design for a massive multiple input environmental sensor network[J]. Digital Communications & Networks, 2016, 2(4): 256-259.

[13] Yang Jian-jun, Fei Zong-ming, Shen Ju. Hole detection and shape-free representation and double landmarks based geographic routing in wireless sensor networks[J]. Digital Communications & Networks, 2015, 1(1): 75-83.