WSN 中基于多项式的节点捕获攻击防御方法*

周 捷[1,2], 郭渊博[1]

(1. 解放军信息工程大学 电子技术学院, 郑州 450004; 2. 中国人民解放军 77651 部队, 拉萨 850000)

摘 要: 针对无线传感器网络中捕获节点所带来的安全威胁,提出一种基于二元多项式的节点捕获攻击的防御方法。该方法将节点密钥信息与节点部署时间和身份标志进行绑定,当节点之间协商会话密钥时,节点间需相互验证部署时间与当前时间的差值,并结合基站验证节点的合法性。方案在阻止攻击者利用捕获节点窃听网络通信的同时,防范捕获节点与合法节点建立会话密钥,有效地防止了捕获节点重新加入网络。通过分析证明了该方案的安全性且系统开销低。

关键词: 无线传感器网络; 对称多项式; 节点捕获攻击; 防御

中图分类号: TP393 **文献标志码**: A **文章编号**: 1001-3695(2012)09-3475-03

doi:10.3969/j.issn.1001-3695.2012.09.073

Polynomial-based defense scheme against node capture attack in WSN

ZHOU Jie[1,2], GUO Yuan-bo[1]

(1. *Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou* 450004, *China*; 2. *PLA Unit* 77651, *Lhasa* 850000, *China*)

Abstract: Considering the security issue caused by captured node in wireless sensor networks, this paper presented a polynomial-based scheme to defend node capture attack. This scheme bounded the key material of each node with its original deployment time and identity. When the nodes negotiated the session key, they needed to mutually authenticate the interval time among the deployment time and the current time, and it made use of the base station to verify the legitimacy of the node. This scheme could prevent attackers from eavesdropping communication, and avoid the captured nodes establishing a session key with legitimate nodes at the same time, which effectively prevented the capture nodes re-joining the network. Analysis shows the safety and low system overhead of the scheme.

Key words: wireless sensor networks(WSN); symmetric polynomials; node capture attack; defense

无线传感器网络得到日益广泛的应用,如监视和跟踪目标、环境采样、远程工厂控制和卫生监督等。一个典型的传感器节点由低成本的硬件构成,在电源、通信和计算能力等方面受到限制。传统的安全机制无法应用于传感器节点,从而使得无线传感器网络面临许多方面的安全挑战,如路由安全、节点捕获攻击、密钥管理与 DoS 攻击等。而节点捕获攻击被认为是最严重的安全威胁之一[1],它易于发动,而难以检测,并且它是复制攻击、Sybil、虫洞、黑洞等攻击的基础。

节点捕获攻击中,攻击的行动可分为三个阶段[2]:

a)物理捕获传感器节点,妥协它们并获取其中的敏感信息,如密钥等。

b)将妥协节点(compromised node)重新部署在网络中。

c)发动内部攻击。

目前,针对节点捕获攻击防御方案的研究大多采用密钥管理方案防范攻击者窃听网络中通信,如虚拟密钥环(virtual key ring)方案[3]和门限密钥共享模型[4]等。此类方案中,攻击须捕获大量的节点才能对网络造成威胁,从而有效防止攻击者捕获并妥协节点后侦听其他节点间安全通信的问题,但不能防止攻击者将捕获节点(capture node)重新部署在网络中进行其他类型的攻击;另一些方案则是研究传感器网络中各种内部攻击的防范机制,如 Sybil 攻击[5]、复制节点攻击[6,7]。而防范节点捕获攻击最有效的方法是在防范攻击者利用捕获节点窃听网络通信的同时,防止捕获节点重新部署到网络中。

本文基于二元对称多项式提出一种防范节点捕获攻击的方案,方案绑定节点部署时间与节点身份标志作为二元多项式中的一项,当节点间进入密钥阶段时,节点间利用部署时间进行相互验证;当利用部署时间无法判断节点是否合法时,节点通过发送验证请求,利用基站验证节点的合法性。本方案基于二元多项式复杂性防止攻击者利用捕获节点中有用信息侦听网络,同时阻止捕获节点与其邻居节点建立会话密钥,从而达到阻止其重新部署到网络的目的。

1 网络模型

假设无线传感器网络是基于分簇的异构网络,有三种不同的节点,分别为基站(BS)、簇首节点和普通节点。图 1 给出了传感器网络的结构。

基站负责整个网络的控制并且接收簇首节点发送的数据。基站通信范围覆盖整个网络,作为网络的控制中心,一般部署在有人值守的环境中。簇首节点负责数据的采集,并将接收的数据预处理后传送给基站;普通节点负责收集数据,然后将数

收稿日期: 2012-01-01; **修回日期**: 2012-03-08 **基金项目**: 河南省科技创新杰出青年计划资助项目(104100510025)

作者简介:周捷(1986-),男,硕士研究生,主要研究方向为无线网络安全(czechou@163.com);郭渊博(1975-),男,副教授,博士(后),主要研究方向为容忍入侵、无线网络安全.

据传送给簇首节点。

各节点中,基站能量、存储空间与计算能力均为最强,普通节点最弱。

假设网络中的传感器节点采用文献[8]中时间同步机制,这样能够解决传感器节点之间时间同步问题,节点在部署到网络中某一位置的瞬间记录下自己的当前时间。

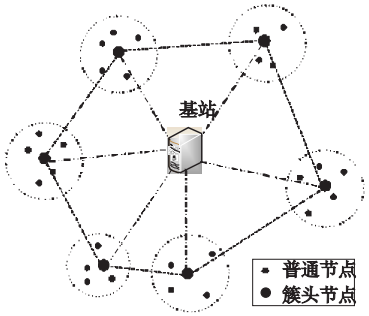

图1 传感器网络结构

2 基于多项式的密钥分配方案

传感器节点部署在指定监测区域之前,由服务器随机产生一个有限域 $GF(p)$ 中的二元对称多项式:

$$f(x,y)=\sum_{i,j=0}^{t}a_{ij}x^iy^j$$

其中:p 为一个大素数,t 为此多项式的度。而对称的含义是对于任何 x 和 y,上述多项式都满足 $f(x,y)=f(y,x)$。此多项式必须保密,每个节点在部署前预装此多项式。表 1 给出了文中所用到的符号。

表 1 符号表示

名称	含义
BS	基站
CH_i	簇头节点
S_k	普通节点
ID_i	节点 i 的标志
t_i	节点 i 的部署时间
T_1	攻击者攻破簇头节点的最短时间
T_2	攻击者攻破普通节点的最短时间
$H(x)$	对 x 进行散列运算
K_{i-j}	节点 i 计算的与节点 j 的对称密钥
$f(x,y)$	t 阶二元多项式
|	连接符号
$K(x)$	用密钥 k 加密 x
N_i	节点 i 产生的随机数
$conf_i$	基站为节点 i 计算的认证数
$K(MAC(M))$	密钥 K 加密的消息 M 的认证码

2.1 节点初始化

首先节点将自己的部署时间值 t_i 与标志 ID_i 代入原始多项式,得到 $f(H(t_i|ID_i),y)$,并永久性删除原多项式。簇头节点与普通节点必须分别在 T_1 与 T_2 时间内完成密钥建立。簇头节点的安全性高于普通节点,因此攻击者攻破簇头节点所用时间大于普通节点,即 $T_1>T_2$。

2.2 密钥建立阶段

2.2.1 簇头节点与基站会话密钥协商

簇头节点完成初始化后,首先与基站建立会话密钥。具体的密钥协商过程如下。

a)簇头节点发送消息给基站

$$CH_i\rightarrow BS:t_{CH_i},ID_{CH_i}$$

基站首先对 CH_i 的身份进行验证,并判断 t_{CH_i} 与当前时间的差值是否小于 T_1,如果不是,由于攻击者攻破一个簇头节点的最短时间为 T_1,于是基站拒绝与 CH_i 建立密钥;如果是,基站对簇头节点的部署时间与身份标志进行散列运算,并生成一个随机数 N_{BS} 代入二元多项式中,生成与 CH_i 的会话密钥 $K_{BS\text{-}CH_i}$:

$$K_{BS\text{-}CH_i}=f(H(t_{CH_i}|ID_{CH_i}),N_{BS})$$

b)基站返回确认消息

基站回复 CH_i 消息,表明同意建立会话密钥:

$$BS\rightarrow CH_i:N_{BS},K_{BS\text{-}CH_i}(MAC(N_{BS})),OK$$

CH_i 生成与 BS 的会话密钥:

$$K_{CH_i\text{-}BS}=f(H(t_{CH_i}|ID_{CH_i}),N_{BS})$$

2.2.2 簇头节点间会话密钥协商

a)CH_i 广播一个 Hello 消息

$$CH_i\rightarrow *:Hello,t_{CH_i},ID_{CH_i}$$

CH_j 接收到 Hello 消息后,检查簇头节点 CH_i 的部署时间与当前时间的差值是否小于 T_1,如不是,则拒绝建立密钥;若是,则计算与 CH_i 的会话密钥 $K_{CH_j\text{-}CH_i}$,然后发送消息给簇头节点 CH_i。

$$K_{CH_j\text{-}CH_i}=f(H(t_{CH_j}|ID_{CH_j}),H(t_{CH_i}|ID_{CH_i}))$$

b)CH_j 发送消息给 CH_i

$$CH_j\rightarrow CH_i:t_{CH_j},ID_{CH_j},K_{BS\text{-}CH_j}(MAC(t_{CH_j}|ID_{CH_j})),OK$$

簇头节点 CH_i 检查 CH_j 的部署时间与当前时间的差值是否小于 T_1,若是,则计算与簇头节点 CH_j 的会话密钥:

$$K_{CH_i\text{-}CH_j}=f(H(t_{CH_i}|ID_{CH_i}),H(t_{CH_j}|ID_{CH_j}))$$

若大于 T_1,则簇头节点 CH_i 需对 CH_j 进行验证。验证方法是节点 CH_i 生成一个随机数经节点 CH_j 交给基站,通过基站生成一个认证数发送给节点 CH_i,以验证节点 CH_j 的合法性。节点 CH_i 生成一个随机数 N_{CH_i},并计算 $f(H(t_{CH_i}|ID_{CH_i}),N_{CH_i})$。

c)CH_i 发送消息给 CH_j

$$CH_i\rightarrow CH_j:K_{CH_i\text{-}BS}(t_{CH_i},ID_{CH_i},N_{CH_i})$$

d)CH_j 转发 CH_i 的消息给 BS

$$CH_j\rightarrow BS:K_{CH_j\text{-}BS}(ID_{CH_j},K_{CH_i\text{-}BS}(t_{CH_i},ID_{CH_i},N_{CH_i}))$$

BS 计算得到认证数:

$$conf_{CH_i}=f(H(t_{CH_i}|ID_{CH_i}),N_{CH_i})$$

e)BS 将计算结果直接返回给 CH_i,簇头节点 CH_i 检查 $conf_{CH_i}$ 与自己的计算结果是否相同,若相同,则与节点 CH_j 建立会话密钥 $K_{CH_i\text{-}CH_j}$;若不同或未收到基站的消息,则拒绝与节点 CH_j 建立会话密钥。

2.2.3 普通节点与簇头节点间会话密钥协商

a)节点 S_k 发送请求消息给簇头节点 CH_i

$$S_k\rightarrow CH_i:Hello,t_k,ID_k,N_k$$

CH_i 计算当前时间与 t_k 的差值是否小于时间 T_2,若大于,拒绝建立密钥;若小于,生成密钥 $K_{CH_i\text{-}S_k}$,并发送消息给 BS。

$$K_{CH_i\text{-}S_k}=f(H(t_{CH_i}|ID_{CH_i}),H(t_k|ID_k))$$

b)CH_i 发送消息给 BS

$$CH_i \rightarrow BS: K_{CH_i\text{-}BS}(ID_{CH_i}, t_k, ID_k, N_k)$$

基站计算认证数 $conf_k = f(H(t_k \mid ID_k), N_k)$,并将此消息发送给簇头节点 CH_i。

c)BS 将认证数 $conf_k$ 发送给 CH_i

$$BS \rightarrow CH_i: K_{BS\text{-}CH_j}(conf_k)$$

簇头节点 CH_i 解密得到 $conf_k$。

d)CH_i 发送认证数给 S_k

$$CH_i \rightarrow S_k: t_{CH_i}, ID_{CH_i}, conf_k, K_{CH_i\text{-}S_k}(MAC(t_{CH_i} \mid ID_{CH_i} \mid conf_k)), OK$$

节点 S_k 验证 $conf_k$ 与自己的计算结果,若相等则与簇头节点 CH_i 建立密钥 $K_{S_k\text{-}CH_i}$。

$$K_{S_k\text{-}CH_i} = f(H(t_k \mid ID_k), H(t_{CH_i} \mid ID_{CH_i}))$$

3　安全分析

本章分析文中方案的安全性。首先说明攻击者可能造成威胁的方式有:a)利用捕获节点中的密钥信息侦听网络中的安全通信;b)利用捕获节点与网络中其他正常节点建立会话密钥,从而实现攻击网络的目的。

本方案中,攻击者捕获某节点后,只能获取到该捕获节点与其他节点的会话密钥,而无法利用这些密钥直接侦听其他节点间的通信。由于网络中各节点在部署到网络后,生成一个多项式,该多项式绑定部署时间与节点 ID,所以各节点中的多项式与其他节点均不相同,而会话密钥只由通信节点双方的部署时间与节点 ID 构成,节点中的某一会话密钥只能用于某一通信节点,而不能用于与该节点外的其他节点进行通信。因此,攻击者获取到的捕获节点中密钥信息无法用于侦听其他节点间的安全通信。

攻击者可能将捕获节点重新部署在网络中发动其他类型的攻击。如果攻击者成功地将捕获节点部署到网络中,则对网络安全造成极大的影响。然而它在实施这些攻击之前,必须与其他节点建立会话密钥才可以接收到其他节点的消息,进而发送或转换其他节点的消息,以达到攻击网络的目的。攻击者可能伪造节点的标志和部署时间,以试图与其他节点建立会话密钥。下面分别对簇头节点与普通节点的安全性进行分析。

如果某簇头节点 CH_i 为捕获节点 $C(i)$,$C(i)$ 试图与其他节点建立会话密钥,则存在以下三种情况:

a)捕获节点 $C(i)$ 与 BS 协商会话密钥。捕获节点 $C(i)$ 发送标志 $ID_{C(i)}$ 与部署时间 $t_{C(i)}$ 给 BS 请求建立会话密钥,BS 接收到该消息后,首先验证 $t_{C(i)}$ 与当前时间的差值是否小于 T_1,若不是,基站拒绝与节点 $C(i)$ 建立密钥;若小于,BS 将 $t_{C(i)}$ 与 $ID_{C(i)}$ 代入二元多项式中,计算 $K_{BS\text{-}C(i)} = f(H(t_{C(i)} \mid ID_{C(i)}), N_{BS})$,并将 N_{BS} 发送给节点 $C(i)$,节点计算 $K_{C(i)\text{-}BS} = f(H(t_{CH_i} \mid ID_{CH_i}), N_{BS})$。由于攻击者必须通过伪造才能通过基站对部署时间差值的验证,部署时间 $t_{C(i)} \neq t_{CH_i}$,所以 $K_{BS\text{-}C(i)} \neq K_{C(i)\text{-}BS}$。因此,捕获节点 $C(i)$ 无法与基站建立会话密钥。

b)捕获节点 $C(i)$ 与相邻簇头节点 CH_j 协商会话密钥。由情况 a)可知,捕获节点通过伪造部署时间而无法与其他节点建立会话密钥。现考虑以下两种可能。

(a)节点 $C(i)$ 请求与相邻簇头节点 CH_j 建立密钥,节点 CH_j 接收到节点 $C(i)$ 的密钥建立请求后,验证 $t_{C(i)}$ 与当前时间的差值,如果 $t_{C(i)} = t_{CH_i}$,其差值必定大于 T_1,节点 CH_j 拒绝建立密钥,如果 $t_{C(i)} \neq t_{CH_i}$,$K_{CH_j\text{-}C(i)} \neq K_{C(i)\text{-}CH_j}$。

(b)新簇头节点 CH_j 请求与节点 $C(i)$ 建立密钥,如果新节点 CH_j 验证 $C(i)$ 的部署时间后,与其建立密钥,由于 $t_{C(i)} \neq t_{CH_i}$,因此 $K_{CH_j\text{-}C(i)} \neq K_{C(i)\text{-}CH_j}$。如果 $t_{C(i)} = t_{CH_i}$,节点 CH_j 验证节点 $C(i)$ 是否为网络中节点,发送消息(t_{CH_j}、ID_{CH_j}、N_{CH_j})给节点 $C(i)$ 让其转交给基站,由于节点 $C(i)$ 无法与基站建立连接,因此,节点 CH_j 接收不到基站的返回值,则不与节点 $C(i)$ 建立会话密钥。

c)捕获节点 $C(i)$ 与普通节点 S_k 协商会话密钥。与情况 b)相似,节点 S_k 需节点 $C(i)$ 提交消息给基站,基站生成认证数后由节点 $C(i)$ 返回给节点 S_k 才可以建立会话密钥。由于节点 $C(i)$ 无法与基站建立连接,因此,节点 S_k 不与节点 $C(i)$ 建立会话密钥。

如果某普通节点 S_k 为捕获节点 $C(i)$,其发送会话密钥建立请求给簇头节点 CH_i,节点 CH_i 验证节点 $C(i)$ 的部署时间 $t_{C(i)}$ 与当前时间的差值,如果 $t_{C(i)} = t_k$,由于攻击者捕获一个普通节点的最短时间为 T_2,则其差值必定大于 T_2,节点 CH_i 拒绝与其建立连接;如果节点 $C(i)$ 通过伪造部署时间获得节点 CH_i 同意密钥建立,由于 $t_{C(i)} \neq t_k$,那么 $K_{CH_i\text{-}C(i)} \neq K_{C(i)\text{-}CH_i}$,节点 $C(i)$ 无法与节点 CH_i 建立会话密钥。

4　开销分析

假设传感器网络中有 n 个普通节点、m 个簇头节点。网络中各种类型节点的通信开销均不相同,普通节点只与簇头节点进行通信,则全网普通节点的通信开销为 $2n$;簇头节点分别与基站、邻居簇头节点、普通节点进行通信,全网簇头节点与基站建立密钥时的通信开销为 $2m$,与普通节点的通信开销为 $4n$。设各簇头节点平均邻居数为 d_1,需认证的平均邻居数为 d_2,那么簇头节点间的通信开销为 $(1 + d_1 + 3d_2)m$;基站的通信主要用于与簇头节点建立会话密钥,以及对普通节点与部分簇头节点进行认证,其通信开销为 $(2d_2 + 2)m + 2n$。因此,本方案中各种类型节点的通信开销如表 2 所示。

表 2　各类型节点通信开销

节点类型	通信开销
普通节点	$2n$
簇头节点	$(1 + d_1 + 3d_2)m$
基站	$(2d_2 + 2)m + 2n$

本方案采用的是一元 t 度对称多项式建立会话密钥,因此攻击者在捕获 $(t+1)$ 个节点后才能够计算出 t 度对称多项式的信息。在本方案中,节点建立会话密钥的计算开销主要是计算一个一元 t 度对称多项式 $\sum_{i=0}^{t} a_i x^i = a_0 + a_1 x + \cdots + a_t x^t$。由于计算加法的开销远小于乘法,因此本方案主要分析乘法运算的开销。假设变量的每个幂运算只计算一次,如已计算出 x^3,计算 x^4 时计一次乘法运算,故本方案中需要进行 $2t-1$ 次乘法运算。

而在存储开销方面,本文方案只需要存储一个一元 t 次多项式。假设多项式中每个系数占用一个存储空间,则它的存储空间为 $t+1$。

5　结束语

节点捕获攻击是一种严重威胁无线传感器网络安全的攻击手段,目前的研究集中于捕获节点部署到网络中所发动的内部攻击,而防范此类攻击最有效的方法应是　(下转第 3482 页)

(上接第 3477 页)阻止捕获节点重新加入到网络中与其他节点进行会话。本文基于二元对称多项式提出一种防御节点捕获攻击的方案,该方案将每个节点拥有的密钥和身份标志与部署时间进行绑定,攻击者仅能获取到捕获节点与其邻居节点的会话密钥,防止攻击者利用捕获节点侦听其他网络通信;而当捕获节点请求与网络中节点建立密钥时,结合部署时间与基站进行验证,防止捕获节点与其邻居节点建立会话密钥,以达到防止捕获节点发动内部攻击的威胁。

参考文献:

[1] PERRIG A, STANKOVIC J, WAGNER D. Security in wireless sensor networks[J]. Communications of the ACM, 2004,47(6):53-57.

[2] DING Wei, YU Ying-bing, YENDURI S. Distributed first stage detection for node capture[C]//Proc of IEEE GLOBECOM Workshops. 2010:1566-1570.

[3] VU T M, SAFAVI-NAINI R, WILLIAMSON C. Securing wireless sensor networks against large-scale node capture attacks[C]//Proc of the 5th ACM Symposium on Information, Computer and Communications Security. New York:ACM,2010:112-123.

[4] 柳亚男,王箭,杜贺. 无线传感器网络门限密钥共享模型[J]. 电子与信息学报,2011,33(8):1913-1918.

[5] NEWSOME J, SHI E, SONG D, *et al*. The Sybil attack in sensor networks: analysis and defenses[C]//Proc of the 3rd International Symposium on Information Processing in Sensor Networks. New York: ACM,2004:259-268.

[6] 伏飞,齐望东. 实现位置及时间绑定的密钥分发——防御传感器网络节点复制攻击的新方法[J]. 通信学报,2010,31(4):16-25.

[7] 廖耀华,王晓明. 无线传感网络中抵抗节点复制攻击新方法[J]. 计算机工程与应用,2011,47(22):64-47,70.

[8] ELSON J, GIROD L, ESTRIN D. Fine-grained network time synchronization using reference broadcasts[C]//Proc of the 5th Symposium on Operating Systems Design and Implementation. New York: ACM,2002:147-163.