无线传感器网络节点复制攻击和女巫攻击防御机制研究

胡蓉华,董晓梅,王大玲
(东北大学信息科学与工程学院,辽宁沈阳 110819)

摘 要: 在无线传感器网络(WSNs)中,节点复制攻击和女巫攻击可扰乱数据融合和阈值选举等网络操作.发起这两种攻击需先通过邻居发现认证过程.考虑到在WSNs中发起邻居认证是不频繁的,提出了一种基于单向密钥链的ID认证防御机制(OKCIDA),降低攻击者在任何时间段发起这两种攻击的可能性.然后基于椭圆曲线离散对数问题,构造对称参数,并组合OKCIDA和利用节点邻居关系,提出了一种无需位置的邻居认证协议(LFNA),以阻止复制节点和女巫节点成功加入网络.最后给出了安全性证明和分析,并在安全和开销方面将LFNA与已有典型防御方案进行了比较,结果表明该方案具有一定的优势.

关键词: 无线传感器网络; 节点复制攻击; 女巫攻击; 认证; 单向密钥链
中图分类号: TP393 **文献标识码:** A **文章编号:** 0372-2112 (2015)04-0743-10
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2015.04.017

Defense Mechanism Against Node Replication Attacks and Sybil Attacks in Wireless Sensor Networks

HU Rong-hua, DONG Xiao-mei, WANG Da-ling
(*School of Information Science & Engineering, Northeastern University, Shenyang, Liaoning* 110819, *China*)

Abstract: In wireless sensor networks (WSNs), node replication attacks and Sybil attacks can disrupt the network's operations such as data aggregation and threshold voting schemes. To launch these attacks, it is necessary to go through the neighbor discovery verification process firstly, which is not frequent in WSNs. Considering the above observations, a one-way key chain ID authentication (OKCIDA) defense mechanism was presented to decrease the probability for attackers to mount such attacks at any time. Moreover, the symmetric parameters was constructed based on the elliptic curve discrete logarithm problem; then combines with OKCIDA and utilizes node neighbor relationship, a location-free neighborhood authentication protocol (LFNA) was introduced to stop replica nodes and Sybil nodes from successfully joining into the network. Finally, the security of LFNA was proved and analyzed. Compared with several existing important mechanisms, the proposed method is superior in security and cost.

Key words: wireless sensor network; node replication attack; Sybil attack; authentication; one-way key chain

1 引言

节点复制攻击和女巫攻击是无线传感器网络(Wireless Sensor Networks, WSNs)面临的两种威胁性极大的攻击.对于前者,攻击者捕获一个或少量节点后,大量复制某个或某几个被捕获节点,然后将副本节点部署在原网络里.由于副本节点具有原始节点的秘密信息,一旦它们成功加入网络,便可以发起各种隐蔽的攻击,对网络的安全构成严重威胁[1].对于女巫攻击,每个恶意节点在网络中呈现多个节点身份,既可盗用其他节点身份,也可伪造网络不存在的身份.女巫攻击可对选举、资源公平分配等机制构成严重威胁[2].

目前已有许多应对节点复制攻击的检测机制[1,3~7]和应对女巫攻击的检测机制[2,8~10].由于检测机制属于一种事后处理策略,具有滞后性,同时开销也较大,因此有必要研究相应的防御策略.目前已有的针对节点复制攻击的防御机制大致可分为基于节点位置信息[11~13]和基于对称多项式[14]两类;而针对女巫攻击的防御机

收稿日期:2013-05-12;修回日期:2014-09-16;责任编辑:孙瑶
基金项目:国家自然科学基金(No. 60873199)

制可分为基于节点位置信息[11~13]、基于密钥预分配[2]和身份证书[15,16]三类. 其中仅有文献[11~13]同时实现了对这两种攻击的防御,但是这些机制依赖于节点位置信息,而在实际应用中很难正确获得每个节点的位置信息[17];同时这些机制也不易扩展和部署. 因此有必要针对这两种攻击设计一种不依赖节点位置信息的、易于扩展和部署的防御机制.

本文通过分析发现,发起节点复制攻击和女巫攻击必须先经过邻居发现认证过程. 同时考虑 WSNs 发起邻居发现的可能时间段,首先提出了一种基于单向密钥链的 ID 认证(One-way Key Chain ID Authentication,OKCI-DA)防御机制,在时间上限制攻击者发起这两种攻击. OKCIDA 的主要思想是将节点 ID 编码与单向密钥链关联,使得副本节点和女巫节点发送或回复的邻居认证请求只有在新节点加入认证过程中才会得到合法节点的回复或确认. 因此出于攻击效果考虑,狡猾的攻击者会选择在新节点加入阶段发起这两类攻击. 而向网络中添加新节点通常是不频繁的,从而 OKCIDA 在时间上大大地限制了攻击者发起这两类攻击的可能性. 其次,为了阻止副本节点和女巫节点在新节点加入阶段成功加入网络,基于椭圆曲线离散对数问题(Elliptic Curve Discrete Logarithm Problem,ECDLP),参考 Duan 等人提出的基于位置的邻居认证(Location-Based Neighborhood Authentication,LBNA)模式中对称参数构造的思想[13],通过构造对称参数并组合 OKCIDA 和利用节点邻居关系,提出了一种轻量级的、易于扩展的且无需位置信息的邻居认证(Location-Free Neighborhood Authentication,LFNA)模式. LFNA 不仅可以阻止副本节点和女巫节点与网络中的旧节点建立有效邻居关系,而且解决了文献[14]中副本节点与新加入的节点建立有效邻居关系的问题. 由于 LFNA 不依赖节点位置信息,既不需要定位设备和安全的定位算法支持,也不需要将节点部署在指定坐标区域,因此相比依赖位置信息的方案[11~13,15,16]更容易部署和扩展. 最后,给出了 LFNA 的安全性证明和分析,并在安全和开销方面与已有的典型防御机制进行了比较和分析,结果表明该方案具有一定的优势.

2 相关工作

目前针对节点复制攻击和女巫攻击的解决方案可分为检测机制和防御机制两大类. 文献[3,4]对节点复制攻击的检测机制作了分类介绍.

文献[1]提出了一种基于分区的节点复制攻击检测方法,通过将部署区域分区,建立基于跳数的坐标,来检测节点复制攻击. 该方法需要将节点部署在指定的划分区域. 文献[5]提出了随机多播和线选择多播两种副本节点检测模式,通过在网络中选择见证节点来检测副本节点. 这两种模式需要每个节点的位置坐标信息已知,同时节点需要执行公钥算法产生签名. 文献[6,7]提出了基于组部署知识的检测模式来识别和撤消副本节点. 将位置声明信息发送到对应组认证,而不像文献[5]中随机选择见证节点,减少了通信和能耗开销. 文中假设所有节点知道每组近似部署的位置,预载自己组的关系和所有组的位置;同一组的节点同时部署在指定位置.

文献[11,12]提出了基于位置的密码机制来防御几种攻击,其中包括节点复制攻击和女巫攻击. 利用基于身份的密码机制(Identify-Based Cryptography,IBC)产生基于节点位置信息的密钥(Location-Based Key,LBK),然后利用双线性映射的双线性和对称性质实现邻居节点认证与对密钥建立. 文献[13]针对文献[12]的模式不能抵御密钥捕获伪装(Key Compromise Impersonation,KCI)攻击和不能实现向前保密的缺陷,提出了基于位置的捕获容忍的密钥管理模式,其不需要任何配对和映射到点的哈希操作,更加适用于 WSNs. 然而这两种模式都需要节点位置坐标信息. 而在大多数情况下,由于存在各种攻击,很难正确获得每个节点的位置信息[17]. 文献[14]提出了一种基于组部署模型和对称多项式建立对密钥的方法,以防御节点复制攻击. 然而该方法没有解决新节点与副本节点建立对密钥的问题.

文献[2]主要讨论了无线设备资源测试方法和随机密钥预分配方法来识别女巫攻击. 文献[8,9]提出了基于接收信号强度指示(Received Signal Strength Indicator,RSSI)的女巫检测方法. 使用来自多个接收者的 RSSI 比率来检测女巫攻击. 文献[10]提出了利用邻居节点关系检验节点身份来检测女巫攻击的方法. 然而该方法仅适用于女巫节点伪造的节点身份密度大于网络平均部署密度的情况. 文献[15]利用单向密钥链和 Merkle 哈希树使得每个节点可以认证网络中其它节点的身份,从而防御女巫攻击. 然而文中的基本模式仅适用于小规模网络,而扩展模式需要每组节点部署在指定坐标区域. 文献[16]提出了类似的防御方法.

3 系统模型

3.1 网络模型

假定网络中的节点随机部署在感兴趣的监测区域,部署后节点不可移动. 在实际的 WSNs 中,当部分旧节点损坏或能量耗尽后,为了维持网络的连通性,需要向网络中补充部署新的节点[3~6,11,12]. 即网络中有些节点可能比其他节点后部署,这样网络中就存在不同批次部署的节点. 假定网络按部署批次递增方式部署,即第 $i+1$ 批次节点部署时,第 i 批次节点已经部署($i \geq 1$). 为了便于描述,作如下记号和定义:

Ds_i 表示部署批次为第 i 批次的批次号;

Id_u 表示节点 u 的主 ID 号;

ID_u 表示节点 u 的标识,由部署批次 Ds 和 Id_u 组成;

$NG_i = \{u \mid ID_u.\ Ds = Ds_i\}$ 表示第 i 批次部署的节点集合,其中 $ID_u.\ Ds$ 表示节点 u 的批次号;

$N_{\text{Set}} = \{NG_i \mid i \leqslant Ds_{\max}\}$ 表示网络中所有已部署节点的集合,其中 $Ds_{\max}$ 表示已部署的最新的批次号.

定义 1　设节点 u 的通信半径为 R_u,如果节点 v 与节点 u 的物理距离 $|d_{uv}| \leqslant R_u$,则称 v 为 u 的邻居节点. 记 $N_u = \{v \mid v \in N_{\text{Set}}$,且 $|d_{uv}| \leqslant R_u\}$.

假设对任何合法节点 u,它至少有一个合法邻居节点,即 $N_u \neq \varnothing$. 对于大多数情况这个假设是合理的.

3.2　攻击模型

假设攻击者能够捕获网络中的少数合法节点,并可以获得被捕获节点的所有信息,包括采用的通信协议和加载的密钥等[1,18]. 如果攻击者能够捕获网络中大部分节点,则没有必要发起节点复制攻击和女巫攻击. 假定每批新节点部署后有一段安全时间与邻居节点建立安全通信密钥,在这段时间里新节点不会被攻击者捕获.

(1) 复制攻击模型

假定攻击者从被捕获节点集 C_{Set} 中选择一个或少量节点复制,将复制出来的副本节点 cp-node 部署在整个网络里,记 Rep_{Set} 为 cp-node 的集合. 同时假定在节点 u 通信范围内,正常邻居节点的个数 $|N_{u,\text{nor}}|$ 比副本邻居节点的个数 $|N_{u,\text{cp}}|$ 多,即 $|N_{u,\text{nor}}| > |N_{u,\text{cp}}|$. 副本节点被部署后,尝试与邻居节点建立安全通信链路,以便像合法节点一样参与到网络中,然后进行信息收集和各种隐蔽攻击.

(2) 女巫攻击模型

假设攻击者既可以部署自己的节点发起女巫攻击,也可以利用被捕获的节点和副本节点发起女巫攻击. 为了便于描述,作如下记号和定义:

定义 2　女巫实体节点是指物理存在的发起女巫攻击的真实节点,可以是攻击者部署的外部节点、被捕获的节点或副本节点,分别称为基于外部节点的女巫实体节点、基于被捕获节点的女巫实体节点和基于副本节点的女巫实体节点,分别记为 ex_sybil_tnode,ca_sybil_tnode 和 cp_sybil_tnode.

定义 3　女巫节点是指女巫实体节点声称的虚假身份. 虚假身份可以是其他合法节点身份、被捕获节点身份或网络中不存在的虚构身份,分别称为盗用身份女巫节点、傀儡身份女巫节点和虚构身份女巫节点,分别记为 im_sybil_fnode,ca_sybil_fnode 和 ex_sybil_fnode.

用 $u.\ Type$ 表示节点 u 的节点类型,根据上述的定义和假设,本文的系统模型可以表示成一个五元组 $(N_{\text{Set}}, C_{\text{Set}}, Rep_{\text{Set}}, \text{sybil\_tnode}_{\text{Set}}, \text{sybil\_fnode}_{\text{Set}})$,其中 $\text{sybil\_tnode}_{\text{Set}} = \{u \mid u.\ Type = \text{ex\_sybil\_tnode}\} \cup \{u \mid u.\ Type = \text{ca\_sybil\_tnode}\} \cup \{u \mid u.\ Type = \text{cp\_sybil\_tnode}\}$; $\text{sybil\_fnode}_{\text{Set}} = \{u \mid u.\ Type = \text{im\_sybil\_fnode}\} \cup \{u \mid u.\ Type = \text{ca\_sybil\_fnode}\} \cup \{u \mid u.\ Type = \text{ex\_sybil\_fnode}\}$.

本文的主要目的是通过设计相应的防御机制阻止异常节点 $\text{ab\_node} \in Rep_{\text{Set}} \cup \text{sybil\_fnode}_{\text{Set}}$ 成功加入网络. 系统攻击模型如图 1 所示.

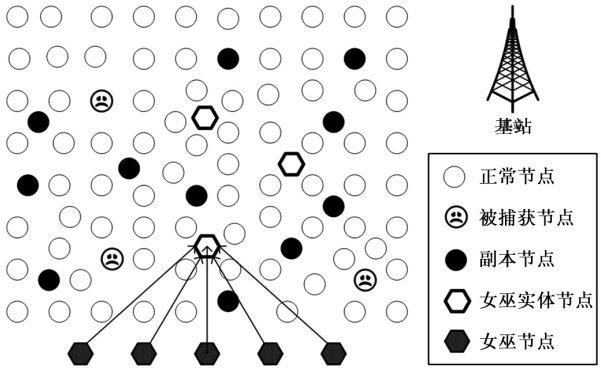


图1　节点复制攻击和女巫攻击模型

4　OKCIDA: 单向密钥链 ID 认证防御机制

在节点复制攻击和女巫攻击中,副本节点和女巫节点首先需要与网络中的节点建立安全链路关系,经过邻居发现和认证处理过程. 对于非移动 WSNs,只有在网络部署初始阶段或向网络添加新节点后一小段时间内网络才会发起邻居发现和认证处理过程. 因此为了在时间上约束攻击者发起这两种攻击,防止副本节点和女巫节点在任何时间发起加入网络的请求,本文提出了一种基于单向密钥链的 ID 认证防御机制 OKCIDA,确保在没有向网络添加合法新节点时,副本节点和女巫节点成功加入网络的可能性为零. 基本思想是在节点 ID 中引入 Ds 域,向每批次部署节点预载单向密钥链中对应的密钥,新节点需要向旧节点提供相应的认证密钥 K_{new},旧节点通过认证 $K_{\text{old}} = h(K_{\text{new}})$ 实现对新节点的过滤. 本文使用的部分记号和含义如表 1 所示.

OKCIDA 包括以下三个部分:

(1) 单向密钥链生成. 选择一个随机数 $k_n \in {}^{*}_{q}$ 和一个哈希函数 $h: \{0,1\}^{*} \rightarrow {}^{*}_{q}$ 并迭代执行 h,形成单向密钥链. 即 $k_i = h(k_{i+1})$,$(1 \leqslant i \leqslant n-1)$,如图 2 所示. 给定 k_{i+1} 很容易计算 k_i; 反之给定 k_i,计算 k_{i+1} 在计算上是不可行的.

(2) 基于节点部署批次 Ds_i 预载单向密钥链中对应

的密钥 k_i,使得 $K(Ds_i)=k_i$. 例如,如图 2 所示,对于第 1 批节点预载共享密钥 $K(Ds_1)=k_1$.

表 1 本文使用的部分记号

记号	含义
p,q	两个大素数
E/F_p	在有限域 F_p 上的一个椭圆曲线
G	在曲线 E/F_p 上点的加群的一个 q 阶子群
W	群 G 的生成器(元)
k	系统随机选择的主私钥
W_{pub}	系统的主公钥
h	一个单向哈希函数,输出值属于 Z_q^*
$\|$	连接符号
Ds_i	第 i 批部署节点批次号
Id_u	节点 u 的主 ID 号
$ID_u=(Ds_i \| Id_u)$	第 i 批节点 u 的 ID 号
$ID_u.Ds$	节点 u 的批次号
$K(Ds_i)$	第 i 批部署节点预载的共享密钥
IK_u	节点 u 预载的私钥
$Ds_{\max}$	节点记录的已部署的最新批次号
$\alpha_u,\beta_u \in Z_q^*$	节点 u 生成的随机数
X_u,Y_u	节点 u 预载的对应于 α_u,β_u 公开信息

(3) 认证 $K(Ds_{i+1})$. 如果第 $i+1$ 批新节点被部署,对于任意的新节点 u 向邻居节点 v 提供 $K(Ds_{i+1})$ 信息. 如果 v 为网络中的旧节点,则检查 $K_{\text{last}}=h(K(Ds_{i+1}))$ 是否成立,其中 K_{last} 表示节点记录的最近通过认证的单向密钥链中的密钥,即 k_i. 如果等式成立,则表明有新节点部署到网络中,通过 OKCIDA 检查; 否则丢弃.

当网络中没有新节点被部署时,由于副本节点和女巫节点没有下一批次新节点的共享密钥,不能通过 OKCIDA 检查,从而阻止了这两类节点加入网络. 因此 OKCIDA 可以在时间上约束攻击者发起节点复制攻击和女巫攻击.

5 LFNA: 无需位置的邻居认证协议

由于 OKCIDA 仅在时间上约束攻击者发起节点复制攻击和女巫攻击,当网络中添加新节点时,副本节点和女巫实体节点监听到新节点发送的认证密钥后可以尝试加入网络. 因此针对 OKCIDA 的不足,组合 OKCIDA 和节点邻居关系,并参考 Duan 等人提出的 LBNA 模式中对称参数构造思想[13],基于椭圆曲线离散对数问题(ECDLP),通过构造出一种无需位置信息的对称参数模式,提出了一种无需位置信息的邻居认证协议(LFNA),以防御这两种攻击. LFNA 包括预部署阶段、部署后邻居认证阶段和后邻居认证更新过滤阶段.

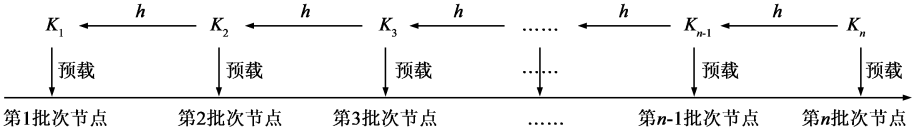


图2 单向密钥链ID认证模型

5.1 预部署阶段

在网络被部署前,网络所有者执行以下操作产生系统参数,参数含义如表 1 所示:

(1) 采用与文献[11~13,19]中相同的方法产生网络系统参数$(p,q,E/F_p,G,W)$.

(2) 选择一个随机数 $k \in Z_q^*$ 作为网络主私钥. 同时设置对应的网络主公钥 $W_{\text{pub}}=kW$. 根据在群 G 里求解离散对数问题(Discrete Logarithm Problem,DLP)困难性性质,对于给定的(W,W_{pub})对,计算 k,在计算上是不可行的[11~13].

(3) 依照 OKCIDA 的单向密钥链生成部分产生一个单向密钥链.

对于第 i 批次任意的预部署节点 u,网络所有者执行以下操作预载相关信息:

(1) 依照 OKCIDA,基于节点部署批次预载单向密钥链中对应的密钥 k_i,使得 u 预载的共享批次密钥 $K(Ds_i)=k_i$.

(2) 选择两个随机数 $\alpha_u,\beta_u \in Z_q^*$,预载 X_u 和 Y_u,其中 $X_u=\alpha_u W$,$Y_u=h(W_{\text{pub}} \| ID_u)\beta_u W$.

(3) 预载 u 的私钥 $IK_u=\alpha_u+h(W_{\text{pub}} \| ID_u)(\beta_u+k)$.

(4) 预载已部署节点最大批次号 $Ds_{\max}=(i-1)$. 如果 $i=1$,表明该批节点为第一批节点,因此 $Ds_{\max}=0$.

u 预载的可公开参数为$(p,q,E/F_p,G,W,W_{\text{pub}},h,K(Ds_i),X_u,Y_u,Ds_{\max})$,秘密参数为 IK_u.

5.2 部署后邻居认证阶段

新节点部署后,首先需要与邻居节点建立安全通信链路. 图 3 描述了正常节点邻居认证的交互过程. 为了便于描述,假设部署第 $i+1$ 批新节点. 对于任意的新节点 u,邻居认证过程如下:

(1) u 向本地广播邻居发现消息 $M_{\text{hello}}=\{ID_u,X_u,Y_u,T_u,K(Ds_{i+1})\}$. 其中 $T_u=t_u W$,t_u 为随机选择的且 $t_u \in Z_q^*$.

(2) 对于 u 的任意邻居节点 v,接收到消息 M_{hello} 后进行以下处理:

(a) 检查部署批次号. 如果 $ID_u.Ds=Ds_{\max}+1$,则表明可能是新部署节点,进入下一步检查; 否则丢弃;

(b) 认证 $K(Ds_{i+1})$. 如果 v 为新节点则比较接收到的 $K(Ds_{i+1})$ 是否与自己预载的共享批次密钥相同; 如

果 v 为旧节点则检查 $K_{\text{last}} = h(K(Ds_{i+1}))$ 是否成立. 如果通过认证,则进入下一步检查; 否则丢弃;

(c) 向 u 回复消息 M_{echo}. 选择一个随机数 $t_v \in {}^{*}_{q}$, 计算 $T_v = t_v W$; 计算与 u 的对密钥 $K(v,u) = h(ID_u, ID_v, Z_1, Z_2, Z_3)$, 其中 $Z_1 = IK_v T_u$, $Z_2 = t_v(X_u + Y_u + h(W_{\text{pub}} \| ID_u) W_{\text{pub}})$, $Z_3 = t_v T_u$; 如果 v 为新节点,则 $M_{\text{echo}} = \{ID_v, X_v, Y_v, T_v, h(K(v,u), T_u, T_v, 1)\}$; 如果 v 为旧节点,则 $M_{\text{echo}} = \{ID_v, X_v, Y_v, T_v, N_v, h(K(v,u), T_u, T_v, N_v, 1)\}$, 其中 N_v 表示在新节点部署前 v 拥有的邻居节点集合. 根据网络模型假设 $N_v \neq \varnothing$. 如果 $N_v = \varnothing$, 接收节点认为回复节点是恶意或无效节点,将直接丢弃.

(3) 当 u 收到 v 的回复消息 M_{echo}, 进行以下处理:

(a) 消息认证. 计算与 v 的对密钥 $K(u,v) = h(ID_u, ID_v, Z_1, Z_2, Z_3)$, 其中 $Z_1 = t_u(X_v + Y_v + h(W_{\text{pub}} \| ID_v) W_{\text{pub}})$, $Z_2 = IK_u T_v$, $Z_3 = t_u T_v$; 然后计算对应的哈希值,比较判断: 如果 v 为新节点,则计算 $h(K(u,v), T_u, T_v, 1)$ 与收到的 M_{echo} 中对应域比较,如果相同,则进入下一步处理,否则丢弃; 如果 v 为旧节点且 $N_v \neq \varnothing$, 则计算 $h(K(v,u), T_u, T_v, N_v, 1)$ 与收到的 M_{echo} 中对应域比较,如果相同,则进入下一步处理,否则丢弃.

(b) 向 v 发送回复确认消息 $M_{\text{ack}} = \{h(K(u,v), T_u, T_v, 2)\}$.

(4) 当 v 收到 u 的回复确认消息 M_{ack}, 进行消息认证处理. 计算 $h(K(v,u), T_u, T_v, 2)$, 与接收的 M_{ack} 中对应内容比较,如果相同,则与 u 的邻居认证成功结束,同时与 u 的对密钥建立完成. 而且可以根据需要依据建立的对密钥 $K(v,u)$ 生成其他安全通信密钥.

以上邻居认证过程是正确的,当 u 和 v 拥有的私钥 IK 为系统预载的合法密钥时,可以保证 $K(u,v) = K(v,u)$. 因为:

(1) $u.Z_1 = t_u(X_v + Y_v + h(W_{\text{pub}} \| ID_v) W_{\text{pub}})$
$= t_u(\alpha_v W + h(W_{\text{pub}} \| ID_v)\beta_v W + h(W_{\text{pub}} \| ID_v) W_{\text{pub}})$
$= t_u(\alpha_v W + h(W_{\text{pub}} \| ID_v)(\beta_v W + W_{\text{pub}}))$
$= t_u(\alpha_v W + h(W_{\text{pub}} \| ID_v)(\beta_v W + kW))$
$= t_u(\alpha_v W + h(W_{\text{pub}} \| ID_v)(\beta_v + k) W)$
$= (\alpha_v + h(W_{\text{pub}} \| ID_v)(\beta_v + k)) t_u W$
$= IK_v T_u = v.Z_1$.

(2) 同样, $u.Z_2 = v.Z_2$.

(3) $u.Z_3 = t_u T_v = t_u t_v W = t_v t_u W = t_v T_u = v.Z_3$.

其中 $u.Z_1$ 表示 u 生成的 Z_1, 其他表示类似. 由以上可知,邻居认证过程是正确的.

5.3　后邻居认证更新过滤阶段

当邻居认证阶段结束后,所有节点需要对相应参数更新. 对于任意节点等待一个预定义的时间段阈值后,如果不再接收或处理任何有意义的邻居认证请求,则认为邻居认证阶段结束.

网络中所有节点都作如下更新操作:

(1) $Ds_{\max} = Ds_{\max} + 1$;

(2) $K_{\text{last}} = K(Ds_{i+1})$;

对于旧节点,将新建立的邻居节点加入邻居列表中. 对于新节点,则建立邻居列表: 将已建立安全通信链路的同批次节点加入邻居列表中; 对已建立安全通信链路的旧节点进行过滤处理. 图 4 描述了对旧节点过滤处理过程.

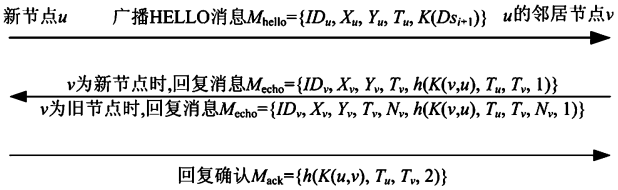


图3　正常节点邻居认证交互过程

假设对于新节点 u, 经过邻居认证阶段后,与它建立安全通信链路的旧节点集合为 $N_{u,\text{old}}$. 例如图 4 中第一阶段, u 的旧节点集合 $N_{u,\text{old}} = \{A, B, C, D, E, F, \text{replica1}, \text{replica2}\}$. 对于任意节点 $v \in N_{u,\text{old}}$, 假设 v 发送给 u 的邻居信息集合为 N_v, 注意 $N_v \neq \varnothing$. 如图 4 中第一阶段,旧节点 A 的邻居信息集合 $N_A = \{B, C, F, L\}$. u 按照以下步骤对 $N_{u,\text{old}}$ 进行过滤处理:

(1) 消减 N_v. 取得 v 消减后的邻居信息集合 $N_{v,\text{flt}} = (N_v \cap N_{u,\text{old}})$. 如图 4 中第一阶段, A 消减后的邻居信息集合 $N_{A,\text{flt}} = \{B, C, F\}$.

(2) 建立 $N_{u,\text{old}}$ 中节点的关系图 map_u. 初始化时将 $N_{u,\text{old}}$ 中每个节点作为一个顶点,无任何边. 之后作以下过滤处理:

对于任意节点 $v \in N_{u,\text{old}}$, 当 $N_{v,\text{flt}} \neq \varnothing$ 时,对任意节点 $w \in N_{v,\text{flt}}$ 计算 $N_{vw,\text{flt}} = (v \cup N_{v,\text{flt}} \cap (w \cup N_{w,\text{flt}}))$. 如图 4 中第二阶段,对于 A, $N_{A,\text{flt}} = \{B, C, F\}$, $B \in N_{A,\text{flt}}$, 则 $N_{AB,\text{flt}} = \{A, B, C\}$. 如果 $N_{vw,\text{flt}} \neq \varnothing$ 且 $v, w \in N_{vw,\text{flt}}$, 则进行以下处理:

(a) 在 v, w 间加入一条边,如图 4 中第二阶段所示,由于 $A, B \in N_{AB,\text{flt}}$, 因此 A, B 间存在一条边;

(b) 对 $N_{vw,\text{flt}}$ 中除 v, w 外的任意节点 o, 在关系图 map_u 中节点 v, o 间和节点 w, o 间分别加入一条边. 如图 4 中第二阶段所示,由于 $C \in N_{AB,\text{flt}}$, 因此 A, C 间和 B, C 间各有一条边;

(c) 对集合 $N_{vw,\text{flt}}$ 中节点的邻居节点集合消减. 对任意节点 $o^{*} \in N_{vw,\text{flt}}$, $N_{o^{*},\text{flt}} = (N_{o^{*},\text{flt}} - (N_{vw,\text{flt}} \cap N_{o^{*},\text{flt}}))$. 如图 4 中第二阶段所示,对于节点 A、B、C 可分别得到消减后的邻居节点集合 $N_{A,\text{flt}} = \{F\}$、$N_{B,\text{flt}} = \{\text{null}\}$、$N_{C,\text{flt}} = \{D\}$.

(4) 检查 $N_{u,\mathrm{old}}$ 中节点的邻居信息集合 N_{flt} 是否为空,如果存在节点 v^* 的邻居信息集合 $N_{v^*,\mathrm{flt}} \neq \varnothing$,则跳转到(2)的过滤处理处继续处理;否则结束关系图 map_u 的建立,进入步骤(3). 如图4所示,经过上一步处理,由于 $N_{A,\mathrm{flt}}=\{F\}$,将继续对 A 的邻居信息集合进行过滤处理,即图4中的第三阶段处理.

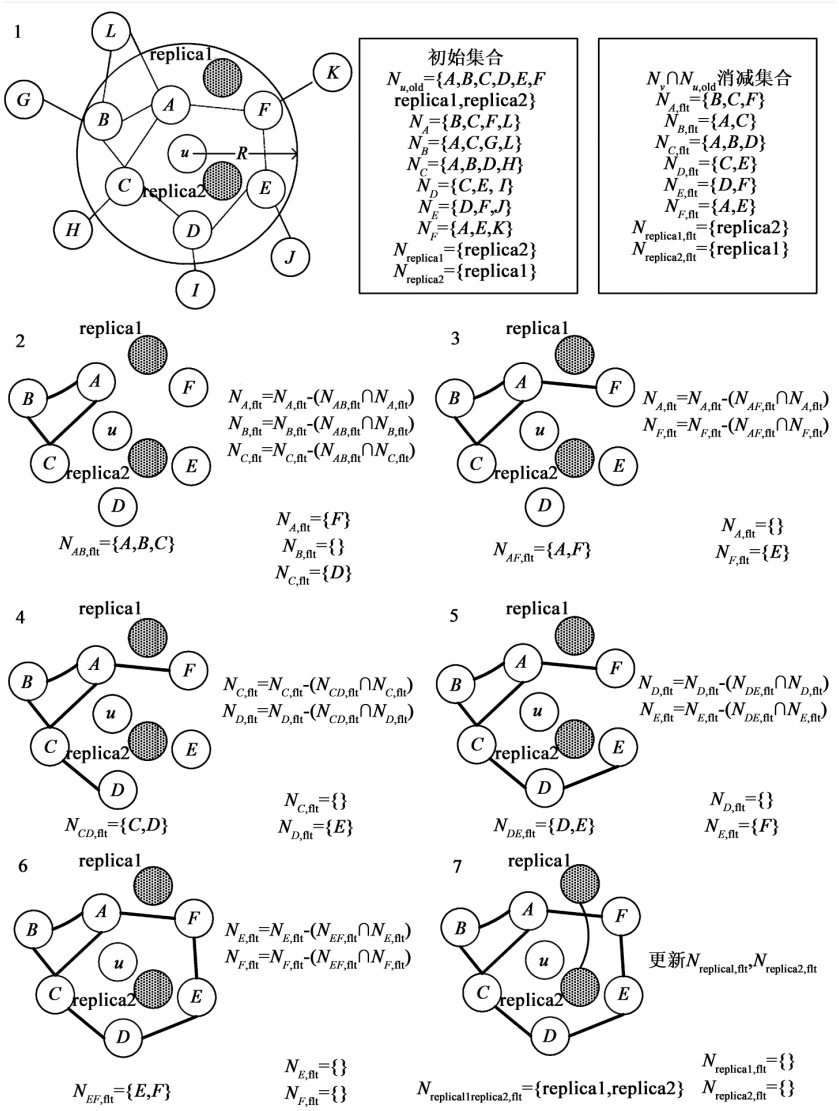


图4 新节点建立邻居列表时对旧节点过滤处理过程

(3) 依据第二步处理建立的节点关系图 map_u,按照一定的选择策略过滤可疑节点. 例如可以选择 map_u 中连通性最强同时节点密度在网络节点密度正常范围内的节点集合作为可信节点,其余节点作为不可信节点,其中连通性最强节点集合表示节点间有边相连且节点个数最多的集合. 如图4中第八阶段所示,得到连通性最强的节点集合{A,B,C,D,E,F}. 注意,当考虑单个节点通信范围内正常节点的个数 N_ρ 时,需要将 N_ρ 作为网络系统参数在节点部署前加载到节点中.

6 安全性证明和分析

6.1 节点私钥 IK 不可伪造性

定理1 对于节点 u 预载的密钥 IK_u,当攻击者捕获密钥 IK_u 甚至捕获 u 后,无法依据捕获的信息获得系统主密钥 k 和伪造任何 ID 对应的合法预载密钥.

证明 假设 u 的预载密钥为 $IK_u=\alpha_u+h(W_{\mathrm{pub}} \| ID_u)(\beta_u+k)$,$X_u=\alpha_u W$,$Y_u=h(W_{\mathrm{pub}} \| ID_u)\beta_u W$. 根据在群 G 里求解 DLP 困难性可知,当攻击者知道 X_u 和 Y_u 后无法获取 α_u 和 β_u,因此攻击者即使获取了 IK_u,也无法得到 k.

可以推广证明,即使攻击者捕获了 n 个节点,也无法获得 k 和伪造任何 ID 对应的合法预载密钥.

考虑一种特殊情况: 所有节点选择的 β 都相同,即 $k^* = (\beta_u + k)$ 都相同. 显然,如果攻击者连 k^* 都无法确定,那么更无法确定 k 值. 当攻击者捕获 n 个节点后,需要依赖 n 个线性方程求解 $n+1$ 个未知数. 依据非齐次线性方程组求解性质,由于系数矩阵和增广矩阵的秩相等且小于 $n+1$,方程组有无穷解. 因此攻击者无法获取 k^*,更无法获取 k 值.

通过以上两种情况分析可知,攻击者无法通过节点捕获而获取系统主密钥 k 和伪造任何 ID 对应的合法预载密钥.

6.2　防御节点复制攻击

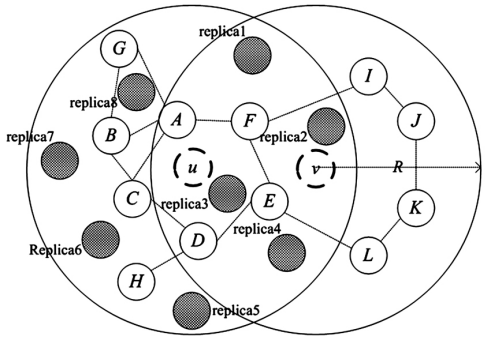
由于 LFNA 融入了 OKCIDA 机制,可在时间上约束攻击者发起节点复制攻击,因此当攻击者捕获节点并产生副本节点后,只有等待添加新节点时发起攻击才可能不被察觉. 因此本小节仅讨论网络中添加新节点时攻击者发起节点复制攻击的情况. 依据在邻居认证阶段网络中请求节点和接收节点的角色,可分以下 2 种情况:

(1) 当请求节点为副本节点,接收节点为合法新节点或正常已工作节点时: 由于副本节点以旧 ID 发起邻居请求认证,接收节点通过 ID 检查即可将这类请求消息过滤.

(2) 当请求节点为合法新节点,接收节点为副本节点时: 副本节点欲与新节点建立合法通信链路. 由于副本节点拥有所有邻居认证阶段的有效秘密信息,因此在邻居认证阶段可以与新节点成功建立对密钥. 但是在后邻居过滤阶段,新节点通过构建旧节点关系图 map 可以过滤掉与副本节点建立的邻居关系. 对于大多数复制攻击,攻击者仅对一个或少数几个被捕获节点复制,然后将副本节点向网络部署. 本文将具有所有被复制节点 ID 的最小副本节点集合称为一个最大部署组. 因此即使攻击者以最大部署组方式部署,在新节点生成的 map 里副本节点组成的连通节点集合的元素个数也小于正常旧节点连通节点集合的元素个数.

考虑两种极端情况: (1) 假设攻击者仅对一个被捕获节点复制,则在新节点生成的 map 里副本节点是一个孤立的点,因此可以很容易过滤掉; (2) 假设攻击者捕获一个节点通信范围内的所有节点后,将所有这些节点复制且以最大部署组方式部署,则在某些新部署节点生成的 map 里会有两个大小相当的强连通节点集合.

如图 5 所示,副本节点 replica1 到 replica8 为攻击者捕获某一通信范围内的所有节点后复制的一个最大部署组节点集合,每个副本节点对应一个唯一的被捕获节点. 在这种情况下受影响的新节点 u 可以向邻居新节点广播请求协作消息 M_{help},消息内容 C_{help} 为从两个大小相当的强连通节点集合中分别选取的部分节点 ID. 假设新节点 v 拥有一个最大连通节点集合 set_v,当它接收到 M_{help} 后,计算 $C_{\text{valid}} = (C_{\text{help}} \cap \text{set}_v)$,如果 $C_{\text{valid}} \neq \varnothing$,则使用建立的对密钥向 u 回复消息 M_{result},消息内容为 C_{valid}. u 收到 M_{result} 后,过滤掉不包含 C_{valid} 的那组节点. 事实上,攻击者以第二种极端方式发起攻击的可能性很小,因为这种攻击方式不仅代价较大,而且也极易暴露.



假设新节点u的两个强连通集合为$\text{set}_{u1}=\{A, B, C, D, E, F, G, H\}$;
$\text{set}_{u2}=\{\text{replica1}, \text{replica2}, \text{replica3}, \text{replica4}, \text{replica5}, \text{replica6}, \text{replica7}, \text{replica8}\}$.
假设$C_{\text{help}}=\{\text{ID}_A, \text{ID}_B, \text{ID}_C, \text{ID}_D, \text{ID}_{\text{replica1}}, \text{ID}_{\text{replica2}}, \text{ID}_{\text{replica3}}, \text{ID}_{\text{replica4}}\}$
假设新节点v的只有一个强连通集合为$\text{set}_v=\{A, D, E, F, I, J, K, L\}$
$C_{\text{valid}}=\{A, D\}$

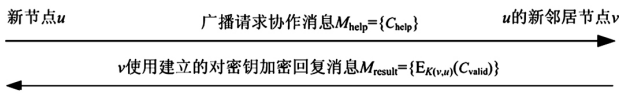


图5　副本节点以最大组部署时处理模型

6.3　防御女巫攻击

与防御节点复制攻击类似,由于 LFNA 可在时间上约束攻击者发起女巫攻击,因此本小节仅讨论网络中部署新节点时攻击者发起女巫攻击的情况. 由定理 1 可知,攻击者不能伪造任何 ID 对应的合法预载密钥,因此对于女巫节点为 ex_sybil_fnode 和 im_sybil_fnode 时,LFNA 均可成功阻止女巫节点加入网络,如表 2 所示.

针对表 2 中第一种情况,由于女巫节点以旧 ID 发起请求认证,与防御节点复制攻击的第一种情况相同,接收节点通过 ID 检查可将这类请求消息过滤.

针对表 2 中的第二种情况,由定理 1 可知,攻击者不能伪造任何 ID 对应的合法预载密钥. 由于攻击者没有其声称的 ID 所对应的私钥,不能生成与回复节点相同的对密钥,因此合法节点收到攻击者回复的消息 M_{ack} 后,通过消息认证即可过滤此类攻击.

针对表 2 中的第三种情况,即女巫节点为 ca_sybil_fnode 时,由于 ca_sybil_fnode 拥有对应被捕获节点

的所有秘密信息,因此在邻居认证阶段可以与新节点成功建立对密钥. 此种情况与防御节点复制攻击的第二种情况类似. 不同之处在于,节点复制攻击由一个或多个物理存在的副本节点发起,而女巫攻击则是由多个 ca_sybil_fnode 发起. 同时多个 ca_sybil_fnode 在后邻居认证更新过滤阶段可以合谋声称彼此为邻居节点. 因此存在以下情况:

(1) 当在单个节点通信范围内的 ca_sybil_fnode 个数明显少于或大于正常节点个数时,通过考虑单个节点通信范围内正常节点的个数,可将节点个数明显小于或大于正常水平的连通节点集合过滤掉.

(2) 当在单个节点通信范围内的 ca_sybil_fnode 个数与正常节点个数接近时,这种情况与讨论防御节点复制攻击的第二种极端情况类似,可以通过发送请求协作消息 M_{help} 来防御 ca_sybil_fnode.

表 2 女巫节点以不同 ID 攻击时 LFNA 防御效果

请求节点	接收节点	(防御效果; 通信开销; 过滤方法)
女巫节点以被复制节点 ID(ca_sybil_fnode)、其他旧节点 ID(im_sybil_fnode)或者虚构的旧节点 ID(ex_sybil_fnode)	合法新节点或正常已工作节点	(完全过滤; 接收一个广播邻居发现消息 M_{hello}; 检测 ID 过滤)
女巫节点以虚构的新 ID(ex_sybil_fnode)或其他合法新节点 ID(im_sybil_fnode)(不结合虫洞)	合法新节点或正常已工作节点	(完全过滤; 新批次节点部署前: 接收一个广播邻居发现消息 M_{hello}, 单向密钥链过滤; 新批次节点部署后,回复一条 M_{echo} 消息,接收确认消息 M_{ack}; 消息验证码过滤)
合法新节点	女巫节点以多个被捕获节点 ID(ca_sybil_fnode)	(完全过滤; 发送一个广播邻居发现消息 M_{hello},接收一条 M_{echo} 消息,回复一条确认消息 M_{ack}; 构建关系图过滤)
合法新节点	女巫节点以被捕获节点邻居旧节点 ID、其他新旧节点 ID(im_sybil_fnode)(不结合虫洞)、虚构的旧节点 ID、虚构的新 ID(ex_sybil_fnode)	(完全过滤; 发送一个广播邻居发现消息 M_{hello},接收一条 M_{echo} 消息; 消息验证码过滤)
合法新节点	合法新节点或正常已工作节点	N/A

针对表 2 中的第四种情况,同第二种情况类似,由于攻击者没有其声称的 ID 所对应的私钥,因此新节点接收到 M_{echo} 后,通过生成对密钥进行消息认证可防御这类攻击.

6.4 抵御 KCI 攻击

假设攻击者捕获节点 u 的私钥 IK_u 后想发起 KCI 攻击,根据本文的 LFNA 机制,攻击者必须等到新节点部署阶段发起攻击,否则会在检测的第一或第二步骤就被过滤掉.

假设预载共享密钥为 $K(Ds_{i+1})$ 的新批次节点部署后,攻击者在 u 附近伪装成节点 A 发起邻居发现消息 $M_{\text{hello}}=\{ID_A, X_A, Y_A, T_A, K(Ds_{i+1})\}$,其中随机数 $t_A, \alpha_A, \beta_A \in {}^{*}_{q}$, $X_A=\alpha_A W$, $Y_A=h(W_{\text{pub}} \| ID_A)\beta_A W$, $T_A=t_A W$, $K(Ds_{i+1})$ 为攻击者监听到的共享批次密钥.

u 收到 M_{hello} 处理认证后发送回复消息 $M_{\text{echo}}=\{ID_u, X_u, Y_u, T_u, N_u, h(K(u,A), T_A, T_u, N_u, 1)\}$,其中 $K(u,A)=h(ID_A, ID_u, Z_1, Z_2, Z_3)$, $Z_1=IK_u T_A$, $Z_2=t_u(X_A+Y_A+h(W_{\text{pub}} \| ID_A)W_{\text{pub}})$, $Z_3=t_u T_A$.

攻击者接收到来自 u 的 M_{echo} 后,试图获取 $K(u,A)$. 但是攻击者不知道 t_u,因此无法以 u 的身份计算出 $K(u,A)$. 由定理 1 知,由于攻击者不能伪造真实的 IK_A,因此也不能以 A 的身份计算出 $K(A,u)$. 即攻击者发起 KCI 失效.

6.5 提供完美的向前安全

假设攻击者获得节点 u 的私钥 IK_u 后想获取 u 与邻居节点 $v \in N_u$ 之间的对密钥 $K(u,v)$,并且之前已经记录了 u 和 v 之间所有的通信信息. 由于攻击者不知道 t_u,因此无法计算出正确的 $K(u,v)$. 即使攻击者同时捕获了 v 的私钥 IK_v,仅能计算出对应的 Z_1 和 Z_2,根据 EC-DLP,攻击者不能计算出 t_u 或 t_v,无法计算出正确的 Z_3,因此也无法获得正确的 $K(u,v)$.

为了防止节点被捕获后,节点与邻居节点间对密钥被攻击者获取而威胁之前通信消息的机密性,通过认证的邻居节点可以根据定义的密钥更新周期,定期更新建立的对密钥.

假设 u 和 v 需要进行对密钥的更新,u 和 v 仅需通过捎带方式将新生成的 T_u 和 T_v 发送给对方,按照计算对密钥的方法即可生成新的对密钥,实现完美的向前安全.

7 比较与分析

本文方案与已有的应对节点复制攻击和女巫攻击的防御方案比较如表 3 所示,其中存储代价仅考虑了

每个普通节点预载的存储开销; 计算代价仅考虑了一对节点三次握手认证的开销; 通信代价考虑了三次握手认证的通信开销 C_{auth} 和节点获取位置信息的通信开销 C_{ac-pst}.

表 3　已有防御节点复制攻击和女巫攻击方案与本文工作比较

方案	依赖位置信息	扩展性	抵御 KCI 攻击	提供向前保密	存储代价	计算代价	通信代价
Zhang 等[11,12]	√	难	×	×	$M_{common}+(G_{new},e,H,l_u,LK_u)$	1 个 pairing + 1 个 map-to-point hash 操作	$C_{auth}+C_{ac-pst}$
Duan 等[13]	√	难	√	√	$M_{common}+(R_u,l_u,LK_u)$	5 个标量点乘操作	$C_{auth}+C_{ac-pst}$
本文方案	×	易	√	√	$M_{common}+(K(Ds_i),X_u,Y_u,Ds_{max})$	5 个标量点乘操作	C_{auth}

由表 3 可知,本文方案 LFNA 在整体上要优于已有防御机制. (1) 在没有位置信息的情况下,LFNA 不仅可以实现邻居节点间认证和密钥建立,同时可防御节点复制攻击和女巫攻击. (2) LFNA 与 Zhang 等和 Duan 等提出的方案相比更易扩展,在每次新节点加入时,新节点无须依靠移动机器或锚节点帮助而获得位置坐标信息. (3) 同 LBNA 模式[13] 一样,LFNA 也可以抵御 KCI 攻击和提供向前保密. (4) 在存储代价上,LFNA 开销较小. 在表 3 中存储代价表示任意节点 u 预载的存储代价. $M_{common}=(p,q,E/F_p,G,W,W_{pub},h,IK_u)$,表示相关模式预载的共同信息; G_{new} 表示一个在有限域 $F_{p^2}^*$ 乘群的 q 阶子群; e 是一个双线性配对映射,$e: G\times G\rightarrow G_{new}$; H 为一映射到点的哈希函数,$H:\{0,1\}^*\rightarrow G$; l_u 表示节点位置信息,可能需要几个参数表示; LK_u 表示节点基于位置信息的密钥; R_u 表示 u 预载的随机数,$R_u\in Z_q^*$; 其他符号含义同前文. (5) 在计算开销上,LFNA 仅需要执行 5 个标量点乘操作,不需要执行任何配对操作和映射到点的哈希操作. 根据文献[13,20]可知,在相同有限域里执行一个配对操作比执行一个点标量乘操作至少需要多 10 倍的乘操作; 同时一个映射到点的哈希操作比一个点标量乘操作在计算时间上更长,因此 LFNA 在计算上是有效的. (6) 在通信代价上,表 3 中所有方案都需要三次握手认证通信,因此 C_{auth} 通信代价相当; 而 LFNA 由于节点不需要获取位置信息,因此没有因获取位置信息而带来的开销 C_{ac-pst}.

8　总结

本文提出了一种适用于无线传感器网络的节点复制攻击和女巫攻击的防御机制 LFNA. 首先,通过分析发现发起这两种攻击必须先经过邻居发现认证过程,同时考虑网络中发起邻居发现的可能时间段,提出了一种基于单向密钥链的 ID 认证(OKCIDA)防御机制,实现了在时间上约束攻击者发起这两种攻击; 其次,基于椭圆曲线离散对数问题(ECDLP),参考 Duan 等人提出的 LBNA 模式中对称参数构造的思想[13],通过构造一种无需位置信息的对称参数模式,并组合 OKCIDA 和利用邻居节点间的关系,提出了无需位置信息的邻居认证(LFNA)模式,阻止副本节点和女巫节点成功加入网络; 最后,给出了 LFNA 的安全性证明和分析,并在安全和开销方面与已有的典型防御机制进行比较分析,结果表明 LFNA 在整体上要优于已有方案.

参考文献

[1] 任秀丽,杨威,薛建生,等. 基于分区的无线传感器网节点复制攻击检测方法[J]. 电子学报,2010,38(9):2095-2100.
Ren Xiu-li,Yang Wei,Xue Jian-sheng,et al. Method of detecting the replication attack based on zoning in wireless sensor networks[J]. Acta Electronica Sinica,2010,38(9):2095-2100. (in Chinese)

[2] Newsome J,Shi E,Song D,et al. The Sybil attack in sensor networks: Analysis & defenses[A]. Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks[C]. New York: ACM,2004. 259-268.

[3] Manjula V,Chellappan C. The replication attacks in wireless sensor networks: Analysis and defenses[A]. Proceedings of the 1st International Conference on Computer Science and Information Technology[C]. Heidelberg: Springer Verlag,2011. 169-178.

[4] Zhu W T,Zhou J Y,Deng R H,et al. Detecting node replication attacks in wireless sensor networks: A survey[J]. Journal of Network and Computer Applications,2012,35(3):1022-1034.

[5] Parno B,Perrig A,Gligor V. Distributed detection of node replication attacks in sensor networks[A]. Proceedings of the 2005 IEEE Symposium on Security and Privacy[C]. New Jersey: IEEE,2005. 49-63.

[6] Ho J W,Liu D G,Wright M,et al. Distributed detection of replica node attacks with group deployment knowledge in wireless sensor networks[J]. Ad hoc Networks,2009,7(8):1476-1488.

[7] Ho J W,Liu D G,Wright M,et al. Distributed detection of replicas with deployment knowledge in wireless sensor networks[A]. Proceedings of the 7th Annual IEEE International Conference on Pervasive Computing and Communications[C]. New Jersey: IEEE CS,2009. 1-6.

[8] Demirbas M, Song Y. An RSSI-based scheme for Sybil attack detection in wireless sensor networks [A]. Proceedings of the International Symposium on a World of Wireless, Mobile and Multimedia Networks [C]. New Jersey: IEEE CS, 2006. 564 – 568.

[9] Wang J T, Yang G, Sun Y, et al. Sybil attack detection based on RSSI for wireless sensor network [A]. Proceedings of the International Conference on Wireless Communications, Networking and Mobile Computing [C]. New Jersey: IEEE CS, 2007. 2684 – 2687.

[10] Wang W T, Ssu K F, Chang W C. Defending Sybil attacks based on neighboring relations in wireless sensor networks [J]. Security and Communication Networks, 2010, 3(5): 408 – 420.

[11] Zhang Y C, Liu W, Lou W J, et al. Securing sensor networks with location-based keys [A]. Proceedings of the 2005 IEEE Wireless Communications and Networking [C]. New Jersey: IEEE, 2005. 1909 – 1914.

[12] Zhang Y C, Liu W, Lou W J, et al. Location-based compromise-tolerant security mechanisms for wireless sensor networks [J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2): 247 – 260.

[13] Duan M J, Xu J. An efficient location-based compromise-tolerant key management scheme for sensor networks [J]. Information Processing Letters, 2011, 111(11): 503 – 507.

[14] Bekara C, Laurent-Maknavicjus M. A new protocol for securing wireless sensor networks against nodes replication attacks [A]. Proceedings of the 3rd IEEE International Conference on Wireless and Mobile Computing, Networking and Communications [C]. New Jersey: IEEE CS, 2007. 1 – 7.

[15] Zhang Q H, Wang P, Reeves D S, et al. Defending against Sybil attacks in sensor networks [A]. Proceedings of the 25th IEEE International Conference on Distributed Computing Systems Workshops [C]. New Jersey: IEEE CS, 2005. 185 – 191.

[16] Yin J, Madria S K. Sybil attack detection in a hierarchical sensor network [A]. Proceedings of the 3rd International Conference on Security and Privacy in Communication Networks [C]. New Jersey: IEEE CS, 2007. 494 – 503.

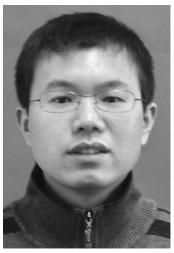
[17] Shokri R, Poturalski M, Ravot G, et al. A practical secure neighbor verification protocol for wireless sensor networks [A]. Proceedings of the 2nd ACM Conference on Wireless Network Security [C]. New York: ACM, 2009. 193 – 200.

[18] 杨峰,周学海,张起元,等. 无线传感器网络恶意节点溯源追踪方法研究 [J]. 电子学报, 2009, 37(1): 202 – 206.
Yang Feng, Zhou Xue-hai, Zhang Qi-yuan, et al. A practical traceback mechanism in wireless sensor networks [J]. Acta Electronica Sinica, 2009, 37(1): 202 – 206. (in Chinese)

[19] 杨庚,王江涛,程宏兵,等. 基于身份加密的无线传感器网络密钥分配方法 [J]. 电子学报, 2007, 35(1): 180 – 184.
Yang Geng, Wang Jiang-tao, Cheng Hong-bing, et al. A key establish scheme for WSN based on IBE and Diffie-Hellman algorithms [J]. Acta Electronica Sinica, 2007, 35(1): 180 – 184. (in Chinese)

[20] Barreto P, Lynn B, Scott M. On the selection of pairing-friendly groups [A]. Proceedings of the 10th Annual International Workshop on Selected Areas in Cryptography [C]. Heidelberg: Springer-Verlag, 2003. 17 – 25.

作者简介



胡蓉华 男,1985 年 5 月出生,湖北荆州人. 2010 年获东北大学计算机软件与理论专业工学硕士学位. 现为东北大学博士生,主要研究方向: 无线传感器网络安全、信息隐藏等.

董晓梅 女,1970 年 5 月出生,河南开封人. 东北大学副教授,主要研究方向为网络与信息安全、信息隐藏、计算机取证等.
E-mail: dongxiaomei@ise.neu.edu.cn

王大玲 女,1962 年 6 月出生,辽宁新民人. 东北大学教授、博士生导师,主要研究方向为据挖掘、机器学习、信息检索等.