ISSN 1004-9037,CODEN SCYCE4
Journal of Data Acquisition and Processing Vol. 36,No. 5,Sep. 2021,pp. 1020－1029
DOI:10. 16337/j. 1004-9037. 2021. 05. 017
© 2021 by Journal of Data Acquisition and Processing
http://sjcj. nuaa. edu. cn
E-mail:sjcj@nuaa. edu. cn
Tel/Fax:＋86-025-84892742

移动场景下异构无线传感器网络密钥管理方法

李　峰[1]，李亚平[2]，张志军[2]，解　鹏[2]，郭学让[1]，袁二东[3]，祁　雷[3]

(1. 国网新疆电力有限公司电力科学研究院,乌鲁木齐 830011;2. 国网新疆电力有限公司调度控制中心,乌鲁木齐 830017;3. 新疆大学信息科学与工程学院,乌鲁木齐 830046)

摘　要：由于移动无线传感器网络支持节点的移动性,使其面临更加复杂的安全性挑战,很难防御一些极具破坏力的攻击,比如节点复制攻击和女巫攻击等。本文提出了在移动异构无线传感器网络模型下一种安全高效的密钥管理方法。所提方法采用椭圆曲线密码学加密算法实现移动节点位置信息到基站的安全上传,以及基于密钥哈希的消息认证码来实现消息源的身份认证。基站则对收集的移动节点位置信息进行统计分析来协助完成固定节点与移动节点间的身份认证及会话密钥建立。实验结果表明,所提方法在密钥建立过程节省了网络资源,同时可有效防御攻击者发起重放攻击、节点复制攻击和女巫攻击等,增强了网络安全性。

关键词：密钥管理;安全性;移动节点;节点复制攻击;移动无线传感器网络

中图分类号：TN918　　**文献标志码**:A

Key Management Method in Mobile Scenarios for Heterogeneous Wireless Sensor Networks

LI Feng[1], LI Yaping[2], ZHANG Zhijun[2], XIE Peng[2], GUO Xuerang[1], YUAN Erdong[3], QI Lei[3]

(1. Electric Power Research Institute, State Grid Xinjiang Electric Power Co., Ltd, Urumqi 830011, China;2. Dispatching Control Center, State Grid Xinjiang Electric Power Co., Ltd, Urumqi 830017, China;3. School of Information Science and Engineering, Xinjiang University, Urumqi 830046, China)

Abstract: Mobile wireless sensor networks (MWSNs) support the mobility of nodes, and face more complex security challenges. It is difficult to prevent attackers from launching some extremely destructive attacks, such as node replication attacks and sybil attacks. This paper proposes a safe and efficient key management method under the mobile heterogeneous wireless sensor network model. The proposed method adopts the elliptic curve cryptography encryption algorithm to realize the safe upload of mobile node location information to the base station, and uses the message authentication code based on key hash to realize the identity authentication of the message source. The base station performs statistical analysis on the collected location information of the mobile node to assist in completing the identity authentication and session key establishment between the fixed node and the mobile node. Experimental results show that the proposed method saves network resources during the key establishment process, and can effectively defend

基金项目:国家自然科学基金(61771416)资助项目。
收稿日期:2020-08-25;**修订日期**:2021-07-06

against attackers from launching replay attacks, node replication attacks, and sybil attacks, thus enhancing network security.

Key words: key management; security; mobile node; node replication attack; mobile wireless sensor networks (MWSNs)

引　言

移动传感器网络(Mobile wireless sensor networks, MWSNs)由于支持节点在有限范围内移动在诸多领域有广泛的应用,比如移动终端用户和移动机器人等用于环境监测、工业过程监测以及军事和民用相关的应用领域,而且节点的移动性可以有效缓解网络自身运行过程存在的一些问题,比如:网络覆盖问题和能量空洞问题[1-3]。Zhang等[4]提出了用于无线传感器网络的节能分布式确定性密钥管理方案,网络模型既支持静态节点间的会话密钥建立,也支持移动节点(Mobile node, MN)与静态节点间的会话密钥建立;所提方案中每个节点利用预加载的初始密钥K_1来间接获取邻居节点信息,同时将邻居节点信息以邻居表的形式进行存储。为抵御女巫攻击和节点复制攻击,文献[4]方法采用一个阈值来限制任何节点的邻居数量,即邻居表中节点数量。当节点的邻居数量达到阈值时,不能在邻居表中添加新邻居,该方案在某种程度上防止了入侵者发起女巫攻击和节点复制攻击,但却限制了节点的移动性,因此对移动节点抵御这两类攻击还需进一步改进。Khan等[5]提出了一种移动异构传感器网络下的高效密钥管理方案。该方案中节点在会话密钥建立之前,通过借助消息认证码和数字签名算法实现了MN与固定节点(Fixed node, FN)间以及MN间的身份认证。文献[5]方法具有较好的网络连通性,但是安全性不足,尽管该方案也采取了抵御节点复制攻击的措施,然而该措施仅适用于移动节点在当前簇移动时的场景,却无法适用于MN从当前簇移动到新簇的过程中存在的节点复制攻击问题。Kar等[6]提出了一种基于双线性配对的半移动异构无线传感器网络安全协议,该协议在节点间认证通过后利用双线性配对的思想完成通信密钥的建立。文献[6]方法增强了网络安全性,比如抵御女巫攻击和重放攻击,然而不具备抵御节点复制攻击的能力,同时密钥建立过程所需耗能较多。Kesavan等[7]提出了支持节点移动性的基于簇的安全动态密钥技术。文献[7]方法在密钥建立过程中采用双向恶意节点检测机制来增强网络安全性,可有效抵御多种攻击等:虫洞攻击、冲袭攻击、黑洞攻击、丢包攻击、HELLO泛洪攻击、DoS攻击、选择性转发攻击以及女巫攻击等,然而同样缺乏抵御移动场景下节点复制攻击的能力。徐震等[8]提出了在移动场景下基于互斥基底系统(Exclusion basis system, EBS)的密钥管理方法,该方法给出了密钥的建立和更新、节点间通信的实现过程以及针对节点的移动性,并给出了节点离开当前簇和加入新簇的实现过程。文献[8]方法有较高的安全连通性和抵御节点捕获攻击的能力,然而一旦攻击者捕获一个节点并复制出多个恶意节点,这些恶意节点可利用方法中采用的认证方式随意进入任何簇,从而对网络安全造成巨大威胁。

在MWSNs面临的诸多安全威胁中,节点复制攻击显得尤为棘手。在移动场景下,如何实现节点间密钥建立过程的有效防御节点复制攻击是本文研究的重点。本文针对在移动场景下密钥管理方法设计中依旧存在的问题进行改进,提出了移动场景下基于节点位置信息的异构无线传感器网络密钥管理方法。本文方法在密钥建立过程中利用基站(Base station, BS)所收集的MN的位置信息,并结合相关信息来分析判断MN从当前簇移动到新簇的过程中是否受到节点复制攻击。

1 相关理论

1.1 基于密钥哈希的消息认证码

哈希消息认证码(Hash message authentication code, HMAC)的运作是利用哈希算法以一个密钥和消息作为输入,以生成的消息摘要作为输出,该消息认证码可以保证传输数据的完整性以及实现某个消息源的身份认证,即有

$$\mathrm{HMAC}_i = H(K, M) \tag{1}$$

式中:H为基于密钥的Hash函数;K为密钥;M为消息。发送者将消息和HMAC_i一起发送给接收者;接收者对消息做基于密钥的Hash操作得到新的HMAC_i,并将生成的新的HMAC_i与发送者发送的HMAC_i进行对比;最后,当两者相同时,可以确定消息是完整的,接收者通过利用相同的密钥可以验证消息源的合法性。

1.2 Diffie-Hellman密钥交换协议

Diffie-Hellman密钥交换算法的安全性依赖于椭圆曲线上离散对数的难解[9],其功能在于为通信的双方协商出会话密钥,且协商过程不会受到中间人攻击[10]。

控制者在有限域F_p: $y^2 = x^3 + ax + b$上选择一个安全的椭圆曲线E/F_p,这里$a, b \in F_p$且$\Delta = 4a^3 + 27b^2 \neq 0$。$E/F_p$满足$\Delta = 4a^3 + 27b^2 \neq 0$时为一个非奇异超椭圆曲线,其更适合于密码应用;由于篇幅限制,关于椭圆曲线密码学(Eliptic curve cryptography, ECC)加密算法的部分可参考文献[11]。$E(F_p)$由椭圆曲线上的点和无穷大的点组成,并构成一个群$\mathbb{G}$。$P \in E(F_p)$为$\mathbb{G}$的生成元。该密钥协商的具体过程如下(以节点u和v为例)。

(1)假设节点u和v协商出一个会话密钥K_{uv}。u选择一个随机数$\mathcal{X}_u \in Z_q^*$作为自身的私钥,并计算出公钥$\mathcal{Y}_u = \mathcal{X}_u P$。$u$对$\mathcal{X}_u$的值保密存放而$\mathcal{Y}_u$值可以被$v$公开获得。类似地,$v$选择一个随机数$\mathcal{X}_v \in Z_q^*$作为自身的私钥,同时计算出公钥$\mathcal{Y}_v = \mathcal{X}_v P$。$v$对$\mathcal{X}_v$的值保密存放而$\mathcal{Y}_v$值可以被$u$公开获得。

(2)当u接收到v的公钥$\mathcal{Y}_v$以后,计算出会话密钥为

$$K_{uv} = \mathcal{X}_u \cdot \mathcal{Y}_v = \mathcal{X}_u \cdot \mathcal{X}_v P \tag{2}$$

(3)当v接收到u的公钥$\mathcal{Y}_u$以后,计算出会话密钥为

$$K_{vu} = \mathcal{X}_v \cdot \mathcal{Y}_u = \mathcal{X}_v \cdot \mathcal{X}_u P \tag{3}$$

(4)由于$K_{uv} = K_{vu}$,因此u和v协商出会话密钥。

2 系统模型

支持移动性的网络模型由功能强大的BS、少量FNs和大量的MNs组成。每个FN节点将充当簇头CH的角色。网络模型假设如下:

(1) 考虑到成本问题,MN没有装备防篡改硬件,一旦被攻击者捕获,那么内部存储信息将被泄露。同时MN可通过一些支持节点移动性的安全位置服务[12]获得自身的位置信息。尽管MN具有移动性,但依然在有限的移动范围内。

(2) FN相对MN来说,由于在网络内承担更多的任务,因此在存储空间以及能量储备上会更多一些,且具有防篡改硬件保护装置。

(3) BS可信且受到保护,同时具有强大的计算能力、宽的通信范围以及充足的存储空间和能量,因此在密钥建立过程中其密钥存储空间占用以及计算开销可忽略不计。

(4) 在通信模式上可采用LEAP+[13]中的通信模式:单播、局部广播和全局广播。

图1为本文方法在移动场景下的网络模型图。

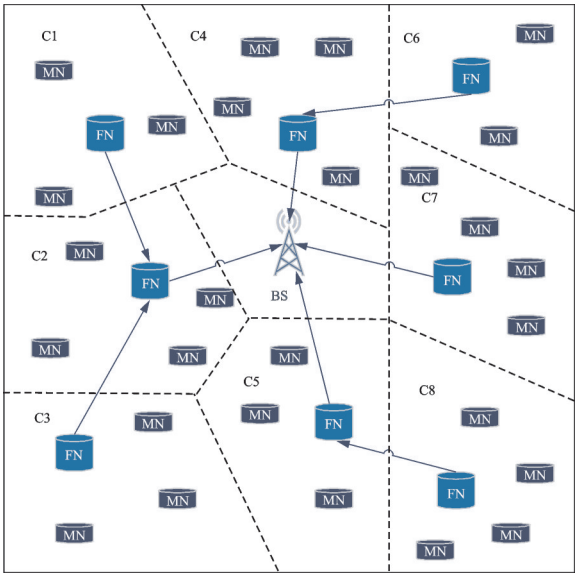

图1　移动场景下网络模型

Fig.1　Network model in mobile scenarios

3　密钥管理方法

为更方便地对本文方法进行描述,表1给出了对一些符号的解释。本文方法中每个MN提前预加载$\{ID_{MN_i}, ID_{FNs}, ID_{BS}, K_{pub_i}, K_{pri_i}\}$;每个FN提前预加载$\{ID_{FN_j}, ID_{BS}, K_{FN_j}, K_H\}$;BS提前预加载$\{ID_{MNs}, ID_{FNs}, ID_{BS}, K_H, K_{pri_s}, K_{FN_s}, v_{max}\}$。

3.1　MN与FN间认证阶段

MN与FN间在建立通信密钥之前需要进行安全认证。所提方案中,FN首先局部广播一个Hello消息,该Hello消息包含FN自身的标识符ID_{FN_j}。网络内MN接收到多个FN的Hello消息后根据信号强度选择信噪比最高的FN作为自身的CH(比如CH_1)。

$$FN \rightarrow *: \text{Hello}\{ID_{FN_j}\} \tag{4}$$

MN(比如u)将与该CH_1完成身份认证,u发送一个加入请求消息给CH_1,此加入请求消息包含u自身的标识ID_{MN_u}、经K_{pub_u}加密处理后的时间戳T_{MN_u}和位置信息l_{MN_u}(建立通信密钥时MN为静止状态)以

表1　符号和描述

Table 1　Symbols and descriptions

符号	描述
ID_{MN_i,FN_j}	MN或FN的身份标志符
ID_{MN_s}	网络MNs的身份标志符链
ID_{FNs}	网络FNs的身份标志符链
l_{MN_i}	MN的位置信息
K_{pub_i}	MN自身ECC加密公钥
K_{pri_i}	MN自身ECC解密私钥
K_{pri_s}	所有MNs自身ECC解密私钥
K_{FN_j}	FN自身的私钥
K_{FN_s}	所有FNs的私钥
K_H	FNs与BS之间的通信密钥
v_{max}	MN的最大移动速度
$T_{MN_i,FN_j,BS}$	MN、FN或BS的时间戳
$E(k,m)$	密钥k对m进行对称或非对称加密
$D(K,m)$	密钥K对m进行对称或非对称解密

及结合K_{pri_u}对加密处理后的时间戳T_{MN_u}和位置信息l_{MN_u}进行哈希函数操作得到HMAC_0。CH_1接收到u的加入请求消息后，先结合自身的私钥$K_{\mathrm{FN}_{\mathrm{CH}_1}}$对$u$的加入请求消息进行哈希函数操作生成$\mathrm{HMAC}_1$；接着利用$K_H$对自身的时间戳$T_{\mathrm{CH}_1}$进行加密处理；最后将自身的$ID_{\mathrm{CH}_1}$、自身加密处理后的时间戳、$u$的加入请求信息以及$\mathrm{HMAC}_1$发送给BS。

$$u\colon \mathrm{HMAC}_0 = H(K_{\mathrm{pri}_u}, E(K_{\mathrm{pub}_u}, T_{\mathrm{MN}_u}\|l_{\mathrm{MN}_u})) \tag{5}$$

$$u \rightarrow \mathrm{CH}_1\colon \left\{ID_{\mathrm{MN}_u}, E(K_{\mathrm{pub}_u}, T_{\mathrm{MN}_u}\|l_{\mathrm{MN}_u}), \mathrm{HMAC}_0\right\} \tag{6}$$

$$\mathrm{CH}_1\colon \mathrm{HMAC}_1 = H(K_{\mathrm{FN}_{\mathrm{CH}_1}}, E(K_{\mathrm{pub}_u}, T_{\mathrm{MN}_u}\|l_{\mathrm{MN}_u}\|\|\mathrm{HMAC}_0) \tag{7}$$

$$\mathrm{CH}_1 \rightarrow \mathrm{BS}\colon \left\{ID_{\mathrm{CH}_1}, ID_{\mathrm{MN}_u}, E(K_H, T_{\mathrm{CH}_1}), E(K_{\mathrm{pub}_u}, T_{\mathrm{MN}_u}\|l_{\mathrm{MN}_u})\|\mathrm{HMAC}_0, \mathrm{HMAC}_1\right\} \tag{8}$$

BS接收到上述信息后先利用CH_1的私钥$K_{\mathrm{FN}_{\mathrm{CH}_1}}$来验证$\mathrm{HMAC}_1$内数据的完整性，同时可确认该消息来自$\mathrm{CH}_1$；同理，再利用$u$的私钥$K_{\mathrm{pri}_u}$来验证$\mathrm{HMAC}_0$内加密处理后的$l_{\mathrm{MN}_u}$的数据完整性，同时可确认该加密消息最初来自$u$，完成对消息源的身份认证；接着BS利用$K_{\mathrm{pri}_u}$解密获得$T_{\mathrm{MN}_u}$和$l_{\mathrm{MN}_u}$以及利用$K_H$解密获得$T_{\mathrm{CH}_1}$，通过验证$T_{\mathrm{CH}_1}$和$T_{\mathrm{MN}_u}$是否有效来保证消息的新鲜度以防止攻击者发起重放攻击（下同）；最后BS将存储ID_{MN_u}、l_{MN_u}和T_{MN_u}，并且通过单播的方式通知CH_1将u加入自身成员列表，该通知消息内包含ID_{BS}、ID_{MN_u}、经K_H加密处理后的T_{BS}、l_{MN_u}和u的私钥K_{pri_u}。CH_1随之存储ID_{MN_u}、l_{MN_u}、T_{MN_u}和K_{pri_u}。

$$\mathrm{BS}\colon T_{\mathrm{MN}_u}\|l_{\mathrm{MN}_u} = D(K_{\mathrm{pri}_u}, E(K_{\mathrm{pub}_u}, T_{\mathrm{MN}_u}\|l_{\mathrm{MN}_u})) \tag{9}$$

$$\mathrm{BS} \rightarrow \mathrm{CH}_1\colon \left\{ID_{\mathrm{BS}}, ID_{\mathrm{MN}_u}, E(K_H, T_{\mathrm{BS}}\|l_{\mathrm{MN}_u}\|K_{\mathrm{pri}_u})\right\} \tag{10}$$

$$\mathrm{CH}_1\colon T_{\mathrm{BS}}\|l_{\mathrm{MN}_u}\|K_{\mathrm{pri}_u} = D(K_H, E(K_H, T_{\mathrm{BS}}\|l_{\mathrm{MN}_u}\|K_{\mathrm{pri}_u})) \tag{11}$$

CH_1获得u的私钥K_{pri_u}后，利用K_{pri_u}加密自身的身份标志符ID_{FN_j}后发送给u。当u利用自身的私钥K_{pri_u}可实现解密时，可确认CH_1身份的合法性。

3.2 节点间密钥建立

当CH_1和u间完成身份认证以后，两者开始建立通信密钥K_{u1}。CH_1首先生成一个标量d，接着d点乘$E(F_p)$上的生成元P得到可公开密钥$K_1 = d\cdot P$；同理，u生成一个标量c，接着在$E(F_p)$上c点乘P得到可公开密钥$K_u = c\cdot P$。u与CH_1分别将K_u和K_1发送给对方，两者随之采用Diffie-Hellman密钥交换协议建立通信密钥$K_{u1} = c\cdot K_1 = c\cdot d\cdot P = d\cdot K_u = d\cdot c\cdot P = K_{1u}$。

两个MN（比如u和v）欲建立通信密钥K_{uv}。u和v首先分别局部广播自身的身份标志符ID_{MN_u}和ID_{MN_v}；接着每个MN（例如u）将ID_{MN_u}、邻居v的身份标志符ID_{MN_v}、经K_{u1}加密处理后的当前时间戳$\bar{T}_{\mathrm{MN}_u}$和新的$\bar{l}_{\mathrm{MN}_u}$发送给CH_1；CH_1接收到这些信息后解密获得u和v新的位置信息$\bar{l}_{\mathrm{MN}_u}$和$\bar{l}_{\mathrm{MN}_v}$以及时间戳$\bar{T}_{\mathrm{MN}_u}$和$\bar{T}_{\mathrm{MN}_v}$；最后CH_1将ID_{CH_1}以及经K_H加密处理后的T_{CH_1}、$\bar{T}_{\mathrm{MN}_u}$、$\bar{T}_{\mathrm{MN}_v}$、$\bar{l}_{\mathrm{MN}_u}$和$\bar{l}_{\mathrm{MN}_v}$发送给BS。

$$v \rightarrow *\colon \left\{ID_{\mathrm{MN}_v}\right\} \tag{12}$$

$$u \rightarrow \mathrm{CH}_1\colon \left\{ID_{\mathrm{MN}_u}, ID_{\mathrm{MN}_v}, E(K_{u1}, \bar{T}_{\mathrm{MN}_u}\|\bar{l}_{\mathrm{MN}_u})\right\} \tag{13}$$

$$\mathrm{CH}_1\colon \bar{T}_{\mathrm{MN}_u}\|\bar{l}_{\mathrm{MN}_u}=D(K_{u1},E(K_{u1},\bar{T}_{\mathrm{MN}_u}\|\bar{l}_{\mathrm{MN}_u})) \tag{14}$$

$$\mathrm{CH}_1\rightarrow \mathrm{BS}\colon\left\{ID_{\mathrm{CH}_1},\mathrm{E}(K_H,T_{\mathrm{CH}_1}\|\bar{T}_{\mathrm{MN}_u}\|\bar{T}_{\mathrm{MN}_v}\|\bar{l}_{\mathrm{MN}_u}\|\bar{l}_{\mathrm{MN}_v})\right\} \tag{15}$$

BS分别利用u和v移动的前后位置信息、时间戳和移动节点最大速度$v_{\max}$来判断u和v是否受到节点复制攻击[14]。

如果BS判断出u和v均为合法MN,BS将更新存储u和v的位置信息$\bar{l}_{MN_u}$和$\bar{l}_{MN_v}$以及时间戳$\bar{T}_{MN_u}$和$\bar{T}_{MN_v}$,并告知CH_1两个节点合法;CH_1利用伪随机函数生成u和v间的通信密钥K_{uv},并分别利用与u和v间的通信密钥K_{u1}和K_{v1}对K_{uv}和自身的时间戳T_{CH_1}进行加密保护,并通过单播的方式发送给u和v。u和v解密获得两者间的通信密钥K_{uv}。

$$\mathrm{CH}_1\rightarrow u\colon\left\{ID_{\mathrm{CH}_1},ID_{\mathrm{MN}_v},E(K_{u1},T_{\mathrm{CH}_1}\|K_{uv})\right\} \tag{16}$$

$$u\colon T_{\mathrm{CH}_1}\|K_{uv}=D(K_{u1},E(K_{u1},T_{\mathrm{CH}_1}\|K_{uv})) \tag{17}$$

$$\mathrm{CH}_1\rightarrow v\colon\left\{ID_{\mathrm{CH}_1},T_{\mathrm{CH}_1},ID_{\mathrm{MN}_u},E(K_{v1},T_{\mathrm{CH}_1}\|K_{uv}K_{uv})\right\} \tag{18}$$

$$v\colon T_{\mathrm{CH}_1}\|K_{uv}=D(K_{v1},E(K_{v1},T_{\mathrm{CH}_1}\|K_{uv})) \tag{19}$$

3.3　簇节点更新过程

网络内MN由于资源限制将面临节点死亡的状况,这将导致CH管辖区域内MN_s数量不足而无法完成一些任务。解决办法是向网络内添加新的MN_s以及MN_s通过移动到其他FN管辖区域来解决。新的MN_s添加可采用上述思想完成节点间的通信密钥建立,而当一个MN(例如u)由当前簇头(比如CH_1)管辖区域C_1移动到下一个簇头(比如CH_2)管辖区域C_2,则需要簇间节点认证。当认证通过后,u与CH_2间生成通信密钥K_{u2}。u完成跨管辖区域的具体认证过程如下:u向CH_1发送离开消息,该离开消息包含ID_{MN_u}以及经K_{u1}加密处理后的T_{MN_u}和l_{MN_u};CH_1利用K_{u1}解密获得u离开管辖区域C_1时的T_{MN_u}和l_{MN_u}。当u移动进入CH_2的管辖区域C_2后,u向CH_2发送加入请求消息,此加入请求消息包含ID_{MN_u}、ID_{CH_1}、以及进入CH_2的管辖区域与CH_2待完成身份认证时的当前的时间戳$\bar{\bar{T}}_{\mathrm{MN}_u}$和$\bar{\bar{l}}_{\mathrm{MN}_u}$,这里$\bar{\bar{T}}_{\mathrm{MN}_u}$和$\bar{\bar{l}}_{\mathrm{MN}_u}$同样经过$K_{u1}$加密处理。

$$u\rightarrow \mathrm{CH}_1\colon\left\{ID_{MN_u},E(K_{u1},T_{\mathrm{MN}_u}\|l_{\mathrm{MN}_u})\right\} \tag{20}$$

$$\mathrm{CH}_1\colon T_{\mathrm{MN}_u}\|l_{\mathrm{MN}_u}=D(K_{u1},E(K_{u1},T_{\mathrm{MN}_u}\|l_{\mathrm{MN}_u})) \tag{21}$$

$$u\rightarrow \mathrm{CH}_2\colon\left\{ID_{\mathrm{MN}_u},ID_{\mathrm{CH}_1},E(K_{u1},\bar{\bar{T}}_{\mathrm{MN}_u}\|\bar{\bar{l}}_{\mathrm{MN}_u})\right\} \tag{22}$$

CH_2接收到u的加入请求消息后,将向CH_1发送请求验证消息,该请求验证消息包括ID_{CH_2}、ID_{MN_u}和经过K_{u1}加密处理T_{CH_2}、$\bar{\bar{T}}_{\mathrm{MN}_u}$和$\bar{\bar{l}}_{\mathrm{MN}_u}$。$\mathrm{CH}_1$利用$K_{u1}$解密获得$u$进入管辖区域$C_2$的待完成身份认证时的$T_{\mathrm{CH}_2}$、$\bar{\bar{T}}_{\mathrm{MN}_u}$和$\bar{\bar{l}}_{\mathrm{MN}_u}$。

$$\mathrm{CH}_2\rightarrow \mathrm{CH}_1\colon\left\{ID_{\mathrm{CH}_2},ID_{\mathrm{MN}_u},E(K_{u1},T_{\mathrm{CH}_2}\|\bar{\bar{T}}_{\mathrm{MN}_u}\|\bar{\bar{l}}_{\mathrm{MN}_u})\right\} \tag{23}$$

$$\mathrm{CH}_1\colon T_{\mathrm{CH}_2}\left\|\bar{\bar{T}}_{\mathrm{MN}_u}\right\|\bar{\bar{l}}_{\mathrm{MN}_u}=(K_{u1},E(K_{u1},T_{\mathrm{CH}_2}\|\bar{\bar{T}}_{\mathrm{MN}_u}\|\bar{\bar{l}}_{\mathrm{MN}_u})) \tag{24}$$

CH_1将ID_{CH_1}和经K_H加密处理后的T_{CH_1}、T_{MN_u}、$\bar{\bar{T}}_{\mathrm{MN}_u}$、$l_{\mathrm{MN}_u}$和$\bar{\bar{l}}_{\mathrm{MN}_u}$发送给BS。BS利用$K_H$解密获得$T_{CH_1}$、$T_{\mathrm{MN}_u}$、$\bar{\bar{T}}_{\mathrm{MN}_u}$、$l_{\mathrm{MN}_u}$和$\bar{\bar{l}}_{\mathrm{MN}_u}$并结合$T_{\mathrm{MN}_u}$和$\bar{\bar{T}}_{\mathrm{MN}_u}$以及$v_{\max}$来判断$u$是否受到复制节点攻击[14]。

$$\mathrm{CH}_1 \rightarrow \mathrm{BS}:\left\{ID_{\mathrm{CH}_1}, E(K_H, T_{\mathrm{CH}_1}\|T\|_{\mathrm{MN}_u}\|\bar{\bar{T}}_{\mathrm{MN}_u}\|l_{\mathrm{MN}_u}\|\bar{\bar{l}}_{\mathrm{MN}_u})\right\} \tag{25}$$

$$\mathrm{BS}: T_{\mathrm{CH}_1}\|T_{\mathrm{MN}_u}\|\bar{\bar{T}}_{MN_u}\|l_{\mathrm{MN}_u}\|\bar{\bar{l}}_{\mathrm{MN}_u} = D(K_H, E(K_H, T_{\mathrm{CH}_1}\|\,T_{\mathrm{MN}_u}\|\bar{\bar{T}}_{\mathrm{MN}_u}\|l_{\mathrm{MN}_u}\|\bar{\bar{l}}_{\mathrm{MN}_u})) \tag{26}$$

如果判断u为合法节点，BS将存储ID_{MN_u}、$\bar{\bar{l}}_{\mathrm{MN}_u}$和$\bar{\bar{T}}_{\mathrm{MN}_u}$，并且安全通知$\mathrm{CH}_2$将$u$加入自身成员列表，该通知消息内包含$ID_{\mathrm{BS}}$、$ID_{\mathrm{MN}_u}$和经$K_H$加密处理后的$T_{\mathrm{BS}}$、$\bar{\bar{T}}_{\mathrm{MN}_u}$和$\bar{\bar{l}}_{\mathrm{MN}_u}$。$\mathrm{CH}_2$随之解密通知消息并存储$ID_{\mathrm{MN}_u}$、$\bar{\bar{l}}_{\mathrm{MN}_u}$和$\bar{\bar{T}}_{\mathrm{MN}_u}$。

$$\mathrm{BS}\rightarrow \mathrm{CH}_2:\left\{ID_{\mathrm{BS}}, ID_{\mathrm{MN}_u}, E(K_H, T_{\mathrm{BS}}\|\bar{\bar{T}}_{\mathrm{MN}_u}\|\bar{\bar{l}}_{\mathrm{MN}_u})\right\} \tag{27}$$

$$\mathrm{CH}_2: T_{\mathrm{BS}}\|\bar{\bar{T}}_{\mathrm{MN}_u}\|\bar{\bar{l}}_{\mathrm{MN}_u} = D(K_H, E(K_H, T_{\mathrm{BS}}\|\bar{\bar{T}}_{\mathrm{MN}_u}\|\bar{\bar{l}}_{\mathrm{MN}_u})) \tag{28}$$

u将采用上述与CH_1建立通信密钥的方式完成与CH_2间的通信密钥建立。

4 性能分析

4.1 安全性分析

(1)捕获攻击。攻击者通过捕获某些节点来获取一些有用信息，且利用这些有用信息获得未被捕获节点的密钥。同时攻击者捕获的节点越多，获得的有用信息越多，网络内未被捕获节点密钥泄露的概率越大。本文方法采用Diffie-Hellman密钥交换协议完成通信密钥的建立，攻击者无法利用捕获节点的信息来获取到未捕获节点的密钥，因此本文方法可有效抵御节点捕获攻击。

(2)重放攻击。攻击者通过重放之前的身份验证代码来误导合法节点，并将其同步到错误的时间上。本文方法中移动节点的转发消息均通过加入加密处理后的时间戳来保证消息的新鲜度，因此本文方法可有效抵御攻击者发起重放攻击。

(3)节点复制攻击。攻击者捕获节点后将其副本放置在多个地理位置用于与合法节点建立非法通信连接。本文方法着重考虑移动场景下MN从当前簇移动到新簇的过程中存在的节点复制攻击。本文方法在MN与FN以及MN间建立会话密钥前采取了身份认证；同时BS通过利用节点移动前后的位置信息、时间戳和MN的最大移动速度来分析节点是否受到节点复制攻击。与其他方案相比，本文方法可有效抵御在移动场景下攻击者发起的节点复制攻击。

(4)女巫攻击。攻击者将一个节点伪造成多重身份来误导合法节点认为所接收消息是来自不同节点，通过这种方式来发起恶意攻击。女巫攻击的防范一般可通过基于身份认证和基于位置验证的方法。攻击者若想伪造多重MN身份来发起女巫攻击，则必须通过身份认证和位置验证。与其他方案相比，本文方法中，节点(MN或FN)通过利用预加载的唯一的私钥(该私钥仅BS可知)来实现节点安全的双向身份认证以及通过位置信息和时间戳来实现位置验证，因而，本文方法可有效抵御攻击者发起女巫攻击。

表2给出了本文方法与文献[5-6,8]中方法在安全性上的对比结果，结果表明本文方法的安全性较好。尽管文献[5]方法也采取了抵御节点复制攻击的措施，然而仅适用于MN在当前簇移动时的场景，无法适用于MN从当前簇移动到新簇的过程中存在的节点复制攻击。文献[6]方法在安全防护方面做得相对较好，然而依然不具备抵御节点复制攻击的能力。文献[8]方法仅考虑了抵御节点捕获攻击和重放攻击，然而在移动场景下对

表2 不同方法的安全性对比

Table 2 Comparison of safety for different methods

方法类型	文献[5]	文献[6]	文献[8]	本文
抵御捕获攻击	是	是	是	是
抵御重放攻击	否	是	是	是
抵御复制攻击	是	否	否	是
抵御女巫攻击	否	是	否	是

女巫攻击和节点复制攻击却无法抵御。本文方法中MN在当前簇移动以及从当前簇移动到新簇的过程均可有效抵御节点复制攻击,从而增强了网络安全性。

4.2　有效性分析

4.2.1　密钥预存储开销对比

假设该网络模型下,FN和MN的数目分别为M和N,这里$M \ll N$。文献[5]方法中每个FN预加载BS的公钥、自身的公/私钥对、私钥生成器SKG、妥协节点监测密钥CNDK和网络私钥K_{prt};每个MN预加载秘密通信密钥SK和网络公钥K_{plc};总的密钥存储空间占用为$6\times M+2\times N$。文献[6]方法中每个FN和MN分别预加载自身基于身份的私钥S_x、与BS通信的对称密钥K_x和全局广播密钥G;总的密钥存储空间占用为$3\times M+3\times N$。文献[8]方法中当每个节点存储的密钥数量超过$k+m$的1/2时,连通率为1,此时每个FN和MN需至少存储10个密钥,总的密钥存储空间占用为$10\times M+10\times N$。本文方法中每个FN预加载自身的私钥K_{FN_j}和K_H;每个MN预加载自身的公钥K_{pub_i}和私钥K_{pri_i};总的密钥存储空间占用为$2\times M+2\times N$。表3为网络节点的分配情况可以更直观地表示密钥存储空间占用情况。表3中1～5分别代表不同网络规模下节点分配情况,数字越大代表网络规模越大。

表3　网络节点分配情况

Table 3　Distribution of network nodes

节点类型	1	2	3	4	5
FN	4	8	12	16	20
MN	196	392	588	784	980

图2为本文方法与上述3种方法在密钥预存储开销上的对比。结果显示本文方法在密钥预存储空间占用上相对较少。文献[5]方法为实现加密和身份认证的功能预加载于FN内的密钥较多,而预加载于每个MN内的密钥数目与本文方法相同。文献[6]方法中每个MN预加载3个相关密钥来实现加密和身份认证的功能,而本文方法每个MN仅预加载自身的公钥和私钥即可。文献[8]采用EBS来生成对密钥,为满足网络连通性为1,每个节点需至少存储10个密钥,这导致密钥存储空间占用最大。本文方法则在密钥预存储开销上较少,节省了节点存储资源。

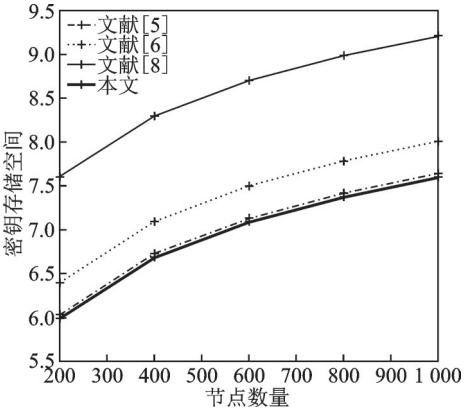

图2　各方法密钥预存储空间占用对比

Fig.2　Comparison of key pre-storage space occupied by each scheme

4.2.2　密钥建立过程的计算开销对比

为了分析算法的计算开销情况,本文在MATLAB R 2016a实验平台上对算法进行了开销计算。实验环境计算机的配置为:2.60 GHz Intel Core i7-9750 CPU 和8.0 GB内存。

移动场景下主要解决MN与FN间通信密钥的建立,因此,本文方法统一考虑单个MN从当前簇移动到新簇过程中完成密钥建立的计算开销。本文根据文献[15]基于GNU高精度算术运算库(GNU multiple precision arithmetic libravy, GMP)的基于配对的密码库(Pairing based cryptography libravy, PBC)获取了一些重要计算参数,表4列出了各种计算操作耗时。图3为各方法中单个MN与FN完成会话密钥建立的耗时对比。

由图3可知,与文献[5-6]方法相比,本文方法完成密钥建立过程的计算开销相对较少。文献[5]方法完成节点间加密操作以及身份认证大多集中在FN与MN自身来完成,而本文方法的节点身份认证计算过程转移到了资源强大的BS上来完成,因此节省了密钥建立过程中的计算开销。文献[6]方法生

成密钥建立过程的会话密钥采用了双线性配对操作,而双线性配对操作与本文方法会话密钥生成所采用的Diffie-Hellman密钥交换协议所执行的点乘相比计算开销较大。文献[8]方法密钥建立过程没有在图3中表示是由于其仅采取了消息认证码和对称加解密操作在计算开销上极少,甚至无法显示。这看似对节省计算开销非常有利,然而由于缺少必要的操作过程导致安全性严重不足。文献[8]方法中移动节点直接将要加入新簇的请求消息发送给汇聚节点(相当于本文所提方法中的BS),该过程未充分利用簇头通信范围广、传递消息快的优势,因此在传递请求消息上是低效的,会为攻击者提供更多的攻击时间;同时该方法缺乏新簇头与旧簇头对移动节点身份和消息的双向认证过程,因此在计算开销上是极少的;然而一旦攻击者捕获一个节点并复制出多个恶意节点,这些恶意节点便可以按照方法所采取的认证措施随意进入任何簇,进而对网络安全性造成巨大威胁。

表4 各种计算操作所需耗时

Table 4 Time-consuming for various calculation operations

操作类型	耗时/ms
ECC上的点加操作	0.028 8
ECC上的点乘操作	2.226 0
群$\mathbb{G}$上的哈希操作	12.419 0
群$\mathbb{G}$上的双线性配对操作	5.811 0
单向哈希函数操作	0.002 3
ECC上加密操作	4.452 0
ECC上解密操作	2.226 0
对称加密/解密操作	0.004 6

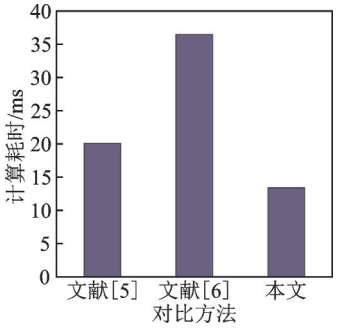

图3 各方法FN与MN会话密钥建立的耗时对比

Fig.3 Comparison of time-consuming in establishment of FN and MN session keys for each method

5 结束语

本文在移动场景下提出了更加安全高效的异构无线传感器网络密钥管理方法。该方法在密钥建立过程中,由BS利用MN的位置信息并结合相关信息来分析判断MN从当前簇移动到新簇的过程中是否受到节点复制攻击,由此来确保节点间密钥建立的合法性;同时,本文方法采用ECC加密算法保护了MN的位置信息,并采用HMAC实现节点间安全的身份认证,不仅保证了密钥建立过程有更好的安全性,而且节省了网络资源。

参考文献:

[1] HUANG H L, SAVKINA A V, DING M, et al. Mobile robots in wireless sensor networks: A survey on tasks[J]. Computer Networks, 2019,148:1-19.

[2] SHA C, REN C, MALEKIAN R, et al. A type of virtual force-based energy-hole mitigation strategy for sensor networks[J]. IEEE Sensors Journal, 2019,20:1105-1119.

[3] 杨明霞,方凯,汪小东,等.一种无线传感器网络感知覆盖空洞搜寻与修复方法[J].传感技术学报,2020,33(5):750-756.
YANG Mingxia, FANG Kai, WANG Xiaodong, et al. Method for searching and repairing wireless sensor network perception coverage holes[J]. Journal of Sensor Technology, 2020,33(5):750-756.

[4] ZHANG X, HE J, WEI Q. EDDK: Energy-efficient distributed deterministic key management for wireless sensor networks[J]. Eurasip Journal on Wireless Communications & Networking,2011(1):1-11.

[5] KHAN S U, LAVAGNO L, PASTRONE C, et al. An effective key management scheme for mobile heterogeneous sensor networks[C]//Proceedings of International Conference on Information Society.London,UK:IEEE,2011:98-103.

[6] KAR D, TATUM R, ZEJDLIK K. MHIP: Effective key management for mobile heterogeneous sensor networks[J]. International Journal of Network Security, 2013,15(4):280-290.

[7] KESAVAN V T, RADHAKRISHNAN S. Cluster based secure dynamic keying technique for heterogeneous mobile wireless sensor networks[J].China Communications, 2016,13:178-194.

[8] 徐震,李秋苇,杨蕾.无线传感器网络中移动场景下的密钥管理方案[J].河南科技大学学报(自然科学版),2020,41(3):35-40.
XU Zhen, LI Qiuwei, YANG Lei. Key management scheme in mobile scenarios in wireless sensor networks[J]. Journal of Henan University of Science and Technology (Natural Science Edition), 2020,41(3):35-40.

[9] GALBRAITH S D, GAUDRY P. Recent progress on the elliptic curve discrete logarithm problem[J]. Designs Codes & Cryptography, 2016,78(1):51-72.

[10] SAQIB N. Key exchange protocol for WSN resilient against man in the middle attack[C]//Proceedings of 2016 IEEE International Conference on Advances in Computer Applications (ICACA). Coimbatore,India:IEEE,2016:265-269.

[11] KEERTHI K, SURENDIRAN B. Elliptic curve cryptography for secured text encryption[C]//Proceedings of 2017 International Conference on Circuit,Power and Computing Technologies (ICCPCT). Kollam,India:IEEE,2017:1-5.

[12] ANGELIS A, FISCIONE C. Mobile node localization via Pareto optimization: Algorithm and fundamental performance limitations[J]. IEEE Journal on Selected Areas in Communications, 2015, 33(7):1288-1303.

[13] ZHU S, SETIA S,JAJODIA S. LEAP+: Efficient security mechanisms for large-scale distributed sensor networks[J].ACM Transactions on Sensor Networks (TOSN), 2006, 2(4):500-528.

[14] HO J W, WRIGHT M, DAS S K. Fast detection of replica node attacks in mobile sensor networks using sequential analysis [C]//Proceedings of IEEE INFOCOM. Rio de Janeiro, Brazil:IEEE,2009:1773-1781.

[15] KILINC H H, YANIK T. A survey of SIP authentication and key agreement schemes[J]. IEEE Communications Surveys & Tutorials, 2014, 16(2):1005-1023.

作者简介:

李峰(1983-),男,硕士,高级工程师,研究方向:网络与信息安全、通信技术、大数据等,E-mail:252491552@qq.com。

李亚平(1967-),男,高级工程师,研究方向:光通信系统、无线通信技术、通信网络安全管理等,E-mail:lyp2926571@163.com。

张志军(1972-),男,高级工程师,研究方向:光通信系统、无线通信技术、通信网络安全管理等,E-mail:kx-bzzj@163.com。

解鹏(1976-),男,高级工程师,研究方向:光通信系统、无线通信技术、通信网络安全管理等,E-mail:tx-cxp123@163.com。

郭学让(1990-),**通信作者**,男,硕士,工程师,研究方向:无线通信技术、无线传感器网络安全等,E-mail:gxrgxr820@163.com。

袁二东(1991-),男,博士,讲师,研究方向:无线传感器网络安全、智能调度优化等,E-mail:577489771@qq.com。

祁雷(1987-),男,博士,讲师,研究方向:物联网技术、嵌入式系统设计、图像目标跟踪等,E-mail:254857301@qq.com。

(编辑:刘彦东)