一种面向WSN的双向身份认证协议及串空间模型

刘 静[1,2] 赖英旭[1,2,3] 杨胜志[4] Lina Xu[5]

(北京工业大学信息学部 北京 100124)[1] (可信计算北京市重点实验室 北京 100124)[2]
(信息保障技术重点实验室 北京 100072)[3] (北京工业大学信息化建设与管理中心 北京 100124)[4]
(爱尔兰都柏林大学计算机学院 都柏林 999014)[5]

摘 要 随着工业互联网、智慧农业、智能家居等领域的发展,无线传感网络(WSN)得到了更广泛的应用,但安全问题也随之凸显。针对无线传感网络中传感器节点易失效、能量和计算存储能力受限等问题,构建了一种基站与传感器节点间的基于状态信息的双向身份认证协议,其能在满足无线传感网络轻量级和低成本要求的同时确保安全性。协议首先在节点接入阶段基于可信网络连接进行平台可信情况的认证,以验证节点的可信情况并实现节点的加密注册。然后在运行阶段通过重要数据双向认证过程对重要数据的传输过程进行保护,利用定时更新认证确认传感器节点的状态和可靠性。协议允许基站定时检测节点的运行状态信息,及时监测到节点的物理损坏,并利用节点的运行状态信息进行认证,以进一步增强协议的安全性。同时,该协议还引入了报警机制,该机制可以区分通信错误、节点的物理损坏以及攻击者攻击。本协议降低了认证过程的通信量,引入的报警消息可以增强排障能力。利用串空间模型对协议进行形式化分析,证明了协议的安全性。最后通过实验验证了设计的双向身份认证协议能提供较好的安全性,而且发送数据增加的延迟时间在可接受的范围内,网络可扩展性好。所提方案能够加强网络接入安全并且有效防御来自节点系统内部的攻击,具有较好的应用价值。

关键词 身份认证协议,无线传感器网络,串空间模型,报警机制

中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2019.09.024

Bilateral Authentication Protocol for WSN and Certification by Strand Space Model

LIU Jing[1,2] LAI Ying-xu[1,2,3] YANG Sheng-zhi[4] Lina XU[5]

(Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China)[1]
(Beijing Key Laboratory of Trusted Computing, Beijing 100124, China)[2]
(National Engineering Laboratory for Critical Technologies of Information Security Classified Protection, Beijing 100072, China)[3]
(Information Technology Support Center, Beijing University of Technology, Beijing 100124, China)[4]
(School of Computer Science, University College Dublin, Dublin 999014, Ireland)[5]

Abstract With the development of industrial Internet, smart agriculture, smart home and other fields, wireless sensor networks (WSN) have been more widely used. However, its security issues have become prominent. Aiming at the problems of the vulnerability to failure as well as the limited capacity of energy and computational storage of sensor nodes in the wireless sensor networks (WSN), this paper constructed a two-way identity authentication protocol based on state information between base station and sensor nodes, which can ensure safety while meeting the requirements of lightweight and low cost of wireless sensor networks. First, the protocol authenticates the trusted situation of the platform based on the trusted network connection in the node access phase, verifies the trusted condition of the node and implements its encrypted registration. Then, during the operation phase, the transmission process of the important data is protected by the two-way authentication process of the data, and the status and reliability of the sensor nodes are confirmed by the timing update authentication. Meanwhile, the protocol allows the base station to periodically detect the running state information of the node, which is used for authentication to further enhance the protocol security, and to timely monitor the physical damage of the node. The proposed protocol reduces the communication process of the au-

到稿日期:2018-08-22 返修日期:2018-11-15 本文受青海省自然科学基金(2017-ZJ-912),北京工业大学国际科研合作种子基金(2018-B9),信息保障技术重点实验室基金(614211204031117),北京市自然科学基金(4162006),国防科技实验信息安全实验室对外开放项目(2015XXAQ09)资助。

刘 静(1978-),女,博士,助理研究员,CCF会员,主要研究方向为网络安全、可信计算,E-mail:jingliu@bjut.edu.cn(通信作者);赖英旭(1973-),女,博士,教授,主要研究方向为网络安全、可信计算;杨胜志(1982-),男,硕士,工程师,主要研究方向为网络安全;Lina Xu(1986-),女,博士,主要研究方向为物联网。

thentication process, while the introduced alarm message can enhance the troubleshooting capability, and the serial space model is used to formally analyze the protocol, proving the security of the protocol. Finally, the experimental results show that under a reasonable safety condition, the designed two-way identity authentication protocol has a good network scalability, and the increased delay time of sending data is within an acceptable range. The solution can enhance network access security and effectively defend against attacks from the inside node system, having good application value.

Keywords Authentication protocol, Wireless sensor networks, Strand space model, Alert mechanism

1 引言

无线传感器网络(Wireless Sensor Networks, WSN)是物联网感知层的重要组成部分,是由部署在监测区域内的大量传感器节点相互通信形成的多跳自组织网络系统[1]。无线传感器网络以协作方式对其覆盖区域内的感知对象进行检测,在工业生产、环境监测、智能家居、空间探索等诸多领域都体现了巨大的应用价值[2-3]。

随着无线传感器网络技术的成熟及其在各领域内的广泛应用,人们对其安全性的关注度越来越高[4]。无线传感器网络的安全性主要体现在两个方面。1)传感器节点硬件上的安全。无线传感器网络的应用范围广泛,传感器节点经常会布置在森林、草场、海洋等场景中,容易被环境腐蚀,更容易被他人恶意破坏,而依靠人力进行定时看管、检测、维护的可能性极小。传感器节点的故障或损坏可能导致重要观测数据的错误或缺失,进而可能导致巨大的损失。2)传感器的网络安全及数据安全。传感器节点易损坏、能量易耗尽的特性,导致系统的网络拓扑更容易出现变化;同时,无线通信的不可靠性和不稳定性,使得无线传感器网络更容易遭到恶意攻击。

无线传感器网络受到硬件尺寸、能量存储、场地环境等因素的制约,需要一套轻量级和低成本的安全方案,在资源受限的情况下尽可能利用身份认证和加密技术来保障数据传递中的保密性、完整性、可用性和真实性,同时可以利用数据鉴别和设备鉴别能力进一步确保无线传感器网络的整体安全性。

本文设计了一种面向 WSN 的双向身份认证协议,以实现传感器节点和基站间的基于状态信息的双向身份认证;并且基于扩展的串空间模型对该协议进行了形式化分析,证明了协议的安全性。

2 相关工作

国内外对面向无线传感器网络的身份认证取得了一定的研究成果。文献[5]提出了传感节点的分布式认证模型,其不需要中心化的认证设备,但是需要大量的传感节点参与认证过程,导致开销不断增大。近两年也有研究采用区块链技术实现无线传感网络的对等身份认证。文献[6]设计了一种安全模型,并提供了基于区块链技术的身份验证机制以及在自组织和演化网络中的信任评估。但是这种方式能耗较大,而且 WSN 中大部分节点也不具备生成区块记录的能力。

目前大部分研究方案还是经过网关节点/基站进行身份认证。文献[7]对 TAI 等[8]提出的身份认证与密钥共识协议进行改进,改进协议可以验证通信双方的真实性,避免假冒攻击,但是文中没有给出协议效率方面的分析。Hammi 等[9]设计了一种基于预共享密钥的双向认证协议,该协议是一种轻量级且有较好健壮性的认证协议,但是使用 HMAC 对数据包进行签名,在计算和执行时间方面消耗较多。Hammi 等[10]又提出了在通信实体之间创建对称安全信道,以便保护交换的数据。该方案在 MAC 子层中实现了相互认证机制,并且在应用层中完成了数据的认证加密,确保了通信实体的相互认证以及对交换数据的完整性和机密性的保护;在每个个人区域网络协调器(Personal Area Network Coordinator, CPAN)创建了一个安全的通信系统,无法在不同的 CPAN 之间实现交互和迁移。文献[11]提出在 WSN 的应用环境下,基于生物特征的匿名身份认证方案和轻量级高效身份认证方案,完成用户、基站/网关节点、传感器节点三者之间的身份认证,并采用 BAN 逻辑证明了协议的安全性。文献[12]通过传感节点的 ID 信息和工作状态信息实现汇聚节点和传感节点之间的双向认证,基站记录节点的 ID 信息和工作状态信息,并采用更新机制进行实时更新。

也有一些方案采用可信接入认证。文献[13]将基站作为可信实体,根据节点行为的表现计算其信任度,再利用信任度判断节点的可信性,实现可信节点间的认证。文献[14]在每个节点配备一个可信平台模块(Trusted Platform Module TPM),在 TPM 中存储每个节点自己的公钥、私钥对以及公钥证书。节点与另一个节点通信时,使用自己的私钥对消息进行签名后,发送消息、签名和公钥的证书。文献[15]应用变色龙哈希函数的概念来构建 WSN 的可信双向认证。基站向传感器节点发送公共数据和私钥,公共数据用于验证节点的合法性,私钥用于与其他节点的公钥建立互信密钥,互信密钥用于安全通信的会话密钥。可信接入身份可信不代表之后行为可信,如果每次交换重要数据时都进行可信认证,通信负载量和计算量都将增大。

已有研究方案在各方面还存在改进的空间,本文提出面向 WSN 的双向身份认证协议,旨在接入阶段采用可信认证方式验证节点可信情况再进行注册;然后在运行阶段对重要数据的传输过程进行保护,利用节点运行状态信息进行认证以进一步增强安全性,满足工业生产控制环境下对认证方案执行效率较高的要求。第 3 节详细描述了协议的工作过程;第 4 节基于协议证明所涉及的内容对串空间模型进行了简述;第 5 节采用串空间模型对所提协议的安全性进行了证明;最后对协议的性能进行了分析。

3 基于状态信息的双向身份认证协议

3.1 协议介绍

本文提出的面向 WSN 的双向身份认证协议是一种传感器节点和基站间的基于状态信息的双向身份认证。该协议首先在节点接入阶段基于可信网络连接(Trusted Network

Connection，TNC）进行平台可信情况的认证，以验证节点的可信情况并实现节点的加密注册。然后在运行阶段通过重要数据的双向认证过程对重要数据的传输过程进行保护，同时允许基站定时检测节点运行状态信息，及时监测节点的物理损坏，并利用节点运行状态信息进行认证，以进一步增强协议的安全性。此外，还引入了报警机制，该机制可以区分通信错误、节点的物理损坏以及攻击者攻击，对管理人员进行不同类别的报警。

协议主要由接入和运行两部分组成。在协议的接入部分，传感器节点将自身的 ID 信息（包括系统内命名、UUID 等）和工作状态信息（运行状态、节点运行电压等）等后续协议使用到的初始信息安全、完整地传输至基站。协议在完成接入部分后转入运行部分，运行部分由重要数据传输双向认证和定时更新认证组成，并引入报警机制对重要数据传输和传感器节点的物理状态等进行了全面的保护。

3.2　协议接入部分

协议在接入部分中使用 TNC 可信接入模型的结构对传感器节点的可信情况进行认证，可以应对不安全设备接入网络后对网络造成的安全威胁。具体认证过程如图 1 所示。

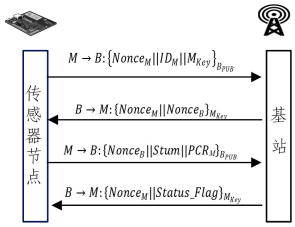


图 1　协议接入部分的认证过程

Fig. 1　Authentication process in access phase

步骤 1　传感器节点 M 向基站 B 发起接入请求。在发起请求的过程中，其向 B 指明本次请求发起方的随机数验证码 $Nonce_M$；同时携带自身的设备信息 ID_M 以便基站对 M 进行对应，ID_M 由系统内命名、传感器节点 UUID 信息等组成。为了保证数据不被窃听，信息同时包含 B 回复时所需要使用的加密密钥 M_{Key}，且上述所有信息采用 B 事先公开的公钥 B_{PUB} 加密[16]，如式(1)所示：

$$M \to B: \{Nonce_M \| ID_M \| M_{Key}\}_{B_{PUB}} \tag{1}$$

步骤 2　B 收到注册消息并成功解密后，判断消息结构是否合法，同时判断 ID_M 内的系统内命名是否符合该系统的命名规则，如两项均合法，则向 M 回复本次接入请求 B 的随机数验证码 $Nonce_B$。出于安全因素的考量，B 回复时须携带 M 提出的随机数验证码。以上信息将采用 M_{Key} 进行加密，如式(2)所示：

$$B \to M: \{Nonce_M \| Nonce_B\}_{M_{Key}} \tag{2}$$

步骤 3　M 认证 B 返回的随机数是否与之前指定的随机数相同。若不同，则终止接入；若相同，则进入可信信息的传输和验证阶段。M 调用可信度量值 PCR_M，并打包发送至 B。在发送数据的同时，携带 M 的状态信息 $Stum$，并且 B 提出随机数 $Nonce_B$ 以验证连接状态。上述信息由 B_{PUB} 进行加密，如式(3)所示：

$$M \to B: \{Nonce_B \| Stum \| PCR_M\}_{B_{PUB}} \tag{3}$$

步骤 4　B 判断完成后，将判断的结果反馈给 M。B 附加上 M 最初规定的随机数以验证本次接入。以上内容采用 M_{Key} 进行加密，如式(4)所示：

$$B \to M: = \{Nonce_M \| Status\_Flag\}_{M_{Key}} \tag{4}$$

3.3　协议运行部分

协议运行部分分为重要数据传输双向认证和定时更新认证两部分。在传感器节点传输普通数据时，协议只对其加以较少的保护；传感器节点监测到重要数据需要进行传输时，与基站间展开重要数据传输双向认证，用以保证重要数据安全地传递给基站。

基站还会定时对传感器节点发出定时更新认证，以监测节点的运行状态信息，进一步确保节点的安全性和合法性。

3.3.1　重要数据传输双向认证

重要数据传输双向认证部分为传感器节点监测到并判断数据是重要数据时，由传感器节点发起的传感器节点和基站间的双向身份认证，用以保障重要数据的安全送达。重要数据传输双向认证过程如图 2 所示。

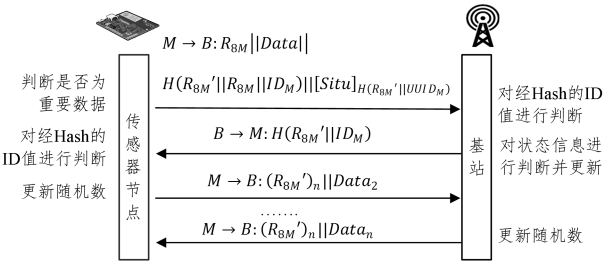


图 2　重要数据传输双向认证过程

Fig. 2　Authentication process in transmission process of important data phase

步骤 1　传感器节点 M 采集到数据后对其进行简单判断，如判断此数据为重要数据则继续步骤 2，否则进行一般数据传输过程。

步骤 2　M 产生一个 8 位新随机数 R_{8M}，将 R_{8M} 和 M 存储的 8 位历史随机数以及 ID_M 级联，并进行哈希。M 将内存储的 8 位历史随机数 R_{8M}' 和 $UUID_M$ 级联并进行哈希后作为密钥使用，AES-128 加密传感器节点自身的状态信息 $Stum$，将新产生的随机数和哈希后的 ID 信息以及加密后的状态信息级联组成双向身份认证请求信息，并将其发送给基站 B，如式(5)所示：

$$M \to B: R_{8M} \| Data \| H(R_{8M}' \| R_{8M} \| ID_M) \| [Situ]_{H(R_{8M}' \| UUID_M)} \tag{5}$$

步骤 3　B 根据收到消息的源地址，从数据库中提取该节点的 ID 信息、历史随机数和收到的随机数进行哈希，并将其与收到的哈希值进行比较。若未找到相应 ID 信息或比较的哈希值不同，则进行伪装传感器节点报警。如找到对应节点，再将该节点的历史随机数和该 ID 中的 UUID 级联并进行哈希运算，将得到的哈希值作为密钥，解密得到的加密状态信息，并将其与数据库中存储的状态信息进行比对。如果误差在可以接受的范围，则将该节点的历史随机数和 ID_M 级联后进行哈希运算回复给 M，并更新基站数据库中该节点的状态信息；否则进行节点物理损坏报警，如式(6)所示：

$$B\rightarrow M:H(R_{8M}'\parallel ID_M) \tag{6}$$

步骤 4 M 收到信息后，将历史随机数和自身 ID 信息级联后进行哈希，并将哈希值与收到的信息进行比对。如果相同，则双向身份认证成功，将历史随机数更新为新随机数，并在之后的 10 min(或自定义时间)不产生新的重要数据传输双向认证，同时在通信中附带新随机数的前两位来提示基站更新随机数；否则双向认证失败，进行伪装基站报警，并重新进行步骤 1。同样，如果在超过设定时间的间隔内没有收到正确的回复信息，则双向认证失败，重新进行步骤 1。连续 3 次双向认证失败则进行紧急报警，并进行闪烁、蜂鸣等物理报警。至此，双向认证过程结束，如式(7)所示：

$$M\rightarrow B:(R_{8M}')_n\parallel Data_2 \tag{7}$$

3.3.2 定时更新认证

在基站与传感器节点双向认证过程中加入传感器节点的状态信息能有效提高认证的安全性，同时也能掌握传感器节点的真实状态，防止节点出现物理损坏，增加传感器网络的可靠性。不过考虑到只有传感器节点检测到数据并判断其为重要数据时才会传回其状态信息，若只利用这一种方式检测并更新节点的状态信息，节点的物理安全性检测和基站数据库中状态信息的更新将完全依赖于传感器节点端重要数据的传输。如果传感器检测到重要数据的频率极低，则单纯利用上述双向认证方案检测并更新传感器节点的状态信息并不合适。为了保证基站中存储的传感器节点状态信息的时效性，并确保基站必须在节点发生物理损坏后尽快发现问题，采用基站对传感器节点的状态信息进行定时更新认证。

由于传感器节点对基站的状态信息更新是由基站发起的，为了尽可能减少通信并增强系统的鲁棒性，更新时基站与传感器的双向认证将完全基于单随机数，基站对传感器节点进行单向认证即可。基站与传感器节点的认证省去了随机数更新时的三次握手过程，同时消除了随机数更新失败产生带随机数更新请求的定时更新认证造成额外通信负担的可能。基站与传感器节点状态信息的定时更新认证过程如图 3 所示。

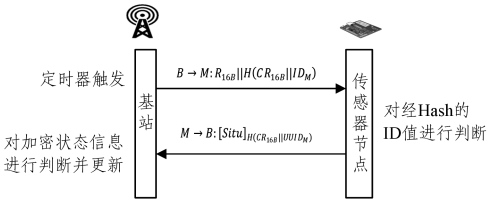


图 3 定时更新认证过程

Fig. 3 Authentication process in periodically detect phase

步骤 1 基站存储的某个节点的定时器触发传感器节点状态信息的定时更新请求，产生一个 16 位随机数 R_{16B}，并对该随机数进行特定的变换，得到变换后的随机数 CR_{16B}，CR_{16B} 和需要更新状态信息的传感器节点信息 ID_M 级联后进行哈希运算，得到加密后的传感器节点 ID 信息。将变换前的随机数和哈希后的 ID 信息级联后作为状态信息更新请求发送给传感器节点，如式(8)所示：

$$B\rightarrow M:R_{16B}\parallel H(CR_{16B}\parallel ID_M) \tag{8}$$

步骤 2 传感器节点收到信息后对随机数进行特定的变换，然后将变换后的随机数和自身 ID 级联后进行哈希运算，最后将得到的哈希值与信息中的 $H(CR_{16B}\parallel ID_M)$ 进行比对。如果结果不同，则进行伪装基站报警；若相同，则对变换后的随机数和 $UUID_M$ 级联进行哈希，将得到的哈希值作为密钥，使用 AES-128 加密自身的状态信息，并将加密的状态信息发送给基站，如式(9)所示：

$$M\rightarrow B:[Situ]_{H(CR_{16B}\parallel UUID_M)} \tag{9}$$

在基站与传感器节点定时更新的认证过程中，协议并未使用储存在基站和传感器节点中的历史随机数。尽量减少历史随机数的更新和使用可以降低传感器网络的总能耗，同时使历史随机数更难被攻击者获取，从而提高了重要数据传输双向认证协议的安全性。

3.4 报警机制

传感器网络中的节点经常会布置在野外的场景中，节点本身容易自然损坏或被他人恶意攻击，利用本文提出的双向身份认证协议可以在认证的同时对节点的运行状态进行判断并发送异常报警。报警分为以下 4 类：

1)伪装传感器节点报警。该报警发生在传感器提出重要数据传输双向认证和传感器节点应答定时更新认证阶段，伪装传感器节点试图与基站通信，基站产生报警。

2)伪装基站报警。该报警发生在基站应答重要数据传输双向认证和基站提出定时更新认证阶段，伪装基站试图与传感器节点通信，传感器节点向基站发送报警信息，真基站收到信息并产生报警。

3)传感器节点损坏报警。该报警表示传感器节点出现故障，且多为物理故障。该报警一般发生在重要数据传输双向认证和定时更新认证过程中，当基站收到的传感器节点加密状态信息与数据库内数据误差较大时触发报警。

4)紧急报警。该报警表示传感器节点始终无法与基站进行重要数据传输双向认证或定时更新认证。

4 串空间模型

串空间模型拥有比其他形式化分析方法更加简洁、高效的模型，可以以尽量简单的方法对协议的安全性进行形式化分析，有助于分析者深入了解协议需要的假设，给出更可信且有帮助的证明与论据。本文选择使用串空间模型对协议的机密性及认证性进行分析。

构造串空间的方法如下：

1)结点的集合记为 N，单个结点记为二元组$\langle s,i\rangle$，其中 s 为结点所处串 i 为该结点的序数。

2)当 $n=\langle s,i\rangle\in N$ 时，$index(n)=i$ 且 $strand(n)=s$。定义 $term(n)$ 为 s 中第 i 个结点的符号项，即$(tr(s))_i$；$uns\_term(n)$ 为 s 中第 i 个结点的无符号项，即$((tr(n))_i)_2$。

3)若 $n_1,n_2\in N$，则定义 $n_1\rightarrow n_2$ 为 $term(n_1)=+a$ 且 $term(n_2)=-a$，即 n_1 发送的消息由 n_2 接收。

4)若 $n_1,n_2\in N$，则定义 $n_1\Rightarrow n_2$ 为 $index(n_2)=index(n_1)+1$，即 n_1 是 n_2 的直接因果前驱。

5)一个无符号项 t 发生在 $n\in N$，当且仅当 $t\in uns\_term(n)$。

6)一个无符号项 t 起源于 $n\in N$，当且仅当 $t\in uns_term(n)$且为加号，对于所有结点 $n'\Rightarrow n$ 且 $t\notin uns\_term(n')$。

7)一个无符号项 t 唯一起源于 $n\in N$,当且仅当 t 起源于唯一的结点 $n\in N$。

8)一个无符号项集 $I\subseteq A$ 的入口点为 n,当且仅当 $t\in I$ 起源于 n,且对于所有结点,$term(n')\notin I$。

9)N 加上两种边 $n_1\rightarrow n_2$ 和 $n_1\Rightarrow n_2$ 组成有向图$\langle N,(\rightarrow\cup\Rightarrow)\rangle$。

簇是上述有向图$\langle N,(\rightarrow\cup\Rightarrow)\rangle$的有向子图,且满足下面的定义:1)$C$ 是无环的;2)C 是有限的;3)若 $C\in N_C$ 且 $term(n)$为减号,则有唯一的结点 n_1 满足 $n_1\rightarrow_C n_2$;4)若 $C\in N_C$ 且 $n_1\Rightarrow n_2$,则 $n_1\Rightarrow_C n_2$。

一个结点 n 在簇 C 中记作 $n\in C$,一个串 s 的所有结点都在簇 C 中,则认为串 s 在簇 C 中,记作 $s\in C$。串 s 的高度记作 $C\text{-}Height(s)$,其值为$\langle s,i\rangle\in C$ 中 i 的最大取值。

定理 1　设 S 是一个边的集合,$S\subset(\rightarrow\cup\Rightarrow)$,定义二元关系 $n_1<n_2$ 为 $n_1\rightarrow n_2$ 或 $n_1\Rightarrow n_2$,此关系是一个闭包的传递关系;定义二元关系 $n_1\leqslant n_2$ 是一个偏序关系,即拥有自反性、反对称性和传递性。

引理 1　$\leqslant$是一种因果次序,只有 n_2 的出现由 n_1 造成时,才会有 $n_1\leqslant n_2$。簇 C 中任意非空结点的子集都有$\leqslant_C$ 最小元。

引理 2　若 n 是$\leqslant_C$ 极小元,则 n 前符号为加号。

引理 3　若 $t\in A$,且 $n\in C$ 是集合$\{m\in C: t\sqsubset term(m)\}$中的$\leqslant_C$ 极小元,则 t 起源于结点 n。

引理 4　若 $t\in A$,且 $n\in C$ 是集合 $I=\{t': t\leqslant t'\}$的入口点,则 t 发生在节点 n。

在集合 A 中定义:1)$T\subseteq A$ 表示正文集合;2)$K\subseteq A$ 表示密钥集合。以上两集合是不相交的。

给出以下 4 条定理,定理的证明详见文献[17]。

定理 2　对于所有 $h\in I, g\in A$,若 I 满足:1)$hg, gh\in I$;2)$\{h\}_K\in I, K\in ek$,记为 $I_K(h)$,对于 $S\in A, h\in S$,有 $I_K[h]\in I_K[S]$。

定理 3　若$\{h\}_{k_n}\in I_K(S)$,则 $k_n\in k$。

定理 4　若 $k\notin k_p$,则$\{h\}_{k_n}, k_n\in k$ 的项不可能起源于攻击者结点。

定理 5　若 h 对于攻击者是机密的,则对于特定随机数 R 有:包含 $H(R\parallel h)$的项不可能起源于攻击者结点。

攻击者能力主要由两方面因素描述:攻击者所掌握的密钥集;攻击者根据自己所获得的消息而产生新消息的能力[18]。

由上述能力可以扩展得到以下行为。

攻击者的原子行为:

M.(正文消息):$\langle+t\rangle$,其中 $t\in T$;

F.(截获):$\langle-g\rangle$;

T.(重发):$\langle-g,-g,+g\rangle$;

C.(连接):$\langle-g,-h,+gh\rangle$;

S.(分割):$\langle-gh,+g+h\rangle$;

K.(密钥):$\langle+K\rangle, K\in K_p$;

E.(加密):$\langle-K,-h+\{h\}_K\rangle$;

D.(解密):$\langle-\{h\}_k,-K^{-1}+h\rangle$;

H.(hash 运算):$\langle-h,+H(g)\rangle$。

攻击者可自由组合原子行为,以生成新的消息。

5　协议安全性分析

协议接入部分的安全性已经在前期的研究成果中进行了论证[19],本文只对协议运行部分的重要数据传输双向认证和定时更新认证进行安全性分析。

5.1　重要数据传输双向认证

定义如下 3 种类型串。

1)攻击者串:$s\in P$。

2)发起者串:$s\in Init[R_{8M}, R_{8M}', Data, ID_M, UUID_M, Situ]$;迹为$(+\{R_{8M}\parallel Data\parallel H(R_{8M}'\parallel R_{8M}\parallel ID_M)\parallel[Situ]_{H(R_{8M}'\parallel UUID_M)}\},-\{H(R_{8M}'\parallel ID_M)\},+\{(R_{8M}')_n\parallel Data_2\})$。

3)响应者串:$s\in Resp[R_{8M}, R_{8M}', Data, ID_M, UUID_M, Situ]$;迹为$(-\{R_{8M}\parallel Data\parallel H(R_{8M}'\parallel R_{8M}\parallel ID_M)\parallel[Situ]_{H(R_{8M}'\parallel UUID_M)}\},+\{H(R_{8M}'\parallel ID_M)\},-\{(R_{8M}')_n\parallel Data_2\})$。

5.1.1　机密性分析

设 $k_1=H(R_{8M}'\parallel UUID_M)$,显然 k_1 并未以明文形式出现在簇 C 中。

命题 1　若 Σ 为协议重要数据双向认证部分的串空间,C 为串空间中的一个簇,包含发起者的串 $s\in Init[R_{8M}, R_{8M}', Data_1, ID_M, UUID_M, Situ]$,且 $k=(K/k_1)$,则对串 s 上的每一个结点 $m\in s, term(m)\notin I_k(k_1)$。

考虑到攻击者行为 C,S 和 H,k_1 可由 $UUID_M$ 得到,须证明 m 不能为 $I_k(UUID_M)$的入口点。

证明:(反证法)若 m 为 $I_k(UUID_M)$的入口点,则 m 符号为加号,且 $UUID_M$ 一定包含于 $uns\_term(m)$。

1)假设 $m=\langle s,1\rangle$,显然意味着 $UUID_M\in H(R_{8M}'\parallel R_{8M}\parallel ID_M)$,或者 $UUID_M\in[Situ]_{H(R_{8M}'\parallel UUID_M)}$,或者 $[Situ]_{H(R_{8M}'\parallel UUID_M)}\in I_k(UUID_M)$。由 Hash 的不可逆性可证 $UUID_M\notin H(R_{8M}'\parallel R_{8M}\parallel ID_M)$,与已知矛盾;对任意项 h,若 $[h]_{H(R_{8M}'\parallel UUID_M)}\in I_k(UUID_M)$,由定理 3 可得 $k_1\in k$,这与已知 $k=(K/k_1)$矛盾。同时,由 Hash 的不可逆性可证 $UUID_M\in[Situ]_{H(R_{8M}'\parallel UUID_M)}$,与已知矛盾。

综上可得,$m\neq\langle s,1\rangle$。

2)假设 $m=\langle s,3\rangle$,由 R_{8M}'和 $Data_2$ 无法得到 $UUID_M$,故 $m\neq\langle s,3\rangle$。

综上所述,命题 1 成立。

命题 2　若 Σ 为协议重要数据双向认证部分的串空间,C 为串空间中的一个簇,包含应答者的串 $s\in Resp[R_{8M}, R_{8M}', Data_1, ID_M, UUID_M, Situ]$,且 $k=(K/k_1)$,则对串 s 上每一个结点 $m\in s, term(m)\notin I_K(k_1)$。

证明:假设 $m=\langle s,2\rangle$,显然意味着 $ID_M\sqsubset H(R_{8M}'\parallel ID_M)$。由 Hash 的不可逆性可证 $ID_M\not\sqsubset H(R_{8M}'\parallel ID_M)$,与已知矛盾。故 $m\neq\langle s,2\rangle$。

综上所述,命题 2 成立。

命题 3　若 Σ 为协议重要数据双向认证部分的串空间,C 为串空间中的一个簇,包含发起者的串 $s\in Init[R_{8M}, R_{8M}', Data_1, ID_M, UUID_M, Situ]$和应答者的串 $s\in Resp[R_{8M}, R_{8M}',$

$Data_1$,ID_M,$UUID_M$,$Situ$],且 $k=(K/k_1)$,则对簇 C 上每一个结点 $m\in C$,$term(m)\notin I_K(k_1)$。

证明:由命题 1 以及命题 2 可证。

考虑到协议形式的一致性,同理可对协议的其他部分进行证明。同时可得命题 4。

命题 4 ID_M 及 $UUID_M$ 对于攻击者是机密的。

5.1.2 认证性分析

命题 5 结点 m 对于任意随机数 R 有$[Situ]_{H(R\parallel UUID_M)}$,$[Situ]_{H(R\parallel UUID_M)}$起源于结点 m,则 m 不可能为攻击者结点。

证明:由定理 4 和命题 1 可证。

命题 6 结点 m 对于特定随机数 R 有 $H(R\parallel ID_M)$,$H(R\parallel ID_M)$起源于结点 m,则 m 不可能为攻击者结点。

证明:由定理 5 和命题 1 可证。

1)B 认证 M

命题 7 若 Σ 为协议重要数据双向认证部分的串空间,C 为串空间中的一个簇,$k_1\notin k_p$,若存在响应者的串 $s\in Resp[R_{8M},R_{8M}',Data_1,ID_M,UUID_M,Situ]$,$C\text{-}Height(s)=3$,则 C 中必然存在 $s_{init}\in Init[R_{8M},R_{8M}',Data_1,ID_M,UUID_M,Situ]$且高度至少为 1;并且由 R_{8M}唯一起源于发起者串可知,发起者串是唯一的。

证明:由命题 4 可得,$[Situ]_{H(R_{8M}'\parallel UUID_M)}$起源于$\langle s,1\rangle$。

2)M 认证 B

命题 8 若 Σ 为协议重要数据双向认证部分的串空间,C 为串空间中的一个簇,$k_1\notin k_p$,若存在发起者的串 $s\in Init[R_{8M},R_{8M}',Data_1,ID_M,UUID_M,Situ]$,$C\text{-}Height(s)=3$,则 C 中必然存在 $s_{Resp}\in Resp[R_{8M},R_{8M}',Data_1,ID_M,UUID_M,Situ]$且高度至少为 2;并且由 R_{8M}'是由发起者和响应者共同确定的可知,响应者串是唯一的。

证明:由命题 6 可得,$H(R_{8M}'\parallel ID_M)$起源于$\langle s,2\rangle$。

由命题 7 和命题 8 可得,发送者和响应者可以相互认证。

5.2 定时更新认证

定义如下 3 种类型串。

1)攻击者串:$s\in P$。

2)发起者串:$s\in Init[R_{16B},CR_{16B},ID_M,UUID_M,Situ]$;迹为$(+\{R_{16B}\parallel H(CR_{16B}\parallel ID_M)\},-\{[Situ]_{H(CR_{16B}\parallel UUID_M)}\})$。

3)响应者串:$s\in Resp[R_{16B},CR_{16B},ID_M,UUID_M,Situ]$;迹为$(-\{R_{16B}\parallel H(CR_{16B}\parallel ID_M)\},+\{[Situ]_{H(CR_{16B}\parallel UUID_M)}\})$。

5.2.1 机密性分析

设 $k_2=H(CR_{16B}\parallel UUID_M)$。

命题 9 若 Σ 为协议定时更新认证部分的串空间,C 为串空间中的一个簇,包含发起者的串 $s\in Init[R_{16B},CR_{16B},ID_M,UUID_M,Situ]$和响应者的串 $s\in Resp[R_{16B},CR_{16B},ID_M,UUID_M,Situ]$,且 $k=(K/k_2)$,则对簇 C 上每一个结点 $m\in C$,$term(m)\notin I_K(k_2)$。

证明同命题 3 的证明。

5.2.2 认证性分析

命题 10 若 Σ 为协议定时更新认证部分的串空间,C 为串空间中的一个簇,$k_1\notin k_p$,若存在发送者的串 $s\in Init[R_{16B},CR_{16B},ID_M,UUID_M,Situ]$,$C\text{-}Height(s)=2$,则 C 中必然存在 $s_{Resp}\in Resp[R_{16B},CR_{16B},ID_M,UUID_M,Situ]$且高度至少为 2,并由 $Situ$ 是唯一起源于响应者的可知,响应者串是唯一的。

证明:由命题 5 可得$[Situ]_{H(CR_{16B}\parallel UUID_M)}$起源于$\langle s,2\rangle$。

由命题 10 可得,定时更新认证可完成基站对传感器节点的认证。

6 协议性能分析

6.1 提高实体的安全性

本协议在接入部分中使用 TNC 可信接入结构进行传感器节点可信情况的认证,通过对感知节点进行信任度量,提高了节点自身的安全性,可以有效地抵御内部节点攻击。本协议对 Sinkhole 攻击、Sybil 攻击等有很好的预防作用。

6.2 降低认证过程的通信量

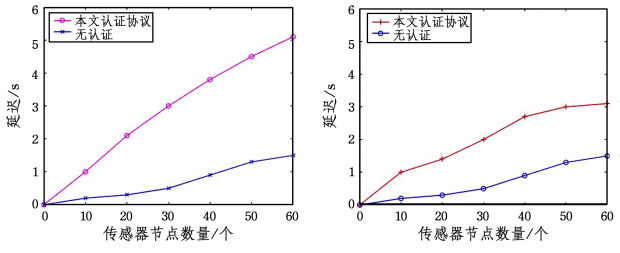
本协议的重要数据传输双向认证部分减少了认证过程中的通信量。利用随机数更新的方式,协议每次双向认证至少比文献[9]的方案减少两字节的通信量。同时,ZigBee 中传感器节点接收消息时会使用向父节点轮询的方式,传感器节点连续两次接收消息往往会产生一定间隔,难以保证实时性。因此,本协议在降低通信数据量的同时,对 ZigBee 网络体现了更好的适应性。

6.3 引入报警消息,增强排障能力

本协议引入了报警消息,通过认证过程检测传感器节点的运行状态等。在无线传感器网络中,网络环境复杂且节点容易出现物理损坏,及时检测到网络或节点硬软件的错误,并对节点的自然损坏错误和攻击者攻击进行一定判别,可以防止将攻击者的攻击误认为节点硬软件或传输错误,避免给予攻击者更多的攻击机会。同时,针对不同种类的错误,可以显示不同的报警信息,使管理人员可以更有针对性地排除节点故障。

6.4 实验验证

实验硬件环境:传感器节点为 arduino pro mini 加 ZigBee 透传模块;基站为树莓派 3 加协调器。多个传感器节点同时向基站发起接入认证和重要数据传输双向认证并发送数据,基站接收到数据的延迟实验结果如图 4 所示。



(a)协议接入部分认证的延时 (b)重要数据传输双向认证的延时

图 4 基站接收到数据的延迟实验结果

Fig. 4 Delay experimental results of data received by bases

根据图 4(a)和图 4(b)的实验结果可知,本文设计的双向身份认证协议在提供较好安全性的情况下,发送数据的延时增加,但增加的延时在可接受的范围内,网络可扩展性好。

结束语 本文设计的面向无线传感器网络的双向身份认

证协议由接入和运行两阶段组成。在接入阶段，基站可以对传感器节点进行可信评估，确认节点本身安全可靠后实现节点的加密注册，能够加强网络接入安全并有效防御来自节点系统内部的攻击。运行阶段通过重要数据双向认证过程对重要数据的传输过程进行保护，有效抵御重放攻击；同时，基站定时检测节点的运行状态信息，以监测节点的异常情况，对物理损坏和攻击进行报警。协议提供了较好的安全性和运行效率，具有较好的应用价值。本协议在能耗方面和定时更新认证时间间隔方面还具有较大的改进空间，下一步将重点在这两方面进行深入论证。

参 考 文 献

[1] QIAN Z H, WANG Y J. Internet of Things-oriented Wireless Sensor Networks Review[J]. Journal of Electronics & Information Technology, 2013, 35(1): 215-227. (in Chinese)
钱志鸿，王义君. 面向物联网的无线传感器网络综述[J]. 电子与信息学报，2013，35(1)：215-227.

[2] BOUBICHE D E, PATHAN A S K, LLORET J, et al. Advanced industrial wireless sensor networks and intelligent iot[J]. IEEE Communications Magazine, 2018, 56(2): 14-15.

[3] STOJKOSKA B L R, TRIVODALIEV K V. A review of Internet of Things for smart home: Challenges and solutions[J]. Journal of Cleaner Production, 2017, 140: 1454-1464.

[4] PAWAR M, AGARWAL J. A literature survey on security issues of WSN and different types of attacks in network[J]. Indian Journal of Computer Science and Engineering, 2017, 8(2): 80-83.

[5] BAUER K, LEE H. A distributed authentication scheme for a wireless sensing system [J]. ACM Transactions on Information and System Security, 2008, 11(3): 1-35.

[6] AXELM, DARTIESB, BARILJ L. Blockchain based trust & authentication for decentralized sensor networks[J]. arXiv: 1706.01730, 2017.

[7] KANG B Y, WANG J Q, SHAO D Y, et al. A Secure Authentication and Key Agreement Protocol for Heterogeneous Ad Hoc Wireless Sensor Networks [J]. Netinfo Security, 2018, 18(1): 23-30. (in Chinese)
亢保元，王佳强，邵栋阳，等. 一种适用于异构 Ad Hoc 无线传感器网络的身份认证与密钥共识协议[J]. 信息网络安全，2018，18(1)：23-30.

[8] TAI W L, CHANG Y F, LI W H. An IoT Notionbased Authent icat ion a nd Key Ag reement Scheme Ensur ingUser Anonymit y for Heterogeneous Ad Hoc Wireless Sensor Networks[J]. Journal of Information Security and Applications, 2017, 34(2): 133-141.

[9] HAMMI M T, LIVOLANT E, BELLOT P, et al. A lightweight mutual authentication protocol for the IoT[C]// Proceedings of International Conference on Mobile and Wireless Technology. Singapore: Springer, 2017: 3-12.

[10] HAMMI M T, LIVOLANT E, BELLOT P, et al. A lightweight IoT security protocol[C]// Proceedings of Cyber Security in Networking Conference (CSNet). Rio de Janeiro: IEEE Press, 2017: 1-8.

[11] WANG Y. Reserch on Secure Authentication Scheme For Resouce-constrained Environments[D]. Taiyuan: Taiyuan University of Technology, 2016. (in Chinese)
王颖. 资源受限环境安全身份认证方案研究[D]. 太原：太原理工大学，2016.

[12] WANG C D, BAI Y, MO X L, et al. Identity of Two-way Authentication Mechanism Research Based on the Internet of Things[J]. Acta Scientiarum Naturalium Universitatis Nankaiensis, 2016, 49(2): 22-28. (in Chinese)
王春东，白仪，莫秀良，等. 基于物联网的身份双向认证机制研究[J]. 南开大学学报(自然科学版)，2016，49(2)：22-28.

[13] LIU T, XIONG Y, HUANG W C, et al. Node behavior and identity-based trusted authentication in wireless sensor networks [J]. Journal of Computer Applications, 2013, 33(7): 1842-1845, 1857. (in Chinese)
刘涛，熊焰，黄文超，等. 无线传感器网络中基于节点行为和身份的可信认证[J]. 计算机应用，2013，33(7)：1842-1845，1857.

[14] FOUCHAL H, BIESA J, ROMERO E, et al. A Security Scheme for Wireless Sensor Networks[C]// Proceedings of Global Communications Conference (GLOBECOM). Washington: IEEE Press, 2016: 1-5.

[15] YEIN A D, LIN C H, HSIEH W S. A secure mutual trust scheme for wireless sensor networks[C]// Proceedings of Industrial Electronics (ISIE), 2017 IEEE 26th International Symposium. Edinburgh: IEEE Press, 2017: 1369-1375.

[16] 刘静，刁子朋，庄俊玺，等. 一种软件定义网络中安全的可信接入方法：中国，CN105933245A[P]. 2016-09-07.

[17] THAYER F J, HERZOG J C, GUTTMAN J D. Strand Spaces: Proving Security Protocols Correct[J]. Journal of Computer Security, 1999, 7(2/3): 191-230.

[18] XU F, GAO X C, HUANG H. Design and Correctness Proof of a Security Protocol for Mobile Computing[J]. Compuer Science, 2008, 35(11): 74-77. (in Chinese)
许峰，高晓春，黄皓. 基于 Strand Space 的移动计算安全协议设计与正确性证明[J]. 计算机科学，2008，35(11)：74-77.

[19] LIU J, LAI Y X, DIAO Z P, et al. A trusted access method in software-defined network[J]. Simulation Modelling Practice and Theory, 2017, 74(5): 28-45.