文章编号:1673-9469(2021)01-0092-07 DOI: 10.3969/j.issn.1673-9469.2021.01.014

基于LoRaWAN协议的双向认证接入机制的研究

马早霞,李 磊*,刘 心
(河北工程大学 信息与电气工程学院,河北 邯郸 056038)

摘要:针对LoRaWAN中终端设备与网络服务器建立连接过程中存在的安全漏洞做出改进。提出一种基于LoRaWAN协议的安全模型,通过终端与服务器之间双向认证机制加强终端与服务器的身份认证的安全性,防止第三方设备窃听,又将身份认证规则进行周期性更新,在防止重放攻击,加强链路安全性的同时,尽可能地降低对功耗的影响。仿真结果表明,该机制对LoRaWAN协议终端认证过程的安全性随着更新周期的缩短而更大,该机制的双方认证过程的能耗随着周期的缩短而增大,但对整体数据传输阶段的能耗和数据传输阶段的接收延迟影响不明显,其中数据传输阶段的接受延迟增加不足7%。

关键词:LoRaWAN;帧重构;双向认证;安全性;安全等级
中图分类号:TN919.2 **文献标识码**:A

Research on Bidirectional Authentication Mechanism Based on LoRaWAN Protocol

MA Zaoxia, LI Lei*, LIU Xin
(School of Information and Electrical Engineering, Hebei University of Engineering, Handan, Hebei 056038, China)

Abstract: Improvements are made to the security issue in the connection process between LoRawan terminal equipment and network server. A security model is proposed based on LoRaWAN protocol which, through the two-way authentication mechanism between the terminal and server, strengthens the security of terminal and server authentication to prevent the third-party equipment eavesdropping. This model updates regularly the authentication rules, prevents the replay attack, strengthens the link safety and at the same time, reduces the impact on the power consumption as far as possible. Simulation results show that that the security of this mechanism for the LoRaWAN protocol terminal authentication process becomes greater with the shortening of the update cycle. The energy consumption of the authentication process of the two parties of this mechanism increases with the shortening of the cycle. But it doesn't have an obvious impact on the energy consumption of the overall data transmission phase and the reception delay of the data transmission phase. The acceptance delay during the data transmission phase increases by less than 7%.

Key words: LoRaWAN; frame reconstruction; bidirectional authentication; security; safety level

物联网产业的飞速发展,对通信技术提出了更高的要求[1-3]。在此背景下,低功耗广域网LPWAN (low power wide area network) 因其能耗小、通信范围广等特点得以广泛应用。LoRa技术作为LPWAN中应用最为广泛的通信技术之一具有低功耗、远距离、广范围的特点,发展相对较快、较为成熟。智慧物联网依托LPWAN,容易陷入隐私泄漏和其他安全危机。数据传输过程是整个物联网信息传输最薄弱的环节,特别是在LoRa无线网络中,由于带宽、数据速率和包大小等受限,数据链

收稿日期:2020-11-11
基金项目:国家自然科学基金资助项目(61440001);教育部新世纪优秀人才支持计划项目(NCET-13-0770);河北省高等学校高层次人才科学研究项目(GCC2014062)
作者简介:马早霞(1995-),女,河北石家庄人,硕士研究生,研究方向为LoRa通信协议。
*通讯作者:李磊(1987-),男,河北邯郸人,博士,讲师,研究方向为远程通信协议优化。

路特别容易受到攻击[4]。LoRaWAN 是基于 LoRa 的上层协议,定义了整个系统的架构和运行过程。LoRaWAN 使用对称密钥加密(AES-128bits)进行加密/解密和 MAC 操作,虽在一定程度上保护网络中传输的数据有效负载,但仍面临数据加密安全度不高,传输链路易被监听等问题[4-5]。

LoRa 广域网的安全性受到广泛关注,文献[6]指出了通信各方由于同步问题易受攻击的漏洞。文献[7]首次对 LoRaWAN 协议的安全性进行研究,主要分析了 LoRaWAN v1.0 和 LoRaWAN v1.1 的密钥交换部分,利用工具 Scyther 提出了一种针对 v1.1 的安全协议模型,定义了基于物理层的 LPWAN 网络的结构和运行。但是该文献提出的模型只是对协议进行安全性检查,并不能解决 LoRaWAN 协议易受攻击和重放的问题。文献[8]针对 MAC 层安全机制提出了一种密钥自动生成机制。文献[9]在此基础上提出一种密钥衍生机制,该机制无差别地对连接请求过程进行加密,并没有考虑对功耗的增加。文献[10]提出一种低功耗的端对端的密钥生成机制。文献[11]展示了密钥管理、通信和网络连接阶段的几个漏洞,讨论了 LoRaWAN v1.0 的一些漏洞。文献[12]指出,在空中激活过程中,终端向服务器发送的连接请求加密等级不高。但是这个问题已经在 LoRaWAN 新版本协议中做出了改进。

本文旨在分析 LoRaWAN 协议传输链路的安全性,在有针对性地解决了重放攻击问题的基础之上,提出了一种基于 LoRaWAN 协议的安全入网机制,保证传输安全性的同时尽可能地降低功耗。

1　LoRaWAN 帧重构机制

1.1　LoRa 网络与 LoRaWAN 协议基本原理

图 1 为 LoRa 传感网络概念架构图。LoRa 网络是一种星型拓扑网络,终端采集数据后上传至服务器,且终端与服务器之间均可以进行双向通信。一个 LoRa 终端可与一个或多个网关相连,网关只对数据进行转发处理[13]。

LoRaWAN 作为 LoRa 网络的 MAC 层协议,定义了 6 种消息类型,如表 1 所示。

服务器根据收到的消息类型判断是否需要进行应答。当发送的数据帧为 confirmed 类型的消息时,服务器要进行答复(即 ACK 要进行重置)。其他消息类型根据需求可不进行答复。本文所做研究针对 LoRaWAN 数据帧 join request 类型进行重构,即对入网请求帧进行重构。

图 1　LoRa 智慧网络概念图

Fig. 1　LoRa Intelligent Network Concept

表 1　LoRaWAN 消息类型

Tab. 1　The type of LoRaWAN message

Mtype	描述
000	Join Request
001	Join Accept
010	Unconfirmed Data Up
011	Unconfirmed Data Down
100	Confirmed Data Up
101	Confirmed Data Down
110	RFU
111	Proprietary

1.2　双向认证机制

双向认证机制是基于终端与网关之间的交互,建立安全的数据链路,防止重放攻击的有效方法。服务器对终端发送的数据帧中 MAC 地址和 IP 地址等进行函数提取以及合法性检测,然后被请求方根据请求方身份信息生成编码重构序列,请求方根据编码重构序列进行帧重构,然后随机生成反向编码重构序列一同发送给被请求方,由被请求方再次验证身份。

图 2 所示为 LoRa 终端与服务器之间双向认证的过程。终端要按照服务器定义的规则对数据帧进行重构,并实现重构后数据帧的网络通信传输。在数据链路建立时,首先由终端发起连接请求,服务器接收到连接请求后获取数据帧的头部信息,判断是否需要进行重构,若需要重构则由服务器向终端发送反向连接请求。终端收到服务器的反向连接请求后根据编码重构序列进行重构,然后第二次向服务器发送符合重构规则的连接请求。服务器接收重构后的连接请求判断是否符合

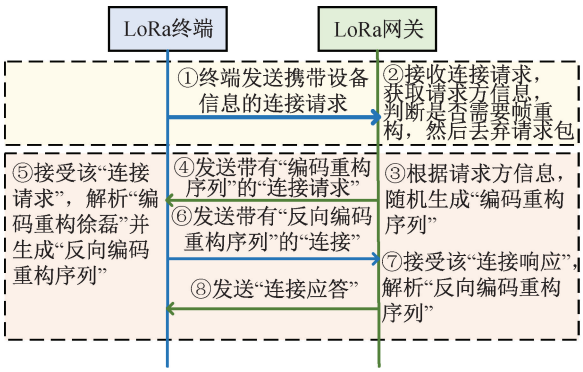

图2 双向认证过程

Fig. 2 Two-way authentication process

规则,若符合规则,则同意连接,至此通信链路建立成功。

该机制只有在数据链路建立的时候才启动五次握手认证。就单次传输来说数据链路的建立和释放的能耗是不可避免的。安全机制的消耗增加主要体现在以下几个方面增加:(1)每次随机生成重构因子的消耗;(2)五次握手机制的消耗;(3)数据链路释放之后,再次建立时的消耗。该机制根据终端发送的请求数据帧的头部信息生成的编码重构序列,再利用编码重构序列完成后续重构规则的通知,在重构规则协商过程中对请求方的设备合法性进行检测,通过双方设备合法性检测的流程实现防止第三方窃听的效果。

图3是进行帧重构规则通知的数据帧结构,Preamble是帧的头部,其中编码了同步字来实现数据收发两方的同步。PHDR为物理头,PHDE_CRC为头校验。MHDR是MAC层帧头,其中MType是消息类型,MIC是4字节校验[14]。MACPayload部分为数据帧的重构部分,其中密钥指示位代表密钥指针指向的位置,通过此指针可以确定相同的密钥。16字节数据用于存放验证信息。编码重构序列由其余三个参数共同确定。

1.3 认证规则的周期性更新

考虑到LoRaWAN通信过程的系统开销,若每次终端节点接入都需要进行双向认证,则会大大增加能耗,所以在这里利用节点的安全性等级来确定认证规则的更新周期。即规定,在一个周期内,终端节点只需在首次连接时进行双向认证,其余连接只需进行网关与终端的单向认证即可。所以节点的安全等级与重构因子的更新周期息息相关,随着信息安全性等级越高,重构因子的更新周期应该更短,才能保证数据的安全性。在本文中,我们按照终端节点所采集信息的隐私程度,将终端节点分为五个安全等级,对应认证规则的5个更新周期。$T=1$时,只需进行一次安全数据链路的建立,一旦数据链路建立,在之后的数据传输中将不再进行终端身份的认证,直到终端身份失效。

在网络服务器端进行重构规则的周期性更新,给定重构因子一个更新周期,在周期内的重构因子不进行变化,而是在达到更新周期后对重构规则进行函数性变化。即不用每次建立数据链路都要生成随机的重构因子,而是在一定时间内使用同一个重构因子,以此来减少系统开销。

为解决重构规则更新时网关和终端双方使用规则的不同步问题,设置一个缓冲区来保存原来的重构规则和已经发送过申请的终端地址合法性。若收到的携带重构因子的申请不符合重构规则但其设备身份是合法的,则该终端可能是按照上一个周期的重构规则进行帧重构的。

该机制的周期性处理流程见图4。

2 仿真及结果对比

2.1 设备合法性检测

为进一步提供通信链路安全性,该机制对双向认证接入方法的重构规则进行周期性更新。为解决重构规则更新时服务器和终端双方使用规则的不同步问题,在网关中设置一个白名单来保存已经发送过申请的终端的地址,白名单随着重构规则进行周期性更新,若发送请求的终端数据帧地址已在白名单中保存,则可以判断该终端在本周期内已经成功建立过连接,则可进一步判断其请求帧是否符合重构规则。若请求帧符合重构规则,则服务器同意其连接请求;若不符合重构规

Preamble	PHDR	PHDR_CRC	PHYPayload									CRC
			MHDR			MACPayload					MIC	
1B	2-255B	16b	Mtype	RFU	Major	密钥指示	隔位指示	起始字节	有效位	验证数据	4B	2B
			3b	3b	2b	8B	1B	2B	2B	16B		

图3 帧重构规则通知报文

Fig. 3 The frame reconstruction rules inform the message

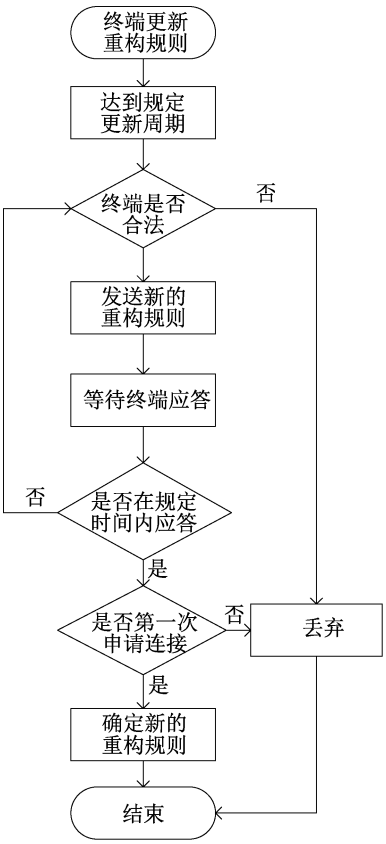

图 4　双向认证机制路程图

Fig. 4　Two-way authentication mechanism road map

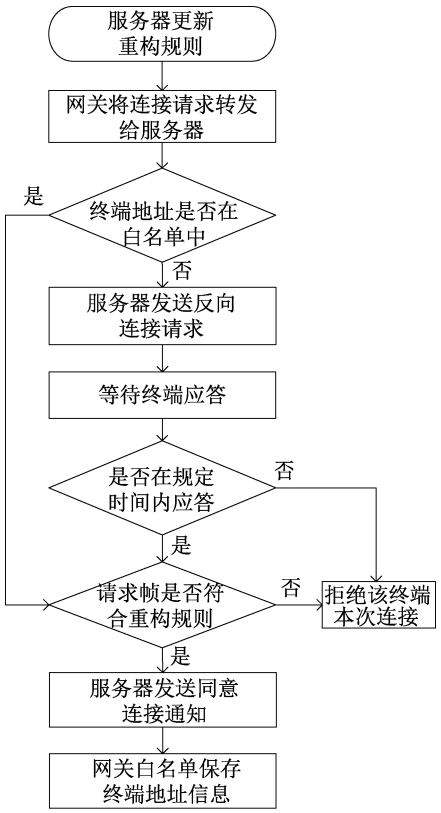

图 5　服务器端设备合法性检测流程图

Fig. 5　Flow chart of server side device legality detection

则,则拒绝该终端本次连接请求。上述流程可见图 5。图 6 所示为终端侧设备合法性检测流程图,是终端发送连接请求后等待接收服务器的响应,并根据服务器响应进行数据帧重构或数据传输,若收到服务器发送的携带编码重构序列的反向连接请求,则对自身请求帧进行响应重构,若接收到服务器的同意连接通知,则可进行数据传输。

2.2　安全性能验证

所有终端的连接请求,经 NS(Network Servers)转发给 JS(Join Servers)处理。DevNonce 是一个由终端设备在请求连接时产生,在一定范围内的随机数[16]。已产生的 DevNonce 由 JS 设立的固定大小的数据池保存。在 JS 处理连接请求过程中,JS 若判断 DevNonce 是个不在数据池内的随机数,则同意连接请求,若与数据池内的数据匹配成功,则对连接请求予以丢弃。因为服务器可连接的终端设备是有限的,且一旦双方建立连接,一般情况下,之后的连接将不再进行身份认证。所以服务器不会删除数据池中保存的 DevNonce。若终端需要重新连接网络,则生成新的 DevNonce。恶意攻击节点抓出这一特点,通过占用大量 DevNonce 使

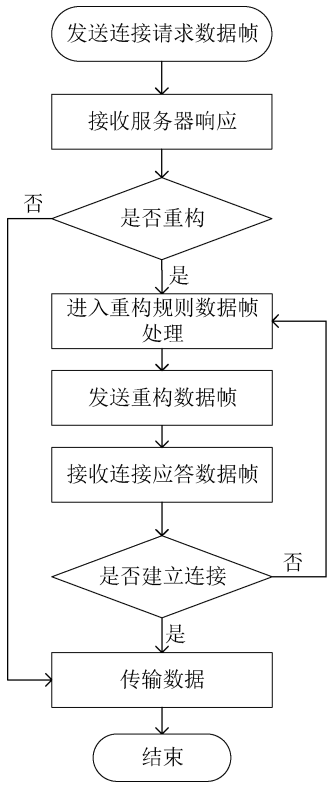

图 6　终端侧设备合法性检测流程图

Fig. 6　Flow chart of legality testing of terminal side equipment

终端设备不能产生规定范围内的随机数,而无法与服务器建立连接。

$$T_r = \frac{N_D}{F_J} \tag{1}$$

式中,T_r(以天为单位)代表攻击节点重放需等待的时间,是表示数据链路安全性的重要系数;N_D代表最终数据池中的序列;f_J(固定值)代表每天每个终端设备的有效连接过程的数量。

从式(1)可以看出,只要N_D越大,即数据池容量够充足,则连接请求就够安全。

而帧重构机制可以在每次身份认证结束后便丢弃已产生 DevNonce,从而有效地防止了重放攻击。

判断算法优越性的指标,除了防止重放的时间之外,还有终端连接的成功率。

假设 DevNonce 在数据集$[1,\cdots,N=2^{16}]$内,S是存储 DevNonce 的集合,$|S| = N_D$,那么在 LoRaWAN v1.1 定义下,终端产生一个已被N_D存储的 DevNonce 的概率是:

$$P[d_k \in S] = \frac{N_D}{N} \tag{2}$$

可以看出N_D越大,则连接成功率就越低。

而在通过业务区分机制中,引入了周期性帧重构的概念。将一天的时间分为n个周期T,在一个周期结束后,服务器存储的已被终端使用过的 DevNonce 数据池将清空。那么终端产生一个已被N_D存储的 DevNonce 的概率就是:

$$P[d_K \in S] = P[d_K \in S \mid T_i] \tag{3}$$

式中,T_i表示当前所处周期,d_k是第k次连接过程中产生的 DevNonce。系数P代表信息的安全性,P系数越高,代表连接成功率越低,即信息传输风险越高。反之,则信息传输风险越低。

为了验证系统性能,在 opnet 中搭建了 LoRa 传感器网络模型,模拟信息发送与接收。根据信息的安全等级不同,将采集到的医疗信息分为五个等级,每个等级有其相应的重构周期。采集到的数据会根据它对应的等级选择相应的重构周期进行发送。所以在实际情况中,周期是可变的。在可变周期下的安全系数的对比见图7。

n 代表着不同程度安全等级,对比其对应着的不同的概率。生成的N_D增大,生成无效 DevNonce 的概率越高,即数据连接建立的成功率越低。但因为周期性进行帧重构的原因,NS 端存储的 DevNonce 不断刷新,终端生成的无效 DevNonce 值

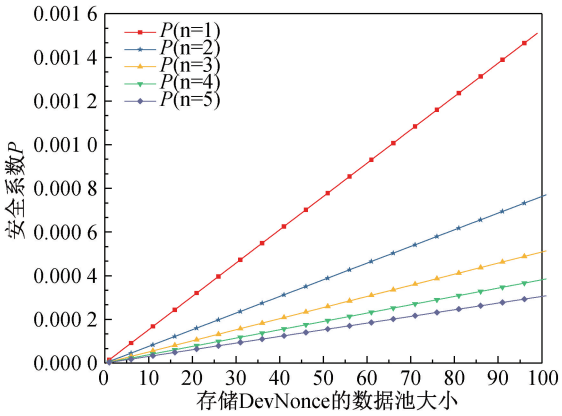

图7 安全系数对比图

Fig. 7 Comparison diagram of safety factor

的概率一直小于标准 LoRaWAN v1.1,且 n 越大,即周期时间越短,生成无效的 DevNonce 的概率越小,即安全数据链路连接成功率越高。

为了对比可变周期下的帧重构与标准 LoRaWAN v1.1 的能量消耗,本文模拟了一段时间内的数据的发送,并对其进行业务区分,按照数据的重要程度对其进行安全度的区分,得到其安全等级变化,见图8。

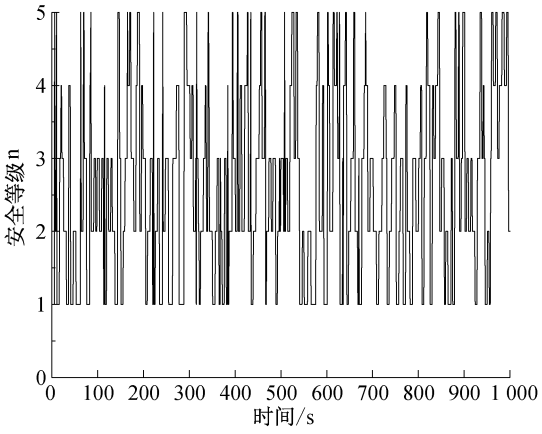

图8 安全等级设置

Fig. 8 Safety level setting

其中$P(n=1)=0.25$,$P(n=2)=0.272\ 5$,$P(n=3)=0.198\ 8$,$P(n=4)=0.127\ 1$,$P(n=5)=0.151\ 6$。依照这部分的不同安全等级的数据进行系统开销的计算。

2.3 系统开销

先设定能量消耗系数,假定发送一比特数据消耗的能量为0.000 5。接收一比特数据消耗的能量为0.001。终端每间隔 20 s 向服务器发送数据。在五个安全等级下(第一等级即按照标准 LoRaWAN 协议发送数据)对能耗进行比较,周期性进行重构的

能量消耗显然比标准 LoRaWAN v1.1 的能量消耗要大,且随着安全性等级越高,其能耗就越高。而各部分数据对安全性的要求也不同,若一味地追求高安全等级,会大大加速终端的能耗。而采用可变周期的方式,将隐私程度较高的数据设置为高安全等级,隐私度较低的数据设置为低安全等级。

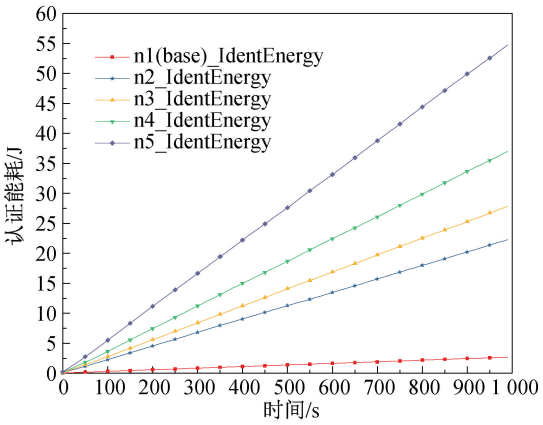

图 9　数据认证过程能耗图

Fig. 9　Energy consumption chart of data authentication process

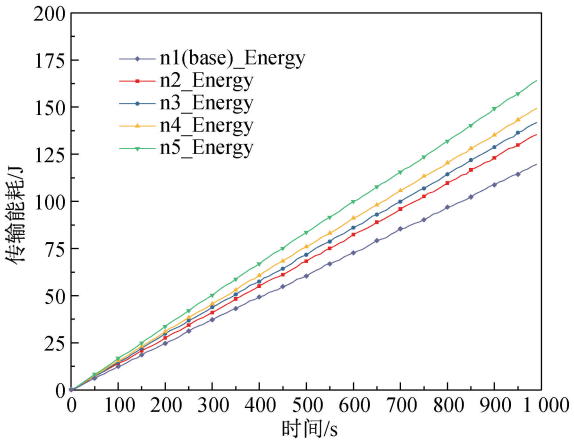

图 10　数据传输过程能耗图(包括认证过程)

Fig. 10　Data transmission process energy consumption diagram

图 9 为 1 000 s 内终端周期性身份认证过程的能耗对比图,在可变周期下产生的总能耗虽高于传统 LoRaWAN v1.1(即 n1(base)_Energy 曲线),但它在考虑安全性的基础上,与单纯追求高安全等级的传输相比,能耗大大降低。

图 10 为 1 000 s 内终端周期性身份认证并进行数据传输所产生的能耗对比图,在可变周期下产生的总能耗虽高于传统 LoRaWAN v1.1,但它在考虑安全性的基础上,与单纯追求高安全等级的传输相比,能耗大大降低。

从短期观察信号延迟问题,通过图 11 所示,由

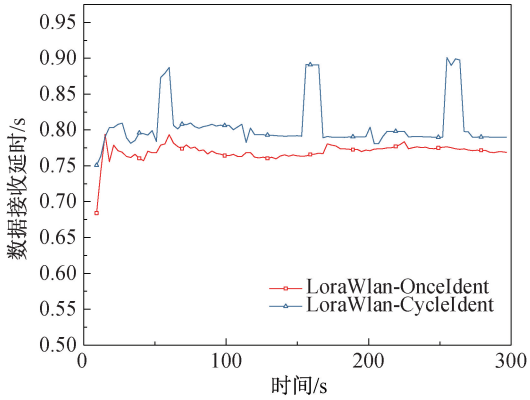

图 11　数据接受延迟分析图

Fig. 11　Data reception delay analysis graph

于在帧重构机制服务器需要对终端进行身份认证,且终端需要根据服务器要求进行帧重构,所以在最初进行数据传输时,本系统的延迟时间略高于标准 LoRaWAN v1.1 协议的延迟时间。当完成身份认证之后,受阻的数据会先后到达服务器,这部分数据在身份验证过程中已经进行重构,所以图中两种模式会有短暂重叠,随后两条线渐渐趋于平缓。一个周期结束后,帧重构机制中终端需要再一次进行身份认证,身份认证结束后,延迟时间又恢复稳定。通过对实验结果分析,在数据传输阶段造成的实验增加不足 7%。

3　结论

本文针对性的 LoRa 无线传感网络的协议安全性问题,提出一种基于 LoRaWAN 协议的双向认证机制,该机制利用数据帧的编码重构,实现终端与服务器之间双向的身份认证,并在此基础上对重构规则进行周期性更新,对不同安全等级的节点进行不同周期的重构规则更新,避免多次重构规则更新造成的系统开销。通过对协议安全性的算法分析,结果表明该机制能够有效提高终端与服务器建立连接过程的安全性,且协议安全性随着重构规则更新周期的缩短而增大。对该机制进行能耗分析,结果显示在双方身份认证过程中造成的能耗会随着周期的缩短而增大,在整体数据传输过程中,能耗增加并不明显,数据时延仅在认证阶段具有显著增加,而在整体数据传输阶段时延增加不过 7%。该协议的安全性、能耗和时延均随重构规则更新周期的变化而变化,故该协议下一步将对更新周期的设置进行进一步研究,以求达到安全性和系统开销的平衡。

参考文献:

[1]DENG Tian. An Adaptive MAC Protocol for SDCS System Based on LoRa Technology[C]//Research Institute of Management Science and Industrial Engineering, 2017.

[2]郭 帅,郭忠文,仇志金. HSMA:面向物联网异构数据的模式分层匹配算法[J]. 计算机研究与发展,2018,55(11):2522-2531.

[3]CHRISTOS Bouras, APOSTOLOS Gkamas, VASILEIOS Kokkinos, et al. Geolocation Analysis for Search And Rescue Systems Using LoRaWAN[J]. International Journal of Communication Systems, 2020,33(17): 38.

[4]TAHSIN C M, DöNMEZ, ETHIOPIA Nigussie. Security of LoRaWAN v1.1 in Backward Compatibility Scenarios[J]. Procedia Computer Science, 2018, 134:51-58.

[5]GAO Shuyang, LI Xiaohong, MA Maode. A Malicious Behavior Awareness and Defense Countermeasure Based on LoRaWAN Protocol[J]. Sensors, 2019, 19(23): 5122-5122.

[6]RAMON Sanchez-Iborra, JESúS Sánchez-Gómez, SALVADOR Pérez, et al. Enhancing LoRaWAN Security through a Lightweight and Authenticated Key Management Approach[J]. Sensors (Basel, Switzerland), 2018,18(6): 1833.

[7]MOHAMED Eldefrawy, ISMAIL Butun, NUNO Pereira, et al. Formal Security Analysis of LoRaWAN[J]. Computer Networks,2018,148: 328-339.

[8]Tomasin S, Zulian S, Vangelista L. Security Analysis of LoRaWAN Join Procedure for Internet of Things Networks[C]//2017 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), 2017:1-6.

[9]XU W, JHA S, HU W. LoRa-Key: Secure Key Generation System for LoRa-based Network[J]. IEEE Internet of Things Journal,2018 (12): 1.

[10]KIM J, SONG J. A Secure DEVICE-TO-DEVICE Link Establishment Scheme for LoRaWAN[J]. IEEE Sensors Journal, 2018,18(5): 2153-2160.

[11]KAZIM Rifat Ozyilmaz, ARDA Yurdakul. Designing a Blockchain-Based IoT With Ethereum, Swarm, and LoRa: The Software Solution to Create High Availability With Minimal Security Risks[J]. IEEE Consumer Electronics Magazine,2019,8(2): 28-34.

[12]NA S, HWANG D, SHIN W, et al. Scenario and Countermeasure for Replay Attack Using Join Request Messages in LoRaWAN[C]//2017 International Conference on Information Networking (ICOIN),2017: 718-720.

[13]IGOR E, SHPARLINSKI. Orders of points in Families of Elliptic Curves[J]. Proceedings of the American Mathematical Society,2020,148(6):2371-2377.

[14]ALOÿS Augustin, JIAZI Yi, THOMAS Clausen, et al. A Study of LoRa: Long Range & Low Power Networks for the Internet of Things[J]. Sensors, 2016, 16(9): 1466.

[15]欧国成,刘小园. 超混沌与AES的混合加密算法[J]. 江西理工大学学报,2020,41(05):80-87.

[16]JAEHYU Kim, JOOSEOK Song. A Dual Key-Based Activation Scheme for Secure LoRaWAN[J]. Wireless Communications and Mobile Computing,2017,2017:1-12.

(责任编辑 王利君)