软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2019,30(Suppl.(1)):105−112

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

压缩感知的 IPv6 无线传感网信息隐藏方法*

王 浩[1,2], 李育桐[1,2], 胡 润[1,2], 卓 兰, 王明存[1,2]

[1](重庆邮电大学 自动化学院,重庆 400065)

[2](工业物联网与网络化控制教育部重点实验室(重庆邮电大学),重庆 400065)

通讯作者: 王浩, E-mail: wanghao@cqupt.edu.cn

摘 要: 保障隐私数据安全是IPv6无线传感网安全的一个重要研究内容,信息隐藏技术能够利用隐私数据的特点实现数据的不可见性,在隐私安全保护方面发挥着重要作用.针对 IPv6 无线传感网的特点和数据隐匿性的安全需求,结合压缩感知理论,实现隐秘传输的计算开销集中在资源富裕的汇聚节点端.利用压缩感知,有效地将感知层节点端的计算开销大幅度降低,提出一种适用于 IPv6 无线传感网环境下的信息隐藏方法.该方法主要包括隐藏密钥的管理、嵌入算法的设计和提取算法的设计,以此为 IPv6 无线传感网敏感数据的传输提供隐匿性,保障网络中敏感数据的安全性.结果表明,该信息隐藏算法在嵌入过程中,随着敏感数据的增加,通信开销低于 25%.

关键词: IPv6 无线传感器网络;信息隐藏;压缩感知;隐匿性

中文引用格式: 王浩,李育桐,胡润,卓兰,王明存.压缩感知的 IPv6 无线传感网信息隐藏方法.软件学报,2019,30(Suppl.(1)):105−112. http://www.jos.org.cn/1000-9825/19011.htm

英文引用格式: Wang H, Li YT, Hu R, Zhuo L, Wang MC. Information hiding method of ipv6 wireless sensor networks based on compressed sensing. Ruan Jian Xue Bao/Journal of Software, 2019,30(Suppl.(1)):105−112 (in Chinese). http://www.jos.org.cn/1000-9825/19011.htm

Information Hiding Method of IPv6 Wireless Sensor Networks Based on Compressed Sensing

WANG Hao[1,2], LI Yu-Tong[1,2], HU Run[1,2], ZHUO Lan, WANG Ming-Cun[1,2]

[1](College of Automation, Chongqing University of Posts and Telecommunications, Chongqing 400065, China)

[2](Key Laboratory of Industrial Internet of Things and Networked Control (Chongqing University of Posts and Telecommunications), Ministry of Education, Chongqing 400065, China)

Abstract: Protecting privacy data is an important research content of IPv6 wireless sensor networks security. Since information hiding technology can achieve the invisibility of data, it plays an important role in privacy protection. In view of the characteristics of IPv6 wireless sensor networks and the security requirements of data concealment, combined with the theory of compressed sensing, the transmission overhead is concentrated on the convergence node. Using compressed sensing to effectively reduce the overhead of the sensing layer node, this paper proposes an information hiding method for IPv6 wireless sensor networks. The method mainly includes the hidden key management, the embedded algorithm and the extraction algorithm, which provides confidentiality for the transmission of sensitive data of the IPv6 wireless sensor networks to ensure the security and the reliability of sensitive data. The results show that the information hiding algorithm has less than 25% communication overhead with the increase of sensitive data.

Key words: IPv6 wireless sensor network; information hiding; compressed sensing; confidentiality

IPv6 作为互联网中广泛应用的网络层协议,其 128 位的地址长度可使地址容量达到 2^{128} 个,足以满足 WSN

* 基金项目: 国家重点研发计划(2017YFE0123000); 2018 年工业互联网创新发展工程([2018]282); 2018 年重庆市技术创新与应用示范专项(cstc2018jszx-cyztzxX0012); 浙江大学教育部重点实验室开放课题(ZJU2019001)

Foundation item: National Key Research and Development Program of China (2017YFE0123000); 2018 Industrial Internet Innovation and Development Project ([2018]282); Chongqing Technology Innovation and Application Demonstration Project in 2018 (cstc2018jszx-cyztzxX0012); Key Laboratory of Zhejiang University Ministry of Education Open Project (ZJU2019001)

收稿时间: 2019-09-15; 采用时间: 2019-10-24

节点的大规模性.6LoWPAN 技术的出现解决了 IPv6 在 WSN 应用的技术问题,有效地实现了 IP 技术与 WSN 技术的无缝连接[1].目前,基于 IPv6 无线传感网也称为 6LoWPAN 网络.

IPv6 无线传感网处于一个开放的、复杂的网络环境中.针对网络中隐私数据的保护研究还较少,信息隐藏作为信息安全领域快速发展的一项新兴技术,将需要保护的隐私数据通过一定的算法嵌入到载体数据中,并且不会影响载体数据的可用性,从而避免引起攻击者的注意和重视,降低隐私数据被泄露的可能性.该技术在 IPv6 无线传感网隐私数据保护方面具有重要的研究意义和广泛的应用前景[2,3].因此,针对 IPv6 无线传感网的特点,提出一种适用于 IPv6 无线传感网的信息隐藏机制是非常有必要的.

1 相关工作

信息隐藏技术作为信息安全理论的一种应用,在 WSN 中大量的信息隐藏方法相继被提出.Feng 等人[4]首次将信息隐藏技术应用在 WSN 的版权保护问题中,以网络中发送的普通数据作为载体数据,具有较好的隐秘性.Xiao 等人[5]提出了一种敏感数据的安全传输的方法,保障敏感数据传输的安全性.董晓梅等人[6]提出了一种基于信息隐藏技术的数据认证方法,该方法在数据融合的过程中能够保留水印信息,从而确保报文中数据的真实性.肖迪等人[7]针对云环境下数据量大,数据缺乏相关安全保护机制的问题,通过原始数据的稀疏表示来实现身份信息的隐藏,从而为数据的版权信息安全提供了保障.

现有研究表明,信息隐藏算法主要通过规则性的嵌入来实现敏感信息的隐藏,通过特定的路径传输到目的节点后利用逆向算法提取出敏感信息.敏感信息的嵌入和提取的规律性难以抵抗倒置攻击和其他安全威胁,一旦敏感信息的嵌入和提取规则泄露,网络的安全性将受到严重的威胁.同时,现有的信息隐藏方法中敏感信息的嵌入和提取过程所需要的开销相差不大,不适合 IPv6 无线传感网节点资源受限而汇聚节点端资源富裕的特点.因此,在现有信息隐藏的相关研究基础上,提出一种适用于 IPv6 无线传感网特点的信息隐藏方法具有重要意义.

2 基于压缩感知的信息隐藏方法

2.1 压缩感知理论模型

本文结合压缩感知理论在数据编码端计算简单而解码端计算复杂的特点,实现隐秘传输的计算开销集中在资源富裕的汇聚节点端,有效地将感知层节点端的计算开销大幅度降低.压缩感知理论表明,只要原始信号是可以压缩的(即稀疏的),就能通过少量的采样值,并且在合适的情况下完美地重构信号[8].根据压缩感知理论架构[9],对于信号 $x(n)\in R^n$,存在稀疏基ϕ满足稀疏矩阵$\alpha=\phi^{-1}x(n)$,可以利用测量矩阵 $A\in R^{m\times n}$,得到它的 $m(m<n)$个线性测量矩阵 $y(m)\in R^m$,满足 $y=Ax$,最后再利用合适的迭代算法就可以精确地重构出稀疏矩阵α,恢复信号 $x'(n)$.

2.2 论文参数符号说明

本文设计方法中使用的所有符号说明见表 1.

Table 1 Symbol specification in the method

表 1 方法中使用的符号说明

符号	符号说明
ID	节点的身份信息
$Hash()$	哈希函数,将数据块映射为固定长度的值
$E_{key}(M)$	使用密钥 key 完成对明文信息 M 的加密
K_i	隐藏密钥,用于嵌入算法和提取算法中
K_a^t	对主密钥 PSK 进行 t 次 Hash 运算后更新的密钥
$E_{key}(K_i,ID_i)$	隐藏密钥 K_i 和节点 ID_i 生成正态随机矩阵

2.3 隐藏密钥的管理

1. 隐藏密钥的建立

系统初始化状态下,汇聚节点和传感器节点存储着全网预配置密钥 PSK,完成隐藏密钥的协商后,传感器节

点将主密钥 PSK 从内存中擦拭,防止预配置密钥 PSK 泄露而危害整个网络.

(1) 传感器节点 i 在加入网络时,利用随机数生成器生成随机数 N_1,利用主密钥 PSK 对 ID_i 和 N_1 进行加密,生成密文 S_1,密文生成方式如公式(1)所示;然后根据生成的密文 S_1、系统当前时间 t_1 以及认证码 MAC_1,认证码计算方式如公式(2)所示;最后将 S_1 和 MAC_1 作为入网认证报文发送给汇聚节点,报文构造方式如公式(3)所示.

$$S_1 = E_{PSK}(ID_i, N_1) \tag{1}$$

$$MAC_1 = Hash(S_1, t_1, PSK) \tag{2}$$

$$Join\_Req_i \rightarrow \{S_1, MAC_1\} \tag{3}$$

(2) 汇聚节点在接收到传感器节点的入网请求报文($Join\_Rsq_i$)后,利用 Hash 函数生成 $MAC_1'=Hash(S_1,t_1,PSK)$,若 $MAC_1'=MAC_1$,则通过认证.汇聚节点生成随机数 N_2,并利用接收到的 N_1 和 N_2 生成隐藏密钥 K_i,隐藏密钥的计算如公式(4)所示.

$$K_i=Hash(N_1, N_2) \tag{4}$$

(3) 汇聚节点根据 ID_j、N_2 以及 K_i 生成密文 S_2,密文生成方式如公式(5)所示;然后根据生成的 S_2、系统当前时间 t_2 以及 MAC_2,认证码计算方式如公式(6)所示;最后将 S_2 和认证码 MAC_2 作为响应报文发送给传感器节点 i,报文构造方式如公式(7)所示.

$$S_2 = E_{PSK}(ID_j, N_2, K_i) \tag{5}$$

$$MAC_2 = Hash(S_2, t_2, PSK) \tag{6}$$

$$Join\_Rsp_i \rightarrow \{S_2, MAC_2\} \tag{7}$$

(4) 传感器节点 i 收到响应报文($Join\_Rsp_i$)后,利用 Hash 函数生成的消息验证码 $MAC_2'=Hash(S_2,t_2,PSK)$,若 $MAC_2'=MAC_2$,则报文通过认证.传感器节点 i 从报文中获取隐藏密钥 K_i,计算 $Hash(PSK)$并擦除 PSK.

至此,完成传感器节点 i 和汇聚节点之间隐藏密钥 K_i 的建立.

2. 隐藏密钥的更新

系统运行一段时间后,传感器节点和汇聚节点共享的隐藏密钥也会不定期地进行更新.每次更新后对主密钥进行一次 Hash 运算,即使捕获某个传感器节点的主密钥 $Hash^t(PSK)$和操作次数 t,也无法得到其他传感器节点当前的隐藏密钥,提高了系统的安全性.

(1) 传感器节点 i 申请更新隐藏密钥时,利用随机数生成器生成随机数 N_3,利用更新后的主密钥对报文进行加密,其中,t 表示主密钥更新的次数,传感器节点 i 根据自身的地址 ID_i 和生成的随机数 N_3 生成密文 S_3,密文生成方式如公式(8);然后根据生成的密文 S_3、系统当前时间 t_3 以及主密钥计算认证码 MAC_3,认证码计算方式如公式(9);最后将密文 S_3 和认证码 MAC_3 作为入网认证报文发送给汇聚节点,报文构造方式如公式(10)所示.

$$S_3 = E_{K_a^t}(ID_i, N_3) \tag{8}$$

$$MAC_3 = Hash(S_3, t_3, K_a^t) \tag{9}$$

$$Update\_Req_i \rightarrow \{S_3, t, MAC_3\} \tag{10}$$

(2) 汇聚节点在接收到传感器节点的入网请求报文($Update\_Req_i$)后,获取 t 并利用公式(11)计算传感器节点 i 的主密钥 K_a^t,利用 Hash 函数生成报文的消息验证码 K_a^t,利用 Hash 函数生成报文的消息验证码 $MAC_3'=Hash(S_3,t_3,K_a^t)$,若 $MAC_3'=MAC_3$,则通过认证.汇聚节点利用随机数生成器生成随机数 N_4,并利用接收到的 N_3 生成更新后的隐藏密钥 K_i',隐藏密钥的计算方式如公式(12)所示.

$$K_a^t = Hash^t(PSK) \tag{11}$$

$$K_i'=Hash(N_3, N_4) \tag{12}$$

(3) 汇聚节点根据生成的随机数 N_4、更新后的隐藏密钥 K_i'生成密文 S_4,密文生成方式如式(13)所示;然后根据生成的密文 S_4、系统当前时间 t_4 以及主密钥计算认证码 MAC_4,认证码计算方式如式(14)所示;最后将密文 S_4 和认证码 MAC_4 作为响应报文发送给传感器节点 i,报文构造方式如公式(15)所示.

$$S_4 = E_{K_a^t}(ID_j, N_4, K_i') \tag{13}$$

$$MAC_4 = Hash(S_4, t_4, K_a^t) \tag{14}$$

$$Update\_Rsp_i \rightarrow \{S_4, MAC_4\} \tag{15}$$

(4) 传感器节点 i 收到响应报文($Update\_Rep_i$)后,利用带 Hash 函数生成验证码 $MAC_4'=Hash(S_4,t_4,K_a^t)$,若 $MAC_4'=MAC_4$,则通过认证.节点 i 从报文中获取隐藏密钥 K_i',将更新次数 t 自加一位,即 $t=t+1$.对主密钥进行 Hash 运算,并擦除原有的主密钥,主密钥的更新方式如式(16)所示.

$$K_a^t = Hash(K_a^t) \tag{16}$$

至此,完成节点 i 和汇聚节点之间隐藏密钥 K_i 的更新.

2.4 数据的嵌入过程

敏感数据的嵌入算法主要集中在网络中资源受限的传感器节点端,具体实现过程如下.

1. 部署在检测环境中的无线传感器节点采集检测环境中安全级别高的敏感数据 S_n 和常规载体数据 E_m,利用第 2.3 节中分发的隐藏密钥对敏感数据进行预处理,通过阈值矩阵实现载体数据的稀疏化,通过简单的矩阵线性运算将敏感数据嵌入到常规载体数据中,生成目标传输数据.

(1) 传感器节点 i 将采到的数据存储到数据缓存区,当缓存区为满时,从中提取 n 个敏感数据 s,组成敏感数据列向量 $S_n=\{s_1,s_2,s_3,\ldots,s_n\}^T$.

(2) 传感器节点 i 利用第 2.3 节中生成的隐藏密钥 K_i 产生矩阵 $\Phi_{m\times n}(m>n)$,即 $\Phi_{m\times n}=E(ID_i,K_i)$,不同的隐藏密钥 K_i 生成的正态随机矩阵不同.其中,E 为正态随机矩阵生成算法.传感器节点对敏感数据列向量进行线性编码,得到敏感数据的测量值 Y_m,计算公式为

$$Y_m = \boldsymbol{\Phi}_{m\times n} S_n \tag{17}$$

(3) 传感器节点 i 从缓存区中提取 m 个载体数据 e,组成载体数据列向量 $E_m=\{e_1,e_2,e_3,\ldots,e_m\}^T$.构造载体数据列向量的稀疏基矩阵 $\Psi_{m\times m}$,使得满足公式:

$$E_m = \boldsymbol{\Psi}_{m\times m} Es_m \tag{18}$$

本方法采用离散余弦变换的方式,将非稀疏的时域信号 E_m 通过离散余弦变换矩阵 $\Psi_{m\times m}^{-1}$,生成频域上近似稀疏的矩阵 Es_m.传感器节点生成阈值矩阵 Q,得到稀疏后的载体数据 Es_m',计算公式为

$$Es_m' = Q \cdot Es_m \tag{19}$$

其中,$Es_m'=\{r_1,r_2,r_3,\ldots,r_\rho\}^T$ 为载体数据稀疏列向量,$r_1,r_2,r_3,\ldots,r_\rho$ 为 Es_m' 列向量中非零元素,Es_m' 的稀疏度为 ρ,即载体数据稀疏列向量 Es_m' 中非零元素的个数.

将公式(19)代入公式(18)可知,常规载体数据与稀疏后的载体数据的关系如下:

$$E_m = \boldsymbol{\Psi}_{m\times m} Q^{-1} Es_m' \tag{20}$$

(4) 通过公式(17)和公式(18)分别获得敏感数据的测量值 Y_m 和载体数据列向量 E_m,通过矩阵加法公式得到目标传输数据 f_m,计算公式为

$$f_m = E_m + \partial Y_m \tag{21}$$

将公式(17)和 Es_m 代入公式(21)中得到:

$$f_m = E_m + \partial \boldsymbol{\Phi}_{m\times n} S_m = \begin{bmatrix} e_1 \\ e_2 \\ e_3 \\ \vdots \\ e_m \end{bmatrix} + \partial \boldsymbol{\Phi}_{m\times n} \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ \vdots \\ s_n \end{bmatrix} \tag{22}$$

其中,∂ 为尺度调节因子,用于控制敏感数据减少对载体的影响,从而降低被恶意第三方发现的可能性.

2. 传感器节点 i 完成一个采集周期的工作后,将嵌入了敏感信息的目标传输数据 f_m,通过网络中节点按照一定的路径转发,传送到汇聚节点.下面介绍数据包转发的主要过程.

(1) 传感器节点 i 完成敏感数据的嵌入后,将生成的目标传输数据 f_m 添加到报文(New_i)中,并添加节点 i 的

地址 ID_i、阈值矩阵 Q、尺度变换因子∂、稀疏矩阵 Ψ 和验证码 MAC_5,验证码计算公式如式(23),报文构造方式如公式(24).

$$MAC_5 = Hash(ID_i, Q, \partial, \Psi, K_a^t) \tag{23}$$

$$News_i \to \{ID_i, Q, \partial, \Psi, f_m, MAC_5\} \tag{24}$$

(2) 传感器节点 i 将下一跳邻居从休眠状态中被唤醒,从邻居列表中选取最近的空闲节点,发送数据包至下一跳节点.

(3) 重复步骤(2)直至数据包传输到目标地址(汇聚节点).

2.5 数据的提取过程

本节提出的敏感数据的提取算法主要集中在资源相对富裕的汇聚节点解码端,实现敏感数据的重构和常规载体数据的提取.汇聚节点接收到包含有目标传输数据的报文,利用第 2.3 节中协商的隐藏密钥 K_i 生成非零矩阵 $\boldsymbol{H}_{k\times m}$,对目标传输数据 f_m 进行预处理并构造出欠定方程组.具体实现过程如下:

1. 汇聚节点收到传感器节点 i 发送的报文(New_i),利用 Hash 函数生成报文的消息验证码 $MAC_5'=Hash(ID_i,Q,f_m,\partial,\Psi,PSK)$,若 $MAC_5'=MAC_5$,则报文通过验证,提取出目标传输数据 f_m.

2. 汇聚节点利用第 2.3 节中协商出来的隐藏密钥 K_i 产生矩阵 $\Phi_{m\times n}(m>n)$,即 $\Phi_{m\times n}=E(ID_i,K_i)$.其中,$E$ 为正态随机矩阵生成算法.汇聚节点利用 $\Phi_{m\times n}$ 生成非零矩阵 $\boldsymbol{H}_{k\times m}(\rho\cdot\log(m/\rho)\leqslant k<m)$,使其满足:

$$\boldsymbol{H}_{k\times m}\times\boldsymbol{\Phi}_{m\times n}=0 \tag{25}$$

通过公式(25)计算矩阵 $H_{k\times m}$ 和步骤 1 中提取出的目标传输数据 f_m,根据矩阵基本运算得到:

$$\left.\begin{aligned} y_k &= \boldsymbol{H}_{k\times m} f_m = \boldsymbol{H}_{k\times m}\left(E_m + \partial y_m\right) \\ &= \boldsymbol{H}_{k\times m}\left(E_m + \partial\boldsymbol{\Phi}_{m\times n} S_n\right) \\ &= \boldsymbol{H}_{k\times m} E_m + \partial\boldsymbol{H}_{k\times m}\boldsymbol{\Phi}_{m\times n} S_n \end{aligned}\right\} \tag{26}$$

根据公式(25)可知,$H_{k\times m}\times\Phi_{m\times n}=0$,得到:

$$y_k = \boldsymbol{H}_{k\times m} E_m \tag{27}$$

根据公式(20)可知,$E_m=\Psi_{m\times m}Q^{-1}Es_m'$,得到:

$$y_k = \boldsymbol{H}_{k\times m}\boldsymbol{\Psi}_{m\times m}Q^{-1}Es_m' = \boldsymbol{\Theta}_{k\times m}Es_m' \tag{28}$$

其中,$\Theta_{k\times m}$ 为传感矩阵,$\Theta_{k\times m}=H_{k\times m}\Psi_{m\times m}Q^{-1}$,将报文($New_i$)中相关数据代入,就可以求解传感矩阵 $\Theta_{k\times m}$.将 Es_m' 代入到公式(28)中,得到:

$$y_k = \boldsymbol{\Psi}_{m\times m} Es_m' = \boldsymbol{\Theta}_{k\times m}\begin{bmatrix} r_1 \\ 0 \\ r_2 \\ \vdots \\ r_\rho \end{bmatrix}_m \tag{29}$$

3. 根据压缩感知原理,在 RIP 条件下[10],能够根据能够由 $k(k<m)$个观测值构成的列向量 y_k 精确重构 Es_m'.

矩阵 $\Theta_{k\times m}$ 中存在任意 2ρ 列线性无关时,则公式(29)具有唯一的解 Es_m'.考虑到 IPv6 无线传感网大规模数据的特点,降低汇聚节点因敏感数据重构而产生的存储开销,本方法采用梯度追踪算法求解欠定方程(28)中 Es_m'.

梯度追踪算法求解过程:设定输入值,包括迭代次数 L、矩阵 $\Theta_{k\times m}$、列向量 y_k、迭代残差 r_0,更新梯度 a^n 和方向 d^n,通过迭代运算$(Es_m')^n=(Es_m')^{n-1}+a^nd^n$ 得到重构信号 Es_m',然后根据公式(20)利用稀疏基矩阵 $\Psi_{m\times m}$ 和阈值矩阵 Q 近似重构出载体数据列向量 E_m.

4. 汇聚节点重构出常规载体数据 E_m 后,将其代入公式(19)中得到:

$$f_m = E_m + \partial\boldsymbol{\Phi}_{m\times n} S_n \tag{30}$$

由公式(30)得到:

$$S_n = (\partial\boldsymbol{\Phi}_{m\times n})^{-1}(f_m - E_m) \tag{31}$$

根据矩阵的基本运算,将汇聚节点提取的目标传输数据 f_m、尺度变换因子∂、随机矩阵 $\Phi_{m\times n}$ 以及步骤 3 中

求得的 E_m 代入公式(31)中,得到敏感数据列向量 S_n.

3 方法性能分析

3.1 安全性分析

1. 抗倒置攻击

倒置攻击是信息隐藏算法中一种常见的攻击方式.为了抵抗这种常见的攻击,本方法在敏感数据的嵌入和提取过程中需要使用唯一的正态随机矩阵 $\Phi_{m\times n}(m>n)$.该矩阵是由隐藏密钥 K_i 生成的.即使攻击者熟悉敏感数据的嵌入规则,在无法获取隐藏密钥 K_i 的情况下,也无法从报文中提取敏感数据 S_n,从而抵抗倒置攻击.

2. 抗主动攻击

本方法主要将安全级别较高的敏感数据隐藏到常规载体数据,从而实现敏感数据的隐秘传输.在敏感数据的嵌入过程中,通过尺度调节因子∂减小嵌入过程敏感数据对载体数据的影响,降低敏感数据被攻击者发现的可能性.从目标传输数据中提取敏感数据需要使用隐藏密钥 K_i 生成正态随机矩阵 $\Phi_{m\times n}$,攻击者无法获取传感器节点 i 和汇聚节点之间的隐藏密钥 K_i,因此无法对报文中的敏感数据进行修改.

3. 抗被动攻击

被动攻击是信息安全中一种常见的攻击方式,攻击者通过对报文信息的分析,能够获取网络中有用信息.信息隐藏将敏感信息隐藏在常规数据中,保证了敏感数据 S_n 的不可见,嵌入目标传输数据 f_m 的报文与原始载体数据 E_m 相差不大,因此有效地避免敏感数据被监听到.

4. 抗重放攻击

重放攻击的目的是干扰传感器节点设备之间的正常认证.本文设计的信息隐藏方法可以抵御对隐藏密钥建立和更新命令的重放攻击,在入网认证报文和隐藏密钥更新请求报文中添加了时间 t 作为消息认证码的输入因子,当接收到报文时延超过最大值 ΔT 时,报文认证失败,从而有效地抵御重放威胁.

3.2 开销分析

1. 通信开销分析

本节对隐藏密钥建立、隐藏密钥更新及数据嵌入过程所产生的通信开销进行分析.其中,协议栈中采用对称加解密算法是 128 位的 AES 加密算法,所使用的哈希函数是 128 位的 MD5 算法.当传感器节点中载体数据的长度为 m bytes 时,根据所采用的各种密码算法可得本文方法各阶段通信报文的长度信息,具体见表 2.

Table 2 Length information of each phase communication message

表 2 各阶段通信报文长度信息

	交互报文	长度(byte)
隐藏密钥建立	$Join\_Req_i\rightarrow\{S_1,MAC_1\}$	32
隐藏密钥更新	$Update\_Req_i\rightarrow\{S_3,t,MAC_3\}$	33
数据嵌入	$News_i\rightarrow\{ID_i,Q,\partial,\Psi,f_m,MAC\}$	21+3m

根据 IPv6 无线传感网实际情况,传感器节点在网络部署的过程中完成隐藏密钥的建立后,隐藏密钥的更新周期要远大于敏感数据嵌入的周期,当网络中节点数量为 N 时,传感器节点的报文长度为((86+3m)N) bytes.查阅 CC2530 数据手册和文献可知,当该类型的节点数据率为 250kbps 时,节点发送数据包的平均能耗为 Etx=196nJ/bit,则在理想情况下,CC2530 节点完成一次数据发送收所消耗的能量约为(2368(86+3m)N)nJ.当网络中节点数量 N 的取值范围为[1,30],载体数据 m 的取值范围为[1,50]时,节点的通信能量开销如图 1 所示.

假如网络中需要隐藏的节点数据 N=1 时,即以单个传感器节点完成一次敏感数据的隐藏所产生的通信开销.将本方法与 Tirkel 等人方法[11]、Cox 等人方法[12]进行对比,对比结果如图 2 所示.

由图 2 可知,传感器节点中嵌入敏感数据时,节点产生的计算开销随着敏感数据的嵌入量增加而线性增加.本文提出的方法在通信开销方面比 Cox 等人的方法要大,增加量约为 12.1%,当敏感数据低于 6 bytes 时,本文提

出方法的通信开销比 Tirkel 等人方法要高,随着敏感数据嵌入量的增加,通信开销量低于 25%.因此,在每次敏感数据隐藏量较小时,本文提出的方法与其他信息隐藏方法相比,在通信开销方面相差不大.

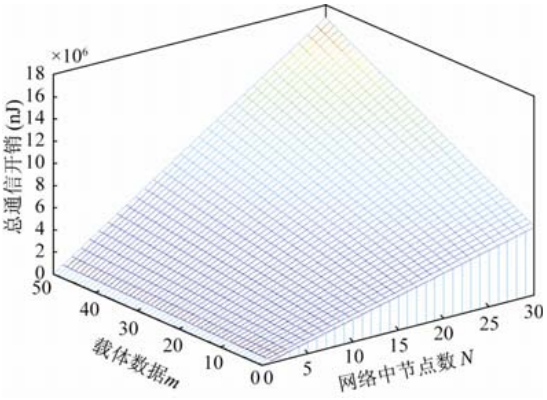

Fig.1 Sensor node communication overhead

图 1 传感器节点的通信开销

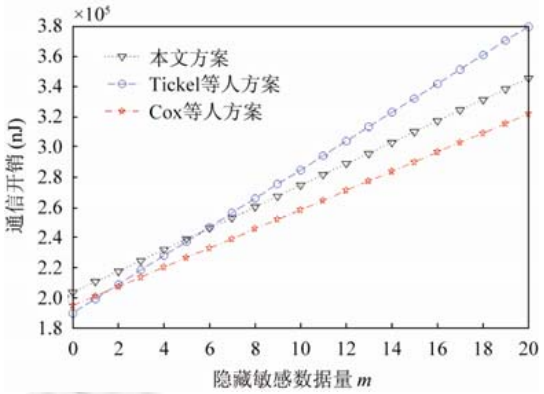

Fig.2 Comparison of communication overhead

图 2 通信开销对比

2. 计算开销分析

由于汇聚节点的计算能力较强、资源富裕,因此这部分的计算开销不必进行理论分析.本文主要针对传感器节点的计算开销进行理论分析,以计算时延作为计算开销的衡量标准,并将本文的计算开销和常用信息隐藏方法进行对比分析.在同一网络环境中,定义了几个计算参数,如下所示.

- T_{line} 表示矩阵线性运算所需的平均计算时延
- T_{hash} 表示哈希函数运算所需的平均计算时延
- T_{sym} 表示对称加密运算所需的平均计算时延

传感器节点在隐藏密钥建立过程中进行了 3 次哈希运算、2 次对称加密运算,在隐藏密钥更新过程中进行了 3 次哈希运算、2 次对称加密运算,在敏感数据的嵌入阶段,进行了 2 次矩阵线性运算.因此,本方法中传感器节点所产生的计算开销为 $6T_{hash}+4T_{sym}+2T_{line}$.在相同的网络环境下,隐藏 n bytes 的敏感数据,传感器节点的计算开销与文献[13]的方法相比,结果见表 3.

Table 3 Computing overhead comparison

表 3 计算开销对比

方法	身份认证者
文献[13]的方法	$5T_{hash}+3T_{sym}+nT_{line}$
本方法	$6T_{hash}+4T_{sym}+2T_{line}$

由表 3 中可以看出,在进行一次敏感数据的嵌入中,文献[13]的方法中嵌入的所产生的计算开销随着敏感数据的字节长度而增加,在系统实际工作过程中,隐藏密钥更新的周期远小于数据嵌入的周期,因此本文所提出的方法中传感器节点端所需要的计算开销小于文献[13]的方法所需要的计算开销.

4 结 论

本文提出了一种适用于 IPv6 无线传感网信息隐藏方法.该方法利用压缩感知在感知层把安全级别较高的敏感数据嵌入到载体数据中,通过中间路由节点转发,最后在汇聚节点完成敏感数据和载体数据的提取,从而实现敏感数据的隐秘传输.通过仿真平台测试敏感数据在无线信道中的提取效果,结果表明:本文提出的信息隐藏算法在嵌入过程中,随着敏感数据的增加,通信开销低于 25%.目前,IPv6 无线传感网与传统 IPv4 网络在链路层存在不同,该方法是无法直接适用于 IPv4 网络应用场景的.

References:

[1] Bouaziz M, Rachedi A. A survey on mobility management protocols in wireless sensor networks based on 6LoWPAN technology. Computer Communications, 2016,74(1):3−15.

[2] SunilKumar KN, Shivashankar. A review on security and privacy issues in wireless sensor networks. In: Proc. of the 2017 2nd IEEE Int'l Conf. on Recent Trends in Electronics, Information & Communication Technology (RTEICT). IEEE, 2017. 1979−1984.

[3] Winkler T, Rinner B. Security and privacy protection in visual sensor networks: A survey. ACM Computing Surveys (CSUR), 2014, 47(1):Article 2.

[4] Fang J, Potkonjak M. Real-time watermarking techniques for sensor networks. In: Wireless Sensor Networks. 2003. 305−323.

[5] Xiao XR, Sun XM, Yang LC, *et al*. Secure data transmission of wireless sensor network based on information hiding. In: Proc. of the 2007 4th Annual Int'l Conf. on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous). IEEE, 2007. 1−6.

[6] Dong XM, Zhao F, Li XH, *et al*. Digital watermarking technique applied to wireless sensor networks. Journal of Wuhan University (Science Edition), 2009,55(1):125−128 (in Chinese with English abstract).

[7] Xiao D, Ma QQ, Wang L, *et al*. Cloud-assisted secure digital watermarking based on sparse representation. Netinfo Security, 2017, 37(1):1−7 (in Chinese with English abstract).

[8] Bora A, Jalal A, Price E, *et al*. Compressed sensing using generative models. Proc. of Machine Learning Research, 2017,70: 537−546.

[9] Tsaig Y, Donoho DL. Extensions of compressed sensing. Signal Processing, 2006,86(3):549−571.

[10] Candes EJ, Tao T. Near-optimal signal recovery from random projections: Universal encoding strategies. IEEE Trans. on Information Theory, 2006,52(12):5406−5425.

[11] Tirkel AZ, Rankin GA, Schyndel RV, *et al*. Electronic watermark. In: Proc. of the Digital Image Computing, Technology and Applications. 1993.

[12] Li Q, Cox IJ. Rational dither modulation watermarking using a perceptual model. In: IEEE Workshop on Multimedia Signal Processing. IEEE, 2005. 1−4.

[13] Xiao XR, Sun XM, Chen MG. Secure data transmission of wireless sensor network based on information hiding. Comuter Science, 2007,34(9):142−147 (in Chinese with English abstract).

附中文参考文献:

[6] 董晓梅,赵枋,李晓华,等.适用于无线传感器网络的数字水印技术.武汉大学学报(理学版),2009,55(1):125−128.

[7] 肖迪,马青青,王兰,等.基于稀疏表示的云协助安全数字水印技术.信息网络安全,2017,37(1):1−7.

[13] 肖湘蓉,孙星明,陈明刚.基于信息隐藏的传感器网络数据安全传输.计算机科学,2007,34(9):142−147.

王浩(1975－),男,重庆市人,博士,教授,主要研究领域为工业物联网,信息安全.

卓兰(1978－),女,高级工程师,主要研究领域为物联网,智能制造.

李育桐(1994－),男,硕士生,主要研究领域为工业物联网,信息安全.

王明存(1994－),女,硕士生,主要研究领域为工业物联网,信息安全.

胡润(1991－),男,硕士,主要研究领域为信息安全,数字通信.