

一种基于数字水印的无线传感器网络敏感数据通信协议

任学军^{1,2}

(1.武警工程学院 通信工程系,陕西 西安 710086;

2.西北大学 信息科学与技术学院,陕西 西安 710127)

摘要: 基于信息隐藏技术开发了一种用于无线传感器网络的隐蔽的敏感数据通信协议。通过牺牲大值传感数据的精度来隐蔽地传输敏感数据,可广泛应用于多个领域。

关键词: 数字水印;信息隐藏;数据通信

中图分类号: TP393, TN929

文献标识码: A

A sensitive data communication protocol for wireless sensor networks based on digital watermarking

REN Xue Jun^{1,2}

(1.Department of Communication Engineering, Engineering College of Armed Police Force, Xi'an 710086, China;

2.School of Information Science and Technology, Northwestern University, Xi'an 710127, China)

Abstract: Based on digital watermarking, this paper proposed a hidden communication protocol for sensitive data transfer. This approach sacrifices the accuracy of large values of the sensor data to covertly transfer sensitive data, and can be widely used in many areas.

Key words: digital watermarking; information hiding; data communication

无线传感器网络具有节点成本低、电源消耗小、网络自组织等优点,已广泛地应用于很多领域^[1]。

无线传感器网络在很多应用中,存在着在节点间传输敏感信息的需求。敏感数据是指密钥、ID、军事领域中的关键数据、节点的身份验证信息等涉及系统安全、稳定运行的一类关键数据。这类数据通常要求采用一种比常规通信方式更安全、可靠的方式传递。敏感数据的传输有很多种方法,比较常见的是基于加密技术来实现。但由于传感器节点资源有限,复杂的算法无法在节点中实现^[2],这些算法在资源耗费方面、加密强度方面尚不完善。

本文基于数字水印的原理来实现敏感数据的传输,通过信息隐藏来实现敏感数据的传输。与加密传输相比,该算法具备简单高效、不易察觉等优点,适合于在无线传感器网络中实现。

数字水印(digital watermarking)技术是实现信息隐藏的一种主要手段。敏感信息可以毫无察觉地嵌入到数据

中,嵌入的信息就叫做水印^[3]。数字水印是信息隐藏学的一个分支,是利用人类感觉器官的不敏感及多媒体数据中存在的冗余,将秘密信息隐藏到宿主信息中,水印的添加不会影响原数据的正常使用^[4-7]。

基于以上原理,本文提出一种基于数字水印技术和信息隐藏的敏感信息通信协议。

目前绝大多数传感器节点都支持16位的寄存器,传感数据在通信时也是基于16位无符号数整数传输的。而16位无符号整数的取值范围是0~65 535。当实际采集的传感数据值比较大时,改变最低位对传感器数据值的影响很小,可以忽略不计。

因此,本文通过16位无符号整数的最低位来传输敏感数据,并利用数字水印嵌入算法将敏感数据嵌入其中,达到敏感数据隐蔽传输的目的。为避免最低位的改变对传感数据的精度造成太大影响,本文设置了一个阈值,只有大于该值的数据才会被嵌入敏感信息。

网络与通信

Network and Communication

1 敏感数据嵌入及提取过程

嵌入敏感信息的方法与数字水印的嵌入方法基本相同。如图 1 所示,首先将敏感信息转化为一个二进制流,命名为输入二进制流;将传感数据转化为一个 16 位无符号整数流,命名为输入整数流;将输出的含有敏感数据的无符号整数流命名为输出整数流。则敏感数据嵌入过程描述如下:如果输入整数流当前位置的传感数据值大于或等于阈值,且输入二进制流中当前位置的二进制值为“1”,则将整数流当前位置的数据最低位置“1”,并添加到输出整数流中,否则置“0”;如果输入整数流当前位置的传感数据值小于阈值,则不添加水印,直接将该数添加到输出整数流中。

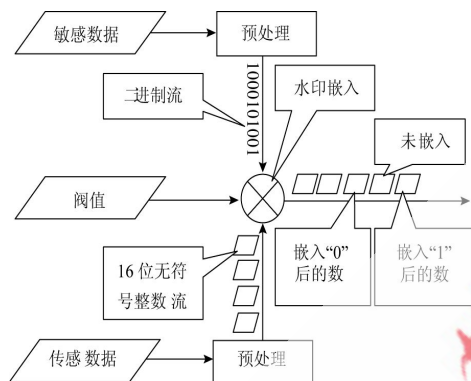


图 1 敏感数据的嵌入过程

敏感数据的嵌入算法描述如下:

```
#define N 0x0100; // 阈值
typedef BitStream TInputBitStream; // 定义输入二进制流
typedef UInt16Stream TInputUIntStream; // 定义输入无符号整数流
typedef UInt16Stream TOutputUIntStream; // 定义输出无符号整数流

//-----
/** 用敏感数据初始化输入二进制流 */
TInputBitStream * TheIBS =
    new TInputBitStream(SensitiveData aData);
/** 用传感数据初始化输入无符号整数流 */
TInputUIntStream * TheIUS =
    new TInputUIntStream(SensorData aData);
/** 用空数据初始化输出无符号整数流 */
TOutputUIntStream * TheOUS = new TOutputUIntStream();
//-----

/** 数字水印嵌入方法
** 注意:本方法假定输入整数流的长度
** 足以嵌入所有的敏感数据
** 参数 TheIBS: 输入二进制流
** 参数 TheIUS: 输入无符号整数流
** 参数 N: 预先定义的阈值
** 返回值: 输出无符号整数流 TheOUS */
```

```
TOutputUIntStream* InsertWaterMarking(TheIBS, TheIUS, N)
{
    uint16_t TheUIntIndex=0; //用于保存输入整数流的位号
    uint16_t TheBitIndex=0; //用于保存输入二进制流的位号
    uint16_t CurrentUIntData; //用于保存当前的无符号整数值
    bit_t CurrentBitData; //用于保存当前的二进制值
    while(TheBitIndex<TheIBS.Size)
    {
        CurrentUIntData=TheIUS.Read(TheUIntIndex, 1);
        CurrentBitData=TheIBS.Read(TheBitIndex, 1);
        /** 若当前无符号整数值小于阈值,则读取下一个值,
        * 直到大于阈值时,停止循环 */
        while(CurrentUIntData<N)
        {
            TheOUS.Write(CurrentUIntData); //将当前值加入输出流
            TheUIntIndex++;
            CurrentUIntData=TheIUS.Read(TheUIntIndex, 1);
        }
        /** 如果当前二进制值为 1, 则将当前无符号整数值
        的最后位置为“1”,并将该值加入到输出流中;否则,将
        最后位置为“0”,并将该值加入到输出流中。 */
        if(CurrentBitData==1)
            TheOUS.Write(CurrentUIntData|0x0001);
        else TheOUS.Write(CurrentUIntData&0xffff);
        TheBitIndex++;
        TheUIntIndex++;
    }
}
```

敏感数据的提取过程与嵌入过程相反,将接收到的含有敏感数据的 16 位无符号整数流命名为输入整数流,将提取出的二进制敏感数据流命名为输出二进制流,将输出的 16 位传感数据流命名为输出整数流。则敏感数据提取过程描述如下:首先将该值添加到输出无符号整数流中,然后检测输入整数流中当前位置的数据值,如果该值大于或等于阈值且最低位为“1”,则将“1”添加到二进制输出流中;否则,将“0”添加到二进制输出流中;如果该值小于阈值,则不往二进制输出流添加数据。最后,将输出二进制流转化为敏感数据,将输出无符号整数流转化为传感数据。

为进一步提升敏感数据传输的安全级别,还可以在预处理时对敏感数据加校验、加签名、加密等。

2 实际验证

无线传感器网络在某军事化应用中,多个节点被布设于一个生疏地域内,实时采集该地域的温度、湿度、光照等环境信息。为检测各个节点未被敌方捕获而传回虚假信息,各节点将不定时地传回自己的“识别码”,以证明自己的身份。“识别码”由节点 ID、当前时间、基站回

网络与通信 Network and Communication

复码等信息实时运算生成,为一串数字。

在该应用中,采用了本文所述方法传输“识别码”。具体做法是:在“光照”传感数据中,当数据值大于 256 (0x0100)时,嵌入“识别码”。如图 2 所示,“光照”数据的值通常白天在 600 以上,均大于阈值,方便嵌入水印,同时,嵌入水印后,对原值影响较小。

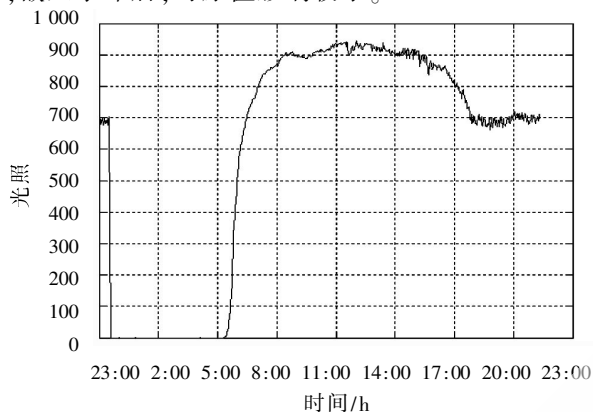


图 2 光照数据

表 1 嵌入“识别码”前后数据对照

未嵌入“识别码”前的数据	嵌入“识别码”后的数据	“识别码”的二进制值
609	609	1
672	672	0
681	681	1
759	759	1
840	841*	1
853	852*	0
857	856*	0
868	868	0
888	889*	1
896	896	0
913	913	1
914	914	0
932	933*	1
938	938	0
900	901*	1
915	915	1
945	944*	0
927	927	1
918	918	0
911	911	1
926	926	0
913	912*	0
908	908	0
906	906	0
897	896*	0
906	907*	1

嵌入“识别码”前后数据对照如表 1 所示。表中左列为未嵌入“识别码”时的“光照”数据,中间列为嵌入“识别码”后的“光照”数据,右列是“识别码”的二进制形式。中间列标有*的数字为嵌入“识别码”后发生变化的数据。

3 结果分析

3.1 水印嵌入对传感数据的影响

采用以上嵌入算法后,对传感数据的影响可分为以下三类:

(1)传感数据的值大于等于阈值,且其最低位在嵌入水印时发生了变化,即原始数据的最低位由“0”变为“1”或由“1”变为“0”。这时,传感数据的值在嵌入水印后发生了变化,变化前后传感数据相差为“1”。其相对变化率如下:

若:

$$d := \text{OldSensorData}$$

$$d' := \text{NewSensorData}$$

$$\Delta d = d' - d$$

则:

$$\delta d = \frac{\Delta d}{d} = \frac{\text{NewSensorData} - \text{OldSensorData}}{\text{OldSensorData}}$$

$$\text{又} \because \text{NewSensorData} - \text{OldSensorData} = 1$$

$$\text{且} \text{OldSensorData} \geq N$$

$$\therefore \delta d \leq \frac{1}{N}$$

可见,其相对变化率小于 $1/N$,当 $N=0x0100$,即十进制数 256 时,其相对变化率小于 0.39%

(2)传感数据的值大于等于阈值,但其最低位在嵌入水印时未发生变化,其值不受影响。

(3)传感数据的值小于阈值。传感数据的值小于阈值时,不嵌入水印,因此,其值不受影响。

3.2 N 值大小对协议的影响

当 N 值较大时,水印嵌入对原始传感数据的影响较小(相对变化率较小),但满足条件的传感数据则会变少,传输敏感数据的周期会变长;当 N 值较小时,水印嵌入对原始数据的影响较大(相对变化率较大),但满足条件的传感数据多,敏感数据传输周期较短。因此,在实际应用中应根据数据的实际取值范围合理地选取 N 值。

本文所提出的基于数字水印原则无线传感器网络敏感数据通信协议,具备以下特点:

(1)可实现敏感数据的隐蔽传输。由于水印嵌入算法仅改变了传感数据的最低位,数据变化微小。在不知道原始数据的情况下,很难发现数据中嵌入了水印。达到了敏感数据隐蔽传输的目的;

(2)对原始数据影响小。采用本协议后,仅大于阈值且最低位与水印当前位不一致的值会发生变化,变化结果为值加“1”或减“1”,相对变化率最大为 $1/N$ 。当选取

(下转第 35 页)

(上接第 31 页)

合适 N 值后, 相对变化率可以控制在 1% 以下, 基本上不会影响传感数据的后续应用;

(3) 算法简单, 易于实现。

因此, 该协议能很好地应用于无线传感器网络需要传输敏感信息的场合中。

参考文献

[1] AKYLIDIZ I F, SU W, SANKARASUBRAMANIAM Y, et al.

Wireless sensor networks: a survey. Computer Networks, 2002.

[2] PERRIG A, SZEWCZYK R, WEN V, et al. SPINS: security protocols

for sensor networks. ACM Wireless Networks, 2002, 8(5): 521–

534.

[3] COX J, MILLER M L. The first 50 years of electronic

watermarking[J]. Journal of Applied Signal Processing, 2002

(2): 126–132.

[4] COX J, KILLIAN J, LEIGHTON F T, et al. Secure

spread spectrum watermarking for multimedia[J]. IEEE

Transactions on Image Processing, 1997, 6(12): 1673–1687.

[5] BRASSIL J, LOW S, MAXEMCHUK N F, et al. Electronic

marking and identification techniques to discourage

document copying[J]. IEEE Journal on Sel. Areas in

Commun. 1995, 13(8): 1495–1504.

[6] BRASSIL J T, LOW S, MAXEMCHUK N F. Copyright

protection for the electronic distribution of text documents

[J]. Proceedings of the IEEE, 1999, 87(7): 1533–1536.

[7] ATALLAH M J, RASKIN V, CROGAN M, et al,

Natural language watermarking: design, analysis, and a

proof-of-concept implementation. In Proc. Int. Workshop

on Information Hiding, 2001(2137) 185–199.

(收稿日期: 2009-08-15)

《微型机与应用》2009 年第 24 期

欢迎网上投稿 www.pcachina.com 35