Copyright Protection in Wireless Sensor Networks by Watermarking

Rong Xiao, Xingming Sun, Ying Yang

School of Computer and Communication, Hunan University, China
{ruong.x@gmail.com, sunnudt@163.com, yingyuang@gmail.com}

Abstract

Since the data of wireless sensor networks play an important role in the communication, many strategies have been devised to protect the security of sensor networks. Due to the importance of copyright protection for valuable sensor data, we present a robust watermark algorithm as the solution in this paper. We make use of the numerical characteristic of sending time of the sensor packet to embed watermark. We compare the performance of three watermarking schemes, i.e., the method without key, the method with 8-bit key length, and with 16-bit key length, through conducting lots of simulation experiments. Simulation results show that our scheme can effectively protect the copyright of data while obtaining the tradeoff on computational cost.

1. Introduction

Copyright protection issue has drawn much attention in behalf of the originators of the works. Thus, many methods as the solutions to such problem have been proposed in the past few years and successfully applied to images [1], text [2], hypertext [3], videos [4], audios [5], etc.

The application[19-21] of wireless sensor networks refers to many fields such as military surveillance, CO or CO2 gas monitoring in coal mine, toxic gases monitoring in chemical industry and forest fire monitoring etc., however, the copyright protection problems of the wireless sensor networks are not sufficiently studied. Although some approaches [6-8] related to the security of the wireless sensor networks have been presented, they all may not protect the copyright of the sensing data. For instance, a malicious adversary [12-14] may duplicate segments of the valuable sensor data [15, 16] for profit. Therefore, copyright protection becomes urgent and necessary.

Digital watermarking [9, 10] as a promising technique to protect the copyright has been widely studied. Sion et al. [10] first introduced and studied the issue of the rights protection for sensor streams data through watermarking and analyzed its resilience to attacks. They also proved that watermarking is well suited for the sensor networks. In addition, Feng et al. [9] developed the first watermarking system by embedding the cryptologically encoded authorship signatures into the data and information acquired by the wireless sensor networks during atomic trilateration process. The scheme also provided favorable tradeoffs between the accuracy and the strength of proof of the authorship.

However, there are more challenges [17-19] in the wireless sensor networks by taking advantage of digital watermarking as copyright protection. Being able to protect against such infringements, in this paper, we first analyze the format of the sensor packet. It provides specific fields to record corresponding information such as sending time of the packet, source address of the packet, destination of the packet, storage space of the data etc. The data section is not suit for embedding watermark. It is because that even if we embed watermark into data section, no matter how to manipulate secretly, it inevitably changes the value of the sensing data. We know the sending time of the packet adopts float-point precision after analyzing the time section. Define the structure of the sending time as 1 byte (8 bits), thus, if the modification is only performed in the LSB (least significant bit) of the sending time, this error is absolutely acceptable in the wireless sensor network. If higher precision is used to represent the sending time, the error resulted from modification will be further reduced.

In light of the fact mentioned above, we propose a robust watermarking algorithm by taking advantage of the characteristic of the sending time to protect copyright. In addition, we design our strategy from following two considerations: 1) the secure strategy should be connected tightly with application; 2) we should ensure the equilibrium between the intensity of computation and security.

The remainder of the paper is organized as follows. Section 2 describes the introduced research methodology in detail and gives the pseudo-code of the
main algorithms. In Section 3, the experimental results are described and analyzed. Finally, we draw the conclusions of our work in Section 4.

2. Research methodology

Many secure works available in the literature focus on either encryption and secure protocol or watermarking scheme. However, they cannot efficiently protect the copyright of the sensor data. To address the issue, our work makes use of the invisible character of watermark to conceal itself in the sensing packets. Note that our watermark adopts the identification number of the sensor node, which is used as the solution of copyright protection.

In this section, we make network and node assumptions first, and then study our watermark scheme which refers to two sub-processes: watermark embedding process and watermark extracting process.

We make four assumptions to the wireless sensor networks. First, we assume the base station is robust and of enough power to deal with the numerous packet information. Second, we assume that all sensor nodes are the same and static in the wireless sensor networks. Third, we assume each sensor can loosely synchronize its time with base station. Finally, we assume that the routing and transport protocols such as directed diffusion have been carried out in each sensor node.

2.1. Watermark embedding Algorithms

In the work, we select the sending time for embedding watermark. It enhances the capacity of against-detecting of algorithm and the capacity of hiding because the sending time is different in each packet. Since modification is only performed in the LSB (least significant bit) of the sending time of each packet, we need several packets to transmit watermark. Our watermark is set 8-bit, so every eight packets to transmit one watermark in the work. Note that the watermark adopts the character of watermark to conceal itself in the sensing packets.

In the embedding process, we firstly find the position where the watermark bits have been embedded in the sending time of packet. Next, we extract the embedded bits by manipulating the embedding bit of the sending time and then decrypt it with the secret key. We can regard the sensing packet is of legal derivation by validating the right watermark. Even if an adversary acts as a normal node to send packets, we can distinguish them as counterfeit according to the extracted watermark. Our work never changes the sampling data and never extends extra space to original packet.

The pseudo-code of data recovery phase is also presented in Algorithm 2.

---

### Algorithm 2 Watermark Extracting Process

**Input:** sensing packet $P$

**Output:** watermark $w$

**Steps:**

1. read sensing packet $P$ into data buffer $buff$
2. initialization, $P.data=P.data\&0xff00$;
   $nu[8]=0x0ff; lower=0x01; cnt=-1$; go to 4)
3. read watermark into data buffer $buff$
4. $P.data=key\ P.data$
5. $m.data=hash(P.data')$
6. if $i<8$ then
7. $m.data=m.data@(watermark>i)$
8. else
9. $i=0$; go to 3)
10. end if
11. for $i=0$ to 8
12. $stime[i]=sent_time[i]\&nu[i]$
13. end for
14. $stime[0]=stime[0]|((m.data)>>cnt)\&lower)++cnt$;
15. $cnt=cnt%8$

---

2.2. Watermark extracting Algorithms

In the extracting process, we firstly find the position where the watermark bits have been embedded in the sending time of packet. Next, we extract the embedded bits by manipulating the embedding bit of the sending time and then decrypt it with the secret key. We can regard the sensing packet is of legal derivation by validating the right watermark. Even if an adversary acts as a normal node to send packets, we can distinguish them as counterfeit according to the extracted watermark. Our work never changes the sampling data and never extends extra space to original packet.

The pseudo-code of data recovery phase is also presented in Algorithm 2.

---

Algorithm 1 Watermark Embedding Process

**Input:** sensing packet $P$, watermark, $key$

**Output:** sensing packet $P$

**Steps:**

1) read sensing packet $P$ into data buffer $buff$
2) initialization, $P.data=P.data\&0xff00$;
   $nu[8]=0x0ff; lower=0x01; cnt=-1$; go to 4)
3) read watermark into data buffer $buff$
4) $P.data=key\ P.data$
5) $m.data=hash(P.data')$
6) if $i<8$ then
7) $m.data=m.data@(watermark>i)$
8) else
9) $i=0$; go to 3)
10) end if
11) for $i=0$ to 8
12) $stime[i]=sent_time[i]\&nu[i]$
13) end for
14) $stime[0]=stime[0]|((m.data)>>cnt)\&lower)++cnt$;
15) $cnt=cnt%8$

---

2.3. Security analysis

In this subsection, we provide a theoretical analysis of the security of our scheme. How to design a better secure scheme to achieve the secure sampling and
Transmission and cut down the expenditure of network at the same time is the goal in common. However, in this paper, our work aims at copyright protection, so we pay attention to ensuring the security of the hiding of watermark, and we do not consider the complex mechanism of encryption in packet for one bit of watermark is embedded in each packet. We acquire an exclusive mapping relation by adopting the predigest idea of MD5 algorithm to compute hash value of sensing data. Even if an adversary intercepts and captures the encryption algorithm, he/she cannot acquire the embedding information because of the complexity of decrypting. Next, we manipulate xor operation of the value produced by mapping relation and the bit be embedded. The mapping value of our algorithm is of (0, 1) uniform distribution and the mapping relation is one-way, irreversible process. The above measures we add to our algorithm are necessary to ensure the secure and reliable transmission of watermark.

3. Experimental Results

3.1. Setting

Our experiments are carried out in a simulated network. The sensor nodes in our simulation tests are randomly distributed. More basic settings on simulation information are listed in Table 1.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>The max size of X</td>
<td>2000</td>
</tr>
<tr>
<td>The max size of Y</td>
<td>2000</td>
</tr>
<tr>
<td>Number of nodes</td>
<td>110</td>
</tr>
<tr>
<td>The size of Packet</td>
<td>1000</td>
</tr>
<tr>
<td>Interval time</td>
<td>20.0</td>
</tr>
<tr>
<td>Initial Power</td>
<td>2</td>
</tr>
</tbody>
</table>

3.2. Simulation results

Through conducting lots of simulation experiments, we compare the performance of three watermarking algorithms, i.e., the method without key, the method with 8-bit key length, and with 16-bit key length. From figure 1, we can draw the conclusion that the transmission rates of the watermark algorithm whose key length is 8 bits are 112%~115% times longer than those of watermark algorithm without key.

4. Conclusions

In this paper, we propose a watermarking algorithm to protect the copyright of the sensor packets. Our strategy aims at protecting the embedded watermark of sensor packets. We verify the scheme from both theoretical analysis and simulations. We can protect the security of watermark effectively while obtaining the tradeoff on computational cost.

Our future work will focus on the robust analysis of watermark under the circumstance that adversaries launch on different attacks.

Acknowledgements

This work is supported in part by National Basic Research Program 973 (No. 2006CB303000), in part by National Natural Science Foundation of China (No. 60573045), and in part National Natural Science Foundation of China (No. 60736016).

5. References


