12

The Digital Watermarking Techniques Applied to Smart Grid Security

Xin Yan and Yang Wu
Department of Computer Science, Wuhan University of Technology
P. R. China

1. Introduction

Power supply in the 21st century is facing more and more challenges, e.g., environment protection, energy shortage etc, such that the techniques related to power supply imminently need to be promoted. Complying with the development of green and low-carbon economy, the concept of Smart Grid has been proposed. By and large, Smart Grid may be regarded as an important application of the techniques of wireless sensor networks and Internet of Things etc in power grid. Smart Grid should be a complicated integrated system with high security, which involves many aspects, e.g., the security of power generation equipments, the security of power transmission equipments, the security of data communications, and so on. Nonetheless, Smart Grid is an open and inclusive system, which makes it unsafe inevitably.

The traditional security methods use cryptography to encrypt data for transmissions, for instance, data encryption, data integrity protection, and two-way authentication etc. The data communication networks employed by Smart Grid involve cable and wireless communication networks. Here wireless communication networks usually refer to wireless sensor networks (Akyildiz et al., 2002). Due to the limited resources at sensor nodes, cryptography methods will seriously abate the life time of sensor nodes. The reason is that encryption algorithms usually need to consume more energy, time, and memory space to compute and store data (Kleider et al., 2004; Zia & Zomaya, 2006). Anyway, the traditional encryption methods are not suitable for handling the security issue of data communications in Smart Grid. Thus, this chapter will investigate how to apply a digital watermarking technique to solve the security problem of data communications for wireless sensor networks in Smart Grid.

2. Smart Grid and wireless sensor networks

Smart Grid is an intelligent network built in some integrated, high-speed, two-way communication networks. Its objective is to implement the power reliability, security, and efficiency, as well as clean energy supply by using advanced sensor technology, measurement technology and advanced decision support systems. Smart Grid transmits a wide variety of data, including the key equipment operation parameters, the power facility information, the power distribution and scheduling information, the electricity usage state, early warning information, and so on (Divan & Johal, 2006). By using the rich information, Smart Grid can efficiently control the power generation, transmission, distribution, scheduling, and sub-time pricing, as well as timely error check etc (Amin & Wollenberg, 2005). The hierarchical model of information flows in Smart Grid is shown in Fig. 1.

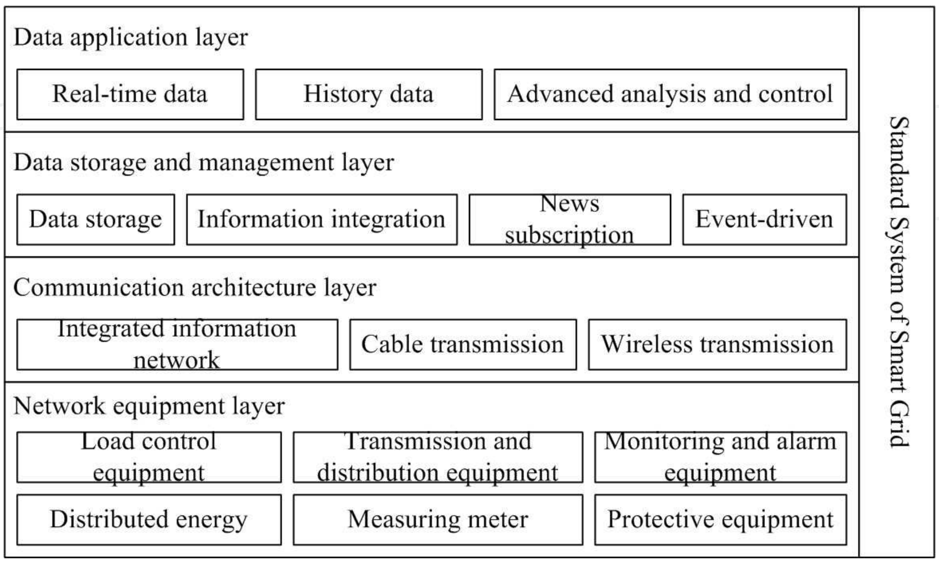


Fig. 1. The hierarchical model of information flows in Smart Grid

The communication networks related to Smart Grid consist of cable networks and wireless networks. The wireless networks mainly refer to wireless sensor networks that are usually used in some places where cable networks are not applicable to deploy or wireless sensor networks is more suitable. Smart Grid has a remarkable feature that its networks must be safer than other networks for general purposes. That is to say, Smart Grid must withstand the physical destructions and malicious network attacks without blackouts or a high cost of recovery (Perrig et al., 2004). Smart Grid security involves many aspects, where the data transmission security is one of the most important issues. Since the security mechanisms and techniques in cable networks are already quite rich and mature, we focus on trying to improve the security of the data in wireless sensor networks for Smart Grid.

Wireless sensor networks are a multi-hop self-organized network system, which contains a large number of miniaturized sensor nodes. These sensor nodes are distributed in a monitored area, and communicate in a multi-hop ad hoc way. They collaborate with each other to collect the sensitive information of monitored objects, and send them to a decision support center. The functions of wireless sensor networks consist of data collection, data transmission, and data analysis and processing. A sensor node, the smallest logical unit of wireless sensor networks, is a micro-system, which is integrated by sensor modules, data processing modules and communication modules. Sensor nodes build up wireless links to form a self-organized and distributed network architecture, depending on a certain network routing protocol that can fuse and aggregate the collected data and transmit them to the information processing centre (Chen et al., 2009). A network architecture of wireless sensor networks is shown in Fig. 2.

Smart Grid involves a large number of wireless sensor networks, so the data transmission security is an important issue in Smart Grid. However, due to wireless sensor networks with the large magnitude of energy-constrained sensor nodes and the high network dynamics caused by the node mobility or node failure, there still exist a lot of potential threats to the security of wireless sensor networks (Wang et al., 2006), e.g.:

1. The unauthorized interception of information. A sensor node transmits information to others by broadcasting, so any of communication devices within its RF radius may receive and intercept the information.
2. Sensor nodes are vulnerable to be captured easily. We must take into account what measurements should be taken to fight against, while a sensor node is captured and used as a pseudo terminal to launch malicious attacks.
3. In the practical environments, we must also consider which routing schemes should be adopted, in the case that some of sensor nodes do not work because of failures or attacks.
4. Tampering with information is usually regarded as the most dangerous attack. The tampered information can be spread throughout networks like normal messages, which can attack or even control the whole networks.

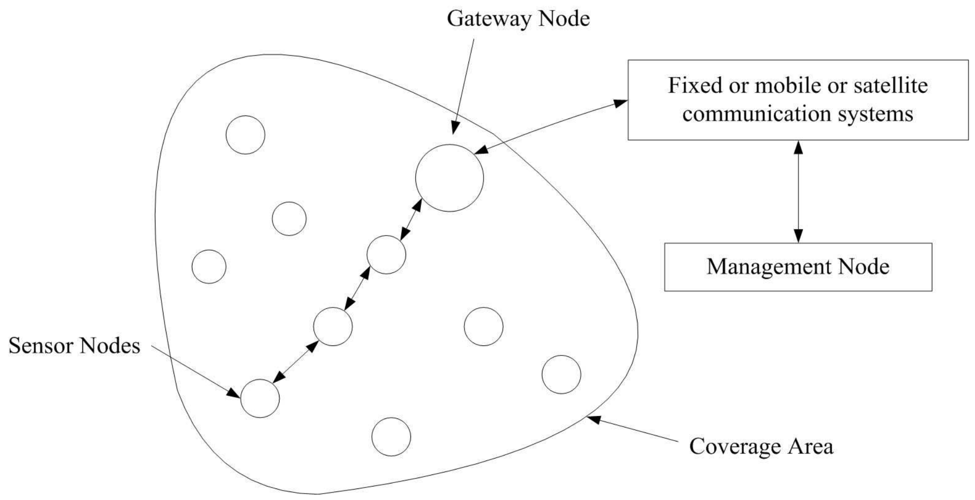


Fig. 2. A network architecture of wireless sensor networks

These potential threats to wireless sensor networks cause unsafe data communications in Smart Grid. To obtain safe communication services from Smart Grid, we must solve the security issues about wireless sensor networks. However, because of the differences between wireless sensor networks and traditional networks, the security policies for wireless sensor networks should not be borrowed directly from the existing mature security solutions for traditional networks. The security policies should be more suitable for wireless sensor networks. Data encryption methods are widely used in traditional networks, where the information needed to be protected is generated to cipher-text information without readability or obvious correlation. Nevertheless, the resources of computation and storage at sensor nodes are scarce and limited. The traditional data encryption methods will seriously consume the expensive resources at sensor nodes, because they require more power and memory space to accomplish the data encryption procedure. Therefore, we need to use digital watermarking methods to implement the security policies in wireless sensor networks, because digital watermarking needs much less resources at sensor nodes than traditional data encryption (Xiao et al., 2008).

3. Digital watermarking

Digital watermarking is a special kind of information hiding techniques, which is used to detect piracies or illegal copies. The watermark is transmitted with the information embedded identity in a digital form. Digital watermarking technique is suitable for the data-centric wireless sensor networks. Reasonable watermarking algorithms can ensure the data security at a low cost of operation, and tolerate effectively the impacts from data processing. Using digital watermarking techniques to solve the security issues in the wireless sensor networks for Smart Grid is a practical and effective solution (Xiao et al., 2007).

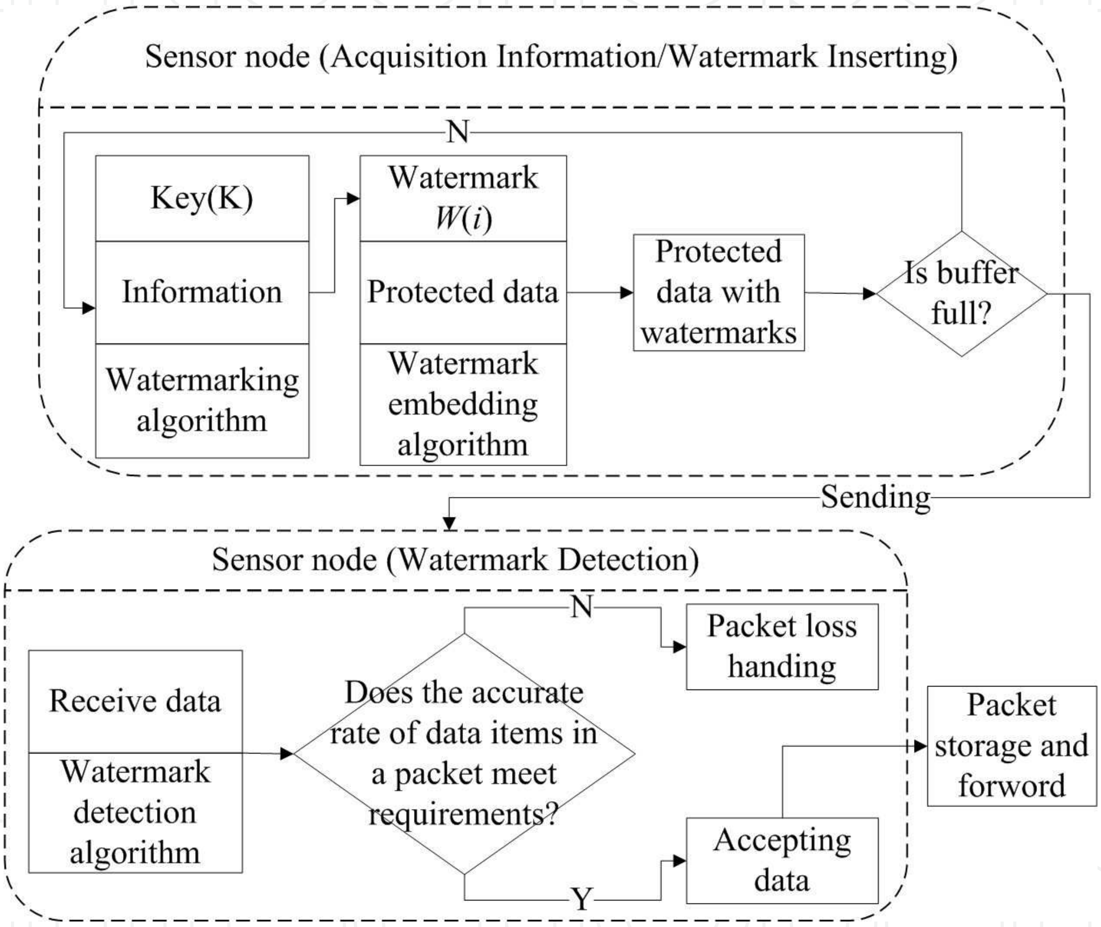

Sensor node (Acquisition Information/Watermark Inserting)
N
Key(K)
Information
Watermarking algorithm
Watermark W(i)
Protected data
Watermark embedding algorithm
Protected data with watermarks
Is buffer full?
Sending
Sensor node (Watermark Detection)
N
Packet loss handing
Receive data
Watermark detection algorithm
Does the accurate rate of data items in a packet meet requirements?
Packet storage and forword
Accepting data
Y

Fig. 3. The operation procedures of watermarking

Digital watermarking algorithms consist of three basic procedures: watermark generation, watermark embedding, and watermark extraction or detection. The main idea of watermarking algorithms is that watermarks are generated by watermark generation algorithms, and then are embedded into the data collected by sensor nodes. The watermark information is stored in the memory at a node before the data in this node is transmitted. The destination nodes operate the watermark detection in terms of the designated keys and parameters. Only the data with correct watermarks can be considered reliable, meanwhile, it must be eligible for storing and forwarding. Otherwise, it is considered counterfeit or damaged, and discarded directly (Feng & Potkonjak, 2003). The detailed operation procedures about watermarking are shown in Fig. 3.

In this chapter, based on alternating electric current and time window respectively, we propose two digital watermarking algorithms in wireless sensor networks for the data transmission security of Smart Grid.

4. Digital watermarking algorithm based on alternating electric current

4.1 Algorithmic process

4.1.1 Watermark generation

The electric current on electric transmission line is alternating, which means its current value and direction change periodically. In addition, the electric current is a monotonic function of time, a sine trigonometric function. That is to say, both current intensity and orientation are a unique value at any given time within a cycle. These features of alternating electric current are ideal for watermark generation (McDaniel & Mclaughlin, 2009). We use the alphabet *I* to represent the electric current. Physically, it is a vector that contains the information of both its value and direction. As electric current is periodic, the value may be equal although the current direction is different at different times. In order to generate diverse watermark information, we make some special changes to the reverse electric current before watermark generation (Cox et al., 2007).

Suppose the format of a sent packet is Packet = (Head, Send_Data), where Head is the packet’s head including routing information, data type, and packet length etc. Send_Data is the data which the sensor node sends at a time. It is also the buffer content at the sensor node when its buffer is full. Send_Data contains a variety of collected data items, and the current at the moment of the data item acquisition. Send_Data = (Data[1], Data[2], Data[3], …, Data[*n*]), where Data[*i*] (*i* = 1, 2, …, *n*) represents one of the data items collected by the sensor node. Its data type definition is shown in Fig. 4.

```
Typedef struct Data_info  {
    I;
/*The current at the moment of the data item acquisition, a vector*/
    Kernal_data;
/*Kernel data, which is the protected data*/
    Flag;
/*Boolean value, which identifies whether this data item has
watermark*/
} Data[i]
```

Fig. 4. The data type definition of Send_Data

Suppose that a packet consists of Head and *m* data items in a collection cycle. The watermark generation algorithm is described as follows:

1. Taking out each data item from Send_Data.
2. Using single hash function to compute its hash value, according to the key and electric current *I* at the moment of data collection. This step can be described as a program statement hsh[*i*] = Hash(Key, Data[*i*].*I*).

3. Getting the most significant bit in hsh[*i*]. The corresponding statement is MSB(hsh[*i*]).
4. Taking Num binary bits from MSB(hsh[*i*]), then XOR them. The result *W*[*i*] is the watermark of data item Data[*i*].

The detailed steps in the watermark generation algorithm are shown in Fig. 5.

```
Generate_W (Data[$i$], Key, Num)  {
    If (Data[$i$].$I$ > 0) then
        $I'$ = Data[$i$].$I$
    Else
        $I'$ = Translate(Data[$i$].$I$)
        /*Making some changes to the reverse current in order to generate a
        variety of watermark*/
    End if
    hsh[$i$] = Hash(Key, $I'$ );
    $W$[$i$] = Produce_W(MSB(hsh[$i$]), Num)
    /*MSB(hsh[$i$]) means obtaining the most significant bit, and the function
    Produce_W means XOR to generate watermark of Data[$i$].*/
    Data[$i$].Flag = 0
    /*Initializing the value of the flag bit before watermark embedding*/
}
```

Fig. 5. The meta-code of the watermark generation algorithm

4.1.2 Watermark embedding

To minimize the varying range of data, only the watermark at the least significant bit of data item is embedded. Considering the fact that the energy at sensor nodes is limited, the watermark algorithm should be designed concisely, so we take the following two measures:

1. Selecting some items randomly from the data items (i.e., Data[1], Data[2], Data[3], …, Data[*m*]) to embed watermark, which can reduce the computational complexity.
2. Deriving the least significant bit of data item Data[*i*], which will be embedded watermark; and selecting some fixed binary bits of the least significant bit, which are the watermark embedding positions. That can simplify the watermark extraction.

The embedding algorithm uses the same key as the generation algorithm. The scaling parameter *u* is selected in terms of the requirements to security, which is used to control the percentage of data items needed to be embedded watermark. We only insert watermark into the data items whose random numbers can divided by *u*. Macroscopically the value of *u* reflects the dense degree of data items embedded watermark in a packet. Larger the value of *u* is, and smaller the probability of related data items inserted watermark is. After determining which data item should be inserted into watermark, we can get the watermark information by using the algorithm in Fig. 5. Next we insert it into the fixed position of the data item's LSB (the least significant bit). The detailed steps of the watermark embedding algorithm are shown in Fig. 6.

```
Embed_W (Send_Data , Key, Num, $u$) {
 For $i$ =1 to $m$
   Generate_W (Data[$i$], Key, Num)    /*Generating watermarks*/
   MSB_Data = MSB(Data[$i$].Kernal_data)
   rd = random (Key, Data[$i$].$I$, MSB_Data)
   If (rd mod $u$ = 0)  then
/*Determining which data item will be embedded watermark*/
      Select_Bits (LSB(Data[i].Kernal_data))
/*Selecting some fixed binary bits from LSB as the embedded
positions*/
       Embed watermark WM[$i$] in the fixed bits
       Flag = 1
   End if
 End for
}
```

Fig. 6. The meta-code of the watermark embedding algorithm

4.1.3 Watermark detection algorithm

The structure of received packet is the same as that of sent data. In order to illustrate it clearly, we describe a received packet as Packet_R = (Head, Receive_Data), where Receive_Data is the content of received packet with watermark information. The watermark detection process is as follows:

1. The node reads each data item in a received packet.
2. Retrieving the state of each data item's flag bit. If the flag is 1, the function Get_LSB (Data[i]) obtains the data item's watermark W', and compare W' to W = Generate_W (Receive_Data[i], Key, Num). If they are same, it means the data item Data[i] is safe.

However, the security of a data item does not ensure the packet is safe. In order to measure the security of a packet, we introduce a threshold parameter P. It represents the correct watermark rate of all data items in a packet, which shows the authentic level of all data items in a packet. If the watermark detection rate of all data items in a packet is larger than P, we say that the credibility of this packet's contents is fully consistent with the requirements. The packet is correct and acceptable; conversely, it should be dropped by the corresponding node. The meta-code of the watermark detection algorithm is shown in Fig. 7.

4.2 Performance analysis

We employ Matlab7.0 as our experimental network environment. The coordinate area of simulation configuration is 40m * 100m, and a total of 50 sensor nodes are distributed uniformly. We draw out 300 packets to analyze, and initialize each node's energy to 2 joules. In order to facilitate and simplify the simulation, the electric current value is measured as follows. The watermarking algorithm makes use of its value directly if the current value is positive. When it is negative, we multiply the current value by a constant, then use the transformed values to generate watermark.

```
Detect_W (Receive_Data, Key, Num, $P$) {
 Right_count = W_count = 0
/*Right_count is the total number of data items that can be correctly
detected the watermark in a packet. W_count is the total number of data
items that contains watermark in a packet*/
 For $i$ = 1 to $m$
   If (Receive_Data[$i$].Flag = 1) then
       W_count = W_count + 1
       $W'$ = Get_LSB (Receive_Data[$i$])
       $W$ = Generate_W (Receive_Data[$i$], Key, Num)
   End if
   If ( $W' = W$ ) then    /*The watermark information is correct*/
        Right_count = Right_count +1
    End if
   End for
   If (Right_count/W_count > $P$) then
       Receive this reliable packet and forward it
   Else
       Drop this packet
   End if
}
```

Fig. 7. The meta-code of the watermark detection algorithm

Before evaluating the performance of this watermarking algorithm, it is necessary to verify that it is reasonable and viable for data security by experiments. Here we can reach the experimental goal by comparing the received watermarked message from a certain data packet to its original watermark message, as shown in Table 1 (three data packets are selected, i.e., Packet 1, Packet 2, and Packet 3). Next, we analyzed the algorithm's performance from three aspects: the security of algorithm, the network throughput, and the node energy consumption.

4.2.1 The security of algorithm

We evaluate this algorithm's security according to the statistics of its probability of handling the data correctly. For this purpose, we introduce the formula of algorithm detection rate.

$$P\_Dective = \frac{Dective\_Sum}{\mathrm{Re}ceive\_Sum} \tag{1}$$

Wherein *P_Dective* is the detection rate of packets, and *Dective_Sum* is the number of packets whose watermark are correctly detected. *Receive_Sum* is the total number of received packets. In this experiment, we add 7 attacking nodes, 3 camouflage nodes, and assign different values to the embedding parameter u at the same time. The results are shown in Fig. 8. Different values of parameter u have different impacts on the detection rate to some extent. Larger the value of parameter is, and less the detection rate is. The reason is that the larger value of u, the smaller probability of embedding watermark in data items, correspondingly, the less amount of watermark information the packet contains. But when *u* takes a smaller value, the detection rate is still quite large (nearly above 95%) regardless of the number of packets increasing. From the experimental results, we are able to anticipate that this algorithm can efficiently operate with a high security when the proper value of *u* is chosen.

Watermarks in Packet 1		Watermarks in Packet 2		Watermarks in Packet 3	
Original	Received	Original	Received	Original	Received
1010	1010	1110	1110	1011	1011
1101	1101	1001	1000	1001	1001
1000	1001	1111	1011	0000	0000
0110	0110	0001	0001	1110	0110
1011	1011	0011	0011	1010	1010
1010	1010	1011	1011	0010	1010
1011	1000	1001	1001	1000	1000
1001	1001	1000	1000	1101	1101
0110	0110	1110	0111	0111	0110
0111	0011	0000	0101	1111	1111

Table 1. The comparison received watermarks to original watermarks in 3 data packets

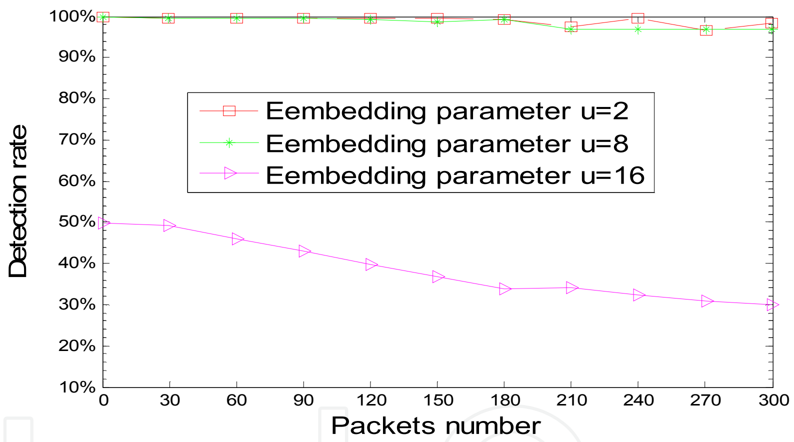


Fig. 8. The comparison of the securities

4.2.2 Network throughput

An important advantage of digital watermarking is that it does not increase the burden of network transmission. In this algorithm, we replace the most important part of the carrier with the watermark through the least significant bit (LSB) method, which does not import an additional data for the original data. Therefore, digital watermarking technique can maintain the throughput of the original network well, as shown in Fig. 9.

In general, the throughput of the networks without watermark information is slightly larger than that of ones with embedded watermark. At the beginning, the number of the nodes forwarding packets is smaller, such that the network is unimpeded and faster. Thus, the network throughput increases rapidly. But as more and more nodes begin to transmit packets, the number of sent packets increases, which leads to a slight decline in the throughput of the networks with watermarks because of the watermark embedding and the data operation frequently. At last, with the end of data collection, forwarding, transportation, and processing etc, the network throughput becomes less and less. From the experimental results, the digital watermarking technique can effectively protect the packet transmission. Moreover, it does not increase the burden of network throughput.

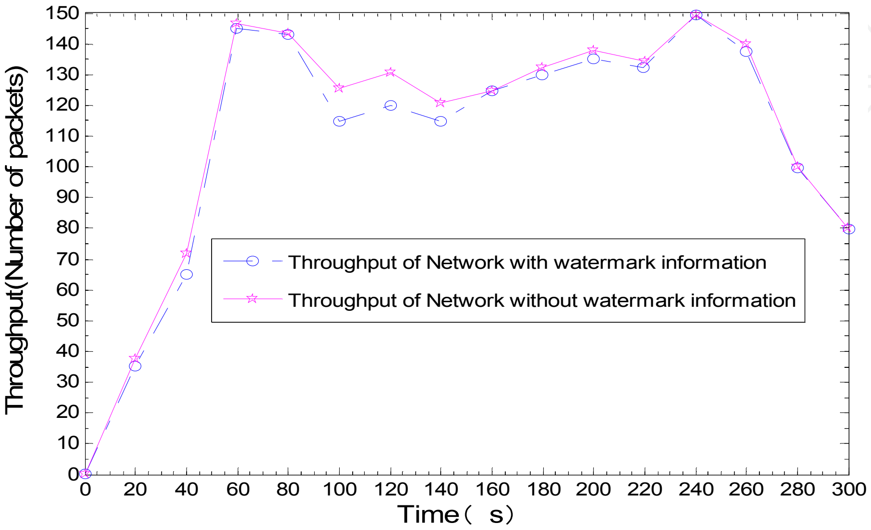


Fig. 9. The comparison of the network throughputs

4.2.3 The node energy consumption

Since the complexity of this watermarking algorithm is $O(m)$, it does not increase the energy cost at sensor nodes, when processing the watermark information. In addition, the watermark is directly embedded into the data item, which does not take up additional storage space at the node. So the node energy is mainly consumed on data transmission process. Therefore, the digital watermarking technique can well meet the requirement that the energy at sensor nodes is limited in wireless sensor networks. Table 2 is the energy consumption statistics of some nodes.

Node number	Node energy consumption (with watermark)	Node energy consumption (without watermark)
1	90	85
3	35	31
6	88	86
7	20	20
9	80	65
12	78	75
16	105	96
23	43	39
25	57	50
33	113	100

Table 2. The energy consumption at a part of nodes (unit: micro joule)

In the experiment, the energy consumption at the nodes that communicate with lots of neighbours is higher. On the contrary, the energy consumption at the nodes with less traffic is lower. Overall, the differences of energy consumption are quite slight in spite of the node with watermark or not.

5. Digital watermarking algorithm based on time window

5.1 Algorithmic process

According to the characteristics of time zone storage format of packets in wireless sensor networks and the digital watermarking, we proposed another new digital watermarking algorithm based on time window. At first, we defined the format of packets with encapsulated format, and divide the packet into eleven parts. The contents of each part are described in Table 3.

1	2	3	4	5	6	7	8	9	10	11

1: Beginning mark of message	7: Group ID
2: ACK	8: Length of data
3: Destination address	9: Content of data
4: Source address	10: CRC
5: Packet type	11: End mark of message
6: Time of sending packet	

Table 3. The definition of packet format

We use one byte to store the sending time of the packet, and set it to the float type. If we operate the lowest bit of this byte with 0 or 1, its value will be certainly changed. However, this change is quite slight, only between -0.3% and 0.3%. The higher accuracy we use, the smaller impact it will be. The offset value is always at the range of the sensor's tolerance deviation. Time information is recorded in the 6th fixed field of the packet format, so it is the lowest bit of the value. In this case, the sensor for different usages will not be affected even if the lowest bit of the time information is changed.

And then, we introduce the watermark embedding and detection algorithms based on time storage format. At first, we deal with the data area (i.e., the 9th field) of a packet by the MD5 algorithm, and get a unique mapping. After that, let the value which is generated by this mapping XOR the watermark. At last, embed the result into the hidden bit. The mapping is one-way and irreversible, such that the watermark adding to this mapping can ensure the better reliability of the transmission (Katzenbeisser & Petitcolas, 2000).

5.1.1 The watermark embedding

The watermark embedding procedure consists of the following four steps (see also Table 4 in detail):

1. Firstly, we select the 4th field of a packet as the original information *M*, and then operate the original information *M* with the key *K* and the watermark generation algorithm *G*. Then we get the watermark *W*.

```
Input: Information packet, and the key $K$
Output: The document embedded information, packet′

1. $W \leftarrow G(M,K)$
2. If (the data buffer is not full) then
3.     Continue collecting to fill the data buffer
4. Else
5.     $X' \leftarrow$ message_hash ($X$,$K$)
6. End if
7. For  $i$ = 0 to 8
8.   If (the $i$'s value is less than the size of the data buffer) then
9.       $X_i'' = X_i' \oplus W_i$
10.      $i = i + 1$
11.  Else
12.      Go to loop 15
13.  End if
14. End for
15. $T_{lsb} = Em(X'', K)$
16. Using CRC algorithm to calculate the designated data in the packet
17. Output packet′
```

Table 4. The process of the embedding watermark based on time window

2. Secondly, calculate the hashing value of the data items of the packet with the MD5 algorithm, and then get a hashing value hsh which is mapping with the data items of the packet.
3. Third, let hsh XOR *W*, and embed the results into the lowest bit of the time information (i.e., the 6th field of the packet).
4. Finally, use CRC algorithm to check from the 3rd to the 9th field in the packet, and put the results into the 10th field in it.

5.1.2 The watermark extraction and detection

After transmitting through the relay nodes, packets will reach the base station. We will extract and detect the watermark.

As shown in Table 5, we use CRC algorithm to check from the 3rd to the 9th field data in the packets, and compare the results with the content in its 10th field. If they are not same, the packet should be discarded. Otherwise, we get the embedded data from the lowest bit in the time information, and then extract the watermark *W*′ with the watermark extraction algorithm. At last, we compare *W*′ with W''. If they are equal, the packet is accepted; if not, it will be discarded.

5.2 Performance analysis

We investigate the efficiency of the algorithm and its network performance by simulation experiments. The experimental configuration in Matlab7.0 is described as follows. The coordinates area is 40m * 100m, and a total of 50 sensor nodes are distributed. There are 300

```
Input: The document embedded information packet′, and the key $K$
Output: The information packet

1. Using CRC algorithm to calculate the designated data in packet′
2. Compare its value with the content in its CRC field
3. If (they are same) then
4.     Go to loop 8
5. Else
6.     The packet loss is marked
7. End if
8. $W' \leftarrow get\_data(T_{lsb})$
9. $W \leftarrow G(M,K)$
10. $X' \leftarrow$ message_hash $(X,K)$
11. $W'' = X' \oplus W$
12. If $W'' = W'$ then
13.     The watermark is right, and this packet is accepted
14. Else
15.     The packet loss is marked
16. End if
17. Output packet
```

Table 5. The process of watermark extraction and detection based on time window

packets are drawn out for analysis, and the size of each packet is set to 128 bit. In addition, each node's energy is initialized to 2 joules. We take the embedded value as the source node's ID, and regard the collecting time of data as its sending time approximately. When the parameter configuration is ready, we start to embed watermark and to transmit data. During the transmission, the energy consumption, the processing speed, the time consumption, and all received data at the base station are recorded in different document files.

Similarly, by comparing the received watermark from a received data packet to its original watermark, as shown in Table 6, it can be seen that this watermark algorithm is also reasonable and viable for data security, because it is able to identify those malicious packets. At the end, we probe its performance from four aspects: the security of algorithm, the network throughput, the network delay, and the node energy consumption.

5.2.1 The security of algorithm

The main objective of this algorithm is to find the counterfeit or damaged data and discarded them directly when there are malicious node attacks during network transmissions. Fig. 10 is the comparison of packet loss between the transmissions with embedded watermark and ones without watermarking in a simulation network environment. In this algorithm, the packet loss in the base station consists of two parts: one is the packet loss in the network communication, and the other is the received packets that are malicious and discarded directly. Seen from Fig. 10, the number of packet loss with embedding watermark is more than that without digital watermarking. We should also note

Original watermark	Received watermark
1	1
0	0
0	0
1	1
1	1
1	0
0	0
1	1
0	0
1	1
0	1
0	0
1	1
1	0
1	1

Table 6. The original watermarks and received watermarks in 15 data packets

that the number of packet loss without watermarking algorithm only is the number of the lost packets during the network communication. However, the number of packet loss in wireless sensor networks with watermarking algorithm not only contains the lost packets during the network communication, but only includes the packet loss during the data processing at the base station. In short, from the experiments we can conclude that this watermarking algorithm for wireless sensor networks can implement the function of identifying and discarding the malicious packets.

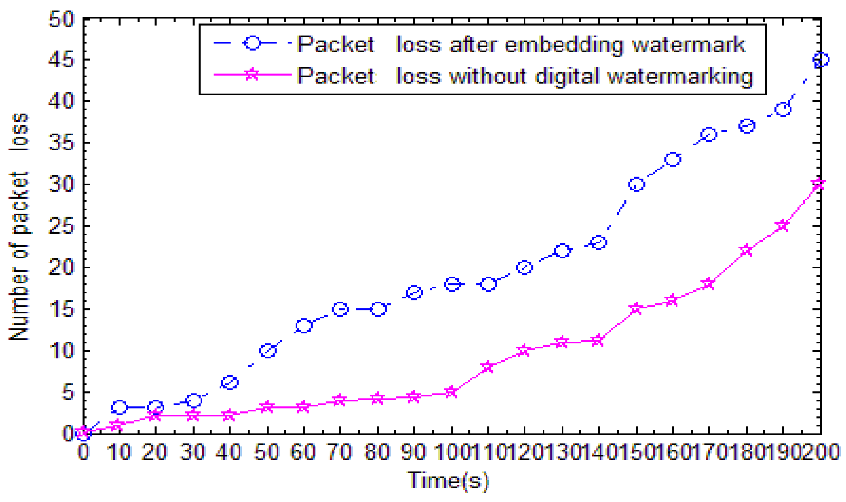


Fig. 10. The comparison of packet loss

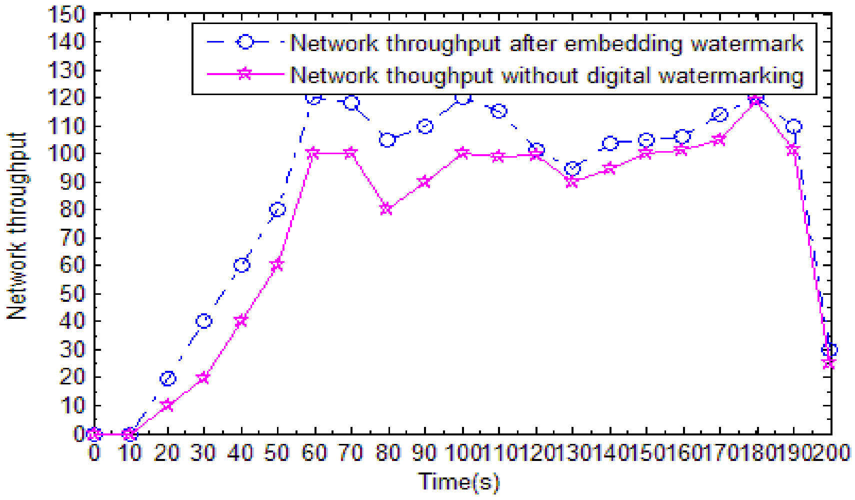


Fig. 11. The comparison of network throughput

5.2.2 Network throughput

It is shown in Fig. 11 that the comparison of network throughput between the wireless sensor networks with embedded watermark and that without watermarking in a simulation network environment. The packets which the whole network can send are changed as the simulation time increases. And the network throughput without watermarking is slightly higher than that containing watermarking, with the maximum throughput difference 20. The reason is that the nodes that transmit and forward packets are less at the beginning, and the network is smooth, fast, and less delay such that the data throughput increases slowly. However, as more nodes join into the transmission of packets, the whole network can send more and more packets. Due to embedding the watermark frequently, the throughput with watermarking algorithm will be slightly slower than that without watermarking. Finally, due to the end of data collection, the number of nodes joining transmission and forwarding gradually become less such that the whole network send less and less packets. And the network becomes smooth with less delay and unaffected data throughput.

5.2.3 Network delay

Generally speaking, the network delay is the interval between the sending time and the receiving time of packets in end-to-end network communication, which consists of the propagation delay, the transmission delay, the queuing delay, and the routing execution delay etc. Fig. 12 is the comparison of network delay between the wireless sensor networks with embedded watermark and that without watermarking. As the simulation time increases, the number of packets which the whole network can send is increasing. At this time, the network delay with watermarking is slightly more than that without watermarking. This reason is that the nodes that transmit and forward packets are less at the beginning, and the network is smooth and fast with less delay. The more nodes join into the transmission, the more packets the base station receives. Due to embedding the watermark frequently in wireless sensor networks with digital watermarking, the network throughput decreases, on the contrary, the network delay increases. Finally, since the transmission comes to a close, the network recovers with less delay.

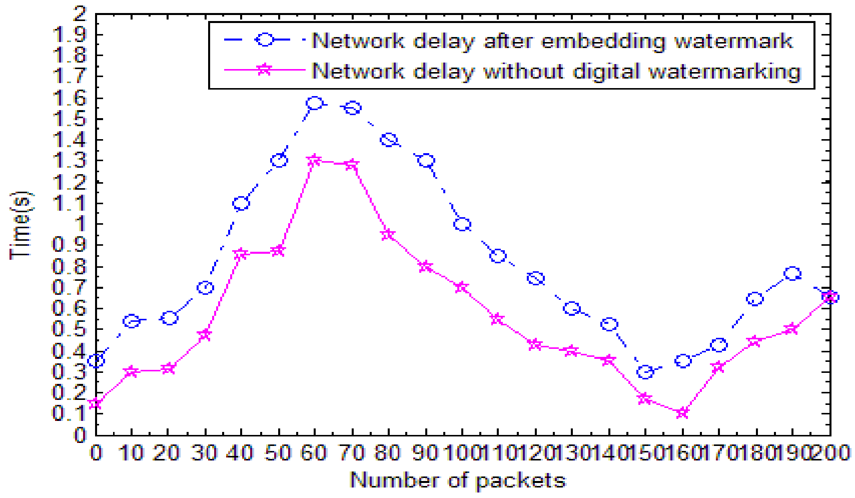


Fig. 12. The comparison of network delay

5.2.4 The node energy consumption

It is shown in Fig. 13 that the comparison of node energy consumption between wireless sensor networks with embedded watermark and that without watermarking in a simulation network environment. The nodes sending data can select their neighbour nodes according to the routing and calculated hop-count to transmit and forward packets. This figure shows that the nodes that frequently use the same path will consume more energy. When a sensor node is failure, the node will automatically select the other neighbor nodes to transmit. However, it will prolong the survival of the entire network. From the figure, we can find that the node energy consumption in wireless sensor networks with watermarking algorithm does not differ much from that without watermarking. Therefore, the digital watermarking based on time window can well meet the requirement that the energy consumption at sensor nodes is limited in wireless sensor networks.

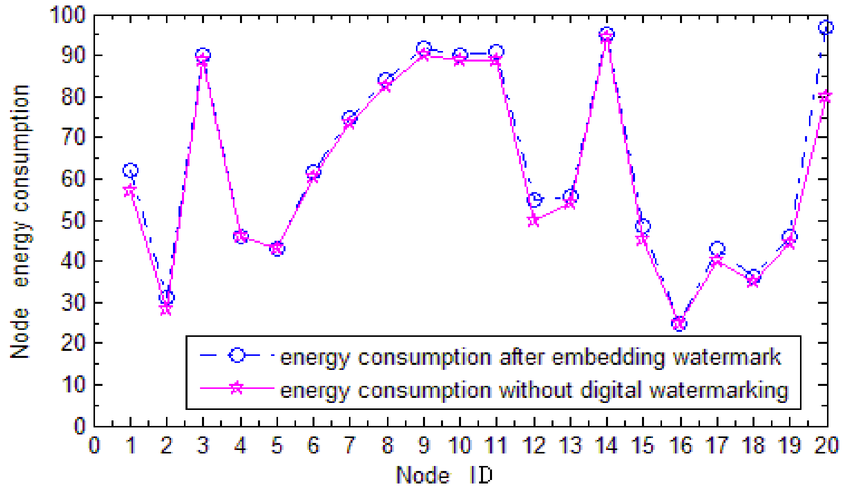


Fig. 13. The comparison of node energy consumption

6. Conclusion

This chapter begins with a general introduction to Smart Grid, wireless sensor networks, and their security issues. Next it is followed up by the basic principle of digital watermarking applied to Smart Grid. The chapter focus on two digital watermarking schemes based on alternating electric current and time window, respectively. Both of them consist of watermark generation, watermark embedding, and watermark extraction or detection algorithms. Afterward, we evaluate the two watermarking schemes from their security, network throughput and energy consumption etc by lots of simulation experiments. The results show that it is reasonable and beneficial to apply digital watermarking to handle the data security in Smart Grid. The watermarking schemes we propose fully take into account the characteristics of both Smart Grid and wireless sensor networks. With the development of wireless sensor networks and digital watermarking techniques, we believe that digital watermarking would play a more and more important role in Smart Grid.

The data communication security in Smart Grid is a comprehensive and complicated research topic. Although some research fruits are obtained in this chapter, there still remain some problems needed to solve. The digital watermarking schemes proposed in this chapter could bring some distortions for data when considering the interference from communication noise. In addition, the robustness of watermark is not explored yet so far. How to design a robust watermarking scheme without distortion is our future work.

7. Acknowledgments

This work is supported by the National Natural Science Foundation of China under Grant No. 61171075, the PhD Program Foundation of Ministry of Education of China under Grant No. 200804971030, and the Visiting Scholarship of State Key Laboratory of Power Transmission Equipment & System Security and New Technology (Chongqing University, China) under Grant No. 2007DA10512710407.

8. References

Akyildiz, I. F.; Su, W. & Sankar, Y. (2002). Wireless Sensor Networks: a Survey. *The International Journal of Computer and Telecommunications Networking*, Vol.38, No.4, (2002), pp. 393-442, ISSN 1389-1286

Amin, S. M. & Wollenberg, B. F. (2005). Toward a Smart Grid: Power Delivery for the 21st Century. *IEEE Power and Energy Magazine*, Vol.3, No.5, (Sept.-Oct. 2005), pp. 34-41, ISSN 1540-7977

Cox, I.; Matthew, M. & Bloom, J. (2007). *Digital Watermarking and Steganography (2nd)*, USA: Morgan Kaufman Publishers, ISBN 978-0-12-372585-1, San Francisco, CA

Divan, D. & Johal, H. (2006). A Smarter Grid for Improving System Reliability and Asset Utilization, *Proceedings of Power Electronics and Motion Control Conference*, ISBN 1-4244-0448-7, Shanghai, Aug. 2006

Feng, J. & Potkonjak, M. (2003). Real-Time Watermarking Techniques for Sensor Networks, *Proceedings of IEEE Int. Conf. on Security and Watermarking of Multimedia Contents*, Santa Clara, CA, USA, Jan 2003

Kleider, J. E.; Gifford, S. & Chuprun, S. (2004). Radio Frequency Watermarking for OFDM Wireless Networks, *Proceedings of IEEE Int. Conf. on Acoustics, Speech, and Signal Processing*, ISBN 0-7803-8484-9, USA, May 2004

Katzenbeisser, S. & Petitcolas F. A. P. (2000). *Information Hiding Techniques for Stegonagraphy and Digital Watermarking*, Artech Print on Demand, ISBN 1-58053-035-4, London

McDaniel, P. & McLaughlin, S. (2009). Security and Privacy Challenges in the Smart Grid. *IEEE Security & Privacy*, Vol. 7, No. 3, (May-Jun 2009), pp. 75-77, ISSN 1540-7993

Perrig, A.; Stankovic, J. & Wagner, D. (2004). Security in Wireless Sensor Networks. *The ACM Communications*, Vol.47, No.6, (June 2004), pp. 53-57

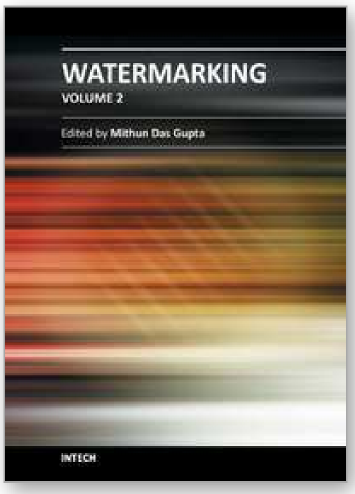
Wang, Y.; Attebury, G. & Ramamurthy, B. (2006). A Survey of Security Issues in Wireless Sensor Networks. *IEEE Communications Surveys & Tutorials*, Vol.8, No.2, (Feb. 2006), pp. 2-23, ISSN 1553-877X

Xiao, R.; Sun, X. & Yang, Y. (2008). Copyright Protection in Wireless Sensor Networks by Watermarking, *Proceedings of IEEE International Conference*, ISBN 978-0-7695-3278-3, New Zealand, Aug 2008

Xiao, X.; Sun, X.; Yang, L. & Chen, M. (2007). Secure Data Transmission of Wireless Sensor Network Based on Information Hiding, *Proceedings of 4th Annual International Conference on Mobile and Ubiquitous Systems: Computing Networking and Services*, ISBN 978-1-4244-1024-8, Philadelphia, PA, USA, Aug 2007

Chen, Y. C.; Chuang, C. C.; Chang, R. I.; Lin, J. S. & Wang, T. C. (2009). Integrated Wireless Access Point Architecture for Wireless Sensor Networks, *Proceedings of ICACT 2009*, ISBN 978-89-5519-138-7, South Korea, Feb. 2009

Zia, P. & Zomaya, A. (2006). Security Issues in Wireless Sensor Networks, *Proceedings of the Int. Conf. on System and Network Communications*, ISBN 0-7695-2699-3, French, Oct. 2006



Watermarking - Volume 2
Edited by Dr. Mithun Das Gupta

ISBN 978-953-51-0619-7
Hard cover, 276 pages
Publisher InTech
Published online 16, May, 2012
Published in print edition May, 2012

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821