Advances in Computer, Signals and Systems (2019) 3: 8-14
Clausius Scientific Press, Canada

DOI: 10.23977/acss.2019.31002
EISSN 2371-8838

Research on WSN Secure Communication Method Based on Digital Watermark for the Monitoring of Electric Transmission Lines

Wang Baoyi[a, *], Hou Zepeng[b], Zhang Shaomin[c]

School of Control and Computer Engineering, North China Electric Power University,
Baoding, 071003, China
[a]email: wangbaoyiqj@126.com, [b]email:1436082661@qq.com, [c]email:zhangshaomin@126.com

Keywords: electric transmission line; WSN; digital watermark; secure communication

Abstract: The wireless sensor network is arranged on the long-chain distributed electric transmission line for real-time monitoring of the electric transmission line. The safe transmission of the collected electric transmission line sensing data is a key issue to be solved urgently. Due to the low processing ability of the sensor nodes, conventional high-complexity security methods such as traditional identity authentication and tamper-proofing can extend the processing time of the node processor, which is unacceptable for real-time data. In addition, due to the high voltage of the electric transmission line, it is impossible to supply power to the wireless sensor nodes directly, and the traditional complicated safety methods have high energy consumption. Therefore, this paper proposes a WSN secure communication solution for electric transmission line based on digital watermark. The algorithm has less time overhead and meets the real-time requirements of WSN communication in electric transmission lines.

1. Introduction

The wireless sensor network collects and transmits the operational data of various power equipment and power grids in the electric transmission line through advanced sensing technology and communication technology. Through the calculation and analysis of the data, the time and place of the faults can be detected. Accordingly, the power equipment and power grid is maintained to achieve reliable, safe and efficient operation of the transmission network [1].

In the electric transmission line, the sensor nodes are installed on each electric transmission line collecting real-time sensing data, and send the collected data to the data aggregation unit(DAU) in one or more hops; one electric transmission line between two towers configures one DAU for each group of nodes, each DAU communicates with substations by Optical Fiber Composition Overhead Ground Wire (OPGW) or GPRS wireless communication network [2-3]. However, some criminals implant some pseudo nodes in the electric transmission line, receiving the data sent by the legal nodes, tamper with it and forward the wrong data packets to the DAU, or pretend to be a legitimate node and send some abnormal sensor data to the network. After receiving the data, the final substation monitoring center will control the power transmission according to these abnormal data.

How to prevent WSN sensor data from being tampered or the node identity is imitated in the electric transmission line is a priority.

The data preventing tampered in the electric transmission line WSN proposed in [4] is based on PKI as the overall security framework. By adding and supplementing related strategy, a total solution is formed to meet its communication security requirements. But behind this proposal, there is a common assumption that all communication devices in the electric transmission line can perform conventional tamper-proof operations, digital signatures, and two-way entity identity authentication. In fact, the energy, communication and computing capabilities of the sensor nodes in the electric transmission line are limited, and the data transmission allowing-delayed in the electric transmission line communication network is millisecond, so the time and energy consumption for the electric transmission line WSN application with high efficiency requirements is unacceptable[5].Therefore, traditional tamper-proof identity authentication and other conventionally complex security methods are no longer suitable for WSN node communication in current electric transmission lines.

2. Design of WSN Secure Communication Scheme Based on Digital Watermark

The digital watermarking technology is used to replace the traditional data entity authentication and tamper-proof technology to realize the secure transmission of data of the WSN equipment at the network layer in the electric transmission line. The electric transmission line between each two towers is a group, and one DAU is configured for each group of nodes. The sensor nodes of the group collect the data and perform watermark generation and embedding operations, and send them to the DAU through one-hop or multi-hop[6]。The DAU performs the watermark extraction and detection using the same key as the sensing node.

According to the security requirements of the data transmission on the electric transmission line, this paper combines the sensor network with OPGW and GPRS, and designs the electric transmission line data transmission network based on WSN. The topology diagram is shown in Figure 1.

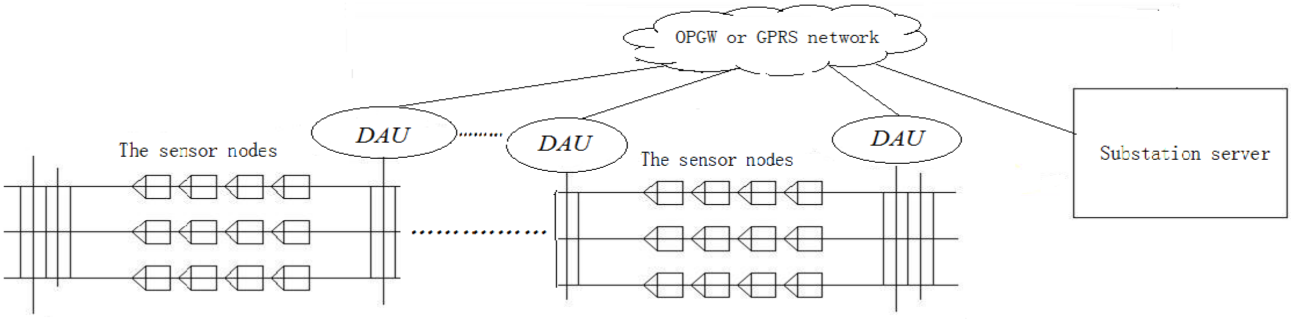


Figure 1: WSN topology on electric transmission line

2.1. Watermark Operation and Communication Design

Digital watermarking technology consists of three basic operations: watermark generation, watermark embedding, and watermark extraction and detection. The key idea is: on the sender side, the watermark is embedded in the data packet to be sent. At the receiving side, the received data packet is watermarked and detected by using the keyword, and only the data packet with the correct watermark can be received. Otherwise, it is considered to be a tampered packet or sent by a fake node and discard it directly [7]。

The specific operation process is as follows: in the watermark generation phase, the sensor nodes in the electric transmission line not only collect the state data of the line, but also uses the data packet generated after the sensor data is collected as the original parameter generated by the watermark, and the watermark is calculated by the digital watermark generation algorithm. The key identifier assigned when each node is added to the network is used as an encryption key, and the watermark is encrypted by a symmetric encryption algorithm; the watermark embedding algorithm is used to embed the encrypted watermark into the last four digits of the data electric transmission time field in the data packet.

2.2. Initial Authentication and Key Distribution of WSN Nodes

In addition to the digital watermark as a solution to the problem that nodes in the electric transmission line WSN are spoofed or the sensor data is tampered with, the node authentication and key distribution technology used by the new node to join the network is also indispensable when the WSN is initially deployed. Technology is a security guarantee for completing watermark information identity authentication.

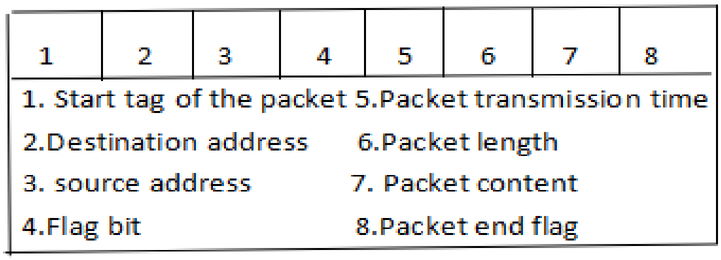
In order to implement the identity entity authentication of the terminal sensor node on the WSN, each node needs to communicate with the substation server when initially arranging the network, confirm the identity legitimacy of the newly joined node, and assign the unique network to each newly joined node. Since the WSN nodes of the electric transmission line are distributed in a chain, first, each DAU node is numbered from 0, and then the sensing nodes inside each DAU group are also numbered from 0, which ensures the uniqueness of the DAU number in the entire network.

Suppose now that the unauthenticated Sensor Node 3 wants to join the group of multi-hop networks. A legitimate node adjacent to an unverified node plays the role of a verifier, passing information between node 3 and the substation server. Each node has its own initial identification key (the identification key for node 3), which is pre-installed and known by the substation server. When node 3 wants to join the set of networks, it should request node 2 that has already been authenticated. After node 2 receives the request, node 3 sends its initial identification key. The node 2 generates an authentication code using the session key (session key between the node 1 and the node 2) and the identification key, and then the node 2 attaches and transmits the authentication code to the node 1 that has been authenticated.

3. Program Realization

In order to prevent the illegal elements from implanting illegal nodes in the electric transmission line WSN, impersonating the legitimate node to send abnormal sensor data or tampering and forwarding the real data, which causes serious damage to the entire transmission network operation, this paper will use the digital watermark technology on the sensor nodes. The transmitted data is embedded in the watermark, and the sink node performs watermark extraction and detection after receiving the data, thereby ensuring the authenticity and reliability of the data in the network transmission process.

In this paper, the data packet Data[i] format of the wireless sensor network communication is shown in Figure 2. It contains 6 fields. The fifth field is usually used to record the time at which the node generated the packet, so the fifth field in the packet is also called the time window [8]. If the lowest 2 bits of the time window information bits are modified, then the modification (usually only -0.27% to 0.27% of the entire packet) is negligible for the accuracy of the entire packet, as this minor modification is usually allowable sensor data error range [9-10]。



1	2	3	4	5	6	7	8

1. Start tag of the packet
2.Destination address
3. source address
4.Flag bit
5.Packet transmission time
6.Packet length
7. Packet content
8.Packet end flag

Figure 2: Packet format in wireless sensor networks

In this paper, the data collection node stores the generated data packet in the sending buffer of the node first, and then waits until the sending buffer is full, and then sends the data packet in the entire buffer. When the sink node receives the data, it also first stores the received data packet in the receive buffer, and then processes and transmits each data packet.

3.1. Time Window Based Digital Watermarking Algorithm

3.1.1. Watermark Generation

Since the sensor node resources are quite limited, the process of watermark generation and embedding should be as simple as possible. To this end, this article takes the following two measures:

(1) This paper randomly selects n data packets from all N data packets stored in the receive buffer for watermark embedding, so that the computational complexity of our algorithm is reduced to n, because n is usually much smaller than N. The amount of information embedded in the watermark is reduced from N to n, and the security of identity authentication of the entire packet information is not reduced.

(2) According to the security requirements of the electric transmission line WSN, the security factor we choose represents the ratio of the number of data items that need to be embedded in the watermark to the total number of data items in the data packet. Based on the safety factor, we define an embedded parameter:

$$\mu = \left\lceil \frac{1}{r_s} \right\rceil = \frac{N}{n}, \quad r_s \in (0,1] \qquad (1)$$

Each data item is generated with a random number generated. We only embed the watermark into the item where the random number can be divisible by μ.

(1) Extracting the eligible data items from the collected transmission line in Sending-Data.

(2) Using the hash function MD5 algorithm, the whole data packet generated by the node is used as the real-time parameter for generating the watermark information, the hash value $M = MD5(Data[i])$ of the calculated parameter, and the lowest 4 bits of the result are extracted by the Get_Lowest_Bits() function.

(3) setting each data item flag bit flag of the generated watermark to 1, indicating that the data item has generated a watermark, and embedding the watermark.

3.1.2. Watermark Embedding

The watermark embedding process includes the following three steps:

(1)Using the symmetric encryption algorithm $E_K(X)$, the identification key Kn is used as the encryption key, and the last four digits X_n of the generated MD5 hash value are used as plaintext to obtain the ciphertext $E_{K_n}(X_n)$, which is used as the watermark W.

(2) Embed W into the lowest 4 bits of the sixth field (the time window) in the packet by the Replace_Lowest_Bits() function.

3.1.3. Watermark Detection

The sink node stores the received data packet in the receive buffer. After the cache is full, the sink node processes the data packet in the cache.

(1)The receiver reads each data item of Received_Data in the received data and retrieves its flag status from each data item. If Data[i].flag=1 in data item i, we can use the function Get_Lowest_Bits() to extract the watermark from the lowest 4 bits of the received W_R of each group.

(2) Using the obtained identification key K_n as the decryption key, using the decryption algorithm $D_K(Y)$ to solve the plaintext $D_{K_n}(W_R)$, and record it.

(3) Using the hash function MD5 algorithm again, generate a hash value by using the data packet received by the sink node, and extract the first 4 bits of the hash value as a new watermark value .

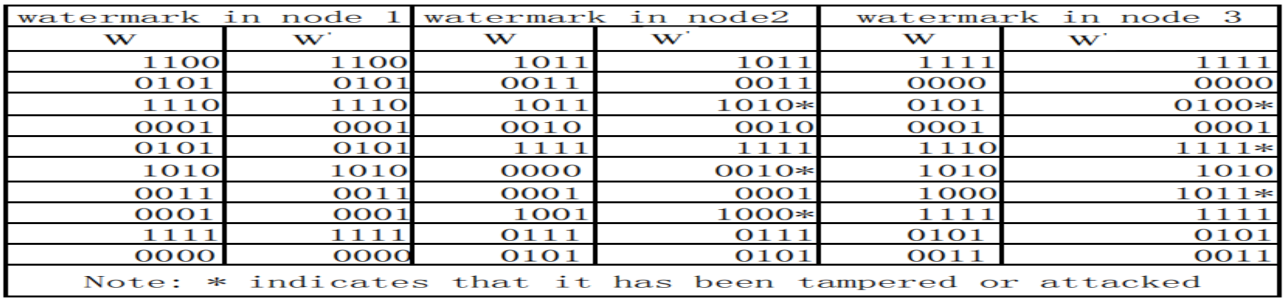
(4) Comparing with W' and W'', if $W'=W''$, it indicates that the data item Data[i] is safe. Please note that once the core data of Data[i] is modified, W'' will be changed.

4. Simulation

4.1. The Correctness and Effectiveness of the Watermarking Algorithm

This is achieved by comparing the watermark extracted from the received packet data with its original watermark. The two received watermarks and the original watermark are three randomly selected from all of the tracking packets listed in Table 1, of which 10 data items are embedded in the watermark and encapsulated in the corresponding data packet.

Table 1: Compares the received data watermark and the original data watermark



watermark in node 1		watermark in node2		watermark in node 3	
W	W'	W	W'	W	W'
1100	1100	1011	1011	1111	1111
0101	0101	0011	0011	0000	0000
1110	1110	1011	1010*	0101	0100*
0001	0001	0010	0010	0001	0001
0101	0101	1111	1111	1110	1111*
1010	1010	0000	0010*	1010	1010
0011	0011	0001	0001	1000	1011*
0001	0001	1001	1000*	1111	1111
1111	1111	0111	0111	0101	0101
0000	0000	0101	0101	0011	0011
Note: * indicates that it has been tampered or attacked					

4.2. WSN Sensor Node Throughput

In this paper, digital watermarking is used for secure transmission. One of the biggest advantages is that digital watermarking does not increase the transmission load of the network. By embedding the least significant bit of the time window, the watermark information is embedded in the least important part of the time window, but replaced, without adding extra data to the original data, so the digital watermark can maintain the original network throughput well. The simulation results are shown in Figure 3.

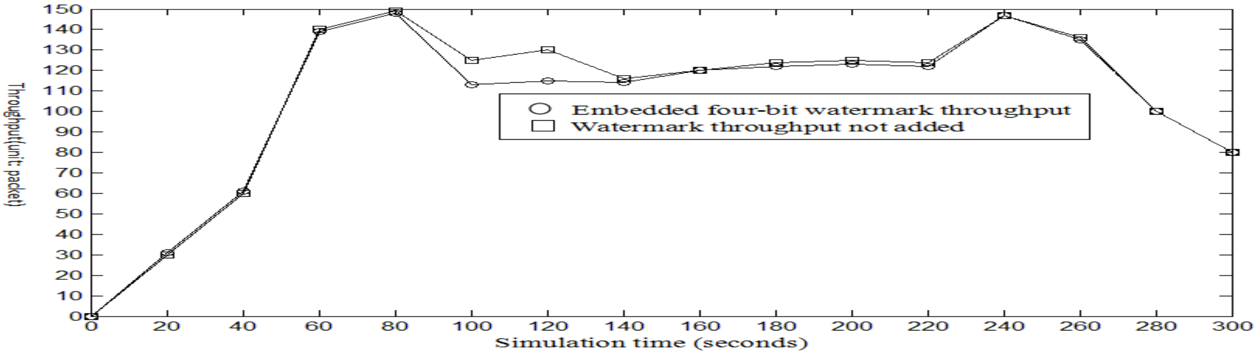
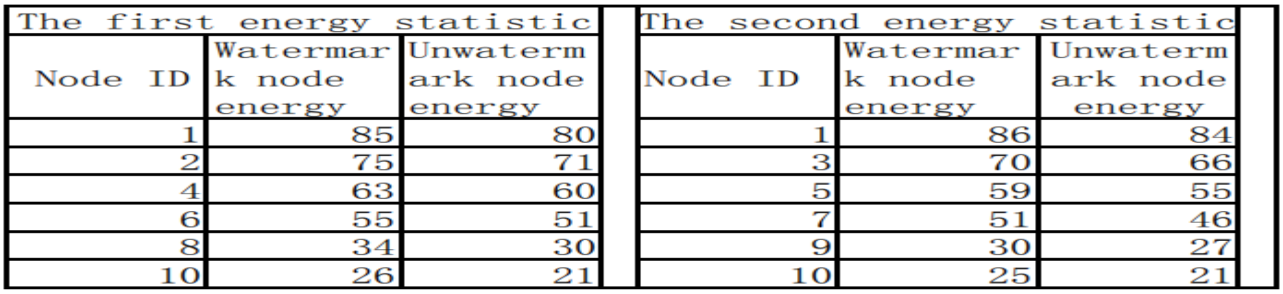


Figure 3: Node throughput test

4.3. Energy Consumption

From the analysis of algorithm complexity, the complexity of the algorithm is so that no additional energy overhead is added during the execution of the watermark algorithm. In addition, the embedding of the watermark does not increase the size of the memory. In summary, the node energy consumption mainly comes from data communication between nodes. As shown in Table 2, the statistics of the energy consumption of some nodes.

Table 2: Partial node energy consumption statistics (unit: micro focus)



The first energy statistic				The second energy statistic			
Node ID	Watermark node energy	Unwatermark node energy		Node ID	Watermark node energy	Unwatermark node energy	
1	85	80		1	86	84	
2	75	71		3	70	66	
4	63	60		5	59	55	
6	55	51		7	51	46	
8	34	30		9	30	27	
10	26	21		10	25	21	

5. Conclusions

Aiming at the abnormal operation of the pseudo node in the electric transmission line WSN to send the abnormal node to destroy the stable operation of the electric transmission line, this paper proposes a time field based digital watermark tamper resistance and node impersonation security algorithm in the electric transmission line WSN. Moreover, the algorithm is simpler to operate and less computational than conventional security algorithms, and is in line with the low energy storage of wireless sensor network nodes, low processing power and high real-time data requirements.

References

[1] Tan Long, Yan Chao. Research on Wireless Sensor Network Security Algorithm [J]. Computer Science, 2015, 42(S1): 438-443.

[2] Li Lifen. Research on Transmission Line Condition Monitoring Data Transmission Based on Wireless Sensor Network [D]. North China Electric Power University, 2013.

[3] Li Tian,Shi Xin,Li Yongqian. Study on Routing Optimization Technology of Wireless Sensor Networks Based on Transmission Line Monitoring [J].Electrical Measurement & Instrumentation, 2015, 52(21):6-10.

[4] Wang Baoyi, Wang Min an, Zhang Shaomin. A GCM-Based Secure Transmission Method for Intelligent Substation Messages [J]. Automation of Electric Power Systems, 2013, 37(03):87-92.

[5] Chhaya L, Sharma P, Bhagwatikar G. Wireless Sensor Network Based Smart Grid Communications: Cyber Attacks,

Intrusion Detection System and Topology Control [J]. 2016, 6(1):5-12.

[6] Jiang Xin, Hu Ping, Wang Wei, Xu Hui. Research on Encryption Algorithm for WSN Environment Data Transmission [J]. Automated Instrument, 2016, 37(11):55-57+65.

[7] Shi Xin, Zhu Yongli. Research on QoS Guarantee Technology for Wireless Transmission Networks for Transmission Line Monitoring [J]. China Electric Power, 2015, 48(03):39-43

[8] Wu Haiyan, Chen Yang. Wireless Sensor Network Authentication Algorithm Based on CRC and Reversible Digital Watermarking [J]. Computer Applications and Software, 2016, 33(06): 294-297+324.

[9] Sen A, Chatterjee T, Dasbit S. LoWaNA: Low Overhead Watermark Based Node Authentication in WSN[J]. Wireless Networks, 2016, 22(7):8-15.