International Journal of Multimedia and Ubiquitous Engineering
Vol.11, No.7 (2016), pp.1-12
http://dx.doi.org/10.14257/ijmue.2016.11.7.01

A Packet Loss Tolerated Method for Data Integrity Protection in Wireless Sensor Networks

Baowei Wang[1, 2], Jingzhou Yan[1, 2], Tao Li[1, 2], Xingming Sun[1, 2] and Li Ma[1, 2, 3]

[1]*School of Computer and Software, Nanjing University of Information Science & Technology, Nanjing 210044, China*
[2]*Jiangsu Engineering Center of Network Monitoring, Nanjing University of Information Science & Technology, Nanjing 210044, China*
[3]*Key Laboratory of Meteorological Disaster of Ministry of Education, Nanjing University of Information Science & Technology, Nanjing 210044*
wbw.first@163.com, yjzfirst@163.com, nuistmail@163.com, sunnudt@163.com, mali1775088@163.com

Abstract

Among existing watermarking methods for data integrity protection in wireless sensor networks (WSNs), the problem of packet loss has not been considered. Most of methods treat packet loss as anomaly attacks, hardly being used in real network. The paper proposes a packet loss tolerated method for data integrity protection in wireless sensor networks based on double-level watermarking and threshold control. Sensory data collected by nodes generate digital watermarking for integrity detection. Watermarking will be stored in sensory data. The network will have watermarking verification and packet loss rate analysis in the sink to ensure data integrity. Through the experiment in real sensor network, this method can effectively protect data integrity with low power.

Keywords*: Watermarking; WSNs; Packet Loss Tolerated; Data Integrity Protection*

1. Introduction

With the development of computer technology, embedded system technology and communication technology, wireless sensor networks (WSNs) have been greatly improved [1]. WSNs have been widely applied in environmental monitoring, military field and medical monitoring [2]. A substantial part of WSNs are deployed in depopulated zone [3], so the data integrity, instantaneity and veracity protection are very important [4]. However, the traditional network solution cannot be applied in WSNs due to the limited resource. Therefore, the low power and high efficiency of WSNs should be taken into full account in data integrity protection.

Digital watermarking is suitable for protecting data integrity in WSNs because of its concealment, detectability and safety [5]. However, most of existing methods treat packet loss as anomaly attacks, hardly being used in real network.

The paper proposes a packet loss tolerated method for data integrity protection in WSNs based on double-level watermarking and threshold control. There are double-level watermarking in WSNs, one is tamper detection watermarking (we called W1 in this paper) to ensure that data has not been tampered or forged in transit, and the other one is packet loss detection watermarking (we called W2 in this paper) to ensure that the network has the prevention of replay attack and deletion attack. Through the packet loss detection watermarking, WSNs can distinguish normal packet loss and anomaly attacks. Sensory data collected by nodes generate double-level watermarking through a hash function, one watermarking is embedded into least significant bit (LSB) [6], and the other one is embedded into the redundant space of the targeted bytes. At the base station side, a

ISSN: 1975-0080 IJMUE

watermarking algorithm is designed to extract the double-level watermarking information, which is compared with recalculated watermarking information to verify the data integrity during the transmission. In a stable WSNs, packet loss rate is within a certain boundary [7]. After ensuring the data has not been tampered or forged, we use packet loss detection watermarking (W2) to determine whether the network has replay attacks. We also use packet loss detection watermarking to analyze the packet loss rate. The networks will issue deletion attack warning once the packet loss rate exceeds a critical threshold.

2. Related Works

Feng *et al*. [8] proposed a method to embed hiding information through positioning errors in wireless sensor network node localization. Many digital watermarking techniques [9-12] were developed for data integrity protection in WSNs. However, there still existed many problems in these techniques. Firstly, these techniques treated the data as streamed data, but it is not the fact. If treated the data as streamed data, many faults would be thrown. Secondly, these techniques need previous and present group data to generate and embed digital watermarking. These schemes bring the problem of increasing energy consumption at the same time, which influenced the application in practical. Thirdly, among existing watermarking methods for data integrity protection in wireless sensor networks, the problem of packet loss has not been considered. Most of methods treated packet loss as anomaly attacks, hardly being used in real network. Sun *et al*. [13] proposed a novel data integrity protection strategy based on fragile digital watermarking technologies, where watermarking information was embedded into the redundant space of the targeted bytes. This algorithm did not increase extra data storage space and remain data accuracy. However, this method also treated packet loss as anomaly attack.

Many digital watermarking techniques need previous and present group data to generate and embed digital watermarking. The problem of packet loss has not been considered. As shown in Figure 1. The W3 is directly associated with Packet3 and W3 is embedded in Packet4. However, if Packet3 is lost, these methods will consider packet2 as unauthentic and reject its data reading because its watermarking doesn't match the extracted watermarking.

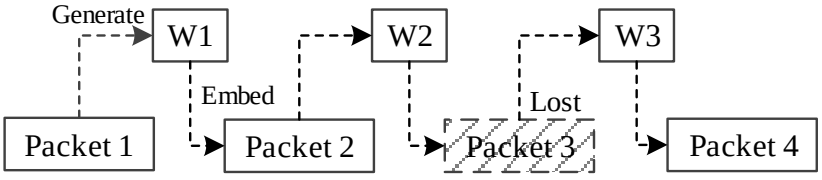


Figure 1. Existing Watermarking Methods Problem Model

3. A Packet Loss Tolerated Method

The method we design is based on double-level digital watermarking algorithms, one watermarking is tamper detection watermarking (W1) to ensure that data has not been tampered or forged in transit, and the other one is packet loss detection watermarking (W2) to ensure the network has the prevention of replay attack and deletion attack.

Double-level digital watermarking embedding and extraction model is shown in Figure 2. The W1 is directly associated with sensory data such as temperature, humidity and light intensity. W2 is associated with sequence number (SN) and its flag bit. The double-level watermarking is generated and embedded at source sensor nodes side. At base station side, it will have watermarking verification and packet loss rate analysis in the sink to ensure data integrity.

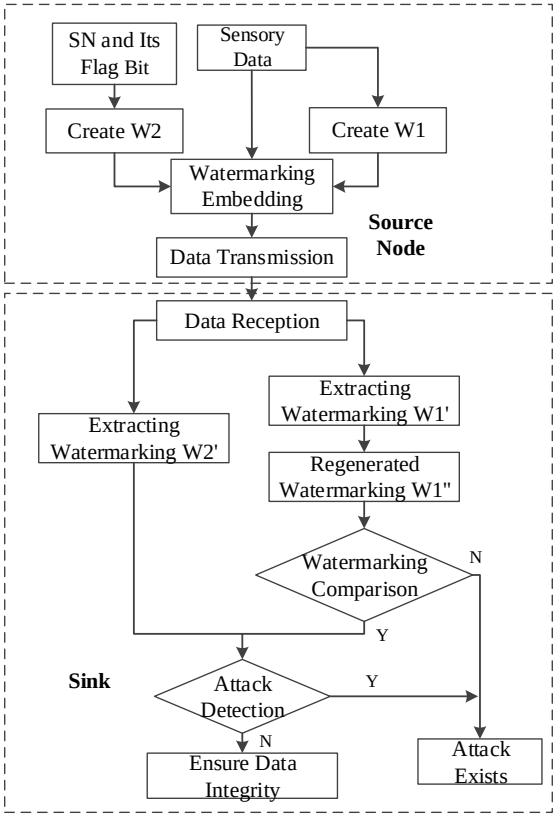


Figure 2. Watermarking Algorithm Model

3.1. Symbols and Rules

Symbols and rules used in the algorithm are defined as follows:

Define 1: In WSNs, nodes collect sensory data such as temperature, humidity and light intensity and stored the data in the data fields. These data fields are denoted as $D=\{d_0,d_1,d_2,\ldots,d_{n-1}\}$, where d_0~d_{n-1} indicate sensory data, and n represents the number of the sensory data.

Define 2: The node generates a serial number SN, and the SN will increment 1 once node sends a packet. The range of SN value is from 0 to 2^x-1.After SN reaches to 2^x-1, it will reset back to 0. Here x is a constant in certain condition and it can be adjusted dynamically in different conditions.

Define 3： We use a flag bit to record SN cycle time. After SN resets back to 0, the flag will be from 0 to 1 or from 1 to 0. The SN and flag can be combined into SNF. SNF=SN+flag, "+"represent connect function, W2=SNF.

Define 4: The packet loss rate P will be calculated every SN cycle time (SN from 0 to 2^x-1). K represents the biggest tolerated packet loss rate in normal WSNs.

Define 5: The size of the data field is in byte for the unit. The range of data acquisition is determined by the data resolution. Taking a Telosb node as an example, which uses sensor SHT11 to collect humidity and temperature data. The resolution of humidity is 0.03%RH, so the humidity data need 12 bits of storage space. Therefore, two bytes are required in the package to store the data, which makes 4 bits as the redundant space [13]. Redundant space is denoted as $R=\{r_0,r_1,r_2...,r_{n-1}\}$, and $R(i)=r_i$ ($0 \le i < n$). r_i represents the size of the redundant space of i^{th} data field. As shown in Figure 3. The msb represents the most significant bit of data filed and lsb represents the least significant bit.

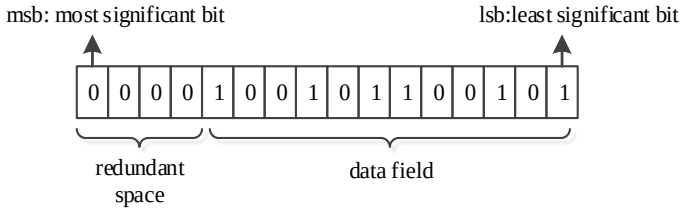


Figure 3. Redundant Space of the Data Field

Rule 1: The watermarking will be embedded into least significant bit, so the least significant bit will be set to 0 before watermarking embedding to eliminate watermarking impact. Set lsb to 0 can be denoted as no_lsb(d_i), $0 \le i < n$.

Rule 2: We use a hash function to calculate each sensed data, denoted as $H(d_i)=HASH(no\_lsb(d_i)), 0 \le i < n$.We also use same hash function to calculate SNF hash value, denoted as H(SNF)=HASH(SNF). Then calculation of the tamper detection watermarking information W1, can be denoted as $W1 = H(SNF) \oplus H(d_0) \oplus H(d_1) \oplus ... \oplus H(d_{n-1})$, in which "$\oplus$"represent XOR operation.

Rule 3: Embed tamper detection watermarking W1 into least significant bit of each data.

Rule 4: Embed packet loss detection watermarking W2 into the redundant space of the data fields R.

Table 1. Notations and Parameters

Symbol	Description
D	Nodes collect sensory data such as temperature, humidity and light intensity and leave the data in the data fields.
SN	Serial number inserted in each D.
W1	Tamper detection watermarking to ensure that data has not been tampered or forged in transit.
W2	Packet loss detection watermarking to ensure the network has the prevention of replay attack and deletion attack.
R	Redundant space of each data field.
Flag	A flag bit to record SN cycle time.
P	Packet loss rate.
K	Critical threshold of packet loss rate.
W1′	Extracted tamper detection watermarking in base station.
W2′	Extracted packet loss detection watermarking in base station.
W1″	Regenerate tamper detection watermarking in base station.
SN′	Extracted Serial number in base station.
flag′	Extracted flag bit in base station.

3.2. Watermarking Embed Algorithm

Input: Data field D and sensory data number n, the size of the redundant space R(i) and SN.

Output: The watermarked data D_send.

Steps:

1) for(int i=0;i<n;i++)
2) { $H(d_i)=HASH(no\_lsb(d_i))$; }
3) H(SNF)=HASH(SNF);
4) $W1=H(SNF) \oplus H(d_0) \oplus H(d_1) \oplus \ldots \oplus H(d_{n-1})$;

5) W2=SNF;
6) i=0;
7) for(j=S_0; j>S_0-R(0); j--)
8) { d_0[j]=W2[i++]; }
9) for(j=S_1; j>S_1-R(1); j--)
10) {d_1[j]=W2[i++];}
11) …
12) for(j=S_{n-1}; j>S_{n-1}-R(n-1); j--)
13) {d_{n-1}[j]=W2[i++];}
14) for(i=0;i<n;i++)
15) {d_i[lsb]=W1[i];}
16) send(D_send)

S_0 represents the highest position of d_0. By this analogy, S_{n-1} represents the highest position of d_{n-1}. d_0~d_{n-1} indicate sensory data. We use the hash function to calculate SN and each sensory data. We xor these hash value to get tamper detection watermarking W1. In our approach, W2 is SNF.

We embed W1 into least significant bit of each data. For example, assume that the original data d_i is {0000 1001 0110 0100}.The watermarking W1 have n bits. We use an array W1[] to store the watermarking W1. The W1[i] will be embedded into the lsb of data d_i. If W1[i]=1.After embedding, the d_i is {0000 1001 0110 0101}.

We embed W2 into the redundant space of the data fields R(i). For example, assume that the W2 is {0000 0010 0011 0110}.The data fields have four data: d_0, d_1, d_2 and d_3.Each data has 4 bits redundant space, R(0)=R(1)=R(2)=R(3)=4. We embed {0000} into d_0 redundant space R(0). Embed {0010} into d_1 redundant space R(1). And so on, embed {0011} into R(2) and embed {0110}into R(3).

The entire embedding process is shown in Figure 4.

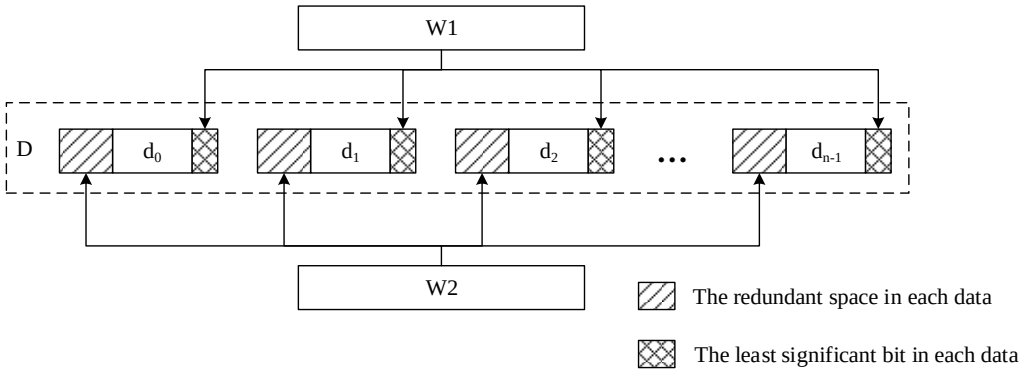


Figure 4. Embedding Process

3.3. Watermarking Extraction Algorithm

Input: The received data, The size of the redundant space R(i). The number of the sensory data n.
Output: W1′, W2′,SN′,flag′
Steps:
1) int i=0,j=0;
2) for(j=S_0; j>S_0-R(0); j--)
3) {W2′[i]=d_0′[j]; d_0′[j]=0; i++; }
4) for(j=S_1; j>S_1-R(1); j--)
5) { W2′[i]=d_1′[j]; d_1′[j]=0; i++; }

6) …
7) for(j=S_{n-1}; j>S_{n-1}-R(n-1); j--)
8) { $W2'[i]=d_{n-1}'[j]$; $d_{n-1}'[j]=0$; i++; }
9) for(i=0;i<n;i++)
10) { $W1'[i]= d_i'[lsb]$; }
11) get SN′ and its flag′ from W2′

At the base station side, a watermarking algorithm is designed to extract the double-level watermarking information, which is compared with recalculated watermarking information to verify the integrity of the data during the transmission.

3.4 Detection Algorithm

Input: The extracted watermarking W′ from base station and regenerate watermarking W″.
Output: The result of data integrity
1) if(compare(W1′,W1″)==equal)
2) return (No Forgery);
3) else
4) {return (Forgery); break;}
5) if(received consecutive identical SN)
6) { if(compare(flag1,flag2)==equal)
7) {return(replay attack) ;break;}}
8) calculate(P);
9) if(P>K)
10) return(deletion attack);
11) else
12) return(data integrity);

We compare W1′ with W1″, if they are same, we judge the data haven't been tampered or forged. Otherwise, we judge the data have been tampered or forged. Because the packet is transferred in a variety of ways, the packet sequence may be changed in the sink. The SN is sequentially stored in an array in the sink. If the sink receives the maximum SN and resets back to 0, the flag will be from 0 to 1 or from 1 to 0.After flag has a jump, we will calculate the packet loss rate P through the array which SN stored in. If the packet loss rate exceeds the critical threshold K, the networks will issue deletion attack warning. If we find the same SN number, we will determine whether the network has replay attacks through some special mechanism. Once the base station receives same SN in a period, it will judge if they have same flag or not. If the flag is same, the networks will issue replay attack warning.

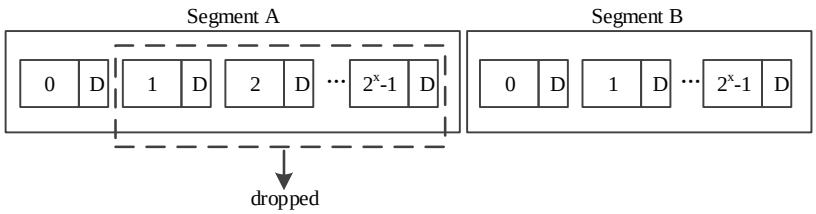


Figure 5. Segment Deletion Attack Scenario

Here we assume that the attacker has managed to delete data of which SN is from 1 to 2^x-1 as shown in Figure 5. The same SN (SN=0) will occur in this case and the receiver issue replay attack warning in spite of the deletion attack. So, in our algorithm, if we

receive consecutive identical SN, we will contrast the flag bit. If flag bit is same, the receiver will issue replay attack warning. Otherwise, replay attack warning will not be issued.

Similarly, we known that if the attacker deletes some packet, detection algorithm may have a failure. For example, if the attacker deletes two segment data, detection algorithm may calculate a wrong packet loss rate and can't give a deletion attack warning. However, if the network loses two segment data, the base station won't receive packet in a very long time. So, if base station can't receive packet in a very long time, it will have a deletion attack warning too.

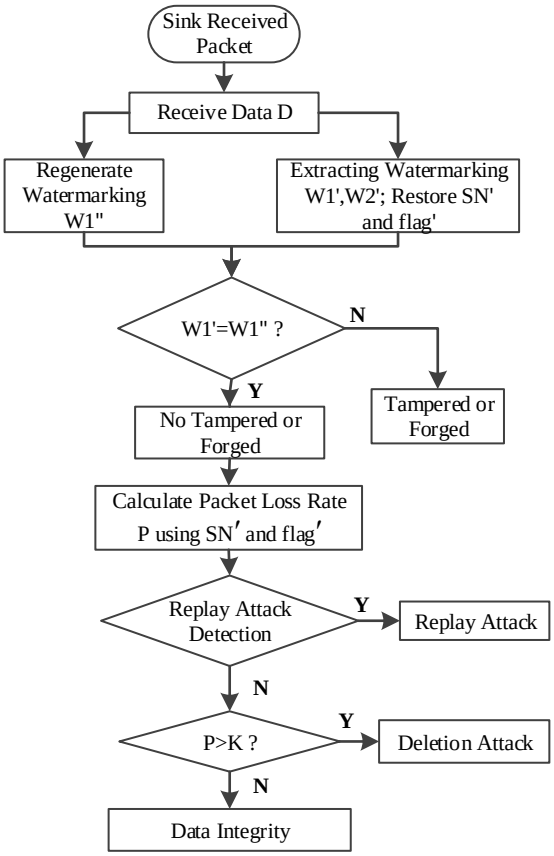


Figure 6. Detection Scheme Model

Our detection scheme is shown in Figure 6.After sink receives a packet, it will use Rule 2 to regenerate watermarking W1″ and use watermarking extraction algorithm to extract watermarking W1′, W2′, SN′ and flag′. If W1′ and W1″ is not same, packet will be dropped because of the tampering or forgery. If the W′ and W″ is same, we will use SN′ and flag′ to determine whether the network has replay attack or not. We will also calculate the packet loss rate, if packet loss rate exceed a critical threshold K, the networks will issue deletion attack warning.

4. Performance Evaluation

4.1. Experiments Setup

In this section, 15 Telosb nodes are deployed in the networks. The nodes use the TinyOS operating system and CTP (collection tree routing) routing protocol. The nesC language is used to implement the watermarking embedding algorithm and C# is for watermarking extraction and attack detection at the base station. Sensory data such as

temperature、humidity and light intensity are transmitted every one minute. In order to save energy in WSNs, no further watermarking extraction and comparison are performed during data transmission.

Figure 7. Sensors Used in Our Experiments

4.2. Experiment Results

Fifteen nodes are developed in the networks, three of them are attack nodes. Every attack node are tested for 50 times. The size of packet payload is 208 bits. The packet has 12 bits least significant bit and 48 bits redundant space (we only use 10 bits to embed W2).In the experiment, the size of W1 is 12 bits and W2 is 10 bits.

Table 2. The Experimental Results of Data Integrity Attacks

Attacks	Number of experiments	Success rate (%)
Packet Tampering	50	100%
Packet Forgery	50	100%
Packet Replay	50	100%

We can see from Table 2, our scheme can achieved 100% detection on packet tampering, packet forgery and packet replay attacks. Packet tampering can cause watermarking changed, so it can be detected in the sink. Packet forgery can cause packet no watermarking or wrong watermarking, so it can be detected in the sink.

In our scheme, we can assure that our scheme can prevent false positive if the network has normal packet loss. Table 3 give a comparison among different schemes.

Table 3. Different Schemes Comparison

Scheme	Exist false positive if the network has normal packet loss
SGW	Yes
FWC	Yes
FWC-D	Yes
Our Scheme	No

4.3. Deletion Attack Experiment

According to experiments, our networks which deployed in laboratory has a stable packet loss rate. The stable packet loss rate is 10%. So, we set the critical threshold in10%. However, the critical threshold should be different in different networks.

The deletion attack and detecting selective forwarding attacks experiment [14] of this paper is shown as follows: The sink calculate packet loss rate by periodic examination and issues deletion attack warning once the packet loss rate exceeds a critical threshold. We set three attack nodes in our network. The selective forward packet of attack nodes cause abnormal packet loss in network. In different critical threshold, the success rate is different.

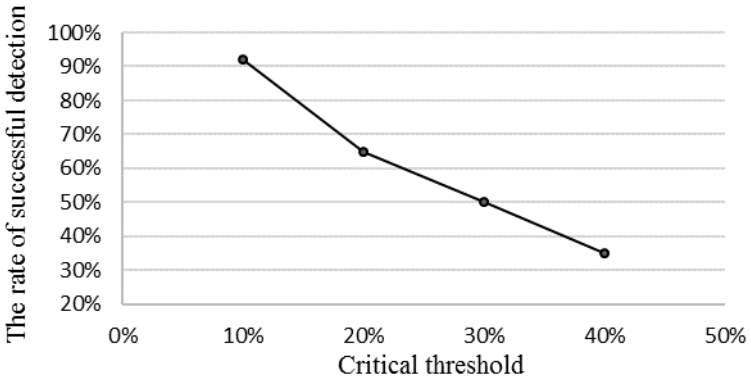


Figure 8. The Rate of Successful Detection in Different Critical Threshold

Experiments with different critical threshold are used to reveal the relationship between critical threshold and success rate. In each critical threshold, we experiment for 50 times.

As seen in Figure 8, success rate is different in different critical threshold. The reason is that not all packets are deleted by attack nodes. Attack nodes delete part of packets which is sent by nodes. If deleted packets are below the critical threshold, we can't detect the attack. So, setting suitable critical threshold is very important. Critical threshold should associate with correct packet loss rate. This can greatly improve successful detection rate.

4.4. Embedding Capacity Analysis

Figure 9 shows that the comparison of embedding capacity among the least significant bit [11], redundant space of the targeted bytes [13], blank character [15] and our algorithm. According to the figure, the embedding capacity of our proposed method is significantly higher than the previous digital watermarking algorithms. Our method embeds watermarking into least significant bit and redundant space of the targeted bytes. It improves watermarking embedding capacity.

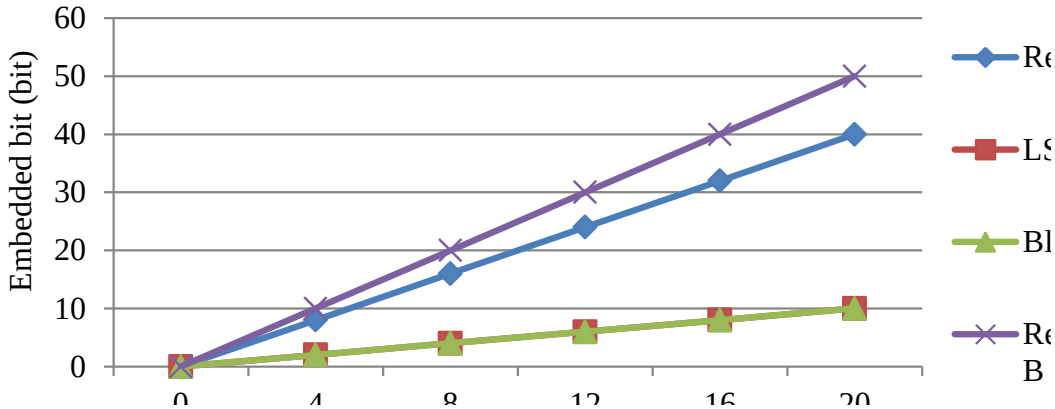


Figure 9. Watermarking Embedded Capacity

Our method is applied in a meteorological sensor network. The meteorological sensor network collects meteorological data. Multi-kinds of meteorological data provide greater redundant space, so we can embed larger digital watermarking. However, in other sensor networks, there may be not enough redundant space. Watermarking size may be larger than the sum size of least significant bit and redundant space. In this case, we can only embed part of watermarking. It might compromise the security guarantee of the watermarking function. We will solve this problem in the next work.

4.5. Energy Evaluation

In WSNs, the main factor which influences the energy consumption includes data storage, watermarking embedding, routing, broadcast and data transmission. Compared with other schemes, our method saves the node energy consumption in data storage. Usually, on the order of 3000 instructions can be executed for the energy cost required to transmit one bit over a distance of 100m by radio [16]. So the consumption of data transmission is higher than calculation. Our method doesn't increased the packet length. So, it's better than adding blank character method in energy consumption. It can also control the energy consumption in an optimum performance.

4.6. Data Accuracy Analyze

Our method embeds watermarking into least significant bit and redundant space of the targeted bytes. The value of data reading has a little change by replace the least significant bit. It may decrease the precision of data reading. However, it can be accepted in most WSNs because the data accuracy is in acceptable range. Embedding watermarking into least significant bit and redundant space don't increase the packet length and data transmission energy consumption. So, our method is better than others in most WSNs under the situation of accepting small data accuracy loss.

5. Conclusion

The paper proposes a packet loss tolerated method for data integrity protection in wireless sensor networks based on double-level watermarking and threshold control. Sensory data collected by nodes generate digital watermarking for integrity detection, which will be stored in sensory data together with watermarking for attack detection. It will have watermarking verification and packet loss rate analysis in the sink to ensure data integrity. Compared with other schemes, our method has a better result. Firstly, it doesn't need multiple buffers and can save nodes' energy in data storage. The life time of network has been improved. Secondly, our method can differentiate normal packet loss and

deletion attack. Thirdly, our method improves watermarking embedding capacity. The watermarking length has been improved and the security also has been improved. The results demonstrate that our method is effective.

Acknowledgements

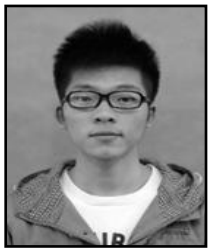
This work is supported by the NSFC (61173136, 61232016, U1405254, 61173141, 61173142, 61373133), 201301030, 2013DFG12860, BC2013012, BY2013095-4-11, and PAPD fund.

References

[1] L. Cui, H. Ju, Y. Miao, T. Li, W. Liu and Z. Zhao, "Overview of Wireless Sensor Networks", Journal of Computer Research and Development, vol. 42, no. 1, **(2005)**.
[2] Y. Liu, Y. He, M. Li, J. W, K. Liu and L. Mo, "Does Wireless Sensor Network Scale? A Measurement Study on GreenOrbs", Proceedings of the 30th IEEE Conference on Computer Communications, Shanghai, China, **(2011)**.
[3] A. Mainwaring, D. Culler, J. Polastre, R. Szewczyk and J. Anderson, "Wireless Sensor Networks for Habitat Monitoring", Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications, New York, **(2002)**.
[4] P. Li, Y. P. Lin and W. N. Zeng, "Search on Security in Sensor Network", Journal of Software, vol. 17, no. 12, **(2006)**.
[5] H. Yin, C. Lin, F. Qiu and R. Ding, "A Survey of Digital Watermarking", Journal of Computer Research and Development, vol. 42, no.7, **(2005)**.
[6] Z. Xia, X. Wang, X. Sun and B. Wang, "Steganalysis of Least Significant Bit Matching Using Multi-order Differences", Security and Communication Networks, vol. 7, no. 8, **(2014)**.
[7] J. Shen, H. Tan, J. Wang, J. W. Wang and S. Lee, "A Novel Routing Protocol Providing Good Transmission Reliability in Underwater Sensor Networks", Journal of Internet Technology, vol. 16, no. 1, **(2015)**.
[8] J. Feng and M. Potkonjak, "Real-time Watermarking Techniques for Sensor Networks", Proceedings of the International Society for Optics and Photonics, **(2003)**.
[9] H. Guo, Y. Li and S. Jajodia, "Chaining Watermarks for Detecting Malicious Modifications to Streaming Data", Information Sciences, vol. 177, no. 1, **(2007)**.
[10] H. Juma, I. Kamel and L. Kaya, "Watermarking Sensor Data for Protecting the Integrity", International Conference on Innovations in Information Technology, Al Ain, **(2008)**.
[11] I. Kamel and H. Juma, "A Lightweight Data Integrity Scheme for Sensor Networks", Sensors, vol. 11, no. 4, **(2011)**.
[12] Y. Cao, X. Sun, B. Wang and H. Deng, "Association Watermarking-Based Data Integrity Protection in WSN", Journal of Computer Research and Development, vol. 46, **(2009)**.
[13] X. Sun, J. Su, B. Wang and Q. Liu, "Digital Watermarking Method for Data Integrity Protection in Wireless Sensor Networks", International Journal of Security and Its Applications, vol. 7, no. 4, **(2013)**.
[14] F. Ma and Y. Pan, "Circumventing selective forwarding attacks in sensor networks", Electronic Design Engineering, vol. 19, no. 21, **(2011)**.
[15] B. Wang, X. Sun and Z. Ruan, "Multi-mark: Multiple Watermarking Method for Privacy Data Protection in Wireless Sensor Networks", Information Technology Journal, vol. 10, no. 4, **(2011)**.
[16] G. J. Pottie and W. J. Kaiser, "Wireless Integrated Network Sensors", Communications of the ACM, vol. 43, no. 5, **(2000)**.

Authors

Baowei Wang, He received his B.S. and Ph.D. degrees in Computer Science from Hunan University in 2005 and 2011, respectively. He is currently working as a lecturer in School of Computer and Software, Nanjing University of Information Science and Technology. His research interests include steganography, wireless networks and securing ad hoc networks.



Jingzhou Yan, He was born on September 9, 1990. Currently he is a master candidate in Nanjing University of Information Science and Technology. He received his bachelor degree in Nanjing University of Information Science and Technology. His areas of interest are wireless sensor networks, meteorological information processing and data assimilation.

Tao Li, He received his MS degree in Computer Application from Nanjing University of Technology in 2004, and his PhD in Signal and Information Processing from Southeast University. He is currently working as a lecturer in School of Computer and Software, Nanjing University of Information Science and Technology. His research interests include wireless sensor network and embedded system.

Xingming Sun, He is a professor in the School of Computer and Software, Nanjing University of Information Science and Technology, China from 2011. He received the B.S. degree in Mathematical Science from Hunan Normal University and M.S. degree in Mathematical Science from Dalian University of Technology in 1984 and 1988, respectively. Then, he received the Ph.D. degree in Computer Engineering from Fudan University in 2001. His research interests include information security, network security, cryptography and ubiquitous computing security.

Li Ma, She received her B.S. degree in 1985 from the Chengdu Institute of Meteorology and her Ph. D degree in 2011 from Nanjing University of Information Science and Technology. She is a professor and tutor for graduates in Nanjing University of Information Science and Technology. Her main research interests include image processing, pattern recognition, and meteorological information processing and data assimilation.

