International Journal of Hybrid Information Technology
Vol.8, No.6 (2015), pp.257-268
http://dx.doi.org/10.14257/ijhit.2015.8.6.25

A Copyright Protection Method for Wireless Sensor Networks Based on Digital Watermarking

Baowei Wang[1,2], Jianwei Su[1,2], Youdong Zhang[3], Biqiang Wang[4], Jian Shen[1], Qun Ding[1,2] and Xingming Sun[1,2]

[1]*School of Computer and software, Nanjing University of Information Science and Technology, Nanjing, 210044, China*
[2]*Jiangsu Engineering Center of Network Monitoring,Nanjing, 210044, China*
[3]*Department of Computer Engineering Huaiyin Institute of Technology, Huaian, 223003, China*
[4]*Hubei Meteorological Service Center, Wuhan, 430074, China*
wbw.first@163.com, sunuist@163.com, z.yd@163.com, 164323517@qq.com, s_shenjian@126.com, dingqun0926@163.com, sunnudt@163.com

Abstract

Wireless sensor networks are composed of numerous sensor nodes in the monitored area, which have been well applied in various practical areas. In these applications, data security from sensors has been threatened. Thereby in this paper, a digital watermarking based copyright protection method is proposed with regard to data security in wireless sensor networks. According to the particular characteristics of collecting data, the embedding capacity can be expanded using this method of manipulating both LSB and MSRB[4] bits of the data field. The data-related information is embedded as the digital watermarking into the data to be forwarded. When the base station receives the data, we use a lookup Table to improve the speed of data parsing. In order to achieve and verify the copyright protection on WSNs, both theoretical analysis and experimental results have demonstrated that the method can effectively detect the data reliability. In addition, we also generate two-dimensional code based on the test results, thereby facilitating the user's copyright authentication.

Keywords: *watermarking, wireless sensor networks, copyright protection, two-dimensional code, lookup Table*

1. Introduction

Wireless Sensor Networks(WSNs) are self-organized multi-hop networks composed of static and/or mobile sensor nodes. Each sensor node has the capability to sense data, process data and communicate with each other in the covered region, so that perceived data to transmit to the base station. At present, WSNs have been typically used in the fields of environmental monitoring, medical care, traffic management and battlefield. However, the sensor nodes are usually deployed in unattended areas and limited by energy, computing power, storage space and communication due to their individual capacity. In addition, the perceived data are vulnerable to external or internal attacks in the transmitting. So it is imperative for us to adopt an effective strategy to ensure the transmission safety of the perceived information.

The security threat in WSNs mainly is the data falsify. The attacker can easy falsify data and send illicit data in the transmission. In response to this security issue, various solutions are proposed. Most of them use symmetric or asymmetric key encryption methods on confidential data to assure data security. In this way, the attacker without the key in the case is more difficult to achieve the correct data. If the data transmission in the

ISSN: 1738-9968 IJHIT

process of being tampered with, we can also be detected by the strategic authentication. Nonetheless, this mechanism cannot meet the needs of communication between these nodes because of the resource limitation of WSN. So the digital watermarking technology is proposed.

Digital watermarking is currently one of the most prevalent technology in the wireless sensor network security research, the content of the research mainly includes the data copyright protection [1-3], data integrity protection [4-8] and selected forwarding attacks [9, 10]. Here the author mainly introduces how to utilize digital watermark to solve the data copyright protection. In [1], J. Feng *et al*., have developed the first system of watermarking techniques to embed cryptologically encoded authorship signatures into data and information acquired by wireless embedded sensor networks. The elementary idea is to impose additional constraints during the data acquisition or sensor data processing. Constraints corresponding to an encrypted signature are selected with consideration of tradeoffs between the accuracy and the strength of proof of the authorship. In [2], X. Dong *et al*., have proposed a fragile watermarking algorithm to identify the status of the sender node. In the method, a unique watermark is embedded directly into the Least Significant Bit of data to save communications bandwidth. When the sink node received the data, it will extract the watermarking to judge the source of data. In [3] have designed a robust digital watermarking algorithm for preserving stringent data copyright protection in wireless sensor network, which uses the Least Significant Bit of sending them as the embed bit. Although these methods solved the problem of data copyright protection, but they do not fully consider the characteristics of the collect data in wireless sensor networks.

In this paper, we propose a kind of large capacity digital watermarking embedded method for data copyright protection in wireless sensor network applications. The collected data from each source sensors are capsulated into news package, which contain diverse data fields for precise sensing sources. Different from existing studies, according to the irreplaceable characteristics of collecting data, we divided the data into three regions, we use the invalid data fields to embed watermarking. According to the experimental consequences, our method can effectively protect the copyright of data.

The rest of the paper is organized as follows. Section 2 describes the watermarking model. Section 3 describes the digital watermarking method, which includes watermarking generation, embedding and extraction process. Section 4 describes in the performance evaluation. At last, we conclude the paper in Section 5.

2. Digital Watermarking Model

The sensor data in the form of a message packet is sended in WSNs and the message package contains numerous data fields, and collected data are stored in these data fields, such as temperature, humidity and illumination. Because most of the sensors are using 16-bit registers, and the sensor acquisition of the digital signal will, in turn, from low to high storage in the 16-bit register. So from the register convert to the data field is directly associated with digital watermark embedding. That is to say. The different carriers directly affect the digital watermark embedding in different ways. Typically, the definition of the data field has two basic types, we respectively defined the data field as the integer structure and floating structure. Integer structure indicates that the sensor nodes will store the data from the 16-bit registers as unsigned 16-bit integer in the data field. When the base station receives data, it will need to parse the data into an actual value. Floating structure indicates that sensor nodes will store the data from the 16-bit registers as floating in the data field, but the sensors need to parse the data from the 16-bit registers into the authentic value firstly. For example, the temperature sensor of SHT15 senses the temperature in the register is represented as 3338, when stored in an integer type structure is still 3338, but when stored in a float type structure is -6.22. Therefore, according to the

structural features of two have different digital watermark embedding model. Compared with the two models, we can clearly see that integer structure of digital watermarking model is more superior to the floating structure model. Thus, according to the integer structure mode, a digital watermarking based copyright protection method is proposed with regard to data security in wireless sensor networks. According to the particular characteristics of collecting data, the embedding capacity can be expanded using this method of manipulating both LSB and MSRB bits to embed watermarks. The MSRB represents the most significant bit of redundancy in the data field of the packet [4]. The watermark embedding structure is shown in **Figure 1**.

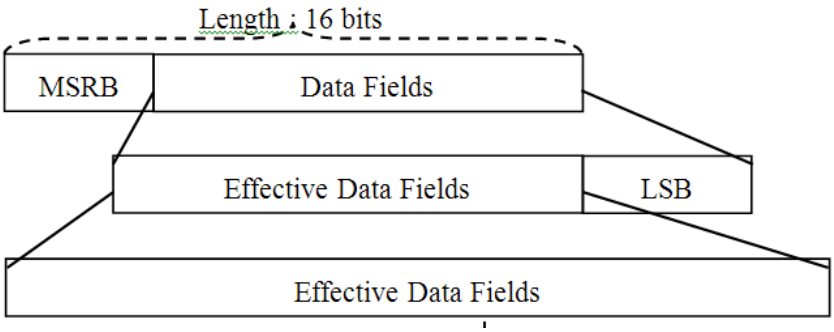


Figure 1. Digital Watermarking Embedded Structure

3. Digital Watermarking Algorithm

In wireless sensor networks, the sensor nodes are vulnerable to physical attack and invasion of external nodes, so identifying the sender node, realizing the data of copyright protection are required in the security of WSNs. Therefore, according to the digital watermarking model in the second part, we proposed a novel digital watermarking algorithm solving the problem of data copyright protection in wireless sensor network. First, sensor periodically collects data and stores the data to the data field in turn. While the data fields filled, digital watermarking information will be embed in the data field and sent to the base station. After the base station receives the data, according to the extraction of the watermarking algorithm for the extraction and detection of the watermark, only the data contains the watermark and the watermark match successful data is considered valid data, otherwise considered invalid data. If the data is successfully verified, the data with watermark information will be stored directly in the database. When you need to use the data, we can find the data from the database, and then directly use a lookup Table for data analysis, so as to ensure the integrity of the watermark information. Therefore, if you need to validate the data copyright, we only need to extract and compare the watermark. Meanwhile, we generate two-dimensional code based on the detection result, thereby facilitating the user's copyright authentication. Here, we introduce a digital watermark algorithm in watermark generation, embedding and detecting process.

3.1 Watermarking Generation Algorithm

In the digital watermarking algorithm, we should first generate a unique watermarking to identify the sender node. The method we designed is based on data correlation, where watermarking information is directly associated with sensor data. In WSNs, sensor nodes periodically collect and transmit data, and sensor data are transmitted in a package including data fields. For a concise description of watermark generation algorithm, we defined the sensor data as $D_i = \{d_1, d_2, ..., d_n\}, (1 \le i \le n)$, in which d_i indicates one sampling, which is expressed in decimal, and n represents the number of the sensor data in a period. Before sending the package, we first according to the D_i calculates S, S is

represented the embedded capacity of watermarking. Then we according to the one-way hash function generate the digital watermark utilize each sensed data, denoted as $H_i = Hash(Key, ID, D_i)$, where the Key is key, ID is node identifier. Finally, we take out S bits from the most significant bit of H_i as watermarking information W, which can be denoted as $W = Get\_MSB(H_i, S)$.The Watermarking Generation Algorithm is shown in **Algorithm 1**.

Algorithm 1. Watermarking Generation Algorithm

Input: Key: Key, Sensed data: D_i, Node identifier: ID
Output: Watermarking information: *W*
1. $S = CalculateEmbedBit(D_i)$
2. $H_i = Hash(Key, ID, D_i)$
3. $W = Get\_MSB(H_i, S)$
4. return *W*

3.2 Watermarking Embedding Algorithm

When the sensor node collecting the data, the range of data acquisition is determined by the data resolution. Taking Telosb node as an example, which uses a temperature sensor of SHT11. The resolution of temperature is 14 bits, in this case, two bytes are required in the package to store the data, which make 2 bits as the redundant space, the redundant space is denoted as MSRB[4]. Secondly, since the least significant bit of sensing data is negligible, so we define it as the least significant redundant data field space, referred LSB. In response to this perceived characteristics of the data field, we proposed a novel digital watermark embedding algorithm of combined the MSRB with LSB. In this algorithm, the length of MSRB is determined by the resolution of the sensor nodes. When the number of bits for embedding watermark is determined, according to the watermarking generation algorithms generate the same number of bits for watermarking information. Then watermarking information replaces the MSRB first and replaces the LSB. Thus, the watermarking embedding process is completed. The watermarking embedding algorithm is shown in **Algorithm 2**.

Algorithm 2. Watermarking Embedding Algorithm

Input: Sensed data: D_i, Watermarking information: *W,* Length*: S*
Output: Embed watermarking data D_i'
1. for (int j=0; j<S; j++)
2. Replace the MSRB and LSB with *W*
3. return D_i'

3.3 Watermarking Extraction Algorithm

In order to reduce the energy consumption of the nodes in the network, watermarking extraction is not performed during the transmission, only the base station received data to extract the watermark and verification. In order to brief descriptions of the watermarking extraction algorithm, we defined the received data of the embedded watermark as $D_i' = \{d_1', d_2', \ldots, d_n'\}, (1 \le i \le n)$。Firstly, according to D_i' recalculates the length S of the embedded watermark, then extract and remove the MSRB of the watermarking in turn. We definite the extracted watermark information as W', and use the same one-way hash function recalculated H_i' according to the Key, ID and has extracted sensing data D_i''. At the same time, generating the watermark information W'' base on H_i' and comparison between W' and W'' decides whether the data have been damaged. The

algorithm for watermarking extraction and verification is shown in **Algorithm 3**.

Algorithm 3. Watermarking Extraction Algorithm

Input: The watermarked data: D_i', Node identifier: ID, Key: Key
Output: The result of verification (True, False)

1. $S = Calculate\_Embedded\_Bit(D_i')$
2. $W' = Extraction\_Watermark(D_i', S)$
3. $H_i' = Hash(Key, ID, D_i'')$
4. $W'' = Get\_MSB(H_i', S)$
5. $IF(Compare(W', W'') == Equal)$
6. return true
7. Else
8. return false

When the Watermarking Extraction Algorithm returns True, it means the data have not been damaged during the transmission. Therefore, the data will be stored with binary data into the database. Since the data in the database used in the external application is in the form of a lookup Table to parse, so there are two ways of data theft. First, if the data is the parsed data with the lookup Table, we should through the lookup Table find the original data in the database, then extract and verify the watermarking. The results of copyright verify is shown in **Figure2**, the internal data represents the data belong to the internal network, or not belong to the internal network. If the data is the original data, we can directly extract and verify the watermarking.

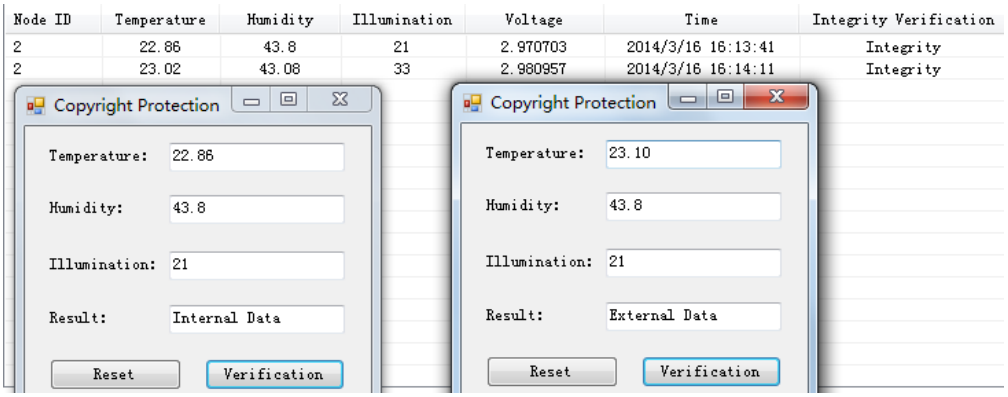


Figure 2. The Results of Copyright Verify On the Parsed Data

4. Performance Evaluation

4.1. Experiments Setup

In this section, we will validate the data copyright protection method of our proposed

having better application value. We do numerous experiments, the experimental environments are based on the real wireless sensor network environment. Each sensor node collected data every 10 seconds. Every packet contains 12 sensory data, and the node sends a data packet every two minutes. The sensor nodes using self-developed specialized meteorological sensor, the temperature sensor use SHT15, as shown in **Figure 3**. The temperature of showed in base station uses the mean value of 12 sets of data. In addition, in order to facilitate the achievement of the copyright protection of sensor data, we generate two-dimensional code based on the results of verification, so that we can direct verify the results and access to data via mobile phones. It is shown in **Figure4** and **Figure5**. Specific experimental environment parameters are as follows.

Temperature Sensor : SHT15	Routing Protocol : CTP
Number of sensors: 100	Node Operating System : TinyOS
Node acquisition cycle : 10 seconds	Node Programming Language: Nesc
Node sends period: 2 minutes	Station programming languages : C #

Figure 3. SHT15 Sensor Node

Figure 4. Two-dimensional Code

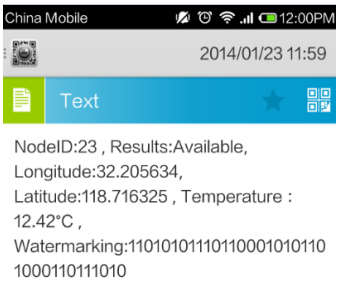


Figure 5. Phone Authentication

4.2 Influence of Watermark Embedding

The digital watermark embedding algorithm is combined the MSRB with LSB method to embed watermark information, so that the original data has been influenced in a certain extent. We randomly selected 5 groups of sensor data for the analysis the changes after embedding the watermark information. As shown in **Table 1**, we can clearly see that, the watermark embedding before and after the change is small, so that we use the digital watermark embedding algorithm errors caused by very slight.

Table 1. The Influence of Watermark Embedding

Group ID	Average of before embedding	Average of after embedding	Standard deviation of before embedding	Standard deviation of after embedding
1	25. 50	25. 50	0. 055801	0. 059084
2	13. 49	13. 48	0. 044950	0. 045727
3	21. 44	21. 43	0. 045768	0. 043557
4	28. 40	28. 40	0. 047900	0. 047339
5	32. 37	32. 38	0. 041986	0. 042095

4.3 Safety Analysis

Different types of attacks were tried to verify its safety. Five nodes were randomly selected as attacking nodes to perform following three attacks respectively: packet forgery, selective forwarding and packet tampering. Each attack has been tested for 100 times, and the experimental results are presented in **Table 2**.

Table 2. The Experimental Results of Three Attacks

Attacks	No. of experiments	Success rate(%)
Packet Forgery	100	100
Selective Forwarding	100	100
Packet Tampering	100	100

Our watermarking scheme divides the data field into three sections. The MSRB and LSB store watermarking information. Watermarking information and the collected data are directly associated. According to the experimental results our method achieved 100% verification on packet forgery, selective forwarding and packet tampering. Therefore, the experimental results show that our proposed watermarking scheme can effectively verify the copyright of the data, and ensure the authenticity and reliability of the data.

4.4 Embedding Capacity Analyses

Watermark embedding capacity is an important indicator to measure digital watermarking algorithm. **Figure 6** shows that the comparison of embedding capacity among the Least Significant Bit [2], add a blank character [7] and our proposed algorithm. According to the **Figure 6**, the capacity of the Least Significant Bit shows a line increment, and same as add a blank character at the end of the data. Whereas the capacity of our proposed method, combine the data fields MSRB and LSB to embed watermarks, is higher than their embedding capacity. More importantly, different sensor node is embedded in a different capacity.

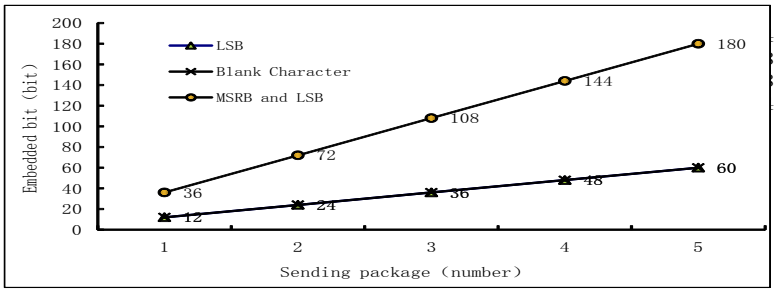


Figure 6. Watermarking Embedded Capacity

4.5 Efficiency of Data Parsing

In the digital watermarking algorithm, improving the efficiency of data parsing is anther highlights. When the digital watermark extraction algorithm is complete. The base station needs to convert the binary data stream to actual values. In the conventional method, the base station picks out each datum from the packet, then gets the real value according to the operating rules of the node. In our method, we get the real value according to the lookup Table to parse the data of the packet. When the base station system starts, we dynamically generate a lookup Table based on the operating rules of the node. When the base station parses the data, only to find the serial number in the lookup Table. **Figure 7** shows that the comparison of efficiency of data parsing between our method and traditional method. We can clearly see that the efficiency of our data parsing method is superior to traditional method.

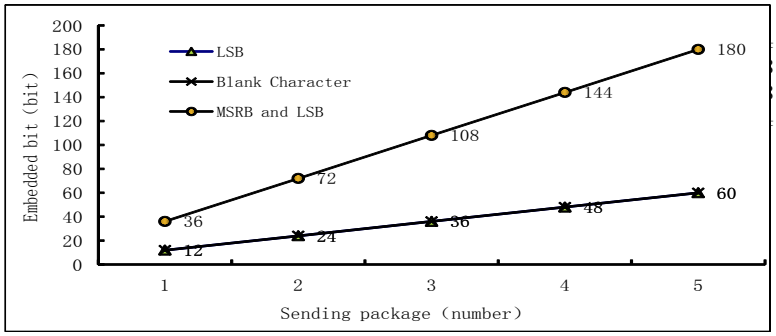


Figure 7. Efficiency of Data Parsing

4.6 Transmission Data Quantity Analysis

Different digital watermarking algorithm causes the different effects on the data. Sometimes, it even directly affects the amount of data transfer. Therefore, a good watermarking algorithm should prevent increase the amount of data transferred. **Figure 8** shows that the comparison of transmission data quantity of among the Least Significant Bit[2], add a blank character [7] and our proposed algorithm. The add blank character method at the end of the data is according to the corresponding data bit of watermark information is 1 or 0, selective adding blank character, so the data quantity exists wave phenomenon. The way of modifying the least significant bit has no effect on the amount of data transmitted. And our proposed digital watermarking method same as the least significant bit, it does not affect the data transmission quantity.

	1	2	3	4	5
LSB	192	384	576	768	960
Blank Character	201	405	605	811	996
MSRB and LSB	192	384	576	768	960

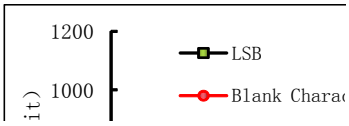


Figure 8. Transmission Data Quantity

4.7 Energy Evaluation

Energy is an important indicator in the applications of wireless sensor networks, which directly affects the cycle of the entire network. And the application of digital watermarking for wireless sensor network energy consumption is mainly reflected in the data storage, embedding, routine maintenance, data communications and so on. We assume that routing maintenance and data storage have fixed. We only consider the consumption of energy in watermark embedding and data communications. In general, 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[11]. So the energy consumption of the data transmission between the nodes is far greater than processing calculation. In our scheme, watermarking information is directly embedded into the LSB and MSRB of the data. It does not occupy additional storage space. Compared to the adding blank character method, the energy consumption of data transmission is significantly reduced. In addition, the watermarking is embedded into the binary data instead of the actual value. Compared with the method of adding blank character and modify the Least Significant Bit, the average energy consumption of each node is reduced. So in terms of energy consumption the cost of our proposed watermarking method has incomparable advantages compared to other ones.

5. Conclusion

In this paper, we have proposed a digital watermark scheme for data copyright protection. The proposed approach can verify the reliability of data, and can also determine the location of the node. Practical experiments have been conducted in a real employed wireless sensor network environment. The results have shown that with regard to energy consumption or embedding capacity, our watermarking algorithm is significantly better than the other algorithms.

In the future, the algorithm can be mainly optimized in two points. First, when the resolution of the collected data is equal to the size of the data field, the watermark embedding capacity of MSRB will be disappearing. Secondly, the robustness of the watermark is not high. So for this type of sensor, the digital watermarking algorithm also needs further improvement.

Acknowledgements

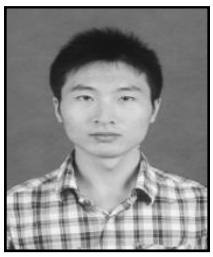
This work is supported by the NSFC (61173136, 61232016, 61173141, 61173142, 61103215, 61373132, and 61373133), GYHY201206033, 201301030, 2013DFG12860, BC2013012, PAPD fund and Prospective Research Project on Future Networks of Jiangsu Province (2013095-4-10).

References

[1] J. Feng and M. Potkonjak, "Real-time Watermarking Techniques for Sensor Networks", SPIE Security and Watermarking of Multimedia Contents, Santa Clara, CA, USA: SPIE Press, **(2003)**, pp. 391-402.
[2] X. Dong and X. Li, "An Authentication Method for Self Nodes Based on Watermarking in Wireless Sensor Networks", WiCom'09.5th International Conference on Wireless Communications, Networking and Mobile Computing, **(2009)**, pp. 1-4.
[3] R. Xiao, X. Sun and Y. Yang, "Copyright Protection in Wireless Sensor Networks by Watermarking", International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Washington DC, IEEE Press, **(2008),** pp. 7-10.
[4] X. Sun, J. Su, B. Wang, *et al*, "Digital Watermarking Method for Data Integrity Protection in Wireless Sensor Networks", International Journal of Security and Its Applications, vol. 7, no. 4, **(2013)** July, pp. 407-416.
[5] H. Guo, Y. Li and S. Jajodia, "Chaining Watermarks for Detecting Malicious Modifications to Streaming Data", Information Sciences, no. 177, **(2007)**, pp. 281-298.
[6] H. Juma, I. Kamel and L. Kaya, "Watermarking Sensor Data for Protecting the Integrity", International Conference on Innovations in Information Technology, Washington DC, IEEE Press, **(2008)**, pp. 598-602.
[7] B. Wang, X. Sun and H. Ren, "Multi-mark: Multiple Watermarking Method for Privacy Data Protection in Wireless Sensor Networks", Information Technology Journal, **(2011)** October, pp. 833-840.
[8] L. Zhou and Z. Zhang, "A Secure Data Transmission Scheme for Wireless Sensor Networks Based on Digital Watermarking", the 9th International Conference on Fuzzy Systems and Knowledge Discovery, **(2012)**, pp. 2097-2101.
[9] H. Deng, X. Sun and B. Wang, "Selective Forwarding Attack Detection using Watermark in WSNs", In: ISECS International Colloquium on Computing, Communication, Control and Management, CCCM, **(2009)**, pp. 109-113.
[10] D. Zhang and C. Xu, "Detecting Selective Forwarding Attacks in WSNs using Watermark", International Conference on Wireless Communications and Signal Processing, **(2011)**, pp. 1-4.
[11] J. Potter and W. J. Kaiser, "Wireless integrated network sensors", Communications of the ACM, **(2000)** May, pp. 51-58.

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.



Jianwei Su, He received his B.S. degree in Computer Science from Nanjing University of Information Science and Technology, China in 2011. Currently he is studying for his M.S degree in Meteorological Information Security at the same university. His research interests include steganography, cryptography and network security.

Youdong Zhang, He is a professor in department of computer engineering Huaiyin Institute of Technology Huaian City, Jiangsu Province, China from 2011. He received the B.S.degree in physics and Applied Electronic Technology from Nanjing Normal University and M.S. degree in Computer Applications Technology from Nanjing University of Aeronautics and Astronautics in 1989 and 2000, respectively. Then, he received the Ph.D degree in Digital

Engineering and Information security at the same university in 2007. His research interests include information security, data mining, Intrusion detection and knowledge engineering.

Biqiang Wang, He received received the M.S. degree in Computer Science and Engineering from Nanjing University of Information Science & Technology, China in 2011. He is now working in Hubei Meteorological Service Center. His research interests include wind and solar power prediction techniques, meteorological data processing and software development.

Jian Shen, He received the B.E. degree from Nanjing University of Information Science and Technology, Nanjing, China, in 2007 and the M.E. and Ph.D. degrees in Computer Science from Chosun University, Gwangju, Korea, in 2009 and 2012, respectively. Since late 2012, he has been a Professor in the College of Computer and Software at Nanjing University of Information Science & Technology, Nanjing, China. His research interests include computer networking, security systems, mobile computing and networking, ad hoc networks and systems, and ubiquitous sensor networks.

Qun Ding, She received her B.S. degree in Software Engineering from Nanjing University of Information Science and Technology, China in 2012. Currently she is studying for her M.S degree in Software Engineering at the same university. Her research interests include wireless networks and network security.

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.

