False Data Identification Method Based on Watermarking

Dengyin Zhang
Key Lab of Broadband Wireless Communication and Sensor Network Technology,
Nanjing University of Posts and Telecommunications, Nanjing, China
Email: zhangdy@njupt.edu.cn

Mingxiang Wan and Chao Xu
Key Lab of Broadband Wireless Communication and Sensor Network Technology,
Nanjing University of Posts and Telecommunications, Nanjing, China
Email: wanmx@foxmail.com, 510739458@qq.com

***Abstract*—The vulnerability of sensor nodes make the sensor network faces enormous security challenges. Attackers can inject false data to the network by capturing the normal nodes, by which the attackers can not only to mislead the data collection center to make the wrong decisions, but also can run out the energy of the nodes which forwarding the data. In order to cope with false data injection attack, this paper present a false data identification method based on the digital watermarking technology, which authenticate the identity of the data and the node by digital watermarking technology. The simulation results show that this method has well recovery rate of the watermark and data, and has higher false data detection rate.**

***Index Terms*—wireless sensor network, digital watermark technology, false data attacks, Witness node authentication**

I. INTRODUCTION

With the sensor networks technology be widely used in military surveillance, environmental detection, traffic management, it become more and more important to ensure the security of the sensor networks. False data injection attacks make it impossible for the base station to get the information correctly and completely from the sensors, and it is not easy to filter the false data.

We assume that once the normal node is captured by the attackers, the node is no longer a normal node, but an attack node. Fig. 1 show that the two clusters are under the attack of false data: in the cluster 1, cluster head and two cluster nodes were the attack nodes, and then the cluster head can send fabricated false data to the base station. In the cluster 2, the cluster head is normal node, but there are 3 attack nodes exist in the cluster. The cluster head aggregates the sensor data from the cluster nodes, if the cluster nodes were attacked and sent the false data, the cluster head can hardly get the correct information for the users and the false data injection attack succeed.

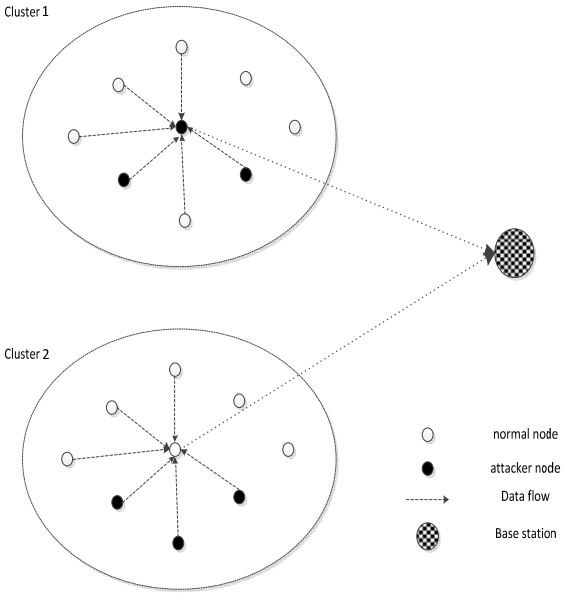


Figure 1. False data injection attacks

II. RELATED WORK

False data injection attack has increasingly become a significant risk of transmission of data security in sensor networks. In recent years, many scholars have studied how to identify and filter false data, the main research achievements are as follows.

Zhu [2] proposed an interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks, shorted for IHA. It presents a scheme that guarantees that the base station will detect any injected false data packets when no more than a certain number t nodes are compromised. Further, the scheme provides an upper bound B for the number of hops that a false data packet could be forwarded before it is detected and dropped, given that there are up to t colluding compromised nodes. The scheme is efficient with respect to the security it provides, and it also allows a tradeoff between security and performance.

Ye [3] presented a statistical En-route filtering mechanism (SEF) to detect and drop false reports during

doi:10.4304/jcp.8.10.2682-2688

the forwarding process. Assuming that the same event can be detected by multiple sensors, in SEF each of the detecting sensors generates a keyed message authentication code (MAC) and multiple MACs are attached to the event report. As the report is forwarded, each node along the way verifies the correctness of the MACs probabilistically and drops those with invalid MACs. SEF exploits the network scale to filter out false reports through collective decision-making by multiple detecting nodes and collective false detection by multiple forwarding nodes.

From the comprehensive analysis of the methods described above, we find that there are two common inadequacies.

A. The Threshold Security Issues

When the number of captured nodes in the network exceeds a certain threshold value, the attacker can conjecture the protection measures of the entire network, such as the overall cryptographic key, and then the attacker forges the false data using the security information, which will mislead the base station to make the wrong judgment.

B. The MAC Security Issues

As the data is transmitted by radio waves, it will be affected by the noise and other interference on the transmission process. The MAC will be easily damaged during transmission in the method above, even if the network is not attacked by false data injection. The MAC which is damaged by the noise or other interference may also mislead the base station to treat the correct data as false data.

In this paper, we use the digital watermarking technology to identify the false data. This method will effectively avoid the security issues of the MAC. Because the watermark is invisible, in the transmission process the data do not need to carry a certain number of the MAC, just add the serial number of nodes' authentication key, which is useless for the attacker to guess the encryption method of the network. In addition, the anti-jamming capability of such information is strong than the MAC generated by one-way function.

III. False Data Identification Method Based-on Watermarking

This paper proposes the false data identification method based on digital watermarking technology. In the initialization phase, the base station maintains the related data, such as cryptographic keys, random seek and so on. Assume the network is safe in the initialization phase. After the sensor nodes are sown in the sensing area, the sensor nodes begin to collect the data and send it to the cluster head, and then the cluster head aggregates the data. The cluster head then sends the aggregated data to the cluster nodes to seek for the witness node to verify the authenticity of the data. The authentication process is as follows. The cluster head send the MSP of the aggregated data and the witness request to the cluster nodes, then the cluster nodes check the MSP with their own collected data, if they are different, they refuse to offer the witness watermark; if they are the same, then calculate the witness watermark and send it with the serial number of the cryptographic key to the cluster head. Until the cluster head get t witness watermarks, it begins to generate the legitimate packets. Firstly, the cluster head uses a one-way function to calculate the watermark with the information received from witness nodes, and then embeds the watermark into the aggregated data with the reversible watermarking algorithm based on the expanded difference; Secondly, the cluster head adds the serial number of the cryptographic keys and the timestamps into the embedded aggregated data. When the data reach the base station, the base station extracts the watermark and recovery the original data to judges whether the data is repeated packet and false data or not. Fig. 2 shows the functional modules of the false data identification method, it includes four parts: network initialization, witness node authentication, legitimate packet generation and base station detection.

A. Network Initialization

The base station will assigns some information to each node during initialization, such as a unique cryptographic key K[p], the key number *p*, the node Serial number *ID* and the modulation value of the difference expansion *d*, and every node's security information will be maintained on a list by the base station. Meanwhile, the BS will assign a random function seed R which is used for generating random numbers and the random numbers will participate in the legitimate packet generation. The BS maintains the entire random function seed list. Every node has two functions: a one-way function $F_1()$ which is used to calculate the watermark and a random function S() which is used to calculate the random number.

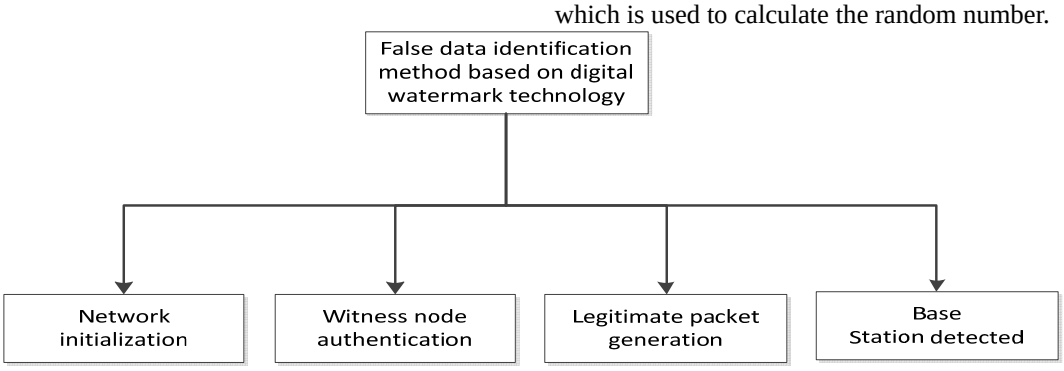


Figure 2. Functional modules of the false data identification method

B. Witness Node Authentication

After the sensor network deployed, the base station send a request to one of the cluster head, the cluster head notify the nodes in the cluster to send the collected data to the head node, and then the cluster head aggregate the received sensor data to get *D*.

Then the cluster head selects t nodes as witnesses and sends a watermark request and the most significant part (MSP) of aggregate data to each witness node. The witness node will compares the MSP with its collected data to mark a judgment whether the aggregate data is legitimate or not. If it is legitimate, the witness node will generate witness watermark, and send it with the serial number of the key to the cluster head; if not, witness node refuses to send witness watermark. Consultation process is shown in Fig. 3.

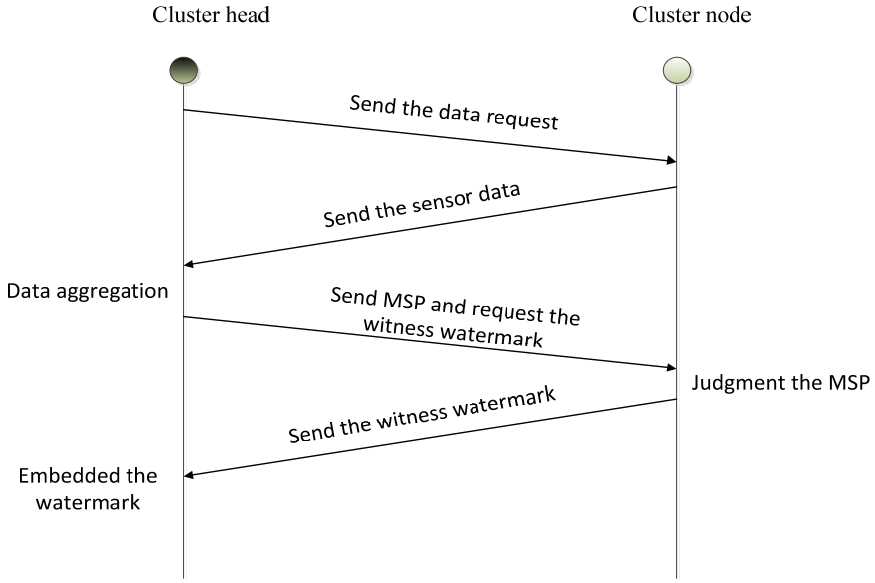


Figure 3. Consultation process of cluster head seeks witness node.

The process of witness node authenticates the aggregate data and generates the watermark is just like the algorithm 1.

Algorithm 1: Witness node authentication algorithm

Step1: aggregate data authentication. After the witness node get request and the *MSP* of aggregate data from the cluster head, it will compare the MSP with data it collected. if they are different, the witness refuses to provide witness watermark information and the authentication process is over; if they are same, go to step2 to generate the witness watermark;

Step2: witness watermark generation. Witness node calculates the watermark using the *MSP* of aggregate data received and its own key by the one-way function F_1. $w[i]=F_1(MSP,K[P])$;

Step3: send the witness information. The witness node sends the witness watermark $w[i]$ and its own serial number of the key p to the cluster head, and the authentication algorithm is over.

C. Legitimate Packet Generation

The cluster head process the data received from the witness node, including watermark information $w=\{ w_1, w_2,\ldots, w_t \}$, and the serial number of the key $\{ p_1, p_2,\ldots, p_t \}$ to get the watermark information be embedded to the aggregate data *D* as shown in Fig. 4, in which D_0 is the most significant part of the aggregate data, (D_1, D_2, ... D_{n-1}) will be used for embedding the witness watermark.

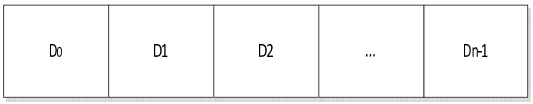


Figure 4. The packet group

The embedded watermark generation is shown in algorithm 2. Meanwhile it selects L (L=m+1) groups to embed the watermark. Where n and m is the network preset value, determined by the different network applications. Legitimate packet generation process is shown in Fig. 5.

Algorithm 2: Embedded watermark generation algorithm

Step1: collect *t* witness watermarks $w = (w_1, w_2,\ldots, w_t)$;

Step2: process the collection witness watermarks and use the one-way function to calculate the watermark $W=F_1(w_1,w_2,\ldots,w_t)$;

Step3: according the preset value of the node *m*, and select the first *m* bits as the embedded watermarks from *W*, where $m<n$-2.

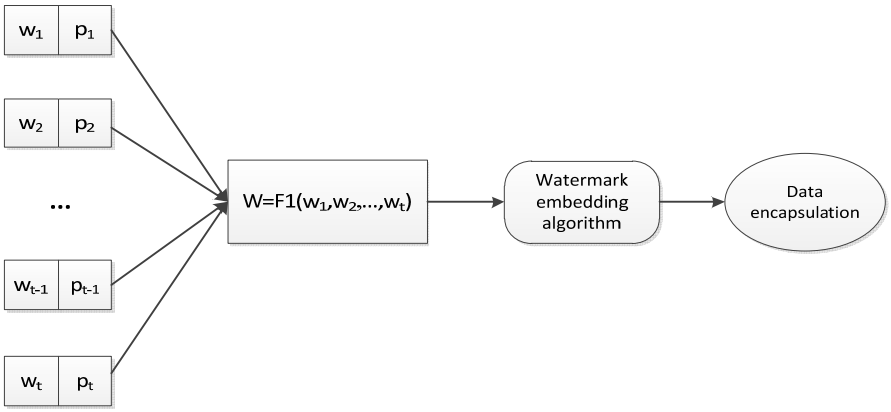


Figure 5. Legitimate packet generation

Using the random function S() and the random function seed *R*, the cluster head calculates the random number *S*, *S*=S(*R*), and then get the baseline data D_j from (D_1,D_2,…D_{n-1}) though *j*=(*S* mod (*n-1*))+*1*. The watermark embedding process is shown in algorithm 3.

Algorithm 3: Watermark embedding algorithm

Step1: gather the baseline data from (D_1, D_2… D_{n-1}) by the random number *S*, where *j*=(*S* mod (*n-1*)) +*1*), then calculate the difference between the (D_1,D_2,…,D_{n-1}) and Dj, get the difference v[i]=D[i]- Dj;

Step2:expand the difference v[i] to v[i]'=d*v[i]+w[i], where the d is preset named difference extended modulation valuesin the sensor node;

Step3: add the baseline data Dj to the expanded difference v[i]', get the embedding data D[i]'= Dj +v[i].

Here is an example of the watermark embedding process. Where watermark w is 011, the difference extended modulation value d is 2. The number of groups L is 4 and the baselines data is assumed as D4. The watermark embedding process is shown in Fig. 6.

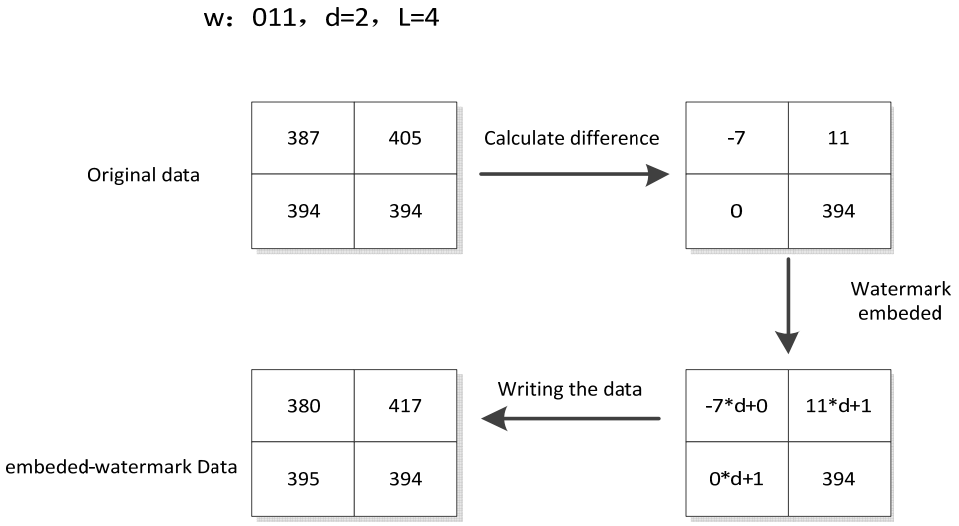


Figure 6. The example of the embedded watermark

When the watermark embedding is completed, the cluster head put the serial number of the key and the timestamp into the data, where the timestamp is used to judge whether the packet is repetition, to avoid the replay attacks, and the serial number of the key is used to rebuild the watermark in the base station. Fig. 7 shows a legitimate packet format, where additional information includes the serial number of the key and the timestamp.

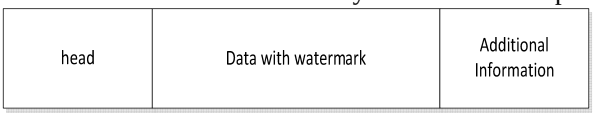


Figure 7. Legitimate packets format

D. Base Station Detection

The base station determines the authenticity of the received data. It checks the timestamp to find the repeated packets, and compare the extracted watermark with the detect watermark to determine the authenticity of the packet. The extracted watermark is extracted from the received data by using the watermark extraction algorithm, and the detect watermark is calculated by data characteristics and additional information. Algorithm 4 gives the watermark extraction process, this algorithm can extract out the watermark and original aggregate data from received data; Algorithm 5 shows the detection of the watermark generation method.

Algorithm 4: Watermark extraction algorithm

Step1: The BS obtains the embedded watermark data (D1', D2',…,Dn-1'), calculates the baseline data Dj' and the difference Ui=Di'-Dj';

Step2: Calculate the extract the watermark wi = mod (Ui, d);

Step3: Recovery the sensor data, anti-modulation of the difference and get the Ui'=$\lfloor U_i / d \rfloor$;

Step4: Recovery the sensor data (D1, D2,…,Dn-1), where Di =Dj + Ui'(i!=j);

Fig. 8 shows the watermark extraction process of the forward example.

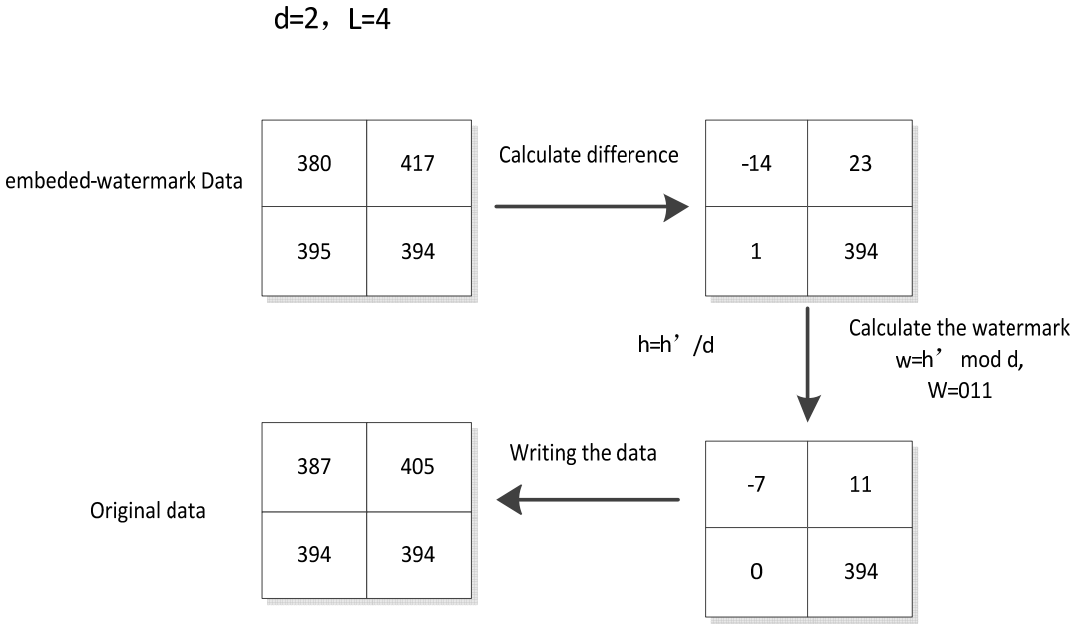


Figure 8. The example of the extracted watermark

Algorithm 5: Detection watermark generation algorithm

Step1: extract the serial number of the key p from the additional information, and get the key information *K*[*p*];

Step2: use the *MSP* of the sensor data D_0 and the key information *K*[*p*] to calculate the w_i', where $w_i'=F_1(D_0,K[p])$;

Step3: process the t watermark information to get the detection watermark *W*', where $W'=F_1(w_1', w_2',\ldots, w_t')$.

Algorithm 6 below tells how the BS judges the data authenticity.

Algorithm 6: Base station detection algorithm

Step1: the base station obtains the timestamp from the additional information and judges whether the packet is a repeated one, if it is, then drop the packet and the detection is over; if it is not, then go to step2;

Step2: the base station detects the number of the witness node key, if it is not t, then judge the packet is false data and drop it; if it is t, then go to step3;

Step3: the base station uses the algorithm 4 to extract the watermark and original aggregate data, and uses the algorithm 5 to obtain the detection watermark, then go to step4;

Step4: the base station compares the extraction watermark and the detection watermark, if they are same, then judge the data is truth, the base station detection is over; if they are different, then judge the data is false.

The base station detection process is shown in Fig. 9.

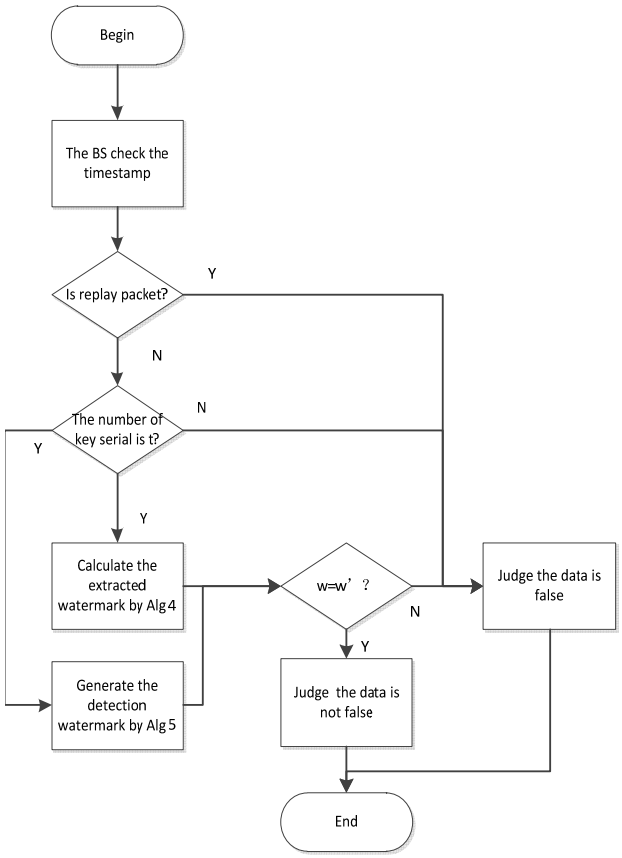


Figure 9. The base station detection process

IV. Simulation Results

In order to achieve the availability and performance of the detection method in this chapter, we use the NS2 and matlab simulation tools, the simulation condition as follows:

We use NS2 to simulate the wireless sensor network environment. The condition is installed like that: 200nodes who are uniformly distributedintheareaof500*500m2, a cluster who contains 10 sensor nodes, a cluster head node, and 5 witness node. The watermark information length m is 8, and the sensing data packet length n is 10.

This chapter involved two algorithms: the one is the reversible watermarking algorithm which is based on difference expansion; the other is the false packets recognition algorithm which is based on digital watermarking technology. So we mainly simulate the two algorithms' performance, and some indicators:

- The noise influence on the watermark information;
- The noise influence on the original data's reduction;
- The probability of detection under different network packet loss rate.

A. The Noise Influence on the Watermark Information

Considering the false packets identification method proposed in this chapter, which judges the false packets according the comparison of the similarity degrees between the extracted watermarking and the calculated watermarking at the base station, Watermark information's change during transmission may cause large misdiagnosis rate. The data embedded by watermark information can't avoid the interferences like noise during the transmission on the wireless channel, so we simulate the watermark information's reductions in the cases of different intensities of Gaussian noise. The specific experimental condition is:

For the 100data, we embed it by watermark information, add noises of different intensities, then we extract the watermark information at the base station and compare it to the original watermark information, at last we get the watermark information's reduction rate. The following results are the means based on the 1000 experimental.

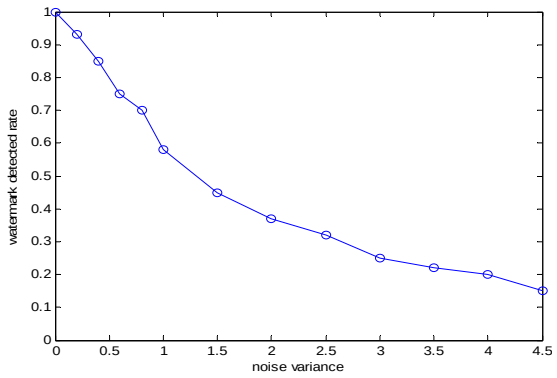


Figure 10. The noise influence on the detection probability of watermarking

From the fig. 10, we can find that the watermark information's correct rate is 100% when the noise variance is 0 and 60% when the noise variance is 1. The correct rate maintains at a high level, which shows that this algorithm can resistant to a certain degree of the noise influence. We can also find that correct rate decreases gradually as the noise variance increases.

B. The Noise Influence on the Restoration of Original Data

The base station extracts watermark information and deducts the data, then gets the sensing data which will be used to judge the situation in the sensing region. So the reduction of the data at the base, which is embedded by watermark information, determines the data's credibility directly. So we simulate the original data's reductions in the cases of different intensities of Gaussian noise. The specific experimental condition is:

The Fig. 11 shows that the original data's reduction rate is 100% when the noise variance is 0 and 80% when the noise variance is 1. It can be found that original data's reduction rate increases gradually as the noise variance decreases.

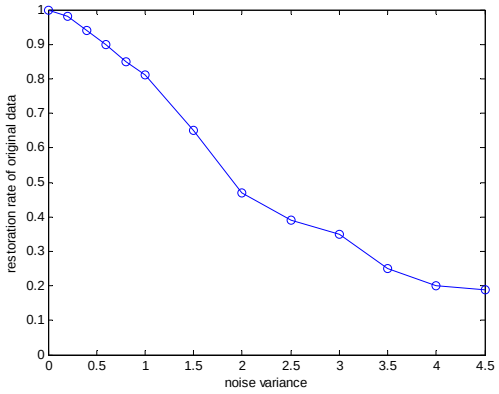


Figure 11. The noise influence on the original data's reduction

C. The Probability of Detection under Different Network Packet Loss Rate.

We will discuss the probability of detection about the false packets identification method based on the watermarking algorithm. The data loss situation is different under different network environment, so the probability of detection of the false packets is different. The following experiment shows the influence on the probability of detection under different packet loss rate at the base station.

We simulate the environment with NS2. The figure followed shows the probability of detection of the false packets under different network environment at the base station. The x-axis represents the packet loss, and the y-axis represents the probability of detection at the base station.

During the experiment, the cluster sent 100 data packets, 20% are duplicate packets, and 80% are false packets. The base station extracted the watermark in formations and judged the correction of the packets by comparison. We got the probability of detection of the

false packets based on several experiments. The circle curve represents there cognition probability of falsified packets, and the Phillips curve represents the probability of detection of the duplicate packets. The results showed in figure 4.15 are the means got by 1000 experiments.

From the fig. 12, we can find that the probabilities of detection of falsified packets and duplicate packets are all greater than 80% when the network packet loss rate is less than 10%. As the network situation gets worse, it shows that the network packet loss rate increases and the probability of detection of the false packets rate reduces. It can also be find that the influence on the probability of detection of duplicate packets is less than falsified packets by network packets loss rate.

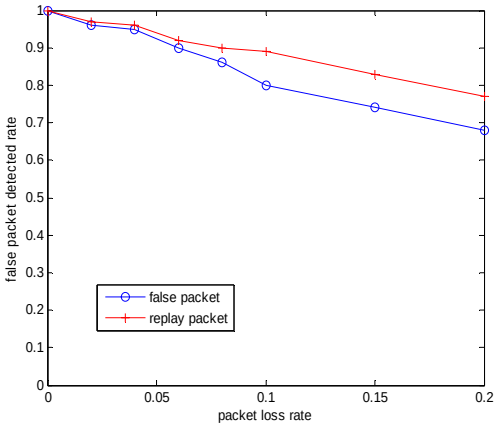


Figure 12. The probability of detection of false packets

V. Conclusions

This paper focuses on how to identify false packets in wireless sensor network using digital watermarking technology. The simulation result prove that the reduction effect of data ,the watermark information, as well as the recognition probability is at a high level with the method proposed in this paper.

Acknowledgment

The work was partially supported by Swedish Research Links [No.348-2008-6212], the National Natural Science Foundation of China [61071093], China's Project 863 [2010AA701202], [CXLX12_0481], and SRF for ROCS, SEM [NJ209002].

References

[1] Guo H, Li Y, Jajodia S. Chaining Watermarking for detecting malicious modifications to streaming data [J], Information Sciences, 2007,177:281-298.

[2] Zhu S C, Setia S, Jajodia S, et al. An interleaved hop-by-hop authentication scheme for filtering false data in sensor networks. Proc IEEE Symposium on Security and Privacy, Berkeley, California, USA, 2004: 259-271.

[3] Ye F, Luo H Y, Lu S W et al. Statistical en-route filtering of injected false data in sensor networks. IEEE Journal on Selected Areas in Communications, Special Issue on Self-organizing Distributed Collaborative Sensor Networks, 2005, 23(4):839-850.

[4] Yang CG, Xiao J. Location-Based pair-wise key establishment and data authentication for wireless sensor networks. In: Proc. of the 2006 IEEE Workshop on Information Assurance. New York: IEEE Press, 2006, 247-252.

[5] I F Akyildiz, W Su, Y Sa, E Cayirci. A Survey on Sensor Networks. In IEEE Communications Magazine, 40(8): 102-144, 2002.

[6] H M Li. A Novel Multi-Path Routing Protocol in Wireless Sensor Networks. In: Proc. of the 4th International Conference on Wireless Communications, Networking and Mobile Computing. Dalian, 2008, 1-4.

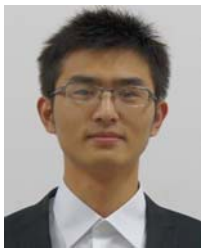
[7] Y Lu, V Wong. An energy efficient multipath routing protocol for wireless sensor networks. International Journal of Communication Systems.2007,pp:747-76

[8] Yongqiang Chen, Yanqing Zhang, Hanping Hu, Hefei Ling. A Novel Gray Image Watermarking Scheme. Journal of Softwear , Vol 6, No 5 (2011).

[9] Mingzhi Cheng, Minchao Xi, Kaiguo Yuan, Chunhua Wu, Min Lei. Recoverable Video Watermark in DCT Domain. JCP, Vol 8, No 2 (2013): Special Issue: Advances in Computational Intelligence.

[10] Cheng Wang, Shaohui Liu, Feng Jiang, Yan Liu. A Robust Scalable Spatial Spread-Spectrum Video Watermarking Scheme Based on a Fast Downsampling Method. JCP, Vol 7, No 9 (2012).

Dengyin Zhang was born in Jiangsu Province in 1964, Professor, received a doctor's degree in signal and information processing engineering from Nanjing University of Posts and Telecommunications, China, in 2004, interested in computer networks, communication systems, signal and information processing.



Mingxiang Wan was born in Jiangsu Province, Mater Candidate of engineering in information and network technology from Nanjing University of Posts and Telecommunications, China, interested in cloud computing, computer networks, digital watermarking.

Chao Xu was born in Anhui Province, received a master's degree of engineering in computer application from Nanjing University of Posts and Telecommunications, China in 2012, interested in computer networks, sensor network, digital watermark.