A New Watermarking Approach for Wireless Sensor Networks

Farid Lalem[1], Ahcène Bounceur[1], Reinhardt Euler[1], and Rahim Kacimi[2]
[1]Lab-STICC UMR CNRS 6285 - Université de Bretagne Occidentale
20, Avenue Victor Le Gorgeu, 29238, Brest, France
[2]Lab-IRIT-UPS - Université de Toulouse
118 route de Narbonne, 31000, Toulouse, France
Email: Farid.Lalem@univ-brest.fr

Abstract

Wireless Sensor Networks are emerging as an innovative technology that can improve our daily lives. Nevertheless, the use of such a technology raises new challenges regarding the development of reliable and secure systems. Securing WSN is thus essential and challenging. This paper proposes a new fully distributed watermarking approach for WSNs. This approach is focused on ensuring integrity and authenticity of data. Moreover, in our approach watermark payload and computational complexity are low. The proposed approach is implemented and simulated with the CupCarbon simulator. The simulation results show that the proposed method is energy efficient.

1. Introduction

Wireless Sensor Networks (WSNs) are distributed embedded systems where each unit is equipped with a certain amount of computation, communication, storage and sensing resources [4].

It is proved that security in this type of networks is of strategic importance, even vital, since their proper functioning involves human lives. Moreover, given the fact that sensors are resource intensive, the traditional intensive security algorithms are not well suited for WSNs [3] Furthermore, malicious attacks such as data modification, data deletion and insertion can affect the quality of data collected by sensor nodes. Therefore, protecting data integrity and authenticity is a necessary process to ensure the quality of sensor data before its use for making decisions.

Watermarking technique is an interesting mechanism to ensure data integrity and authenticity for WSNs. It is the art of hiding data in the host data in a secure manner, where the authorized user can extract and use that data [2]. Watermarking can be classified based on the embedding technique into spatial and frequency domains. A spatial technique embeds the watermark into the data directly while a frequency technique embeds the watermark into the coefficients of the data. It is robust but more complex than spatial techniques [1].

In this paper, we propose a new distributed approach based on a semi-blind watermarking technique. In the step of collecting data, each network node uses the same locally fixed watermark in order to integrate it dynamically into the data packet and transmits it to its neighbors. The watermark verification is performed by the receiver nodes. When the data packet is received, it is used to calculate a new watermark and then compared with the locally fixed watermark. If their values are not the same then the received data packet is rejected.

2 The proposed model

The flowchart of Figure 1 describes the process of the proposed technique and summarizes the phases executed by each node.

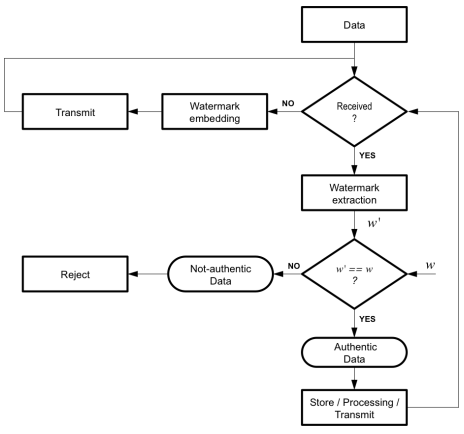

Figure 1. Flowchart of the proposed authentication method.

Any node can be a transmitter or a receiver. When a node receives data, it extracts the watermark w' and compares it with the original watermark w. If these values are the same, the node concludes that the data is authentic

and accepts to receive it for storing, processing or transmitting. Otherwise, the data will be rejected by the node. If the node is a transmitter, then it embeds the watermark into the data before sending it.

3 Performance Evaluation

The objective of this section is to evaluate by simulation the effectiveness of our approach and its energy efficiency. This allows us to validate whether the proposed approach is really useful for saving data authenticity and integrity. In the context of this work, we have used the platform CupCarbon that allows to visualize the simulation process and offers an easy to use and debug interface.

3.1 Results and Discussion

As illustrated by Figure 2, we have generated $N = 15$ sensor nodes including $M = 1$ transmitter node and $K = 1$ malicious node.

The transmitter node S_5 marked with yellow color is programmed to send data in a broadcast mode after the embedding process. All its neighbor nodes S_1, S_2, S_4, S_6, S_7 and S_{10} will receive this data. These nodes will check the data's authenticity and integrity. A malicious node S_{21} marked with red color is programmed to create either false data with false information or to modify all or some of the received data that it is supposed to route. In these two cases, all neighbor nodes of the malicious node will detect its presence in the network and reject the data routed by it. Figure 2 illustrates the situations when a node receives a data and after the watermark extraction. A node will be marked with a green color when the received data is authentic and with an orange color when a malicious node is detected.

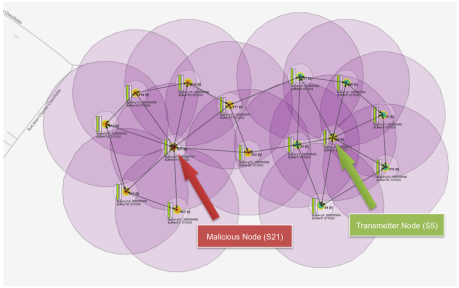

Figure 2. WSN with 15 nodes.

According to simulation results, Figure 3 shows that the proposed watermarking scheme can effectively verify the integrity of the data, and ensure authenticity and reliability when the scheme achieves 100% detection of data tampering and forgery attacks. Moreover, we have calculated the BER (Bit Error Rate) and its value is zero which means that the extracted watermark is perfectly equal to the original watermark. As a result, our approach is absolutely ensuring integrity and authenticity.

Classically, when the number of the nodes of a WSN is increasing, the number of data exchanged between these

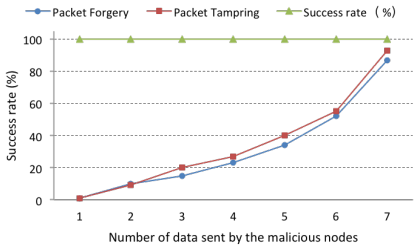

Figure 3. Accuracy of extracted watermark under tampering and forgery attack.

nodes will increase. Therefore, the energy consumption of the network will increase too, which is obvious. However, in our case, the receiver nodes will check the integrity and the authenticity of the received data. If the data is rejected then it will not be routed, which leads to a reduction of the number of exchanged data in the network, which will reduce the energy consumption of the network. Therefore, the proposed approach of watermarking is able to reduce the energy consumption and the traffic of the network considerably due to the self-verification performed by each node.

4 Conclusion

In this paper we have proposed a distributed method based on a semi-blind watermarking technique. Each node in the network verifies the authenticity and integrity of the received data. To study the performance of the proposed method, we have used the simulator CupCarbon. We have considered two types of attacks: data forgery and data tampering. The obtained results show that our method is efficient in terms of energy consumption. Also, the number of exchanged data is reduced drastically by detecting locally in each sensor all the false data. This allows to reduce the network traffic and the energy consumption of the whole network.

References

[1] A. Benhocine, L. Laouamer, L. Nana, and A. C. Pascu. New images watermarking scheme based on singular value decomposition. *Journal of Information Hiding and Multimedia Signal Processing*, 4(1):9–18, 2013.

[2] I.-C. Dragoi and D. Coltuc. On local prediction based reversible watermarking. *Image Processing, IEEE Transactions on*, 24(4):1244–1246, 2015.

[3] B. Harjito, V. Potdar, and J. Singh. Watermarking technique for wireless multimedia sensor networks: a state of the art. In *Proceedings of the CUBE International Information Technology Conference*, pages 832–840. ACM, 2012.

[4] J. L. Wong, J. Feng, D. Kirovski, and M. Potkonjak. Security in sensor networks: watermarking techniques. In *Wireless sensor networks*, pages 305–323. Springer, 2004.