International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Volume 3, Issue 6 (November-December, 2015), PP. 20-22

SURVEY PAPER ON REVERSIBLE WATERMARK AUTHENTICATION SCHEME FOR WSN

Prasad U. Malwatkar[1], Somanath G. Choudhari[2], Sachin R. Jadhav [3], Dinesh B.Chavan[4]
Prof. Subhash G. Rathod[5]
Department of Computer Engineering
Marathwada Mitra Mandal's Institute of Technology
Pune, India
[1]prasad.malwatkar@mmit.edu.in
[2]somanath.choudhari@mmit.edu.in
[3]sachin.jadhav@mmit.edu.in
[4]dinesh.chavan@mmit.edu.in
[5]sgrathod@mmit.edu.in

Abstract— **In some critical application in WSN there is huge demand for authentication. Irreversible modification where made in watermarked data according to previous watermarking based approach. So by using new technique on the basis of prediction error expansion and DCT we are going to achieve the integrity of data in WSN. The authentication scheme based on this technique allows reversible modification in which sensor nodes placed at different location gather the stream data and non-overlapping authentication group composed of two adjacent data group. The first data group is going to compute watermark bits and these beats are embedded into consecutive group before transmission .Verification and complete restoration is done by the sink. According to this paper live copy of data element is buffered rather than entire data group which highly reduce the delay.**

Index Terms **WSN, Reversible authentication, Non-overlapping, and DCT.**

I. INTRODUCTION

Now a days wireless sensor networks is being used widely that contains sensor node with limited capabilities. Sensors can be used for the purpose to monitor the environment and for the other application purpose. The information are send through the node called sink node, the requirement for security in WSN is authenticating integrity of the sensory information. Cryptography is the expensive traditional solutions for integrity because of the limited storage space, computational capacity and energy in sensor nodes.

On the based on digital watermarking some papers [2, 3, 6, 7] are proposed stream authentication schemes. Digital watermarking techniques is much lighter and having no additional overheads than cryptographic algorithms. some critical applications such as medical care or military application which requires the absolutely accurate original data.

In this paper we proposed a reversible authentication scheme based on watermarking algorithm for WSN. This scheme can verify the collected data by the embedded watermark bits, and restore the accurate original data completely. That meets the demand of the original data in some specific application in WSN's.

II. RELATED WORK

Kamel and Guma [3] they proposed a FWC-D scheme which is lightweight forward chaining watermarking scheme, using the hash function watermark is generated and organize into the one data group, and generated watermark are embedded into the previous data group for a forward-chaining. Chen et al. [2] proposed a DTA (Data Transparent Authentication) scheme in where it will authenticates data stream by adjusting inter packet delay. In this scheme there is requirement that no change in the original data and no extra communication overhead.

TinySec [1] is completely implemented in link layer security protocol for Wireless Sensor Network, which provides data integrity and confidentiality authentication. By calculating a 4 byte Message Authentication Code (MAC) is attached with packet. TinySec is designed to achieve a balance between security and limited resource, but still occurs additional communication overhead. Yang et al. [4] 'A reversible data hiding algorithm' that uses PE (prediction errors) in the color variation domain for images of mosaic effect with the Bayer's color filter array is proposed.

Zhang et al. [5] monitor the sensory data combined them from the whole network at a various time snapshot as an image. Each and every node is considered as a pixel with reading and represents the pixel's intensity. So, watermark is

applied on the sensor data as an image and robust for JPEG compression techniques.

III. PROPOSED WORK

Wireless sensor networks includes three types of nodes: sensor node, transmission node and sink node. Sensor nodes annually send their collected data to the sink with the help of the transmission nodes. Collected data is made available as a part of the data stream. The watermark bits is produced and embedded in the one node and validate in the other node of the transmission. So we can says that the sensor node is to encode where data is buffered and managed, the sink is for decoding, and the intermediate nodes responsible for the transmission.

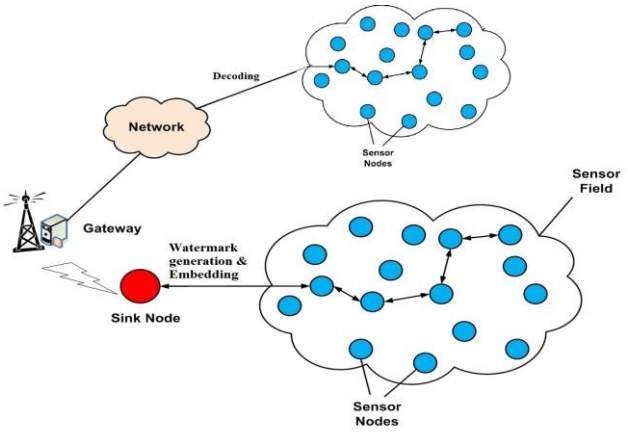

Figure 1 WSN Architecture with watermarking schemes.

Sensor node collects data firstly in one groups, and adjacent data groups makes the non-overlap authentication group.

The watermark bits are calculated from the one group and embed in to the other one just before transmission. At the

Receiver side, sink organizes the data groups, checks the watermark bits by calculating and extracting and then restores the genuine data.

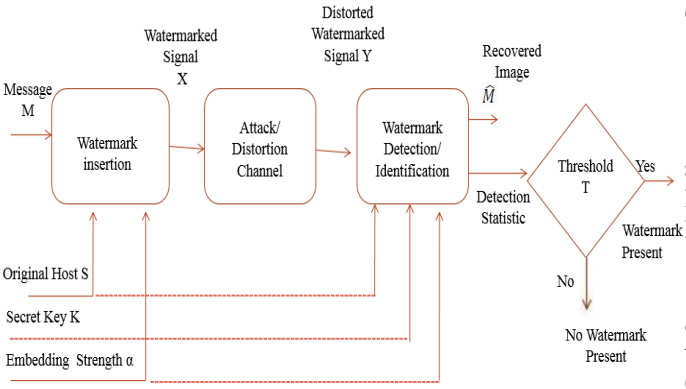

Figure 2 Watermark Embedding and Extraction

A. Grouping

In this paper dynamically grouping is take up for ensuring the number of elements from the each group is unstable. For convenience, we declared an infinite data stream S which is sensed by sensor, and data element in the stream is denoted as si. When a data element si is available in the stream in one data group, the secure hash value hi is calculated according to the pre-distribution key K. To get fixed length output we used MD5 or SHA-1 as hash function.

In pursue to take the same groups at both ends, we calculate the secure hash value hi of the watermark data element s0. Declare as a data elements as organizing point if its hash value

$$hi \bmod m = = 0;$$

Where m is a parameter group select the medium length of data group. The watermark is generated from the one data group and then embed into the other data group, so the two groups are noted as originated group and courier group.

B. Watermark Generation and Embedding

This module is the main module, which does the calculation of watermark bit based on the hash values Hi, and then the output is converted into binary format to send over the network by embedding watermark bit to the original message M.

C. Watermark extraction Decoding

Decoding module is the reverse of user module, it does the matching process for prediction error and watermark bit. If the authentication successful then file decoding is done otherwise system returns to failure.

IV. CONCLUSION

In this paper, we proposed reversible watermarking authentication scheme for WSN. This scheme authenticates the originality of the data and recovers genuine data completely. Data is transferred after the watermark embedding process, so the delay not affect on actual time stream. No communication overhead is occurs with less computation.

REFERENCES

C. Karlof, N. Sastry, D. Wagner, TinySec: a link layer security architecture for wireless sensor networks, in: Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, Baltimore, MD, USA, 2004, pp. 162–175

S.Q. Chen, S.P. Chen, X.Y. Wang, Z. Zhang, S. Jajodia, An application-level data transparent authentication scheme without communication overhead, IEEE Transactions on Computer 59 (7) (2010) 943–954.

I. Kamel, H. Guma, A lightweight data integrity scheme for sensor networks, Sensors 11 (2011) 4118–4136.

W.J. Yang, K.L. Chung, H.Y.M. Liao, Efficient reversible data hiding for color filter array images, Information Sciences 190 (2) (2012) 208–226.

W. Zhang, Y.H. Liu, S.K. Das, P. De, Secure data aggregation in wireless sensor networks: a watermark based authentication supportive approach, Pervasive and Mobile Computing 4 (5) (2008) 658–680.

H. Guo, Y. Li, S. Jajodia, Chaining watermarks for detecting malicious modifications to streaming data, Information Sciences 177 (1) (2007) 281–298.

I. Kamel, H. Guma, Simplified watermarking scheme for sensor networks, International Journal of Internet Protocol Technology 5 (2010) 101–111.