Review on Data Authenticity and Integrity in Wireless Sensor Networks Based on a Watermarking Approach

Prachi Shukla, Suresh Gawande, Sher Singh

[1] Research Scholar, Department of Electronics and Communication Engineering,
Bhabha Engineering Research Institute, Bhopal,

[2] Assistant Professor, Head, Department of Electronics and Communication Engineering,
Bhabha Engineering Research Institute, Bhopal.

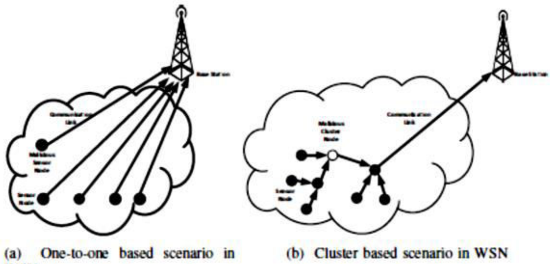
[3] Assistant Professor, Department of Electronics and Communication Engineering,
Bhabha Engineering Research Institute, Bhopal.

Abstract: Wireless Sensor Networks are emerging as an innovative technology that can change and 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 imperative and challenging. Unfortunately, he conventional security measures based on data encryption are not well suitable to WSNs due to energy and computational resource constraints. However, watermarking techniques usually have light requirements of resource. This approach is focused on ensuring integrity and authenticity of data. Moreover, in our approach watermark techniques is discussed.

Introduction: A wireless device network (WSN) may be an assortment of little sized, distributed, and self-configurable sensors (also referred to as nodes), deployed within the space for specific tasks. Device nodes have the power to sense totally different parameter of interest like temperature, pressure, motion, and so on. The perceived info is then communicated with the sink conjointly referred to as a Base Station (BS) directly or hop by hop communication. WSNs may be used for a variety of applications, like environmental observance, patient observance, military police investigation, traffic transportation, and so on.Due to the unattended atmosphere and therefore the distributed design of WSN, nodes in arc usually in danger of being compromised by Associate in nursing resister. Because the nodes are usually deployed in unreliable environments, they'll face differing kinds of attacks, like packet drop, packet forgery, knowledge and packet replay. Confidentiality, integrity, freshness and dependableness arc the essential security necessities that has to be that has to each knowledge integrity protection theme. To realize authentication, integrity, possession and possession usage of information measure, watermarking permits to embedding watermark with the info. In watermarking method, every device node embeds a novel watermark to device knowledge and will verify the integrity of information. Watermarking techniques are originally designed to shield transmission content and later for defense of relative databases. However, the character of streaming atmosphere imposes variety of challenges on the applying of watermarking based mostly security techniques for WSN, as given within the following:

- Large sized watermark data should be efficientlymanaged;
- Watermarked data should be securely transmitted.
- Bandwidth utilization must beminimized;

To ensure the integrity of information in WSN, several researchers planned watermarking techniques. Most of the present watermarking schemes generate the watermark from uneven cryptography functions, adding distinctive digits within the Least Significant Bit (LSB) and a few different helpful functions. However, uneven cryptographically schemes as computationally overpriced and caused further storage overhead on WSN. Due to the resource strained nature of WSN, the utilization of uneven cryptography functions as computationally overpriced, that cause additional energy consumption at nodes.



(a) One-to-one based scenario in WSN

(b) Cluster based scenario in WSN

Fig. 1Cluster Scenario in WSN

Related to Work: In this section we'll discuss some existing work handling the credibleness and therefore the integrity of information in WSNs mistreatment digital watermark based mostly techniques. The technique bestowed in (Sun et al. 2013) relies on a fragile watermarking methodology to shield knowledge integrity in WSNs. Collected knowledge from every supply sensors are encapsulated into new knowledge packets, that contain numerous knowledge numerous for specific sensing sources, no intrusions to the initial knowledge ar performed. Instead, redundant house of information bytes is used. Also, supply sensors use a unidirectional hash operate for collected knowledge to make watermark info, that is then related to the info by embedding it into the redundant house of the targeted bytes. At the bottom station aspect, a watermarking algorithmic rule is meant to extract the watermark info, which is compared to recalculated watermark info so as to verify the integrity of the info throughout the transmission.

In (Kamel and Juma 2011), the authors planned a fragile watermarking algorithmic rule (FWC-D) to notice unauthorized alterations in WSN knowledge streams. FWC-D organizes the device knowledge readings into teams of constant sizes. FWC-D uses a hash operate, that is applied to the concatenation of all individual knowledge parts within the cluster together with a secret key to calculate the watermark. The hash operate may be MD5 or SHA. The watermark is keep within the previous cluster to create it additional for the wrongdoer to insert or delete a whole cluster while not detection. Mistreatment the key, the receiver will extract the watermark (calculated at the transmitter side) from the received knowledge. To verify the integrity of the received cluster, the receiver recalculates the water- mark and checks against the extracted watermark. If the 2 watermarks are matching, the cluster is taken into account authentic; else, the cluster is reportable as not authentic.

In (Wang et al. 2011), the authors planned a multiple watermarking methodology, referred to as Multi-Mark. It consists of Associate in Nursing annotation half and a fragile half. At the info supply node, the annotation watermark is embedded into the routine observance knowledge. Then, the delicate watermark is generated and embedded into the obtained results of results of watermark embedding. Once the once watermarked knowledge ar transmitted through the WSN any mistakes would possibly happen due to the dangerous network condition or malicious attacks. They will be detected from the sink, wherever the meddling detection relies on authenticating fragile watermarking technique. Once required, the annotation watermark may be extracted.

In (Ding et al. 2015), the authors planned Associate in Nursing authentication theme (RDE) supported a lossless fragile watermarking algorithmic rule for WSNs. supply sensors use a unidirectional hash operate to come up with the watermark info counting on the adjacent knowledge and so plant it into these knowledge. When receiving the info, the manager node restores the initial knowledge and verifies the dependableness. Associate in Nursing RDE theme will verify the sensory knowledge through the embedded watermark bits, and restore the initial knowledge fully.

In (Dong and Li 2009), the authors planned algorithms for identity generation, embedding and sleuthing. The identity of a causing node was generated by remodeling a key and therefore the knowledge assortment time. The reworked result fashioned the watermark is embedded into the info to send. The receiving node judges the credibleness of the info by confirmatory this watermark. Once the watermark was detected, the info would be keep and transmitted. Otherwise the info would be discarded.

Most of the planned solutions ar supported centralized algorithms during which the watermarked knowledge is shipped entirely to be verified either by the cluster head or by the bottom station. Sadly, the centralized models suffer from high communication overheads in transmittal the complete knowledge for transmittal. As mentioned before, the most a part of the energy of any device is consumed throughout the transmission instead of the process task. Therefore, it is higher to think about the distribution of the integrity and credibleness detection in or-der to attenuate the energy consumption. Then, every device node will check domestically the integrity and therefore the credibleness by extracting the watermarked knowledge from the received knowledge. This permits to get quickly the credibleness of information. The node can reject the info just in case of a non-authentic watermark, otherwise, it'll settle for it. What is more, if the authentication of {the knowledge the info the information} is checked by the centralized destination and therefore the data is fallacious, all the nodes of the communication path {that can which will that may} route {the knowledge the info the information} to the centralized destination will consume loads of energy whereas transmittal fallacious data. This is often inappropriate with relevance energy constraints within the device nodes.

Sun et al. [15] addressed the info integrity downside in WSN by mistreatment digital watermarking. The theme provides protection against the assorted sorts of attacks, like packet forgery attack, selective forwarding, packet replay, packet transfer delay, and packet meddling. The limitation of this theme is that lost knowledge can't be detected fully at receiving aspect. Panah et al. [3] explored the information integrity downside by embedding many signature codes in data stream mistreatment digital watermarking. The most purpose of those signature codes is to preserve the applied math properties of information streams before passing to the embedding watermarks. one in every of the shortcomings of the same theme is that secret writing method has to examine the complete length of streaming knowledge and should be performed on-line, that incurs further overhead.

Zhang et al. [28] used a digital watermarking theme to manifest knowledge in WSN, which provides inherent support for in-network process and finish to finish authentication. This theme will with success notice the info notice. Chow dynasty et al. [17] planned digital watermarking theme to forestall sensory knowledge from eavesdropping and meddling attacks. The mentioned theme is efficient in terms of storage similarly as detection of packet loss attack and meddling attack.

Kamel et al. [25] planned a distortion free watermarking theme for secure sensory digital communication in WSN. This watermarking theme is powerful against numerous sorts of attacks like knowledge attack, insertion attack, and deletion attack. Similarly, in one in every of the opposite works, Kamel et al. planned a fragile watermarking theme, referred to as lightweight weight bound watermarking theme to shield the integrity of information in WSNs. The planned theme detects unauthorized modifications in knowledge streams. The planned theme doesn't give knowledge give.

Wang et al. [9] proposed an information hiding technique to secure data transmission in WSN. The proposed scheme especially designed to stop attacks with forge identities by attacker. An area efficient arrangement called Bloom filter, is employed to embed secret information into original data. Experimental results and performance evaluation show that embedded information can detect malicious node with forge identity. However, proposed scheme isn't efficient to detect the attacks exercised by the malicious nodes against the integrity of the info. Copyright protection of the sensory data is additionally a challenging issue in WSN. Xiao et al. [30] proposed a strong watermarking algorithm to guard copyright of knowledge. The embedded watermark consists of numerical properties of sending time of packet. The performance of proposed robust scheme is evaluated on the idea of three parameters. i.e., without key method, with 8-bit key length method, and with 16-bit key length.

Wang et al. [8] proposed a digital watermarking technique to guard the copyright of knowledge in WSNs. The watermark embedded in original data by using both the LSB and MSRB bits of knowledge field. Both, the first data and watermark are sent to BS for verification of copyright of knowledge. Additionally to the copyright, a lookup table is employed to enhance the efficiency of knowledge parsing. Experimental results and analysis of the proposed scheme show that data is authenticated and reliable during transmission.

Problem Identification: Due to the unattended environment and therefore the distributed architecture of WSN, nodes in are often in danger of being compromised by an adversary. Because the nodes are often deployed in unreliable environments, they'll face differing types of attacks, like packet drop, packet forgery, data modification and packet replay. Confidentiality, integrity, freshness and reliability are the essential security requirements that has got to be fulfilled by every data integrity protection scheme. To realize authentication, integrity, ownership and efficient usage of bandwidth, watermarking allows to embedding watermark with the info. To make sure data integrity and authenticity in wireless sensor networks, we'll now present the proposed method that uses a semi-blind watermarking technique. this system is convenient for the spatial domain since the watermark are often embedded directly into the first data so as to scale back the complexity by avoiding several additional operations and to save lots of the node energy. The tactic consists of two phases: an embedding phase and an extraction phase. Counting on its role, each node can act as a transmitter or a receiver.

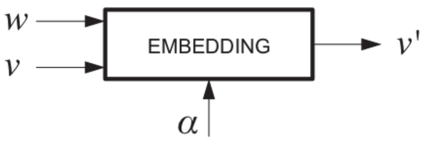


Fig. 2 Watermark embedding scheme.

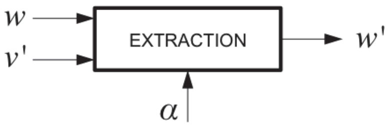


Fig. 3Watermark extraction scheme.

The nodes in WSN are application specific and are tightly coupled with the physical environment and provides distributed services. This differs the implementation of WSN from other wireless networks.

Proposed Scheme: In this section, we will present the proposed authentication method for data integrity and authenticity supported digital watermarking during a WSN. First, we'll present the overall idea of the approach. Then, we'll present the algorithms for the embedding and extraction processes.The flowchart of Figure 4 describes the method of the proposed technique and summarizes the phases executed by each node. Any node are often a transmitter or a receiver. When a node receives data, it extracts the watermark wJ and compares it with the first watermark w. If these values are an equivalent, the node concludes that the info is authentic and accepts to receive it for storing, processing or transmitting. Otherwise, the info are going to be rejected by the node. If the node may be a transmitter, then it embeds the watermark into the info before sending it.

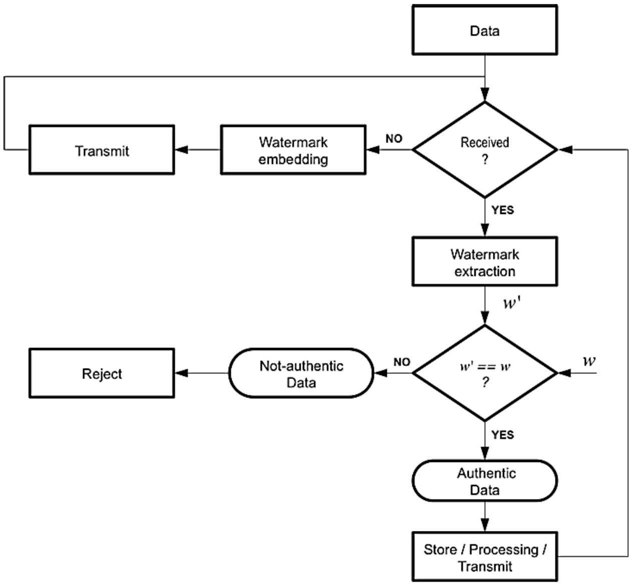


Fig. 4.1 Process of the proposed technique

Expected outcomes: In this work, we tend to propose a secure knowledge transmission theme in WSN supported a watermarking technique. Although, zero watermarking technique has already applications within the security of transmission content and relative databases. However, to the most effective of our information, generation of watermark supported the employment of the characteristics of the initial knowledge and its application to the info integrity in WSN atmosphere is that the during this research paper. In zero watermarking technique, no external knowledge from the atmosphere is employed within the watermark generation method. A watermark is generated on the idea of sensor's own knowledge characteristics, like knowledge length, digit incidence frequency, and knowledge sensing time of device nodes. Every device node embeds a novel watermark to device knowledge and send it to the information. Then, verify the integrity of information by mistreatment the embedded watermark in contrast to previous watermarking schemes, our planned theme doesn't involve any uneven cryptography functions.

References:

[1] Chandan Kumar, Amit Kumar Singh &Pardeep Kumar. Dual watermarking: An approach for securing digital documents. Springer Notes, Multimedia Tools and Applications volume 79, ages7339–7354(2020)

[2] UmairKhadam, Muhammad Munwar Iqbal , MeshrifAlruily, Mohammed A. Al Ghamdi, Muhammad Ramzan, and Sultan H. Almotiri. Text Data Security and Privacy in the Internet of Things: Threats, Challenges, and Future Directions, Recent Advances in Security and Privacy Issues for Internet of Things Applications, Hindavi Publications. 2019.

[3] A. S. Panah, R. van Schyndel, T. Sellis, and E. Bertino, "In the shadows we trust: A secure aggregation tolerant watermark for data streams,"IEEE 16th International Symposium on a, In World of Wireless, Mobile and Multimedia Networks (WoWMoM), pp. 1-9,2018.

[4] Q. Ding, B. Wang, X. Sun, J. Wang, and J. Shen, " A reversible watermarking scheme based on difference expansion for wireless sensor networks," International Journal of Grid Distribution Computing Vol.8, No.2, pp.143-154,2016.

[5] R. Jain and M. Jain, "Digital image watermarking using 3-level dwt and fft via image compression," International Journal of Computer Applications, vol. 124, no. 16, 2015.

[6] C. S. Gosavi and S. N. Mali,"Video authentication and copyright protection using unique watermark generation technique and singular value decomposition, International Journal of Computer Applications, vol. 123, no. 3, 2015.

[7] A. Paul and E. Sunitha, "Distortion less watermarking of relational databases based on circular histogram modula-tion," in International Conference on Circuit, Power and Computing Technologies (ICCPCT), pp. 1-5, 2015.

[8] B. Wang, J. Su, Y. Zhang, B. Wang, J. Shen, Q. Ding, and X. Sun, " A Copyright Protection for Wireless Sensor Networks based on Digital Watermarking," International Journal of Hybrid Information Technology. 8, No. 6, pp. 257-268, 2015.

[9] B. Wang, H. Qian, X. Sun, J. Shen, and X. Xie, " A Secure Data Transmission Scheme Based on Information Hiding in Wireless Sensor Networks," In International Journal of Security and Its Applications 9, No. 1, 2015.

[10] S. Sultana, G. Ghinita, E. Bertino, and M. Shehab, "A lightweight secure scheme for detecting provenance forgery and packet drop attacks in wireless sensor networks," in IEEE Transactions on Dependable and Secure Computing, 2014.

[11] S. R. Hussain, C. Wang, S. Sultana, and E. Bertino, "Secure data provenance compression using arithmetic coding in wireless sensor networks,"IEEE International in Performance Computing and Communications Con-ference (IPCCC), pp. 1-10,2014.

[12] X. Shi and D. Xiao, "A reversible watermarking authenti-cation scheme for wireless sensor networks," Information Sciences, vol. 240, pp. 173-183, 2013.

[13] A. Khan and S. A. Husain, " A fragile zero watermarking scheme to detect and characterize malicious modifications in database relations," The Scientific World Journal, vol. 2013.

[14] S. Sultana, M. Shehab, and E. Bertino, " Secure prove-nance transmission for streaming data," in IEEE Trans-actions on Knowledge and Data Engineering, vol. 25, no. 8, pp. 1890-1903, 2013.

[15] 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, pp. 407-416, 2013.

[16] R. K. Tripathi, " Base station positioning, nodes localization and clustering algorithms for wireless sensor networks," Dissertation, Indian Institute of Technology Kanpur, 2012.

[17] L. Zhou and Z. Zhang, "A secure data transmission scheme for wireless sensor networks based on digital watermarking," in 9th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD),pp. 2097-2101, 2012.

[18] S. Sultana, E. Bertino, and M. Shehab, "A provenance based mechanism to identify malicious packet dropping adversaries in sensor networks," in 31st International Conference on Distributed Computing Systems Workshops (ICDCSW),pp. 332-338,2011.

[19] I. Kamel and H. Juma, "A lightweight data integrity scheme for sensor networks," Sensors, vol. 11, no. 4, pp.

[20] H. Hu and Z. Yang, "Spatial correlation-based distributed compressed sensing in wireless sensor networks," in 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM), 2011.

[21] R. M. Prasad and S. Koliwad, "A robust wavelet-based watermarking scheme for copyright protection of dig-ital images," in International Conference on Computing Communication and Networking Technologies (ICCCNT), pp. 1-9, 2010.

[22] I. Kamel and H. Juma, "Simplified watermarking scheme for sensor networks," In International Journal of Internet Protocol Technology 5, No. 1-2, pp. 101-111, 2010.

[23] R. Hasan, R. Sion, and M. Winslett, " The case of the fake picasso: Preventing history forgery with secure provenance," in FAST, vol. 9, pp. 1-14, 2009.

[24] I. Kamel, " A schema for protecting the integrity of databases," computers and security, vol. 28, no. 7, pp. 698-709, 2009.

[25] I. Kamel, O. Al Koky, and A. Al Dakkak, "Distortion-free watermarking scheme for wireless sensor networks," in International Conference on Intelligent Networking and Collaborative Systems (INCOS), pp. 135-140, 2009.

[26] M. N. Halgamuge, M. Zukerman, K. Ramamohanarao, and H. L. Vu, " An estimation of sensor energy consumption," Progress In Electromagnetic Research B, Vol. 12, 259-295, 2009.

[27] S. Gowrishankar, T. D. H. Manjaiah, and S. Sarkar, " Issues in Wireless Sensor Networks, "in Proceedings of the World Congress on Engineering., London, U.K, July 2008.

[28] W. Zhang, Y. Liu, S. K. Das, and P. De, "Secure data aggregation in wireless sensor networks: a watermark based authentication supportive approach," Pervasive and Mobile Computing, vol. 4, no. 5, pp. 658-680, 2008.

[29] H. Juma, I. Kamel, and L. Kaya, "Watermarking sensor data for protecting the integrity," in International Confer-ence on Innovations in Information Technology(IIT), pp. 598- 602, 2008.

[30] R. X. Xiao, X. Sun, and Y.Yang, " Copyright Protection in Wireless Sensor Networks by Watermarking," in 8th International Conference on Intelligent Information Hid-ing and Multimedia Signal Processing (IIHMSP)

[31] H. Guo, Y. Li, and S. Jajodia, "Chaining watermarks for detecting malicious modifications to streaming data," Information Sciences, vol. 177, no. 1, pp. 281-298, 2007.

[32] J. L. Wong, J. Feng, D. Kirovski, and M. Potkonjak, "Se-curity in sensor networks: watermarking techniques," in Wireless sensor networks. Springer, pp. 305-323, 2004.

[33] J. Fang and M. Potkonjak,"Real-time watermarking tech-niques for sensor networks," in Electronic Imaging Inter-national Society for Optics and Photonics, pp. 391-402, 2003.