5.6 Water Marking Techniques

5.6.1 The Attack Models

Compared to wired networks, the WSNs that deploy in the extreme environment face more threats, and what is more, the public communication protocol adopted by WSNs exacerbates the risk of physical tampering.

The sensed node owns limited computational capabilities and energy resources which increase the difficulty of designing security protocols.

Main attack models are as follows,

(i) **Packet tampering -** A malicious node added to WSNs tampers with the value of the packets and forwards the tampered packets which can lead to extremely serious consequences in some special cases.

(ii) **Packet forgery -** A malicious node added to WSNs keeps sending the fake packets to other nodes, greatly increasing network traffic and resulting in wasting energy of the whole WSNs.

(iii) **Selective forwarding -** A malicious node added to WSNs deletes partial packets and forwards some packets to destination selectively. The data loss may cause the bad situation that the sink node fails to make the correct response.

(iv) **Packet replay -** A malicious node added to WSNs forwards the packets that have been forwarded, once more or repeatedly to other nodes which will cause the traffic congestion and energy waste.

(v) **Transfer delay -** A malicious node added to WSNs forwards the packets later than the predetermined time which will lead to the fact that the sink node drops the packets due to the timestamp.

5.6.2 Watermarking Technique

1. It is WSNs data integrity protection strategy based on fragile digital watermarking to protect the sensed data from the above four categories of attack models.
2. This technique makes use of the characteristic that the fragile watermarking is sensitive to modification. Once the host data is modified, the watermark is destroyed. The malicious node without the prior knowledge of watermarking algorithms cannot effectively restore real data.
3. Data tampering and data forgery are similar, which can be seen as malicious data generated by malicious nodes. The malicious sensed data generated by the malicious node cannot be verified by watermarking technique/algorithm after reaching the sink node.
4. The algorithm introduces the packet sequence number which is used for positioning the added packet or deleted packet.
5. This watermarking algorithm includes three processes, namely, digital watermark generation, digital watermark embedding, and digital watermark extraction.
6. **Firstly,** each sensing node collects the sensing data and generates the digital watermark according to the fragile watermarking algorithm. **Secondly,** the watermark is merged into the sensed data through the predefined rule to form a data packet that is transferred to the sink node through the transmission node. The packet may suffer from an unreliable transmission and face different kinds of attacks. **Thirdly,** the sink node receives the data and then extracts the watermark and restores the sensed data according to the predefined rule. The restored data is used to generate watermark according to the same algorithm. The data integrity is verified by comparing the regenerated watermark

and the extracted watermark. If the regenerated watermark is not the same as the extracted watermark, the data is proved to be tempered during transmission. Otherwise, the data is proved safe.

7. The digital watermark is copied with the copy of the digital media, and the process is hidden. If the predefined method is not known, the digital watermark is difficult to detect.
8. **Watermark Generation Algorithm -** The watermark generation algorithm uses the SHA-1 hash function to calculate the hash value. SHA-1 hash function not only guarantees data integrity, but also has a lightweight feature that uses 65% less memory than other hash algorithms, such as the MD5 algorithm, which is more suitable for resource-constrained WSNs. The secret key K is the specific information that is only known to the sender and the receiver.
9. **Watermark Embedding Algorithm -** The watermark embedding algorithm improves from the following two aspects – (i) The packet is redesigned and added m bits for watermark to ensure that the watermark is transparently embedded in the packet. It does not cause any interference to the data and meets the high-precision requirements. (ii)In order to solve the vulnerabilities brought by fixed embedding location, algorithm introduces a new position random function to dynamically calculate the watermark embedding position which effectively solves potential vulnerabilities and greatly improves the security of the algorithm.
10. **Watermark Extraction Algorithm -** When the packet is transmitted to the sink node, the sink node extracts the digital watermark information and restores the sensed data.