Data Aggregation Integrity inWireless Sensor Networks Using Cross Layer Watermarking

C.Manjula[1] | R.Pooja[2] | K.Ramya[3] | V.Saranya[4]
[1](Department Of ECE, KTVR knowledge park for engineering and technology, cbe, India, manjulasekar94@gmail.com)
[2](Dept Of ECE, KTVR knowledge park for engineering and technology, cbe, India, poojharajan20@gmail.com)
[3](Dept Of ECE, KTVR knowledge park for engineering and technology, cbe, India, kramya551995@gmail.com)
[4](Dept Of ECE, KTVR knowledge park for engineering and technology, cbe, India, saranktvr@gmail.com)

Abstract*—Ensuring data aggregation integrity in heterogeneous wireless sensor networks using cross layer watermarking mechanism. The proposed security method ensures maximum security based on new fragile watermarking technique which involves a dynamic embedding mechanism and a cross layer approach. Comparing to the existing security solution, our proposed method has an efficient integrity of data for both homogeneous and heterogeneous sensor networks.*

Keywords*— *Cross-layer watermarking, data aggregation integrity, heterogeneous wireless sensor network

1. INTRODUCTION

Wireless sensor network is spatially distributed autonomous sensors. Wireless sensor networks involves monitoring environmental conditions such as temperature, sound, pressure, wind direction, speed etc and to pass their data through the network to a main location. Wireless sensor networks have application in wide range like military application for security purpose and in Law enforcement etc.

Now a day's networks are bidirectional and also have control of sensor activity. Basically a network is made up of source nodes and a sink node. Sink node acts as a base station. Packets from source to destination are transmitted through intermediates nodes. The source sends data packet with source id and destination id to its neighboring nodes.

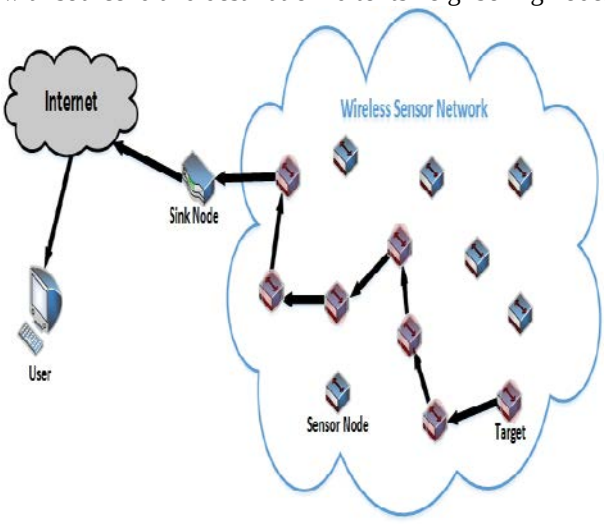

Fig. 1. Network Model

If the received data packet dose not matches the intermediate nodes it forwards to its next neighboring nodes using routing path, likewise the data is transmitted to the destination through minimum path using routing table. The intermediate nodes may be a hacker or malicious nodes and the data may be used according to the need of the hackers or destroyed.

Hence data aggregation integrity is major importance in wireless sensor networks for both homogeneous and heterogeneous network

2. LITERATURE SURVEY

Data aggregation techniques are used to reduce the amount of data communication with in a wireless sensor networks and thus conserves battery power. Data are needed to be collected by individual sensor and processed to produce data representative of the entire wireless sensor network. Sensors can send their values to certain special nodes are called aggregators. Each aggregator condenses the data prior to sending it on.

In privacy homomorphism [PH] [10] has been used in heterogeneous wireless sensor networks (CDAP [9], SDAKM [6]). The cipher text is encrypted using PH and at the receiver side the PH decryption is applied to get the plain text. There is no need for decryption other than PH at receiver side to get plain text.

Watermarking technique [2] [4] has a lightweight characteristic and used to protect data transmission in wireless sensor networks. This technique is energy efficient and reduces delay. In multimark [5], the tampering is detected using fragile watermark and the personal information is protected by using annotation watermark.

In digital watermarking [3], the source sensors uses a one way hash function for collected data to create watermark information and it is embedded in to the redundant space of the data packet. Aggregation approach [4] can be applied to reduce the amount of sending data.

End- to- End guarantee aggregation approach required to ensure good data reception. End- to- End method based on elliptic curve cryptography.Elliptical Curve Diffie-Hellman Key Exchange (ECKE- 1) protocol [7] is vulnerable to key- compromise impersonation attacks, so the improved protocol ECKE- 1N is used overcome the drawbacks of ECKE-1.

3. EXISTING METHOD

The Existing method are not efficient for data aggregation security because the encryption and decryption process produce computation complex at each aggregation node and also they are not suitable for heterogeneous sensor networks.

In privacy homomorphism, the homogeneous nodes encrypt sensed data and send them to the heterogeneous nodes and aggregated using privacy homomorphism algorithm, the encryption mechanism will produce overloads to homogeneous nodes which have a limited resources.

This encryption algorithm injects key distribution mechanism which has energy inefficient. Traditional watermarking technique was used in the multimedia research area to secure the integrity of multimedia data [5] [6] [7].

In proposed method the watermarking technique used to guarantee data aggregation process in difference to privacy homomorphism based protocols. Therefore we use new security protocol called CLWDA (Cross Layer Watermarking Based Aggregation) which is based on dynamic embedding mechanism and cross layer algorithm to provide the security.

PROPOSED METHOD

In our proposed method we are using two categories a) Fragile watermarking (FW) classification which is applicable for homogeneous sensor nodes b) Reinforced fragile watermarking (RW) classification which is applicable for heterogeneous sensor nodes, here keys are used to generate and extract the watermark.

Fragile watermarking technique is used to generate and verify the watermark. When collecting data, each node generates a watermark and integrates it in the data packet and transmits it to the next node in the routing path. After receiving the data packet, the receiver node executes a verification algorithm to check the integrity of the received data.

F Fragile watermark generation algorithm combines the sensed data and the MAC address of the sensor nodes using XOR function obtained result is hashed with MD5 (Message Digest) the message is compressed to a fixed size (128 bits). The generated watermark is hidden in the data packet on a proposed cross layer based dynamic embedding mechanism

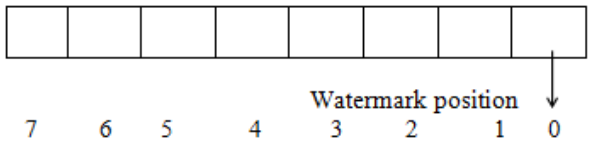

Fig. 2. Integration of watermark

The watermark generation algorithm is reinforced at the level of heterogeneous nodes, where generated watermark is encrypted.

At receiver end, new watermark is compared with the received watermark. If the two watermark are not identical then that the data packet is rejected.

4. SIMULATION METHOD

NS2 simulation software is used to evaluate our proposed method. It is open source software. Here, C++ and TCL (Tool Command Language) object oriented languages are used. AODV (Ad-Hoc On Demand Distance Vector Routing Protocol) is a reactive type protocol. It is suitable for both homogeneous and heterogeneous sensor networks.It does not need frequent updating of routing table. In AODV, the topology information is only transmitted by nodes on-demand. In our proposed method we have used this protocol and made changes in the protocol (AODV) according to our concept.

Comparison between the existing ECDH and our proposed watermarking method:

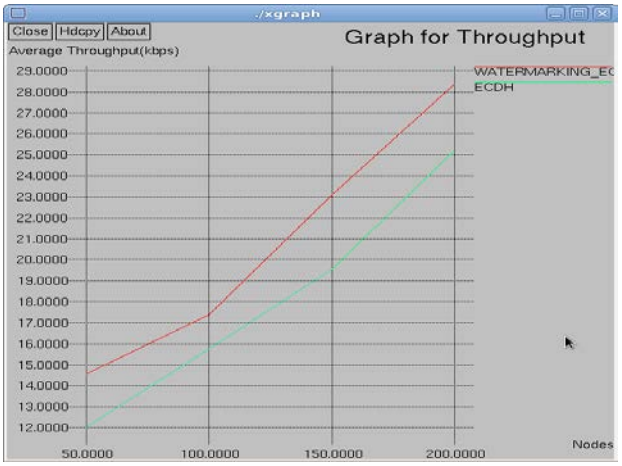

Fig. 3. Average Throughput versus Nodes

The above figure shows the graph of Average Throughput versus Nodes of both ECDH (Elliptic Curve Diffie-Hellman) and the Watermarking_ECDH. It can be observed that the input processing of Watermarking_ECDH is better than ECDH.

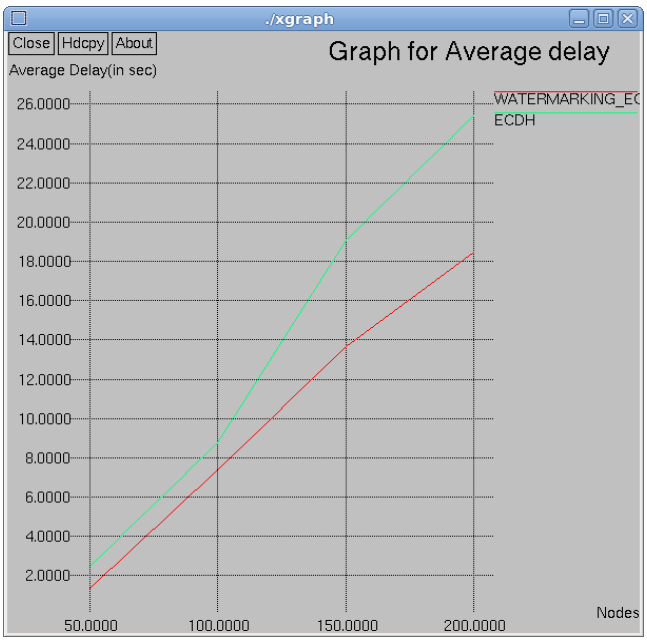

Fig. 4. Average Delay versus Nodes

The above figure shows the graph of Average Delay versus Nodes of both ECDH (Elliptic Curve Diffie-Hellman) and the Watermarking_ECDH. The delay is minimized in Watermarking_ECDH while compared to ECDH.

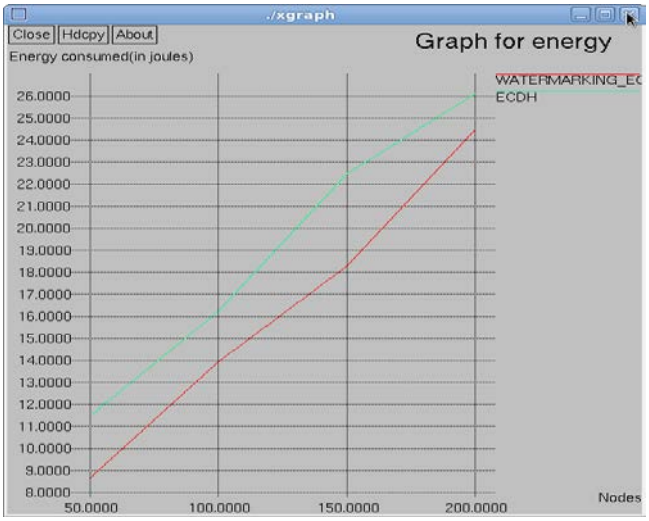

Fig. 5. Energy Consumption versus Nodes

The above figure shows the graph of Energy Consumption versus Nodes of both ECDH (Elliptic Curve Diffie-Hellman) and the Watermarking_ECDH. The Watermarking_ECDH consumes less power while comparing to ECDH.

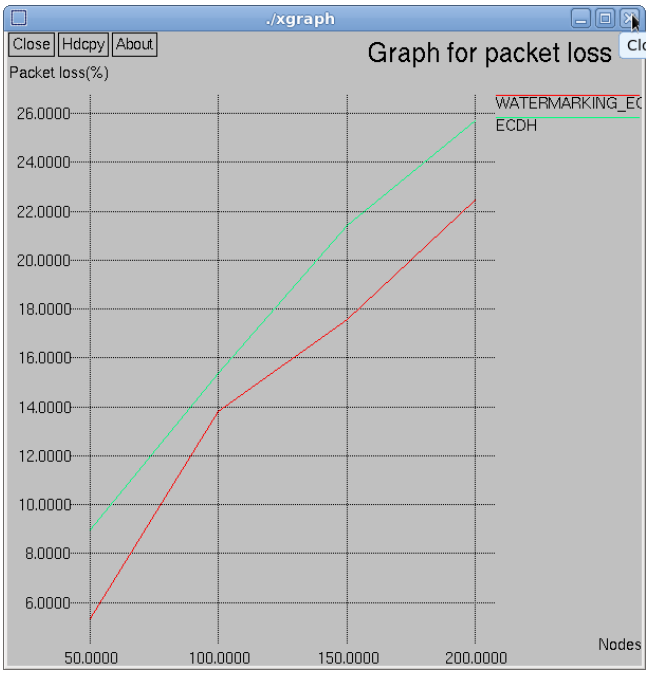

Fig. 6. Packet Loss versus Nodes

The above figure shows the graph of Packet Loss versus Nodes of both ECDH (Elliptic Curve Diffie-Hellman) and the Watermarking_ECDH. Minimum number of packets is lost in Watermarking_ECDH while comparing to ECDH.

5. RESULT AND CONCLUSTION

Compared to existing protocols, our protocol provides maximum integrity and improves the performance of wireless sensor network. Due to the use of watermarking and cross layer approach, the network becomes energy efficient and the sensor node energy is preserved. Our watermarking based protocol ensures authentication and data integrity of heterogeneous sensor networks.

REFERENCES

[1] DjallelEddineBoubiche, Sabrina Boubiche, and AzeddineBilami, “A Cross-Layer Watermarking-Based Mechanism for Data Aggregation Integrity in HeterogeneousWireless Sensor Networ,” inproc.IEEE, vol. 19, no. 5, may20 15.

[2] X. Y. Li, Y. J. Zhong, F. B. Liao, and R. Li, “An improved watermarking scheme for secure data aggregation in wireless sensor networks,” Appl. Mech. Mater., vol. 556-562, pp. 6298-6301, 2014.

[3] S. Xingming, S.Jianwei, W. Baowei, and L. Qi, “Digital watermarking method for data integrity protection in wireless sensor networks,” Int. J. Security Appl.,vol. 7 , no. 4, pp. 407-416, Jun. 2013.

[4] E. Elbasi and S. Ozdemir, “Secure data aggregation in wireless multimedia sensor networks via watermarking,” in Proc. IEEE AICT, 2012, pp. 1-6.

[5] B. Wang, X.Sun, and H. Ren, “Multi-mark: Multiple watermarking method for privacy data protection in wireless sensor networks,” Inf. Technol. J., vol.10, no. 4, pp. 833-840, Oct. 2011.

[6] M. K. Sandhya and K. Murugan , “Secure framework for data centric heterogeneous wireless sensor networks,” in Proc. CNSA, Chennai, India, Jul. 23-25, 2010, pp. 1-10.

[7] S. Wang, Z. Cao, M. A. Strangio, and L. Wang,”Cryptanalysis and improvement of an elliptic curve Diffie-Hellman Key agreement protocol,” IEEE Commun.Lett.vol. 12, no. 2rgff, pp. 149-151, Feb. 2008.

[8] W. Zhang, Y. Liu, S. K. Das, and P. De, “Secure data aggregation in wireless sensor networks: A watermark based authentication supportive approach,” Pervasive Mobile Compute., vol. 4, no. 5, pp. 658-680, Oct. 2008.

[9] S. Ozdemir, “Concealed data aggregation in heterogeneous sensor networks using privacy homomorphism, in Proc.ICPS, Istanbul, Turkey, 2007, pp. 165-168.

[10] C. Castelluccia, E. Mykletun, and G. Tsudik, “Efficient aggregation of encrypted data in wireless sensor networks,” in Proc. MobiQuitous 200, 2005, pp. 109-117.

[11] F. Hartung and M. Kutter, “Multimedia watermarking techniques,” Proc. IEEE, vol. 87, no.7 , pp. 1079-1107,Jul. 1999.