Advances in Computational Sciences and Technology
ISSN 0973-6107 Volume 10, Number 5 (2017) pp. 1037-1047
© Research India Publications
http://www.ripublication.com

An Approach for Data Aggregation Strategy in Wireless Sensor Network using MAC Authentication

Jitendra Kurmi[1], Ram Singar Verma[2] and Sarita Soni[3]

[1,2,3] Department of Computer Science
[1,2,3] BBA University (A Central University), Lucknow, India

Abstract

The WSN is currently in demand due to is bright application in both of the field of military and civil. However, for the wireless sensor network has limited energy and routing protocols are not suitable for traditional network. Data aggregation is an approach which supports lifetime of the wireless sensor networks (WSNs) against the limited energy. The proposed methodology deals with MAC authentication scheme for secure data aggregation that helps to achieve efficient secure data integrity and privacy with the improvement of energy efficiency and security. To avoid data loss in WSN, network is separated in different clusters, each cluster is headed by an aggregator (Cluster Head) and directly connected to sink through other CH. The methodology uses an algorithm for finding the cluster head on the basis of threshold value. The protocol uses a Homomorphic Encryption with secure hash Function algorithm for encryption and for calculating the hash value to maintain the integrity.

Keywords: Wireless Sensor Network, Homomorphic Encryption, SHA3, Energy Efficient Clustering Protocol, Multi-Hop routing, Data Aggregation.

1 INTRODUCTION

The theme of this paper is a secure and reliable data aggregation in WSN. The main focus of the Research, we propose an efficient confidentiality and integrity aggregation protocol and provide the secure communication between nodes. To perform the secure communication (Aggregation) based on the homomorphic encryption algorithm with hash function. This chapter presents general overview of WSNs and Data Aggregation and further chapters organized as Secure Data Aggregation, Related Work, Proposed Methodology, Simulation Results and Analysis and Conclusion and Future Scope used in Research work

1.1 OVERVIEW

Wireless sensor networks [1] contain small computing devices where they have the power of generating digital representation of real-world phenomena in figure

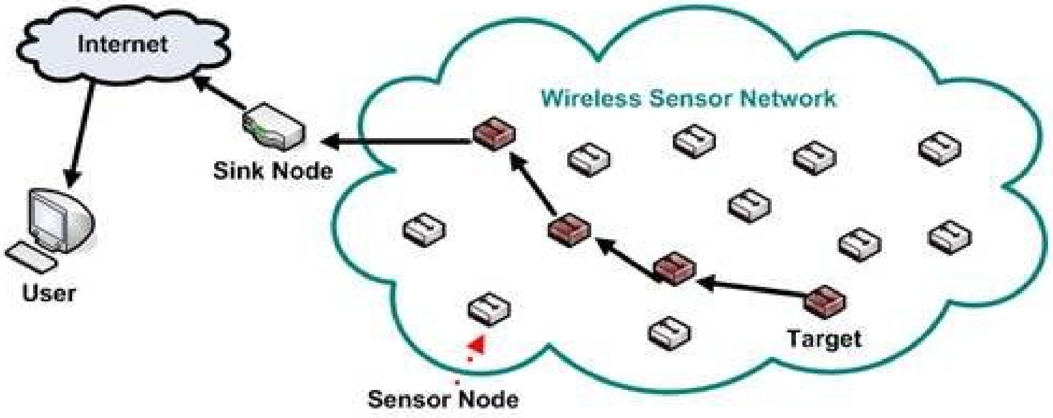

Fig. 1.1. Wireless Sensor Network

The information that is being generated by nodes in network propagates by network over wireless links. Now a day's radio communications are more reliable and efficient than computational operations with respect to energy consumption [4]. Data aggregation is a technique which supports to accomplish efficiency via compressing the data redundancy and reduce bandwidth usage in real-time. Data aggregation is a process collection of data which is passing through sensor nodes with the help of each intermediate node and route towards the sink node by reducing the communication overhead in the WSN.

2 SECURE DATA AGGREGATION

In WSNs, the Aggregation of data [3] increases if the Cluster head performs data aggregation regularly forward, whenever data are being transmitted to the base node. Security protocols desire nodes, encrypt it and by encrypting authenticity of any sensed data is tested before to its transmission and, choose data to be decrypted only via the base node. Providing security to aggregate data in WSNs is known as secure data aggregation. Generally the DA [4] can be classified based on the network topology, network basis, quality of services and many more. The techniques are being following on basis of the network topology in current research.

A. Challenging Issues in the data aggregation of WSN - In the data aggregation[2] of WSNs various security issues are:

- **Data Confidentiality**: The data confidentiality is the process of protecting the system data from unauthorized access. To do so, public key cryptography is used which drains the sensors power rapidly. Data Confidentiality is the measurement unit of the system to protect its data.
- **Data Integrity**: Due to the Lack of, the highly tampered resistant hardware, SNs can be easily aggregated. An aggregated node is able of forging, modifying, and discarding the (Data) messages.

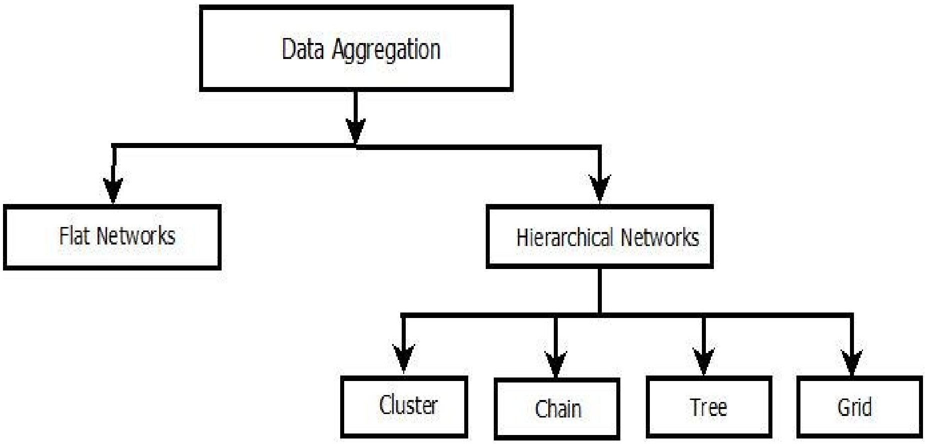

Fig. 2. Data Aggregation Techniques

B. Methods of Secure Data Aggregation - Generally, for SDA [5] in WSNs, can use two methods. They are following secure aggregation of data schemes.

- **Encrypted data aggregation using Hop by Hop:** In this technique, the SNs encrypts the data and ANs decrypts the data.. The ANs again aggregate the data by encrypting the aggregated result. In the last step, now sink node (BS) achieves the final encrypted aggregated result by decrypting it again.
- **Encrypted data aggregation using End to End:** The technique deals with, ANs only aggregate the data of intermediate node and in the last aggregated data is encrypted only once.

3 RELATED WORK

Chan et al. [6] present secure hierarchical the DA scheme based on the aggregation-commit verify techniques, which efforts to commit to its preferred of the results of aggregation, then allows sensors to authenticate whether the aggregation contributions are appropriate or not. In that scheme communication & the computation overheads are still very large.

Castelluccia et al. [7] present simple & provably secure scheme based upon an expansion of OTP encryption method. The privacy & integrity of scheme are based on monotony of the pseudorandom function, but its aggregation authentication scheme is only against the outsider attacks. Papadopoulos et al. [8] present scheme, named the SIES that arrange both integrity and confidentiality by the homomorphic encryption and secret sharing. It covers many aggregates and return exact results to the cluster head. Although this scheme only introduces small amount of the bandwidth consumption, data transmission efficiency is less because of oversize space of secret keys.

In [9], the authors detailed SDA proposed scheme, Secure Data Aggregation Protocol for the large scale SNs. The secure data aggregation uses dividend rule to commit and uses aggregation tree to attest the rules. To provide the secure data aggregation scheme we need aggregation trees. Now the groups are formed to achieve the highly significant level of nodes in tree and these processes are called as hop by hop aggregation technique. The consumption of energy and overhead of the communication is mitigate with the help of hop by hop aggregation. The problem arises when node is aggregated, which adds the false value in aggregation data. Thus, BS is required to the monitor aggregation data. Each group is then attested if the doubtful value of aggregation is created. Chan et al. [10] describe a technique to verify the sensor node using a MAC based aggregation. Frikken et al. [11] discuss an methodology for scheme called as integrity preserving which results, do not accept fake aggregated data from BS and also verify at the cluster head by doing so, it states that packet received by the BS are genuine.

Albath et al. [12] deals with the problem of end-to-end security services and CIA trade using Elliptic Curve EI-Gamal, called as hierarchical aggregation in WSNs.

Zhou et al. [13] propose a novel SDA scheme, named SDA-HP to accomplish a homomorphic encryption based on symmetric key to ensure privacy and data integrity for aggregated data with the help of homomorphic MAC.

Liehuang Zhu et al. [14] describe a homomorphic MAC based scheme for aggregation to ensure confidentiality, integrity of data, called as ECIPAP, and result-checking mechanism. Each SN can verify its data to the sum of final aggregation result with the help of result-checking mechanism, and that uses a scheme to RNG techniques to modify the saved keys to avoid replay attacks.

4 PROPOSED METHODOLOGY

- **Problem Statement**

To design and implement a Secure Data Aggregation in WSNs for secure communication via Energy Efficient Multi-hop hierarchal clustering routing protocol and Homomorphic encryption algorithm with SHA3 authentication.

- **Energy Efficient Multihop Hierarchical Clustering Scheme (EEMHCS)**

We uses dynamic clustering to minimizing the energy by operating the network for the largest period of time [15]. Before the SNs were deployed in the monitor area, every SN shared a private key $k_{i,}$ a large integer M and unique ID_i with the BS. The symmetric additively homomorphic encryption algorithm and Hash function SHA3 are also preset. When aggregation process begins, we create a hierarchical clustering by the Leach protocol and each cluster multi-hop routing perform.

4.1. Assumptions

The proposed multihop hierarchical clustering routing algorithm can be represent by following steps.

- Dividing the area into equal parts by which cluster formation is achieved.
- On the basis of threshold value cluster head are selected from each cluster.
- A process is called as data aggregation which collects data from sensor node with in its cluster head.
- Data transmission is a process in which data is transferred from the cluster heads to other CHs or to the base stations.

In EEMHCS [15] proposed a methodology to mitigate the control message overhead. The sensor node does the cluster formation, data sensing, forwarding packets and transferring information to the BS.

- **Cluster Head Selection:**

After the nodes deployment [15], the base station BS broadcast a 'HELLO' message with initial status to all the nodes directly sends their initial status messages by updating the status to the BS. T (n) is computed as:

$$T(n) = \Sigma_0^1 \frac{p}{1-p*(r \bmod \frac{1}{p})} \qquad \text{if } n \in G \text{ ,}$$

The Cluster head notify their neighborhood with an advertisement packet that they become Cluster Head.

- **Cluster Formation:**

On receiving status from the node to the base station. Each sensor node checks the condition to become a cluster head.

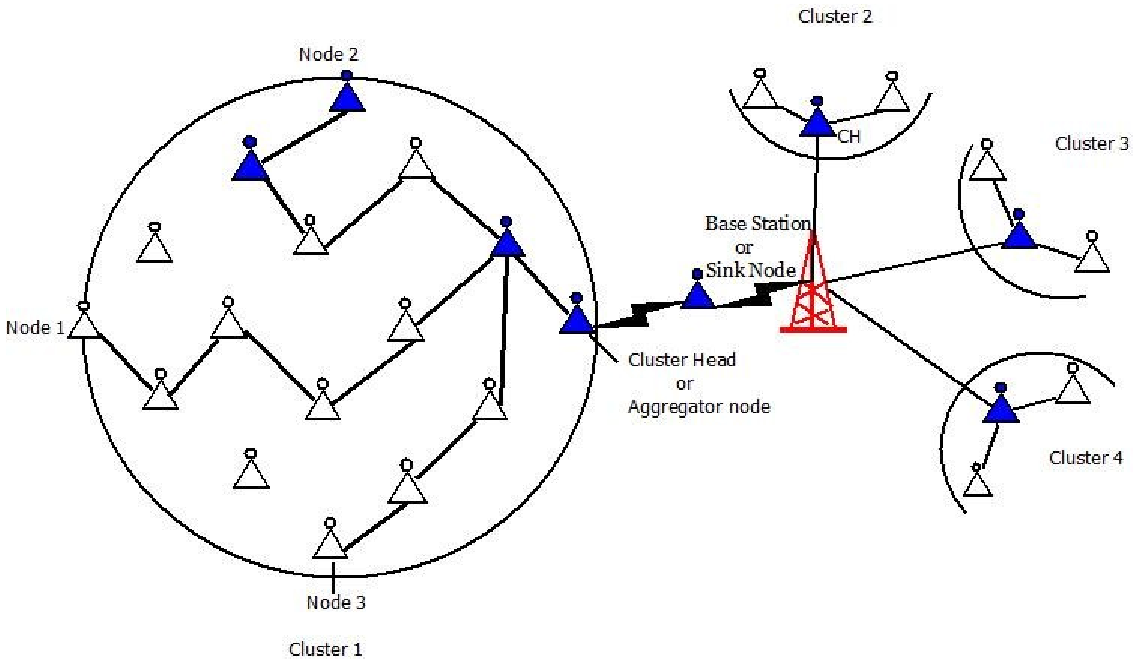

Fig. 4.1. Proposed architecture of Secure Data Aggregation

We improve E-SHM [14] by using result-checking mechanism instead of secret sharing. Then we propose an efficient confidentiality and integrity preserving aggregation protocol. The homomorphic encryption used in our protocol can guarantee end-to-end data confidentiality.

In Steady Phase Data Aggregation and Data Transmission process are discussed.

After Formation of Clustering we performed Data Transmission. In that Following Steps are [38],[39]:

1. After CH election and cluster formation we perform routing schemes by the hierarchal in that assume some nodes form transfer data.
2. Firstly we Upload the data in all selected SNs then routing start by Neighbors nodes are selected on the basis of residual energy checking the energy of nearest node from elected node which node have high energy then SN transfer the data.
3. Steps follow until reached the elected SNs data to the nearest Cluster Head.
4. When data reached the CH then it aggregate the data and send to the base station through the other CHs.
5. When we start the Data transfer we used the Homomorphic encryption algorithm for data encryption and (collision resistant) Hash Function SHA 3 for Hash value Calculate. Encryption:

$$\text{Ciphertext } c = \text{Enc } (m, kr,) = (m + kr) \bmod M$$

6. After the data send to the CHs we aggregate the data and as well as Decrypted the data and Hash value calculate and then and then matched the data information, if it matched then send to the BS if not matched then it tempered.

   Decryption:

$$m = \text{Dec}\ (c, kr,) = (c - kr)\ \text{mod}M$$

Addition:

$$ci = \text{Enc}\ (mi, ki,,M)$$

$$cj = \text{Enc}\ (mj, kj,,M)$$

$$c = (c\ i + cj)\ \text{mod}M$$

$$mi + mj = \text{Dec}\ (ci + cj, ki, + kj, r, M)$$

7. Finally safely transfer of data to the BS it request message to the CH and CH send request to the SNs for verification of process.

4.2. Simulation Result and Analysis

Table 4.2: Simulation Environment

Simulation Framework	DOT NET 4.5
Simulation Time	200 Sec
Total No. of Nodes	350
No. of message	6000
Area/Dimension	1100*600
Packet Rate	4-200 Packets/Sec
Graph version	C# Visual

- **Communication Overhead**

Figure 4.3 represents the graph of communication overhead.

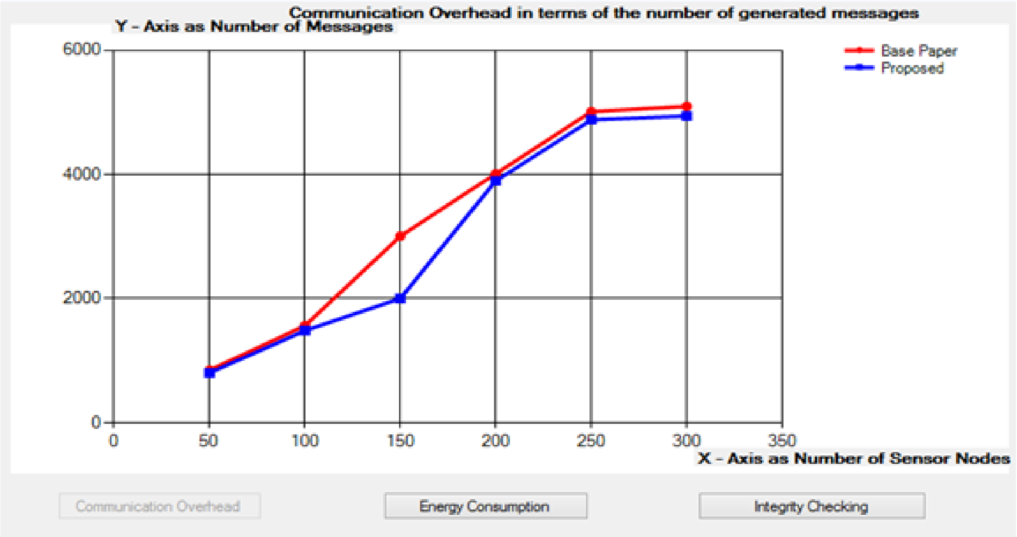

Fig. 4.3. Communication overhead due to the number of generated messages

So, EEMHCS is better for wireless sensor network than others.

- **Energy Consumption**

Figure 4.4 represents the graph by showing the energy consumption ration.

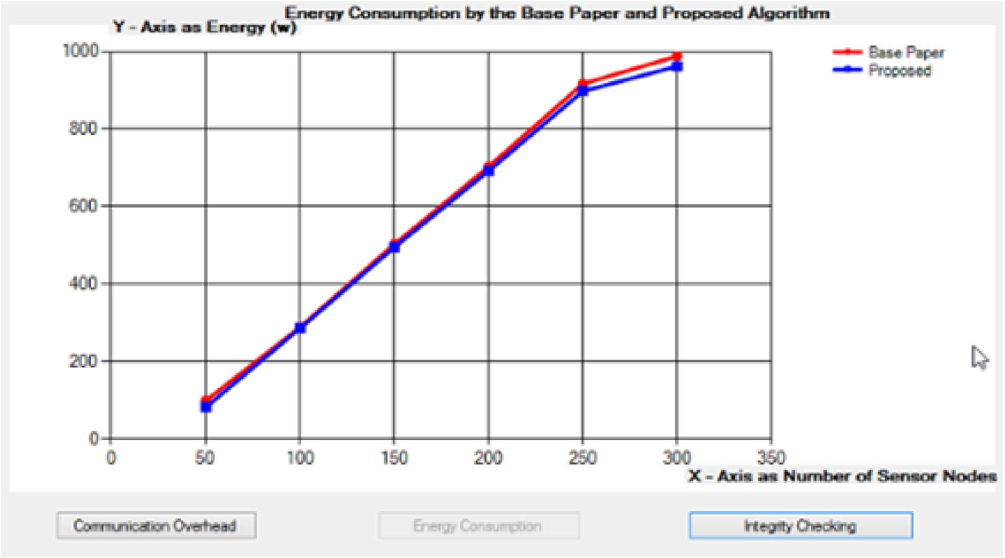

Fig. 4.4. Energy consumption rate by E-SHM and EEMHCS

- **Integrity checking rate**

Figure 4.5 shows the performance of different schemes in terms of integrity. Previous schemes and Proposed both maintain the integrity of its data received.

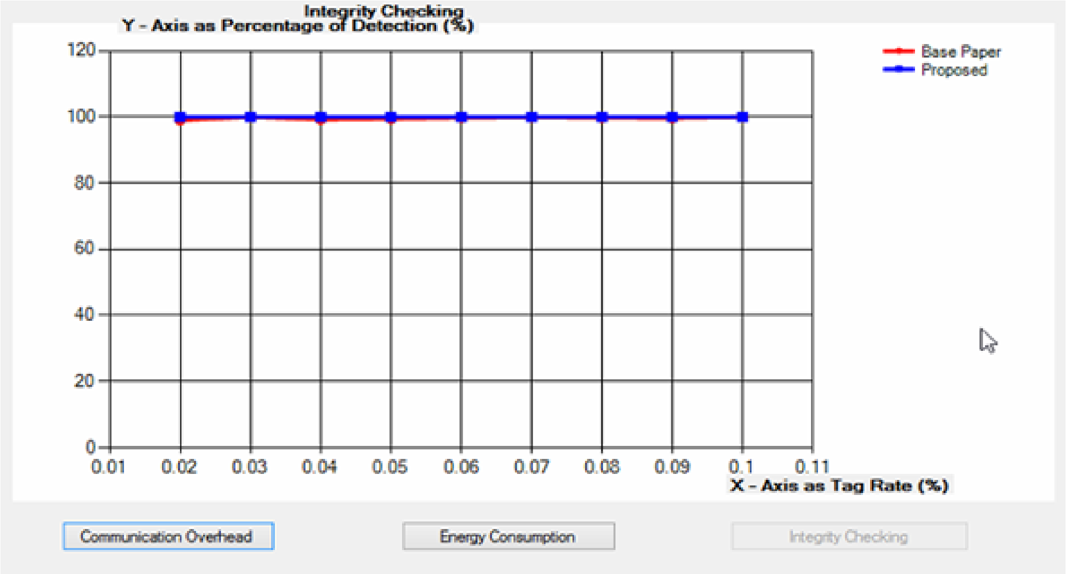

Fig. 4.5. Integrity checking

5 CONCLUSION AND FUTURE WORK

WSN carry maximum number of SNs which transfer the data from one system to another system without making use of any wires., The Lifetime of the network is Limited because All these SNs in the network are resource constraint. So, various researchers allowed numerous approaches for maximize the lifetime of the WSNs. Data aggregation concept has been introduced in this address as it is one of the important techniques that increase the lifetime of the network. The main focus of our work is to achieve data integrity and confidential during the data exchange in wireless sensor network that support data availability. In that paper has presented a Homomorphic encryption Algorithm with SHA-3 Hash function, we conclude that despite certain drawbacks, hierarchical or cluster type of multi-hop routing in WSN surely take more time and high power consumption and improves the overall life time of the wireless sensor network. Future work, several improvements can be allowed and could start to a further minimize in power consumption and taking the more time of simulation. It also include exploration of other matrices and mobility of the nodes.

REFERENCE

[1] I. F. Akyildiz, W. Su, Y. Sankara subramaniam, and E. Cayirci. “Wireless sensor networks: a survey”. Computer Networks, 38(4):393–422, 2002.

[2] Chalermek Intanagonwiwat, Deborah Estrin, Ramesh Govindan, and John Heidemann. “Impact of network density on data aggregation in wireless sensor networks”. In Proc. of IEEE ICDCS, page 457, Washington, DC, USA, 2002. IEEE Computer Society.

[3] Bhaskar Krishnamachari, Deborah Estrin, and Stephen B. Wicker. “The impact of data aggregation in wireless sensor networks”. In Proc. of IEEE ICDCSW, pages 575–578, Washington, DC, USA, 2002. IEEE Computer Society.

[4] K. Akkaya, M. Demirbas, R.S. Aygun, “The Impact of Data Aggregation on the Performance of Wireless Sensor Networks”, Wiley Wireless Communication. Mobile Computer. (WCMC) J. 8 (2008) 171–193.

[5] I. Hu, D. Evans, “Secure aggregation for wireless networks”, in: *Proceedings of the Workshop on Security and Assurance in Ad Hoc Networks*, Orlando, FI, and 28 January 2003.

[6] H. Chan, A. Perrig, and D. Song, “Secure hierarchicaI in network aggregation in sensor networks,” in *Proceedings of the13th ACM Conference on Computer and Communications Security* (CCS ’06), pp. 278–287, AIexandria, Va, USA, November 2006.

[7] C. CasteIIuccia, A. C.-F. Chan, E. MykIetun, and G. Tsudik, “Efficient and provabIy secure aggregation of encrypted data in wireIess sensor networks,” *ACM Transactions on Sensor Networks*, voI. 5, no. 3, pp. 1–36, 2009.

[8] S. Huang, “SEA : Secure Encrypted-Data Aggregation in MobiIe WSNs,” pp. 848–852, 2007.

[9] Y. Yang, X. Wang, and S. Zhu, “SDAP : A Secure Hop-by-Hop Data Aggregation ProtocoI for Sensor Networks,” 2006.

[10] A.C.Chan, C.Castelluccia,“On the (im)possibility of aggregate message authentication codes”, IEEE ISIT, pp.235-239, 2008.

[11] K. B. Frikken and J. A. Dougherty IV, “An efficient integrity preserving scheme for hierarchicaI sensor aggregation,” in *Proceedings of the 1st ACM Conference on WireIess Network Security* (WiSec ’08), pp. 68–76, AIexandria, Va, USA, ApriI 2008.

[12] Q.Zhou, G.Yang, L.He,“An Efficient Secure Data Aggregation Based on Homomorphic Primitives in Wireless Sensor Networks”, *International Journal of Distributed Sensor Networks*, 2014.

[13] L.Zhu, Z.Yang, J.Xue, C.Guo,“Efficient Confidentiality and Integrity Preserving Aggregation Protocol in Wireless Sensor Networks”, *International Journal of Distributed Sensor Networks,* 2014.

[14] Haythem Hayouni, Mohamed Hamdi, and Tai-Hoon Kim, “A NoveI Efficient Approach for Protecting Integrity of Data Aggregation in WireIess Sensor Networks”, *WireIess Communications and MobiIe Computing Conference* (IWCMC), 2015 InternationaI.

[15] M.Ye, C.Li,G.Chen and J.Wu,EECS:”An Energy Efficient Clustering Scheme in Wireless Sensor Networks”, National Laboratory of Novel Softaware Technology, Nanjing University, China.

[16] V. Loscri, G. Morabito, and S. Marano, “A Two-Level Hierarchy for Low Energy Adaptive Clustering Hierarchy”, DEIS Department, University of Calabria.

[17] H. Krawczyk, R. Canetti, and M. Bellare, “HMAC: keyed hashing for message authentication,” Tech. Rep. RFC 2104, Internet Society, Reston, Va, USA, 1997.

[18] X. Long and Z. Jian, “Improved leach cluster head multi-hops algorithm in wireless sensor networks,” in *International Symposium on Distributed Computing and Applications to Business Engineering and Science*, Aug. 2010, pp. 263–267.

[19] Lee, H.S., K.T. Kim, and H.Y. Youn, “A New Cluster Head Selection Scheme for Long Lifetime of Wireless Sensor Networks,” ICCSA, 2006. 3983.