An Efficient Secure Data Aggregation Strategy in Wireless Sensor Network using MAC Authentication

Mamta[1], Dr. Shiva Prakash[2]

[1]Department of Computer Science & Engineering MMMUT, Gorakhpur, India
Email: *mamta. aec009[at]gmail.com*

[2]Department of Computer Science & Engineering, MMMUT, Gorakhpur, India
Email: *shiva.plko[at]gmail.com*

Abstract: ***In recent years, the wireless sensor networks (WSN) attract increasing attention due to its bright application prospect in both military and civil fields. However, for the WSN is extremely energy limited, the traditional network routing protocols are not suitable to it. Energy conservation becomes a crucial problem in WSN routing protocol. Data aggregation is the most commonly used approach for extending the lifetime of the wireless sensor networks (WSNs). we propose a secure data aggregation based on MAC Authentication scheme that provide efficient secure data integrity and privacy with better energy efficiency and security and to avoid data loss initially network is separated into 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 and Data Aggregation

1. Introduction

The theme of this dissertation is a secure data aggregation in wireless sensor network. 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

2. Overview

Wireless sensor networks [1] contain small computing devices where they have the power of generating digital representation of real - world phenomena in figure 1.1.

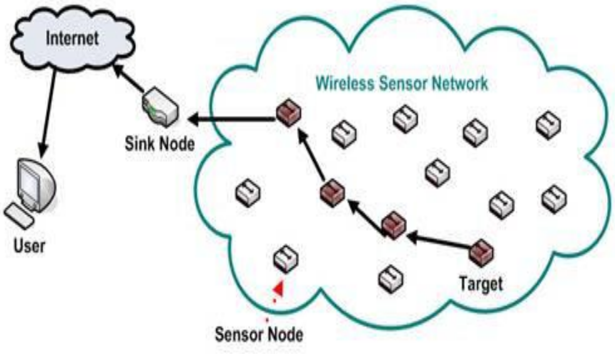

Figure 1.1: Wireless Sensor Network

The information that is being generated by nodes in network propagates by network over wireless links. In particular, radio communications are also demanding than computational operations in terms of energy consumption [4]. To that consequence, *data aggregation* has been put onward as an essential technique to accomplish power efficiency via compressing data redundancy and reduce bandwidth usage. Data aggregation subsists of processing data collected via sensor nodes at every intermediate node and route to the sink in form to reducing the number of messages transmitted in the WSN.

3. Secure Data Aggregation

In WSNs, the benefit of Data Aggregation (DA) [3] increases if the intermediate nodes (Cluster head) perform data aggregation regularly forward, when data are being delivered to the base node. Security protocols desire nodes to encrypt and test authenticity of any sensed data 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. Security Issues in the data aggregation of WSN - In the data aggregation [2] of WSNs various security issues are:

- **Data Confidentiality**: The data confidentiality is in the hostile climate, where the wireless channel is more liable to eavesdropping. The operation associated to difficult

Paper ID: SR24515122308 DOI: https://dx.doi.org/10.21275/SR24515122308

encryption and decryption of huge numbers in public key based cryptosystems and uses the sensors power rapidly.

Data Integrity: It avert the alteration of the conclude aggregation value by the aggregator nodes. Due to the Lack of the high tampering - resistant hardware, SNs can be easily aggregated. A aggregated node is able of forging, modifying, and discarding the (Data) messages.

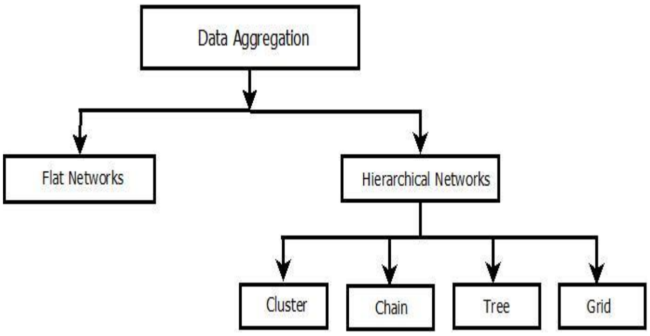

Figure 2.1: Data Aggregation Techniques

B. Methods of Secure Data Aggregation

Generally, for SDA [5] in WSNs, can used two methods. They are following encrypted data aggregation.

- **Hop - by - Hop encrypted data aggregation**: In this technique, the encryption of the data is operate by the SNs and decryption by the ANs. The ANs aggregate the data and again encrypt the aggregation result. In the last, the sink node (BS) on achieve the final encrypted aggregation result and decrypts it.
- **End to End encrypted data aggregation:** In this technique, the aggregator nodes (ANs) in middle have no decryption keys and can only act as aggregation on the encrypted message (data).

4. Related Work

Chan et al. [6] present secure hierarchical the DA scheme based on the aggregation - commit verify techniques, which efforts adversary to commit to its preferred of the aggregation results and 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 on an expansion of one - time pad 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 combination of homomorphic encryption & secret sharing. It can cover many aggregates & return exact results. 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 in the Large scale WSN with static nodes. They proposed scheme, **SDAP (Secure Data Aggregation Protocol)** for the large - scale SNs. Divide & conquer rule, commit & attest rules are followed in SDA. The aggregation trees are major component of this scheme. The aggregation trees are partition into groups to reduces high significance level nodes in tree and its called as the hop by hop aggregation technique. This reduces energy consumption and the communication overhead. 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 aggregation value is create. Chan et al. [10] uses a MAC aggregation to verify (authenticate) the certain SNs. Frikken et al. [11] propose an efficient (powerful) integrity preserving scheme to avert the BS from accepting a fake aggregate data. This scheme allows verification at cluster head (ANs), which insure that packets received by the BS are only from consistent and efficiency nodes.

Albath et al. [12] introduce a hierarchical aggregation of encrypted data in WSNs. This solution treats end - to - end security services, which confidentiality is assured using Elliptic Curve EI - Gamal, and integrity is afforded by a MAC changes.

Zhou et al. [13] propose a novel SDA scheme, named SDA - HP, based on homomorphic primitives. The scheme accomplish a symmetric key homomorphic encryption to conserve privacy and combines it with homomorphic MAC to arrange data integrity for aggregated data.

Liehuang Zhu et al. [14] propose a confidentiality and integrity preserving aggregation scheme, named ECIPAP, based on homomorphic MAC and result - checking mechanism. by the result - checking step, each SN can verify if its data was sum to the final aggregation results and that uses a random number mechanism to update the saved keys to provide the data freshness against replay attacks.

5. 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)

Our aim is to operate the network for the longest possible time, use dynamic clustering to ensure evenly distributed draining of energy [34]. 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.

a) Assumptions

The proposed hierarchical routing algorithm can be summarized using following steps

- The nodes are homogeneous, randomly distributed and have no mobility.

- Cluster formation is done by dividing the area into equal parts.
- Cluster heads are selected from each cluster on the basis of Threshold value.
- Data aggregation phase which involves the gathering of collected data by the cluster head (CH) from the sensor nodes within its cluster.
- Data transmission phase in which data is transferred from the cluster heads to other CHs or to the base stations.

In EEMHCS, the [34]CH set - up algorithm is executed at the BS to reduce control message overhead and sensor nodes are responsible for forming clusters, sensing data, forwarding packets and transmitting information to BS. The operation of WSN is distributed into rounds where each round is made up of a set up phase and a steady state phase. The set up phase consists of two steps: CH selection and cluster formation.

Cluster Head Selection:

Initially, after nodes deployment [35], BS transmits a ‘HELLO’ message telling its’ location information to all the nodes and each node directly transmits their initial status messages to the BS. a SN elects random number between 0 and 1. If this number is Less than the threshold T (n), the node becomes a Cluster head. T (n) is computed as:

$\mathrm{T}(n) = \sum_{0}^{l} \frac{p}{l - p * (r mod \frac{l}{p})}$ if n∈ G , otherwise

G is the selection of nodes not elected as a CH in the Last 1/ p rounds.

r is the current round;

p the desired percentage for becoming CH;

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

Cluster Formation:

After receiving CH announcement messages from BS, each sensor node checks whether it is a candidate CH or a member node. If it is a CH, then it broadcasts an advertisement message to all its neighbours. Based on the signal power received, each member node selects to which CH it belongs to and sends a joining request message as a member to its closest CH. After each CH receives [37] all the messages from the member nodes, it generates a time division multiple access (TDMA) schedule which tells the node when to transmit. Then, the CH broadcasts the TDMA slot to all its member nodes and the data transmission of steady state phase starts instantly.

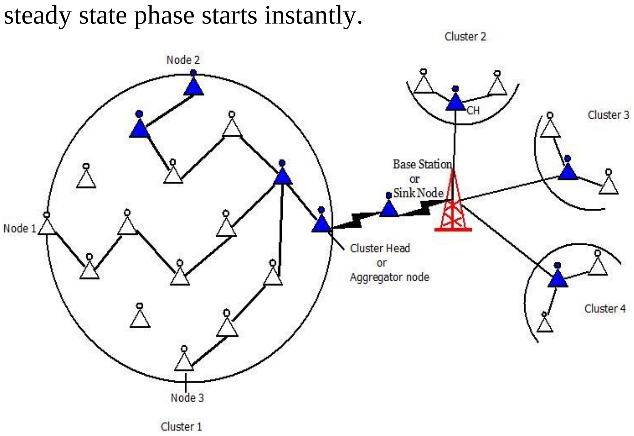

Figure 4.1: Proposed architecture of Secure Data Aggregation

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.

Algorithm for Broadcasting: Elected node broadcast selected aggregator node using CSMA - MAC Protocol.

- All elected nodes transmit with same energy.
- Based on the received selected aggregator node signal strength, other nodes or Leaf node Choose its clusters.
- The node choose the cluster head whose selected node has the highest received power. Since the amount of transmit energy needed to communicate to this cluster head is minimal.

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:

   Ciphertext c = Enc (m, kr, M) = (m+ kr) mod$M$
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 = Dec (c, kr, M) = (c − kr) mod$M$

   Addition:

   ci = Enc (mi, ki, r, M)

   cj = Enc (mj, kj, r, M)

   c = (c i+ cj) mod$M$

   mi +mj = Dec (ci + cj, ki, r + 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.

Simulation Result and Analysis

Table 6.1: 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 5.1 presents communication overhead in terms of the number of generated messages during the different steps for our scheme, to varying number of sensor nodes. However, the number of messages in the E - SHM and EEMHCS increases with the number of sensor nodes.

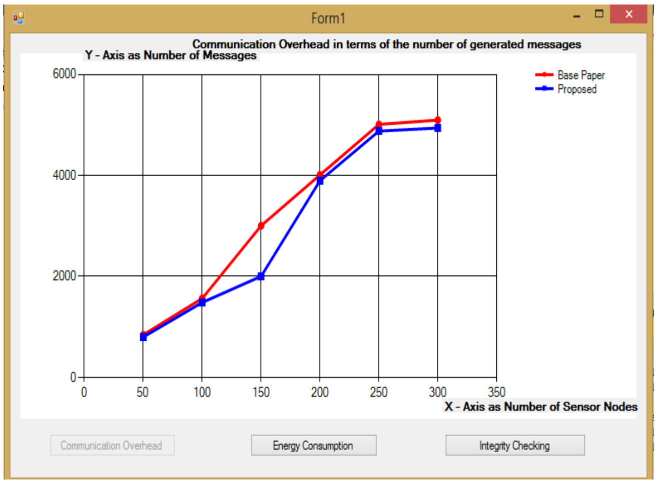

Figure 5.1: Communication overhead in terms of the number of generated messages

So, EEMHCS is better than to other schemes, which generate unnecessary messages in the network.

Energy Consumption

Figure 5.2 shows the energy consumption by the three schemes with varying number of sensor nodes. However, the dissipated energy by EEMHCS increases with the number of nodes. So, the energy consumption by EEMHCS is Lower than that of previous schemes.

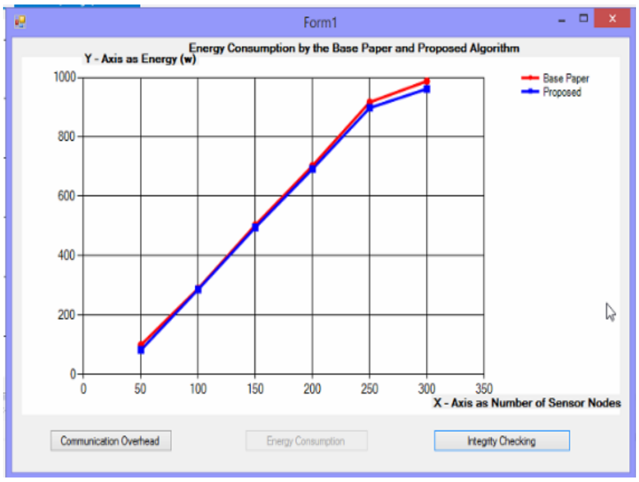

Figure 5.2: Energy consumption by the E - SHM and EEMHCS

Integrity checking rate

Figure 5.3 shows the performance of different schemes in terms of the detection ratio of polluted tags for integrity checking. Previous schemes and Proposed both maintain the integrity of its data received.

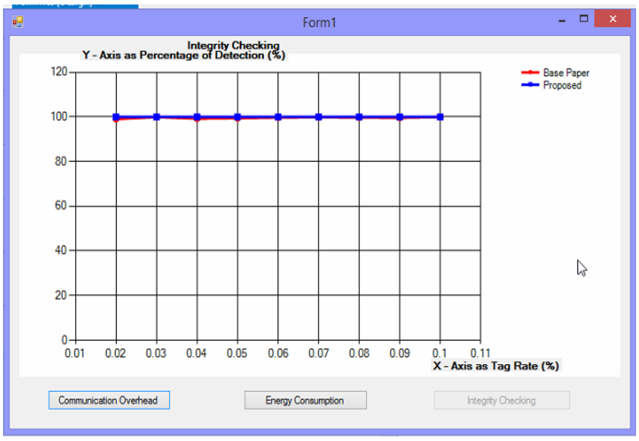

Figure 5.3: Integrity checking

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 network Lifetime. The main focus of our work is on a scheme for a integrity and confidential data exchange in WSNs that support DA. 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. The proposed scheme makes use of two types of tags affix to the encrypted message, to arrange resistance against attacks and assure dated privacy an integrity.

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

References

[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.

Paper ID: SR24515122308 DOI: https://dx.doi.org/10.21275/SR24515122308

[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.

[20] Lindsey, S. and C. S. Raghavendra. “PEGASIS: Power - efficient gathering in sensor information systems”. in *Proceedings of the IEEE Aerospace Conference*.2002.