(IJAER) 2015, Vol. No. 10, Issue No. VI, December **e-ISSN: 2231-5152/ p-ISSN: 2454-1796**

AN EFFICIENT ENERGY BALANCE AND SECURE DATA AGGREGATION IN HETEROGENEOUS WIRELESS SENSOR NETWORKS

***M. Anitha, ** Dr. T. Senthil Prakash, * J. Jahina**

**II year M.E(CSE), Sri Venkateshwara Hi-Tech Engineering College, Gobi, India*
***Professor & HOD, Sri Venkateshwara Hi-Tech Engineering College, Gobi, India*

I. INTRODUCTION

A wireless sensor network (WSN) (sometimes called a wireless sensor and actor network [1] (WSAN)[1]) are spatially distributed autonomous sensors to monitor physical or environmental conditions,[2] such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. A large amount of different key distribution schemes were implemented, targeting different types of WSNs. These schemes face issues with respect to their requirements, implementations, and theoretic foundations [3]. Though security is regarded as a standalone component of the architectures of many systems, in case of wireless sensor networks, it must get adequate attention. In most application domains, the sensors are used to collect a specific type of data from particular target areas, and the collected data are often considered secret and are not intended for public disclosure. Hence, efficient and secure mechanisms are needed to transmit acquired data securely to the appropriate recipients.

A typical heterogeneous wireless sensor networks consists of a large number of normal nodes and a few heterogeneous nodes. The normal node, whose main tasks are to sense and issue data report, is inexpensive and source-constrained. The heterogeneous node, which provides data filtering, fusion and transport, is more expensive and more capable. It may possess one or more type of heterogeneous resource, e.g., enhanced energy capacity or communication capability. They may be line powered, or their batteries may be replaced easily. Compared with the normal nodes, they may be configured with more powerful microprocessor and more memory. They also may communicate with the sink node via high-bandwidth, long-distance network, such as Ethernet. The presence of heterogeneous nodes in a wireless sensor network can increase network reliability and lifetime. In heterogeneous wireless sensor network, one basic and important deployment problem is to decide how many and where heterogeneous nodes should be deployed in the network.

To cope with the security risks, several studies have been proposed to secure data aggregation in WSNs, and they can be classified into two categories: hop-by-hop security schemes and end-to-end security schemes. In the former, the data is encrypted in each node of the network, and before encrypting, each intermediate node needs to decrypt and aggregate the data, this process not only prevents the secrecy of data, but also, results in an important computation overhead and delays. In order to provide data secrecy, several end-to-end security schemes have been proposed in which the data is concealed end-to-end i.e. the data is encrypted only at sensing nodes and decrypted only at the base station. In these schemes, the intermediate nodes perform the aggregation function over encrypted data without decrypting which leads to lesser computation overhead and provides the end-to-end data confidentiality [4]. However, in these solutions, the homomorphic encryption is used and it is known that this kind of encryption suffers from malleability, in other word, given a cipher text an attacker can easily generate a cipher text c' in order to deceive the base station by accepting the corresponding m' that is related to the original plaintext m, and without necessarily known to the attacker [5]. Therefore, it is of primordial importance to develop secure in-network aggregation schemes that provide both data confidentiality and data integrity.

II. RELATED RESEARCH

A. *SDA: Secure Data Aggregation:*

SDA protocol aims at providing lightweight security mechanism to effectively detect node misbehavior (dropping, modifying or forging messages, transmitting false aggregate value). It exploits two main ideas: delayed aggregation and delayed authentication. Therefore, the sensor readings are forwarded unchanged over the first hop and then aggregated at the second hop instead of aggregating at the immediate next hop. This increases the confidence in the sensor readings integrity but data can be altered once a parent and child in the hierarchy are compromised.

Even if a compromised node is detected, no practical action can reduce the damaged caused by it. This protocol saves resources by authenticating messages after a time delay instead of authenticating them right away, which enables authentication keys to be symmetric keys. The process of the proposed scheme starts with the leaf nodes which send their sensed data, node id, and message authentication code (MAC) to their parent node. The parent nodes store the message and MAC for a specified time so as to receive messages from all the child nodes and then retransmit the messages and MACs to its parent node. This parent node will aggregate the data received from its grandchildren (via its children) and transmit it to its parent along with the MAC of the aggregation value. The process goes on till messages arrive at the base station.

B. *SIA: Secure Information Aggregation:*

This SIA framework provides resistance against a special type of attack called stealthy attack where the attacker's goal is to make the user accept false aggregation results, which are significantly different from true results determined by the measured values, while not being detected by the user.

So the security goal is to prevent the user from accepting incorrect results i.e. to prevent the stealthy attacks. This scheme consists of three types of nodes: a home server, a base station, and sensor nodes.

SIA assumes that each sensor node has a unique identifier and shares a separate secret cryptographic key with the home server and the aggregator. If data confidentiality is requires, then these keys enable message authentication and encryption. Furthermore, it assumes that a set of uncorrupted sensor nodes in the network can reach each other via paths composed of only uncorrupted sensor nodes. Moreover, it assumes that the home server and base station can have a mechanism, such as TESLA broadcast authentication protocol, to broadcast authentic messages.

C. *Energy-Efficient and Secure Pattern-based Data Aggregation Protocol:*

It is a cluster-based data aggregation protocol. In ESPDA, cluster-head first broadcasts the pattern seed to the sensor nodes and requests them to send the corresponding pattern code for the sensed data. These pattern codes are generated using the secret pattern seed sent by cluster-head which prevents the retrieval of real data from pattern codes and the pattern generation algorithm (PG). These patterns are analyzed by the pattern comparison algorithm at the cluster-head. If multiple sensor nodes send the same pattern code to the cluster-head because of sensing the common data, then only one of them is permitted to send the data to the cluster-head. Thus, data aggregation is performed even before the actual data is transmitted from the sensor nodes. ESPDA also provides security because it aggregates data by pattern codes, so cluster-heads need not to know the contents of the transmitted data. Thus, the sensor data is transmitted to base station in encrypted form without decrypted anywhere in the transmission path. ESPDA employs a Non-blocking Orthogonal Variable Spreading Factor (NOVSF) code hopping technique. Sensor nodes compute a node-specific-secret-key (NSSK) using their unique secret built-in key and a session key broadcasted by the base station. This NSSK is used to encrypt and decrypt all the data transmissions during a session. Thus, ESPDA is an energy-efficient, bandwidth efficient, and secure protocol which provides data confidentiality, authentication, and data freshness.

D. *Secure DAV: A Secure Data Aggregation and Verification Protocol:*

Secure DAV is a cluster-based data aggregation protocol. An elliptic curve cryptosystems (ECC) is used for establishing cluster keys in sensor networks using verifiable secret sharing. ECC is used for key management because of its smaller key size, faster computations and reduction in processing power, storage space, and bandwidth. Each sensor within a cluster has a share of the secret cluster key. For each cluster, once the cluster-head receives the sensor readings, it aggregates them and computes its average. It then broadcasts the computed average to all the sensor nodes within its cluster. Then each sensor in the cluster compares its reading with the average value received from the cluster-head. Then, each sensor node partially signs the average value only if the difference between the received average value and its reading is less than a threshold and then send signed average to the cluster-head. The cluster-head combines the partial signatures to form a full signature of the aggregated result and then send this full signature along with the average reading to the base station. The validity of this signature is verified at the base station who has the corresponding public key. There are some drawbacks of this protocol such as it requires high communication costs on data validation, and it supports only the AVG aggregation function. Secure DAV provides data confidentiality, data integrity, and authentication.

E. *SRDA: Secure Reference-Based Data Aggregation Protocol:*

The data aggregation technique called SRDA that sends the differential data i.e. difference between the sensed data and the reference value instead of the raw sensed data. Reference value is taken as the average value of previous sensor readings. Each sensor node first sense the data from environment, then computes the differential data, encrypts it, and send it to the cluster-head. SRDA provides a key distribution scheme with low memory overhead to establish secure communication links in the network and to save energy it implements variable strength security at different levels of the clustering hierarchy i.e. the security level of the network is gradually increased as the data is traveled to higher level cluster-head. Increasing security levels are implemented by using a cryptographic algorithm RC6 with adjustable parameters such as the number of rounds to achieve different level of security in the WSN. Increasing or decreasing the number of rounds changes the security strength of the RC6 that can be measured by a parameter called Security Margin.

F. *SDAP: Secure Hop-by-Hop Data Aggregation Protocol:*

This general purpose data aggregation protocol has three steps. First step is tree construction and query dissemination, in which an aggregation tree is constructed and thereby all nodes identify their parents, after which the base station disseminates the aggregation query message through the tree. Second step is probabilistic grouping and data aggregation, in which SDAP uses the divide-and-conquer principle to divide the network tree into multiple logical subtrees based on a probabilistic grouping technique which depends on group leader selection. Then it generates one group aggregate from each group by hop-by-hop aggregation.

G. *RSDA: Reputation-based Secure Data Aggregation:*

The proposed a new protocol RSDA that integrates the aggregation functionalities with the advantages that are provided by a reputation system in order to enhance the network lifetime and the accuracy of aggregated data. RSDA is composed of two types of identities: a base station and normal sensor nodes. The target terrain, where RSDA is implemented, is divided into smaller non-overlapping cells of equal areas. During the bootstrap period when the network is not vulnerable to any type of attacks, each sensor node discovers its neighboring nodes and computes its cell key and shared keys with neighboring cells. Each sensor node monitors the behavior of other nodes within the same cell and then calculates the reputation value for them. Based on the calculated reputation values, one of the sensor node is selected to be the Cell Representative.

H. *Integrity Protecting Hierarchical Concealed Data Aggregation:*

In this protocol, each sensor node encrypts its sensed data using the public key of its corresponding region and sends it to the data aggregator of its region. The data aggregator aggregates the received encrypted data from the sensor nodes in its region and then computes the MAC of the aggregated data using a unique symmetric key that it shares with the base station. The encrypted data of several regions is hierarchically aggregated into a single piece of data without violating data confidentiality and the MAC of each region is combined using the XOR function and then sent to the base station. During the decryption, the base station can classify the aggregated data based on the encryption keys and verify the MAC of the aggregated data, thereby achieving data integrity.

IPHCDA provides resistance to various attacks such as cipher text analysis, known plaintext attack, replay attack, malleability, unauthorized authentication, forge packets, and physical attacks. IPHCDA provides data confidentiality, data integrity, data freshness, and authentication.

I. *Secure Data Aggregation Scheme:*

Cryptographic primitives are fundamental building blocks for security protocols. It is not too much to say that the selection and integration of appropriate cryptographic primitives into the security schemes determines the efficiency and energy conservation of the whole scheme. In this paper, we showed how to integrate a set of the cryptographic primitives into a SDA scheme in HSNs to achieve security requirements. We proposed a practical SDA scheme, Sen-SDA, based on the combination of the HE scheme, ECElGamal þ and the pairing-free IBS scheme, m ID-Sch and the batch verification with BQS for finding invalid signatures in heterogeneous clustered WSNs. Sen-SDA provides end-to-end confidentiality and hop-by-hop authentication. We determined the size of a cluster depending the ratio of the number of invalid signatures to minimize the efficiency of CHs’ batch verifications.

III.ATTACKS IN HETEROGENEOUS WIRELESS SENSOR NETWORK

Heterogeneous Sensor networks are particularly vulnerable to several types of attacks. HWSN may be a large number of attacks, each with own goals. For example, some attacks are intended to affect the integrity of messages flowing through the network, while others are aimed at reducing the availability of the network or its energy.

J. *Sybil Attacks:*

In this attack, a malicious node can claim different identities to participate in distributed algorithms such as the election and take advantage of the legitimate nodes. A malicious node may be able to determine the outcome of any vote by vote all its multiple identities for the same entity. The authentication and encryption algorithms can prevent a foreign launch a Sybil attack on the sensor network.

K. *Denial of Service Attacks:*

Denial of Service is denials as malfunctioning sensors by malicious action. Denial of service may not be the result of an attack, but a simple event that prevents the normal functioning of its services. A simple denial of service is to prevent the normal operation of the sensor victim by sending a lot of unimportant messages, and denying access to other users.

L. *Physical Attacks:*

As WSN are often deployed in areas without any protection, they are very vulnerable to physical attacks. Under these conditions, an attack will aim to recover the cryptographic hardware such as keys used for encryption. Another objective would be to reprogram the sensor to disrupt the network and the application voluntarily causing abnormal behaviour of the node.

M. *Data corruption attacks:*

The attacker repeat, delay or alter the content of messages in transit. Messages can contain data collected perception and configuration data or routing. These types of attacks are among others to create loops, or draw him away from the traffic, generate false errors.

IV.PRELIMINARIES

N. *Divide and Conquer Tree :*

Divide-and-conquer is a top-down technique for designing algorithms that consists of dividing the problem into smaller sub problems hoping that the solutions of the sub problems are easier to find and then composing the partial solutions into the solution of the original problem.

- Divide-and-conquer paradigm consists of following major phases:

Breaking the problem into several sub-problems that are similar to the original problem but smaller in size, Solve the sub-problem recursively (successively and independently), and then Combine these solutions to sub problems to create a solution to the original problem. Binary Search (simplest application of divide-and-conquer)

Binary Search is an extremely well-known instance of divide-and-conquer paradigm. Given an ordered array of n elements, the basic idea of binary search is that for a given element we "probe" the middle element of the array. We continue in either the lower or upper segment of the array, depending on the outcome of the probe until we reached the required (given) element.

O. *LEACH protocol:*

This elaborates the benefits provided in LEACH protocol as well as spanning it. It has concerns for energy savings and discovering a way of efficient data aggregation. It selects cluster heads in its network to build a data sinking path. Then it establishes a weighted divide and conquer tree using the cluster heads which does the weighted calculation of the weighted value. This calculation contains factors such as remaining energy of the cluster heads, distribution of surrounding nodes and the distance to the other cluster heads. Then, after aggregating the data, it is sent to the base station through the tree.

Proposed schema is based on LEACH (low-energy adaptive clustering hierarchy) protocol, which is one of the clustering based data aggregation protocols, and minimum spanning tree between the cluster heads. This study presented a combination method, which preserves advantages of the mentioned methods and minimizes disadvantages of the clustering and tree based approaches. Specifically, CTDA is energy efficient and consists of two main phases: set-up phase, which includes cluster head selection step, cluster formation step, and tree construction of cluster heads step, and steady-state phase, which includes data transmission.

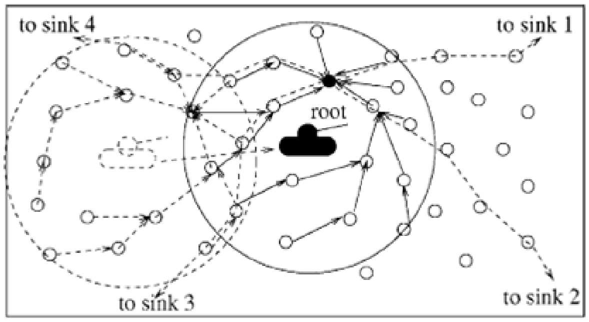

Fig 1. Cluster based Divide and conquer tree

Tree Based Data Aggregation. In tree based data aggregation (e.g., a Divide and conquer tree) base stations are roots and source nodes are considered as leaves. Each node has a parent node to forward its data. Flow of data starts from leaves nodes up to the base station and aggregation is done by parent nodes.

P. *Elliptic Curve Cryptography:*

Elliptic Curve Cryptography (ECC) is a public key cryptography method, which evolved from Diffie Hellman. To understanding how ECC works, let's start by understanding how Diffie Hellman works. The Diffie Hellman key exchange protocol, and the Digital Signature Algorithm (DSA) which is based on it, is an asymmetric cryptographic systems in general use today. It was discovered by Whitfield Diffie and Martin Hellman uses a problem known as the Discrete Logarithm Problem (DLP) as its asymmetric operation. The DLP concerns finding a logarithm of a number within a finite field arithmetic system. Prime fields are fields whose sets are prime. In other words, they have a prime number of members. Prime fields turn out to be of great use in asymmetric cryptography since exponentiation over a prime field is relatively easy, while its inverse, computing the logarithm, is difficult. The "Diffie-Hellman Method for Key Agreement" allow two hosts to create and share a secret key.

Mathematically, a proof to this effect is neither known nor thought to be forthcoming. Before wide-scale implementation, it is thus of the utmost importance that an extensive investigation of the true complexity of the problem is done in order to obtain the highest degree of confidence in the security of discrete logarithm based cryptographic systems. Such an investigation is in progress by various researchers around the world.

V.PROPOSED RESEARCH SCHEME

Q. *Network Model :*

A HWSN is controlled by a base station (BS). A BS has large bandwidth, strong computing capability, stable power, and sufficient memory to support the cryptographic and routing requirements of the whole WSN. Besides the BS, sensors (SNs) are also deployed to sense and gather responsible results for the BS. Typical SNs are small and low cost; hence, SNs are limited on, storage, communication capability and computation. Generally, all SNs in a HWSN may be divided into several clusters after being deployed. Several research, have shown that a cluster-based WSN has several advantages such as better scalability of MAC (medium access control) or routing and efficient energy management etc. Each cluster has a cluster head (CH) responsible for collecting and aggregating sensing data from SNs within the same cluster. A CH sends the aggregation results to the BS. In a heterogeneous Wireless Sensor Network, cluster heads act as normal SNs.

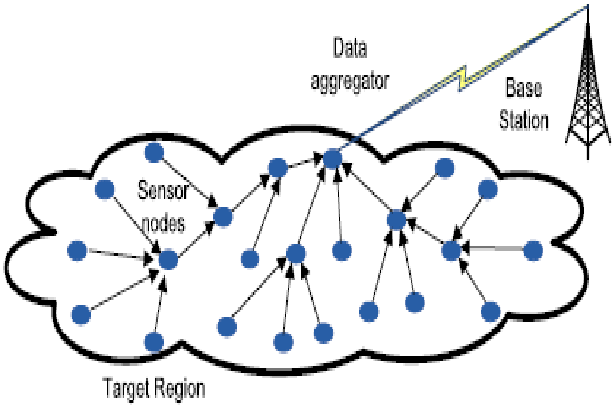

Fig 2. Data aggregation in a heterogeneous wireless sensor network

The cluster heads act as by powerful high-end sensors, in a heterogeneous WSN which incorporates different types of SNs with different capabilities.

R. *Divide and conquer Tree Creation using LEACH protocols:*

LEACH using divide and conquer based data aggregation protocol that promotes the parent energy-awareness is propose. In this protocol, parent selection is based on sensor nodes’ distance to the base station and their residual energy level. There are also data aggregation protocols that consider information theory as routing metric. For example, proposes a centralized approach that routes the packet based on their joint entropies. However, this protocol is not feasible as it depends on the global knowledge of the information entropy of each sensor node as well as the joint entropy of each node pair.

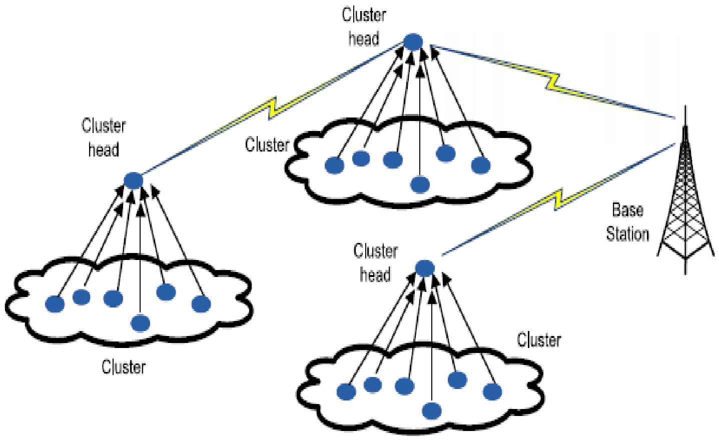

Fig. 3. LEACH Cluster-based data aggregation.

Self-organizing and adaptive clustering protocol, called Low-Energy Adaptive Clustering Hierarchy (LEACH) is proposed. LEACH takes advantage of randomization to evenly distribute the energy expenditure among the sensor nodes. LEACH is a clustered approach where cluster heads act as data aggregation points. The protocol consists of two phases. In the first phase, cluster structures are formed. Then, in the second phase, cluster heads aggregate and transmit the data to the base station. LEACH's cluster head election process is based on a distributed probabilistic approach as follows. In each data aggregator selection round, sensor nodes calculate the threshold.

$$T(n) = \begin{cases} \dfrac{p}{1 - p(Rmod(\frac{1}{p})} & if\ n \in G \qquad (1) \\ 0 & oherwise \end{cases}$$

Here P is the desired percentage of cluster heads, R is the round number, and G is the set of nodes that have not been cluster heads during the last 1=P rounds. In order to be a cluster head, a sensor node n picks a random number between [0,1] and becomes a cluster head if this number is lower than T. Cluster head advertisements are broadcasted to sensor nodes and sensor nodes join the clusters based on the signal strength of the advertisement messages. Based on the number of cluster members, each cluster head schedules its cluster-based on TDMA to optimally manage the local transmissions. In the second phase, sensor nodes send their data to cluster heads according to the established schedule.

S. *Secure Data Aggregation :*

ECC is a public key cryptography approach based on the algebraic structure of elliptic curves over finite fields. There are two types of finite fields where the elliptic curves are defined: prime fields Fp, where p is a large prime number, and binary fields F2m. In this work, we are interested in the use of elliptic curves over prime fields E (Fp). Let p > 3, then a non supersingular elliptic curve E over Fp is defined as the solution of (x, y) ∈ Fp x Fp to the cubic equation:

$$y^2 = x^3 + ax + b \; mod \; p \quad (2)$$

Where a, b ∈ Fp such that $4a^3 + 27b^2 \neq 0$ (mod p) together with a special point ∞ called *the point at infinity*, The group of points forms an abelian group with addition operation so that the addition of any two points results in another point on the same curve. The addition operation between two points is defined as follows: Given two points P1 and P2, with the coordinates (x1, y1), (x2, y2), respectively. Note that the inverse of a point P1 is –P1= (x1,-y1) and P1 + ∞ = ∞ + P1 = P1, The product Q = k.P of a point P on curve with a scalar k is called *scalar point multiplication* and it is performed by a sequence of point addition and point doubling. The security of all cryptographic protocols based on elliptic curves depends on the Elliptic Curve Discrete Logarithm Problem (ECDLP). The ECDLP can be defined as the problem of finding the scalar k such that Q=kP given Q and P. The reader is referred to for more detail.

The additive homomorphism for EC El Gamal

KeyGen: Given the domain parameters (a,b,p,G,n,E) of an elliptic curve E over finite field Fp where p is a large prime that satisfy equation (3). Where G is the base point of order n, note that n*G = ∞, the private key x is randomly selected from [1, n-1], the public key is Y=xG, another point on the curve.

Encryption: Given the plaintext m and Y, output C

1. k ∈ [1, n – 1]

2. M = map (m)= mG

3. C= (R, S) = (kG, kY+mG)

Homomorphic operation:

Given C1, C2... Cn, output C'

C'= (k1G, k1Y+m1G)+(k2G, k2Y+m2G)+…+(knG, knY+mnG)

C'= ((k1+k2+..kn)G, (m1+m2+mn)G+(k1+k2+..kn)Y)

Decryption:

Given C' and the private key x, output m

1. M = S – xR

2. m =rmap(M)

The map function satisfies the desired additive homomorphic property. However, the reverse mapping function is the shortcoming of this scheme, the reverse function maps a given point M into a plaintext m, and thus, the ECDLP (defined above) on M must be resolved.

VI.CONCLUSION AND FUTURE RESEARCH DIRECTIONS

This paper provides a detailed of secure data aggregation concept in heterogeneous wireless sensor networks. To give the motivation behind cluster based secure data aggregation, first, the security requirements of wireless sensor networks are presented and the relationships between data aggregation concept and these security requirements are explained. To provide the security and performance analysis, current secure data aggregation protocols are compared in a number of different ways: the aggregation model they follow, security services they provide, cryptographic primitives they use, attacks they secure against, and the number of bits they require nodes to send in order to accomplish the aggregation phase. In future work, aim to improve the performance of the most expensive elliptic curve operations of our scheme namely the scalar point multiplication and the point decompression and also, provide further simulations.

REFERENCES

[1] J. Jose, J. Jose, and F. Jose, “A Survey on Secure Data Aggregation Protocols in Wireless Sensor Networks”, in International Journal of Computer Applications, Volume 55, October 2012.

[2] N. S. Patil, P. R. Patil, “Data Aggregation in Wireless Sensor Network”, in IEEE International Conference on Computational Intelligence and Computing Research, 2010.

[3] S. Ozdemir, Y. Xio, “Secure Data Aggregation in Wireless Sensor Networks: A Comprehensive Overview”, in Journal of Computer Networks, Elsevier, Volume 53, Issue 12, 13 August 2009, pp. 2022–2037.

[4] L. Hu, D. Evans, “Secure Aggregation for Wireless Networks”, in Symposium on Applications and the Internet Workshops, 27-31 January 2003, pp. 384-391.

[5] B. Przydatek, D. Song, and A. Perrig, “SIA: Secure Information Aggregation in Sensor Networks”, in proceedings of the 1st International Conference on Embedded Networked Sensor Systems, 2003, pp. 255-265

[6] H.Cam, S.Ozdemir, P. Nair, and D. Muthuavinashiappan, “ESPDA: Energy-Efficient and Secure Pattern-Based Data Aggregation for Wireless Sensor Networks”, in Computer Communications, Elsevier, Volume 29, Issue 4, February 2006, pp. 446–455.

[7] A. Mahimkar, T. S. Rappaport, “SecureDAV: A Secure Data Aggregation and Verification Protocol for Sensor Networks”, in IEEE Conference on Global Telecommunications, Volume 4, 29 November – 3 December 2004, pp. 2175-2179.

[8] H. OzgurSanli, S. Ozdemir, and H. Cam, "SRDA: Secure Reference-Based Data Aggregation Protocol for Wireless Sensor Networks", in IEEE 60th Conference on Vehicular Technology, VTC2004-Fall, Volume 7, 26-29 September 2004, pp. 4650–4654.

[9] J. Girao, M. Schneider, and D. Westhoff, "CDA: Concealed Data Aggregation in Wireless Sensor Networks", in IEEE International Conference on Communications, Volume 5, 16-20 May 2005, pp. 3044-3049.

[10] Y. Yang, X. Wang, S. Zhu, and G. Cao, "SDAP: A Secure Hop-by-Hop Data Aggregation Protocol for Sensor Networks", in Journal of ACM Transactions on Information and System Security (TISSEC), Volume 11, Issue 4, July 2008, Article No. 18, New York, USA.

[11] S. Ozdemir, "Secure and Reliable Data Aggregatiob for Wireless Sensor Networks", in proceedings of 4th International Symposium, UCS 2007, Tokya, Japan, 25-28 November 2007, pp. 102-109.

[12] M. Bagaa, N. Lasla, A. Ouadjaout, and Y. Challal, "SEDAN: Secure and Efficient Protocol for Data Aggregation in Wireless Sensor Networks", in 32nd IEEE Conference on Local Computer Networks, 15-18 October 2007, pp. 1053-1060.

[13] H. Alzaid, E. Foo, and J. G. Nieto, "RSDA: Reputation-based Secure Data Aggregation in Wireless Sensor Networks", in 9th IEEE International Conference on Parallel and Distributed Computing, Applications and Technology, 1-4 December 2008, pp. 419-424.

[14] A. S. Poornima, B. B. Amberker, "SEEDA: Secure End-to-End Data Aggregation in Wireless Sensor Networks", in 7th IEEE International Conference on Wireless and Optical Communications Networks (WOCN), 6-8 September 2010, pp. 1-5.

[15] H. Li, K. Lin, K. Li, "Energy-Efficient and High-Accuracy Secure Data Aggregation in Wireless Sensor Networks", in Journal of Computer Communications, Elsevier, Volume 34, Issue 4, 1 April 2011, pp. 591–597.

[16] S.Ozdemir, Y.Xiao, "Integrity Protecting Hierarchical Concealed Data Aggregation for Wireless Sensor Networks", in Journal of Computer Networks, Elsevier, Volume 55, Issue 8, 1 June 2011, pp. 1735–1746.

[17] C. M. Chen, Y. H. Lin, Y. C. Lin, and H. M. Sun, "RCDA: Recoverable Concealed Data Aggregation for Data Integrity in Wireless Sensor Networks", in IEEE Transactions on Parallel and Distributed Systems, Volume 23, Issue 4, 18 August 2011, pp. 727-734.

[18] R. Lathamanju,P. Senthilkumar, "CRSR Algorithm: A Secure Data Aggregation Algorithm in WSN", in International Journal of Advanced Research in Electronics and Communication Engineering, Volume 2, Issue 9, September 2013.

[19] J. Jose, M. Princy, and J. Jose, "PEPPDA: Power Efficient Privacy Preserving Data Aggregation for Wireless Sensor Networks", in IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology, 25-26 March 2013, pp. 330-336.

[20] T.Wang, X.Qin, and L.Liu, "An Energy-Efficient and Scalable Secure Data Aggregation for Wireless Sensor Networks" in International Journal of Distributed Sensor Networks, Hindawi Publications, 2013.

[21] L. Zhu, Z. Yang, J. Xue, and C. Guo, "An Efficient Confidentiality and Integrity Preserving Aggregation Protocol in Wireless Sensor Networks", in International Journal of Distributed Sensor Networks, Hindawi Publications, 2014.

AUTHORS BIOGRAPHY

Mrs.M.Anitha Pursuing ME (CSE) degree in Shree Venkateshwara Hi- Tech Engineering College, Erode, India in 2014-2016 and B.E (CSE) degree from the Excel College of technology, Erode,India in 2019-2013 and . She is a Member of Computer Society of India (CSI). She published 1 National Conferences, 5 Workshops. Her research interests include Mobile Computing, Cryptography and network security,cloud computing.

Dr.T.Senthil Prakash received the Ph.D. degree from the PRIST University, Thanjavur, India in 2013 and M.E(CSE) degree from Vinayaka Mission's University, Salem , India in 2007 and M.Phil.,MCA.,B.Sc(CS) degrees from Bharathiyar University, Coimbatore India, in 2000,2003 and 2006 respectively, all in Computer Science and Engineering. He is a Member in ISTE New Delhi, India, IAENG, Hong Kong..IACSIT, Singapore SDIWC, USA. He has the experience in Teaching of 10+Years and in Industry 2 Years. Now He is currently working as a Professor and Head of the Department of Computer Science and Engineering in Shree Venkateshwara Hi-Tech Engineering College, Gobi, Tamil Nadu, and India. His research interests include Data Mining, Data Bases, Artificial Intelligence, Software Engineering etc.,He has published several papers in 17 International Journals, 43 International and National Conferences.

Mrs.J.Jahina Pursuing ME (CSE) degree in Shree Venkateshwara Hi- Tech Engineering College, Erode, India in 2014-2016 and B.E (CSE) degree from the Jansons Institute of Technology, Coimbatore, India in 2010-2014 and . She is a Member of Computer Society of India (CSI). She published 1 National Conferences, 4 Workshops. Her research interests include Mobile Computing, Networks, Data Mining.