International Journal of Advanced Technology in Engineering and Science
Vol. No.3, Special Issue No. 01, November 2015
www.ijates.com
ijates
ISSN 2348 - 7550

DEVELOPING ALGORITHM FOR AGGREGATION OF KEY EXCHANGE MANAGEMENT IN WIRELESS SENSOR NETWORK

V.Jayaraj[1,] U.Durai[2] , S. Hemalatha[3]

[1,3]*Bharathidasan University, Thiruchupalli, (India)*

[2]*Research Scholar, Periyar University, Salem, (India)*

ABSTRACT

Data Aggregation is an effective technique in Wireless Sensor Network (WSN) because it reduces the number of packets to be sent to sink and increases the lifetime of sensor network by aggregating the similar packets. This technique uses cluster method and clustering has been shown to improve network lifetime, reduce network traffic and the contention for the channel. There are certain drawbacks in the cluster method. The master node is a single point of failure and if a master node fails then the entire sub network fails. To make a WSN successfully operate mater failures or malicious attacks are to be avoided. This paper investigates disparities between mathematical security and practical security in wireless sensor networks. This paper proposes a key exchange management scheme that enables two users for exchanging a key securely and that key can be used for sequent encryption of messages. A Sande–Tukey Algorithm is developed for splitting sensor nodes to provide the key. Especially this technique is used to aggregate the total computation outputs and to identify the total number of failures within the environment.

Keywords: Traffic Collusion Malicious Attack, Key Exchange Management Technique, New Sande Tukey Algorithm.

I. INTRODUCTION

Wireless Sensor Networks (WSN) provides a simple and economic approach for the deployment of distributed monitor and control device. The confusing profusion of wireless protocol will continue to persist as one of the biggest challenges for application developer. Wireless sensor network is typically self-organizing and self-healing [1]. Wireless sensor networks into a broader perspective and gives a number of application scenarios the nodes without such a network contain at least some computation, wireless communication, and sensing or control functionalities. Some of the few popular ones are temperature, humidity, visual and infrared light (from simple luminance to cameras), acoustic, vibration (e.g. for detecting seismic disturbances), pressure, chemical sensors (for gases of different types or to judge soil composition), mechanical stress, magnetic sensors (to detect passing vehicles), potentially even radar a wide diversity in deployment options. They range from well planned, fixed deployment of sensor nodes (e.g. in machinery maintenance applications) to random deployment by dropping a large number of nodes from an aircraft over a forest fire. The sensor nodes are homogeneous and energy constrained. Sensor nodes and sink are stationary and located randomly. Every node knows the

geographic location of itself by means of a GPS device or using some other localization techniques. Every node senses periodically its nearby environment and has data to send to the sink in each round. A number of pair-wise key establishment schemes have been discussed by several researchers. Wireless communication will be a core technique, a direct communication between a sender and a receiver is faced with limitations. In particular, communication over long distances is only possible using prohibitively high transmission power. Self-healing network allows node to reconfigure their link associations and find alternative pathway around failed or powered down nodes. Self-organizing network allow a new node to automatically join the network without the need for manual intervention.

Wireless Sensor Networks use three basic network topologies:

- point to point (point to point is simply a dedicated link between two points)
- star , mesh (point to multipoint)

Star network are an aggregation of point to point links, with a central node that manages a fixed number of slave nodes and serves as the conduit for all upstream communications. Master node can also link with other master nodes to extend star network into various configurations called cluster tree network, in the mesh topology, every node has multiple pathways to every other node, providing resiliency and flexibility. Most of the Practical mesh networks utilize a type of pseudo mesh with peer to peer communication links that support routing.

WSNs usually consist of a large number of sensor nodes, which are battery powered devices. These device perform three basic tasks

- Sampling a Physical quantity from the surrounding environment
- Processing the acquired data
- Transferring them through wireless communication to a data collection point called a sink node

Key management poses a main concern for security operation in sensor network. Many key management protocols are used homogeneous sensor network, however these networks have limited performance and security heterogeneous sensor network are proposed to outcome these drawbacks. In this method using wireless sensor network that consisted of three types of key method, that's are Random key, deterministic key and Hybrid key. Random key can randomly chooses several key from the key pool and to create chain. Deterministic key can use dynamic computation to generate key that can enhance the connection between sensor nodes. Key pre distribution is the method of distribution of key on to nodes before deployment. The nodes build up the network using secret key after deployment. Key predistribution schemes are various methods has been developed by academicians for a better maintenance of key management. A key predistribution has three phases key distribution, shared key, discovery, path key establishment.

II. RELATED WORK

Several researchers have studied problem related to Duplicate-insensitive Synopsis diffusion algorithm to Compute aggregate such as count and sum, this method are based on a probabilistic algorithm [1] for counting the number of distinct element in a multi set.

In this paper [2], they present one privacy-preserving data aggregation scheme for additive aggregation functions, which can be extended to approximate MAX/MIN aggregation functions. The first scheme Cluster-based Private Data Aggregation (CPDA)-leverages clustering protocol and algebraic properties of polynomials.

It has the advantage of incurring less communication overhead. The second scheme Slice-Mix-AggRegaTe (SMART)-builds on slicing techniques and the associative property of addition.

In this paper [3], shown the effectiveness of the randomized dispersive routing in combating CN and DOS attacks

In this problem, they develop to overcome mechanisms Randomized Multipath Routes Shares.

2.1 Network Module

First, the packet is broken into M Shares using threshold secret sharing mechanism.

This module identifies the Neighbour nodes using Pythagorean Theorem

Distance=sqrt ((x-x1) ^2+(y-y1) ^2)

2.2 Shamire's Module

It is a form of secret sharing where a secret is divided into parts, giving each participant its own unique part.

Polynomial formula:

F(x) =a0+a1x+a2x^2+……+ak-1x^k-1.

2.3 Lagrange's Module

This module is used for reconstruction of secret data from secret shares.

(x0, y0)……., (xj, yj),…….. (xk, yk);0<m<k; m#j.

A parameter model referred to a global normal concept [7], they collected where a Patients temperature or Physiological variable should be continuously monitored in a hospital application, in that temperature 38.5^{0}_{C} and 41.0^{0}C collected interval of only 60S.

$$\propto(\mu) = \frac{\propto min + \mu(\propto max - \propto min)}{100}$$

Adaptive Aggregation Algorithm have been developed [6], find out the maximum temperature value and the correspondent minimum humidity value in geographical region "30a43'08 S-38o31'51 W "and "30 43' 16 S-380 31'14" W.In this paper[4], present a secure keying protocol where each sensor needs to store (n+1)=2 keys, which is much less than the n-1 keys that need to be stored in each sensor in the original keying protocol.

In this paper [5], they make the synopsis diffusion approach secure against attacks in which compromised nodes contribute false sub aggregate values. In particular, they present a novel lightweight verification algorithm by which the base station can determine if the computed aggregate (predicate Count or Sum) includes any wrong contribution.

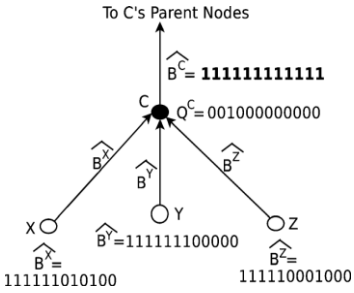

Fig.2.1 Example of Falsified Subaggregate Attack: Node is Supposed to Aggregate its Local Synopsis (from Child Nodes x, z and z)

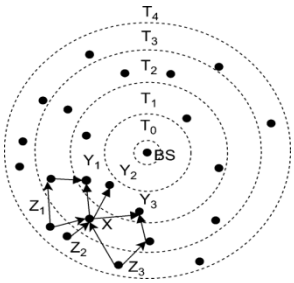

Fig. 2.2 Synopsis Diffusion Over a Ring Topology-A Node May Have Multiple Parents x has Three Parents y_1, y_2, y_3.

III. PROBLEM STATEMENT

Place Wireless sensor network can successfully operate in the presence of component transfer failure or malicious attack, this paper has to study on important potential problem in the sensor node, such as compromised node attack. Here is analysis total energy data values, and gathering the total outcome solution in network environment. In this solution have one potential wormhole node attacks to be faced by sensor nodes. In reality, a stronger attack could be formed, whereby the opponent selectively compromises node a large number of sensor that are several hops.One of the most important things in WSN research is providing or designing efficient key management schemes. This is because regardless of the encryption mechanism chosen for WSNs, the keys must be made available to the communicating nodes, end node and sink node. The keys could be distributed to the sensors before the network deployment or they could be redistributed (rekeying) to nodes on demand as triggered by keying events.

This paper investigates about the security problem that exists in the above cryptography Encryption method. First, this method is no longer valid if the adversary can compromise nodes. To overcome the security problem, this paper proposes a sande-tuky algorithm. In this algorithm, the total paths energy is computed in a randomized way each time when information packets are to be sent.

This paper evaluates the goodness of these dispersive routes in terms of avoiding black hole attack. The symmetric methods analysis is to be conducted (i.e. assuming infinite number of nodes) for determining the best case packet interception probability and energy efficiency by using the use aggregation key scheme. Our analysis helps us better to understand how security is achieved under dispersive routing.

IV. METHODOLOGY

Network Environment: First case is to collect the data without compromised or sink node attack. Complexity of the binary search algorithm

$$C(n) = \log_2 n$$

Compare the one node to another node with the key value in the middle of the key list and continue the process until finding name key and node ID in the list. Sande-tukey Techniques is developed for splitting sensor nodes to provide the key. Especially this technique to aggregate the computation outputs.

A Represents the stage of the computation outputs.

$$F_t = \{10^0C, 15^0C, 22^0C, 24^0C\}$$

This formula can also be represented the key

$$F_t = \sum_{k=0}^{k=9} (f_{key}\, w_9^{pask})$$

First step divided the sum of the terms

$$F_t = \sum_{k=0}^{4} (f_{key}\, w_9^{pask}) + \sum_{k=5}^{7} (f_{key}\, w_8^{pask})$$

This variable can be make change and add value even Components

$$F_p = \sum_{k=0}^{4} (f_{key}\, w_8^{pask})$$

$$\sum_{k=0}^{4} (f_{key+5}\, w_9^{pask+5})$$

Computation of the total collection of data

$$F_k = 1/n \sum_{p=0}^{n-1} (f_{key}\, w_n^{+pask}) \quad kp = 0,1,2 \ldots . n-1$$

Let the function f(t) alternative values and let $f_0, f_1, f_2 \ldots . f_7$ be a sequence of values of f(t)

$$F_p = \sum_{k=0}^{n} (f_{key}\, w_n^{pask})$$

If f (t) is a discrete time signal with period N, Power p is defined by the relation w_0=2Π, T (w) is called the fundamental frequency K-key values.

w_n = nth root of values

$$w_n = e^{-2\pi\iota/n}$$

$e^{-2\pi}$ Series of sines and cosines, $2\pi/\text{time(w)}$ is called fundamental frequency the total computation form periodic sequence range

p = 0, 1, 2, 3, 4…….n

Example: Fig4.1

Each sensor node edge points are connected to a set of data points, N number of data in this cluster method

(x_1,y_1) (x_2,y_2),…….(x_n,y_n)

A frequently encountered data to base station and fitting a sum of exponentials of the form

$$B = f(c) = A_1 e^{\lambda 1 x} + A_2 e^{\lambda 2 x} + \cdots A_n e^{\lambda n x}$$

Assume that n is the sum of all the line in the given range is equal to 1 f(c) c (1, 5)

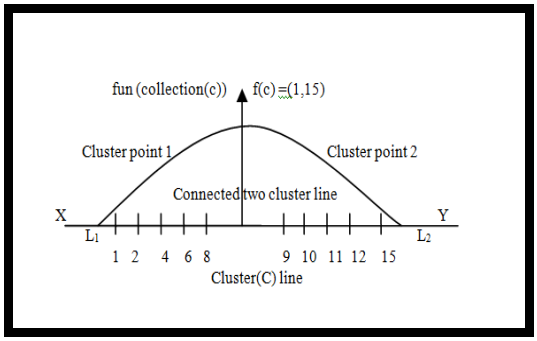

Fig 4.1 Connection of Cluster Line

4.1Establishing unique key Exchange:

4.1.1Backward reply without Modification:

CH determines the coordinate for each node S before their deployment as S: uniqueID, new_mac () address=(x, y).

The key are generated using hash table, so that key is used for generating the authority Key [A] for that parent node.

Parent [A] =id, new_mac ()

new_macAdd()=Arrays.CopyOf(mac,mac_length)

S: →keyset (K)

Set SourceID ()

Set Destination ()

Set IntermidiateID ()

S: KeySet (K)

The novelty of this new scheme is that, no need for storing the key formula in a keyset because the key are generated randomly after deployment of nodes.

Algorithm 1: // Encrypt the data

Compute DKey (EcnData, neighborIDclr)

begin

j txIDclr

cnt

if j =1 then

Kj-2; IV Cn

else

Kj F→ Kj-1

end if

return Kj;

end.

Algorithm 2: // Timer ID algorithm

Input: Total number of nodes n and the number of

nodes n ≤ N to be tagged

Output: An ID in {0, 1. . . N12….n } for all N

nodes.

Let u1. . . uG be the nodes and Δγ ≥ G a fixed

Ẃϕ integer.

Step1: For all i ∈ ni,j the node ui runs a timer

initially set to a random value

Step2: tj ∈ [γ]. Sets its counter ci ← 1 ; For all i∈N

Step3: The node ui listens to the medium when its

timer.

Step4: Transmission it considers the value of ci as

its tag and broadcasts it. , i

ci ← ci + 1 and defers its transmission ;

if (Ct< n)

then

return to 2. ;

Algorithm 3: // Aggregation of key function

Compute Agg (funK (n))

For (i=1 to f) DO

Step1: When the pair of nodes pn of Ai.which also send last forwarding node fj, Receive the data (Ch→p1+p2).

Step2: If (hu successfully verify Ch) than (Si←m) Ai decrypts Ekbi, p1 (Di) and obtain the plain data Di, encrypt the using group key group and broadcasts{ ki group(Di), agg(Ai)}.those the pair nodes on pn that are p1, p2 same parameter key.

Step3: Assign {p1=1, p2=1} monitoring node to verify the integrity Di. if the verification fails, Au discards Di else

A1 discards D1 about the unsuccessful verification of di

End

V. PERFORMANCE EVALUATION

The proposed scheme has simulated Energy consumption with increasing the lifetime of sensor network by decreasing the number of packets to be sent to sink. If aggregate the data before reaching the base station and it can be decrease the number packets in the network.

5.1 Simulation Parameters

The following are the simulation parameters considered for the implementation of our proposed new static key management scheme.

Node factory class: Flooding

Node of Radio Range: 400

Threshold time: interval -1.5,-2.5,-3.5,-4.5

Path: Randomized Multipath

Network Topologies: NT 400 node.

Attack: Blackhole, sinkhole.

Environment Attenuatior: -1,-2,-3,-4,-5,-6,-7,-8,-9,-10……-150,0,1,2,3,4,5,6,7,8,9,10…….150

Number of SN within cluster is 9

It Consider a 400*400 m field that is uniformly covered by sensors. The center of this square is the origin point. All coordinates are in the unit of meters. The sink and the center of the black hole attack are placed at(200,0) and (100,0).For each topology,2,000 information packets are sent from the source node to sink .our simulation results indicate that the 400 nodes location have a significant impact on the absolute value of the packet interception probability of a given scheme.

VI. RESULT AND DISCUSSION

For realistic, our simulation uses the Gussian radio model the communication model. The Complexity Formula C (n) =$\log_2$ n represent the neighbour key when a SN sends or receives an O (n) bit message which is to compute the average path length based on numerical simulation, and the energy result can be obtained as 6.5916.

Research works in the past work have used statistical methods to create the dynamic key. But this proposed method has each sensor need to store new formula by using discrete mathematics for creating the sequence key using symmetric method. The new method consumes less node power compared to the methods in the past [1] and also takes less time to send the data. The proposed system eliminates traffic and finds the information stored in the entire sensor node unlike the existing methods which are only providing the dynamic key. On the other hand, the compute total communication network connectivity path length $|Z| = |N| = \wp$ in order to construct a grid deployment model ensures the network life time and coverage. The analytical analysis and simulation conducted are used to compare our new solution to existing ones. The results showed that our approach provides a good secure coverage of large scale networks with a low key storage overhead and a good network resiliency.

Figure 6.1 shows that the energy decreases linearly with total number of energy output window. Figure 6.2 shows the variation of time taken in establishment of unique keys of node when the number of nodes in the network is varying. Figure 6.3 shows that energy consumption when the distance between sender and receiving nodes is varying with the total number of energy.

Transmission = 13.309,67%

Receiving = 6.576, 33%

Total Energy Spend = 28.0730235

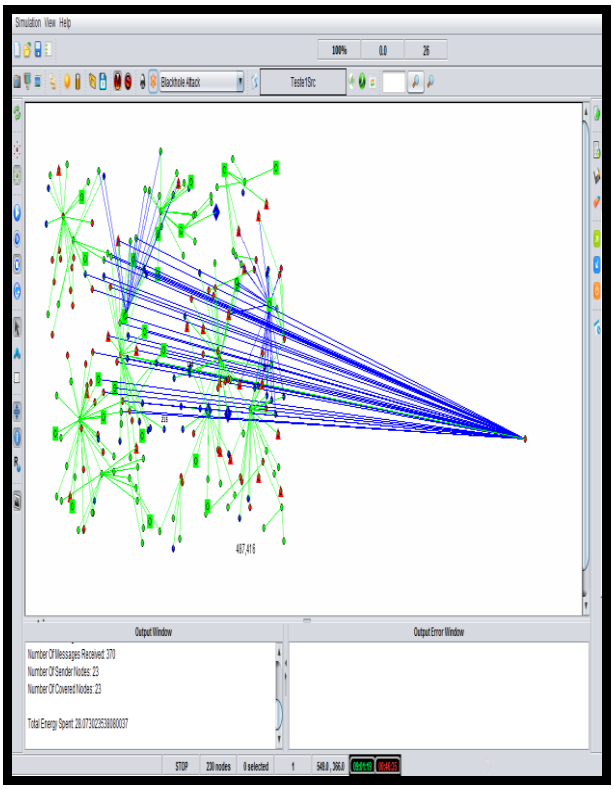

Fig. 6.1 Total Energy Output Window

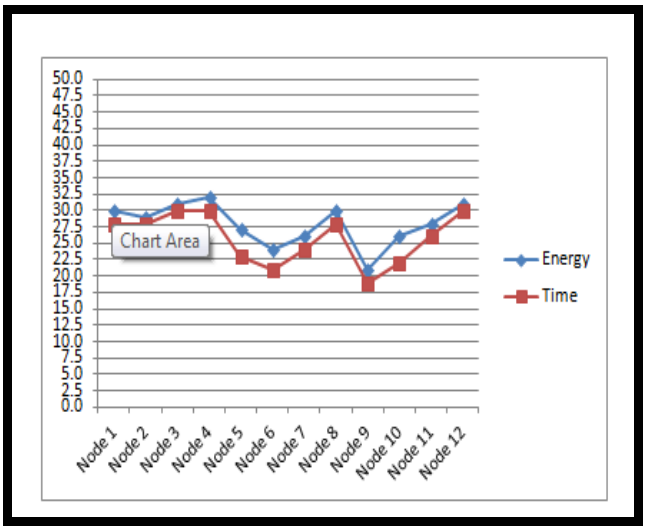

Fig.6.2 Energy and Time Consumed Vs Number of Node

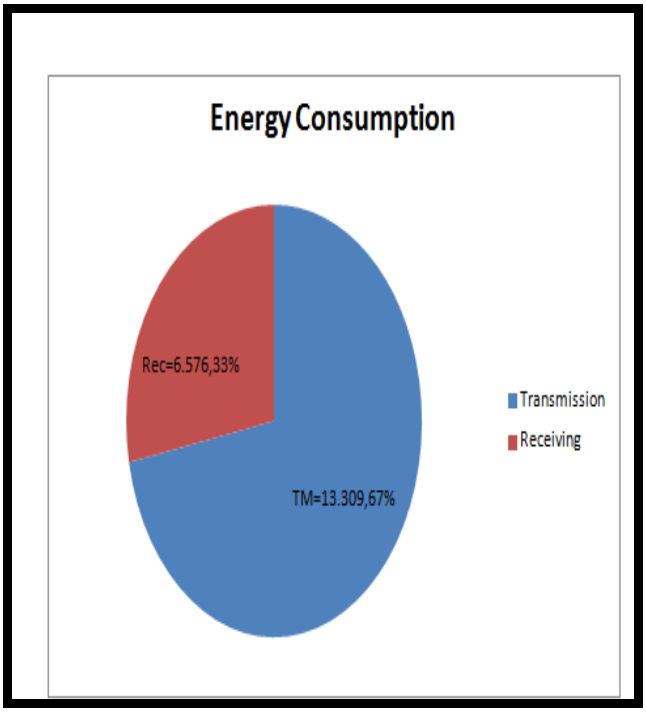

Fig 6.3 Remaining Energy of Nodes Vs Distance Between Sender and Receiving Nodes

VII.CONCLUSION

Information and Communication process is a high cost thing for wireless sensor networks (WSNs) and for certain WSN applications. Independent of the goal of saving energy, it may be very important to minimize the exchange of messages between the networks. This paper has proposed a key exchange management scheme for enabling two users to securely exchange a key that can be used for sequent encryption of messages when the sensors are allowed to perform in network aggregation of data packets with the given complexity of the key function algorithm. Our analysis and simulation results have shown the effectiveness of the sande-tuke algorithm in black hole attack. This algorithm can be applied to selective discrete method in WSN to provide additional security levels against adversaries attempting to acquire these packets. There are a number of

important issues related to the maximum lifetime data gathering problem that needs to be investigated in the future. Further, the presented experimental results demonstrates that the proposed method attain significant improvements in system lifetime, when compared to existing protocols. This method consumes less time and eliminates traffic with less energy level.

REFERENCES

[1] Priyanka Goyal, Dr.Mukesh Kumar, Ritu Sharma A Novel and Efficient dynamic KeyManagement Technique in Wireless SensorNetwork Int. J. Advanced Networking and Applications Volume:04 Issue:01 PP:1462-1466 (2012) ISSN : 0975-0290

[2] He, W., Liu, X., Nguyen, H. V., Nahrstedt, K., and Abdelzaher, T. 2011. "Privacy-preserving data aggregation for information collection "ACM Transaction Sensor Network. Article 6 (**August 2011**. DOI = 10.1145/1993042.1993048

[3] Tao Shu, Marwan Krunz Sisi Liu, **"**Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes**,"** IEEE Transactions On Mobile Computing, Vol. 9, No. 7, JULY 2010**.**

[4] Taehwan Choi H. B. Acharya, The Best Keying Protocol for Sensor Networks, 978-1-4577-0351-5/11/$26.00 c **2011** IEEE

[5] Sankardas Roy, Mauro Conti, Sanjeev Setia, and Sushil Jajodia, "Secure Data Aggregation in Wireless Sensor Networks", ieee transactions on information forensics and security, vol. 7, no. 3, june 2012

[6] Angelo Brayner, André L.V. Coelho, Karina Marinho, Raimir Holanda, Wagner Castro, "Information fusion for wireless sensor networks: On query processing in wireless sensor networks using classes of quality of queries", 2012 Elsevier.

[7] Angelo Braynera, Aretusa Lopesa, Diorgens Meiraa, Ricardo Vasconcelosa, Ronaldo Menezesb, "Signal Processing : Toward adaptive query processing in wireless sensor networks" ,Elsevier(87 (2007) 2911–2933.

[8] Deshpande, A, Nath, S., Gibbons, P. B., and Seshan, S," Cache-and-query for wide area sensor databases". ACM SIGMOD International Conference on Management of Data. July 2012.

[9] Agrawal r. and srikant, r. "Privacy preserving data mining". ACM SIGMOD Conference on Management of Data. 439–450, June 2012..

[10] Angelo Brayner, André L.V. Coelho, Karina Marinho, Raimir Holanda, Wagner Castro, "Information fusion for wireless sensor networks: On query processing in wireless sensor networks using classes of quality of queries", 2012 Elsevier.

[11] Intanagonwiwat, C, Govindan, R., Estrin, D, Heidemann, J, and Silva F, "Directed diffusion for wireless sensor networking".IEEE/ACM Trans. Netw. 11, Jan, 2012.

[12] K. B. Frikken and J. A. Dougherty, "An efficient integrity-preservingscheme for hierarchical sensor aggregation," ACM Conf. Wireless Network Security (WiSec), 2008.

[13] S. Hedetnieme, S. Hedetnieme, A. Liestman, "A survey of gossiping and broadcasting in communication networks", Networks 18 (1988) 319–349.

[14] S. Roy, S. Setia, and S. Jajodia, "Attack-resilient hierarchical data aggregationin sensor networks," in Proc. ACM Workshop Security of Sensor and Adhoc Networks (SASN), 2006.

[15] Sankardas Roy, Mauro Conti, Sanjeev Setia, and Sushil Jajodia, Secure Data Aggregation in Wireless Sensor Networks, IEEE transactions on information forensics and security, vol. 7, no. 3, June 2012

[16] Y. Zhu, R. Vedantham, S.-J. Park and R. Sivakumar, "A Scalable Correlation Aware Aggregation Strategy for Wireless Sensor Networks," Elsevier Information Fusion, Journal, 2007.

[17] Sankardas Roy, Mauro Conti, Sanjeev Setia, and Sushil Jajodia, Secure Data Aggregation in Wireless Sensor Networks, IEEE transactions on information forensics and security, vol. 7, no. 3, June 2012

[18] E.F. Nakamura, A.A.F. Loureiro, A.C. Frery, "Information fusion for wireless sensor networks: methods, models, and classifications", ACM Comput. Survey. 2007.

[19] Deshpande, A, Nath, S., Gibbons, P. B., and Seshan, S," Cache-and-query for wide area sensor databases". ACM SIGMOD International Conference on Management of Data. July 2012.

[20] M. Sartipi and F. Fekri, "Distributed Source Coding in Wireless Sensor Networks using LDPC Coding: A Non-uniform Framework," IEEE Data Compression Conference, pp. 477-477, March 2005.

[21] J. Newsome, E. Shi, D. Song, A. Perrig, "The Sybil attack in sensor networks: analysis and defences" IEEE/ACM Information Processing in Sensor Networks (IPSN'04), pp. 259–268, 2004.