ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 9, November 2013

Secure Data Collection and To Avoid the Densely Traffic Collusion Attack in Wireless Sensor Network

V.Jayaraj[1], M.Indhumathi[2]

Associate Professor, Dept. Of CSE, Bharathidasan University, Thiruchupalli, India[1]

Research Scholar, Dept. Of CSE, Bharathidasan University, Thiruchupalli, India[2]

Abstract: Data collection is a very important function provided by wireless sensor networks. In the entire, sensor node spread in the critical area in an unplanned manner. Sensor network are collection of sensor node which co-operatively send sensed data to sink node. After sensing the each sensor to deployed densely data to the base station so that a WSN can successfully operate in the presence of component failures or Densely Traffic Collusion Attack. In this environment it's very difficult to continuously surveillance. Its currently research potential in securing data aggregation in the WSN. So we solved this problem using Cartesian product sets, Inductive Reasoning Implementation and Translating Method. In this Article, we propose New Sequence Key (NSKey) Algorithm to avoid the Densely Traffic Collusion Attack. In particular, we present a Path File List (PFlist) Algorithm which the sink node can determine if the compute aggregate (SRA Value) include any wrong contribution.

Keywords: Densely Traffic Collusion Attack, New Sequence Key (NSKey) Algorithm, Path File List, Data collection

I. INTRODUCTION

A sensor (also called detector) is a converter that measures a physical quantity and converts it into a signal [1]. The collection of individual sensor nodes can be connected into a wireless sensor network and the principal tasks are node-computation, storage, communication, and sensing. The components which are required to perform this task can be roughly categorized into three categories Passive, Omni-directional sensors. These sensors can measure a physical quantity at the point of the sensor node without actually manipulating the Environment by active probing.

– In this sense, they are passive [2] [3]. There is no notion of "direction" involved in these measurements. Examples for such sensors include thermometer, light sensors, vibration, Microphones, humidity, mechanical stress or tension in materials, chemical sensors sensitive for given substances, smoke detectors, air pressure, and so on.

– Passive, narrow-beam [2] [3] sensors these sensors are passive as well, but have a well-defined notion of direction of measurement. A typical example is a camera, which can "take measurements in a given direction, but has to be rotated if need be.

– Active sensors this last group of sensors actively probes the environment, for example, a sonar or radar sensor or some types of seismic sensors.

Wireless Sensor Networks (WSN) is an challenging technology that has a wide range of potential applications, including environmental monitoring (e.g., traffic and habitat), industrial sensing and diagnostics (e.g., factory and supply chains),infrastructure protection (e.g., water distribution), battlefield awareness (e.g., multi-target tracking) and home computing(e.g., intelligent home)[1].

Wireless sensor network use three basic networking topologies - Point to Point (Simply a dedicated link between two points) - Star (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 communication, Master nodes can also link with other master nodes to extend star network in to various configurations called cluster or cluster tree network) - Mesh (Point to multipoint, In the mesh topology every node has multiple pathways to every other node, providing resiliency and flexibility). One drawbacks of a star topology is that the master node is a single point of failure, if a master node fails, the entire sub network fails [3] [4]. Most practical mesh network utilize type of pseudo mesh with peer to peer communication, links that support routing.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 9, November 2013

II. SECURE DATA AGGREGATION ALGORITHM AND ROUTING PATH PROTOCOL

Several researchers have studied problem related to data aggregation in wireless sensor network.

"Energy-efficient Data Gathering in Wireless Sensor Network [6]" The problem of data gathering in environments where data from the different sensors are correlated. Authors in independently proposed, how best the data may be fused inside the network using 1) cues from the network state, 2) energy-efficient aggregation trees rooted at the sink, and 3) congestion reduction techniques.

"Cue-based Networking [20]" New approach called cue-based networking that uses hints or cues about the physical environment to optimize networked application behaviour. Results reveal that have proposed probabilistic algorithm.

"Sink-to-sensor Congestion Control [8]" Here, only focus on providing congestion control from the sink to the sensors in a sensor field. They identify the different reasons for congestion from the sink to the sensors and show the uniqueness of the problem in sensor network environments. The generic framework has been designed that addresses congestion from the sink to the sensors in a sensor network. Author proposed an adaptive, explicit rate control approach, called Congestion control from SInk to SEnsors (CONSISE).

"Scalable Correlation-Aware Aggregation [6] [7]" Sensors-to-sink data in WSNs are typically characterized by correlation along the spatial, semantic, and/or temporal dimensions. Here, they identify that most of the existing upstream routing approaches in WSNs can be when compared with Decentralized Shortest Path Trees (DPST); authors observe that the cost of DSPT is up to 200% of SCT cost, as the number of nodes increases. The cost of DSPT s also increases faster than that of the SCT approach as node number increases translated to a correlation-unaware data aggregation structure - the shortest-path tree (SCT).

"Distributed Source Coding in Sensor Networks [14] [15] [16][17]" DSCISN focus on two different types of correlation - near and far correlation. Near correlation, define as the correlation between content sent by sensors in the same vicinity. For example, the detection of the same event by multiple sensors in a region will result in near correlation. Far correlation, define as the correlation between content sent by sensors that are far apart. Such correlation can happen due to either large range events or semantic correlation between data sent by far apart sensors. Here assume that it's have full knowledge of the correlation values before sensor deployment. This prior information is used to optimally design the source coding. Each node compresses its data without communicating with the other node and sends the compressed data to the next node that is closer to the sink. Here author propose a novel clustering scheme called Annular Slicing-based Clustering, and show that the proposed scheme performs near-optimally.

"MAC-Free Reading of Correlated Sensor Networks [6] [10]" The data gathering process is the first step towards realizing a complete network solution for WSNs. While the classical approach establishes multihop routes to the sink from the sources, it involves considerable energy expense. Here author investigate a cooperative approach for aerial reading of a wireless sensor network. More specifically, a data aggregation method called as cooperative spectrum fusion (CSF) is devised to read data from the WSN without using Medium Access Control (MAC) signalling.

III. DATA AGGREGATION USING MATHEMATICAL IMPLEMENTATION

Max/Min Aggregation Function to proposed two Methods of algorithm such as Method (1): Cluster based Private Data aggregation (CPDA) Based on the leverages clustering protocol and Algebraic properties of polynomial function [18] [19]. Each sensor node find out the neighbours share common key with itself and path key assigned to the pair of neighbour sensor node that do not share common key but can be connected by two or more mutihop secure links. With Key pool size K=1000, Key ring size R = 200.

$$P - CONNECT = 1 - \frac{((K-R)!)^2}{(K-2R)!\,K!}$$

$$P - CONNECT = 1 - \frac{(1000-200!)^2}{(1000-2(200))!\,1000!}$$

$$P - CONNECT = 98.3\%$$

Step 1: The first step in CPDA is to construct cluster to perform intermediate aggregation, Let assume Q=query server or sink node.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 9, November 2013

Step 2: Q –query by a hello message, upon receiving the hello message.
Step 3: A sensor node elects itself as cluster leader Pc (probability of cluster leader), the cluster leader was preselected parameter for all the nodes and it will forward the hello message to neighbour's.
Step 4: Otherwise a node waits for a certain period of time to get hello message its neighbour's, and then it decides to join one of the cluster by broadcasting a join message.

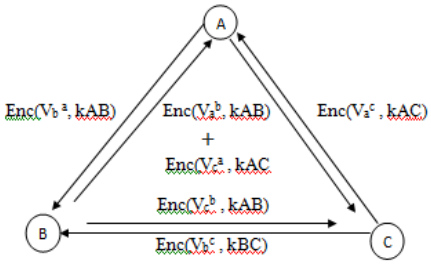


Fig1: CPDA construct function

Node A Calculate:

$v_a^b = a + r_1^a x + r_2^a x^2$

$v_b^a = a + r_1^a y + r_2^a y^2$

$v_c^a = a + r_1^a z + r_2^a z^2$

Similar only node a and b calculate for regenerating function, here v is aggregate power. The node A Encrypts v_b^a and send to B using the sharing key between $a$and b. Similarly node b Encrypts $v_b^a$to a,v_c^b to c.Node A Calculate Assembled values

$F_a = v_a^a + v_b^a + v_c^a(a + b + c) + r_1 x + r_2 x^2$

Similarly node a node b calculate Assembled values, where

G= $\begin{bmatrix} 1 & x & x^2 \\ 1 & y & y^2 \\ 1 & z & z^2 \end{bmatrix}$

U=$\begin{bmatrix} a+b+c \\ r_1 \\ r_2 \end{bmatrix}$

F=$[F_a + F_b + F_c]$

IV. PROBLEM SOLUTION

In this article, a sensor network is modelled as a Cartesian product of set (A, B), where sensor node set are represented as A, the fact that a sensor data of a set A (denoted by $a \in A$), we call it as a belongs to A. The total of data set is called elements. If $m$is Malicious node, m is not an element of A, then we write $(m \notin A)$.Suppose A *and* B, C *and* D are four set of region or domain and each domain have lot of element. So sensor element can cope with separate regions.

In case A is a total densely set of area WSN architecture, then we say that A is a sub set of B, C and D, example $(A \subseteq B)(A \subseteq C)(A \subseteq D)$. If C *and* D are two sets, then x is the authorized node $x/x \in C$ or $x \in D$. C *and* D Provided the same result of value is denoted by$A \cup B$.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 9, November 2013

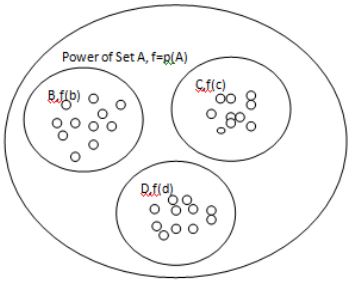


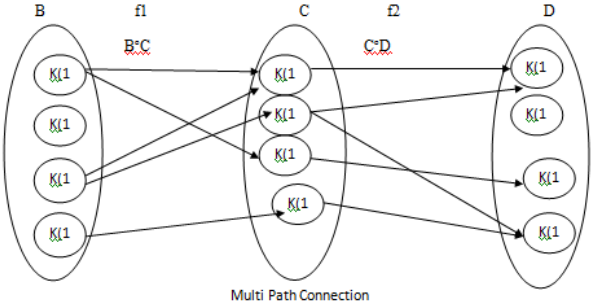
Fig2: Region set before pre-processing.

The proposed new equally pair wise key rules:

(i) Let A be sets. A function f from A is a subset of B, C, D such that,
For $l, m, n, o, p \in B$ // l, m, n, o, p is a member of node set B
$a, b, c, d, e \in C$ // a, b, c, d, e is a member of node set C
$x, y, z, i, j \in D$ // x, y, z, i, j is a member of node set D.

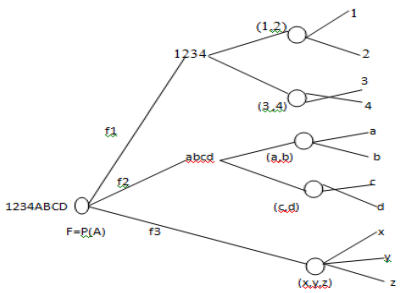
(ii) We calculate the total area in the network $f[f = P(A)]$, this $P(A)$is called the power of set and its denoted symbol(A).

(iii) If B, C, D is called the domain $S(b, c, d)/S$ - Sink node,$(x, y, z)$is called region of co domain $F(P(A)) = [B, C, D] \cup [X, Y, Z]$.



Let $B(k) = \{1,2,3,4\}$, $C(k) = \{a, b, c, d\}$, $D(k) = \{x, y, z\}$, $Relation\ R(B, C) = \{(1, a)(2, d)(3, a)(3, b)(4, d)\}$ and $Relation\ R(C, D) = \{(a, x)(b, x)(b, z)(c, y)(d, z)\}$

Consider the arrow diagrams b, c, d observe that there is an arrow from 2 to d which is followed by an arrow from $d$to z, we can view these two arrows as a path, which connects the sink node $D \in A$.



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 9, November 2013

V. EVALUATION

5.1 Verifying the Key Rule using tree method

We can view these two arrow as a "path" which "connect" the element 2∈B to the element Z∈D,2(BoC) since 2to d and d to z similarly there is path from 3 to z.

Hence 3(CoD)x and 3(CoD)z

$M_{c,d}=\begin{bmatrix}1&0&0\\1&0&1\\0&1&0\\0&0&1\end{bmatrix}$

$M_{b,d}=\begin{bmatrix}1&0&0\\0&0&1\\1&0&1\\0&0&1\end{bmatrix}$

(CoD)={(2,z),(3,x),(3,z)}

$|Z| = |N| = \wp$

Accordingly $|Z| = |N| = \wp$

Sensor node	1	2	3	4	5	6	7	8	9
|Z|(key)	0	1	-1	+2	-2	+3	-3	+4	-4

The following function $f = N - Z$

$$|Z| = f(n) \begin{cases} n/2 \text{ if } n \text{ is even} & n = 2,4,6,8,10,12 \dots \dots \\ (1-n)/2 \text{ if } n \text{ is odd} & n = 1,3,5,7,9,11,13 \dots \dots \end{cases}$$

(i) Condition I (n is even)

$n/2 = \frac{2}{2}, \frac{4}{2}, \frac{6}{2}, \frac{8}{2} \dots \dots . K$

$K = 1,2,3,4 \dots \dots \dots . n$

(ii)Condition II (n is odd)

$(1-n)/2 = \frac{1-3}{2}, \frac{1-5}{2}, \frac{1-7}{2}, \frac{1-9}{2}, \frac{1-11}{2} \dots \dots \dots \dots$

K= -1,-2,-3,-4,-5,-6,-7……

Solution will be analyse matrix format:

$$B, C = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 0 & -1 & -2 & -3 \end{bmatrix}$$

The D of linear equation is equivalent to the matrix equation A(B)= D, were 1(-0) = -0,2(-1) = -2,3(-2) = -6,4(-3) = 12.Let B(x,y) be the statement // x, y sensor node

Statement 1: "y is the best friend of x".

The meaning is that, for every sensor node x there is another neighbour node of y, such that y is the best friend of x and if z is a node other than y, but z is not best friend of x

Statement 2: Let observe the sentences used and Related Expression.

For every node $x \forall x$

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 9, November 2013

There is other node $y \exists y(x \neq y)$
Y is the best friend of x B (x, y)
Z is the node other than $z \neq y$
Z is not best neighbour node of x
For every node z other than $y \forall z$ (z≠y)
Calculation of the total communication in the network: Next, We Propose accuracy in a formal measures for the SRA.

$$SRA = \sum_{i=1}^{n} \left(\frac{TCi}{PCi}\right) * 100$$

$$\frac{1}{n}\left[\frac{1}{s1}\right]\left[\frac{1}{s2}\right]\left[\frac{1}{s3}\right]\left[\frac{1}{s4}\right]\left[\frac{1}{s5}\right] \dots\dots\dots \left[\frac{1}{sn}\right]$$

$$\frac{50}{5}\left[\frac{2}{1}\right] + \left[\frac{4}{1}\right] + \left[\frac{6}{2}\right] \dots\dots\dots$$

$$\frac{12}{4} * 100$$

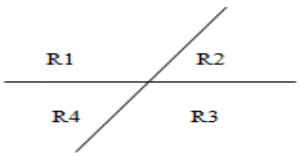
$$\frac{1}{n}\,[12 * 25]$$

$$\frac{1}{600}\,[12 * 25] = 0.501$$

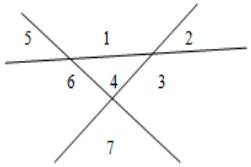
5.2 Example of verification Line Plane Diagram
L_n Maximum number of regions defined by n- lines in the plane as following,

Step (i) n =0 the plane with no lines implies that one Region $L_0 = 1$
Step (ii) the plane with one line implies that it has two Region $L_1=2$

Step (iii) n=2 the plan with one line implies that two region $L_2 = 4$



Step(iv): n=3 plan with three lines implies that it has following seven Region $L_3=7(4+3) \rightarrow L2+3$



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 9, November 2013

Sensor Region	Total number of Region($L_{n=r}$)	Maximum number of line(n)
1	L_1=2	n=1
4	L_2=4	n=2
7	L_3=7	n=3
11	L_4=11	n=4

5.3 Sensor node Moving path using Translating Method

Transfer the all node from c to d

Transfer the data from node k(1) to K(x) k(1)→k(a),k(c)
k(a)→k(x),k(c)→k(y) 3 Moves

Transfer the data from node k(2) to k(z) k(2)→k(d)→k(z) 2 Moves

Transfer the data from node k(3) to k(x) k(3)→k(a),k(b)
k(a)→k(x),k(b)→k(x) 3 Moves

Transfer the data from node k(4) to k(z) k(4)→k(d)→k(z) 1 Moves

Total Number of Moving path 9 Moves

Algorithm1: Agg(fun(K(n)) // Aggregation of key function

Step1: Let work and complete be Aggregate Information f(n), a, b, c, d, x, y, z are sensor node.100°C 200°C 300°C are sensor Information respectively. Initialize Work: = Currently process and Complete [a]: = false for 1, 2, 3, 4, 5, 6…….n.

Step2: Find and 'a' such that nearest node

(i) Complete [a] = false

Step3: Incomplete process means node 'a' intimate sink node. The sink node to re- arranges order and produce the key using mathematical condition Re-arrange [order] = a ↔b, b↔c, c↔d, d↔x, x↔y, y↔z.

(ii) Need ≤ work. If no such a exists (go to step 4) // 'a' have false means Work = work + re-process node = node + key(n).

$$\begin{matrix} n/2 \\ (1-n)/2 \end{matrix} \quad \begin{matrix} \text{if n is even} \\ \text{if n is odd} \end{matrix}$$

Step4: If Complete [a] =true.For all a, b, c, d, x, y, z. Then the node is in a safe state.

Algorithm2: Sec(fun(Loc Pi))

The Security Algorithm assumes that the path link are failure or not and that process send this message to the nearest neighbour on their node. In this algorithm we proposed security file list, a list that contain the seniority (or) Alphabetical order of all process node. When the Algorithm ends, each process maintain its OWS file LIST.

Step1: If process Pi detects a path failure, it create a new path file list that is initially empty, then sends a Acknowledgement Message to its right nearest neighbour, and add the new path link Li to its FILE LIST.

Step2: If next node (Nj) receive a message from the process on the list

(a) If this is the first(sec) message it has send,
Pi Create a new path list Pi→Nj P[i]=ΣP (i =key)

(b) if(Pi≠nj) that is message received does not contain Pi then Pi add j to path list and forward the Message to its right neighbour.

(c) if Pi=nj, that is after receiving the (LOC FILE LIST) message, than path list for Pi contain the number of path list in the file.

VI. CONCLUSIONS

In our proposed WSNs provide better power computation capacities and memory, the storage method in such that networks might expose to the Densely Traffic Collusion Attack targets. In this situation it's very difficult for continuously surveillance. So, it is a challenging task to provide security to the data. In this paper, we propose a New Sequence Key (NSKey) Algorithm to avoid the Densely Traffic Collusion Attack. In particular, we present a Path File

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 9, November 2013

List (PFlist) Algorithm which the sink node can determine if the compute aggregate (SRA Value) include any wrong contribution. Assignments and also discuss the non-uniform File-list (Loc) algorithms for the slotted Aggregation function.

REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "A survey on sensor networks" IEEE Commun. Mag., 40 (8) (2002), pp.102–114.
[2] J. Yick, B. Mukherjee, D. Ghosal., "Wireless sensor network survey" Comput. Networks, 52 (12), pp. 2292–2330, 2008.
[3] K. Akkaya, M. Demirbas, R.S. Aygun, "The Impact of Data Aggregation on the Performance of Wireless Sensor Networks", Wiley Wireless Commun. Mobile Comput. (WCMC) J 8, pp. 171–193, 2008.
[4] 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.
[5] A. Perrig, R. Szewczyk, D. Tygar, V. Wen, D., "Culler SPINS: security protocols for sensor networks" Wireless Networks J. (WINE), 2 (5) , pp. 521–534, 2002.
[6] R. Cristescu, B. Beferull-Lozano, M. Vetterli, "On network correlated data gathering"IEEE Computer and Communications Societies, vol. 4, pp. 2571–2582, 2004.
[7] S. Lindsey, C. Raghavendra, K.M. Sivalingam Data gathering algorithms in sensor networks using energy metrics IEEE Trans. Parallel Distrib. Sys., 13 (9), pp. 924–935, 2002.
[8] R. Vedantham, R. Sivakumar and S.-J. Park, "Sink-to-Sensors Congestion Control," Elsevier Ad Hoc Networks Journal, vol. 5, no. 4, pp. 462-485, May 2007.
[9] A. Akanser and M. A. Ingram, "MAC-free Cooperative Spectrum Fusion (CSF) in Wireless Sensor Networks (WSN)," IEEE Transactions on Aerospace and Electronic Systems (AES), 2008.
[10] A. Akanser and M. A. Ingram, "MAC-free reading of a network of correlated sensors," IEEE Conference on Military Communications (MILCOM), 2007.
[11] B. N. Vellambi and F. Fekri, "Finite-Length Rate-Compatible LDPC Codes: A Novel Puncturing Scheme," IEEE Transactions on Commmunications, April 2008.
[12] K. Sundaresan, Y. Zhu, and R. Sivakumar, "Exposing two critical myths about correlation aware data aggregation," ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC), May 2005.
[13] K. Sundaresan, Y. Zhu, and R. Sivakumar, "Practical limits on achievable energy improvements and useable delay tolerance in correlation aware data gathering in wireless sensor networks,"IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Network (SECON), Santa Clara, California, 2005.
[14] 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.
[15] M. Sartipi and F. Fekri, "Distributed source coding in wireless sensor networks using LDPC coding: The Entire Slepian-Wolf Rate Region," IEEE Wireless Communications and Networking Conference, March 2005.
[16] M. Sartipi and F. Fekri, "Distributed Source Coding using Finite-Length Rate-Compatible LDPC Codes: The Entire Slepian-Wolf Rate Region," IEEE Transactions on Commmunications, Vol. 56, No. 3, March 2008.
[17] M. Sartipi and F. Fekri, "Lossy Distributed Source Coding Using LDPC Codes," IEEE Communication Letters, May 2008.
[18] R. Subramanian and F. Fekri, "A Clustering-based Framework for Energy Aware Data Gathering in Distributed Sensor Networks," Journal of Ad-Hoc and Sensor Wireless Networks, August 2008.
[19] S.-J. Park, Y. Zhu, R. Vedantham and R. Sivakumar, "A scalable correlation aware aggregation strategy for wireless sensor networks," in IEEE International Conference on Wireless Internet (WICON), Budapest, Hungary, 2005.
[20] Y. Jeong, S. Lakshmanan, S. Kakumanu, and R. Sivakumar, "Cue-based Networking using Wireless Sensor Networks: A Video-over-IP Application," IEEE Comm, Society Conf. on Sensor, Mesh and Ad hoc Communications and Networks (SECON), San Francisco, CA, June 16-20, 2008.
[21] 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.

BIOGRAPHY

Dr.V.Jayaraj Associate Professor and Director, University Informatics Centre, Bharathidasan University Trichy, India. His research interests are Data Mining, Computer Networks (wireless Networks), Adhoc Network, web etc.

M.Indhumathi is a Research Scholar in the Department of Computer Science and Engineering, Bharathidasan University Trichy, India. She received Master of Computer Application (MCA) degree in 2010 from Anna University Chennai,India. Her research interests are Computer Networks (wireless Networks), Adhoc Network, web etc.