ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Hierarchical Groups Structure for Privacy-preserving Top-K Query Results in Sensor Networks

Vemula Naga Harish
M. Tech Student
Department of CSE
Sree Rama Institute of Technology & Science
Kuppenakuntla(v) Penuballi(M) Kammam(Dist.)

K.Nageswara Rao
Assistant Professor
Department of CSE
Sree Rama Institute of Technology & Science
Kuppenakuntla(v) Penuballi(M) Kammam(Dist.)

ABSTRACT:

Most large-scale sensor networks are expected to follow two-tier architecture with resource-poor sensor nodes at the lower tier and resource-rich master nodes at the upper tier. Master nodes collect data from sensor nodes and then answer the queries from the network owner on their behalf. In hostile environments, master nodes may be compromised by the adversary and then instructed to return fake and/or incomplete data in response to data queries. Such application-level attacks are more harmful and difficult to detect than blind DoS attacks on network communications, especially when the query results are the basis for making critical decisions such as military actions. This paper presents three schemes whereby the network owner can verify the authenticity and completeness of fine-grained top k query results in tired sensor networks, which is the first work of its kind. The proposed schemes are built upon symmetric cryptographic primitives and force compromised master nodes to return both authentic and complete top-k query results to avoid being caught. Detailed theoretical and quantitative results confirm the high efficacy and efficiency of the proposed schemes.

Introduction

In sensor networks for records compilation, while there might be unhinged correlation between the authority (and network proprietor) and association, a core tier with the rationale of caching the sensed data for data archival and query response becomes necessary. The network model of this paper is illustrated where the authority can issue queries to retrieve the sensor readings. The core tier is serene of a petite number of storage-abundant nodes, called storage nodes. The bottom tier consists of a large number of resource-constrained ordinary sensors that sense the atmosphere. In the beyond tiered architecture, sensor nodes are usually partitioned into disjoint groups, each of which is associated with a cargo space node. Each group of sensor nodes is called a cell. The sensor nodes in a cell form a multi-hop network and always forward the sensor readings to the associated storage node. The storage node keeps a facsimile of customary sensor readings and is responsible for answering the queries from the authority.

To motivate effective dummy reading based anonymization framework, under which the query result integrity achieve the lower communication complexity at the cost detection. OPE has been applied widely to encrypted catalog reclamation. Regrettably, in the literature, the information is all assumed to be generated and encrypted by a single authority, which is not the case in our consideration. In addition, because the number of possible sensor readings could be limited and known from hardware specification, the relation between plaintexts and cipher texts might be exposed. For example, if the sensors can solitary spawn 20 kinds of possible outputs, then practically the adversary can derive the OPE key by investigating the numerical order of the eavesdropped cipher texts despite the theoretical security guarantee.

The genuine top-k results are distributed to several sensor nodes. Through assured prospect, the influence will find query result incompleteness by checking the

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

other sensor nodes' sensor readings. Amalgam routine is a collective use of supplementary facts and crosscheck, attempting to equilibrium the communiqué cost and the query result incompleteness detection capability. Top-k query result integrity was also addressed in where distributed data sources generate and forward the sensed data to a proxy node.

The query result completeness is achieved by requiring sensors to send cryptographic one-way hashes to the storage node even when they do not have fulfilling readings. In SMQ apiece sensor applies muddle operation to the received data and its hold data, generating a certifiable entity of the sensor readings of the entire network. The basic idea behind SMQ is to construct an aggregation tree over the sensor nodes.

The bucket index used in SMQ [34] leaks the possible value range for each sensor reading, which could be valuable information, to the adversary. Order Preserving Encryption (OPE), randomized and distributed OPE (rdOPE), is first developed to establish the privacy guarantee in the proposed Verifiable top-k Query (VQ) schemes. Our study evolves in a number of successive steps; we present Global Dummy reading-based VQ (GD-VQ) and Local Dummy reading based VQ (LD-VQ), which constitute the foundation of our proposed dummy reading-based anonymization skeleton. Subsequently, they are superior to be Advanced Dummy reading-based VQ (AD-VQ), which reduces the communication overhead significantly.

Groups Structure Based Multi Cast Routing: An ordered cross layer approach for QoS provisioning by clogging control

Measuring degree of clogging at Relay hop level node:

Contrary to established systems, nodes in the ad hoc system display a high degree of heterogeneity regarding both hardware as well as software designs. The heterogeneity of the exchange hop nodes can show as different radio range, maximum retransmission counts, also barrier capability. Therefore the degree of transmission load, packet drop occurrence, also degree of buffer conservation at relay hop standard node is minimal combination to choose the degree of clogging. The use of these three purposeful values aids to decouple the clogging determines procedure from other MAC layer activities.

The degree of network load, packet drop level as well as degree of load procedure together incorporates a scope to envisage the blocking because of improper ratio inside collision as well as retransmission count. Whenever retransmissions in contrast with collision rate are considerably low then outflow delay of relay hop node will enhance proportionally, which produces clogging as well as shown as clogging because of buffer overflow.

Measuring degree of clogging at path level traffic

The level of clogging at every relay hop collectively assists to recognize the degree of clogging at route level traffic from provider to target node. Every relay hop level node obtains the degree of clogging from its neighbor node in structure. As the destiny node, which is final node of the routing path is not release the emptiness position. Therefore the destination node leads to to evaluate the degree of clogging at route level traffic. The interrupted enhancements of clogging condition at every relay hop standard node to it's heir in routing gateway is considerably energy consuming procedure. Thus to protect the energy, the clogging improvement approach concerns two restricted activities, which ensues:

1. Degree of blocking $d_c(h_i)$ at relay hop level node h_i will be sent to its successor h_{i+1} iff the ‘ $d_c(h_i)$, is greater than the node level clogging threshold $d_c(\tau)$. Hence the energy conserves due to conditional transmission.
2. If degree of blocking at path level traffic $d_c(rp)$ that received by node h_i from its doorway initiator h_{i-1} is smaller than $d_c(h_i)$ then it update the $d_c(rp)$ else it remains same, hence energy conserve

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

due to prevention of $d_c(rp)$ update.

Cross layered model for Clogging Control

The packet dipping usually happens in Manets. The causes for this packet dropping are as under

- Transmission Link failure.
- Inferred Transmission because of weighed down Inflow that prospects inflow balancing capability to low. This can also declare as packet dropping because of blocking at routing.

The clogging control is often considered in two phases by transforming over of the zonal head with the system portioned into Cells as ensues

- The Status of blocking at intra Group level
- The status of clogging at inter Group level

This assists in minimization of source standard outflow balancing cost as well as balances the power utilization.

Network and Node activities under projected topology:

The system is to be crack into Cells

For every Group i where $i = 1..|Z|$; ($|Z|$ is entirety amount of Cells)

Select Group-head for every Group i

Find spread load threshold ζ_n for every Group i

By using ζ_n of every Group spread load threshold for entire system can be determined.

Splitting the network into Groups:

We prefer to the strategy illustrated by Mohammad M. Qabajeh et al [15]. With the information of the provided nodes the region is split into equivalent partitions. Hexagon is mainly chased for the zonal shape due to it covers a maximum surface and reveals the enhancement of interacting with neighbors as they have near spherical form of the sender. The accessibility of small, affordable low power GPS recipient produces it feasible to use position-based in MANETs. The interaction range of node is represent as R also the side of hexagon as L. Considering that the nodes must be capable of correspond with one another the R as well as L are associated as $L = R/2$. Every Group has a Group attributes (zid), Group Header (zh) as well as Group Leader Backup (zh'). The zh node provides in sequence about each of the nodes in a Group with their positions as well as IDs. Furthermore, sustain information about the zh of the neighboring Cells as revealed in the fig 1. The CLB node preserves a copy of the information stored at the zh so that it is not misplaced when the zh node is off or touching the Group. By determining the coordinates of a node location, nodes can perform our self-mapping algorithm of their current regions onto the current Group also measure its zid simply. Fig 1. displays the general summary of the system architecture.

Selecting Group Heads

A group head selection occur under the pressure of the Following metrics:

a. Node positions: A node with a position *p* that is close to the centre is more likely to act as a Group head.
b. Optimum energy available: a node with higher energy e more probably acts as a Group head.
c. Computational ability: the node with high computational ability c is more possible to act as a Group Head.
d. Low mobility: the mobility *m of* a node is inversly proportional to its selection as a Group head.

Each node of the Group broadcasts its (p,e,c,m). The node that identified itself as most optimal in (p,e,c,m) metrics, announces itself as Group head zh. The next optimal node in sequence claims itself as reserve Group head zh'.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Information sharing within multicast group [between Node and group head]

Each node n that is a subset to Group Z verifies the Inflow load and shares degree of inflow load dil_n with Group head. Once $ndil_k$ received from each node k of the Group i, the Group head zh calculates the degree of inflow load at Group level $zdil_i$.

$$zdil_{z_i} = \frac{\sum_{k=1}^{zn_i} ndil_k}{zn_i}$$

Multicast Group Level Clogging Evaluation and Handling Algorithm (MGLCEH)

Multicast Group Level Clogging Evaluation and Handling Algorithm abbreviated as MGLCEH is presented in this section. MGLCEH is an optimal algorithm that helps in locating the packet dropping under clogging. This evaluation occurs under Mac layer and then alerts network layer.

Multicast Group Level Load Balancing Algorithm (MGLLBA)

This event occurs if Mac-layer alert indicates the clogging circumstance. Once the routing topology [4] gets an alert from the Mac layer a propos the blocking at a node i, it alerts the fellow citizen node which is the source node s for conflict node i. Hence s evaluates it's dil_s by comparing with $zdil$ of Z_c (Group of the node s). If dil_s is more in magnitude than $zdil_{z_c}$ the variation between dil_s and $zdil_{s_z}$ should be either greater or equal to the outflow threshold ε then node s regularizes the outflow load by manipulate its buffer time BT_s such that $ndil_s \geq zdil_{s_z} + \varepsilon_{s_z}$.

Here ε can be calculated with following equation

$$\varepsilon_j = \frac{\sum_{k=1}^{zn_j} zdil_j - dil_k}{zn_j}$$

In case that the node s not able to normalize its outflow so that disagreement node i terminates blocking then it alerts the zh_{s_z} (Group-head of the Z_c, $s \in Z_c$). Subsequent that event zh_{z_c} alerts all the nodes in the network building the all nodes in the upstream of source node to way out load using the above stated slant. Then all nodes update their $ndil$ and send to Group-head zh_{z_c}, then Group-head zh_{z_c} calculate $zdil$ and confirms integrity of the $zdil$ by evaluation with dil. $zdil_{z_c} \geq dil + \bar{\varepsilon}$ Concludes that clogging at contention node maintained by outflow regularization at current Group level. If $zdil_{z_c} < dil + \bar{\varepsilon}$ then CEA will be started at Z_p, which is adjacent upstream Group to Z_c in transmissible. In this process Group head of the Z_c firstly alerts the Group head of the counterpart Z_p then zh_{z_p} alerts all nodes that belongs to Z_p, of the route path. The above procedure of outflow regularization at Group level can be referred as BGLLBA (Multicast Group Level Load Balancing Algorithm). Hence the nodes belong to Z_p regularize their outflow load by utilize BGLLBA and alert Group-head about their efficient degree of inflow load $ndil$. Then zh_{z_p} measures $zdil_{z_p}$ and verifies the result of $zdil_{z_p} \geq dil + \bar{\varepsilon}$ .True indicates the elimination or minimization of clogging at the Group due to the outflow regularization at Group Z_p, if false then Group head of the Z_p performs the action of alerting all other Group heads using a broadcasting[12] instrument about the clogging at adjacent Group in downstream of the heridetary. Hence all Cells in the

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

upstream side of the Z_p apply BGLLBA and the Cells in downstream side of the Z_p fill in their $zdil$. Then all Cells broadcast $zdil$ to resource Group. Hence the source Group revaluates the dil.Basing on the dil ,source node regularize its outflow load.

Notations used in Algorithm:

i: Node that had been effected by emptiness

s: source node of the i.

Z_c : current Group where $i, s \in Z_c$

Z_p : Immediate Group to Z_c in upstream side of the pecking order.

$\{n_{u1}, n_{u2}, ..., n_{uk}\}_{Z_c}$: All upstream nodes to s.

$\{n_{d1}, n_{d2}, ..., n_{dk}\}_{Z_c}$: All downstream nodes to s.

$\{Z_S, Z_{u1}, Z_{u2}, ..., Z_{uk}\}$: Set of upstream Cells to Z_p in routing path, here Z_S is a Group that contains source node of the routing path

$\{Z_{d1}, Z_{d2}, ..., Z_{dm}, ..., Z_T\}$: Set of downstream Cells to Z_p in routing path, here Z_T is a Group that contain target node of the routing path

ε : Group level outflow threshold

$\bar{\varepsilon}$: Network level Outflow threshold

Algorithm:

Mac layer alerts about the blocking at node of Group Z_c to routing topology, hence the following steps perform in sequence

$$\varepsilon_{Z_C} = \frac{\sum_{k=1}^{zn_{Z_C}} zdil_{Z_C} - dil_k}{zn_{Z_C}}$$

complete following at node s

If $ndil_s > zdil_{Z_c}$ and $ndil_s - zdil_{Z_c} \geq \varepsilon_{Z_c}$ begin

$BT_s = BT_s + bt$

Note: Value of buffer threshold bt should be certain such that $dil_S \geq zdil_{Z_C} + \varepsilon_{Z_C}$

Return.

Endif

s sends alert to zh_{Z_c} about conflict node i.

zh_{Z_c} alerts all nodes that belongs to Group Z_c

$\{n_{u1}, n_{u2}, ..., n_{uk}\}_{Z_c}$ updates their $ndil$ by apply BGLLBA recursively and alerts zh_{Z_c}

$\{n_{d1}, n_{d2}, ..., n_{dk}\}_{Z_c}$ measures their $ndil$ and alerts zh_{Z_c}

zh_{Z_c} Measures $zdil$ as fallows

$$zdil_{Z_C} = \frac{\sum_{k=1}^{zn_{Z_C}} ndil_k}{zn_{Z_C}}$$

If $zdil_{Z_c} > dil$ and $(zdil_{Z_c} - dil) \geq \bar{\varepsilon}$ begin

Alert: blocking at contention node handle at current Group Z_c level.

Return.

Endif

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

zh_{Z_c} Alerts zh_{Z_p}

zh_{Zp} Alerts all nodes that belong to Group Z_p

For each node $n \in Z_p$ begin

If $ndil_n > zdil_{Z_p}$ and $ndil_n - zdil_{Z_p} \geq \varepsilon_{Z_p}$ begin

$BT_n = BT_n + bt$

Note: Value of barrier threshold bt should be decided such that $dil_n \geq zdil_{Z_C} + \varepsilon_{Z_C}$

Endif

Find dil_n and send dil_n to zh_{Z_p}

End-of-for each

zh_{Z_p} measures $zdil_{Z_p}$

if $zdil_{Z_p} > dil$ and $(zdil_{Z_p} - dil) \geq \bar{\varepsilon}$ begin

Alert: Outflow regularization at Z_p leads to overcome clogging situation at contention Group.

Return;

Endif

zh_{Z_p} Alerts all Group heads in network regarding clogging contention Group.

For each Group z in $\{Z_S, Z_{u1}, Z_{u2}, ..., Z_{uk}\}$ begin

zh_z Alerts all nodes that belongs to Group z

For each node $n \in z$ begin

If $ndil_n > zdil_z$ and $ndil_n - zdil_z \geq \varepsilon_z$ begin

$BT_n = BT_n + bt$

Note: Value of barrier threshold bt should be understood such that $dil_n \geq zdil_z + \varepsilon_z$

Endif

Find dil_n and send dil_n to zh_z

End-of-foreach

zh_z Measures $zdil_z$ and broadcast towards source Group.

End-of-foreach

For each Group z in $\{Z_{d1}, Z_{d2}, ..., Z_{dm}, ..., Z_T\}$ begin

For each node n belong to Group z begin

determine $ndil_n$ and sends to zh_z

End-of-foreach

zh_z measures $zdil_z$ as

$$zdil_z = \frac{\sum_{k=1}^{zn_Z} ndil_k}{zn_Z}$$

zh_z Sends $zdil_z$ to source Group via propagation [12]

End-of-foreach

Z_S Measures dil as

$$dil = \frac{\sum_{i=1}^{|Z|} zdil_i}{|Z|}$$

Hence source node S of Group ZS, which is source node of the routing path regularize it's outflow load to

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

direction-finding path

Hence source node S of t's outflow l oad to direction-finding path.

Fig 3: Multicast Group Level Load Balancing Algorithm

Simulations and results discussion

In this section we discuss the outcome acquired from simulation conducted using a simulation model developed by using MXML in this section. We evaluated concert using madhoc with the following considerations:

The simulations are conducted on three routes differing by the no of hops and length.

a. Short length path: A route with 15 hops
b. middling length : A route with 40 hops
c. Max Length: A route with 81 hops

The same load is given to all the paths with regular intervals. The figure 3 indicates the load given in simulations. The fig 4 concludes the improvement of MGLCEH over clogging control topology[8] in clogging control cost. A. The clogging detection cost evaluation between MGLCEH and clogging control topology[8] is explore in fig 5 that elevates the energy good organization achieved under .

The process of capacity of clogging control and clogging detection cost is as follows:

Based on the resource ease of use, bandwidth and energy, for individual operation a threshold value between 0 and 1 assigned. In the mechanism of clogging detection and control the total cost is calculated by summing the cost threshold of every involved event. In fig 5 the judgment between clogging costs observed for MGLCEH and clogging and contention control model [8] are shown.

$$\cos t_{ch} = \sum_{e=1}^{E} ct_e$$

Here $\cos t_{ch}$ is the price of a clogging controlling activity ch, E is total amount of events included. ct_e is the threshold cost of an event e. The example events are:

1." alert to source node from Mac layer"

2. "Alert from node to Group head", "propagation by Group head to other Group heads"

3. "Inflow judgment and outflow regularization".

4. Alert about $d_c(h_i)$

5. bring up to date $d_c(rp)$

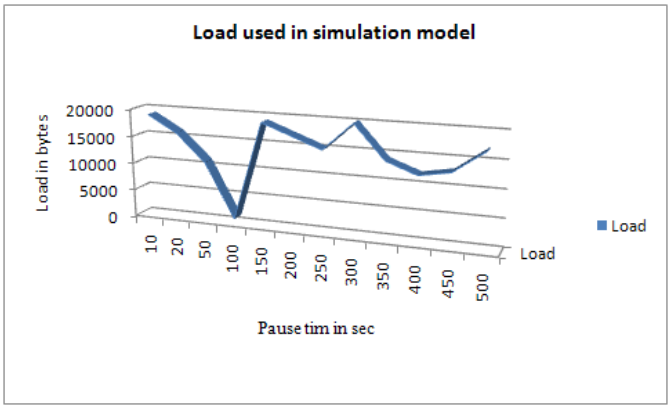

Fig 3: Load in bytes drive by source node of the routing path [in regular interval of 10 sec]

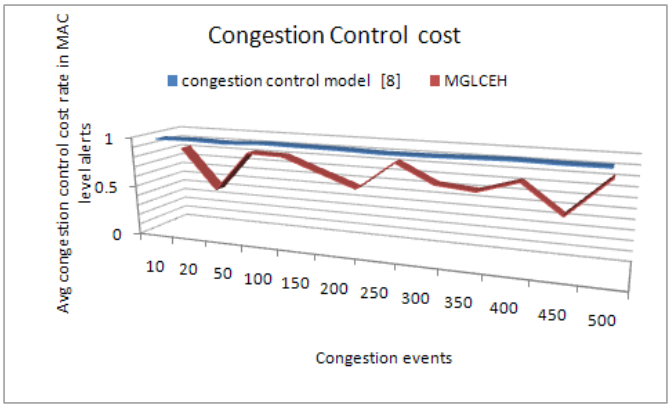

Fig 4: Clogging Control cost

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

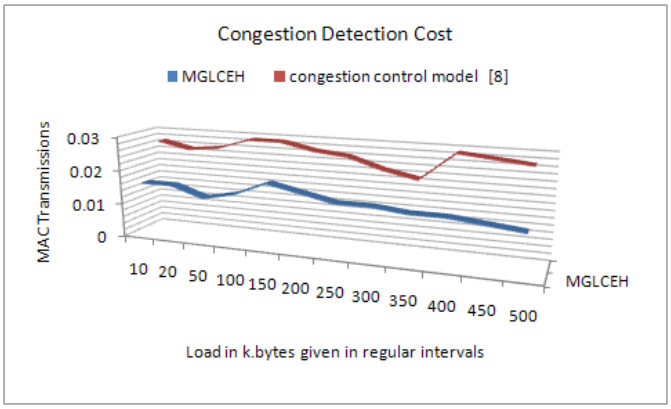

Fig 5: Clogging detection cost

CONCLUSION

We explore the problem of top-k query on time slot data set in two-tier wireless sensor network, and establish a set of privacy and correctness requirements for such a secure top-k scheme to become practical. We propose Top-k schemes meeting different privacy and correctness requirements in consideration of three levels of threat models. Thorough analysis investigating privacy, detection rate and efficiency guarantee of proposed scheme is given, and experiments on the real-world dataset further show the efficiency of proposed schemes.

REFERENCES

[1] C. Liu and G. Cao, "Distributed monitoring and aggregation in wireless sensor networks," in IEEE INFOCOM, 2010.

[2] A. Mainwaring, D. Culler, J. Polastre, R. Szewczyk, and J. Anderson, "Wireless sensor networks for habitat monitoring," in ACM WSNA, 2002.

[3] N. Xu, S. Rangwala, K. K. Chintalapudi, D. Ganesan, A. Broad, R. Govindan, and D. Estrin, "A wireless sensor network for structural monitoring," in ACM SenSys, 2004.

[4] A. Giridhar and P. R. Kumar, "Computing and communicating functions over sensor networks," IEEE Journal on Selected Areas in Communications, vol. 23, pp. 755–764, 2005.

[5] R. Cristescu, B. Beferull-Lozano, and M. Vetterli, "On network correlated data gathering," in IEEE INFOCOM, 2004.

[6] J. Li, A. Deshpande, and S. Khuller, "On computing compression trees for data collection in wireless sensor networks," in IEEE INFOCOM, 2010.

[7] D. Luo, X. Zhu, X. Wu, and G. Chen, "Maximizing lifetime for the shortest path aggregation tree in wireless sensor networks," in IEEE INFOCOM, 2011.

[8] Y. Wu, S. Fahmy, and N. B. Shroff, "On the construction of a maximumlifetime data gathering tree in sensor networks: NP-Completeness and approximation algorithm," in IEEE INFOCOM, 2008.

[9] A. Goel and D. Estrin, "Simultaneous optimization for concave costs: Single sink aggregation or single source buy-at-bulk," in SODA, 2003.

[10] M. Enachescu, A. Goel, R. Govindan, and R. Motwani, "Scale free aggregation in sensor networks," in ALGOSENSORS, 2004.

[11] N. Thepvilojanapong, Y. Tobe, and K. Sezaki, "On the construction of efficient data gathering tree in wireless sensor networks," in IEEE ISCAS, 2005.

[12] B. Yu, J. Li, and Y. Li, "Distributed data aggregation scheduling in wireless sensor networks," in IEEE INFOCOM, 2009.

[13] C. Park and P. H. Chou, "Ambimax: Autonomous energy harvesting platform for multi-supply wireless sensor nodes," in IEEE SECON, 2006.

[14] X. Jiang, J. Polastre, and D. Culler, "Perpetual environmentally powered sensor networks," in IPSN, 2005.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[15] P. Dutta, J. Hui, J. Jeong, S. Kim, C. Sharp, J. Taneja, G. Tolle, K. Whitehouse, and D. Culler, "Trio: Enabling sustainable and scalable outdoor wireless sensor network deployments," in IPSN, 2006.

[16] R. Hassin, R. Ravi, and F. S. Salman, "Approximation algorithms for a capacitated network design problem," Algorithmica, vol. 38, pp. 417– 431, 2004.

[17] C. P. Low, "An approximation algorithm for the load-balanced semimatching problem in weighted bipartite graphs," Information Processing Letters, vol. 100, pp. 154 – 161, 2006.

[18] M.-J. Tsai, H.-Y. Yang, and W.-Q. Huang, "Axis-based virtual coordinate assignment protocol and delivery-guaranteed routing protocol in wireless sensor networks," in IEEE INFOCOM, 2007.

[19] X. Cheng, D.-Z. Du, L. Wang, and B. Xu, "Relay sensor placement in wireless sensor networks," Wireless Networks, vol. 14, pp. 347–355, 2008.

[20] X. Han, X. Cao, E. L. Lloyd, and C.-C. Shen, "Fault-tolerant relay node placement in heterogeneous wireless sensor networks," in IEEE INFOCOM, 2007.

[21] S. Misra, S. D. Hong, G. Xue, and J. Tang, "Constrained relay node placement in wireless sensor networks to meet connectivity and survivability requirements," in IEEE INFOCOM, 2008.

[22] M. R. Garey and D. S. Johnson, Computers and Intractability: A Guide to the Theory of NP-Completeness. New York, NY, USA: W. H.Freeman, 1979.

[23] F. S. Salman, J. Cheriyan, R. Ravi, and S. Subramanian, "Approximating the single-sink link-installation problem in network design," SIAM J. on Optimization, vol. 11, pp. 595–610, 2000.

[24] S. Khuller, B. Raghavachari, and N. Young, "Balancing minimum spanning trees and shortest-path trees," Algorithmica.