International Journal of Electronics and
Communication Engineering (IJECE)
ISSN 2278-9901
Vol. 2, Issue 1, Feb 2013, 7-18
© IASET

International Academy of Science,
Engineering and Technology
Connecting Researchers; Nurturing Innovations

SECURED POWER AWARE AND ENERGY EFFICIENT ROUTING PROTOCOL (SPAEERP) FOR WIRELESS SENSOR NETWORKS

R. PREMA[1] & R. RANGARAJAN[2]

[1]Assistant Professor, Department of Electronics, Karpagam University, Coimbatore, India

[2]Principal, Indus College of Engineering, Indus Valley, Alandurai, Coimbatore, India

ABSTRACT

Several wireless sensor network applications have to to decide the inherent discrepancy between energy efficient communication, power aware routing and the requirement to attain preferred quality of service (QoS) such as packet delivery ratio, delay and to reduce the power and energy consumption of wireless sensor nodes. In addition to that the protocols which are developed aims in providing better QoS with compromising security aspect. For addressing this challenge, we propose the Secured Power Aware and Energy Efficient Routing Protocol (SPAEERP), which attains application-specified communication delays at low energy cost by dynamically adapting transmission power and routing decisions along with incorporating a novel cryptosystem. Through extensive simulation in NS2 the results prove that the proposed SPAEERP attains better QoS and reduced power and energy consumption. Cryptool is used to test the novel proposed cryptosystem.

KEYWORDS: Sensor Networks, Secured Power Aware Routing, Energy Efficient Routing, Novel Cryptosystem

INTRODUCTION

Wireless Sensor Networks

Smart environments represent the next evolutionary development step in building, utilities, industrial, home, shipboard, and transportation systems automation. Like any sentient organism, the smart environment relies first and foremost on sensory data from the real world.

Sensory data comes from multiple sensors of different modalities in distributed locations. The smart environment needs information about its surroundings as well as about its internal workings; this is captured in biological systems by the distinction between exteroceptors and proprioceptors.

The challenges in the hierarchy of: detecting the relevant quantities, monitoring and collecting the data, assessing and evaluating the information, formulating meaningful user displays, and performing decision-making and alarm functions are enormous.

The information needed by smart environments is provided by Distributed Wireless Sensor Networks, which are responsible for sensing as well as for the first stages of the processing hierarchy.

The importance of sensor networks is highlighted by the number of recent funding initiatives, including the DARPA SENSIT program, military programs, and NSF Program Announcements. Desirable functions for sensor nodes include: ease of installation, self-identification, self-diagnosis, reliability, time awareness for coordination with other nodes, some software functions and DSP, and standard control protocols and network interfaces.

This is an extension of our previous work [1]. In [1] we proposed secured power aware routing protocol for wireless sensor networks. In this paper we ought to propose an adaptive novel cryptosystem.

LITERATURE REVIEW

In [2], Chien-Yuan Chen, Cheng-Yuan Ku, and David C.Yen found ways to use the LLL algorithm to break the RSA system even when the value of d is large. According to their proposed cryptanalysis, if d satisfies |X - d| < N0.25, the RSA system will be possible to be resolved computationally.

In [3], Kwok-Wo Wong, Sun-Wah Ho, and Ching-Ki Yung, customized the chaotic cryptographic scheme to reduce the length of the ciphertext to a size slightly longer than that of the original message. Moreover, they introduced a session key in the cryptographic scheme so that the length of the ciphertext for a given message is not fixed.

In [4], Chang-Doo Lee, Bong-Jun Choi, and Kyoo-Seok Park proposed a block encryption algorithm, which is designed for each encryption key value to be applied to each round block with a different value. This algorithm needs a short processing time in encryption and decryption, has high intensity, and can be applied to electronic commerce and various applications of data protection.

In [5], Mark G. Simkin discusses five encryption techniques: transposition ciphers, cyclic substitution ciphers, Vigenere ciphers, exclusive OR ciphers, and permutation ciphers. Accompanying these discussions are explanations of how instructors can demonstrate these techniques with spreadsheet models.

In [6], Jun Wei, Xiaofeng Liao, Kwok-wo Wong, and Tao Xiang proposed a new chaotic cryptosystem. Instead of simply mixing the chaotic signal of the proposed chaotic cryptosystem with the ciphertext, a noise-like variable is utilized to govern the encryption and decryption processes. This adds statistical sense to the new cryptosystem.

In [7], Osama Mahmud Abu Abbas, Khalid Mohammad Nahar, and Mohammad Ahmad Tubishat, uses Arabic letters and their diacritics for encrypting English messages and vice versa. A pseudo random generator is used to generate integer numbers to represent each character in Arabic language. The same numbers are used again after sorting them to represent the English characters. The conclusions that extracted indicate the efficiency of ARAE system according to security and time performance.

Nevertheless, the diversities of all the above stated encryption methods, but all of them are common in some characteristic such as: The encryption operation can be implementing as a one to one relation, Usually there is a language redundancy problem,Semi random encryption methods, and Finding a way to cryptanalysis them is applicable, nevertheless, the needed time is.

Energy-efficient routing algorithms allow WSNs to be deployed with smaller battery packs and to achieve longer lifetime for a given battery size [9,10]. There are mainly two ways to achieve energy-efficient route selection in WSNs: Minimum cost routing and maximum network lifetime routing. One classical energy-efficient routing algorithm for minimum cost routing is minimum energy routing (MER). The MER algorithm has been used to minimize the transmission energy in [11–14]. On the other hand, maximum lifetime routing, which aims to extending network lifetime by balancing traffic load is studied in [15–17]. Other energy- efficient routing algorithms focusing on energy-consumption as well as other metrics of network performance such as queueing delay, congestion or maximum data yield have been proposed [18,19].

Energy efficient routing algorithms subject to latency constraints are also investigated in [20]. Recent works have looked at exploiting the data correlation by using data aggregation along the multi-hop path [14–18]. In general routing algorithms with data aggregation fall into one of two categories: Routing-driven aggregation and aggregation-driven routing. In routing-driven algorithms, source data is routed through a specific path to the sink node (e.g. shortest path or minimum energy path depending on the application), data is aggregated opportunistically when data streams meet [21, 26–29].

Most routing- driven algorithms use a full aggregation model, that is, all data packets received from child nodes are fully aggregated into one single packet at the parent node. This assumption may be practical for large scale WSNs where the correlation level between nodes vary significantly. In aggregation-driven routing algorithms [8,23,24], the route selected by each source node to the sink node is informed by the correlation between the data collected by the nodes. As data moves along the route, it is aggregated with data from sources on the route, reducing the traffic load at links closer to the sink. The reduction in the required bit rate resulting from aggregation affects the relative cost of each link. Thus, the route chosen by any source will not necessarily be the shortest or the minimum energy path to the sink.

SECURED POWER AWARE ROUTING PROTOCOL (SPAEERP) FOR WIRELESS SENSOR NETWORKS

Entropy

The entropy defined as the amount of information in a message, and it is a function of the probability distribution over the set of all possible messages:

Let x1,…,xn are n possible messages occurring with probability p(x1),…,p(xn). Entropy of a given message is:

$$H(X) = -\sum_{i-1}^{n} p(X = x_i)\log_2 p(X = x_i) \qquad \text{......... (1)}$$

Rate of Language & Absolute Rate

The average number of bits of information in each character

$$r = \frac{H(x)}{N} \qquad \text{......... (2)}$$

Where N is the length of the message is defined as a Rate of Language. In English language $1 \le r \le 1.5$

Absolute Rate is defined as the maximum number of bits of information that could be encoded in each character. If there are L characters in the language is:

$$R = \log_2 L \qquad \text{......... (3)}$$

For English Language

$$R = \log_2 26$$

= 4.7 (bits/letter)

This means 25=32 combinations, The Redundancy of a language with rate r and absolute rate R is define by [8]:

D=R-r .... (4)

Applying above values gives

D=4.7-1.5

=3.2

D/R*100=8%

Unicity Distance

The amount of ciphertext needed to uniquely determine the key:

If Hc(k) $\geq$ 0, then the cipher is unconditionally secure.

Unicity distance gives the number of characters required to uniquely determine the key, it does not indicate the computational difficulty of finding it, and given by [8]:

$$H_c(k) = \sum_k P_c(k)\log_2(1/P_c(k))$$,........ (5)

Modular Classes

If $x \equiv a(\text{mod}n),$ then a, is called a residue of x modulo n. the residue classes of a modulo n, denoted by [a]n, is the set of all those integers that are congruent to a modulo n. that is [9]:

[a] n= {x: x $\in$Z and $x \equiv a(\text{mod}n)$ } ....(6)

= {a + k n: k $\in$ Z}

As an example, let n=5, then there are five residue classes, module 5, namely the sets:

$$\begin{array}{lllllllll} [0]_5 & = & \{ & \cdots & -5 & 0 & 5 & \ldots & \} \\ [1]_5 & = & \{ & \ldots & -4 & 1 & 6 & \ldots & \} \\ [2]_5 & = & \{ & \ldots & -3 & 2 & 7 & \ldots & \} \\ [3]_5 & = & \{ & \ldots & -2 & 3 & 8 & \ldots & \} \\ [4]_5 & = & \{ & \ldots & -1 & 4 & 9 & \ldots & \} \end{array}$$

The Novel Cryptosystem Methodology

The basic idea of our proposed cryptosystem method is depend on set theory. The encryption is defined as a relation between the language alphabetic and a set of sets "one set for each alphabetical element", while the decryption is a relation from a set of sets to the language alphabetic.

As an example for the set of sets is the set of residue classes for a given number N. Hence, the encryption process is defending a relation between the language alphabetic and the prime modular classes P for a given N integer number, where N>P, N is represent as a secret information between the sender and the reserve, which each of them agree on using a secret channelled. The sender uses our proposed encryption algorithm to send a message to the receiver, through unsecured channel, and the receiver uses our proposed decryption algorithm to read the received message.

The encryption algorithm and the decryption algorithm are implemented in the next sub section for the English alphabetical language

Encryption Algorithm

Input: Plaintext, N

Output: Cipher text

Process:

Step1: Find the modular classes for the input N

Step2: Apply each alphabetical English letter Li, to

a prime class Pi, 1=0,…25

Step3: For each input Plaintext letter Xj, randomly

Select a number which belong to the correspond classes.

Step4: Apply a permutation operation to the result cipher text

Step5: End

Decryption Algorithm

Input: Cipher Text, N

Output: Plaintext

Process:

Step1: Find the modular classes for the input N

Step2: Apply each alphabetical English letter Li, to a prime class Pi, 1=0…25

Step3: Apply an inverse permutation operation to the input cipher text

Step4: For each input Ciphertext letter Yj, find the correspond class, that the digital number is belong to.

Step5: End.

SECURED POWER AWARE ENERGY EFFICIENT ROUTING PROTOCOL

Estimation of Link Quality

Due to the mobility of nodes present in wireless sensor network it becomes mandatory to consider the quality of the link. To be able to see that when a node in the wireless sensor network is moving and hence a route is about to break. So that factor, it is probable to measure the quality of the signal and based upon that presumption, when the link is going to break. This information which is identified by the physical layer is send to the upper layer when packets are received from a node, and then indicate that node is in pre-emptive zone.

Pre-emptive zone is the region where the signal strength is weaker which leads to the link failure. Pre-emptive zone uses the pre-emptive threshold value to fix the pr-emptive zone's location. Thus, using the received signal strength from physical layer, the quality of the link is predicted and then the links which are having low signal strength will be discarded from the route selection.

When a sending node broadcasts RTS packet, it piggybacks its transmission power. While receiving the RTS packet, the projected node quantifies the strength of the signal received.

$$P_R = P_T (\lambda / 4 \prod d)^2 * (UG_T) * (UG_R) \qquad \text{--- (7)}$$

Hence,

$L_q = P_R$

Where, P_R refers Power of the Receiving node, P_T stands for Power of the Transmitting node, λ stands for wavelength carrier, d is the distance between the sending and the receiving node, UG_R stands for unity gain of receiving omni-directional antenna, UG_T stands for unity gain of transmitting omni-directional antenna.

Energy Efficient Routing

We assume that there is a target bit error rate (BER) which ensures successful communication across a link. We assume that our system has perfect error detection but no error correction capability. Automatic retransmission request is used so that a packet with error is retransmitted until received correctly.

Suppose that the packet length is M. Then the probability of correct reception of the packet is $P_c(\gamma) = (1 - 2BER(\gamma))^m$ where $BER(\gamma)$ is bit error rate corresponding to a signal to interference and noise ratio (SINR) γ. The BER (.) fuction will depend on the modulation scheme and the noise environment. In this research work, CDMA system is used for which cumulative interference can be assumed to be Gaussian. Non-coherent frequency shift keying is used by which $BER(\gamma) = 0.5\exp(-0.5\gamma)$ under Gaussian noise and interference.

The proposed protocol uses synchronous direct sequence CDMA in which nodes use variable spreading sequences. The preading factor for each transmitter L can be adjusted to meet the Quality-of-Service (QoS) requirements. The minimum spreading gain between the nodes to reach a certain target SINR, is given in the below equation.

$$L_{ij} = \frac{\gamma^* \left\lfloor \sum_{k=1,k\neq i,j}^{N} h_{k.j} P_k \right\rfloor}{h_{ij} P_i = \gamma^2 \sigma^2} \quad \text{--- (9)}$$

Where d_{ij} is the distance between the nodes, p is the path loss exponent, σ^2 is the thermal noise power. The energy per bit represents the total energy consumed in order to deliver one data bit to the destination node. This research considers the energy used for transmission. The energy per bit for packet transmissions between nodes can be defined by the equation (10).

$$E_b^{i,j} = \frac{MP_i}{m\Omega_{ij} P_c(\gamma)} \quad \text{--- (10)}$$

Where M is the length of the packet, m represents the number of control/information bits in a packet, P_i is the constant transmit power.

Working Mechanism of SPAEERP

RN = max ($L_{q\,\&}$ R_{POW}, Min[$E_b^{i,j}$]) --- (8)

Where, CV = Cost Value, L_q = Link quality, R $_{POW}$ = Residual Power of the sensor node

In the proposed work Power Aware Routing Protocol (SPAEERP) a cost value (CV) is calculated. CV is computed based on the on the quality of the link of each wireless sensor node.

Among all the sensor nodes in the network, there are some robust nodes. These robust nodes serve as the backbone for the routing in wireless sensor networks. The remaining sensor nodes are common sensor nodes. Each robust node maintains a table of sensor node power at other robust nodes.

So in the route, each robust node will compute the end-to-end power from itself to any other robust nodes. The sensor node power is estimated and updated periodically by each robust node. The robust node which is nearest to the source node finds the robust nodes which are along the route towards destination sensor node. Then packets will be forwarded through these robust nodes to the destination node. Since robust nodes have better communication capability than common nodes, most of the time the power is less than the maximum power.

- Each robust node can arrive at nearby robust nodes directly. When a robust node goes out of a grid, it initiates a robust node election process in the grid and a new robust node will be selected.
- Each Robust node holds a table of node power. Each Robust node can calculate the end-to-end power from itself to any other robust nodes. The node delay is estimated and updated periodically by each robust node.
- Incase a source node S needs to setup a route to a destination D. It is considered by the case where the source node S itself is a robust node. In this case, first the robust node S needs to know about the current location of the destination node D. With the information of D’s location, S knows about the grid Ld where D stays, and the Robust node Ltd in the grid Ld.
- Then S calculates the minimum power between S and Ltd by means of the power table, and also discovers the route with the minimum power. If the minimum power is greater than the required power, then the route can not be established. The source sensor node generates a unique req id for each route request. When an intermediate node obtains the REQ packet, it adds the powers of the incoming link and itself to t power, and compares the updated t power with the max power. If t power is less than the max power, it adds up itself to the route list, and forwards the REQ packet to the neighbors. If t power is greater than max power, the node will drop the REQ packet.
- If the minimum power between S and Ltd is less than the maximum power, sensor node S will notify Ltd to locate a route to the destination D. Then Ltd will update the t power by adding the power between Ltd and D. If the updated t_power is less than max_power, a valid route is found. Ltd will send an ACK (acknowledge) packet to S along the reverse path to ascertain that the route is setup. And each node in the route will updates its node power. After that S can start sending data.
- If S is not a Robust node, then S will first discover a path to the nearby Robust node with less power than required. Node S sends out the route request (REQ) packet by flooding to all the sensor nodes in its grid. Only sensor nodes in the same grid will process and forward the REQ packet. When a node gets the REQ packet, it will update the power from source to their locations (t power). If t power is less than max power, it adds itself to the route list, and forwards the REQ packet to the neighbors. If t power is larger than max power, the node will drop the REQ packet. When the Robust node in this grid gets the first REQ packet, it also updates the t power and compares it with max power. If t_power is less than max power, it will calculate the minimum power between itself and the robust node which is nearest to the destination. The remaining steps are the same as above.
- Sensor node power and current location information of robust nodes has to be updated and distributed among all robust nodes. The distribution is done periodically, and the length of the updating period depends on the network dynamics, such as sensor node mobility, sensor network traffic, sensor node communication capability, etc.

Election of Robust Node

At the start, one robust node is set in each grid. We need an election mechanism to produce new Robust nodes because robust nodes also move around. When a Robust node leaves its current grid or due to any other reason there is no robust node in the grid. Suppose, there are more Robust nodes in the current grid of the network, then, the next node with least weighted value from the sorted list will be chosen as the new Robust node for the grid.

In the proposed routing algorithm, we need to compute the minimum delay between two robust nodes, and find the path with the minimum delay.

```
For each valid path Pi,
    For every node nk in Pi
        t_power = t_power + power (nL, nk) + power (nk)
        If t_power >= max_power, delete this path, break.
        If t_power >= min_power, delete this path, break.
        If nk is the destination D, and t_power< min_power, min_power = t_power;
        best_path = Pi + {nk};
        Else add node nk to the end of the path,
    End For
End For
```

Pseudo code for Robust Sensor node election

SIMULATION SETTINGS, PERFORMANCE METRICS

Simulation Settings

Table 1: Simulation Settings

No. of Nodes	50, 75, 100, 125 and 150
Area Size	1000 X 1000
Mac	802.11
Radio Range	250m
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	512 KB
Mobility Model	Random Way Point
Speed	5 m/s
Pause time	100 Seconds

Performance Metrics

Average end-to-end delay: The end-to-end-delay is averaged over all surviving data packets from the source sensor node to the destination sensor node.

Average Packet Delivery Ratio: It is the ratio of the number of packets received successfully and the total number of packets sent.

Total power consumption: It is the average power consumption of all the sensor nodes in the network.

RESULTS

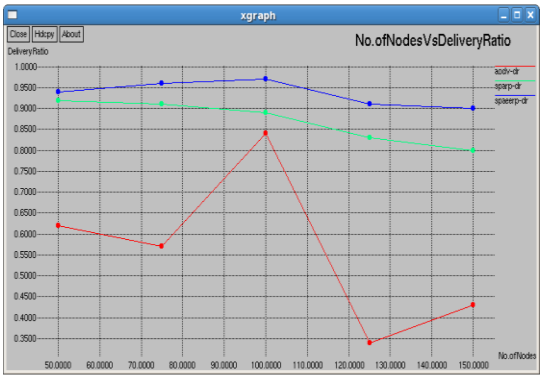

Figure 1: No. of Nodes vs Packet Delivery Ratio

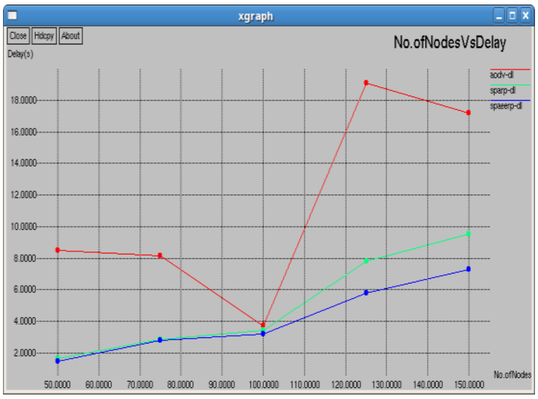

Figure 2: No. of Nodes vs Delay

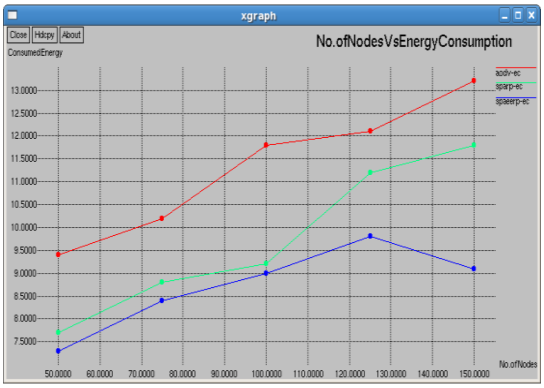

Figure 3: No. of Nodes vs Energy Consumption

CONCLUSIONS

In this paper in order to attain preferred quality of service (QoS) such as packet delivery ratio, delay and to reduce the power consumption and energy efficiency of wireless sensor nodes we proposed secured power aware energy efficient routing protocol (SPAEERP), which attains application-specified communication delays at low energy cost by dynamically adapting transmission power and routing decisions along with incorporating a novel cryptosystem.

Through extensive simulation in NS2 the results proved that the proposed SPAEERP attains better QoS and reduced power and energy consumption. For security validation Cryptool is used to test the novel proposed cryptosystem.

REFERENCES

1. R. Prema and R. Rangarajan, "Secured Power Aware Routing Protocol (SPARP) for Wireless Sensor Networks," International Journal of Computer Applications, Vol. 51 No. 17, August 2012, pp. 13-18.
2. Chien-Yuan Chen, Cheng-Yuan Ku b and David C.Yen, "Cryptanalysis of large RSA exponent by using the LLL algorithm", in Proceedings of The Tenth National Conference on Information Security, Taiwan, Pages: 45-50, 2000.
3. Kwok-Wo Wong, Sun-Wah Ho, and Ching-Ki Yung, "A chaotic cryptography scheme for generating short ciphertext", Physics Letters A, Volume 310, Number 1, Pages:67-73, 2003.
4. Chang-Doo Lee, Bong-Jun Choi and Kyoo-Seok Park, "Design and evaluation of a block encryption algorithm using dynamic-key mechanism". Future Generation Computer Systems, Volume: 20, Issue: 2, Pages: 327 - 338, 2004.
5. Mark G. Simkin, "Using Spreadsheets to Teach Data Encryption Techniques", AIS Educator Association, Volume 1, Number 1, pages 27 - 37, 2006.
6. Jun Wei, Xiaofeng Liao, Kwok-wo Wong, and Tao Xiang, "A new chaotic cryptosystem", Chaos Solitons & Fractals 30 (5): 1143-1152 Dec 2006.
7. Osama Mahmud Abu Abbas, Khalid Mohammad Nahar, and Mohammad Ahmad Tubishat, "Arae Cipher System", Computer Science Department, IT Faculty, Yarmouk University, Jordan, 2007.
8. [8] E. Zeydan, D. Kivanc, C. Comaniciu, Efficient routing for correlated data in wireless sensor networks, in: IEEE MILCOM’08, 2008.
9. C. Jones, K. Sivalingam, P. Agrawal, A survey of energy efficient network protocols for wireless networks, ACM Journal of Wireless Networks (WINET) 7 (4) (2001) 343–358.
10. I.F. Akyildiz, W. Sue, Y. Sankarasubarmaniam, E. Cayirci, A survey on sensor networks, IEEE Communications Magazine 50 (8) (2002) 102– 114.
11. S. Banerjee, A. Misra, Minimum energy paths for reliable communication in multi-hop wireless networks, in: MobiHoc ’02: Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking & Computing, 2002, pp. 146–156.
12. V. Rodoplu, T. Meng, Minimum energy mobile wireless networks, IEEE Journal on Selected Areas in Communications 17 (8) (1999) 1333–1443.
13. M. Ettus, System capacity, latency, and power consumption in multihop-routed SS-CDMA wireless networks, in: IEEE Radio and Wireless Conference (RAWCON’98), 1998.
14. I. Stojmenovic, X. Lin, Power aware localized routing in wireless networks, IEEE Transactions on Parallel and Distributed Systems 12 (11) (2001) 1122–1133.
15. R. Madan, S. Lall, Distibuted algorithms for maximum lifetime routing in wireless sensor networks, IEEE Transactions on Wireless Communications 5 (4) (2006) 2185–2193.

16. C. Hua, T.P. Yum, Optimal routing and data aggregation for maximizing lifetime of wireless sensor networks, IEEE/ACM Transactions on Networking 16 (4) (2008) 892–903.

17. H.O. Tan, I. Korpeoglu, I. Stojmenovic, Computing localized power efficient data aggregation trees for sensor networks, IEEE Transactions on Parallel and Distributed Systems 22 (3) (2011).

18. L. Tu, H. Hong, G. Zhou, Minimum cost routing with a lifetime guarantee in wireless sensor networks, in: IEEE/ACM International Conference on Green Computing and Communications and International Conference on Cyber, Physical and Social Computing, 2010.

19. L. Mottola, G.P. Picco, MUSTER: adaptive energy-aware multi-sink routing in wireless sensor networks, IEEE Transactions on Mobile Computing 10 (12) (2011) 1694–1709.

20. H. Sabbineni, K. Chakrabarty, An energy-efficient data delivery scheme for delay-sensitive traffic in wireless sensor networks, International Journal of Distributed Sensor Networks, 2010. Article ID 792068.

21. A. Scaglione, S. Servetto, On the interdependence of routing and data compression in multi-hop sensor networks, in: ACM Wireless Networks, vol. 11, 2005, pp. 149–160.

22. H. Luo, Y. Liu, S.K. Das, Routing correlated data with fusion cost in wireless sensor networks, IEEE Transactions on Mobile Computing 5 (11) (2006) 1620–1632.

23. R. Cristescu, B.B. Lozano, M. Vetterli, R. Wattenhofer, Network correlated data gathering with explicit communication: NP completeness and algorithms, IEEE/ACM Transactions on Networking 14 (1) (2006) 41–54.

24. [24] P. von Rickenbach, R. Wattenhofer, Gathering correlated data in sensor networks, in: DIALM-POMC ’04: Proceedings of the Joint Workshop on Foundations of Mobile Computing, 2009.

25. S. Pattem, B. Krishnamachari, R. Govindan, The impact of spatial correlation on routing with compression in wireless sensor networks, ACM Transactions on Sensor Networks 4 (4) (2008) 1–33.

26. L. Krishnamachari, D. Estrin, S. Wicker, The impact of data aggregation in wireless sensor networks, in: 22nd International Conference on Distributed Computing Systems Workshops, 2002, pp. 575–578.

27. S. Lindsey, C. Raghavendra, K.M. Sivalingam, Data gathering algorithms in sensor networks using energy metrics, IEEE Transactions on Parallel and Distributed Systems 13 (9) (2002) 924–935.

28. C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, F. Silva, Directed diffusion for wireless sensor networking, IEEE/ACM Transactions on Networking 11 (1) (2003) 2–16.

29. W.B. Heinzelman, A.P. Chandrakasan, H. Balakrishnan, An application specific protocol architecture for wireless microsensor networks, IEEE Transactions on Wireless Communications 1 (4) (2002) 660–670.