ISSN:0975-9646

Garaga Subba Rao et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (4) , 2012,4718 - 4722

False Data Detection in Wireless Network using Dynamic Security Protocol

Garaga Subba Rao, Kothapalli Ramesh

Dept. of CS,
KIET, KORANGI.

Abstract- in the Wireless sensor networks often consists of a large number of low-cost sensor nodes that have strictly limited sensing, computation, and communication capabilities. The security of wireless sensor networks is a challenging problem in the process of data aggregation. As data are send though sensor network confidentiality plays and important role between source and destination. Secure data aggregation is proposed to enhance the data security of wireless sensor networks. In wireless sensor networks, compromised sensor nodes can inject false data during both data aggregation and data forwarding. The existing false data detection techniques consider false data injections during data forwarding only and do not allow any change on the data by data aggregation. In this paper we can see how the data is being remain confidential between source and destination by using Dynamic security protocol for securing the data in wireless sensor network.

Keywords: data integrity, network-level, security, sensor networks. DSP(Dynamic security protocol).

I. INTRODUCTION

Wireless sensor networks are usually composed of hundreds or thousands of inexpensive, low-powered sensing devices with limited memory, computational, and communication resources [1,2]. These networks offer potentially low-cost solutions to an array of problems in both military and civilian applications, including battlefield surveillance, target tracking, environmental and health care monitoring, wildfire detection, and traffic regulation. Due to the low deployment cost requirement of wireless sensor networks, sensor nodes have simple hardware and severe resource constraints [6]. Hence, it is a challenging task to provide efficient solutions to data gathering problem. sensor networks are vulnerable to many types of security attacks, including false data injection, data forgery, and eavesdropping [1]. Sensor nodes can be compromised by intruders, and the compromised nodes can distort data integrity by injecting useless data. The transmission of useless data depletes the constrained battery power and degrades the bandwidth utilization. Useless data can be injected by compromised sensor nodes in various ways, including data aggregation and relaying. Data aggregation is essential to reduce data redundancy and to improve data accuracy. In addition to useless data detection, data confidentiality is required by many sensor network applications to provide safeguard against eavesdropping. Therefore, in order to reduce the power consumption of wireless sensor networks, several mechanisms are proposed such as radio scheduling, control packet elimination, topology control, and most importantly data aggregation [2,3]. Data aggregation protocols aim to combine and summarize data packets of several sensor nodes so that amount of data transmission is reduced. data aggregation scheme is presented a group of sensor nodes collect information from a target region. When the base station queries the network, instead of sending each sensor node's data to base station, one of the sensor nodes, called data aggregator, collects the information from its neighboring nodes, aggregates them (e.g., computes the average), and sends the aggregated data to the base station over a multi-hop path. As illustrated by the example, data aggregation reduces the number of data transmissions thereby improving the bandwidth and energy utilization in the network. paper will serve as a useful guide and starting point for the researchers who are interested in conducting research in the secure data aggregation area. is given by evaluating each protocol based on the security requirements of wireless sensor networks.

II. SECURITY REQUIREMENTS OF WIRELESS SENSOR NETWORKS

In the network environments and unique properties of wireless sensor networks, it is a challenging task to protect sensitive information transmitted by wireless sensor networks [1]. In addition, wireless sensor networks have security problems that traditional networks do not face. Therefore, security is an important issue for wireless sensor networks and there are many security considerations that should be investigated. In this section, we present the dynamic security protocol mechanisum for essential security requirements that are raised in a wireless sensor network environment and explain how these requirements relate with data aggregation process. illustrates the interaction between wireless sensor network security requirements and data aggregation process.

Data integrity

Although data confidentiality guarantees that only intended parties obtain the un-encrypted plain data, it does not protect data from being altered. Data integrity guarantees that a message being transferred is never corrupted. A malicious node may just corrupt messages to prevent network from functioning properly. In fact, due to unreliable communication channels, data may be altered without the presence of an intruder. Thus, message authentication codes or cyclic codes are used to prevent data integrity. Data aggregation results in alterations of data; therefore, it is not

possible to have end-to-end integrity check when data aggregation is employed. Moreover, if a data aggregator is compromised, then it may corrupt sensor data during data aggregation and the base station has no way of checking the integrity of this aggregated sensor data. Providing data integrity is not enough for wireless communication because compromised sensor nodes are able to listen to transmitted messages and replay them later on to disrupt
the data aggregation results. Data freshness protects data aggregation schemes against replay attacks by ensuring that the transmitted data is recent.

Source security

Since wireless sensor networks use a shared wireless medium, sensor nodes need DSP mechanisms to detect maliciously injected or spoofed packets. Source authentication enables a sensor node to ensure the identity of the peer node it is communicating with. Without source authentication, an adversary could masquerade a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes. Moreover, a compromised node may send data to its data aggregator under several fake identities so that the integrity of the aggregated data is corrupted. Faking multiple sensor node identities is called Sybil attack and it poses significant threat to data aggregation protocols [5]. If only two nodes are communicating, authentication can be provided by DSP. The sender and the receiver share a secret key to compute the message authentication code (MAC) for all transmitted data.

Data aggregation

In a typical wireless sensor network, a large number of sensor nodes collect application specific information from the environment and this information is transferred to a central base station where it is processed, analyzed, and used by the application. In these resource constrained networks, the general approach is to jointly process the data generated by different sensor nodes while being forwarded toward the base station [8]. Such distributed in-network processing of data is generally referred as data aggregation and involves combining the data that belong the same phenomenon. The main objective of data aggregation is to increase the network lifetime by reducing the resource consumption of sensor nodes (such as battery energy and bandwidth). While increasing network lifetime, data aggregation protocols may degrade important quality of service metrics in wireless sensor networks, such as data accuracy, latency, fault-tolerance, and security. Therefore, the design of an efficient data aggregation protocol is an inherently challenging task because the protocol designer must tradeoff between energy efficiency, data accuracy, latency, fault-tolerance, and security. In order to achieve this trade off, data aggregation techniques are tightly coupled with how packets are routed through the network. Hence, the architecture of the sensor network plays a vital role in the performance of different data aggregation protocols. There are several protocols that allow routing and aggregation of data packets simultaneously. These protocols can be categorized into two parts: tree-based data aggregation protocols and cluster-based data aggregation protocols. Earlier work on data aggregation focused on improving the existing routing algorithms so as to make data aggregation possible. As a result, many data aggregation protocols based on shortest path tree structure have been proposed [10,17]. To reduce the latency due to tree-based data aggregation, recent work on data aggregation tends to group sensor nodes into clusters so that data are aggregated in each group for improved efficiency.

III. SECURE DATA AGGREGATION USING DSP

By using traditional symmetric key cryptography algorithms, it is not possible to achieve end-to-end confidentiality and in-network data aggregation together. If the application of dynamic security protocol algorithms is combined with the requirement of efficient data aggregation, then the messages must be encrypted hop-by-hop. However, this means that, in order to perform data aggregation, intermediate nodes have to decrypt each received message, then aggregate the messages according to the corresponding aggregation function, and finally encrypt the aggregation result before forwarding it. Clearly, this is not an energy efficient way of performing secure data aggregation and it may result in considerable delay. In addition, this process requires neighboring data aggregators to share secret keys for decryption and encryption. In order to achieve end-to-end data confidentiality and data aggregation together without requiring secret key sharing among data aggregators privacy homomorphic cryptography has been used in the literature [16]. A privacy homomorphism is an encryption transformation that allows direct computation on encrypted data. Let E denotes encryption and D denotes decryption. Also let þ denotes addition and _ denotes multiplication operation over a data set Q. Assume that Kpr and Kpu are the private and public keys of the base station, respectively. An encryption transformation is accepted to be additively homomorphic since, additively and multiplicatively homomorphic cryptographic functions support additive and multiplicative operations on encrypted data, respectively, data aggregators can perform addition and multiplication based data aggregation over the encrypted data. In Concealed Data Aggregation (CDA) [22], sensor nodes share a common symmetric key with the base station that is kept hidden from intermediate aggregators. The major contribution of this work is the provision of end-to-end encryption for reverse multicast traffic between the sensors and the base station. In the proposed approach, data aggregators carry out aggregation functions that are applied to cipher texts (encrypted data). This provides the advantage that intermediate aggregators do not have to carry out costly decryption and encryption operations. Therefore, data aggregators do not have to store sensitive DSP which ensures an unrestricted aggregator node election process for each epoch during the wireless sensor network's lifetime. Unrestricted data aggregator selection is impossible for hopby- hop encryption because only the nodes which have stored the key can act as a data aggregator. As the privacy homomorphic encryption function, the proposed protocol employs the function proposed by Domingo-Ferrer

[42]. Domingo-Ferrer's encryption function is probabilistic in the sense that the encryption transformation involves some randomness that chooses the ciphertext corresponding to a given plaintext from a set of possible ciphertexts. The public parameters of Domingo-Ferrer's encryption function are a positive integer d P 2 and a large integer g that must have many small divisors. In addition, there should be many integers less than g that can be inverted modulo g. The secret key is computed as k ðr; g0Þ. The value r 2 Zg is chosen such that r1 mod g exists where $\log_{g0}$ g indicates the security level provided by the function. The set of plaintext is Zg0 and the set of ciphertext is ðZgÞd. Encryption and decryption processes are defined . The ciphertext operation is performed by cross-multiplying all terms in Zg , with the d1-degree term by a d2-degree term yielding a t-degree term. Then, the terms having the same degree are added up. The ciphertext operation + is relatively easy compared to operation and is performed component-wise. As it is seen from the above definitions, Domingo-Ferrers asymmetric key based privacy homomorphism is computationally expensive for resource constrained sensor nodes. Authors of [26] compared the clock cycles required by asymmetric key based privacy homomorphism and symmetric key based encryption solutions. The results show that encryption, decryption, and addition operations that are needed to implement Domingo-Ferrers function are much more expensive compared to those are necessary to perform symmetric key based RC5. However, the authors argue that this disadvantage is acceptable as CDA advantageously balance the energy consumption. Using symmetric key based encryption solutions to perform hop-by-hop data aggregation results in shorter lifetime for data aggregator nodes. Therefore, as data aggregators are the performance bottleneck when maintaining a connected wireless sensor network backbone, it is preferable to employ CDA's asymmetric key based privacy homomorphism to balance the energy consumption of data aggregators. In [20], a secure data aggregation protocol, called CDAP, takes advantage of asymmetric key based privacy homo- morphic cryptography to achieve end-to-end data confidentiality and data aggregation together. The authors point out that asymmetric cryptography based privacy homomorphism incurs high computational overhead which cannot be afforded by regular sensor nodes with scarce resources. To mitigate this problem, CDAP protocol employs a set of resource-rich sensor nodes, called aggregator nodes (AGGNODEs), for privacy homomorphic encryption and aggregation of the encrypted data. In CDAP, after the network deployment each AGGNODE establishes pairwise keys with its neighboring nodes so that neighboring nodes can send their sensor readings securely. In data collection phase of protocol CDAP, each AGGNODE queries its neighboring nodes. Each neighboring node encrypts its data (using RC5 algorithm) sends the encrypted data to its AGGNODE. The AGGNODE decrypts all the data received from its neighbors, aggregates them, and encrypts the aggregated data using the privacy homomorphic encryption algorithm. Once the data are encrypted with the privacy homomorphic encryption algorithm, only the base station can decrypt them using its private key. Due to homomorphic property, intermediate AGGNODEs can aggregate those encrypted data during data forwarding. Therefore, the data collected by sensor nodes are aggregated by AGGNODEs as they travel towards the base station. The base station decrypts the final aggregated data using its private key. Due to the computational overhead of privacy homomorphic encryption algorithms, in CDAP, only AGGNODEs are allowed to encrypt and aggregate the collected data using privacy homomorphic algorithms. Therefore, during the initial data collection phase of the protocol CDAP, sensor nodes uses symmetric key algorithms for encryption. Due to the symmetric encryption, a compromised AGGNODE may disclose the secrecy of its neighboring nodes' data or inject false data into the data. However, the authors argue that the effect of this attack is local, and hence, it can be tolerated. In [23], a simple and provably secure additively homomorphic stream cipher that allows efficient aggregation of encrypted data is proposed. The proposed technique is based on an extension of the one-time pad encryption technique using additive operations over modulo n. The main idea of the proposed scheme is to replace the Exclusive – OR operation of stream ciphers with modular addition ðþÞ. The encryption and decryption processes can be summarized as follows. Represent message m as , the proposed scheme is additively homomorphic. The proposed scheme significantly reduces the energy consumption of sensor nodes due to encryption process. However, in the proposed scheme, each aggregate message is coupled with the list of nodes that failed to contribute to the aggregation. When the aggregation tree is large, the list of sensor nodes become larger and results in a significant communication overhead. This problem has been solved in [18] by adapting a hierarchical data aggregation model. Similar to [17,18], a layered secure data aggregation protocol in wireless sensor networks that offers end-to-end data confidentiality by using homomorphic functions and interleaved encryption is proposed in [19]. The proposed protocol ensures that, in the presence of less than n compromise nodes, an attacker cannot get access to any aggregated data from the network. When more than n nodes are captured, the attacker can only get access to the aggregated values received by the captured nodes. In [41], the authors realize the fact that existing privacy homomorphism based in-network processing protocols can only work for some specific query-based aggregation functions, e.g., sum, average, etc. Hence, instead of privacy homomorphism, the authors take advantage of digital watermarking and propose an end-to-end, statistical approach for data authentication that provides inherent support for data aggregation. The novel idea of this work is to modulate authentication information as watermark and superpose this information on the sensory data at the sensor nodes. The watermarked data can be aggregated by the intermediate nodes without incurring any en route checking. In order to check whether the data has been altered by the compromised nodes, upon reception of the sensory data, the data sink is able to authenticate the data by

validating the watermark. More specifically, the proposed technique visualizes the sensory data gathered from the whole network at a certain time snapshot as an image, in which every sensor node is viewed as a pixel with its sensory reading representing the pixels intensity. Since senor data is represented as an ‘‘image” digital watermarking can be applied to this image. In order to balance the energy consumption among sensor nodes, a direct spread spectrum sequence (DSSS) based watermarking technique is used. While each sensor node appends a part of the whole watermark into its sensory data, verification of watermark which requires an extensive computational resource is left to the sink. The proposed scheme adopts the existing image compression schemes as the aggregation functions to reduce network load while retaining the desired details of the data. Moreover, using a DSSS based watermarking scheme, the proposed technique is enabled to survive a certain degree of distortion and therefore naturally support data aggregation presents the comparison of secure data aggregation schemes with respect to wireless sensor network security requirements. As seen from almost all secure data aggregation protocols ensure data integrity and DSP. Protocols in [16,20,17] focus solely on aggregation of encrypted data and do not provide data integrity and source authentication support. However, these protocols can be modified easily to support data integrity and source authentication. Table 1 also shows that some of the secure data aggregation protocols ([26]) do not support data confidentiality which is essential for mission critical wireless sensor network applications. Therefore, these protocols should be used only in applications in which the transmitted data is not secret. Among the protocols that provide data confidentiality, the protocols proposed in [29] can offer end-to-end data confidentiality.

IV. RELATED WORK

In this paper, we present a comprehensive overview of Dynamic security protocol concept in wireless sensor networks. We survey the state-of-the-art data aggregation protocols and categorized them based on network topology and security. Although the presented research addresses the many problems of data aggregation, there are still many research areas that needs to be associated with the DSP, especially from the security point of view. As for the general data aggregation concept, the relation between routing mechanisms and DS protocols have been well studied as they are highly correlated topics. In addition to diffusion and tree-based data aggregation protocols, many cluster-based data aggregation protocols that route aggregated data over cluster heads have been proposed. Although, these protocols shown to be very efficient in static networks in which the cluster structures do not change for a sufficiently long time, in dynamic networks they perform quite poorly. Hence, data aggregation in dynamic environments is a possible future research direction. The impact of sensor node heterogeneity over the data aggregation protocols is another unexplored research area [10]. The protocols that use powerful sensor nodes as data aggregators presented promising results. However, determining locations of these powerful nodes for the best data aggregation results needs further research. Security is an important issue for data aggregation process and it needs to be further investigated. Clearly, there are still secure data aggregation issues that have not been addressed by the existing research. One such problem is compromised data aggregators that inject false data during data aggregation. Because data aggregation usually results in alterations in collected sensor data, false data injections by compromised data aggregators are hard to detect. There is only limited work targeting this problem and the proposed techniques are all based on extensive node monitoring mechanisms [22]. The efficiency of these node monitoring protocols is not fully evaluated and they usually incur high radio and sensing resource consumption. Hence, development of lightweight DSP monitoring mechanisms specifically for secure data aggregation process is an interesting problem for future research. In order to provide end-to-end security, privacy homomorphism based secure data aggregation protocols have drawn considerable attention recently. However, the design and implementation of resource efficient privacy homomorphic aggregation functions yet to be explored. Many existing public key cryptography based privacy homomorphic functions are not feasible for resource limited sensor nodes. Hence, in some secure data aggregation schemes elliptic curve cryptography is employed [16]. However, these elliptic curve cryptography based privacy homomorphic functions can only work for some specific query-based aggregation functions, e.g., sum, average, etc. Therefore, design of efficient privacy homomorphic functions that are able to work with all types of data aggregation functions needs to be explored. In addition, for certain wireless sensor network settings where real-time data delivery is demanded, symmetric key cryptography based privacy homomorphic encryption schemes are recommended [3]. But, there are not many symmetric key based privacy homomorphic schemes. Hence, exploration of symmetric key cryptography based privacy homomorphic functions in the secure data aggregation concept is another promising research area. Using ‘‘digital watermarking” schemes to replace the expensive privacy homomorphic functions is a newly introduced concept in secure data aggregation [11]. However, this method allows only one way authentication of sensor data at the base station. Hence, investigation of two-way authentication by using watermarking techniques that will allow in-network DSP in the network may be a good research direction. In addition, the application of source coding theory for data aggregation has drawn a little attention so far. Considering that sensor data is highly correlated, data aggregation can be achieved by employing source coding techniques. Existing research in this area focuses on only theoretical results and there are no practical algorithms applicable to wireless sensor networks yet. Moreover, there is no secure data aggregation protocol that uses the idea of source coding which may seamlessly integrate data confidentiality and aggregation together. Therefore, there is

significant scope for future work in source coding based DSP. Secure hierarchical data aggregation is expected to produce a vast amount of research in the future. Many secure data aggregation protocols assume that sensor data are aggregated at a single sink or data aggregator. Especially for privacy homomorphic secure data aggregation protocols providing hierarchical aggregation is not a trivial task. Hence, extending the current single level secure data aggregation protocols to multi layer hierarchical data aggregation protocols is an interesting problem for future research.

V. CONCLUSION

This paper provides a detailed review of Dynamic security protocol concept in wireless sensor networks. To give the motivation behind secure data aggregation, first, the security requirements of wireless sensor networks are presented and the relationships between data aggregation concept and these security requirements are explained. Second, an extensive literature survey is presented by summarizing the state-of-the-art data aggregation protocols in wireless sensor network.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankara subramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Commun. Mag., vol. 40, no. 8, pp.102–114, Aug. 2002.

[2] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical en-route detection and filtering of injected false data in sensor networks," in Proc. IEEE INFOCOM, 2004, vol. 4, pp. 2446–2457.

[3] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "Interleaved hopby- hop authentication against false data injection attacks in sensor networks," ACM Trans. Sensor Netw., vol. 3, no. 3, Aug. 2007.

[4] H. Yang and S. Lu, "Commutative cipher based en-route filtering in wireless sensor networks," in Proc. IEEE VTC, 2004, vol. 2, pp.1223–1227.

[5] Z. Yu and Y. Guan, "A dynamic en-route scheme for filtering false data in wireless sensor networks," in Proc. IEEE INFOCOM, Barcelona, Spain, Apr. 23–27, 2006, pp. 1–12.

[6] C. Intanagonwiwat, D. Estrin, R. Govindan, and J. Heidemann, "Impact of network density on data aggregation in wireless sensor networks," in Proc. 22nd Int. Conf. Distrib. Comput. Syst., Jul. 2002, pp. 575–578.

[7] A. Perrig, R. Szewczyk, D. Tygar, V. Wen, and D. Culler, "SPINS: Security protocols for sensor networks," Wireless Netw. J., vol. 8, pp. 521–534, Sep. 2002.

[8] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Trans. Inf. Theory, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.

[9] L. Hu and D. Evans, "Secure aggregation for wireless networks," in Proc. Workshop Security Assurance Ad hoc Netw., Orlando, FL, Jan. 28, 2003, pp. 384–394.

[10] B. Przydatek, D. Song, and A. Perrig, "SIA: Secure information aggregation in sensor networks," in Proc. SenSys, 2003, pp. 255–265.

[11] D. Wagner, "Resilient aggregation insensor networks." ACM Workshop on Security of Ad Hoc and Sensor Networks, 2004, pp. 78-87.

[12] D. Seetharam and S. Rhee, "An efficient pseudo random number generator for low-power sensor networks," in Proc. 29th Annu. IEEE Int. Conf. Local Comput. Netw., 2004, pp. 560–562.

[13] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A pairwise key predistribution scheme for wireless sensor networks," in Proc. 10th ACM CCS, 2003, pp. 42–51.

[14] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, A survey on sensor networks, IEEE Commun. Mag. 40 (8) (2002) 102– 114.

[15] J. Yick, B. Mukherjee, D. Ghosal, Wireless sensor network survey, Comput. Networks 52 (12) (2008) 2292–2330.

[16] 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 (2008) 171–193.

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

[18] A. Perrig, R. Szewczyk, D. Tygar, V. Wen, D. Culler, SPINS: security protocols for sensor networks, Wireless Networks J. (WINE) 2 (5) (2002) 521–534.

[19] Crossbow Technologies Inc. <http://www.xbow.com>.

[20] E. Fasolo, M. Rossi, J. Widmer, M. Zorzi, In-network aggregation techniques for wireless sensor networks: a survey, IEEE Wireless Commun. 14 (2) (2007) 70–87.

[21] R. Rajagopalan, P.K. Varshney, Data aggregation techniques in sensor networks: a survey, IEEE Commun. Surveys Tutorials 8 (4) (2006).

[22] C. Intanagonwiwat, D. Estrin, R. Govindan, J. Heidemann, Impact of network density on data aggregation in wireless sensor networks, in: Proceedings of the 22nd International Conference on Distributed Computing Systems, 2002, pp. 457–458.

[23] C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, F. Silva, Directed diffusion for wireless sensor networking, in: IEEE/ACM Transactions on Networking, vol. 11, 2003, pp. 2–16.

[24] B. Krishnamachari, D. Estrin, S. Wicker, The impact of data aggregation in wireless sensor networks, in: Proceedings of the 22nd International Conference on Distributed Computing Systems Workshops, 2002, pp. 575–578. S. Ozdemir, Y. Xiao / Computer Networks 53 (2009) 2022–2037 2035

[25] M. Ding, X. Cheng, G. Xue, Aggregation tree construction in sensor networks, in: Proceedings of the 58th IEEE Vehicular Technology Conference, vol. 4, 2003, pp. 2168–2172.

[26] R. Cristescu, B. Beferull-Lozano, M. Vetterli, On network correlated data gathering, in: Proceedings of the 23rd Annual Joint Conference of the IEEE Computer and Communications Societies, vol. 4, 2004, pp. 2571–2582.

[27] S. Madden et al., TAG: A Tiny AGgregation Service for Ad Hoc Sensor Networks, OSDI, Boston, MA, 2002.

[28] B. Zhou et al., A Hierarchical Scheme for Data Aggregation in Sensor Network, IEEE ICON 04, Singapore, 2004.

[29] M. Lee, V.W.S. Wong, An Energy-Aware Spanning Tree Algorithm for Data Aggregation in Wireless Sensor Networks, IEEE PacRrim, Victoria, BC, Canada, 2005.

[30] S. Lindsey, C. Raghavendra, K.M. Sivalingam, Data gathering algorithms in sensor networks using energy metrics, IEEE Trans. Parallel Distrib. Sys. 13 (9) (2002) 924–935.

[31] G. Di Bacco, T. Melodia, F. Cuomo, A MAC Protocol for Delay-Bounded Applications in Wireless Sensor Networks, Med-Hoc-Net, Bodrum, Turkey, 2004.

[32] W.B. Heinzelman, A.P. Chandrakasan, H. Balakrishnan, An application-specific protocol architecture for wireless microsensor networks, IEEE Trans. Wireless Commun. 1 (4) (2002) 660– 670.