Journal of Theoretical and Applied Information Technology
31st May 2016. Vol.87. No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

EFFICIENT ENERGY MOBILE AGENT COLLECTOR FOR INTRUSION DETECTION SYSTEM IN WIRELESS SENSOR NETWORK

[1]YOUSEF EL MOURABIT, [1]AHMED TOUMANARI, [1]MARYAM EL AZHARI, [2]ANOUAR BOUIRDEN,

[1]Equipe signaux, systems et informatique (ESSI), Faculty of sciences, Ibn Zohr University, Agadir Morocco.

[2]Laboratoire thermodynamique et energitique, faculty of sciences Agadir, Ibn Zohr university, Morocco

E-mail: *yousef.elmourabit@edu.uiz.ac.ma

ABSTRACT

Wireless sensor networks (WSNs) consists of a small size battery powered sensor nodes. Due to their constrained characteristics, WSNs are vulnerable to various attacks, which make the security a major concept to handle. Intrusion detection system (IDS) becomes essential tools to ensure the safety of this kind of network. However, since sensors nodes are usually equipped with small and limited energy resources, a significant limitation is presented mainly in terms of energy autonomy which therefore affects the network lifetime. Thereby, It is greatly important to ensure an efficient IDS by strategically deploying an appropriate collector to minimize the amount of energy consumed. In this paper we propose an efficient mobile agent collector to minimize energy consumption and delay transmission for IDS in WSN. The proposed mobile agent collector is validated through simulation experiments using OMNET++ and Castalia simulator, sensor nodes positions are predefined by the base station whilst Dijkstra's algorithm is used to find the optimal path towards the base station passing by source nodes to gather the required data. The simulation provides empirical results illustrating the effectiveness of our approach.

Keywords: *Mobile Agent, Intrusion Detection, Data Collection, Energy Consumption, Wireless Sensor Network.*

1. INTRODUCTION

Wireless sensor networks (WSNs) consist of sensor nodes, which are small devices equipped with wireless transceiver, battery, microcontroller and sensors. Sensor nodes have the capability of self-healing and self-organizing. The main objective of a sensor node is to collect data from its surrounding environment and transmit it to the base station (BS). WSNs have several applications used in scenarios such as monitoring environments and habitats, detecting climate changed, military and surveillance applications [1],they are deployed in hostile environments where nodes are always vulnerable to various types of attacks and security risks damages. Furthermore, low battery power supply, distributed operations using open wireless medium, limited bandwidth support, are such characteristics of sensor networks that make security the major challenge to handle. Many security-related solutions for WSNs have been proposed such as secure routing or security mechanisms for specific attacks, authentication, and key exchange, however, this solution cannot guarantee the required security for this type of networks, for instance, an attacker has the possibility to compromise any sensor node. Even though cryptographic techniques [2] seem to be a promising solution, they still cannot eliminate most of the security attacks [3]. Hence, in order to ensure WSNs security, intrusion detection system (IDS) has been proposed as a second line of defense. The first phase of IDS development in WSNs is the data collection phase. In this very critical step, we get the data that is used to decide whether it is an attack or intrusion. Our IDS is based on mobile agent approach[4], which deploys mobile agent for the collection task ,it is a flexible, robust, and distributed solution to data collection problem in wireless sensor networks. However,the approach of using a mobile agent has a a significant impact on data collection efficiency. Routing Protocols designed for WSNs put a high emphasis on energy conservation, since the nodes run on limited battery

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

power. Data generated by the sensor nodes is transmitted to the sink node either periodically or based on events occurrences enhancing though the possibility of the sensor nodes batteries running out of energy and leading to a frequent disconnection and loss of the corresponding zone coverage, these constraints highly encouraged the use of mobile agent approach to collect data and increase the network lifetime[5];In this paper, we propose an efficient mobile agent collector, we also address the metrics of energy efficiency to prolong the network lifetime and minimize data transmission delay. The rest of this paper is organized as follows: Section 2 introduces a survey of IDS in WSNs and the efficiency of our proposed IDS [4]. In section 3 we analyze and evaluate the newly data collection approaches in WSNs coupled with our proposed approach. Section 4 presents the experiment results and finally, a conclusion is presented in section 5.

2. INTRUSION DETECTION SYSTEM IN WIRELESS SENSOR NETWORK

As previously mentioned, we cannot achieve the satisfactory level of security in WSNs by merely using cryptographic techniques ,the attacker can compromise and retrieve the cryptographic material of various nodes [6], therefore, in order to counter this threat, intrusion detection system (IDS) have to be deployed. An IDS is a collection of the tools, methods, and resources which help to identify, analyze, and report intrusions [7]. Different IDS for WSN has been proposed, Krontiris et al. proposed distributed IDS for WSNs based on collaborative neighborhood watching [8], the authors evaluated the effectiveness of their IDS scheme against selective forwarding and Black hole attacks. In [9],the authors presented an IDS for WSNs based on detection of packet receive power level anomalies. The detection scheme was focused on packet arrival rates of the neighboring nodes, and the transceiver behaviors. In [4], we proposed a new architecture of IDS for WSNs. Our approach is based on mobile agent collector, as can be shown in figure 1.The system consists of four parts:

Collector Agent: Collector Agent is the first agent in the system, it collects the data from the wireless environment, and give an input to the misuse detection agent. It's a very essential phase, for efficient IDS in WSNs, because a critical issue to efficient IDS is to define and use an appropriate collector to minimize the amount of energy consumed, and maximize the lifetime of this network. We will present our mobile agent collector approach in the next section.

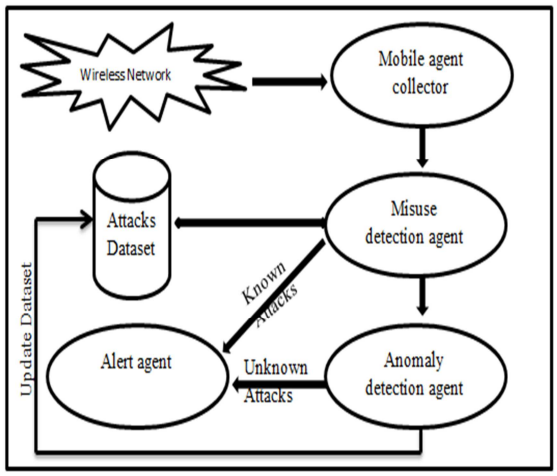

Figure 1: IDS Architecture

Misuse Detection Agent: Analyzes the audit data in search of attacks predefined scenarios in a database attack signatures, it reports to alert agent if there is a similarity between the collected packets and attack signatures in the database, if not, it routes data to the anomaly detection agent. We can say that this agent detect the known attacks in network, using misuse detection approach [10-11].

Anomaly Detection Agent: detects the unknown attacks, if the incoming data is detected as attack, it reports to alert agent about the attack, and updates the detected attack in the database. In this approach we used the Random Forest algorithm [12], which is the efficient algorithm, according to our comparative evaluation of newest anomaly detection intrusion techniques used in wireless sensor networks [12]. True positive rate, false positive rate, and the ROC curve are given as efficient metrics [12]. Furthermore, in [13] it is highly recommended to use the Random Forest technique to effectively detect intrusions and attacks in WSNs, as shown in figure 2.

Alert Agent: this agent is used to alert the system if an intrusion occurs in the network.

3. DATA COLLECTION IN WIRELESS SENSOR NETWORK

There are three principal components of IDS: Collector entity, analyzer entity, and alert entity [14].The collector entity is a very essential step, of IDS development in WSNs. The critical issue to ensure efficient IDS is to use an appropriate collector in order to extend the network lifetime by minimizing the energy consumption. Multiple approaches have been proposed for collecting data measured in the WSNs. These approaches can be classified into multipath approaches, query

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

propagation approaches, and mobile agent (MA) approaches [15]. In fact, multipath approaches focus on reliability whilst query propagation approaches provide flexibility but lack in reliability, however, the MA approaches offer both reliability and flexibility as it allows a great degree of flexibility regarding which data is collected and in what manner whilst the reliability is provided by guaranteeing a greater degree of fault-tolerance than query propagation and single-path approaches compared to multipath approaches [16]. The MAs have been found to be particularly useful in facilitating efficient data fusion and dissemination in WSNs [17].

Data-gathering approaches using MAs satisfy successfully the requirement of WSN and their resource constraints by collecting data from all the sensors in networks [18–19]. However, the use of MAs in data gathering creates the problem of the hot spot, moreover, it is of uttermost value to determine the number of MA collectors needed to be deployed to get an efficient collection, besides, the MA collector term can be referring to a mobile node surrounding the area to coverage and collecting data as it can also be considered as a packet roaming the network following a particular path, in this paper we compare both approaches, in term of energy consumption and transmission delay in a way to highlight the effective functioning of our approach.

The MA collector deployment depends mainly on the several parameters. The cost of an agent, g, visiting a node, N, following a trajectory, T, is denoted Cg(N;T). This cost is defined in terms of the agent weight, Wg(N; T), the amount of energy remaining in the sensor node, En, and the transmission delay the node, Dn, as follows:

$$Cg(N,T) = \frac{\mathrm{Wg(N,T)}}{\mathrm{En\ x\ Dn}} \qquad (1)$$

The agent weight "g". Wg(N, T), returns the weight, in bytes, of an agent g, visiting node "N", following trajectory "T". The weight of an agent is related to the size of its code and the size of the data being carried. The size of its code is fixed, whereas the size of the data varies and depends on the application in use upon visiting each node. Some applications do not require visiting each sensor node since they are densely deployed. To resolve this issue, we relax the problem by introducing a density variable "α". The density variable, "α", specifies how many nodes within the network need to be visited to explored the network. A network is considered explored if all nodes have either been visited. Note that if "α=0", the exploration problem is restored to visiting every node. For example, if the agent collect the maximum temperature (pure-aggregation) [20], the size of the data remains constant (a single temperature reading). Therefore, if the agent collects all of the temperatures (pure-collection) [20], the amount of data increases with each hop [21].

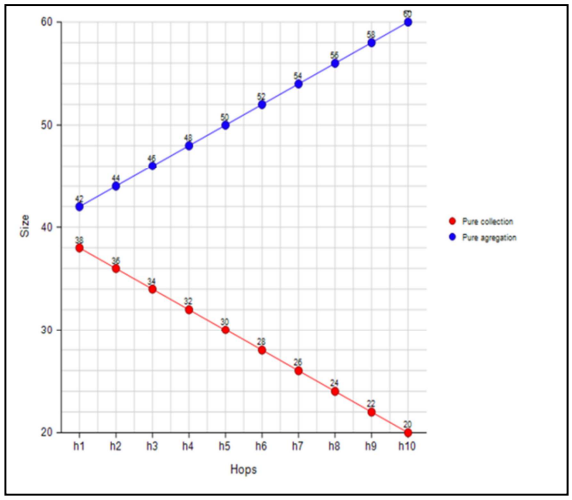

Figure2: Weight of Mobile agent collector

Figure 2 shows how the weight of an agent changes as it progresses along its path. Note that the pure-collection agent increases in size as it picks up additional sensor data values (in this case, the additional sensor data out weights the decrease in path length). The pure-aggregation agent decreases in size since the amount data remains constant, while the path length decreases. Regardless of whether the data changes, the network exploration data always decreases with each hop. This is because as it traverses its path, it can forget a portion of the path that has already been fulfilled. Finally, let T be the set of all trajectory, given a sensor network "φ", and Tn be the set of trajectory that include node n. We can formulate the following minimization problem:

$$min \sum_{N\epsilon\varphi} \sum_{t\epsilon Tn} \frac{\mathrm{Wg(N,T)}}{\mathrm{En\ x\ Dn}} \qquad (2)$$

Therefore, we need to minimize the sum of all individual node costs, where the individual cost is the quotient of all the bytes transmitted by that node, and the amount of energy the node had initially. The goal is to minimize the sum of all node costs based on an estimate of the initial energy

Journal of Theoretical and Applied Information Technology
31st May 2016. Vol.87. No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

remaining at each node, and the transmission delay of bytes transmitted by that node.

It's clear that energy consumption and data transmission delay are two major metrics to perform the used mobile agent collector in our IDS. The following section presents a simulation of our approach and a comparative evaluation with other agent collection.

4. EXPERIMENT RESULTS

As previously mentioned, the mobile agent has been widely adopted as it has proven its efficiency in terms of self-data management. Hence, data can be collected and treated instantly based on the code held by the mobile agent destined to manage data collection. The mobile agent was in first place designed to perform intelligent tasks in the networks for instance collecting a different types of data parameters when certain conditions are verified. Otherwise, the mobile agent work depends mainly to the input parameters, as the number of the parameters to be collected grows, the size code grows too and the energy needed by the transceiver to send/receive data or to proceed to data aggregation becomes important as well. The mobile agent term can be referring to a packet roaming the network to collect data following a particular path, this mobile agent packet will be retransmitted by each node within the path until it reaches the destination which will indeed consume an important amount of energy batteries for there is a correlation between the data code size and the distance towards the destination node as mentioned in [22]. On the other side, a mobile agent can also refer to a mobile node surrounding the area of coverage and collect data. Therefore, two parameters are considered in this case: energy consumption and end to end delay. We performed our simulation in Castalia simulator and the following metrics are considered: the radio initial reception mode set to "high" which stands for: 1024 for data rate (kbps), DIFFQPSK modulation type, bandwidth (MHz), sensitivity (dBm) and power consumed (mW) equal respectively to: 20,-87 and 3.1. Bypassrouting module, and BypassMac module are choosing. Dijkstra's algorithm has also been put in use to find the optimal path towards the base station passing by source nodes to gather the required data, the sensor position coordinates and the initial simulation parameters are defined respectively in table 1 and table 2.

Table 1: Sensor node initial position coordinates

	Sn1	Sn2	Sn3	Sn4
x	2	4	5	8
y	2	4	5	8
z	0	0	0	0

Table2: Simulation parameters

Simulation time	100s
Network dimension (l × L)	300 × 340
Network size	5
Bytes collected size	200 bytes
Mobile agent code size	1024 bytes
reduction factor	10 %
Aggregation energy	0.000000005
Eamp	100 pJ/bit/m2
Eelec	50 nJ/bit

Figure 3 shows the average energy consumption within WSNs when both mobile agent packet and the used approach are implemented, as can be seen, Our approach shows a better performance in terms of energy consumption as it reaches a maximum value equals to 0,080115 mJ (Sn2) versus 0,555522 mJ (Sn4) in case of mobile agent packet, this behavior is to be expected as the energy consumption model of sensor nodes depends on the data and the code size, also the distance between the sender and the receiver.

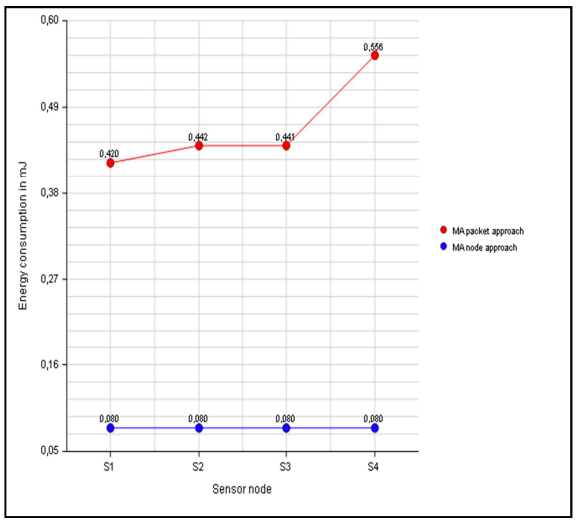

Figure 3: Energy consumption of MA collector approaches

However, the mobile agent packet size increases exponentially which contributed in a huge part to the results being found. The mobile agent packet needs to verify connectivity condition between two consecutive sensor nodes in its pre-

Journal of Theoretical and Applied Information Technology
31st May 2016. Vol.87. No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

established path otherwise it is lost in the way since there is no such forwarding mechanism taking place, however, when it comes to mobile agent node, data packets are aggregated locally meaning that the sensor node communicates the same amount of data size each time it is interrogated by the mobile agent located within its communication range, and the maximum energy consumption will be formulated in respect to the communication range length of the sensor node.

Figure 4 shows that the mobile agent packet presents an important advantage in terms of data transmission latency which is reduced to 0,13s (Sn4) compared with 8s (Sn4) in case of mobile agent node, again, this was expected as the latter roams the network with a particular speed (m/s) value in order to get to the following destination which explains the delay being presented. Based on the aforementioned results, we can obviously base our mobile agent approach choice on minimizing EPD factor (Energy × Delay) which main purpose is to give us a tradeoff balance between the energy consumption and the end to end delay.

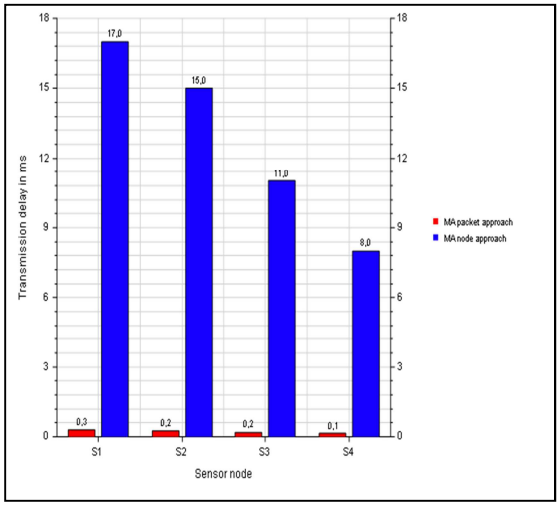

Figure 4: Data delay transmission of MA collector approaches

In order to investigate the performance of our IDS in term of the memory consumption, mobile agent code size, byte collected size, misuse detection agent size, and anomaly detection size are compared with properties of sensor node that we can use in deployment of wireless sensor network, we choose MICA2 and Telosb, as showing in the table 3 below. Knowing that MICA2 is equipped with a processor running at 7.37 MHz, 4KB of RAM, 128KB of flash memory and a radio transmitter on 433 MHz. For Telosb, is equipped with an 8 MHz clock processor, 10K RAM, 48K of program memory, and 1024K flash storage.

Table 3: Memory consumption

Name	Memory (KB)	MICA2	Telosb
Mobile agent code size	1		
Bytes collected size	0,2		
Misuse detection code size	4		
Anomaly detection code size	11,62		
Total Memory	16,82	128 KB	1024 KB

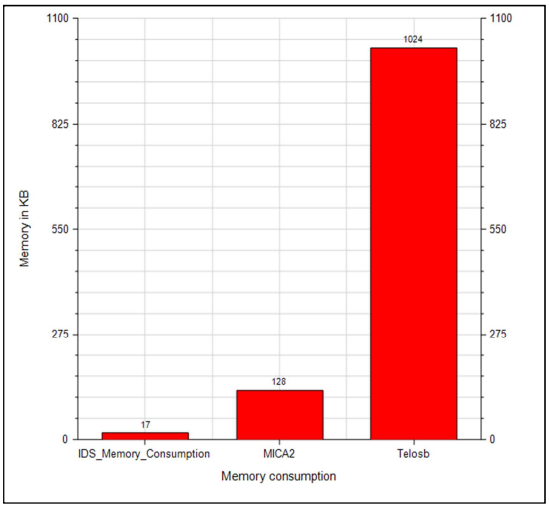

Figure5: Memory consumption

The figure below proves that the memory capacity of the sensor node, (128 KB for MICA2, 1024 KB for Telosb), is largely sufficient for deployment our IDS, which costs only 16.82 KB. This shows the feasibility of Our Intrusion detection system and the efficiency of the used mobile agent collector approach.

5. CONCLUSION

In this work, we have presented an efficient mobile agent collector approach for finding the optimal path and reducing the amount of energy consumed in the proposed IDS. Our study provides a new way to define the number of mobile agents based on data transmission delay and energy consumption, we formulate the cost of the mobile agent collector in the WSN using a minimization problem as a mathematical model. Our mobile agent collector achieves high network lifetime, minimum memory used, and minimum energy consumption than the existing approach (mobile packet collector). Therefore our IDS attains the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

more energy efficiency and achieve high network lifetime, it has a specifically positive impact in terms of the Data transmission delay, and also the amount of memory and energy consumed. While the performant functioning of our IDS, according to simulation results, the choice of the mobile agent collector approach will certainly serve several applications. Some applications will put much emphasis on the end to end delay making it though compulsory to use a mobile agent which latency does not overcome a specific threshold. Other applications priority is to maintain the network lifetime as long as possible meaning that the energy consumption is the main issue to tackle. So we can obviously base our mobile agent approach choice on minimizing EPD factor (Energy × Delay) which main purpose is to give us a tradeoff balance between the energy consumption and the end to end delay.

REFRENCES:

[1] C. S. Raghavendra, K. M. Sivalingam, and T. Znati, Wireless Sensor Networks. Springer Academic Publishers, 2004.

[2] Xiao Y, Rayi VK, Sun B, Du X, Hu F, Galloway M. A survey of key management schemes in wireless sensor networks. Comput Commun, 2007, P: 30-23,14–41.

[3] Y. Maleh, A. Ezzati, "A review of security attacks and intrusion detection schemes in wireless sensor network", International Journal of Wireless & Mobile Networks (IJWMN) Vol. 5, No. 6, December 2013.

[4] El Mourabit, Y., Toumanari, A., Bouirden, A., Zougagh, H., & Latif, R. (2014, November). Intrusion detection system in Wireless Sensor Network based on mobile agent. In Complex Systems (WCCS), IEEE, Second World Conference, 2014, pp. 248-251.

[5] K. Ota, M. Dong, X. Li, TinyBee: mobile-agent-based data gathering system in wireless sensor networks, in: Proceedings of 2009 IEEE International Conference on Networking, Architecture and Storage, 2009, pp. 24–31.

[6] Schaffer, P.,Farkas,K.,Horváth,Á.,Holczer,T.,Buttyán,L. ,2012.Secureandreliable clustering inwirelesssensornetworks:acriticalsurvey.Comput.Networks56, 2726–2741.

[7] M. Ngadi, A.H. Abdullah, and S. Mandala, "A survey on MANET intrusion detection",International J.Computer Science and Security, volume 2, number 1, 2008, pages 1-11.

[8] I. Krontiris, T. Dimitriou and F.C. Freiling, "Towards Intrusion Detection in Wireless Sensor Networks", Proc. 13th European Wireless Conference, 2007.

[9] I. Onat and A. Miri, "An Intrusion Detection System for Wireless Sensor Networks", IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, 2005.

[10] F. Haddadi, M. Sarram, Wireless intrusion detection system using a lightweight agent, in: Second International Conference on Computer and Network Technology, Bangkok, Thailand, 2010, pp. 84–87.

[11] L. Ying, Z. Yan, O. Yang-jia, The design and implementation of host-based intrusion detection system, in: Third International Symposium on Intelligent Information Technology and Security Informatics, Jinggangshan, China, 2010, pp. 595–598.

[12] Y. EL Mourabit et al , " A COMPARATIVE EVALUATION OF INTRUSION DETECTION TECHNIQUES IN WIRELESS SENSOR NETWORK", Journal of Theoretical & Applied Information Technology (jatit), vol. 76, no 1, 2015.

[13] Y. EL Mourabit et al, "Intrusion Detection Techniques in Wireless Sensor Network using Data Mining Algorithms: Comparative Evaluation Based on Attacks Detection", International Journal of Advanced Computer Science and Applications (IJACSA),Vol. 6, No. 9, 2015.

[14] DE. Boubiche et al, "CROSS LAYER INTRUSION DETECTION SYSTEM FOR WIRELESS SENSOR NETWORK", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012.

[15] B. Deb, S. Bhatnagar, and B. Nath, \Reinform: Reliable information forwarding using multiple paths in sensor networks," in IEEE International Conference on Local Computer Networks (LCN'03), 2003.

[16] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, \Highly-resilient, energy efficient multipath routing in wireless sensor networks," ACM Mobile Computing and Communications Review, 2003.

[17] H. Qi, F.Wang, "Optimal itinerary analysis for mobile agents in Ad Hoc wireless sensor networks", Proc. IEEE 2001 Int. Conf.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Communications (ICC 2001), Helsinki, Finland, 2001.

[18] M. Chen, S. Gonzalez, and V. C. Leung, "Applications and design issues for mobile agents in wireless sensor networks," IEEE Wireless Communications, vol. 14, no. 6, 2007, pp. 20-26.

[19] Y. Xu and H. Qi, "Distributed computing paradigms for collaborative signal and information processing in sensor networks," Journal of Parallel and Distributed Computing, vol. 64, no. 8, 2004, pp. 945-959.

[20] D. Massaguer, "Multi Mobile Agent Deployment in Wireless Sensor Networks", UNIVERSITY OF CALIFORNIA,IRVINE, 2005.

[21] J. Zheng and M. J. Lee, \Will IEEE 802.15.4 make ubiquitous networking a reality?: A discussion on a potential low power, low bit rate standard," IEEE Commun. Mag., vol. 42, June 2004, no. 6, June 2004.

[22] M. N. Halgamuge, M. Zukerman, K. Ramamohanarao, and H. L. Vu, "An estimation of sensor energy consumption," *Progress In Electromagnetics Research B*, Vol. 12, 2009, 259-295.