Hindawi Publishing Corporation
Journal of Sensors
Volume 2014, Article ID 938480, 15 pages
http://dx.doi.org/10.1155/2014/938480

Research Article

TDAL: Thoroughly Data Aggregation of Low Energy Devices in Secure Heterogeneous Wireless Sensor Networks

Tristan Daladier Engouang, Yun Liu, and Zhenjiang Zhang

The Key Laboratory of Communication and Information Systems, Beijing Municipal Commission of Education, Beijing Jiaotong University, Beijing 100044, China

Correspondence should be addressed to Tristan Daladier Engouang; trist_dal1@yahoo.fr

Received 21 April 2014; Accepted 13 October 2014; Published 27 November 2014

Academic Editor: Marco Grassi

The heterogeneous wireless sensor networks (HWSNs), composed of multiple types of tiny devices (sensor nodes) with wireless communication capability and suffering from computational resources constrains, enable interacting with the physical world, like never before. Innovative applications are developed for security, industrial production, monitoring, and tracking, but theoretical assumptions on these distributed data may not hold in a real scenario. In this paper, the emphasis is on accurate data and sensor nodes privacy preserving while transmitting their sensory information amongst neighbors toward the sink based on parent-child relationship in the wireless sensor network (WSN) environment, while ensuring energy saving. Data aggregation is a known energy efficient technique that is investigated through in-depth analysis of sensor communication through game theory, considering various embodiments of methods like elliptic curve cryptography for secrecy between nodes. This paper endeavors to provide new perspective for secure and energy efficient data aggregation models, where the heterogeneity of a sensor network environment makes it more complex to predict the overall network outputs.

1. Introduction

Nowadays, tiny devices of different types with wireless communication capabilities, resources, and computational constraints (sensor nodes) are deployed in the physical world from hundred to thousand forming heterogeneous wireless sensor networks (HWSNs) [1], with the aim of sensing and providing genuine and important knowledge of a specific occurrence of event needed in their specific targeted environments or surroundings despite their low communication bandwidth [2], for multiple purposes such as weather, earthquakes, and fire monitoring and also military, vehicular, and patients tracking. Data aggregation [1] is a well known energy efficient method investigated in this paper, and we aim at encompassing all aspects in network lifetime from node scarce energy resource and at securing data being exchanged between nodes communicating with each other through the wireless channel with risk of exposure to external attacks [3], considering privacy, integrity, and efficiency [4]. According to [2], a secured information exchange between different users necessitates establishing a secured collusion-free relation, which requires cooperation between nodes being synchronized.

This paper endeavored to provide a method based on an in-depth analysis from context background of the various methods cited in the references of a secure and energy efficient data aggregation in heterogeneous sensor networks as shown in Figure 1, by securing data based on elliptic curve cryptography (ECC) [4], prior to passing it over, amongst sensor nodes from source to destination, which is a method that finds its drawbacks, respectively, in Miller [5] and Koblitz [6]. After privacy preserving and data integrity, the cost in terms of energy is modeled using the game theory approach [7] involving two players with an altruism cooperation [8], which is playing a very important central role in strategic forms, highlighting prior art being previously utilized as described in literature [9, 10], and should be considered as admitted in this paper, unless otherwise statement says that this game is in a collision form. Using a game theory like in paper [2] that only considers homogeneous environment, we

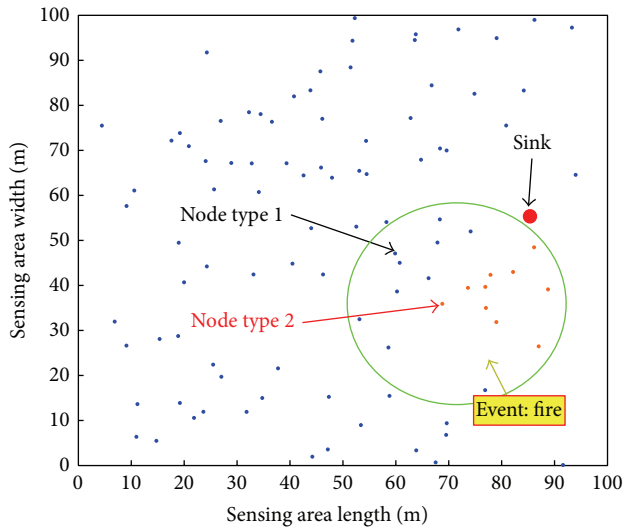

FIGURE 1: A heterogeneous secure wireless sensor network.

extend our study in a more wide and complex heterogeneous environment where each node's type and characteristics may be different from one another, whereas the ultimate aim is to minimize the energy expenses while data are securely aggregated in distributed heterogeneous wireless sensor nodes environment. The main contribution of this paper is first to provide a heterogeneous wireless sensor network data aggregation scrutiny, from each single node's communication computational details and energy cost through algorithm simulation, and, in a second aspect, using the game theory approach to emphasize the energy consumption by nodes from simple triad and compare their performance with and without heterogeneous patterns. In addition, the paper tackles both security-related and energy-related issues at the same time and proposes an efficient method for this type of hierarchically distributed sensor nodes.

The remainder of this paper is organized as follows. Section 2 presents the main objectives of the study and system model while our framework of cooperative players is formulated and emphasizes both security and energy problems. Section 3 presents the simulation results, which are discussed in Section 4, and Section 5 concludes the paper with perspectives for new research.

2. Proposed Thoroughly Aggregation Model for HWSNs

2.1. The Objectives. This paper endeavors to analyze existing secure data aggregation models such as [2, 4], hence finding problems stated and addressed in different environments such as heterogeneous wireless sensor networks (HWSNs), which is different from the homogeneous discussed in [2].

In a successful communication between sensor nodes, data are transmitted or exchanged as packets, and due to scarce energy resource, less computational approaches have been provided in the literature [11], in order to use energy efficiently, but for ensuring safety measures, additional tasks such as ciphering performance are required locally at each node level [9], and which tasks are not to be neglected as the algorithm used for that security purpose is consuming also the energy. In addition, we tackle both security- and energy-related issues considered as the most crucial at the same time, from a pair of sensors with respect to Claude Shannon's information theory perfect secrecy [2, 12], aiming at avoiding possible attacks (e.g., jamming and eavesdropping [13]) on data transmitted as packet formats on the vulnerable wireless medium, and we compare the pros and cons of each environment in terms of privacy preserving and energy efficiency, where different patterns are defined by nodes position and their types along a given path assuming a random distribution in the environment, where each is defined as a sending node, forwarding node, or receiving node. The simulation results compare the performance based on each pattern, with respect to security, reliability, and scalability and considering also their extensibility, because paths are transformed as the number of liked nodes increases and so it the energy consumption

2.2. The System Model. We consider a heterogeneous environment of two types Ψ_1 and Ψ_2 of wireless sensor nodes randomly distributed as shown in Figure 1, where their exchanges in the network resulting in multiple patterns as shown in Figure 2 are modeled as a n-players' game in which each node represents a single player with three different strategies matching their possible task such as sending, receiving, and forwarding data. We could refer to this hop-by-hop distributed network as a graph $G = (V, E)$, where the main specificities of a vertex $v \in V$ (e.g., a nonempty set of vertices or positions) are either the source or a receiver, and an edge $e = (v, u)$, with $e \in E$, the function showing a given node v, is sending data to a node u. And also the length of every path is assumed Hamiltonian [14, 15], from a given source node (i_0) sending data to a sink (i_n) as path length $\leq n$, which is a sequence of $(i_0, i_1, i_2, i_3, \ldots, i_m)$ with m as the length of the path.

In addition, because nodes are randomly distributed in the targeted environment, there exist probabilities $(0 \leq \delta \leq 1)$ having homogeneous pairs resulting from Figure 3 as shown in Figures 5, 6, 7, 9, 10, and 11, thus showing a probability $\rho = 1 - \delta$ having heterogeneous pairs of sensors. And in such communication, there exist a probability $(0 \leq \delta_1 \leq \rho)$ having a path of only homogeneous nodes of type Ψ_1 and a probability $(0 \leq \delta_2 \leq \rho)$ having a path of only homogeneous nodes of type Ψ_2, where their sum results in the probability of having only the homogeneous communication case presented in [2], discussed briefly in this paper. Consider the following:

$$\delta : \begin{cases} \delta = \delta_1 + \delta_2 = 1 - \rho = \dfrac{2}{2^3} = \dfrac{1}{4} \approx 25\%, \\ \delta_1 = \delta_2 = \dfrac{\delta}{2} = \dfrac{1}{8} \approx 12{,}5\%, \end{cases} \tag{1}$$

$$\rho = 1 - \delta = \frac{3}{4} \approx 75\%.$$

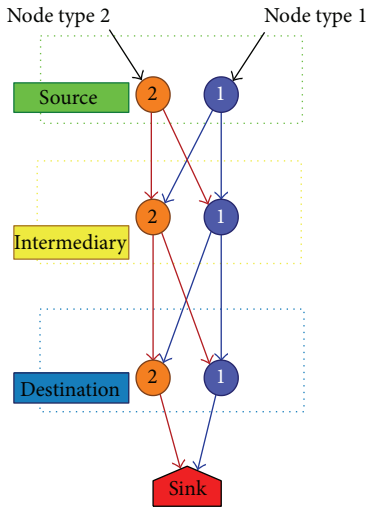

Figure 2: Network general patterns definition as source → intermediary → destination.

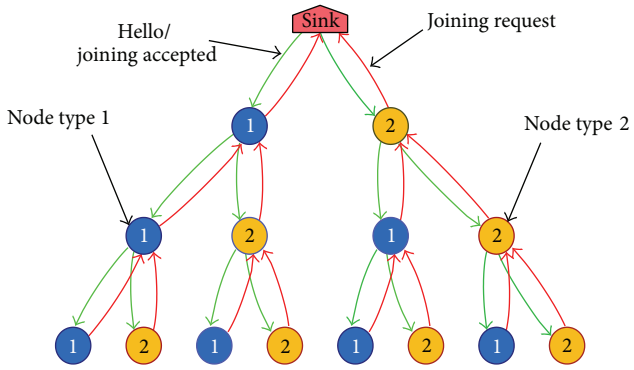

Figure 3: Final aggregation tree construction process.

Moreover, from the game theory approach, we intend to emphasize each single node involved in the aggregation process to understand the overall network, thus simulating the performance of the proposed approach. In fact, we consider the approach of a simple partitioning based on breadth first search (BFS) algorithm [16] of a graph. So for a given connected direct graph $G = (N, E)$ and a specific node r (root) in N, the breadth first search will produce a subgraph (the subgraph has the same nodes and a subset of the edges) T of G, where r is the root of the tree T, and associate a level ζ with each node k, which is the number of edges on paths from r to k in T. And this is very important because the BFS tree respects our hierarchical structure (*source* → *intermediary* → *destination*), which means that there are no edges connecting nodes in levels differing by more than 1 (due to a parent-child relationship), because all edges are between pairs of nodes in the same or adjacent levels.

In other words, a node at source level cannot connect directly with a node at final destination level; instead, it has to get through the nearest one-hop neighbouring. We mean that simply partitioning the graph into nodes at lower level

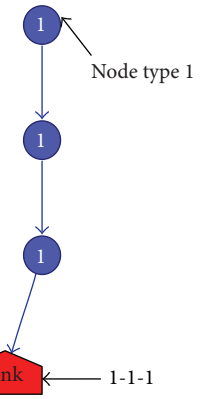

Figure 4: Patterns with node type 1 as a source 1 → 1 → 1.

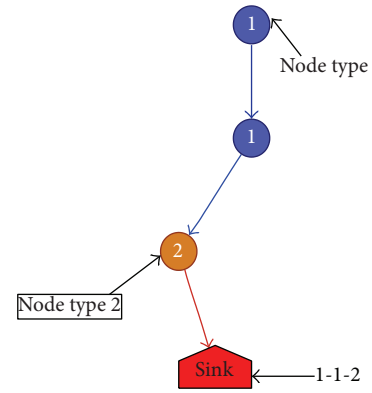

Figure 5: Patterns with node type 1 as a source 1 → 1 → 2.

noted ζ_0, and nodes at higher level, say ζ_{0+1}, assure that only adjacent level edges will be cut.

Hence, no "extra" edges' connection, say the sink (root) to the leaves of the tree (source), exists, as shown in Figure 3, where there are 8 nodes above the source level ζ_0 (leaf of tree) and 4 nodes above these assigned ζ_{0+1} forwarding nodes and the 2 nodes in level ζ_{0+1+1} destination, prior to reaching the sink.

2.2.1. Aggregation Tree Construction. Our hierarchical distributed network is supporting the heterogeneity as shown in Figure 1; we assume an aggregation tree with base station as its root where the construction goes as follows.

The root broadcasts a "*Hello*" message to all one-hop neighbor nodes, which will be replied with a "*joining_request*" message by only nodes, without parent to that "*Hello*" message' sender (e.g., root). In case of recursive "Hello" messages from different senders, the receiver will randomly select only one amongst these senders to be its parent node, "And will send it a "joining_request" message; Also after receiving this "joining_request" message, the recipient will accept the new sender of the "joining_request" message as its child," thus replying with a "*joining_accepted*" message. Figure 3 gives the final outlook of our constructed aggregate tree as in [9] and a detailed description of aggregation tree forming is found in [17].

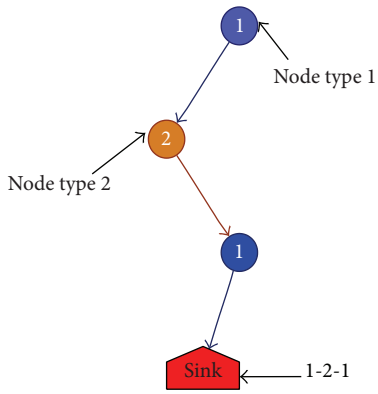

Figure 6: Patterns with node type 1 as a source 1 → 2 → 1.

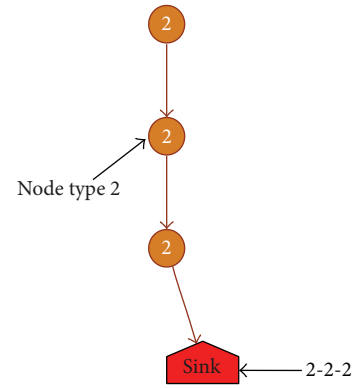

Figure 8: Patterns with node type 2 as a source 2 → 2 → 2.

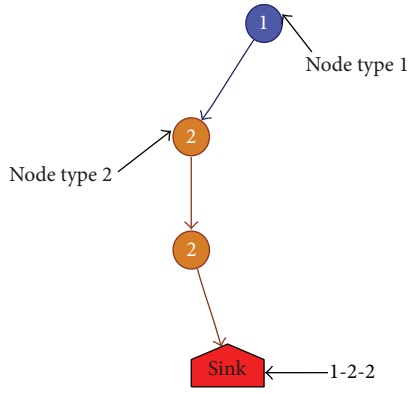

Figure 7: Patterns with node type 1 as a source 1 → 2 → 2.

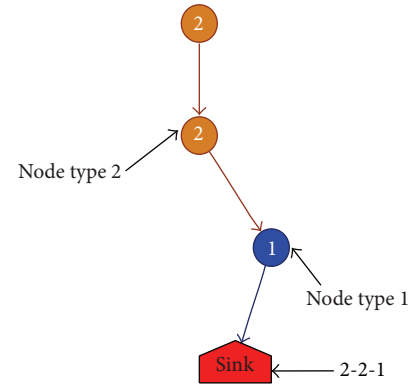

Figure 9: Patterns with node type 2 as a source 2 → 2 → 1.

Consider an edge as a direct secure link of a pair of sensors, denoted by $\mathscr{L}_{(az)}$, where a is the source vertex and z is the destination and multiple pairs links $\mathscr{L}_{out}(z) \geq 2$, yielding a cost in terms of energy which can be expressed as the sum of cost of each direct link, as given in (2).

In addition, the aggregation is processed by node receiving data on through in-going links and transmitting these to upper layer nodes on through outgoing layer and yields (2) energy cost as follows:

$$E^i = \sum_{in} \mathscr{L}_{(az)} + \sum_{out} \mathscr{L}_{(az)} + \beta_i^*, \quad (2)$$

where β_i^* is the energy cost of a given node i for securing single link of communication, which we could reformulate as in (3), with respect to the scalar multiplication in homomorphic elliptic curve cryptosystems discussed in Section 2.3. Consider the following:

$$\beta_i^* = 2\xi_i^* + 2\varphi_i^* + \varsigma_i^*, \quad (3)$$

where ξ_i^*, φ_i^*, and ς_i^* are, respectively, the cost for transmitting and receiving packets during exchange and ς_i^* is the cost for computing the sh-key.

From what precede, we could understand that the aggregation concerns all nodes, but the cost in energy consumption of each yield is differentiated by their task in the network, based on their degrees of communication. Let us denote the nodes S, I, and D as, respectively, source, intermediary, and destination because our aggregation tree admits an Euler chain, as each edge is visited only once, and the degrees of node S and V are odd, whereas degrees of I nodes are even.

2.2.2. A Sending Node (Source). Different types of nodes are randomly distributed in the sensing area forming a heterogeneous WSN. At source level of the event of occurrence, the sending node (source), prior to sending its data (readings or sensory information) in packet formats to its surrounding neighbors, will use the elliptic curve discrete logarithm function to perform the data encryption with security level $\wp$ (128 bit) and this encryption will cost ξ_i of energy, (elliptic curve discrete logarithm function has been proved to be harder to break than RSA and Diffie-Hellman [4]). In addition, the potential in-going degree (ingoing links) yield of a source node is zero, when uploading its content with throughput demand γ_i^* as defined in equation (3). Also, based on it degree of communication (outgoing links, connecting the sending node to its child node (of limited number)); we could defined the energy expenses by each type of node when

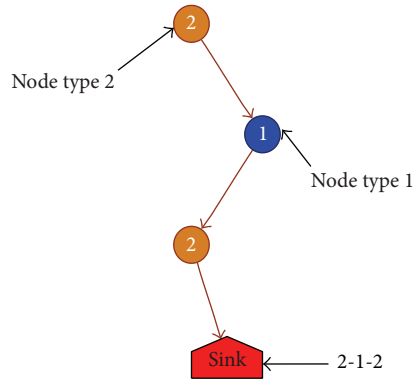

Figure 10: Patterns with node type 2 as a source 2 → 1 → 2.

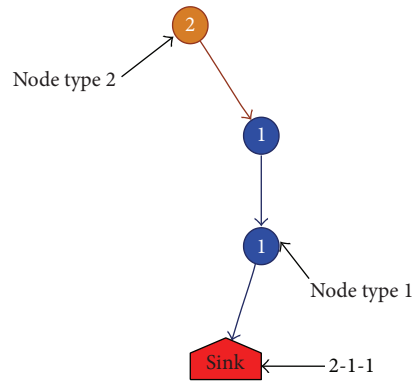

Figure 11: Patterns with node type 2 as a source 2 → 1 → 1.

transmitting data, given respectively by ξ_1 n for type 1, and by ξ_2 for type 2.

$$\gamma_i^* \begin{cases} \gamma_1 = \Theta\left(\dfrac{1}{\sqrt{N \log N}}\right) & \text{(homogeneous)} \\ \gamma_2 = \Theta\left(\dfrac{1}{\sqrt{N}}\right) & \text{(heterogeneous)}. \end{cases} \tag{4}$$

2.2.3. Receiving Node (Destination). A receiving node say j is considered as capable of storing data from neighboring sources in a single path with φ_j being the receiving data energy cost, but it has to detect incoming packets first, which cost additional α_j of energy. For simplicity, we may consider cost in both tasks as equal, along this paper. Hence because both tasks are coupled, we may denote the receiving as $2\varphi_j$.

2.2.4. Forwarding Node (Intermediary). A forwarding node, say f, is considered as an intermediary node, which has at least one in-going degree and at least one outgoing degree, thus executing both tasks of receiving first and then sending out data which it aggregates at the price of Å$_i$ energy cost of aggregation function.

This node links two adjacent edges along the path of at least 3 vertexes and is used to convey the data, which means that an intermediary node sharing the network, say an aggregator (Agg), transfers data received from its lower layer node (child) through its in-going degree to its higher layer node (parent) through its outgoing degree, for each type. An in-depth analysis focusing on this category of node is given in Section 3.2 to understand the overall HWSN system.

2.2.5. Network's Patterns. The network's patterns are defined based on parent-child relationship as the aggregate tree is formed by each pair of nodes as shown in Figure 3. We consider each type at every level of the network, as data flows from source → (through) intermediary → (to) destination, thus modeling the relation between nodes of a pair in a game of 2 players with only 3 strategies and each path from a given source to sink as Hamiltonian path [14], as data visits each node exactly once [15].

2.3. Security Parameters. This section assumes that sensor nodes' sensory information is secured for communication based on the elliptic curve cryptography method as in [4] and the data privacy preserving and integrity follows the same lines as in [4] as introduced in Sections 2.3.1, 2.3.2, 2.3.3, and 2.3.4. The scalar multiplication (kP) operation (5) is used for generating digital signature as elliptic curve discrete logarithm problem (EDLP), which we assume to have successfully solved the ECDLP, by computing operation with the aim of finding value of the scalar integer k, with the curve point P and with respect to (5). From a two nodes' communication perspective, each has the knowledge on the parameters of the ECC curve (P and Q are assumed to be prime numbers) with starting point "P" and the resulting point "Q." This emphasized the hardness to compute scalar multiplication, and thus its appropriateness for our security objectives because it will not be easy for any possible attacker to invert this type of operation. Consider the following:

$$Q = kP = \underbrace{P + P + \cdots + P}_{k \text{ times}}. \tag{5}$$

In addition, this scalar multiplication presents k as the private key to remain always secretly denoted by sk and Q as the public key to be shared denoted by pk, also for a given node, say i, with a starting point τ on the curve, substituting these values to (5) which shows that the public key pk$_i$ is generated by each sensor node as many times as a link exists between two in pairs as follows:

$$\text{pk}_i = \underbrace{\tau + \tau + \cdots + \tau}_{\text{sk}_i \text{ times}} = \text{sk}_i * \tau. \tag{6}$$

Moreover, the aggregation tree, formed with secure links between nodes in pairs as shown in Figure 12, consists of exchanging (when exchanging data, each node sends and receives from the other node it communicates with) public keys, then exchanging ciphering keys, and computing the shared secret key (sh-k) locally [2] as detailed in (7). In fact, this shared secret key establishment between nodes in pairs is the very first step prior to providing security services, say

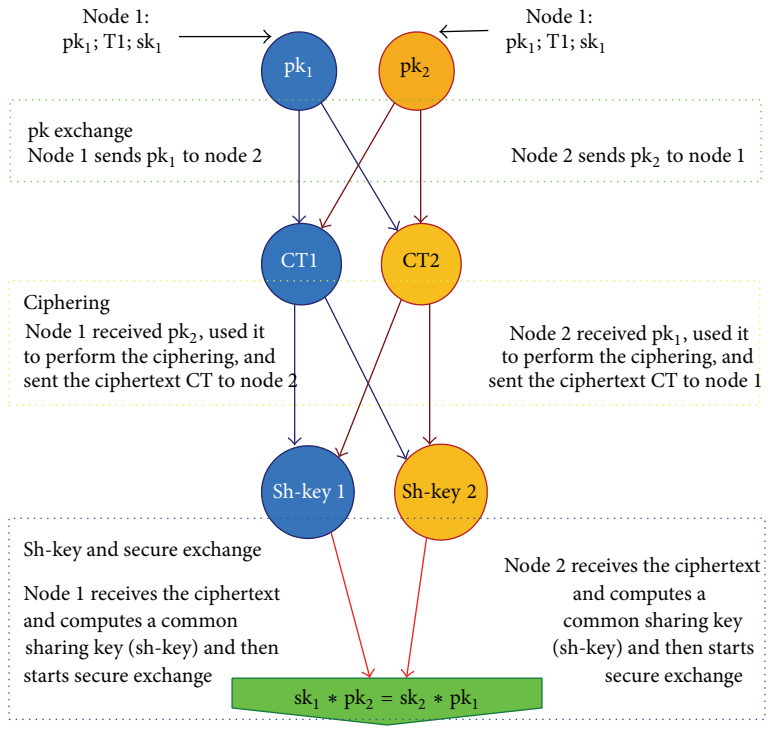

Figure 12: Secure link establishments for exchanges between nodes.

encryption in wireless sensor networks [18], and prior to normal communications. Consider the following:

$$\begin{aligned} sk_1 \times pk_2 &= sk_1 * (sk_2 * \tau) \\ &= (sk_1 * sk_2) * \tau \\ &= sk_2 * (sk_1 * \tau) \\ &= sk_2 * pk_1. \end{aligned} \tag{7}$$

Furthermore, according to [4], the following criteria introduced in Sections 2.3.1, 2.3.2, 2.3.3, and 2.3.4 must hold for an aggregation system to be secured.

2.3.1. Privacy. In this context, the sensory information is known only by the sensing node itself, which means that each node in the network should be robust enough aiming at preventing malicious nodes such as eavesdropping on the communications in order to steal private data which is a serious security breach issue. Hence data privacy preserving is a key to a successful securing data system.

2.3.2. Accuracy. This context refers to blinded nodes, which means that none of the sensor nodes knows the exact value of its neighbors, and it is one of the criteria to estimate the privacy performance.

2.3.3. Integrity. The integrity refers to an obligation of protecting the data during its aggregation process, due to crucial scrutiny at base station, for decisions making. Hence avoiding being overheard, and according to [17], the accuracy of the aggregate results depends on the scheme efficiency, which means, everyone is playing the its best response to its neighbor in the network.

2.3.4. Efficiency. The efficiency refers to lowering the communication overhead, as we highly value the scarce energy resource in WSN environment. That implies reducing efficiently the resources usage which is by contrast causing some security issues, which is why efficiency must hold the most important spotlight when it comes to finding the strategic equilibrium (e.g., Nash equilibrium) between security and energy consumption.

2.4. Energy Assessment

2.4.1. Game Theory Perspective. We emphasize the cost per task in terms of energy during the communication of nodes in our experimental heterogeneous sensor network environment; we modeled it in a game of two plays, each represented by one type of node. And because it is relaying the information by coupling both receiving and sending tasks, an intermediary node (e.g., aggregator) is a very important part of a given path as defined by the given patterns in Figures 4, 5, 6, 7, 8, 9, 10, and 11.

In this game, we consider using the Nash equilibrium denoted by NE [19]; the statement considers two players denoted by Ψ_1 and Ψ_2, with three strategies (sending, receiving, and forwarding) and all characteristics defined in Section 2.2, where costs are directly related to specific task, and with the demand throughput based on the types of nodes communicating as defined, respectively, in (3) and

(4). The altruism [8] between players cooperating to avoid data collusion is considered in this game and we assumed that the security measures completely settled as described in Section 2.3.

Definition 1 (strategy profile). A strategy profile denoted that $(s_1^*, s_2^*, \ldots, s_\lambda^*)$ is a Nash equilibrium (NE), if for each player λ the strategy's choice s_λ^* is the best response to other players' choices $s_{\lambda-1}^*$, which means that each player is playing the best response to each other player.

In addition, for the collusion-free communications, requiring cooperation between players, we say that two players cannot be sending packets at the same time and only the transmission throughput changes according to each type. Table 1 gives the n-players' game (where $n = 2$)results for a heterogeneous communication energy cost, and Table 2 gives the n-players' game results for a homogeneous communication energy cost for patterns in Figures 4 and 8.

Considering that the cost of detection is equal to the cost of receiving data ($\alpha_i = \varphi_i$), we could write $\alpha_i + \varphi_i = 2\varphi_i$. Hence from Table 2's results we can obtain the following bimatrix given by (8) in which the first and second components of the pairs represent, respectively, the pair representing player 1 and player 2's payoffs, and all rows are representing player 1 strategies and columns for player 2 strategies. And for simplicity, let us describe (8) using (9) as $m \times m$ pair of matrices T and D (T, D) as in (9), in which player 1 playing a given row i while player 2 playing row j means that player will get T_{ij} and player 2 gets D_{ij}. The complexity of this game lies in the fact that the sum of payoff $\neq 0$. Consider the following:

$$\begin{bmatrix} (\gamma_2 + \xi_1; \gamma_2 + \xi_2) & (\gamma_2 + \xi_1; 2\varphi_2) & (\gamma_2 + \xi_1; 2\varphi_2 + \gamma_2 + \xi_2) \\ (2\varphi_1; \gamma_2 + \xi_2) & (2\varphi_1; 2\varphi_2) & (2\varphi_2; 2\varphi_2 + \gamma_2 + \xi_2) \\ (2\varphi_1 + \gamma_2 + \xi_1; \gamma_2 + \xi_2) & (2\varphi_1 + \gamma_2 + \xi_1; 2\varphi_2) & (2\varphi_1 + \gamma_2 + \xi_1; 2\varphi_2 + \gamma_2 + \xi_2) \end{bmatrix}. \tag{8}$$

$$T = \begin{bmatrix} (\gamma_2 + \xi_1) & (\gamma_2 + \xi_1) & (\gamma_2 + \xi_1) \\ (2\varphi_1) & (2\varphi_1) & (2\varphi_2) \\ (2\varphi_1 + \gamma_2 + \xi_1) & (2\varphi_1 + \gamma_2 + \xi_1) & (2\varphi_1 + \gamma_2 + \xi_1) \end{bmatrix},$$

$$D = \begin{bmatrix} (\gamma_2 + \xi_2) & (2\varphi_2) & (2\varphi_2 + \gamma_2 + \xi_2) \\ (\gamma_2 + \xi_2) & (2\varphi_2) & (2\varphi_2 + \gamma_2 + \xi_2) \\ (\gamma_2 + \xi_2) & (2\varphi_2) & (2\varphi_2 + \gamma_2 + \xi_2) \end{bmatrix}. \tag{9}$$

Furthermore, there is a transmission order to each node sharing the network and using the wireless medium by pairs (hop-by-hop), where each node receives transmissions from its peers on that medium. So, when the source or sending node first transmits its data, the intermediary node which is the next in the path receives it and then forwards it over toward the sink on the network. It is obvious that data transmitted in packet forms by nodes are moving in a queue as the transmission order is being updated. To avoid possible data collision when considering our HWSN, because nodes might attempt to use the data channel simultaneously, we have to define some rules that every node of the HWSN must obey. That is why the authors of work [20] proposed to use a proper time slot to ensure the collision free transmissions, and [21] proposed the duty cycling by scattering of wake-up times. These two approaches are determining how long each node should wait to perform its task, but they are costly.

Rule 1. Two nodes of a pair cannot send data at the same time, to avoid data collusion; hence, we have the following summary (from Table 2, this means $T_{ij} \neq D_{ij}$; $i = 1$ and $j = 1$):

$$\text{Rule 1} = \begin{cases} \Psi_1 \cap \Psi_2 = (\gamma_2 + \xi_1); 0 & (\Psi_1 \text{ is sending node}) \\ \Psi_1 \cap \Psi_2 = 0; (\gamma_2 + \xi_2) & (\Psi_2 \text{ is sending node}). \end{cases} \tag{10}$$

Rule 2. Because the communication mode is on hop-by-hop perspective, any action by an intermediary node must respect Rule 1. Consider the following:

Rule 2

$$= \begin{cases} \Psi_1 \cap \Psi_2 = \{(\alpha_1 + \varphi_1) + (\gamma_2 + \xi_1)\}; (\alpha_2 + \varphi_2) \\ \qquad (\Psi_1 \text{ is forwarding node}) \\ \Psi_1 \cap \Psi_2 = (\alpha_1 + \varphi_1); \{(\alpha_2 + \varphi_2) + (\gamma_2 + \xi_2)\} \\ \qquad (\Psi_2 \text{ is forwarding node}). \end{cases} \tag{11}$$

2.5. The Framework Algorithm. Our trivial algorithm is based on simple mathematical logic, with respect to cooperation between players based on all patterns illustrated in Figures 4, 5, 6, 7, 8, 9, 10, and 11, aiming at achieving collusion-free experiences and thus system scalability and energy efficiency (see Algorithm 1).

2.5.1. Algorithm Analysis. We have modeled our unicast interaction between n-players (neighbors) with $n = 2$, by a bidirectional link $\mathscr{L} = (u, v)$, in a game that is in contrast to multicast where a cluster head shares data amongst multiple parties [22]. The algorithm considers the hop-by-hop as the many-to-many and proposes to compute each specific sensor node's energy consumption with respect to the environment specificity. In addition, the algorithm is trivial, as it is based on simple mathematical logic that considers the direct link of neighbor's role in a pair of sensors, with restrictions by Rule 1 and Rule 2, in Section 2.4.1. Hence, we could understand easily that the algorithm emphasis is on communication and that everyone has a direct impact on its in-going or outgoing link neighbor, as their tasks are related, so is their energy consumption.

In other words, we could notice that the energy efficiency of the algorithm is directly impacted by the node altruistic

Table 1: n-player game algorithm for node energy efficiency with $n = 2$.

Player 1 (Ψ_1)	Player 2 (Ψ_2)		
	Sending (S)	Receiving (R)	Forwarding (F)
S	$(\gamma_2 + \xi_1); (\gamma_2 + \xi_2)$	$(\gamma_2 + \xi_1); (\alpha_2 + \varphi_2)$	$(\gamma_2 + \xi_1); \{(\alpha_2 + \varphi_2) + (\gamma_2 + \xi_2)\}$
R	$(\alpha_1 + \varphi_1); (\gamma_2 + \xi_2)$	$(\alpha_1 + \varphi_1); (\alpha_2 + \varphi_2)$	$(\alpha_1 + \varphi_1); \{(\alpha_2 + \varphi_2) + (\gamma_2 + \xi_2)\}$
F	$\{(\alpha_1 + \varphi_1) + (\gamma_2 + \xi_1)\}; (\gamma_2 + \xi_2)$	$\{(\alpha_1 + \varphi_1) + (\gamma_2 + \xi_1)\}; (\alpha_2 + \varphi_2)$	$\{(\alpha_1 + \varphi_1) + (\gamma_2 + \xi_1)\}; \{(\alpha_2 + \varphi_2) + (\gamma_2 + \xi_2)\}$

Table 2: n-player game algorithm for node energy efficiency with $n = 2$.

Player 1 (Ψ_*)	Player 2 (Ψ_*)		
	Sending (S)	Receiving (R)	Forwarding (F)
S	$(\gamma_1 + \xi_1); (\gamma_1 + \xi_2)$	$(\gamma_1 + \xi_1); (\alpha_2 + \varphi_2)$	$(\gamma_1 + \xi_1); \{(\alpha_2 + \varphi_2) + (\gamma_1 + \xi_2)\}$
R	$(\alpha_1 + \varphi_1); (\gamma_1 + \xi_2)$	$(\alpha_1 + \varphi_1); (\alpha_2 + \varphi_2)$	$(\alpha_1 + \varphi_1); \{(\alpha_2 + \varphi_2) + (\gamma_1 + \xi_2)\}$
F	$\{(\alpha_1 + \varphi_1) + (\gamma_1 + \xi_1)\}; (\gamma_1 + \xi_2)$	$\{(\alpha_1 + \varphi_1) + (\gamma_1 + \xi_1)\}; (\alpha_2 + \varphi_2)$	$\{(\alpha_1 + \varphi_1) + (\gamma_1 + \xi_1)\}; \{(\alpha_2 + \varphi_2) + (\gamma_1 + \xi_2)\}$

cooperation because the opposite scenario could not only lead to data collusion but also to a very important waste of energy, which would make one important node of each path to run short of energy before time, also the algorithm would have failed to meet the long-time goal of the overall network lifetime. And repeating the iteration helps to get the information of the whole network, thus reaching the desired goal.

3. Discussion

This section endeavors to provide an in-depth analysis in terms of energy cost assessment from game results performed in Section 2.4, which considers our distributed HWSN and discusses the aggregation algorithm prior to describing results as the culmination of simulations that have been performed with respect to all existing patterns as shown in Figures 4, 5, 6, 7, 8, 9, 10, and 11.

3.1. Energy Cost Assessment. This section endeavors to show the residual energy levels after deducting the consumed energy from initial value and evaluates each node (Ψ_1 and Ψ_2) according to each different situation (sending, forwarding, and receiving), in order to verify if performing a single node payoff computation could also provide the information of the whole network in heterogeneous environment, like it does in homogeneous environment [13]. After considering the first scenario, shown in Figures 4 and 8, which is presenting a homogeneous path (same type of node), we have to consider the second scenario, as shown in Figures 5, 6, 7, 9, 10, and 11, presenting a heterogeneous path, which includes only different types of node. We could observe that the order of visited nodes per type makes the specificity of the pattern and the nodes interact with each other continuing to bounce between energy costs. In fact, when a connection is established, the value of energy consumption is set to β_i^* which is a default value for any new link, with respect to the fact that the connection is established once for all between two in a pair, as long as the network will last a lifetime, and the energy level is updated to

$$\mathrm{E}\Psi^*_{\mathrm{Level}} = \mathrm{E}\Psi^*_{\mathrm{initial}} - \beta_i^*. \tag{12}$$

3.1.1. Homogeneous Scenarios. The homogeneous scenario discussed in this paper concerns two patterns of types Ψ_1 and Ψ_2 as shown in Figures 4 and 8. These two homogeneous environments are relatively similar and could give the same results in case of identical characteristics. In addition, this status holds only when every two adjacent nodes are of the same type to validate the status of the path, based on parent-child relationship between pairs of nodes, according to whether two adjacent nodes of a given path are source and intermediary or intermediary and destination. The readers are referred to game results of Table 2 where costs are γ_1 related.

3.1.2. Heterogeneous Scenarios. This section involves the 6 different heterogeneous patterns as shown in Figures 5, 6, 7, 9, 10, and 11, which refers to the heterogeneous wireless sensor environment where nodes of both types are visited at least once in a given path and costs are γ_2 related. Because when communicating, a given node i is either receiving incoming data or transmitting out its own sensory information; we could summarize these patterns that remain true in both cases as follows.

(1) In a given Hamiltonian path $\mathfrak{T}_{u,v}$ an intermediary node j is either receiving data from its neighbor of the same type (homogeneous) or receiving from its neighbor of different type (heterogeneous).

(2) In a given Hamiltonian path $\mathfrak{T}_{u,v}$ an intermediary node is either transmitting data out to its neighbor of the same type (homogeneous) or transmitting data out to its neighbor of different type (heterogeneous).

3.1.3. The Sending Task Energy Expense. From the definition of the sending node in Section 2.2.2 and game results from Section 2.4.1, we could formulate the estimate sending task energy cost as follows:

$$E_s = \beta_i + \wp + \gamma_i + \xi_i. \tag{13}$$

3.1.4. The Receiving Task Energy Expense. From the definition of the receiving task in Section 2.2.3 and game results from

Input: Create a network $\Omega\{1, 2, 3, \ldots, k\}$ and define a source node i, of any type Ψ_*^i
Output: The energy consumption $E\Psi_*^i$
(1) Create a network Ω of nodes = $\{1, 2, 3, \ldots, k\}$;
(2) Choose the source node $\Psi_{u_i} \in \Omega$ as $\{i = 1, 2, 3, \ldots, k\}$; then Start a loop;
(3) Select the destination node $\Psi_v \in \Omega$ $\{v = 1, 2, 3, \ldots, k-1\}$;
(4) If the type Ψ_u and Ψ_u are heterogeneous ($\Psi_u \not\equiv \Psi_v$), then perform the n-players heterogeneous game with γ_2 and $n = 2$
(5) If the type Ψ_u and Ψ_u are homogeneous ($\Psi_u \equiv \Psi_v$,), then perform the two player's homogeneous game with γ_1;
(6) Make sure that rules 1 and rule 2 are verified as defined in Section 2.4.1;
(7) End the loop;
(8) Compute the energy consumption of the given node $E\Psi_*^i$
(9) Repeat Step (9) of game for next pair of sensors until reaching final destination,
(10) If no value changed in this iteration,
(11) Return $E\Psi_*^i$
(12) End Algorithm

Algorithm 1: n-player game algorithm for node energy efficiency with $n = 2$.

Section 2.4.1, we could formulate the estimate receiving task energy cost as follows:

$$E_R = \alpha_i + \varphi_i + \text{Å}_i + \beta_i. \tag{14}$$

3.2. In-Depth Analysis. Let us suppose that two nodes Ψ_1 and Ψ_2 are connected by an edge and that according to our flow process Ψ_1 is visited first by the algorithm. Then Ψ_2's level is at least as large as the level of Ψ_1; in other words the level of Ψ_2 can be at most one higher than the level of Ψ_1 because it will be visited as a child of Ψ_2. The arithmetic sequence of Ω terms of our network, with progressive difference of −1, helps to formulate the number of all possible pairs of nodes in (15), which does not necessarily mean that these nodes are already connected, because the communication between a given node i and its 1-hop neighbor nodes depends on ϑ their probability to be connected. Consider the following:

$$\mathcal{g} = \frac{\Omega(\Omega - 1)}{2}. \tag{15}$$

During aggregation process, data are conveyed in a given Hamiltonian path $\mathfrak{T}$ [14], of length $(1 \le \hbar \le \Omega)$, from node u to node v (sink), with positive adjacent edges, identical in both directions, where each is visited only once; thus we shall deduct one edge which is part of the Hamiltonian cycle to obtain the exact number of pairs in a given path as in (16) as follows:

$$\mathcal{g}_{\text{path}} = \left(\frac{\hbar(\hbar - 1)}{2} - 1\right). \tag{16}$$

In addition, let us recall that beside source node and destination node, our hop-by-hop based model involves also some intermediate nodes which are allowing data to be forwarded without requirement of a permanent connection between both extremities, say source and destination during communication, and the payoff of a given node i, in a pair, as in (9), depends on the relationship (e.g., parent/child and vice versa) with its neighbor in some defined hierarchy. This is indeed verified from game results in Section 2.4.1 that a player is either sending data out or receiving data; also when referring to (2), we could reformulate the energy consumption of a given pair of nodes as follows:

$$\begin{aligned} E_{\mathcal{g}} &= \rho \times \left(\left(\gamma_i + \xi_i + \beta_i + \wp\right) + \left(\alpha_i + \varphi_i + \beta_i + \text{Å}_i\right)\right) \\ &= \rho \times \left(\alpha_i + \varphi_i + \gamma_i + \xi_i + 2\beta_i + \wp + \text{Å}_i\right), \end{aligned} \tag{17}$$

where $\wp = 128$ bit security level is the cost of data encryption at source level using the elliptic curve discrete logarithm function, which has been proved to be harder to break than RSA and Diffie-Hellman [4], and Å_i is the energy cost of aggregation function at receiving node level.

Moreover, we consider that, the data is encrypted once, at source level thus for should not be encrypted again by some intermediary node, thus that cost of energy should not be deducted from (18), also knowing as said earlier that in a given Hamiltonian path $\mathfrak{T}$, of length $(1 \le \hbar \le \Omega)$, from node u to node v (sink), with positive adjacent edges, identical in both directions, we have exactly $\hbar - 2$ intermediary nodes; also we could formulate the estimate energy consumption of the TDAL approach in a single path (assumed to be for one round) considering (14) and (15) as follows:

$$\begin{aligned} E_{\text{path}} &= \left(\mathcal{g}_{\text{path}} \times E_{\mathcal{g}}\right) - \left(\wp \times (\hbar - 2)\right) \\ &= \rho \times \left(2\left(\varphi_i + \beta_i\right) + \gamma_i + \xi_i + \wp + \text{Å}_i\right) \\ &\quad \times \left(\frac{\hbar(\hbar - 1)}{2} - 1\right) - \left(\wp \times (\hbar - 2)\right). \end{aligned} \tag{18}$$

Furthermore, from what precede, when recalling all patterns defined from the aggregation tree given in Figure 3, we could formulate the energy cost of each as follows:

$$
\begin{aligned}
H_{111} &\equiv \Bigg(\left(\delta \times \left(2\varphi_1 + \text{Å}_1 \right) + \delta \times \left(\gamma_1 + \xi_1 + \wp \right) \right) \\
&\quad \times \left(\frac{\hbar \left(\hbar - 1 \right)}{2} - 1 \right) + 2\beta_1 - \left(\wp \times \left(\hbar - 2 \right) + \text{Å}_1 \right) \Bigg) \\
&\quad \times \text{Data} \\
H_{112} &\equiv \Bigg(\left(\delta \times \left(2\varphi_1 + \text{Å}_1 \right) + \rho \times \left(\gamma_2 + \xi_1 + \wp \right) \right) \\
&\quad \times \left(\frac{\hbar \left(\hbar - 1 \right)}{2} - 1 \right) + 2\beta_1 - \left(\wp \times \left(\hbar - 2 \right) + \text{Å}_1 \right) \Bigg) \\
&\quad \times \text{Data} \\
H_{121} &\equiv \Bigg(\left(\rho \times \left(2\varphi_2 + \text{Å}_2 \right) + \rho \times \left(\gamma_2 + \xi_2 + \wp \right) \right) \\
&\quad \times \left(\frac{\hbar \left(\hbar - 1 \right)}{2} - 1 \right) + 2\beta_2 - \left(\wp \times \left(\hbar - 2 \right) + \text{Å}_2 \right) \Bigg) \\
&\quad \times \text{Data} \\
H_{122} &\equiv \Bigg(\left(\delta \times \left(2\varphi_2 + \text{Å}_2 \right) + \delta \times \left(\gamma_1 + \xi_2 + \wp \right) \right) \\
&\quad \times \left(\frac{\hbar \left(\hbar - 1 \right)}{2} - 1 \right) + 2\beta_2 - \left(\wp \times \left(\hbar - 2 \right) + \text{Å}_2 \right) \Bigg) \\
&\quad \times \text{Data} \\
H_{222} &\equiv \Bigg(\left(\delta \times \left(2\varphi_2 + \text{Å}_2 \right) + \delta \times \left(\gamma_1 + \xi_2 + \wp \right) \right) \\
&\quad \times \left(\frac{\hbar \left(\hbar - 1 \right)}{2} - 1 \right) + 2\beta_2 - \left(\wp \times \left(\hbar - 2 \right) + \text{Å}_2 \right) \Bigg) \\
&\quad \times \text{Data} \\
H_{221} &\equiv \Bigg(\left(\delta \times \left(2\varphi_2 + \text{Å}_2 \right) + \delta \times \left(\gamma_2 + \xi_2 + \wp \right) \right) \\
&\quad \times \left(\frac{\hbar \left(\hbar - 1 \right)}{2} - 1 \right) + 2\beta_2 - \left(\wp \times \left(\hbar - 2 \right) + \text{Å}_2 \right) \Bigg) \\
&\quad \times \text{Data} \\
H_{212} &\equiv \Bigg(\left(\delta \times \left(2\varphi_1 + \text{Å}_1 \right) + \delta \times \left(\gamma_2 + \xi_1 + \wp \right) \right) \\
&\quad \times \left(\frac{\hbar \left(\hbar - 1 \right)}{2} - 1 \right) + 2\beta_1 - \left(\wp \times \left(\hbar - 2 \right) + \text{Å}_1 \right) \Bigg) \\
&\quad \times \text{Data} \\
H_{211} &\equiv \Bigg(\left(\delta \times \left(2\varphi_1 + \text{Å}_1 \right) + \delta \times \left(\gamma_1 + \xi_1 + \wp \right) \right) \\
&\quad \times \left(\frac{\hbar \left(\hbar - 1 \right)}{2} - 1 \right) + 2\beta_1 - \left(\wp \times \left(\hbar - 2 \right) + \text{Å}_1 \right) \Bigg) \\
&\quad \times \text{Data}. \qquad (19)
\end{aligned}
$$

3.3. Simulation and Results

3.3.1. Procedure. This section endeavors to describe the simulation procedure utilized for the calculations, with Figure 3 that illustrates the flow chart of data from each visited node, say the general patterns as described in Figures 4, 5, 6, 7, 8, 9, 10, and 11. Hence, it shows exactly how the programs work together to estimate the residual energy value (or energy level) using the plot function under simulation software MATLAB. These procedures described are repeated for each pattern amongst the Ω nodes in the initial distribution used for these calculations. Precompiled input data, initially read into the algorithm, are placed into two-dimensional matrices indexed by E-level and time. The data is normalized as a direct graph partitioning problem starting with graph $G = (N, E)$ using the parameters in Section 3.2, evaluated for total number of nodes as we aim at adjusting the value of energy consumption to a lower drift. The two types of nodes are chosen in equal amount and the procedure is repeated for all patterns and the cost in terms of energy is simulated based on (19).

3.3.2. Compilation of Simulation. According to [23], WSNs are considered as merging programming methodologies, networking, system hardware, and system software in order to enable new applications, hence having compiled all information collected from all previous sections and computed the performance measures under consideration with MATLAB R2011a on Windows 7 Ultimate 64-bit operating system using also C++ statements, which aim at great flexibility. In addition, because deploying a hierarchical network can support the heterogeneity we could define "typed" input/output that is implemented as data queues, thus performing a data processing operation on input data. Thus we could trace the energy level and time duration of each type of node which drains the computational power less aggressively according to the patterns defined in Figures 4, 5, 6, 7, 8, 9, 10, and 11. Because we set the time to be 10 s it cannot exceed this value. And we do not consider packet losses, although in a real practice deployment, this is not to be neglected with a probability $0 \leq \text{Þ} \leq 1$, where detection of lost packets is performed via a time-out mechanism or by high level of duplicates transmissions.

3.3.3. The Two Models of Sensors and Energy. This section aims at determining the energy models of these two sensors models MICAz mote [24] and the IRIS mote [25] that constitute our experimental research network, which we will use later along this paper, for the estimation and analysis of the energy efficient method studied from literature. According to [25], the running open source TinyOS from its internal flash memory of 512 Kbytes, IRIS mote, is based on the low-power 8-bit microcontroller Atmel ATMega1281 with running at a speed of 8 MHz and including an IEEE 802.15.4 compliant RF 230 transceiver 250 Kbps high data rate radio, whereas the MICAz is composed of a low-power 8-bit microcontroller Atmel ATmega128L running also the open source TinyOs from its internal flash memory of 512 Kbytes at a speed of 8 MHz and including the IEEE 802.15.4 compliant RF

Table 3: IRIS and MICAz characteristics used for compiling the simulation.

Elements	Symbols	IRIS type Ψ_1	MICAz type Ψ_2
CPU (active mode)	ς_i	96 nJ × bit^{-1}	96 nJ × bit^{-1}
RF transmit	ξ_i	156 nJ × bit^{-1}	209 nJ × bit^{-1}
RF receive/detect	φ_i/α_i	192 nJ × bit^{-1}	236 nJ × bit^{-1}
Transmit data rate	ω_i	250 kbps	250 kbps
Battery power	2 AA	21600 J	21600 J
Security key 128 bit	β_i	101376 nJ	126208 nJ

CC2420 transceiver offering a data rate of 250 Kbps and assuring a symmetric encryption using AES −128 hardware security [24]. Both IRIS and MICAz are supplied by 2xAA, nickel-cadmium (NiCd) 1000 mAh batteries attached pack, which, used in parallel, are able to supply 2A in an hour. Hence by simulating the implementation in a span time (T = 10 s) and supplying a voltage of 3 V, we could calculate the initial energy value as in (20). In addition, most ECC-based algorithm can offer great security level using smaller key size [4], thus using a 128 bit key when implementing the TDAL approach. Hence we can determine the energy cost for securing data locally at each chosen sensor level as follows in (21) and (22):

$$E\Psi^1_{\text{initial}} = E\Psi^2_{\text{initial}} = \frac{2\,\text{Ah} \times 3\,\text{V} \times 3600\,\text{s}}{h} = 21600\,\text{J}, \quad (20)$$

$$ES_1 = 128\,\text{bit} \times 792\,\text{nJ} \times \text{bit}^{-1} = 101376\,\text{nJ}, \quad (21)$$

$$ES_2 = 128\,\text{bit} \times 986\,\text{nJ} \times \text{bit}^{-1} = 126208\,\text{nJ}. \quad (22)$$

In addition, from IRIS [25] and MICAz [24], we summarize their characteristics in Table 3.

From Table 3, we can see that the main difference of the two types of nodes chosen for this heterogeneous WSN is their RF transceiver communication board characteristics. The key notation of symbols used for the compiling the simulation is shown in Notation section.

3.3.4. Simulation Settings and Results. The present study considers a WSN with 200 nodes randomly deployed in a 100 by 100 area, as shown in Figure 1, where a given node is studied while implementing the proposed TDAL approach in homogeneous and heterogeneous game theory perspective based on game results in Section 2.4.1. In addition, we gradually increased the number of nodes ħ and adopted the time span of 10 s, while data size S_{ize} = 8 bit. And the MATLAB R2011a software running under Windows 7 Ultimate 64-bit operating system using also C++ statements helped to create multiple 2-D line plot of the data in y-axis (e.g., energy consumption) versus the corresponding values in x-axis (e.g., time and data size) as follows.

(1) The homogeneous environments: the simulation of this environment is completed using the computationally slow throughput to estimate the first two homogeneous cases of Figures 4 and 8 with results shown in Figure 13.

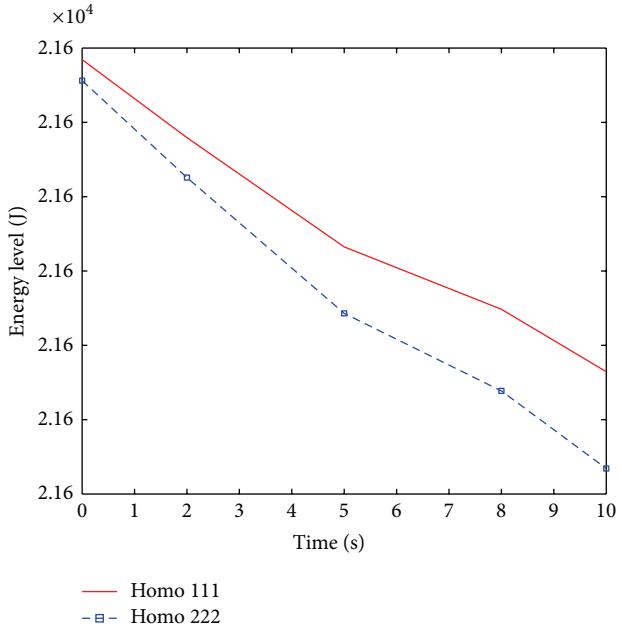

Figure 13: Energy cost per node type in homogeneous environment.

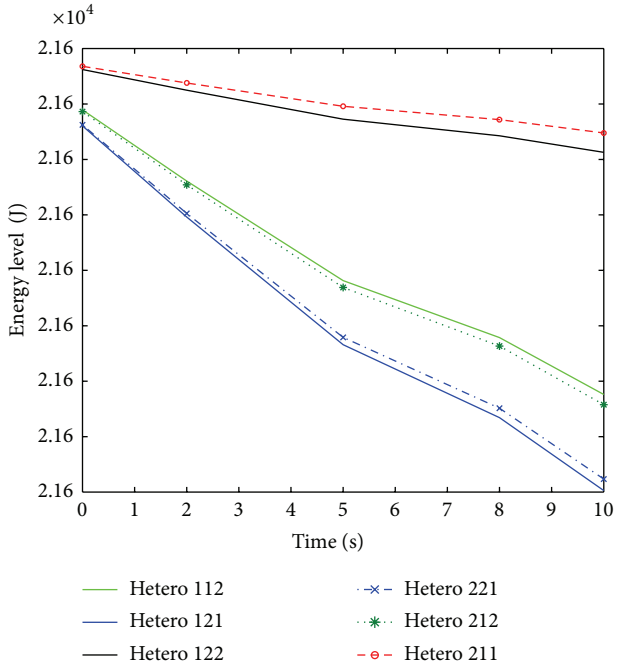

Figure 14: Energy cost per node function in heterogeneous environment.

(2) The heterogeneous environments: the simulation of this environment is completed using the computationally fast throughput γ_2 to estimate the remaining 6 patterns of Figures 5, 6, 7, 9, 10, and 11, with their energy consumption shown in Figure 14.

In addition, Figure 15 shows the energy consumption of each pattern, with node type 1 as source node, while Figure 16

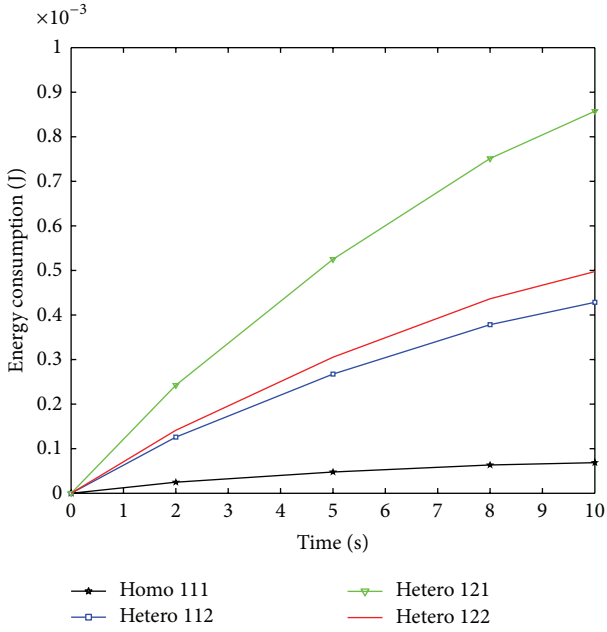

Figure 15: Energy cost with node of type 1 as source node.

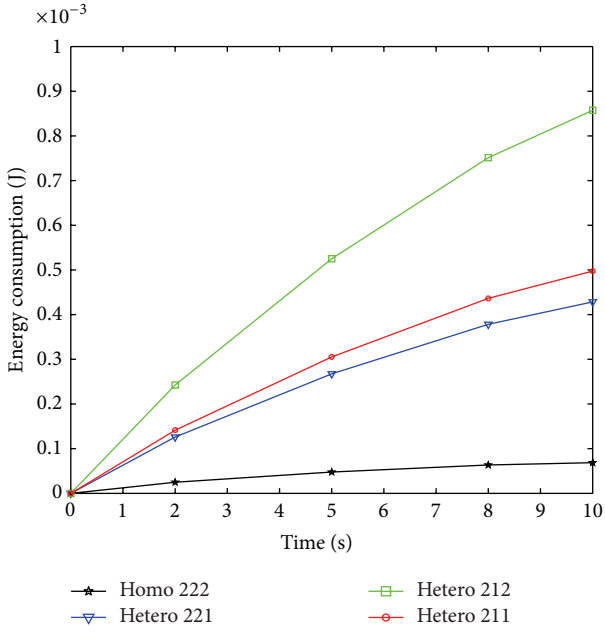

Figure 16: Energy cost with node of type 2 as source node.

shows energy consumption in patterns with node type 2 as source node. Figure 17 illustrated a global comparison of the energy consumption in all of the patterns in a time span of 10 s, where patterns Hetero 121 and Hetero 221 are almost similar, and the same observation is for patterns Hetero 112 and Hetero 212. From Figure 18, we observed that pattern hetero 1-2-2 runs short of energy few second before hetero 2-2-1, while Homo 1-1-1, lasts longer.

Furthermore, assuming a data packet size of 16 bits (e.g., temperature measurement), Figure 19 shows a global view

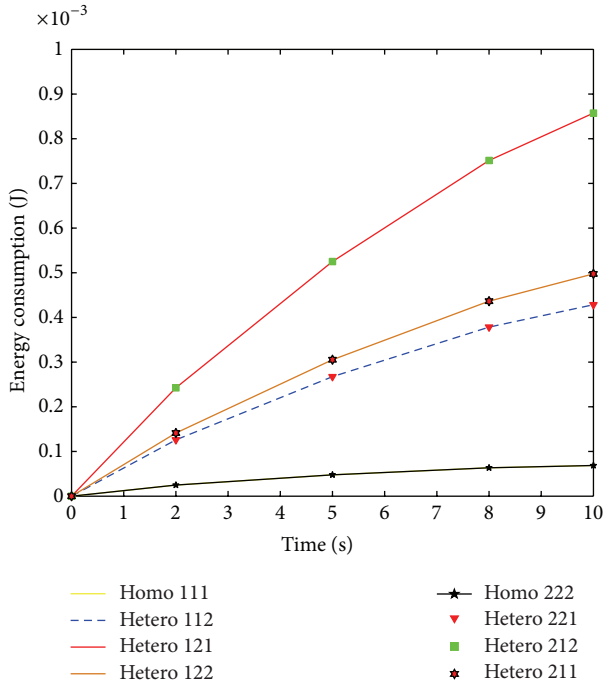

Figure 17: All patterns of energy consumption in $T = 10$ s.

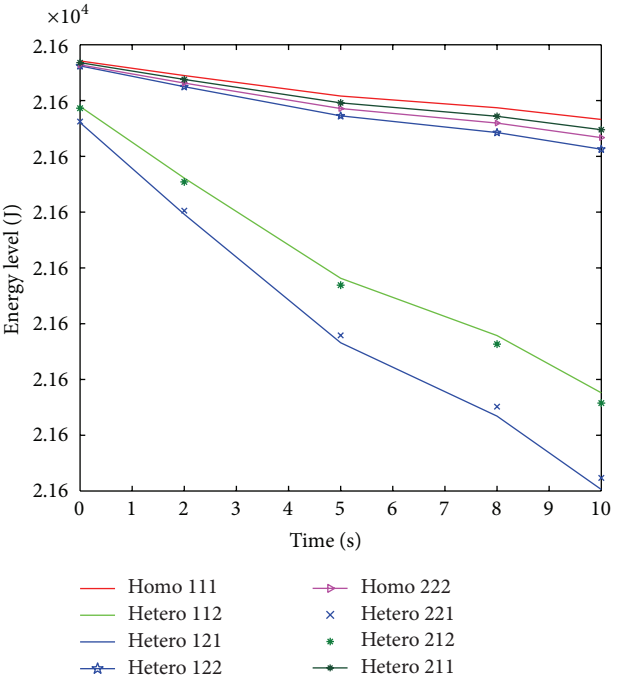

Figure 18: All patterns of energy ending in $T = 10$ s.

of the simulation of all patterns defined in the triad. The global network of 500 nodes, showing that costs from patterns hetero 1-2-1 and hetero 2-2-1 are almost the same, which is confirmed by Figure 20, shows a zooming view of all the patterns' energy consumption in which the plotted results are from 100 nodes to 130 nodes. Also we confirm that each

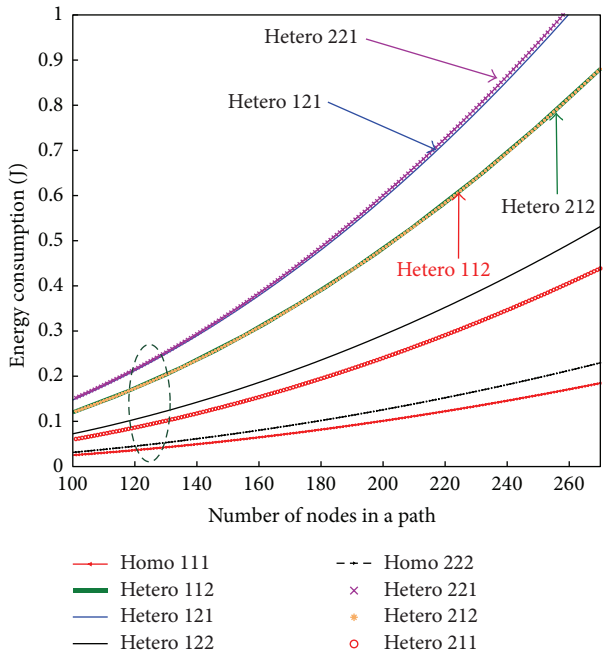

FIGURE 19: Energy consumption by intermediate nodes in each pattern based on number of nodes in a given path.

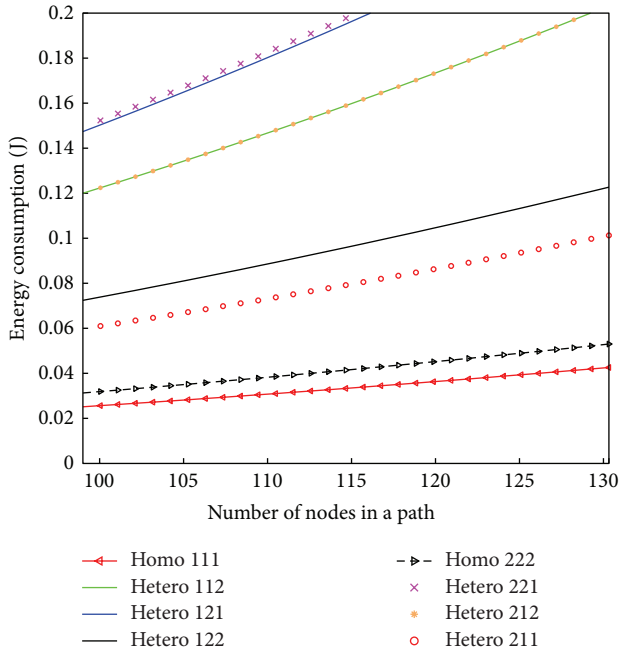

FIGURE 20: Closer look at energy consumption by pattern based on paths from 100 to 130 nodes.

given path linking the source to sink is identical in both sides. Hence, these results are accurate.

4. Related Drawback

Many recent works investigate more secure and energy efficient models in the context of wireless sensor networks, where high focus is put on the usability of cryptography, such as the elliptic curve Diffie-Hellman key exchange with authentication (the ECC-based SSL/TLS handshake) discussed in [18], in which the authors assessed the cost using energy models of the sensors based on measurements. And also the symmetric encryption using RSA is discussed [4].

As presented in 2014, the game-based secure and energy efficient data aggregation model (GABs) [2] proposes a similar game base approach to TDAL that is investigating the security aspects by modeling the cryptographic criterion of secure communications from the pairwise key establishment, but this model is limited to the homogeneous sensor nodes distributed network, which is covered by this study in Section 3.2 (e.g., Figures 4 and 8). Hence we could consider our paper as a somewhat extension of GABs due to its total inclusion.

The ESMART (energy efficient slice-mix-aggregate) [17] was proposed recently in 2013, by Li and Liu, as a novel secure data aggregation scheme for WSN which aims at addressing both energy efficiency and privacy preservation of the network using the data slicing and mixing technique, first introduced in SMART [26].

Moreover, the HEEP published in 2013, by Liu et al. [11], stands for high energy efficient and privacy preserving secure data aggregation for wireless sensor networks. And just like ESMART, HEEP is using the slicing technology that consists of slicing the raw sensory information of the sensor node into pieces, in order to achieve the preservation of data privacy in the network, where parts of the pieces are encrypted prior to being sent to the neighbor nodes, which necessitates some additional communication cost as shown in the simulation result of SMART scheme in paper [17].

In addition, because homogeneous environment discussion is included in this paper, we consider the GABs as fully discussed with extension to heterogeneous environment. Recalling ESMART and HEEP, these two methods, built on slicing techniques, lead to considering a given data of size B-bit, which means that if it is intent to be sent to, for example, k-neighbors, the sending node will slice that B-*bit* data size files into k pieces, amongst which $(k-1)$ pieces will be encrypted prior to being sent to the neighbor nodes, while the remaining piece is kept by the sending node. Because eavesdropped communication concerns the wireless link, the security aspect of this HEEP approach is related to one single piece kept by the k pieces' generator, whose piece is mandatory for any attackers to recover the original message. The TDAL model appears to be more secure than the HEEP, based on the probability of the complete secrecy ensured by homomorphism [27] of the elliptic curve used for encryption.

5. Conclusion

Wireless sensor networks' application has unlimited requirements such as topologies, size of the network, sensor types, reliability, and other resources such as energy. This endeavor provides a secure and energy efficient data aggregation in heterogeneous environment modeled using the n-player's

game theory with $n = 2$ for pairs, which highlights prior art previously utilized in others works, which we included in this paper. Studying an intermediary node, which jointly performs receiving and sending tasks, helps to appreciate the overall network performance.

The mathematical hardness of the elliptic curve cryptography approach highly secures data from forgery and hence its privacy during aggregation in the network, where cooperation between players ensures a complete secrecy. From our trivial model, the simulation results have given impressive outputs and satisfied our expectations, in terms of security and energy cost related to the intermediary nodes within a given path from a source to destination.

Future work is needed for an in-depth analysis on a disproportional distribution of nodes types and also for finding a suitable ratio for the main goal of energy efficiency based on pattern cost.

For the sake of energy saving, future work could also consider a smart pattern cost-based routing approach. With the remaining energy level a new performance metric to consider for every potential 1-hop destination node, comparing with the empirical graph shortest path or the DIJKSTRA algorithm.

Key Notation of Symbols

Ω: Network with a set $\{1, 2, 3, \ldots, k\}$
Ω_{pair}: Number of pairs of nodes
ρ: Heterogeneous path probability
ρ_1: Probability homo-path node 1
γ_1: Homogeneous link throughput
$\mathscr{L}_{uv}$: Path from u to v
T: Time 1 s
Ψ_1: Node of type 1 (node 1)
$\text{E}\Psi^1_{\text{initial}}$: Node 1 initial energy value
$\text{E}\Psi^1_{\text{Cons}}$: Node 1 energy consumption
$\text{E}\Psi^1_{\text{Level}}$: Node 1 energy level
ϖ_1: Node 1 forwarding data cost
P: Curve starting point of ECC
pk_1: Node 1 public key
sk_1: Node 1 secure key
$\text{Ct}x_1$: Node 1 ciphertext
δ: Pairing nodes probability
Ω_{path}: Number of possible patterns
$(1 - \rho)$: Homogeneous path probability
ρ_2: Probability hetero-path node 2
γ_2: Heterogeneous link throughput
$\mathscr{L}_{vu}$: Path from v to u
Δ_{size}: Data packet size {16} bits
Ψ_2: Node of type 2 (node 2)
$\text{E}\Psi^2_{\text{initial}}$: Node 2 initial energy value
$\text{E}\Psi^2_{\text{Cons}}$: Node 2 energy consumption
$\text{E}\Psi^2_{\text{Level}}$: Node 2 energy level
ϖ_2: Node 2 forwarding data cost
Q: Curve resulting point ECC
pk_2: Node 2 public key
sk_2: Node 2 secure key
$\text{Ct}x_2$: Node 2 ciphertext.

Conflict of Interests

The authors declare that the work presented in this paper has no conflict of interests.

Acknowledgments

The work presented in this paper is supported by Beijing Science and Technology Program under Grant Z121100007612003 and Beijing Natural Science Foundation under Grant 4132057. This work is also partially supported by the Agence Nationale des Bourses du Gabon (ANBG) under Grant OP 890/2014.

References

[1] S. Madden, M. J. Franklin, J. Hellerstein, and W. Hong, "TAG: a tiny aggregation service for ad-hoc sensor networks," in *Proceedings of the 5th Symposium on Operating System Design and Implementation*, Boston, Mass, USA, 2002.

[2] T. D. Engouang, L. Yun, and Z. J. Zhang, "GABs: a game-based secure and energy efficient data aggregation for wireless sensor networks," *International Journal of Distributed Sensor Networks*. In press.

[3] J. M. Bahi, C. Guyeux, and A. Makhoul, "Secure data aggregation in wireless sensor networks. Homomorphism versus watermarking approach," in *Proceedings of the 2nd International Conference on Ad Hoc Networks*, vol. 49, pp. 344–358, Victoria, Canada, 2010.

[4] T. D. Engouang and L. Yun, "Aggregate over multi-hop homomorphic encrypted data in wireless sensor networks," in *Proceedings of the 2nd International Symposium on Instrumentation and Measurement, Sensor Network and Automation*, pp. 248–252, December 2013.

[5] V. S. Miller, "Use of elliptic curves in cryptography," in *Advances in Cryptology—CRYPTO'85 Proceedings*, H. C. Williams, Ed., vol. 218 of *Lecture Notes in Computer Science*, pp. 417–426, Springer, New York, NY, USA, 1985.

[6] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987.

[7] H.-Y. Shi, W.-L. Wang, N.-M. Kwok, and S.-Y. Chen, "Game theory for wireless sensor networks: a survey," *Sensors*, vol. 12, no. 7, pp. 9055–9097, 2012.

[8] A. P. Azad, E. Altman, and R. El-Azouzi, "Routing games: from egoism to altruism," in *Proceedings of the 8th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt '10)*, pp. 528–537, Avignon, France, June 2010.

[9] T. D. Engouang, Y. Liu, and Z. J. Zhang, "Chapter 6: measurement technology, instruments and sensors, detection technologies," in *Mechatronics and Industrial Informatics II*, P. Yarlagadda and S.-B. Choi, Eds., vol. 596 of *Applied Mechanics and Materials*, pp. 519–527, 2014.

[10] M. Michalopoulou and P. Mähönen, "Game theory for wireless networking: is a Nash equilibrium always a desirable solution?" in *Proceedings of the IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC '12)*, pp. 1249–1255, September 2012.

[11] C.-X. Liu, Y. Liu, Z.-J. Zhang, and Z.-Y. Cheng, "High energy-efficient and privacy-preserving secure data aggregation for

wireless sensor networks," *International Journal of Communication Systems*, vol. 26, no. 3, pp. 380–394, 2013.

[12] E. Chui, J. Lin, B. Mcfrron, N. Petigara, and S. Seshasai, *Mathematical Theory of Claude Shannon*, 2001.

[13] Y. Mao, P. Zhu, and G. Wei, "A game theoretic model for wireless sensor networks with hidden-action attacks," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 836056, 9 pages, 2013.

[14] W. R. Hamilton, Wikipedia-Hamiltonian path, 2014, http://en.wikipedia.org/wiki/Hamiltonian_path.

[15] E. W. Weisstein, Hamiltonian Cycle, April 2013, http://mathworld.wolfram.com/HamiltonianCycle.html.

[16] J. Kleinberg and E. Tardos, *Algorithm Design*, Pearson Education, Tsinghua Univerisity Press and Prentice Hall, Beijing, China, 2006.

[17] C. Li and Y. Liu, "ESMART: energy-efficient slice-mix-aggregate for wireless sensor network," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 134509, 9 pages, 2013.

[18] G. de Meulenaer, F. Gosset, O.-X. Standaert, and O. Pereira, "On the energy cost of communication and cryptography in wireless sensor networks," in *Proceedings of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communication (WiMob '08)*, pp. 580–585, Avignon, France, October 2008.

[19] J. Huang, L. Wang, and D. Schonfeld, "Compressed-sensing game theory (CSGT): a novel polynomial complexity solution to Nash equilibria in dynamical games," in *Proceedings of the 38th IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP'13)*, pp. 6551–6555, Vancouver, Canada, May 2013.

[20] L. Hui, J. Li, H. Li, and Y. Ma, "Negotiation-based TDMA scheme for Ad Hoc networks from game Theoretical Perspective," *China Communications*, vol. 8, no. 7, pp. 66–74, 2011.

[21] A. Giusti, A. L. Murphy, and G. P. Picco, "Decentralized scattering of wake-up times in wireless sensor networks," in *Wireless Sensor Networks: 4th European Conference on Wireless Sensor Networks (EWSN '04), January 29–31, 2007, Delft, The Netherlands*, vol. 4373 of *Lecture Notes in Computer Science*, pp. 245–260, 2007.

[22] T. D. Engouang and L. Yun, "The characteristics of spread spectrum CDMA based systems and China market impacts," in *Proceedings of the 8th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM '12)*, pp. 1–8, IEEE, Shanghai, China, September 2012.

[23] T. D. Engouang, L. Yun, and Z. J. Zhang, "Pallier based homomorphic encrypted data aggregation in wireless sensor networks," *Applied Mechanics and Materials*, vol. 543–547, pp. 3017–3022, 2014.

[24] MICAZ-Memsic, memsic.com., January 2014, http://www.memsic.com/userfiles/files/Datasheets/WSN/micaz_datasheet-t.pdf.

[25] IRIS-Memsic, memsic.com, 2014, http://www.memsic.com/userfiles/files/Datasheets/WSN/IRIS_Datasheet.pdf.

[26] W. He, X. Liu, H. Viet, K. Nahrstedt, and T. Abdelzaher, "PDA: privacy-preserving data aggregation for information collection," *ACM Transactions on Sensor Networks*, vol. 8, no. 1, article 6, 2011.

[27] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proceedings of the 41st Annual ACM Symposium on Theory of Computing (STOC '09)*, pp. 169–178, Bethesda, Md, USA, 2009.