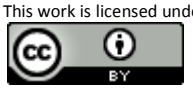
Available online at: https://ijact.in

Date of Submission	12/10/2018
Date of Acceptance	26/10/2018
Date of Publication	31/10/2018
Page numbers	2838-2842 (5 Pages)



ISSN:2320-0790

An International Journal of Advanced Computer Technology

INFORMATION CREDIBILITY MODELING IN A WSN VIA LEACH ROUTING PROTOCOL

Karim LAHMA[1], Mohamed HAMRAOUI[2]

[1]RITM Laboratory, CED Engineering Science, Hassan II University of Casablanca, Morocco
[1]karim.lahma@gmail.com
[2]RITM Laboratory, CED Engineering Science, Hassan II University of Casablanca, Morocco
[2]hamraoui@hotmail.com

Abstract: The purpose of wireless sensor networks is to transmit physical quantities from the sensor node to the base station. This requires collaboration between the various devices for proper operation. In this work, we propose a model to evaluate the credibility of information exchanged in a wireless sensor network. Indeed, the credibility evaluation of the data is done at the level of the sensor node and at the cluster head. This model has been realized in respect of the topology of the LEACH routing protocol. We also propose an improvement for LEACH routing protocol and the detection of Dead Node, based on residual energy and on the calculation of the credibility index CIN for each sensor node.

Keywords: Wireless Sensor Network, Routing Protocol, LEACH, Credibility Index of Node (CIN), Fault Tolerance.

I. INTRODUCTION

Wireless Sensor Network technology (WSN) is invading daily life, where the credibility of the information exchanged by its devices represents a main element allowing a smooth functioning of critical applications.

In many applications, WSNs operate under hostile conditions, sensor nodes are vulnerable to the risk of being damaged. This can affect data coverage and fidelity, which can lead to major degradation of sensor node operation.

Fault detection at the sensor node is designed to detect possible data faults based on various parameters. It aims to treat defects with less energy depletion. The information collected by the cluster head and / or the base station allows visibility of sensor faults at the region level, thus detecting the failure of the link between the sensor nodes and consequently increasing the quality of the sensor. In addition, the quality of the information exchanged by the WSN depends on the routing protocol used. This information is retrieved, transferred and processed by various devices. It is supposed to be credible for the proper functioning of the system. Indeed, the result contributes to decision-making in order to develop strategic objectives.

The credibility of the exchanged information reflects the treatment's quality of the various sensors. Indeed, the notion of credibility is characterized by the credibility index [1] [2] (CIN). It represents the reliability rate of information exchanged between sensor nodes. This credibility index is based on the parameters locally calculated for each sensor, those parameters are: Life Time (LT), Aberrant Value (AV), Energy Level (EL), Uncertainty (UN), Sudden Fault (SF), Noise Fault (NF) and Fault of Blocking (FB).

A rigorous approach is essential for the choice of the appropriate routing protocol for the credibility algorithm introduced in [1] [2]. The objective of this work is to propose a model to evaluate the credibility of the WSN on one hand, and on the other hand to describe the steps for evaluation the credibility of the WSN to reduce the risk of disruption to the shared information (Credibility).

II. STATE DE ART

In the literature, works that focus on the credibility of the network are limited: [3],[4]. The credibility notion is related to the life time sensor node batteries in many works. However, in practice, the links between the sensors are unreliable in the majority of cases despite having sufficient energy in the sensors. In [5], the authors proposed a mechanism for improving the reliability of submarine network sensors that benefit from multipath communications coupled with Forward Error Correction (FEC).

In paper [6], the authors applied the data fusion optimization algorithm based on the learning machine. They showed that this algorithm improves the efficiency of the merger and the overall reliability of the network. It also extends the life and reduces the energy consumption of the WSN. In [7], the authors present a model that tolerates dynamic failures in a WSN based on cascading failure (Cascading Faillure). Thanks to this model, the authors have improved the dynamic fault tolerance performance of the system.

In recent years, research has focused on routing protocols aimed at conveying the information captured to the base station, optimizing energy consumption [8] and reducing the risk of physical disturbance. This helps to prolong the life of the WSN and ensures the functioning of the entire system LEACH [9],[10], PEGASIS [11], TEEN [12].

Our approach is different from those mentioned above because we deal with both the credibility of the data exchanged within the network and the credibility of the WSN.

Figure 1 illustrates the flow of information through the WSN. We can distinguish between two cases, the case of the Mono-Skip where the information is conveyed to the Sink through a single node of sensors, and the case of Multi-Skip whose information is transferred to the sink through several sensor nodes. The Multi-skip architecture promotes the availability of information and contributes to the smooth operation of the system.

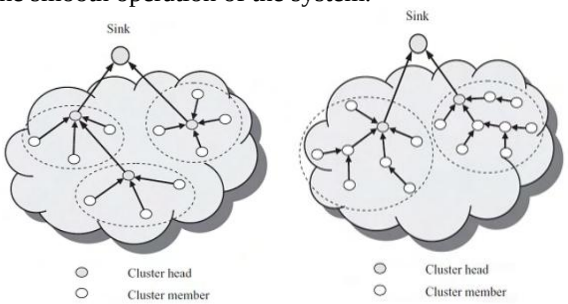


Figure 1: Architecture of a Mono-skip and Multi-skip Clustering

In this research, we are interested in the reliability of delivery of shared information at LEACH protocol level.

LEACH Protocol

In [9] [10], Heinzelman and al. proposed a distributed clustering algorithm called LEACH for routing in homogeneous sensor networks. The LEACH protocol is one of the first protocols to be proposed and studied. It consists in partitioning the network into zones and clusters in a distributed way, cluster heads nodes are constituted and then used as relays to reach the destination by optimizing the energy consumption. According to the policy of Round-Robin management, the LEACH protocol assigns randomly the cluster head role to guarantee a fair power consumption between different nodes, since the cluster-head function consumes the most energy. In order to reduce the amount of information transmitted to the base station, the cluster heads aggregate the data captured by the other nodes of the cluster and send an aggregated packet to the base station (Figure 2).

The hierarchical routing protocol is based on the dynamic partitioning of the network into a set of clusters. It must ensure optimal network operation by minimizing resource consumption in terms of energy and information delivery times. The implementation of the protocol goes through three phases of operation: a phase of announcement and creation of clusters, a phase of scheduling and a phase of transmission.

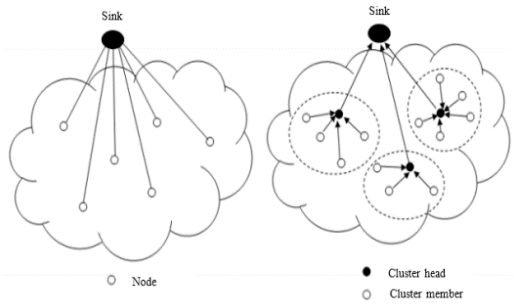


Figure 2: Illustration of the Leach Routing Protocol

III. EVALUATION MODEL OF CREDIBILITY

The authors of [15] proposed a reliability model of the WSN automatically generated from its topology, its routing algorithms as well as the battery level of each sensor constituting it. This model considers that the WSN may fail due to links or sensor nodes. The proposed models were evaluated in three scenarios. Using these scenarios, it has been possible to observe that the reliability of a particular region is affected by the adopted routing protocol, the number of nodes belonging to the region, and the distance of these regions to the receiving node.

In this work, we propose a model for evaluating the credibility of data exchanged in a WSN. We distinguish three blocks (Figure 3): Editor, Generator and Evaluator:

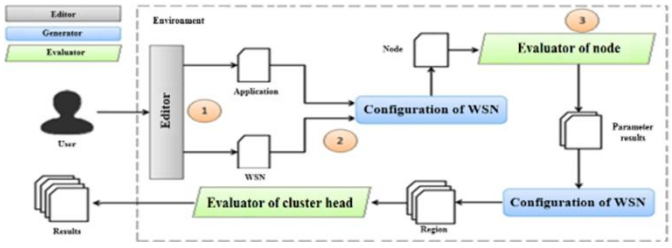


Figure 3: WSN credibility evaluation steps

The Editor: the user implements and configures the parameters of the WSN platform: application, routing protocol, degree of criticality, outlier intervals of the different physical quantities.

The Generator: the different sensor nodes self-elect to be cluster heads according to a probability of election and a percentage of selection established in advance [5% to 15%]. The cluster heads are elected as follows: each node chooses a random number between 0 and 1. If this value is less than a threshold T (i), the node becomes cluster head. The threshold is defined as follows:

$$\mathbf{T(n)}=\begin{cases}\frac{p}{1-p*rmod\ (1/p)} & if n \in G \\ 0 & else\end{cases} \quad (1)$$

Where p is the desired percentage of clusters, r is the current round and G is the set of nodes that have not yet elected cluster head on the last 1 / p rounds.

The Evaluator: the credibility evaluation runs in two steps: the credibility evaluation step at the level of sensors (Figure 4) and the credibility evaluation step of the WSN regions through the clusters heads (Figure 6).

Our approach allows verifying the credibility of the WSN, especially on the cluster head. The failure of the cluster head leads to the functioning disrupts of the whole WSN.
The loop of the credibility evaluation for each sensor node is illustrated in Fig. 4. The inputs of the system are represented by the physical quantities (Temperature, Humidity, etc.) to be measured. During the installation, the CIN algorithm is configured according to the field of use in order to calculate the different output parameters. Those are the seven parameters [1] [2] that contribute to the credibility index calculation.
The feedback loop (Figure 4) represents optimizer that allows regulating the system inputs from the desired outputs. It bases on the energy level and the value of certain pre-calculated parameters, to warn of the failure alarm in case of sensor malfunctioning. The threshold value of the energy level and those of the parameters are given during the configuration of the CIN algorithm.

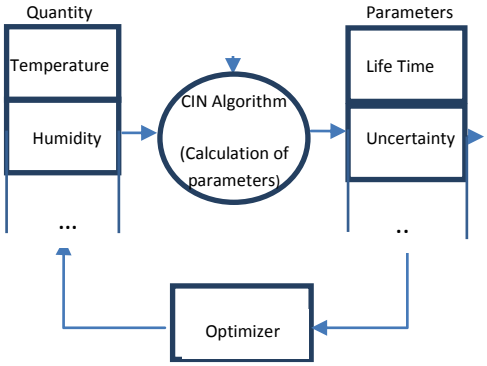


Figure 4: The node credibility evaluation model

During each iteration, the LEACH protocol performs the calculation of $E_{TX}(K, d)$ in order to collect the Dead Node. The parameter $E_{TX}(K, d)$ represents the energy dissipated by the radio module, it is calculated using the following formula (2) :

$$E_{TX}(K,d)=\begin{cases}KE_{elec}+K\varepsilon_{fs}d^2 if d<d_0 \\ KE_{elec}+K\varepsilon_{mp}d^4 \quad \text{else}\end{cases} \quad (2)$$

With: $d_0 = \sqrt{\frac{\varepsilon_{fs}}{\varepsilon_{mp}}}$

K : Number of bits per frame;

d: Distance between two sensor nodes;

E_{elec} : Energy dissipated per information transmission/reception bit;

$\varepsilon_{fs}, \varepsilon_{mp}$: Transmission amplifier parameters

The basic radio model is shown in the figure 5:

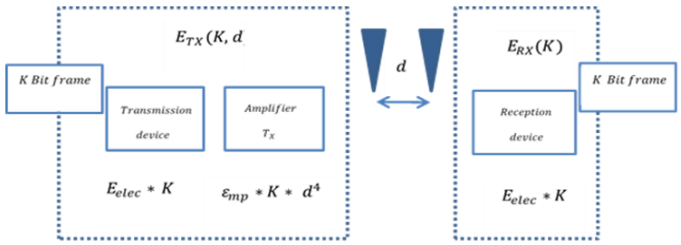


Figure 5: The model of energy dissipation by radio

Our contribution allows detecting faulty sensors by verifying only one of the following equations:

- Dissipating energy of sensor i :
  $E_{TX}(K,d) < 0$ (3)
- Residual energy of sensor i :
  $E_r(i) < E_{seuil}$ (4)
- Value of the credibility index or the level of credibility of the sensor i :
  $CIN(i) < CIN_{seuil}$ (5)

The faulty sensor giving erroneous information is excluded from information sharing.

Therefore, its users ignore it.

The evaluation loop of each cluster head is shown in the figure 6, the system inputs are the data of the frames from the different sensor nodes (Sensor 1 frame, Sensor 2 frame ...) of the region of the cluster head. Subsequently, the CIN algorithm is configured by taking into account the domain of use in order to calculate the various output parameters, the latter being the seven parameters that contribute to the calculation of the credibility index (CIN).

The optimizer (Figure 6) allows acting from the desired outputs on the inputs of the system. Obviously, this depends on the values of the credibility index as well as the residual energy of the various sensors. The threshold value of the residual energy (E_{seuil}) and the credibility index (CIN_{seuil}) are given during the configuration of the algorithm CIN.

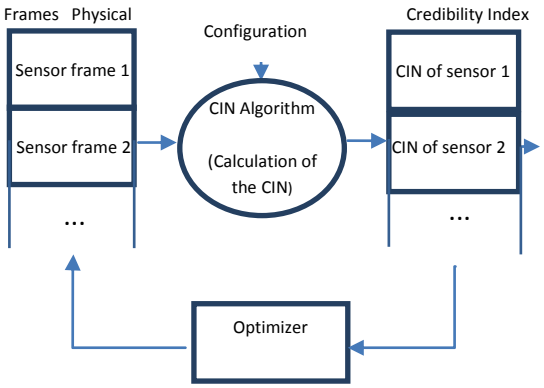


Figure 6: The cluster head credibility evaluation model

IV. SIMULATION

The table below shows the parameters of the platform of simulation used:

Parameters	Value
Simulation Area	De (0,0) à (100,100)
Base Station Location	(50,50)
Transmission Amplifier: ε_{fs}	10 nJ/bit/m2
ε_{mp}	0.0013 nJ/bit/m2
Data Aggregation Energy	5*0.000000000001
Transmission Energy : E_{TX}	50 nJ/bit
Receiving Energy : E_{RX}	50 nJ/bit

Table 1: The parameters of the platform of simulation

The probability of a fault alarm P_{FA} [16], [17], is the ratio of the number of fault alarms α_{is} generated by the sensor s for its neighbor i and the total number of packets β_{si} received by s of i.

$$P_{FA} = \frac{\sum_s \sum_i \alpha_{is}}{\sum_s \sum_i \beta_{si}}$$

The following figure shows the variation of the probability of default P_{FA} of the LEACH protocol with our LEACH-CIN algorithm as a function of time (second). It shows that LEACH-CIN is more accurate than LEACH in the interval [30s-60s].

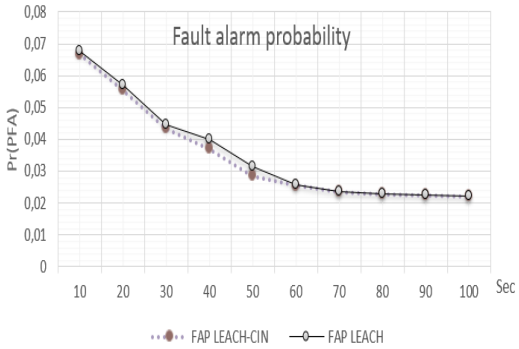


Figure 7: Variation of PFA as a function of time

The following table illustrates a performance comparison between the LEACH and LEACH-CIN protocols. We distinguish that the LEACH-CIN has an advantage at the level of the detection of fault which is done through the model of evaluation of the credibility.

Protocols	Mobility	Auto-organization	distributed	homogeneous	Fault Detection
LEACH	Yes	Yes	Yes	Yes	No
LEACH-CIN	Yes	Yes	Yes	Yes	Yes

Table 2: Comparison between protocols LEACH and LEACH-CIN performances

V. CONCUSION

This article proposes an evaluation model to evaluate, through the CIN credibility algorithm [1] [2], the credibility of the data exchanged in the WSN. This model is based on three blocks namely: the Editor, Generator and Evaluator block. They contribute to the credibility of the shared information routing protocol in the WSN through a two steps evaluations. Using the LEACH routing protocol topology, the first evaluation step is performed at the sensor node while the second operates at the cluster head. We subsequently proposed an improvement of the LEACH routing protocol to improve the choice of the Dead Node, based on the residual energy and the CIN credibility index of each sensor node.

VI. REFERENCES

[1] K.Lahma, M.Hamraoui, H.Belhadaoui. Study of the credibility of the information shared by a wireless sensor network. 2015 5th World Congress on Information and Communication Technologies (WICT), (pp. 113-116). IEEE.

[2] K.Lahma, M.Hamraoui, Evaluation de la crédibilité de l'information d'une chaine de nœuds de capteurs : RCSF. Mediterranean Telecommunications Journal, Vol. 8, N° 2, July 2018.

[3] E. Rahm and H.H. Do,Data Cleaning: Problems and Current Approaches, IEEE Data Eng. Bull., vol. 23, no. 4, pp. 3-13, Dec. 2000.

[4] E.Elnahrawy, B.Nath, Cleaning and querying noisy sensors, WSNA 03 Second ACM International Workshop on Wireless Sensor Networks and Applications, San Diego, CA, USA, Sep. 2003.

[5] M.P. Singh, Prabhat Kumar, An Efficient Forward Error Correction Scheme for Wireless Sensor Network, 2nd International Conference on Computer, Communication, Control and Information Technology (C3IT-2012) on February 25 - 26, 2012.

[6] QiumingZhang. A Reliability Optimization Algorithm for Wireless Sensor Network. International Journal of Online Engineering iJOE, Vol. 14, No. 6, 2018

[7] Yang Xiao. Dynamic Fault Tolerant Topology Control for Wireless Sensor Network Based on Node Cascading Failure. International Journal of Online Engineering iJOE, Vol. 14, No. 5, 2018.

[8] Y. Yousef, Routage pour la gestion de l'energie dans les réseaux de capteurs sans fil, Universite De Haute Alsace Faculté des Sciences et Techniques, 2010, France.

[9] Yaye M. Sarr, Réduction des clusters singletons dans le protocole LEACH pour les réseaux de capteurs sans fil, CNRIA-2015 , Sénégal.

[10] Heinzelman, W. Application-Specific Protocol Architectures for Wireless Networks. Ph.D. Thesis,Massachusetts Institute of Technology, Cambridge, MA, USA, 2000.

[11] Mohsin Raza Jafri, Nadeem Javaid, AkmalJavaid, Zahoor Ali Khan, Maximizing the Lifetime of Multichain PEGASIS using Sink Mobility, World Applied Sciences Journal 21 (9): 1283-1289, 2013.

[12] AratiManjeshwar, Agrawal and D.P., TEEN: A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks Proceedings, 15th International on Parallel and Distributed Processing Symposium, 2000.

[13] Senouci, M.R.; Melouk, A.; Senouci, H.; Aissani, A. Performance evaluation of network lifetime spatial-temporal distribution for WSN routing protocols. J. Netw. Comput. Appl. Elsevier 2012, 35, 1317–1328.

[14] Ko, Y.-B.; Choi, J.-M.; Kim, J.-H. A new directional flooding protocol for wireless sensor networks. In Information Networking. Networking Technologies for Broadband and Mobile Networks , Springer: Berlin/Heidelberg, Germany, 2004; pp. 93–102.

[15] A. Dâmaso, N. Rosa, P. Maciel, Reliability of Wireless Sensor Networks ,Sensors 2014, 14(9), 15760-15785.

[16] J.Mu-jing, Q. Zhao-wei, Efficient neighbor collaboration fault detection in WSN, The Journal of China Universities of Posts and Telecommunications, Elsevier, 118-121, 2011.

[17] H.Dhawan ,S.Waraich, A Comparative Study on LEACH Routing Protocol and its Variants in Wireless Sensor Networks: A Survey,International Journal of Computer Applications Volume 95– No.8, June 2014.

[18] K. Lahma, M. Hamraoui, H. BelhadaouI'Characterization of the information exchanged within a wireless sensor network by a credibility index',International Journal of Computer Science and Information Security, Vol. 15, No. 6, JUN 2017.