Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 52 (2015) 641 – 646

Procedia Computer Science

The 6th International Conference on Ambient Systems, Networks and Technologies (ANT 2015)

# A Distributed and Safe Weighted Clustering Algorithm for Mobile Wireless Sensor Networks

Dahane Amine*, Berrached Nasr-Eddine, Loukil Abdelhamid

*Intelligent Systems Research Laboratory, University of Sciences and Technology of Oran, Algeria*

**Abstract**

The main concern of clustering approaches for mobile Wireless Sensor Networks (WSNs) is to prolong the battery life of the individual sensors and the network lifetime. In this paper, we propose a distributed and safe weighted clustering algorithm which is an extended version of our previous algorithm (ES-WCA) for mobile WSNs using a combination of five metrics. Among these metrics lie the behavioral level metric which promotes a safe choice of a cluster head in the sense where this last one will never be a malicious node. The goals of the proposed algorithm are: detecting common routing problems and attacks in clustered WSNs, based on behavior level. The highlight of our work is summarized in a comprehensive strategy for monitoring the network, in order to detect and remove the malicious nodes. Generating a reduced number of balanced and homogeneous clusters in order to minimize the energy consumption of the entire network and prolong sensors lifetime. We implemented and tested a simulation of the proposed algorithm to demonstrate its performance.


Peer-review under responsibility of the Conference Program Chairs

*Keywords:* WSNs; Clustering; Security attacks; Malicious node; Simulation.

## 1. Introduction

After the success of theoretical research contributions in previous decade, Wireless Sensor Networks (WSNs)[1,2] have become now a reality. Their deployment in many societal, environmental and industrial applications makes them very useful in practice. These networks consist of a large number of small size nodes which sense ubiquitously

* Corresponding author: DAHANE Amine. Tel: +213(0) 698-132-193
*E-mail address:* amine_usto.info@yahoo.fr


Peer-review under responsibility of the Conference Program Chairs
doi:10.1016/j.procs.2015.05.064

some physical phenomenon (temperature, humidity, wind speed, etc.) and report the collected data to the sink station by using multi-hop wireless communications. Although, the nodes are able to self-organize and collaborate together in order to establish and maintain the network[3]. WSNs have no clear line of defense and no fixed infrastructure. There are many factors and constraints that influence the architecture of WSNs (energy consumption, fault tolerance, dynamic topology, self organization, etc.), and the most challenging factor influencing the architecture of WSNs currently is security. The clustering concept, that means grouping nodes that are close to each other, has been studied largely in Ad-hoc networks[2,4,5,6] and recently in WSNs[3,7,8] where the purpose in general is to reduce useful energy consumption and routing overhead[3]. The main idea of our algorithm to ensure the choice of a legitimate Cluster Head (CH) is to never elect a node that moves frequently even if it has the best performance metrics. So, in this paper, the ES-WCA algorithm detects the internal misbehavior nodes during distributed monitoring process in WSNs by the follow-up of the messages exchanged between the nodes. It is based on the ideas proposed by Da Silva *et al.*[9] used in his efficient and accurate "Intrusion Detection System" (IDS) in detecting different kinds of simulated attacks. We propose a distributed and safe weighted clustering algorithm for mobile WSNs using a combination of the above metrics to which we added a behavioral level metric. The latter metric is decisive and allows to the proposed clustering algorithm to avoid any malicious node in the neighborhood to become a CH, even if the remaining metrics are in its favor. The election of CHs is carrying out using weights of neighboring nodes which are computed based on selected metrics. So this strategy ensures the election of legitimate CHs with high weights.

## 2. Related Works

In this section, we outline some approaches introducing the security aspect in clustering mechanism. Elhdhili *et al.*[10] propose a Reputation Based Clustering Algorithm (RECA) that aims to elect trustworthy, stable and high energy CHs but during the election procedure, not after forming clusters. Yu *et al.*[6] try to secure the clustering mechanism against wormhole attack in Ad-hoc networks (communication between CHs). Safa *et al.*[4] propose a novel Cluster-Based Trust-aware Routing Protocol (CBTRP) for Mobile Ad-hoc networks (MANETs) to protect forwarded packets from intermediary malicious nodes. The proposed protocol ensures the passage of packets through trusted routes only by making nodes monitor the behavior of each other and update their trust tables accordingly. However, in CBTRP, all nodes monitor the network which lead rapid drainage of node energy and therefore minimize the lifetime of the network. Benahmed *et al.*[8] used clustering mechanism based on weighted computing as an efficient solution to detect misbehavior nodes during distributed monitoring process in WSNs. However, they focused only on the misbehavior of malicious nodes and not on the nature of attacks, the formed clusters are not homogeneous, the proposed Secured Distributed Clustering Algorithm (SDCA) is not coupled with routing protocols and doesn't give much importance to energy consumption. Hai *et al.*[11] propose a lightweight intrusion detection framework integrated for clustered sensor networks by using an over-hearing mechanism to reduce the sending alert packets. In the context of these surveyed research works about clustering in both Ad-hoc networks and WSNs, we classified our contribution among approaches based on the computing of the weight of each node in the network. This approach focuses around strategy of distributed resolution which enables to generate a reduced number of balanced and homogeneous clusters in order to minimize the energy consumption of the entire network and prolong sensors lifetime. With the introduction of this new metric (the behavioral level metric) which promotes a safe choice of a CH in the sense where this last one will never be a malicious node. Moreover, the highlight of our work is summarized in a comprehensive strategy for monitoring the network, in order to detect and remove the malicious nodes (see section 4). In our current work, the focus is on the misbehavior of malicious nodes and the nature of attacks. The typical attacks in WSNs include Sinkhole attack, Black Hole attack, Hello Flood attack and Node outage which are the most common network layer attacks on WSNs[11,12,13].

## 3. Metrics for CHs Election

This section introduces the different metrics used for CH election by focusing on behavior level metric. Mobility $(M_i)$, connectivity$(C_i)$, residual energy $(Er_i)$ and distance of node $n_i$ $(D_i)$ to its neighbors are cited in our previous paper[3].