International Journal of Wireless Networks and Broadband Technologies
Volume 5 • Issue 1 • January-June 2016

Safety of Mobile Wireless Sensor Networks Based on Clustering Algorithm

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

Nasr-Eddine Berrached, Intelligent Systems Research Laboratory, University of Sciences and Technology of Oran, Oran, Algeria

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

ABSTRACT

Clustering approaches for mobile wireless sensor networks (WSNs) tend to extend the battery life of the individual sensors and the network lifetime. Taking into account the mobility of the network, a powerful mechanism to safely elect a cluster head is a challenging task in many research works. As a proposed technique to deal with such problem, the approach based on the computing of the weight of each node in the network is chosen. This paper is intended to propose a new algorithm called "S-WCA" for safety of mobile sensor networks based on clustering algorithm using a combination of five metrics. Among these metrics lies 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. Moreover, a summary of the highlight of the authors' work is provided in a comprehensive strategy for monitoring the network, so as to detect and remove the malicious nodes. Simulation study is used to demonstrate the performance of the proposed algorithm.

KEYWORDS

Behavior Level, Clustering, Monitoring, Security Attacks, Wireless Sensor Networks

1. INTRODUCTION

Clustering means grouping nodes which are close to each other and has been studied largely in ad-hoc networks (Chatterjee, 2002; Choi, 2006; Zabian, 2008; Agarwal, 2012) and recently in WSNs (Dahane, 2015; Dahane, 2014; Dahane, 2015; Benahmed, 2013) where the purpose in general is to reduce useful energy consumption and routing overhead. Recent research studies recognize that organizing mobile WSNs, in the sense defined above, into clusters by using a clustering mechanism is a challenging task. This is due to the fact that cluster heads (CHs) carry out extra work, and consequently consume more energy compared with cluster members (CMs) during the network operations and this will lead to untimely death causing network partition and therefore failure in communication link. For this reason, one of the most frequently encountered problems in this mechanism is to look for the best way to elect CH for each cluster. Indeed, it is possible to select a CH by computing quality of nodes, which may depend on several metrics: connectivity degree, mobility, residual energy and distance of a node from its neighbors. Combining these metrics can achieve a significant improvement in performance of this quality. In this paper, safe weighed clustering algorithm for mobile WSNs is proposed using a combination of the above metrics with the behavioral level metric which we have added. The latter metric is decisive and allows 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

DOI: 10.4018/IJWNBT.2016010105

carried 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. In previous works (Dahane 2014; Dahane, 2015) three clustering schemes, ES-WCA, BS-WCA and HS-WCA are studied. Authors used only one Set-Up-Phase and Re-affiliation phase they tried to reduce the number of clusters formed and reorganize them in order to obtain balanced and homogeneous clusters. Moreover, using 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. As an extension of the clustering schemes proposed in (Dahane 2014; Dahane, 2015), we further improve our work on two aspects. On the one hand, we detecting common routing problems and attacks in clustered WSNs, based on behavior level. In our current work, focus is put on the misbehavior of malicious nodes and the nature of attacks.

On the other hand, maintaining stable clustering structure and offering a better performance in terms of the number of re-affiliations using the proposed algorithm S-WCA.

Furthermore, we try to Compare our algorithm with WCA (Chatterjee, 2002), DWCA (Choi, 2006) and SDCA (Benahmed, 2012) to demonstrate the effectiveness of 'S-WCA' in terms of number of equilibrate clusters, number of re-affiliations so the preliminary results obtained through simulation study prove that.

This paper is organized as follows: Section 2 provides a brief survey of related work on clustering schemes, security in WSNs. In section 3, an emphasis is put on the security problems in WSNs; Section 4 is devoted to introduce and explain the selected metrics for the proposed approach of clustering. A special attention was reserved for this last aspect in this research. More details on the proposed algorithm are provided in section 5. As concerns section 6 it is designed to present simulation results while conclusions are offered in section 7.

2. A SURVEY OF CLUSTERING SCHEMES

In this section, a review of some approaches of clustering in ad-hoc networks and WSNs is provided. A summary of all the examined algorithms is presented in Table 1. Using this table, we want to further clarify the main features of different types of clustering approaches. Furthermore, this way of presenting makes easier the comparison between various techniques. The first column specifies the algorithm name. The second column specifies the authors of the proposed approach. The other columns are devoted to the most representative grouping functions with which we can easily see the basic differences and common aspects of different approaches. The meaning of each column is explained in the following text:

Lifespan: This field specifies the metric used by the authors to evaluate the lifetime of the network. In this case, it is considered that the network will be invalid when the nodes in the neighborhood of the sink exhaust their energy.

Energy efficiency: This field indicates if the proposed algorithm guaranty energy saving in order to extend the lifespan of the network or not. Energy consumption in a sensor node can be due to either "useful" or "wasteful" sources. Useful energy consumption can be due to transmitting/ receiving data, processing query requests, and forwarding queries/data to neighboring nodes. Wasteful energy consumption can be due to Idle listening to the media, retransmitting due to packet collisions, overhearing, and generating/handling control packets.

Load balancing: This field specifies the parameters enabling to generate a reduced number of stable and balanced clusters in each scheme.

Security: This field specifies the robustness of the scheme to detect specific misbehavior in the network and, the very important thing, the type of these attacks. The metrics we used in our algorithm, Stability *(M_i),* Connectivity (C_i), Residual Energy (Er_i), Behavior Level of Node *(BL_i),* Distance between node and its neighbors ($Di_)$ are well explained in section 4.