ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A Flaw Lenient Interaction Design Behind Grave Regulatory with Wireless Sensor Networks

Mahender Reddy Bobbala
Assistant Professor,
Ramanandatirtha Engineering College,
Nalgonda.

D.Prasad
Associate Professor,
Ramanandatirtha Engineering College,
Nalgonda.

Abstract :

This paper deals with an integrated MAC and Routing protocol, able to manage faults occurring in Wireless Sensor Network (WSN). To this end, the protocol design has been inspired by the cross-layer principle to minimize both theSignaling overhead and power consumption. After an accurate functional characterization, the performance is presented for the most relevant figures (recovering efficiency and latency, as well as the length of established end-to-end paths). The satisfactory results suggest the application to more complex scenarios where the nodes mobility is allowed.

INTRODUCTION:

Wireless Sensor Networks (WSNs) have introduced a novel paradigm for reliable monitoring. They outperform conventional sensor systems, which use large, expensive macrosensors to be placed and wired accurately to an end user. In particular, WSNs may contain a great number of physically separated nodes that do not require human attention. WSNs can be deployed in almost any environment, especially those in which conventional wired sensor systems are impossible, unavailable, or inaccessible. Thus the network have to be tolerant of error and fault . For many WSN applications, data must be delivered reliably over the noisy, error-prone, and time-varying wireless channel. In addition to links also sensors are prone to fail. Faults in WSNs are not an exception and tend to occur frequently, due to energy shortage and the occurrence of denial of service attacks, i.e., the result of any action that prevents any part of a WSN from functioning correctly or in a timely manner.

As a consequence, fault tolerance is an important issue in network design in order to avoid system failures, while continuing to produce acceptable information and to deliver it to destination (survivability). A crude approach could resort to redundant deployment of sensors and replication of information between sensor nodes can be adopted to overcome some of the related problems. An alternative solution consists in providing to the whole system self- capabilities in a cooperative way: whenever a sensor dies, irst, its neighbor nodes can provide the same or similar information. The self organization feature of sensor networks provides the agility to adapt to unforeseeable situations, diverse environments, and dynamic changes. Sensors in these multi-hop networks detect events and then communicate the collected information to a central location where parameters characterizing these events are estimated.

Since the cost of transmission is higher than processing, it may be advantageous to organize the sensors into clusters. In the clustered environment, the data gathered by the sensors is communicated to the data processing center through a hierarchy of cluster heads (CHs). The processing center determines the final estimates of the parameters in question using the information communicated by the CHs. Since the sensors are now communicating data over smaller distances in the clustered environment, the energy consumption and the delivery latency can be significantly reduced. Many clustering algorithms in various contexts have been proposed [3]-[4]. These algorithms are mostly heuristic in nature and aim at generating the minimum number of clusters such that any node in any cluster is at most d hops away from its CH.

However, due to inherent complexity and need of strict time synchronization, in a critical application scenario, like the one proposed in this paper, a static clustering scheme has been adopted. In this paper, robust communications architecture, providing a fault tolerant communications support for emergency applications with WSNs, is proposed. Despite more complex solution have been proposed in the literature, the adopted approach combines effectiveness and easy implementation in real user defined scenarios as [5]. Since the main parameters to be optimized are both the message delivery and reconfiguration latencies , the investigated solution adopts a tiered architecture. In particular, a two tier topology is applied to enhance scalability and efficiency of the communications protocols.

According to it, once a cluster has been established through a set up procedure, ordinary nodes (ONs) are continuously monitored by their own CH that is also in charge of remote data delivering. Whenever a link quality degradation is detected, a warning is sent to the decision making system. If the problem still occurs due to an abnormal operative condition, the involved ONs are assumed to be definitely lost and an alarm is remotely delivered, suggesting the presence of amalicious attack1. Finally, CH is able to manage an orphanage procedure to recover ONs lacking of their original CH, which has been irreparably damaged. However, if no CH is available, a group of ONs jointly adopts a multihop routing strategy , setting up a sort of ad hoc network to reach anyway the remote server, according to a cross-layer design .The paper is organized as it follows: In Section II-A, possible application scenarios are characterized to apply the network architecture and protocols proposed, respectively, in Section II and III. Then communications performance is analyzed in Section IV, for what the standard conditions and anomalous situations are concerned. Finally, some conclusions are drawn in Section V.

II. ADOPTED NETWORK STRUCTURE:

A.Envisioned Scenario:

The purpose of the proposed network architecture is to answer for safety of areas open to the public, such as:

- places of historic and cultural relevance as old downtowns;
- seats of everyday commercial and leisure activities as parks, market square, cinemas, commercial districts, museums;
- government and administration buildings;
- transportation systems (airports, harbors, and railways stations);
- home automation.

Besides, the envisaged solution is supposed to effectively manage emergency situations occurring in the above mentioned scenarios by notifying the presence of anomalous operative conditions, while autonomously preserving the overall functioning (self healing). It has been adopted an architecture comprised of severalsensor nodes making a whole WSN connected with a remote server, in charge of data processing and adequate decisions making. It is worth noticing that, due to complexity of involved phenomena, each sensor is not able to detect a potential risk nor it could be viable to perform a distributed data fusion algorithm; as a consequence, only a centralized approach is possible. Under these hypotheses, the main parameter to be optimized is the sensed data delivering latency, as it impactson the time the remote processor need to send a warning or an alarm to the competent authorities2.

B. Network Topology:

The main aspect affecting the overall system performance is represented by the network topology, as nodes deployment is usually subject to constraints imposed by the particular phenomenon to be observed3 or by the planimetry of the area under investigation. To match the requirement of a continuous, low latency and safe monitoring, a two-tier network architecture has been adopted, interconnecting several clusters by making the CHs able to communicate each other over a wiredbus connection. In particular, the hierarchical architecture is composed of two different kind of nodes, that is the CH (Sink) and ON (Source), both connected to external electrical power supply and also endowed with additional buffer batteries to maintain the nominal functioning as long as possible. depicts the above characterized system.

c.Nodes Characterization:

A generic WSN is composed of several clusters, which are defined in the set-up phase. Every cluster is responsible for a specific geographical region.

A WSN is defined and maintained by adopting a set-up, regime and recovery phases that are further explained.

Cluster Head Node:

its main task consist in coordinating the nodes belonging to its own cluster, collecting the data samples and forwarding them to the remote server together with providing bidirectional commands (ping, node description, battery level request) and alarms. CH is endowed with two different air interfaces, acting as a gateway. It plays a crucial role in network building, maintaining and recovering and to reduce network load by adopting data fusion algorithms.Ordinary-node: an ON carries out the monitoring of a particular spatial area it is responsible for and then transmits data with a secure approach.Remote server: even though it does not make part of WSN, it has the function to storage, process and display data to the remote user in a suitable way.

III. PROPOSED RELIABLE COMMUNICATIONS PROTOCOLS:

A. Protocol Description

As previously introduced in Section II-C, there are three main operations during the overall lifetime of a WSN: set-up phase, regime phase and recovery phase. In the set-up phase ONs are associated with their own CH, by properly defining the cluster size and then making the network infrastructure ready to deliver data. As soon as a CH becomes active, it periodically broadcasts a HELLO packets with a time period THELLO . The overall setup phase duration TSetUp depends upon the number of nodes, network topology and size. The HELLO packet's header comprises at least two fields: the sender identifier ID(S) and sequence number SN.

Upon the reception of this message, an ON replies to the CH with an acknowledgment message (ACK) in unicasting modality. At the end of this phase, every CH knows of its neighbor ONs, while each ON is aware of its own CH; this information is locally stored by each node in its neighbors' table (Table-Update). If an ON receives more than one HELLO packet from different CHs4, it is associated with first CH, while keeping trace of other backup CHs.

Once the set-up phase is completed, regime phase begins ONs are able to transmit data (Data-Message) to their CHs. Addition packets are also sent to monitor the status of the bidirectional link between CH and ON (Control-Message) and to notify an abnormal behavior (Alarm). In this case the remote server generates an alarm. Both a short and long term periodical channel evaluations are delivered to the remote server together with a list of the network clusters. Moreover, each CH could allow a remote interaction with WSN by sending either a QUERY or a PING message to ONs in order to read the node's battery level or the network status. For the sake of reliability each message is acknowledged with a proper ACK packet. To provide fault tolerant communications, a recovery phase is introduced, managing situations in which a CH has been damaged. In this case, orphan ONs are associated with another CH in a direct or indirect way. The former approach needs establishing a link-to-link path (at Layer 2), while the latter requires a more complex multihop solution (at Layer 3). These solutions are described in the following.

PERFORMANCE ANALYSIS:

A.MAC Layer:

With the aim of characterizing the performance of the proposed solutions, several communications scenarios have been investigated:

- 200×200 m2 area with 1 CH;

- 400×400 m2 area with 4 geometrically deployed CHs;
- 200×800 m2 area with 4 linearly deployed CHs.

For all the before mentioned cases ONs have been uniformly distributed on the test area. The most relevant simulation parameters are summarized in TABLE I.

It could be noticed that in the first case, the performance quickly decreases from 100% to 80% as the number of ONs approaches 32-64, while in the second one it reaches 74% if the ONs are 16-32 and, finally, in the last scenario the set-up latency become 77% for the same value of nodes 6. This is due to the hidden node effect: in fact some ONs are not associated with a CH within their coverage radius because a hidden node transmission collided with its ACK messages. Nevertheless, the invisible ONs are recognized in the regime phase, since CHs are always ready to affiliate new ONs:

upon the reception of data messages from ONs, CH adds them into its MAC neighbors table. It is worth noticing that the square topology (red curve in Fig. 5) implies an addition 6% of performance loss due to ONs interfering from adjacent areas. This allows to avoid packet collision, whilst reducing the link throughput. To conclude the analysis of the MAC layer performance, the latency7 for the recovery phase as a function of the number of deployed nodes has been evaluated, for a single cluster scenario in which a backup CH has been also deployed but no multihop scheme is activated. Starting from an the initial latency value, that is not null to avoid false positives, it is a linear function of the number of deployed ONs, thus highlighting a good network scalability.

B. Network Layer:

In this case a 800×500 m2 area comprised of 4 CHs linearly distributed with a different number of uniformly distributed ONs has been taken into account. The delivering latency of data messages and the related endto- end (e2e) path length8 have been evaluated. the delivering latency has been pointed out shows the value of time-latency parameter as a function of time for different number of functioning CHs in a region of 800×800 m. It could be noticed an initial rising until a regime value is quickly approached, this meaning the completion of the recovery phase. The same behavior might be pointed out for the e2e path length. the maximum mean delivering latency has been summarized as a function of both the number of deployed ONs and available CHs. It is pointed out that the latency increasing is in inverse proportion to the number of available CHs, as e2e paths length decreases. Besides, latency is affected by the number of deployed ONs since collisions are likely to occur, while in the case of 1 or 2 available CHs latency not surprisingly decreases as it is referred to the number of ON effectively recovered, i.e., below the cluster capacity. These results summarizes the simulations carried out and could beused during the network planning to set the optimal number of ONs and CHs density to match a particular latency value.

CONCLUSION :

The WSN application is widely considered as the most promising solution for intelligent environments instrumenting, provided that effective protocols are designed taking into account specific constraints, as far as the limited resources and the unattended operations. Thus the network have to be tolerant of error and fault. This paper proposes an effective fault management scheme by introducing a recovery phase within the communications framework, in accordance to a cross-layer design. Novel MAC and Network layer protocols are accordingly proposed, aiming at facing fault by autonomously reconfiguring the network topology , without increasing the signaling overhead and reducing latency value. The proposed solution has been characterized along with its set-up, regime and recovery phase, together with validating its performance. Future developments of the present research activity might include the protocol implementation and testing over realistic user defined scenarios such as ,where a subset of nodes are allowed to dynamically change their position with a consequent air link failure.

REFERENCES :

[1] I.Akyldiz, W.Su, Y.Sankarasubramaniam, and E.Cayirci, “A survey on sensor networks,” IEEE Comm. Mag., pp. 102–114, August 2002.
[2] A.Ha´c, Wireless Sensor Networks Designs. John Wiley & Sons, 2003.
[3] A.Ruzzelli, L.Evers, S.Dulman, L.V.Hoesel, and P.Havinga, “On the design of an energy-efficient low-latency integrated protocol for distributed mobile sensors networks,” in Proc. of IWWAN 2004, 2004.
[4] A.B.McDonald and T.Znati, “A mobility based framework for adaptive clustering in wireless ad-hoc networks,” IEEE Journal on Selected Areas in Communications, vol. 17, pp. 1466–1487, August 1999.
[5] DustBot-Project, http://www.dustbot.org [May 15, 2009].
[6] Y.Yu, B.Krishnamachari, and V.Prasanna, “Energy-latency tradeoffs for data gathering in wireless sensor networks,” in Proc. of IEEE INFOCOM 2004, 2004.
[7] J.N.Al-Karaki and A.E.Kamal, “Routing techniques in wireless sensor networks: a survey,” IEEE Comm. Mag., pp. 6–28, 2004.
[8] S.Shakkottai, T.S.Rappaport, and P.C.Karlsson, “Cross-layer design for wireless networks,” IEEE Comm. Mag., October 2003.