**Distributed Faulty Node Detection in Delay Tolerant Networks Design and Analysis**

**ABSTRACT:**

Propagation of faulty data is a critical issue. In case of Delay Tolerant Networks (DTN) in particular, the rare meeting events require that nodes are efficient in propagating only correct information. For that purpose, mechanisms to rapidly identify possible faulty nodes should be developed. Distributed faulty node detection has been addressed in the literature in the context of sensor and vehicular networks, but already proposed solutions suffer from long delays in identifying and isolating nodes producing faulty data. This is unsuitable to DTNs where nodes meet only rarely. This paper proposes a fully distributed and easily implementable approach to allow each DTN node to rapidly identify whether its sensors are producing faulty data. The dynamical behavior of the proposed algorithm is approximated by some continuous-time state equations, whose equilibrium is characterized. The presence of misbehaving nodes, trying to perturb the faulty node detection process, is also taken into account. Detection and false alarm rates are estimated by comparing both theoretical and simulation results. Numerical results assess the effectiveness of the proposed solution and can be used to give guidelines for the algorithm design.

**EXISTING SYSTEM:**

* In the context of distributed estimation via consensus in a WSN, [17]–[20] have considered the simultaneous estimation of a common quantity from measurements corrupted by different levels of bias or of variance. A distributed ranking among nodes is performed according to the performance of their sensor. The proposed solution allows an identification of defective nodes with sensors producing measurements of high bias or high variance. Nevertheless, the proposed solution highly relies on the measurement models and on the communication conditions.
* A problem related to DFD in DTNs has been considered in [21] in the context of VDTN. A large number of sensor nodes are fixed and some vehicles, called mobile carriers (MC) collect data from these sensors. The sensor nodes can only communicate with the MCs in their vicinity. A MC needs to collect enough measurements to perform a test to decide which have been produced by defective sensors. Once a node is deemed defective by a MC, it is added to its blacklist. The MC provides information to sensors about their status. MCs also exchange their blacklists to accelerate the faulty node detection.
* A collaborative approach is proposed in [23], where each node can detect whether the encountered node is selfish using a local watchdog. The detection result is disseminated over the network to increase the detection precision and to reduce the delay. Trust/Reputation management is another important aspect to help DTNs to resist various potential threats. For example, [24] provides an iterative trust management mechanism to fight against Byzantine attacks in which several nodes are totally controlled by the adversary.
* In [25], a defense against Sybil attacks [26] is introduced, which is based on the physical feature of the wireless propagation channel. A trust model in the scenario of underwater acoustic sensor networks is presented in [27] to take into account several trust metrics such as link trust, data trust, and node trust.

**Disadvantages**

* There is no Accurate Fault Node detection due to absence of Local outlier detection test techniques.
* More Packet Drops

**PROPOSED SYSTEM:**

* In the proposed system, differently from previous works in the field, we consider that in a distributed way each node performs a self-determination on whether its sensors are producing outliers in the context of DTNs. In this case, new issues arise, mainly related to the limited proximity time of DTN nodes and the sporadic contacts which call for the consideration of the history of contacts in the identification process. Also, the system provides a mathematical characterization of the problem and proves the convergence of the algorithm.
* The proposed system also considers the problem of distributed faulty node detection (DFD) in DTNs. A node is considered as faulty when one of its sensors frequently reports erroneous measurements. The identification of such faulty nodes is very important to save communication resources and to prevent erroneous measurements polluting estimates provided by the DTN. This identification problem is quite complicated in DTNs when interactions are mainly between pairs of encountering nodes. Most of the classical DFD algorithms are using measurements of spatially-correlated physical quantities collected by many nodes to determine the presence of outliers and identify the nodes producing these outliers.

**Advantages**

* Fully distributed and easily implementable algorithm to allow each node of a DTN to determine whether its own sensors are defective.
* Local Outlier Detection Test (LODT) is assumed to be able to detect the presence of outliers in a set of measurements, without necessarily being able to determine which the outliers are.

**SYSTEM SPECIFICATION**

**Hardware Requirements:**

* System : Pentium IV 3.5 GHz.
* Hard Disk : 40 GB.
* Monitor : 14’ Colour Monitor.
* Mouse : Optical Mouse.
* Ram : 1 GB.

**Software Requirements:**

* Operating system : Windows XP or Windows 7, Windows 8.
* Coding Language : Java – AWT,Swings,Networking
* Data Base : My Sql / MS Access.
* Documentation : MS Office
* IDE : Eclipse Galileo
* Development Kit : JDK 1.6