Light-weight Sensor Network Monitoring Using Asynchronous Protocol Events

Yi-Hsuan Chiang
Graduate Institute of Communication Engineering, Taiwan University, Taiwan
junctionQQ@gmail.com

Abstract
As the application of wireless sensor networks (WSNs) for long-term monitoring purposes becomes real, the issue of WSN system health monitoring grows increasingly important. Since those deployments are often situated at locations with poor accessibility and left unattended, an automated operation support is required for enabling the efficient system operation. The more amount of ongoing system data can be collected through the network, the more level of detail in which state can be inferred from this data. However, WSNs are more restrictive with respect to additional monitoring traffic. The goal is to minimize the introduced traffic overhead by using an asynchronous, event-based transmission scheme while still being able to isolate possible root causes in the network. This paper presents a light-weight health monitoring system that consists of an event logging mechanisms that runs on sensor nodes as well as an algorithmic framework that analyzes received information after data has been received at the sink.

1 Thesis Statement
Recent research efforts have led to WSNs being deployable long-term at scale. As a consequence of this success, the number of people who actively rely on those networks applied to various domains is also growing. Especially for those applications remotely deployed targeting on harsh climate/environmental monitoring [1], or wildlife habitat tracking [4], the long-term sustainability of WSN is a suitable way to reduce the need for labor-intensive field trips. However, the systems unavoidably experience the uncontrollable impacts from hardware, software and the surrounding environment. If all observed anomalies need manually troubleshooting or human intervention to find the root causes, human efforts would turn out to be the highest maintenance costs.

Moving towards more serious applications will require system health monitoring support that enables network operators to solve problems timely and efficiently. Often knowledge of prior states feeding back from nodes within the network is necessary for understanding the potential risk on the system performance. A fundamental concern lies in the amount of extra computation and traffic overhead that can be injected into a low-power, resource-constrained WSN. The global behavior can be reconstructed from individual states of distributed nodes. Motivated by the observation that it is internal state transitions instead of state itself that sufficient to reveal important messages of system operation. By transmitting those protocol transitions asynchronously (comparing to periodical application data traffic), the amount of transferred information is kept as low as possible. The goal of this thesis is to benefit from those asynchronous event to extract vital signs for run-time system health assessment and possible root causes isolation.

2 Related Works
Initial deployment experiences [16] motivated many researchers to tackle the problem of achieving the reliable operation of WSNs, e.g., by instrumenting codes such as using high-level programming abstractions [11], or by developing Testbeds, simulators [7] and debugging tools [15]. In order not to interfere the debugged application, some also add extra passive sniffers [13]. Extensive analysis capabilities are created when those sniffers are used in combination with a scheme adding messages based on programmatically defined assertions on the network state [14].

Other methods operating on different design points of the trade-off between the achievable diagnosis granularity and the introduced overhead have been proposed. An traffic overhead of up to 31% is introduced by Sympathy [12], a system that collects several metrics for network debugging outside the network. Liu et al. [9] proposed the usage of belief networks for inferring the root causes of an observed behaviour. While only an insignificant traffic overhead is introduced by the path marking scheme used, this system is not able to narrow down the root causes of an observed behaviour with a high confidence. TinyD2 [8] and LD2 [10] are two novel systems that infer local system health inside the network. While those approaches require sensor nodes to solve computationally complex tasks, e.g., to achieve a local consensus, less traffic overhead is introduced given problems are already detected inside very large networks.
3 Methodology Approach

The proposed Light-weight Sensor Network Monitoring (LSNM), a health monitoring system that infers the performance of a WSN from asynchronously transmitted event logs. It is adopted to Matterhorn deployment of PermaSense project [5] which is situated in the hardly accessible high-Alpine area above 4,000 m sea level collecting data for environmental science. This three-tiered architecture consists of a sink, a back-end, and sensor nodes running a tree-based data gathering protocol, Dozer [2].

1) Event Logging Mechanism, implemented on each sensor node, and 2) LSNM Engine running at the back-end in charge of system diagnosis, implemented on each sensor node, and 2) LSNM Engine, running at the back-end in charge of system diagnosis are two major components in LSNM, as shown in Figure 1.

Integrating the event logging mechanism into the protocol stack allows to extract protocol state at the level of a debugger. Only important state transitions, i.e., protocol events, are recorded and eventually transmitted over the radio. Each detected event is stored in the event queue once occurred, the type of the detected event, and an associated numeric argument. A dedicated type of LSNM packet is generated either when a fixed detected event is stored in the event queue once occurred and is represented by an event log item that has three properties, namely the time of event occurrence, the type of the detected event, and an associated numeric argument. A dedicated type of LSNM packet is generated either when a fixed event log item is received in the event queue of the node, or when a previously set timer fired to further reduce traffic overhead. Interested events and LSNM packet format are shown in Figure 2, where timestamping is measured by Elapsed Time on Arrival (ETA) algorithm [6].

Not only keeping the amount of transferred information as low as possible with overhead less than 2% [3], expensive computation is also shifted out of the sensor network towards powerful infrastructure behind the network sink. Outside the sensor network, received events are continuously analyzed in LSNM Engine for a) rebuilding a global view of the sensor network, for b) quantitatively measuring the current network performance, and for c) eventually investigating the root causes of an observed drop in performance in real-time:

a) Topology reconstruction. The topology is assembled by either adding or removing a link between two nodes whenever connection-related events are received.

b) Vital Sign Analysis. The system behavior is tracked and assessed by the high-level vital signs listed below, which are regularly derived from the reception of event logs. Their statistics build up the knowledge that is then used as indication for system diagnosis.

- Connection/Disconnection Duration: How long a connection can sustain relative to the network stability, while the later reflects the time needed for the node returning to the network.
- Transmission Efficiency: The fraction of successful transmissions during connection represents the efficiency of packet transmission.
- Link Traffic Flow: The traffic load can be revealed from the accumulated number of upstream packets transmitted through a certain link.
- Parent Availability: The matrix denotes the connection frequency between two arbitrary nodes, and also yields communication capability and preference of each node.

c) Diagnosis Process. It is initiated when a significant decrease of the packet throughput, i.e., symptom, is detected, which could be related to various possible anomalies. Benefited from knowledge of topology reconstruction and vital signs analysis, the most probable anomaly can be isolated through a decision tree shown in Figure 3.

1. if packet throughputs of all nodes decrease to zero, potential problem is related to the network infrastructure:
   Sink Outage. The sink is no longer sending beacon messages, forcing all nodes to gradually disintegrate from the network.
   Back-end Failure. Data must be buffered within the sensor network because of a problem between the network sink and the back-end, while the connectivity inside the WSN still remains.

2. else examine all nodes that are found to have a low packet throughput individually.
   Node Isolation. The network is temporarily split because a node disconnected from the network. Check the current parent availability.
   Node Failure. A node failure, e.g., due to a depleted battery or a software crash, is suspected when the disconnection far exceeds the historical maximum value.
   Unreliable Link. Intermittent connectivity that is caused by unreliable links can be observed by consec-

Figure 1: System Architecture

Figure 2: Interested events and LSNM packet format

Figure 3: Decision tree used for localizing the root causes
Traffic Overload. If no topology changes can be observed, the packet throughput might still decrease because of nodes experiencing back-pressure from a saturated link. Traffic overloads can be detected and localized through the link traffic flow metric.

4 Preliminary results

This case study is based on 1-year long traces of 2011 that has been collected at the Matterhorn deployment. This long-term deployment consists of circa 24 TinyNode (MSP430+SX1211 radio) nodes that have been initially installed in 2008. An overview of found anomalies in 2011 is shown in Figure 4. The following, partially also previously unobserved, finding are shown:

Impact of long-lasting outages. Sink Outage and Back-end Failure last for time spans ranging from two hours to up to one day. It is the mere length of those incidents that renders their occurrences rather fatal since the amount of delayed or even lost data increases as long as no action has been taken. Normal network operation can usually not continue before backlogged packets have been delivered to the back-end. The temporary saturation of several communication links is represented by detected Traffic Overload.

Found protocol design deficiency. Regarding Traffic Overload anomalies, we can even find more distant child nodes to be able to starve out sensor nodes that are closer to the sink, i.e., a node has to drop locally generated packets because its local send queue was constantly fully occupied by forwarding traffic.

Non-optimal node placement. Another important operational aid is given when a large number of detected Node Isolations anomalies can be accounted to a few nodes because of their deficiency of parent nodes.

Seasonal variations. The fragile connectivity during winter is visible in the high frequency of Unreliable Link anomalies. While 90% of the parent changes between November and December can be accounted to a single node, we can infer that this node was probably suffering the most from extremely severe environmental conditions, e.g., was surrounded by ice and snow.

5 Conclusions and future work

With the proposed Light-weight Sensor Network Monitoring system, only a low traffic overhead is introduced by sporadically transmitted event logs. If accurate transitions of other type of protocol are captured, LSNM can be generalized to other WSNs. The preliminary results demonstrate that we can benefit from the light-weight logging mechanism. My intention is to further evaluate available metrics to improve the algorithms, i.e., decision tree, for automated diagnosis at the back-end.

6 References


Biographical Sketch.

Yi-Hsuan Chiang is a 4th year Ph.D. student in the Graduate Institute of Communication Engineering, National Taiwan University, with expected date of dissertation submission in Feb. 2014. Her advisor is Polly Huang, professor at NTU in the field of WSNs and multimedia networking. Her co-advisor is Jan Beutel, senior researcher at ETH Zurich, interested in the development, test and validation of WSNs.