Poster Abstract: Understanding Radio Activity Signature of Wireless Sensor Network Protocols

Dong Han
University of Houston
donny@cs.uh.edu

Omprakash Gnawali
University of Houston
gnawali@cs.uh.edu

Abhishek Sharma
NEC Laboratories America, Inc.
absharma@nec-labs.com

Abstract

In this poster, we present a novel approach to study and reveal network protocol information from radio activities instrumentation in wireless sensor network. Recent studies have analyzed radio activities; however, most of these studies focus on estimating energy consumption, since radio chip usually dominates the energy consumption of nodes. In our work, we analyze radio activities with a different purpose, which aims to reveal network protocols and application workloads by an analysis of fine-grained low level radio activities on the nodes. We design a feature called Radio Awake Length Counter and use it to classify and reveal network activity. Results from experiments on a real world testbed indicate that our approach can achieve up to 97% accuracy to identify the routing protocols, average 85% accuracy to distinguish application workloads.

1 Introduction

Identifying abnormal node operation and detecting compromised nodes in a network has been explored in recent years[1]. Doing so using radio activities monitoring is one effective approach [2][4]. Although detection of anomalies or validation of node activities is useful, we take radio activities instrumentation one step further by asking: could radio activities instrumentation be used to understand various aspects of network operation? For example, can we tell what protocol is running in the network, especially when the hardware and software on smart devices are not open source? Our results from analyzing one-million radio activity points indicate that radio activities and carefully designed features can not only reveal information about the network protocol but also useful information about the application workload.

2 Feature Design

We first describe three commonly used features, then compare them against our proposed feature. The experimental results show the feature of radio activities can outperform features extracted from energy consumption to reveal the network information.

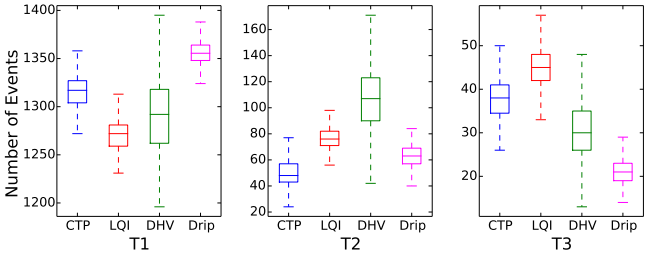


Figure 1: Distribution of RALC of four protocols in three groups during a 3600s experiment length.

- Energy Consumption (EC)
  Mean, *Variance* and *Standard Deviation* values of energy consumption within a 10s window.
- Statistics of Awake Nodes (SAN)
  Mean, *Variance* and *Standard Deviation* values of the number of awake nodes within a 10s window size.
- Number of Snooped Packets (NSP)
  NSP is the number of packets snooped per second in a sliding window of 10s, with 1s step size. NSP can be determined by deploying snooper nodes in the network.
- Radio Awake Length Counter (RALC)
  We define Radio Awake Length (RAL) as the total time that a node stayed in awake mode during each awake-sleep cycles. Based on our experiment observations of the radio awake length to perform send and receive operations, we use the threshold values 0.025s and 0.10s to divide the RAL into three ranges. Within 10s disjoint window size, we count the total number of RAL in each of these ranges, and use these three counters as the RALC. The three counters are named as T_1,T_2 and T_3. Figure 1 shows each protocol has its unique distribution of RALC in above three counters.

3 Evaluation

In this section, we describe our results on how accurately we are able to infer network and application characteristics using features derived from radio activities instrumentation.

SenSys'14, November 3–5, 2014, Memphis, TN, USA.
ACM 978-1-4503-3143-2/14/11.
http://dx.doi.org/10.1145/2668332.2668368

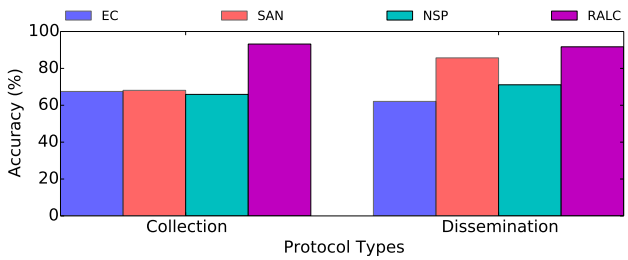


Figure 2: TPR to identify two sets of protocols using J48

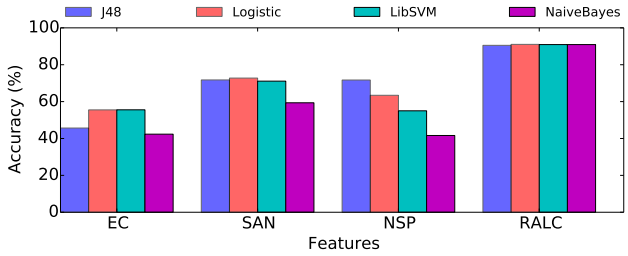


Figure 3: TPR to distinguish across four protocols using four classification algorithms, RALC reports highest accuracy.

3.1 Experiment Settings

We evaluate the design of our radio activities instrumentation and classification accuracy of our proposed RALC feature by doing extensive experiments on FlockLab [3]. In our experiments, we consider four different protocols, two collection protocols (**CTP** and **MultihopLQI**) and two dissemination protocols (**Drip** and **DHV**). The evaluation includes **more than 30 test cases** across different topologies, various application layer packet sizes and transmission intervals.

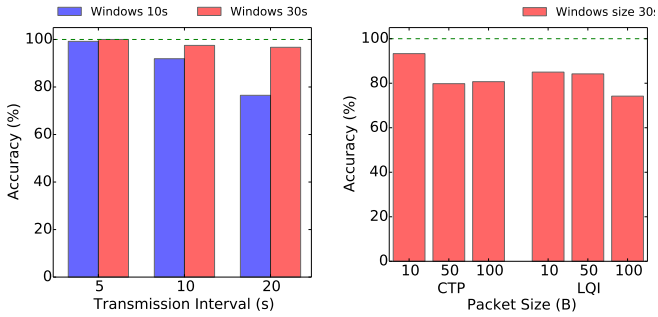
To evaluate the robustness of our proposed approach across various algorithms, we use four classify algorithms (J48, Logistic, LibSVM and NaiveBayes). 90% of samples are used for training and 10% used for testing. We perform 10-fold cross-validation to compute the accuracy of different classifiers, the accuracy results are averaged across the 10 folds.

3.2 Identify Routing Protocols

First we evaluate the ability of the four features mentioned in section 2 to distinguish one protocol from two collection protocols. The result is shown in figure 2 left part. It shows RALC outperforms other features by 38% on average. Similar experiments performed on dissemination is shown in figure2 right side, RALC is 10% better than SAN feature. In the second step, we put all four protocols together, figure 3 again confirms RALC has the highest classification accuracy and most stable performance across 4 features. Experiments verified RALC achieves more than 90% accuracy to distinguish the selected four protocols. RALC achieved similar results with different topologies, packet transmission rates and payload sizes.

3.3 Determine Application Workloads

Next, we evaluate the ability of RALC to determine and distinguish between different application workloads, including various application layer packet transmission interval and packet size. Figure 4(a) shows the True Positive Rate (TPR) for three different packet transmission intervals. The average TPR is above 80% with RALC calculated using 10s window size. When RALC is calculated with 30s window size, the average TPR increases to 96.5%. Figure 4(b) shows that, when we put the radio activity data from 2 protocols with 3 packet sizes altogether, RALC is able to distinguish 1 of the 6 combinations of packet size and routing protocols with more than 83% accuracy in terms of average TPR.



(a) Packet transmission interval 5s, 10s, 20s on CTP.

(b) 6 combinations of packet size and routing protocols.

Figure 4: TPR to distinguish application workloads.

4 Conclusions

In this poster, we demonstrated that radio activities instrumentation can be a powerful tool to study and reveal information about the network protocol and application workload. We designed features for classification and analysis based on radio activities instrumentation. We found that the feature called Radio Awake Length Counter is especially versatile in revealing information across protocols and application workload. Our extensive experimental results performed on real world testbed suggest that RALC can outperform existing commonly used features in terms of its ability to reliably identify network and application characteristics.

5 Acknowledgments

This work was partially supported by a gift from Cisco.

6 References

[1] A. Dunkels, J. Eriksson, N. Finne, and N. Tsiftes. Powertrace: Network-level power profiling for low-power wireless networks. 2011.

[2] C.-F. Huang and Y.-C. Tseng. The coverage problem in a wireless sensor network. *Mobile Networks and Applications*, 10(4):519–528, 2005.

[3] R. Lim, F. Ferrari, M. Zimmerling, C. Walser, P. Sommer, and J. Beutel. Flocklab: A testbed for distributed, synchronized tracing and profiling of wireless embedded systems. In *IPSN*, pages 153–166. ACM, 2013.

[4] S. Tennina, O. Gaddour, F. Royo, A. Koubaa, and M. Alves. Monitoring large scale ieee 802.15. 4/zigbee based wireless sensor networks. 2013.