User-adaptive Energy-aware Security for Mobile Devices

Sriram Sankaran, Ramalingam Sridhar
University at Buffalo, The State University of New York, Buffalo, NY

***Abstract*—Energy Management is of primary importance in mobile devices due to increasing functionality coupled with rapid battery drain. Our analysis reveals that users differ in their context and resource usage patterns which can be profiled towards developing predictive models for energy savings. A key challenge lies in providing user-adaptive security in an energy-aware manner due to increasing sensitivity of user data and analyzing the energy-security trade-offs which we address in this work. Towards this goal, we develop a statistical user model to predict available energy at a given time instant using historical user data and further describe a generic multi-level security model for mobile devices. The available energy from the user model in conjunction with the energy estimates from the security model can be used for energy-aware security adaptation in mobile devices.**

I. Introduction

Energy Management is one of the foremost concerns in mobile devices. This is primarily due to increasing functionality in mobile applications which rapidly drains battery power in these devices. Our premise is that individual user behavior can be profiled towards developing predictive models for energy savings. Security contributes towards energy drain due to mechanisms needed to handle the increasing sensitivity of user data in mobile devices. Further, these mechanisms require models for estimating the energy consumption of security protocols.

A key challenge lies in providing user-adaptive security in an energy-aware manner and analyzing the energy-security trade-offs. In contrast to existing works [1] [2], we develop statistical user models for predicting available energy given time of the day and day of the week and a multi-level security model for mobile devices.

II. User Modeling

A. Model Training

We develop our model using real world traces obtained from the Livelab [3] dataset. The goal of our model is to predict available energy for individual users given time of the day and day of the week. Since users follow a unique pattern every day of the week, we obtained the values for available battery power across all days of the week.

Figures 1 (a), 1 (b) and 1 (c) display available battery energy across all Mondays by the hour for user 1, user 2 and user 3 respectively. The figures indicate that the battery drain pattern for each of the users is consistent across all Mondays except for a few curves which show inconsistent behavior. Thus, we averaged the battery drain across all Mondays and constructed the training set.

Our resulting hypothesis from training the model is a polynomial equation of the following form since battery drain is not strictly linear and that users charge their phones at regular intervals thus resulting in a polynomial curve. However, the degree of the polynomial curve varies for individual users.

$$y = a + b * x + c * x^2 + d * x^3 .... z * x^n \tag{1}$$

B. Model Validation

We validate our hypothesis for each day of the week using cross-validation data to evaluate the robustness of the predictor. Simulations were performed using Matlab for training and cross-validation. In particular, we estimated training and cross-validation errors for polynomial curves of degrees between 1 and 20. Root-mean-square (RMS) error for training and cross-validation can be computed using the following equation

$$RMS = \sqrt{\sum_{i=1}^{n} (y_{Predicted} - y_{Actual})^2} \tag{2}$$

where n refers to number of data samples used for training and cross-validation and $y_{Predicted}$ and y_{Actual} are the predicted and actual values respectively.

Figures 2 (a), 2 (b) and 2 (c) display training and cross-validation errors for polynomial curve of varying degress across Mondays for users 1, 2 and 3 respectively. The results indicate that as degree d increases, training error decreases since it fits the curve with greater accuracy. However, cross-validation error decreases with increase in degree d until a particular point when it starts to increase. The polynomial curve of degree d with minimum cross-validation error can be used for predicting available energy for each user.

III. Multi-level Security Model

Table I contains our multi-level security model for mobile devices. It consists of a 3-level security solution where each level is associated to a cryptographic algorithm. A higher security protocol implies a cryptographic protocol with higher security strength. For instance, traditional RC5 and AES at the low and medium levels respectively offer authentication but not integrity. On the other hand, HMAC-MD5 at the highest level offers both authentication and integrity.

We estimate the execution time and energy consumption of security protocols using Avrora, a cycle-level power profiling tool. Table II contains the results for execution time and energy consumption.

978-1-4799-0895-0/13/$31.00 ©2013 IEEE

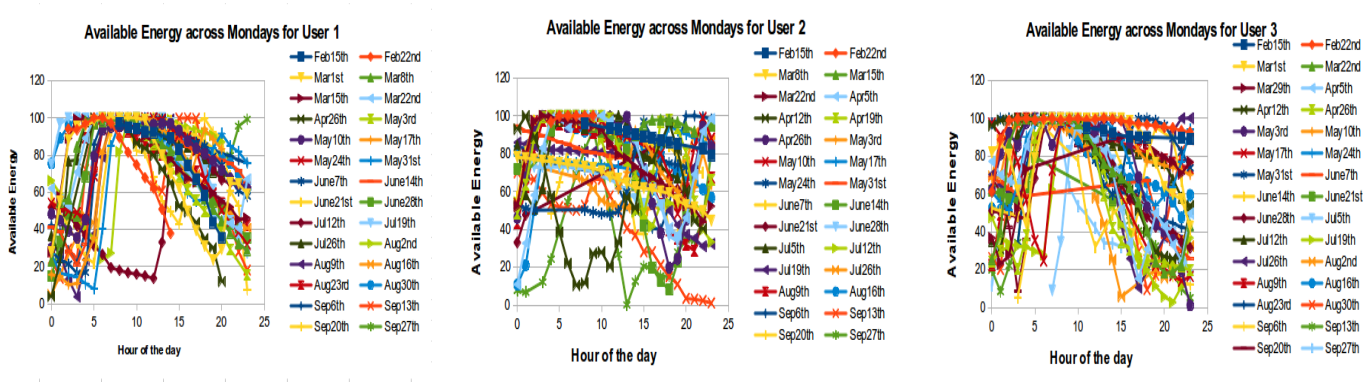

Fig. 1: Available Energy for User 1, User 2 and User 3 across Mondays

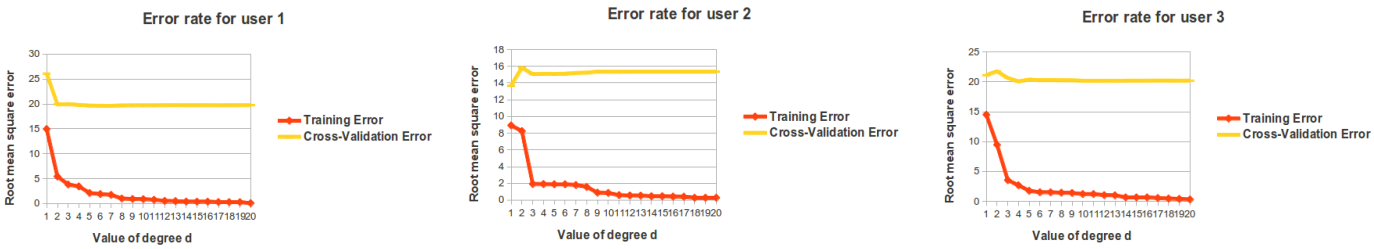

Fig. 2: Training and Cross-validation Error rates for User1, User2 and User3

TABLE I: Multi-level Security

Security Level	Security Property	Crytographic Protocol
Low	Authentication	RC5
Medium	Authentication	AES
High	Authentication and Integrity Protection	HMAC-MD5

TABLE II: Energy and Performance Evaluation

Cryptographic Protocol	Execution Time	Energy Consumption
RC5	0.2029s	5.435 mJ
AES	0.3406s	9.124 mJ
HMAC-MD5	4.547s	121.8 mJ

Our model is generic in that it addresses the broader goal of providing adaptable security in mobile devices. Since users desire higher level of security due to increasing sensitivity of user data, higher security translates into increased energy consumption and performance. For instance, HMAC-MD5 requires a hash and digest to be computed which incurs higher execution time compared to AES and RC5 as evident from Table II.

IV. Overhead Analysis

In this section, we estimate the power overhead of polynomial curves for varying degrees using Wattch. Figure 3 displays the results for average power consumption for varying number of users. The results indicate that as the degree of the polynomial curve increases, number of instructions needed for computation increases thus increasing the power consumption.

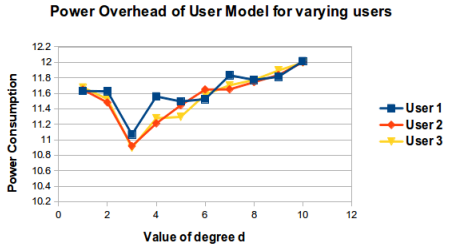

Fig. 3: Power Overhead of user model for varying users

V. Conclusion

We presented user models for predicting available energy for varying users at a given time instant. These models have been trained and cross-validated and the power overhead evaluated for polynomial curves of varying degrees. The available energy from the user model in conjunction with the energy estimates from the security model can be used for energy-aware security adaptation in mobile devices.

References

[1] S. Futaci, K. Jaffres-Runser, and C. Comaniciu, "On modeling energy-security trade-offs for distributed monitoring in wireless ad hoc networks," in *MILCOM*, 2008, pp. 1–7.

[2] H. Falaki, R. Mahajan, S. Kandula, D. Lymberopoulos, R. Govindan, and D. Estrin, "Diversity in smartphone usage," in *Proc. of Mobisys 2010.*

[3] C. Shepherd, A. Rahmati, C. Tossell, L. Zhong, and P. Kortum, "Livelab: measuring wireless networks and smartphone users in the field," *SIGMETRICS Perform. Eval. Rev.*, vol. 38, no. 3, pp. 15–20, 2011.