

Modeling Context-Adaptive Energy-Aware Security in Mobile Devices

Swapnoneel Roy*, Sriram Sankaran†, Preeti Singh*, Ramalingam Sridhar‡

*School of Computing, University of North Florida, Jacksonville, Florida 32224

s.roy@unf.edu, n00955122@ospreys.unf.edu

†Center for Cybersecurity Systems and Networks, Amrita Vishwa Vidyapeetham, Amritapuri, Kollam, Kerala- 690525

srirams@am.amrita.edu

‡Department of Computer Science and Engineering, University at Buffalo, SUNY, Buffalo, New York 14260

rsridhar@buffalo.edu

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 context and resource usage patterns which can be leveraged for power savings. A key challenge lies in providing context-adaptive security in an energy aware manner due to increasing sensitivity of user data and analyzing energy-security trade-offs. Towards this challenge, we model the problem of context-adaptive energy-aware security as a knapsack problem and develop a pseudo-polynomial dynamic programming (DP) based framework to maximize user utility corresponding to a power budget. Further, we prove the decision version of the problem to be NP-hard via a reduction from KNAPSACK and design a greedy heuristic for optimal assignment of security levels towards meeting a given power budget. Finally, we design a Fully Polynomial Time Approximation Scheme (FPTAS) for the problem which improves upon the DP based approach. The proposed mechanisms are optimal in that, they can be used to facilitate efficient allocation of resources pertaining to user needs.

I. INTRODUCTION

Energy Management has become one of the foremost concerns in mobile devices. This is primarily due to the increasing functionality in mobile applications which rapidly drains battery power in these devices. Security significantly contributes towards energy drain due to the computation-intensive cryptographic operations involved in securing communications. These motivate the need for developing energy aware security mechanisms in mobile devices. Further, these mechanisms require models for estimating the energy consumption of security protocols.

Current approaches to security often do not cater to varying user context thus resulting in inefficient energy usage. Further they do not adapt to the available energy for making energy-security trade-offs that vary for individual users. Our analysis reveals that user patterns are unique and driven by context which result in varying energy usage. Further, tailoring security to user context can facilitate efficient usage of energy thus enabling the user to meet a given power budget. Thus, context-adaptive security designs are a promising approach for facilitating efficient energy usage.

Context-adaptive security designs must not only adapt security but also prioritize the allocation of resources for mobile

devices. Current approaches to allocation are often static and do not scale resources pertaining to user needs. In contrast, approaches for maximizing user utility subject to the power constraints are needed. This may require the development of heuristic solutions for optimizing user utility towards meeting a given power budget. Such an approach can facilitate efficient allocation of resources which may result in effective energy usage.

A. Our Contributions

In this work, we model context-adaptive energy-aware security for mobile devices as a combinatorial optimization problem and develop solutions for effective allocation of resources such that user's utility is maximized. In particular, we prove that the decision version of the problem is NP-hard and design greedy, dynamic programming based, and FPTAS algorithms to solve the problem for optimal assignment of security levels towards meeting a given power budget. Our major contributions include:

- Formulating the problem, analyzing different cases and designing a pseudo-polynomial dynamic programming algorithm to solve the problem.
- Proving that the the decision version of the problem is NP-Complete through a reduction from KNAPSACK and designing a greedy algorithm that maximizes security depending on user context while meeting a given power budget.
- Design a FPTAS for the problem which improves upon the execution time of the dynamic programming algorithm.

II. RELATED WORK

Prior approaches to security analyzed the energy consumption of security protocols. Potlapally *et al.* [1] and Hodjat *et al.* [2] evaluate the energy consumed by symmetric and asymmetric security protocols in traditional wireless networks. Karri *et al.* [3] optimized IPsec to suit the needs of the resource constrained devices. Chang *et al.* [4], Ganesan *et al.* [5] and Lee *et al.* [6] evaluate the energy consumed by security protocols within the context of wireless sensor networks.

In addition to energy evaluation, model-based approaches for understanding energy-security trade-offs were explored.

Mckay *et al.* [7] used a decision-theoretic model to analyze the energy-security trade-offs in traditional wireless networks. Hwang *et al.* [8] analyzed energy-memory-security trade-offs in sensor networks using a key management protocol. Futaci *et al.* [9] proposed a game-theoretic framework for modeling the energy-security trade-offs due to intrusion detection in wireless sensor networks. Gogniat *et al.* [10] proposed a re-configurable architecture for security using FPGAs. Chandramouli *et al.* [11] and Massey *et al.* [12] proposed an optimization framework that maximizes security subject to power and delay constraints respectively.

Numerous approaches [13] [14] [15] [16] [17] [18] [19] [20] [21] have considered the importance of context for security in mobile environments. These approaches propose adaptable mechanisms for security which configures security according to the needs of the environment. In contrast, we model context-adaptive energy-aware security as an optimization problem and develop heuristics and FPTAS for optimum assignment of security levels towards meeting a given power budget.

III. MODEL DESCRIPTION

We consider a scenario where there is a *single* mobile user who travels through n *different* locations. Each location has a preferred *security level*. As an example, the level of security of a Wi-Fi network might vary according to the location of the user (e.g. home, office, public, etc.). We also consider there are m security levels $\{S_1, S_2, \dots, S_m\}$. Each security level S_i has a *power consumption* P_{S_i} and a *user benefit* (in terms of the amount of security) b_i associated with it.

Now the user, who travels through n locations is constrained by a total energy budget E , which is the amount of energy the user does not want to exceed during travel. The user also has a total benefit B , which is the minimum total benefit the user wants to achieve during travel to guarantee a certain level of security depending on the locations.

The problem is to find an allocation of security levels (from the set of m security levels) to the n locations the user travels through, such that, the total energy consumed does not exceed E , and the benefit is at least B , subject to the constraint that we allocate preferred security levels to as many locations possible. The same energy level can be allocated to multiple locations (we consider there are unlimited copies of each of the m security levels).

There can be an offline version of this model where the user knows the all n locations and their preferred security levels beforehand. There is also an online version, where the locations and their preferred levels are revealed one at a time.

A. Problem Formulation

The problem of context-adaptive energy-aware security can be formulated as follows.

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

Table I
MULTI-LEVEL SECURITY

CONTEXT-SEC PROBLEM

INPUT: User's energy budget E with power consumed due to security, $p_{S_1} \dots p_{S_m}$ for varying security levels $S_1 \dots S_m \in \mathbf{S}$, and the corresponding user benefits $b_1 \dots b_m$, n locations through which the user travels.

OUTPUT: Maximize $\sum_{i \in S} b_i$ subject to $\sum_{S_i=1}^n p_{S_i} \leq E$.

QUESTION: Given integer B , is $\sum_{i \in S} b_i \geq B$

such that $\sum_{S_i=1}^n p_{S_i} \leq E$?

B. Scope of this work

In this work we consider an off-line version of the CONTEXT-SEC problem where the locations do not contain preferences of security levels. In other words, we have n locations (without any associated preferences), and m levels to be allocated to those locations such that the total energy consumption is at most E and the total user benefit is at least B .

IV. OUR APPROACH

In this section, we discuss our approach to the context-adaptive security problem in mobile devices. Specifically, we analyze different cases such as the special case where there exists a finite amount of security levels each with corresponding values and energy estimates and a general case where there exists an infinite number of security levels.

A. The Special Case

In the special case, we consider a finite amount of security levels pertaining to user context. To aid in the discussion of our special case, we propose a multi-level security model for context-adaptive security in mobile devices. The following subsection describes the security model for mobile devices.

1) *Multi-level Security Model*: Table I contains our proposed multi-level security model for mobile devices. The proposed approach 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, AES and RC5 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.

Energy-awareness requires the energy consumption of security protocols to be estimated. We estimated the execution time and energy consumption of security protocols using AvroraZ

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

Table II
ENERGY AND PERFORMANCE EVALUATION

[22], a cycle-level power profiling tool. Table II contains the results for execution time and energy estimates of security protocols.

Our model is generic in that it is not confined to the above security protocols but to address the broader goal of providing adaptable security in mobile devices. Towards the goal, we classify security depending on security properties where the highest level of security provides authentication and integrity protection. Since users desire higher level of security due to data sensitivity, higher security translates into increased energy consumption and performance. For instance, HMAC-MD5 requires a hash and digest to be computed which incurs significant time and overhead for message encryption and verification.

2) *Optimal Dynamic Programming Algorithm*: CONTEXT-SEC can be solved using a dynamic programming algorithm which computes the optimal assignment of security levels for users towards maximizing user utility corresponding to a power budget. We describe the dynamic programming algorithm for computing the optimal power budget in Algorithm 1.

Algorithm 1 Algorithm for optimal power budgeting

```

1: procedure OPTIMAL POWER BUDGETING
   ALGORITHM( $b, p_S, n, B$ )
2:   for  $i = 1:n$ 
3:     for  $x = 0:B$ 
4:       if  $b[i] \leq x$ 
5:          $A[i, x] \leftarrow \min(A[i-1, x], A[i-1, x-b[i]] +$ 
            $p_S[i])$ 
6:       else
7:          $A[i, x] \leftarrow A[i-1, x]$ 
8:       end if
9:     end for
10:  end for
11: end procedure

```

Let B be the benefit of the most beneficial security level. That is, $B = \max_{a \in \mathbb{S}} b_a$. From this, we can upper bound the benefit that can be achieved as nB for the n security levels. Let $\mathbb{S}_{i,b}$ denote a subset of security levels $\{S_1, \dots, S_i\}$ that has a total benefit of exactly b and consumes the least amount of power possible. Let $A(i, b)$ be the power consumed by the set $\mathbb{S}_{i,b}$, with a value of ∞ to denote no such subset. For $A(i, b)$, we have the base cases $A(1, b)$ where $A(1, b_1)$ is p_{S_1} , and all other values are ∞ .

In the dynamic programming algorithm, an array $A[0 \dots n, 0 \dots B]$ will be constructed. Any element $A[i, b]$ (for

Approach	Time Complexity
Brute-force	$O(2^n)$
Dynamic Programming	$O(n^2 * B)$

Table III
OVERHEAD COMPARISON

$1 \leq i \leq n$ and $1 \leq b \leq B$) will store the least amount of power consumed by any subset of security levels $\{S_1, S_2, \dots, S_i\}$ with a benefit of exactly b . Once all the elements of this array is computed, $A[n, B]$ will contain the minimum power consumed with a benefit of B . In other words $A[n, B]$ will contain an optimal solution for CONTEXT-SEC.

We comparatively analyze the running time of the brute-force approach and dynamic programming algorithm. Table III contains the results for the running time evaluation.

The results indicate that the running time of dynamic programming algorithm is $O(n^2 * B)$ where n and B indicate the number of security levels and the benefit of the most beneficial security level, and that it performs better than the brute-force approach. Algorithm 1 is still an exponential (pseudo-polynomial) algorithm. Its runtime grows exponentially in the number of bits needed to represent B .

With the input from multi-level security model, we ran the dynamic programming algorithm for varying power budgets and estimated the execution time and power consumption using the Wattch [23] simulator. Figure 1 contains the results for execution time and power consumption. The results indicate that as power budget increases, there is a linear increase in power consumption and execution time of the dynamic programming algorithm due to the recursive computation.

Dynamic Programming Algorithm

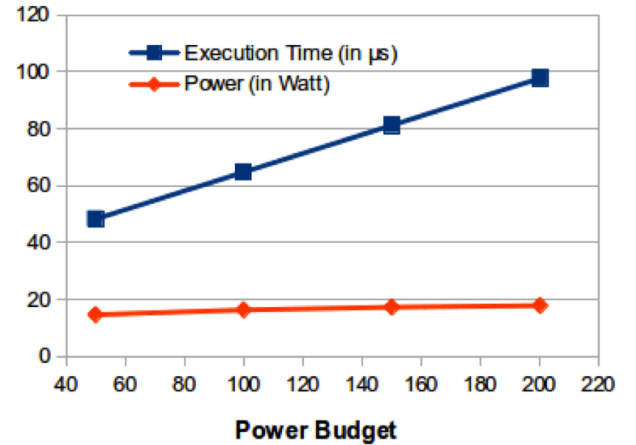


Figure 1. Performance Evaluation of Dynamic Programming

B. General Case

In the general case, the decision version of CONTEXT-SEC cannot be solved using a polynomial time algorithm since there exists numerous security levels each with different energy and performance requirements pertaining to user context. We prove that the problem to be NP-Complete through a reduction from KNAPSACK. The KNAPSACK problem is defined as follows:

KNAPSACK

INSTANCE: $S = (W_1, V_1), (W_2, V_2) \cdots (W_k, V_k)$,
 $V \in \mathbb{Z}^+$, $W \in \mathbb{Z}^+$,

where W and V refer to weights and values respectively.

QUESTION: Is there $S' \subset S$ s.t.

$$\sum_{i=1}^n W'_i \leq W \text{ and } \sum_{i=1}^n V'_i \geq V?$$

Theorem 1. *The decision version of CONTEXT-SEC is NP-Complete.*

Proof: Given an arbitrary instance of KNAPSACK, we construct a definite instance of CONTEXT-SEC as follows:

- 1) For each i (where $1 \leq i \leq k$), set $p_{S_i} = W_i$, and $b_i = V_i$.
- 2) Set $B = V$ and $E = W$.
- 3) The set S of items for KNAPSACK is exactly the same set of security levels in CONTEXT-SEC.

Since the above reduction function is essentially a bijection, the following hold

- If $(S, W, V) \in \text{KNAPSACK}$, then $(S, E, B) \in \text{CONTEXT-SEC}$.
- If $(S, E, B) \in \text{CONTEXT-SEC}$, then $(S, W, V) \in \text{KNAPSACK}$.

Therefore the theorem is true. $\square$

C. A Greedy Algorithm

The greedy algorithm greedily maximizes security pertaining to user context indicated by user benefits while meeting the given energy budget. We adapt the Max-Value heuristic to this problem. Algorithm 2 contains the description of the Max-Value Greedy Algorithm.

Algorithm 2 Max-Value Algorithm

- 1: **procedure** CONTEXT-ADAPTIVE ENERGY-AWARE SECURITY(S, E, B)
 - 2: Sort Security levels in descending order of $\frac{b_i}{p_{S_i}}$.
 - 3: Continue adding security levels until we hit a power level p_{S_i} too high, ($\sum_{S_k=1}^i p_{S_k} > E$).
 - 4: Select the better of $\{S_1, S_2, \dots, S_{i-1}\}$ and $\{S_i\}$ based on $\max(\sum_{k=1}^{i-1} b_k, b_i)$.
 - 5: **end procedure**
-

Algorithm 2 has an execution time of $O(n \log n)$, where $|S| = n$ due to the sorting step.

Theorem 2. *Algorithm 2 is a 2-approximation algorithm for CONTEXT-SEC.*

Proof: Let OPT be the output of an optimal algorithm for CONTEXT-SEC. Now if the solution of Algorithm 2 was suboptimal, the total power consumption will be strictly less than E (let it be $E - F$). Assume Algorithm 2 was allowed to select fractional values for security levels. Therefore by adding $\frac{E-F}{p_{S_{k+1}}} b_{k+1}$ to the user benefits, Algorithm 2 will either match or exceed OPT (since OPT is not allowed to choose fractional values). Therefore either $\{b_i, b_2, \dots, b_{i-1}\} \geq \frac{1}{2} OPT$, or $\{b_i\} \geq \frac{1}{2} OPT$. Since Algorithm 2 chooses the greater of the two sets, the output of Algorithm 2 $\geq \frac{1}{2} OPT$. $\square$

D. A Fully Polynomial Time Approximation Scheme (FPTAS)

In the FPTAS, we scale down the benefits enough such that the benefits of all the security levels are polynomially bounded in n , use dynamic programming on the new instance, and return the resulting subset. By scaling with respect to the desired ε , we will be able to get a solution that is at least $(1 - \varepsilon) \cdot OPT$ in polynomial time with respect to both n and $1/\varepsilon$, achieving a FPTAS.

Algorithm 3 Fully Polynomial Time Approximation Scheme

- 1: **procedure** FPTAS($b, p_S, n, B, \varepsilon > 0$)
 - 2: Let $K = \frac{\varepsilon B}{n}$.
 - 3: For each security level S_i , define $b'_i = \lfloor \frac{b_i}{K} \rfloor$.
 - 4: With these as benefits of security levels, use the dynamic programming algorithm (Algorithm 1) to find set with the most benefit, say S' .
 - 5: Output S' .
 - 6: **end procedure**
-

Lemma 1. *The solution S' produced by Algorithm 3 has a total benefit of at least $(1 - \varepsilon) \cdot OPT$.*

Proof: Assume O to be the optimal set of security levels with the maximum benefit possible, and $B(S)$ to be the benefit produced by set of security levels S . Because we scaled down by K and then rounded down, any security level S_i will have benefit $K \cdot b'_i \leq b_i$ with the difference at most K . Therefore the benefit of the optimal set O can at most decrease at nK for K per possible member of the set. Therefore we have, $B(O) - K \cdot B'(O) \leq nK$.

Now after the dynamic programming step, we get an optimal solution with the scaled (smaller) benefits. The solution is as good as choosing O with the smaller benefits. Therefore $B(S') \geq K \cdot B'(O) \geq B(O) - nK = OPT - \varepsilon B \geq (1 - \varepsilon) \cdot OPT$. $\square$

Theorem 3. *Algorithm is a fully polynomial approximation scheme for CONTEXT-SEC.*

Proof: Lemma 1, shows the solution produced by Algorithm 3 to fall within a $(1 - \varepsilon)$ factor of OPT . The running time of Algorithm 3 is $O(n^2 \lfloor \frac{P}{K} \rfloor) = O(n^2 \lfloor \frac{n}{\varepsilon} \rfloor)$, which is polynomial in both n and $1/\varepsilon$. $\square$

V. PERFORMANCE COMPARISONS

We are currently in progress implementing the three algorithms described. The development source code is currently available in the following location in GitHub [24]. For our implementations, we consider the benefits associated with each security level as a discrete quantity (e.g. an integer). The levels with their corresponding power consumptions will be obtained from the following dataset [25]. We plan to compare the performances of the three algorithms for the problem in terms of allocations. We present a few numbers from our initial performance comparisons here.

VI. CONCLUSION

In this work, a context-adaptive energy-aware approach to security was developed for mobile devices. In particular, we modeled the problem of context-adaptive energy-aware security as a knapsack problem and proposed a pseudo-polynomial dynamic programming framework towards maximizing user utility corresponding to a power budget. In addition, we proved that the decision version of the problem is NP-Hard through a reduction from knapsack problem and developed a greedy heuristic which prioritizes the allocation of resources towards meeting a given power budget. Finally, we designed FPTAS which improves upon the execution time of the dynamic programming algorithm.

VII. ACKNOWLEDGEMENT

This work was supported in part by NSF grant CNS-1422304.

REFERENCES

- [1] N. R. Potlapally, S. Ravi, A. Raghunathan, and N. K. Jha, "Analyzing the energy consumption of security protocols," in *Proceedings of the 2003 international symposium on Low power electronics and design*. ACM, 2003, pp. 30–35.
- [2] A. Hodjat and I. Verbauwhede, "The energy cost of secrets in ad-hoc networks (short paper)," 2002.
- [3] R. Karri and P. Mishra, "Optimizing ipsec for energy-efficient secure wireless sessions," in *System-Level Power Optimization for Wireless Multimedia Communication*. Springer, 2002, pp. 133–152.
- [4] C.-C. Chang, D. Nagel, and S. Muftic, "Balancing security and energy consumption in wireless sensor networks," *Mobile Ad-Hoc and Sensor Networks*, pp. 469–480, 2007.
- [5] P. Ganesan, R. Venugopalan, P. Peddabachagari, A. Dean, F. Mueller, and M. Sichitiu, "Analyzing and modeling encryption overhead for sensor network nodes," in *Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications*. ACM, 2003, pp. 151–159.
- [6] J. Lee, K. Kapitanova, and S. H. Son, "The price of security in wireless sensor networks," *Comput. Netw.*, vol. 54, no. 17, pp. 2967–2978, Dec. 2010. [Online]. Available: <http://dx.doi.org/10.1016/j.comnet.2010.05.011>
- [7] K. McKay, "Trade-offs between energy and security in wireless networks," Ph.D. dissertation, Worcester Polytechnic Institute, 2005.
- [8] D. D. Hwang, B. Cheng Charles Lai, and I. Verbauwhede, "Energy-memory-security tradeoffs in distributed sensor networks," in *In ADHOC-NOW*, 2004, pp. 70–81.
- [9] R. Chandramouli, S. Bapatla, K. Subbalakshmi, and R. Uma, "Battery power-aware encryption," *ACM Transactions on Information and System Security (TISSEC)*, vol. 9, no. 2, pp. 162–180, 2006.
- [10] S. M. Futaci, K. Jaffrès-Runser, and C. Comaniciu, "On modeling energy-security trade-offs for distributed monitoring in wireless ad hoc networks," in *Military Communications Conference, 2008. MILCOM 2008. IEEE*. IEEE, 2008, pp. 1–7.
- [11] G. Gogniat, T. Wolf, and W. Burleson, "Reconfigurable security primitive for embedded systems," in *System-on-Chip, 2005. Proceedings. 2005 International Symposium on*, 2005, pp. 23–28.
- [12] T. Massey, P. Brisk, F. Dabiri, and M. Sarrafzadeh, "Delay aware, reconfigurable security for embedded systems," in *Proceedings of the ICST 2nd international conference on Body area networks*, ser. BodyNets '07. ICST, Brussels, Belgium, Belgium: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2007, pp. 12:1–12:5.
- [13] C. T. Hager, "Context aware and adaptive security for wireless networks," Ph.D. dissertation, Virginia Polytechnic Institute and State University, 2004.
- [14] G. D. Abowd, A. K. Dey, P. J. Brown, N. Davies, M. Smith, and P. Steggles, "Towards a better understanding of context and context-awareness," in *Proceedings of the 1st international symposium on Handheld and Ubiquitous Computing*, ser. HUC '99. London, UK, UK: Springer-Verlag, 1999, pp. 304–307. [Online]. Available: <http://dl.acm.org/citation.cfm?id=647985.743843>
- [15] G. Fischer, "Context-aware systems: the 'right' information, at the 'right' time, in the 'right' place, in the 'right' way, to the 'right' person," in *Proceedings of the International Working Conference on Advanced Visual Interfaces*, ser. AVI '12. New York, NY, USA: ACM, 2012, pp. 287–294.
- [16] S. Sankaran, "Lightweight security framework for iots using identity based cryptography," in *2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Sept 2016, pp. 880–886.
- [17] A. Jameson, "Modelling both the context and the user," *Personal Ubiquitous Comput.*, vol. 5, no. 1, pp. 29–33, Jan. 2001. [Online]. Available: <http://dx.doi.org/10.1007/s007790170025>
- [18] N. Botezatu, V. Manta, and A. Stan, "Self-adaptability in secure embedded systems: an energy-performance trade-off," in *The 2011 International Conference on Information Security and Internet Engineering, World Congress on Engineering*, 2011.
- [19] S. Sankaran and R. Sridhar, "User-adaptive energy-aware security for mobile devices," in *Communications and Network Security (CNS), 2013 IEEE Conference on*. IEEE, 2013, pp. 391–392.
- [20] A. Gawanmeh and A. Alomari, "Taxonomy analysis of security aspects in cyber physical systems applications," in *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE, 2018.
- [21] H. Al-Hamadi, A. Gawanmeh, and M. Al-Qutayri, "Lightweight security protocol for health monitoring in ambient assisted living environment," in *Communications Workshops (ICC Workshops), 2017 IEEE International Conference on*. IEEE, 2017, pp. 1282–1287.
- [22] R. de Paz Alberola and D. Pesch, "Avroraz: extending avrora with an ieee 802.15.4 compliant radio chip model," in *Proceedings of the 3rd ACM workshop on Performance monitoring and measurement of heterogeneous wireless and wired networks*, ser. PM2HW2N '08. New York, NY, USA: ACM, 2008, pp. 43–50. [Online]. Available: <http://doi.acm.org/10.1145/1454630.1454637>
- [23] D. Brooks, V. Tiwari, and M. Martonosi, "Wattch: a framework for architectural-level power analysis and optimizations," in *Proceedings of the 27th annual international symposium on Computer architecture*, ser. ISCA '00. New York, NY, USA: ACM, 2000, pp. 83–94.
- [24] "Modeling context adaptive energy aware security in mobile devices (source code)," <https://github.com/p09singh/Modeling-Context-AdaptiveEnergy-Aware-Security-in-Mobile-Device>, accessed: 2018-01-11.
- [25] "Livellab: Measuring wireless networks and smartphone users in the field," <http://livellab.recg.rice.edu/traces.html>, accessed: 2018-01-11.