Comparison of security protocols in Mobile Wireless Environments: Tradeoffs between level of security obtained and battery life[1]

Fernando C. Colón Osorio, Kerry McKay and Emmanuel Agu,
WPI System Security Research Laboratory *(WSSRL)*,
Computer Science Department, Worcester Polytechnic Institute,
Worcester, MA 01609, USA, {fcco, kerrym, emmanuel}@cs.wpi.edu

Abstract

A e a e e c ea e , e e ee ec e . I ece ea , a e ea c e a e e a e ec ec a a ec e e e , a e a e e ec e a c e ba e e. H e e , e e a bee e e ea c e e - ec a ec ec a b e e ce a e ac e e a e. T a a c - a a a ea e e c e a c a a ac e e a a ac e ca a a e ce' ba e b a e ea e ec e e e e e a .

I a c , e e a e a e a - a a e- be ee e e a ec - e b C O e a. T e ea c e c be a e e e a a e ec - e a e a ca , e ba e c a . We a e e a a a e be ee e e a a ec c e a e e e e c .

1 Introduction

The use of wireless networks has seen explosive grow in the last few years. For example, the sales of embedded wireless devices grew 66.2% each year for the last four-(4) years (see, http://www.instat.com). In addition, the number of public hotspots worldwide grew from a mere 1,200 in 2001 to approximately 150,000 today (Source: Gartner Dataquest, June 2003). Further, newer generations of mobile computing equipment come with wireless support standard. In 2003, 55% of laptops sold had embedded wireless support built in, and this percentage is expected to grow even more. From corporate networks to home networks, the number of wireless networks and clients is on the rise. As the world becomes more dependent on wireless networks, it also becomes more dependent on the mechanisms that protect them. Unfortunately, mobile wireless devices suffer from a set of limitations which are not present in their wired counterparts. One such key limitations is battery capacity. While memory and processor technologies roughly double every semiconductor generation (approximately 18 months), battery technology is increasing at the much slower rate of 5%-10% per year[6]. This trend has created, what is commonly referred to as the "battery gap" for mobile devices. This battery gap refers to the gap between the increasing computing capabilities of mobile devices and the corresponding need for increasing power density of their battery vs. what is available (figure 1). Some may argue that this is not important, because people often plug in their laptops during wireless network usage. In this manuscript, our primary focus is mobile wireless handheld devices, which are rarely plugged into a power supply during normal usage.

Research in the power consumption of wireless handhelds has been primarily done in three areas: (1) energy utilization of the network interface card; (2) overall impact of the NIC on mobile systems; and (3) power management techniques. However, to our knowledge, there has been no conclusive research on making intelligent trade-offs between security and energy consumption. If trade-offs between security and energy can be represented in a mathematical form, then we can use that information to better choose a security level for a given application. This knowledge will lead to optimal energy usage, with respect to such a security profile.

In studying the energy consumption of wireless devices, it is readily apparent that the largest source of power drain is associated with packet transmission. Within this context, security protocols, specif-

[1]This work was conducted as part of a larger effort in the developement of next generation Intrusion Detection & CounterMeasure Systems at WSSRL. The work is conducted under the auspices of Grant ACG-2004-06 by the Acumen Consulting Group, Inc., Marlboro, Massachusetts.

0-7803-9469-0/05/$20.00 ©2005 IEEE

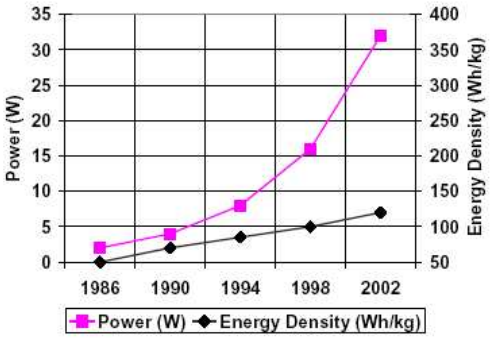


Figure 1: growing gap between battery technology and power requirements[6]

ically the authentication portion, may require many or few transmissions, depending on the protocol. For instance, WEP authentication contains only two messages sent by the client whereas EAP-based methods require the client to send at least four messages - a minimum 100% increase. The client needs to send a message to get a ticket-granting ticket, and then for every service, a message requesting a ticket and a message for logging into that service are required. Clearly, the security protocol applied has a direct and significant impact on the number of transmissions, and subsequently on the battery life.

In addition to the cost of transmission, there are large differences in energy consumed by other factors of each protocol. The energy drained by cryptographic computations does matter, as reducing the energy cost will extend the time that a mobile device can be used. Although transmission is the biggest source of energy consumption, finding optimizations with respect to the security profile are advantageous.

In this manuscript, we first review current 802.11 security standards and their limitations. We then use a model proposed by Colón Osorio et al.[2] to understand how such protocols affect the energy consumption of a mobile device. More specifically, we attempt to quantify how much additional power is expended by a mobile device in order to achieve a given security profile. This model will be used to evaluate WEP, WPA, 802.1x/EAP, and CCMP, see section 7.2. They are first evaluated by analytical methods used to create a hypothesis, and then compared with the empirical measurements.

2 Previous Work

A careful review of the wireless security literature shows that the bulk of research has been concentrated in two broad areas. These are: (1) Security of the Wireless Channel and associated protocols; and (2) Power Limitations of Mobile Devices and their Impact on Security.

Sec e W ee C a e: The weaknesses of the current 802.11 security standard (WEP), WEP2, and protocol extensions to WEP have been well documented, Fluhrer, et. al., Nikita Bosrisov et.al., and others. In order to deal with these limitations, a set of extensions have been proposed that attempt to ameliorate 802.11 security weakness by: (1) Using longer keys; (2) Decomposing the problem into three phases: *a e ca* ,*a a* , and *acce c* ; and (3) Modifying key distribution and management methods to use a trusted certificate authority.

One problem with this approach is that it ignores key limitations of wireless devices, such as their limited battery life. Since mobile nodes have a lower amount of memory, battery power, and bandwidth, malicious attacks on system resources will affect wireless devices quicker and have more pronounced effects than their wired counterparts.

Furthermore, by separating authentication, authorization, and access control, the proposed protocols increase the overhead required per packet of data transfered. This, leads to greater utilization of scarce resources. As we point out in section 4, an approach to get around this limitation is to investigate security from the perspective of effective resource utilization. A complete summary of the limitations associated with current and proposed wireless security protocols is presented in section 3.

P e L a M b e De ce a e I - ac Sec :

Specifically, in the area of power limitations of mobile devices, the focus has been in understanding the effects of the network card on overall energy utilization. Stemm and Katz (In IEICE Transactions on Communications, Aug 1997) provided us with a model for breaking down energy expended in wireless communication. They examined packets of b bytes, and derived costs for energy used in the idle state, transmission and reception of packets, and the total energy.

While the approaches investigated thus far are useful in reducing the power and resource consumption of wireless devices, the additional power and resource utilization drain that security protocols imposed are less understood. A notable exception to this statement

is the work by Potlapally, *e a* [7]. In their work, they examined the energy consumed by a PDA to communicate with a secure connection via wireless network. While their paper did not use the same modeling that we employ here, it provided a solid foundation for an experimental structure. Their work made an attempt to analyze trade-offs between security and energy, but focused primarily on the key-sizes of encryption algorithms rather than the security of the protocol as a whole.

Karri et al.[4] also had a related work, although they did not attempt to perform any trade-off analysis. In their work they measured the energy usage by the encryption algorithm, packet transmission, the reception of packets, and that of the idle state.They also examined the effect of compression on the power utilization.

The one missing element of the works cited above is an attempt to provide an analytic model across multiple protocols layers that can effectively explained the energy wastage imposed. Colon Osorio, et.al., attempted to correct this situation by introducing the concept of security vs. energy tradeoffs. For example, if known security techniques from the "Wired-World", such as Authentication and Ticketing servers (e.g., Kerberos IV, V) are used, then, power utilization of the device will necessarily go up. Upon such a consideration, it becomes clear that there exist a tradeoff between security, as measured by some metric, S, which captures the security or protection provided by protocol and the incremental energy consumption required, albeit in the case of flawed protocols the expenditure of additional energy does not guarantee increased security.

As stated previously in the introduction, we are concerned with the number of messages that must be passed during the authentication portion of the protocol. It follows that we need to take into account the amount of disassociation that occurs in a typical mobile session. Several studies have been conducted where students analyze the traffic of their campus network[5][3][9][1]. Tang and Baker traced wireless connections within buildings, as well as a metropolitan area network (MAN). Additionally, a study conducted by U.C. San Diego and Microsoft attempted to characterize user behavior with respect to wireless networks during a conference.

The most comprehensible and applicable of these studies are those by Kotz et al.[5][3] in 2002 and 2004. During their observations of wireless activity on the Dartmouth campus, they gathered sufficient information to identify clients roaming between access points. In their 2004 study, they found that half of all wireless clients roamed between access points. In their previous study, only one third of the clients roamed. Indeed, they found that the number of wireless clients overall and the percentage of those that were mobile had increased in two years. This observation of the rise in roaming sessions supports our claim that the cost of reassociation needs to be factored into energy measurements.

The key problems in this area are twofold. First, the problem of how to measure security is a difficult one. A logical approach will be to used Shannon's concept of "operational security". However, the problem of defining a measure of security across multiple layers of a wireless protocol is significantly more difficult. The difficulty lies in the definition of what " *e a a ec* " means, and how to quantify it.

Secondly, there is the challenge of measuring the energy consumed across multiple protocol layers. Given such challenges, the approach we follow here, is to first create a model that will allow the computation of the energy wastage per security level obtained analytically. Having established such a model, then you can measure on the actual devices the energy consumed using different protocols. In this paper, the analytical framework in [2] will be used, and a set of popular security protocols will be evaluated using such a framework.

The remaining of this paper is organized as follows. In section 3 a summary of the limitations with wireless security protocols is presented. Section 4 presents the security-energy tradeoffs model. In section 5 the major contributions of our work are presented, while in section 9 a summary of the results and future work is presented.

3 Background: Current and Proposed Wireless Security Protocols

In this section, we present a brief summary of the currently used and proposed wireless protocols. Due to space constraints, we shall keep this review short but refer the user to [2] for a more detailed discussion.

3.1 Summary of 802.11 Protocol

In order to understand the security protocols available for wireless networks, let us first examine the 802.11 protocol. 802.11 is a MAC layer protocol which uses radio frequencies in unlicensed portions of the spectrum. Currently, those frequencies are 2.4 GHZ (802.11b and 802.11g) and 5 GHz (802.11a). The range of each radio's transmission creates a cell. If two access points are nearby, then there cells will overlap and a client may connect to either of them, but not both.

In order for a client to connect to an access point, it first has to authenticate. This authentication is performed by a challenge-response. If authentication is successful, the client then needs to associate with the access point. Should a client wander outside of its current cell, then it will be disconnected and need to associate again. During a mobile session, a client may travel from one access point to another within the same network. Here, the client will need to reassociate with the new access point. When the client resides in an overlap between two such access points, then it may constantly disassociate and reassociate as the signals fluctuate that change which is the stronger access point. Such reaasociations could have a significant impact on the energy consumption of different protocols, as it will be shown later.

3.2 How Does Security on a WLAN Differ from a Wired LAN?

The greatest factor that separates wired and wireless security is the concept of *ca ec* . Before WLANs, access to internal networks could be limited to those who were allowed to get in close proximity to machines on the network. Walls and doors protected unauthorized users from gaining access. Wireless signals leak outside these boundaries. In the earlier years of WLAN deployment, companies would put access points inside their firewalls, allowing anyone in range of the signal to crack their way in. This was known as the "parking lot attack". Presently, similar tactics are still being employed. "Wardriving" and "Warchalking" are still occurring. In these activities, the goal is to find an open network or breach the security, and gain access to the network.

Several wireless security protocols have been implemented or proposed in the last few years. Starting with the Wired Equivalent Privacy (WEP) protocol, the goal has been the same. That is, to create a way to ensure the same level of privacy for wireless communication as there is for wired communications. The reader is refer to [2] for an in-depth discussion of WEP, WPA, 802.11x, and the next Wireless Security Standard, whose current front runner is the Counter CBC-MAC Protocol (CCMP).

4 Analyzing Trade-offs Between Energy and Security

From the previous literature survey, it is clear that battery power is one of the most precious resources to a mobile client. Thus, it is important to understand the relevant energy and battery trade-offs involved in any protocol attack or its associated countermeasure. Specifically, each class of protocol attack leads to potential loss in efficient battery use. Similarly, any proposed countermeasure can provide a given level of security-reliability but will also requires an additional expenditure in energy by mobile nodes. At this point, we will refer to the security-reliability goal simply as security.

Colón Osorio et.al. in [2] first introduced a decision-theoretic model where the relationship between a given attack countermeasure and the level of security-reliability provided could be calculated. In addition, a relationship between the energy spent in carrying out a countermeasure and the energy level that is potentially lost if a given attack is successful was also discussed. For completeness, we now summarize the main features of this model. The model has two components. The first component involves the definition of an energy cost function, C^E. This energy cost function represents the amount of effort required for a countermeasure M_k against a protocol vulnerability V_i, or $C^E(M_k, V_i)$. Secondly, a security measure R_M, designed to capture the level of security obtained in the system by implementing a set of countermeasures is defined. Next, a *C e ea e E e Q e (CEQ)*, Q_M, is defined as the ratio of the security obtained for a set of countermeasures divided by the energy required to implement them. This *CEQ* as captured here by Equations 1 and 2 is in effect their security-energy tradeoff model.

$$C^E = \sum_i C^E(M_k, V_i) \tag{1}$$

$$Q_M = \frac{R_M}{C^E} \tag{2}$$

Notice that in equation 1 combinations of countermeasures may not be additive since some countermeasures may perform multiple functions and countermeasures may be correlated or interdependent. In order to compensate for this problem, they introduced a variable, A, which takes into account a specific attack on a vulnerability V_i. The energy consumed given in Equation 1 changes to $C^E(M_k, V_i, A)$. Next, consider $p(A_i^V|E)$ as the probability that the attack A on vulnerability V_i has occurred given some evidence, E. This evidence in practice could be incorrect checksums or protocol timeouts. Thus the expected energy consumption for all countermeasures is:

$$C^E = \sum_i p(A^{V_i}|E) C^E(M_k, V_i) \tag{3}$$

The above model is for single attacks on specific vulnerabilities. However, in real life, entire classes of attacks are possible on a given vulnerability. Thus, these classes of attacks are somewhat correlated and

the model should reflect this. Hence, a further modification was introduced. That is, a group of attacks S_j which is possible on a given protocol vulnerability is defined such that

$$C^E = \sum_i \sum_j p(A^{V_{ij}}|A^{S_j}, E)p(A^{S_j}|E)C^E(M_k, V_i) \tag{4}$$

4.1 Static Protocols - An Energy Consumption Perspective

Consider a simple protocol such as WEP or TKIP. These wireless protocols were designed to protect the system from three classical vulnerabilities, $V_1, V_2, and V_3$, where V_1 is the confidentiality or robustness of the cryptographic algorithm, V_2 is robustness of the integrity check (integrity); and V_3 is the robustness of the authentication, authorization and access protocol (availability)

Traditionally, the integrity checks and encryption have been grouped together, but for the purposes of our model they have been separated. Authentication, authorization, and access have been split despite the fact that they all are associated with availability. The reason behind this is related to message passing. Some protocols, such as WEP, group these operations into one. However, protocols exist where each of these steps requires a message. Protocols which use ticket granting mechanisms, such as Kerberos, are examples of this.

Further, the energy expenditure function associated with each countermeasures $M_1, M_2, and M_3$, $C^E(M_k, V_i)$ is defined by the protocol itself and the parameters used. For example, in WEP, the countermeasure against V_1 is simply the RC4 cryptographic algorithm. In this case, the energy expenditure to achieve the desire level of security is simply $C^E(K_{length}, V_i) = f(\#computationsinRC4)$. In this example, C^E can be easily calculated by multiplying the Number of computations required by RC4 times the energy consumed in joules by a single computation. Using Stemm & Katz approach, and these simplifications, Equation 4 can be expressed as in Equation 6:

$$Energy_{Total} = K_0 + \alpha_1 E_{cryp} + \ldots \\ \ldots + \alpha_2 E_{SendRcvd_{ap}} + \alpha_3 E_{SendRcvd_{tgs}} \tag{5}$$

5 Major Contributions

Our work formalizes the concept of operational security as a function of energy consumption in a wireless network. Operational security is similar to the concept of "practical secrecy" introduced by Shannon in his classical 1946 paper *Ma e a ca T e C a* . This concept is rather simple. That is, given a bounded time period $[\, t_0\, , t_0 + \delta\,]$, the system under consideration is operationally secure, iff, it can guarantee the confidentiality, integrity, and availability of the system with a probability, P_s, where, $P_s = 1 - P\{"BreakingtheSystem"\} = 1 - \epsilon$. Or conversely, if $P\{"BreakingTheSystem"\} = \epsilon$, where $\epsilon \to 0$.

The problem of defining such a measure of security across multiple protocols layers is significantly more difficult. The difficulty lays on the definition of what does "operational security" mean?, and how to quantify it. For example, if "the system" under consideration provides a set of services such as authentication, key distribution, and access to a set of distributed resources, then, "Breaking The System" will corresponds, at the very least, to "Breaking the Cryptographic Protocol". Hence, in order to apply the model described in section 4, one needs to answer the question of how secure is the cryptographic protocol?

Given such challenges, our approach is to first understand the model in terms of the energy utilization. Specifically, we will investigate energy consumption and wastage as it relates to security features. Two distinct approaches will be taken. First, we will study current and proposed extensions to security protocols for wireless networks. Evaluate the energy consumption associated with different services and attributes that the protocol provides using our energy-security model, and Equation 4. We will call this, intrinsic energy evaluations. However, in order for our analysis to be useful, we need *CEQ*, or Q_M, as in Equation 2, and hence, need a methodology for computing the security profile of a given wireless security protocol.

5.1 Security Proxy

To our knowledge, there is currently no theoretical or empirical means of measuring the security of a given protocol. In our work, we have derived a proxy as an estimate. Our proxy is an ordinal scale that ranks security profiles by counting vulnerabilities and the countermeasures against them, see Table 1. It is important to note that because this scale is a , the numbers have no meaning on their own. Meaning can only be obtained by saying $x\ R\ y$, where R is a relation. This also means that our quotient, Q_M, is on an ordinal scale.

In our approach, the aspects of each protocol are rated against the classic categories of attacks. If it withstands the attack, then it receives a 1 in that category. If not, then it receives a 0. For vulnerabilities that are not simply a 'yes' or 'no', but vary in diffi-

Vulnerability		64-bit WEP	128-bit WEP	CKIP+MMH	WPA-LEAP	AES-CCM
encryption	key not renegotiated when exhausted	0	0	0	1	1
	known (practical) attacks on cipher	0	0	0	0	1
	key discovery through packet collection	0	0	1	1	0
	key size (key size)/(highest keysize in these profiles)	5.42101E-20	1	1	1	1
	keyspace (packets till key exhausted)/(keyspace in max profile)	4.93038E-32	4.93038E-32	1	1	1
integrity	birthday attack	1.52588E-05	1.52588E-05	1.52588E-05	0.125	1
	origin not protected	0	0	0	0	1
	bit-flipping attack	0	0	1	1	1
	anyone can compute	0	0	1	1	1
authentication & authorization	authentication without secret	0	0	0	0	1
	open authentication allowed	0	0	0	1	1
	authenticate hardware, not person	0	0	0	1	1
		1.52588E-05	1.000015259	5.000015259	8.125	11

Table 1: Security proxy

culty, such as brute force and birthday attacks, ratios are used to assign a number between 0 and 1. This method of comparison assumes that all vulnerabilities are equal. This is not an accurate assumption, as some vulnerabilities are worse than others. For instance, one vulnerability may only allow blocks of a message to be rearranged so that the resulting message is gibberish, while another vulnerability may render the network unusable. Clearly, the latter has a more severe impact than the former. While our assumption is not true in practice, we believe that our proxy is sufficient for purposes of illustrating the model.

5.2 Intrinsic Energy Model - 1^{st} Results

Me : In section 4, we introduced the Security-Energy model. In order to effectively use such model, we would like to apply the closed-form analytic solutions presented in Equations 1,2, 3, 4, to a set of wireless security protocols such as WEP, TKIP, TKIP enhanced by CISCO proprietary authentication protocol LEAP, and others. As a first step, we need to understand the energy consumed on a per block transfer for each one of the protocols under consideration. Here, we break down each protocol into the primitive operations required to accomplished a single transfer. This was accomplished by reviewing the Standards in question, drafts, RFCs, and textbooks. Available pseudo-code and explanations from these sources were used to create tables recording the number of occurrences of operations used by each protocol.

However, data dependencies greatly affect the number of operations used to accomplish a block transfer. For this reason "real world" parameters were needed in order to establish a bound on the number of computations. One such case, where real data was required, is EAP-TLS. In this particular case, we used the firefox web browser with TLS enabled and SSL disabled while a secure connection to amazon.com was established. This transaction was captured with the Ethereal network protocol analyzer. The length of each message was then used to compute the number of operations of the corresponding TLS message during EAP-TLS authentication phase.

Using the information provided by these tables, and the energy consumed on a $\frac{joules}{computation}$, we can compute the total energy overhead per block of information transferred, E_{total}, as given in Equation 6. The exact value of $\frac{joules}{computation}$ varies depending on several critical parameters. These are: (1) Type of computation used in a particular encryption algorithm; and (2) The specific implementation of both the wireless network card and access point; and (3) The hardware/software tradeoff selected by the particular vendor to implement the encryption algorithm.

Here, we will use the industry standard metric of $\frac{joules}{mac}$. Recently, Fuller has shown that today state of the art DSP spends about one-(1) milliwatt per million of MAC's (multiply and accumulate) operations or 10^{-15} joules per single MAC. Using, modern DSP processors as the basis for energy consumption in our analysis, and our earlier estimates of the number primitives operations, we can now compute the total energy utilization as required by Equation 4.

6 Analytical Study

The first part of this research consisted of an analytical study involving WEP, WPA, and CCMP. Each of the computational algorithms was examined for a specified packet size based on RFC information and observations. This study provided insight, but was clearly not sufficient.

In order to perform a valid analysis, we obtained code for 802.11i from an IEEE member David Johnston (https://www.deadhat.com/wlancrypto). This code includes C files for CCMP MPDU encryption, TKIP key mixing, RC4, and Michael. This code was created to follow the algorithms described in the drafts exactly, not implement any efficiency improvements.

Based on these algorithms, we studied, the energy costs associated with encryption operations. From this work, [2], we can see that for encryption only, AES is the cheapest in terms of computation, while WEP and TKIP required almost the same amount of energy. This is a because both WEP and TKIP use the RC4 stream cipher, and TKIP only adds a little extra computation for the key mixing.

When the integrity check is factored in, AES and TKIP become the most expensive in terms of energy consumption. This is due to the relatively high cost of the integrity function to that of WEP's.

In addition, we conducted and earlier analysis which contained an estimation of authentication costs, shown in figure 2. Unfortunately, the EAP authenti-

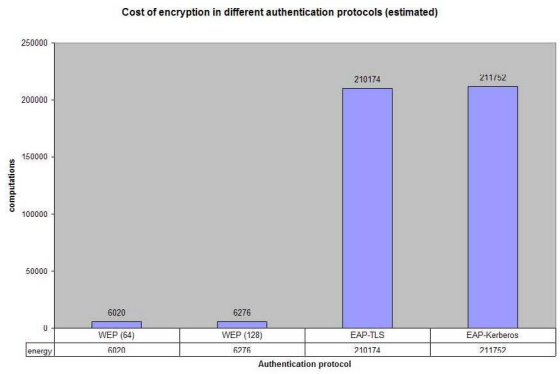


Figure 2: Costs associated with availability countermeasures

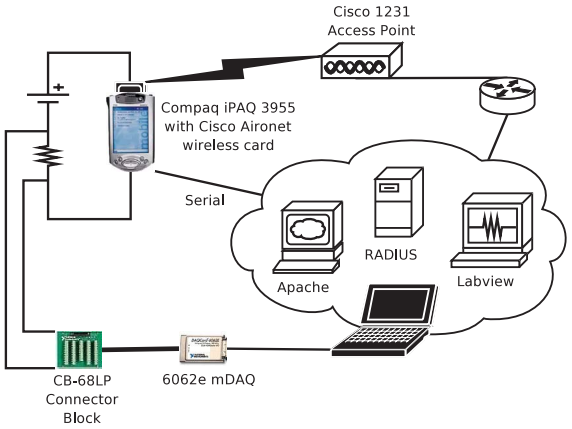


Figure 3: Experiment setup

cation methods that we selected in this analysis were not included in the experiment due to lack of support. However, we can still see that the cost of EAP methods is far greater than that of WEP's authentication.

Based on this preliminary analysis we quickly concluded that the most significant element affecting the energy consumption of a wireless device security protection mechanism will be those associated with authentications. Similarly, we speculated that there will be very little differences across cryptographic protocols from an energy consumption perspective. While only one authentication is required to start a session, weak signals, reassociation, and roaming can all cause more authentications to take place. Therefore, it can be assumed that a session may have multiple authentication handshakes.

6.1 Experimental Design

In order to verify our hypothesis, an experiment was constructed for the basic scenario where we have a mobile device that wishes to retrieve a web page via the wireless channel. The test bed, depicted in figure 3, consists of a wireless client (supplicant), access point (authenticator), and RADIUS server (authentication server). The test bed was completely isolated from our internal network in order to prevent interference and uncontrolled events. To prevent others from accidentally connecting to our test bed, we disabled beacon messages from being transmitted by the access point and enabled MAC filtering.

Power measurements were obtained using Labview 7.1 by National Instruments. This product obtains signals via a data acquisition (DAQ) card that connects to the PC. For this experiment, we used a 6062E multi function DAQ card with a CB-68LP connector block. A Radio Shack Universal Breadboard was used for all wire connections.

In order to determine the power consumed, Labview measured the voltage drop over a 0.47 Ohm resistor to determine the current. Using Joule's law we can determine the total power consumed (in Watts) during the measurement period. First, the current at each point (the sample rate is 1 millisecond) is measured. The area under this curve is calculated and the total energy (Joules) used to perform each transaction is then calculated.

In our experimental design, the iPAQ is connected directly to the measurement system via an out of band serial port. This allows us to send signals at the start and stop of each transaction, isolating the exact period that our transaction takes place. To measure the cost of disconnection and reassociation, we use the access point command line interface to kill the connection between itself and the client.

6.2 Experimental Design - the Software Environment

Apache 2, distributed by the Apache group, was chosen as the web server for this experiment. Apache is one of the most commonly used web servers, and is free under the GPL. Our server runs a basic installation which does not include CGI processing or additional features, such as SSL.

In our experiment, Ethereal was used as the packet analyzer to capture TCP and UDP traffic. This was necessary for verification that transactions were completing properly, and was exceedingly useful for troubleshooting. TCP traffic was observed to verify HTTP requests and responses, while UDP captures were used to verify RADIUS transactions.

The PDA runs a special browser tailored to our

research objectives. The browser is extremely basic - it was designed with only three functions:

- send get requests to our web server
- receive and display ASCII representation of objects
- send a signal to Labview at the start and end of every transaction

The address bar is a drop-down list of all the possible pages in the experiment. This removes the need to type in the URL for each scenario, therefore increasing speed and reducing error rate. Once the URL has been selected and the download button has been pressed, the application sends a start signal to Labview, retrieves all objects associated with the URL, and then sends Labview a stop signal. A message is displayed in the single-line text area indicating whether or not the page was successfully downloaded. The multi-line text area displays the ASCII representation of each object.

This application was developed using Microsoft Embedded Visual C++. This development environment was selected due to its integration with Microsoft ActiveSync, Microsoft Foundation Classes (MFC), and a variety of sample applications.

Once waveforms were obtained, they were run through two perl scripts. The first script, `power.pl`, calculates the power consumed in each run. The second script, `average.pl`, finds the average of the power expenditure in two different ways - over the entire data set, and over the IQR. There were often runs that were un usually long and greatly affected the results, so the IQR average was the one used for our measurements.

The RADIUS (remote authentication dial-in user service) software selected for this project was Funk Steel-belted RADIUS Enterprise Edition (SBR EE). The selection of this software was based on the supported inter operability with Cisco's products and proprietary protocols (LEAP and EAP-FAST). However, no EAP-FAST functionality could be found. Cisco Systems claimed that SBR EE supported EAP-FAST, but nowhere in Funk's documentation could we find a way to enable it. The authentication methods supported by Funk are LEAP, MD5-Challenge, TLS, and MS-CHAP-V2.

There were three different wireless client programs installed on the PDA, Cisco's Aironet Client Utility (ACU), Funk Odyssey Client for PPC 4.0beta, and the Meetinghouse AEGIS client. The reason for multiple clients lies in the authentication support provided by each one. ACU could not be removed, as doing so also removed the driver for the wireless adapter. The only EAP authentication methods supported by this device are LEAP and EAP-FAST, which could be used in both open and WPA association modes.

Funk's Odyssey client added support for WPA, however, it would not associate with the access point. Upon examination with Ethereal, the problem seemed to lie in the client or AP. The RADIUS server sent the RADIUS ACCEPT message, but the client would always disconnect and start the authentication process over. Odyssey could clearly not be used with WPA, however, it did offer more authentication methods to be used with open 802.1x authentication. Although several other methods were configurable, only MD5-Challenge was common between it and SBR EE.

The AEGIS client also had difficulty with association methods other than open and shared, and was not used in testing. It did not add any configurations that we could not accomplish with the other two client programs, and had the worst interface. It did not give much feedback, making it very difficult to determine what was happening.

6.3 Experimental Design - Workload

In any experimental setup of this nature, it is important to capture data while executing workloads which are "closely" representative of actual Internet traffic. Fortunately, over the last several years researchers have studied the problem of accurate representation of Internet workloads. In general, the network community has settled on a model for network traffic which goes under the name of "mice and elephants". In this model, mice are small objects that are transferred often, such as text messages, TCP acknowledgments, etc. Elephants are large objects, such as multimedia files, of which there are fewer occurrences.

Several studies have been conducted which examine network loads and their effects on performance. One such study out of the University of Washington[8] was used to construct the data transmitted during our experiment. In their research, Saroiu et al. compared HTTP traffic over various applications, such as WWW, Kazaa, and Gnutella. For this experiment, we are only focusing on WWW traffic, since surfing the web is a common use of mobile devices. The data from this study became the basis for our workload creation. In effect, we set out to reproduce a workloads which highly correlates the type of objects and traffic experienced by Saroiu, et al.[8] while at the same time making it possible to understand the behavior of a handheld device. For each object, we use the number of requests reported as a percentage of the top

workload name	object size (KB)	workload construction
text2	2	single 2KB text-only HTML file
text5	5	single 5KB text-only HTML file
text9	9	single 9KB text-only HTML file
text10	10	single 10KB text-only HTML file
text20	20	single 20KB text-only HTML file
text30	20	single 30KB text-only HTML file
text40	40	single 40KB text-only HTML file
2img	2	48 <img src=...> in HTML file
5img	5	22 <img src=...> in HTML file
9img	9	22 <img src=...> in HTML file
10img	10	2 <img src=...> in HTML file
20img	20	2 <img src=...> in HTML file
30img	30	1 <img src=...> in HTML file
40img	40	1 <img src=...> in HTML file

Table 2: Workload

ten objects in the study as a proxy for the number of instances that object should appear in our workload. Once this was done, three types of pages were constructed to model the Internet:

- text-only pages
- text and many smaller images
- text and fewer larger images

The text-only pages are stand-alone (call no additional objects), and there is one page for each object size listed in table 2. Seven image pages were constructed for this experiment, also based off the numbers in table 2. The HTML pages are the bare minimum, containing only the basic opening and closing HTML tags and the img tags necessary to request each image. The number of times that an image is called from its accompanying page corresponds with the instance field of table 2.

The images used for this experiment were created using Adobe Photoshop Elements. All images are based on the same basic image, but vary in the title layer (which labels the image with it's size for easy identification) and the final dimensions and quality. After each image was finished as a .psd file, it was exported for the web as a jpeg file. In order to achieve the desired file size, the image dimensions and jpeg quality were altered until the file size needed was achieved.

7 Empirical Results

7.1 Empirical Results - Encryption

Figure 4 depicts our measurements of workload transfers when varying the encryption cipher. For these measurements, the client adapter was configured using the Cisco ACU. All measurements are taken *a - e* the client was authenticated and associated, so they convey only the cost of confidentiality and integrity countermeasures.

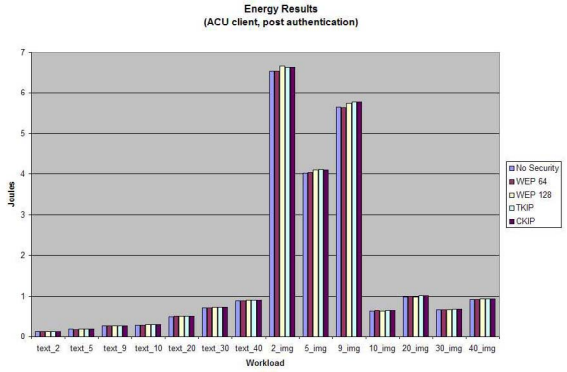


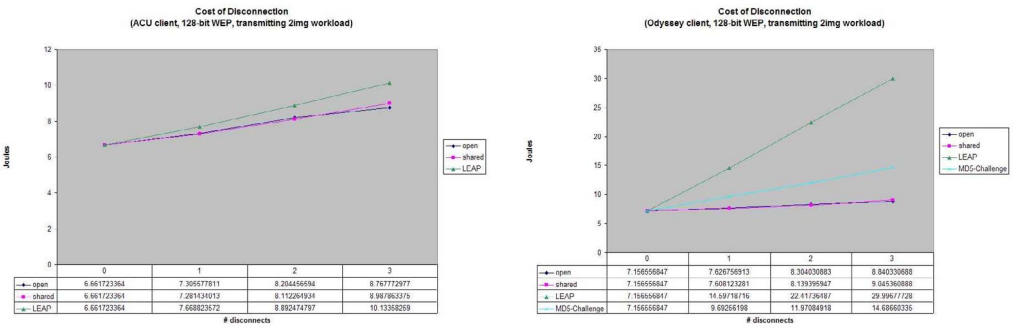
Figure 4: Energy used over workloads after association established

From this data, we can see that the impact of encryption on the battery life is very minimal. Workloads which only requested one object, namely the text-only workloads, showed trivial energy differences between profiles. This is not a surprise, as all of the ciphers shown here are based on the RC4 stream cipher and RC4 is very cheap in terms of energy. In the workloads that require more requests, specifically the 2img, 5img, and 9img workloads, you can see how the different variations on WEP affect the total energy consumed. In these workloads we can see how the 128-bit ciphers break further away from the rest. The cost of 64-bit WEP remains very close to that of no security. Hence, from an encryption algorithm perspective the user is well advised to use the larger key sizes without suffering any significant impact on the battery life of the device.

7.2 Empirical Results - Authentications

Mobile clients do not necessarily stay connected to the same access point during an entire session. Several factors may cause disconnection to occur. The client may wander outside the range of the access point, the AP may deauthenticate when the authentication period expires, the connection may be dropped due to low signal strength, etc.

In order to see the difference in cost of disconnection, we studied three different authentication types: open, shared, and LEAP. LEAP was configured without WPA key management, as WPA requires TKIP or AES-CCM as a cipher. Additionally, we could not perform open and shared authentication with TKIP or AES-CCM. Therefore, WPA measurements are not grouped with these results. As anticipated, the differences between open and shared authentication are trivial. To close the connection, we deauthenticated



(a) ACU client

(b) Odyssey client

Figure 5: Transfer of 2img workload with disconnection

the client through the AP's CLI. We took measurements using two different clients, Cisco ACU and Funk Odyssey client, as Odyssey supported additional EAP methods. The results are shown in figures 5(a) and 5(b), respectively.

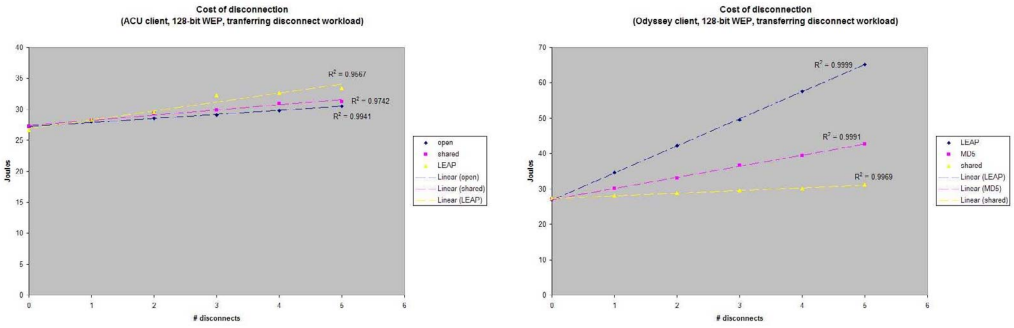
Both clients consume approximately the same amount of energy for open and shared authentication. However, in figure 5(b), the cost of LEAP authentication is significantly greater than in figure 5(a). MD5-Challenge EAP authentication may not be compared between the clients, as ACU does not support this method.

In order to gain an insight into the additional energy consumed due to roaming or dis-associations from the access point a new workload need to be created, the disconnect workload. Simply, even our longest session workload, the 2img workload, did not remained connected long enough to understand this problem. This workload was simply an extended version of 2img which latest through 7 disconnections. However, due to time constraints, only 0-5 disconnections were recorded. The results are shown in figures 6(a) and 6(b). These graphs also contain trend lines and correlation coefficients. From this graphs we note that the Odyssey client consumes significantly more energy than the Cisco ACU for LEAP authentication.

In order to understand the reason for the seemly lightweight nature of the Cisco client, we collected several traces during disconnection of clients. The traces captured on the wired side (between the access point and RADIUS server) showed no differences between the number and nature of packets transmitted. For the wireless channel, we used an Orinoco wireless card on a laptop running the Knoppix STD distribution. This configuration allowed us to put the card into promiscuous mode and monitor the traffic exchange between the PDA and access point.

We collected 10 traces for each client. What we found is that the time between the reassociation request and subsequent WEP-encrypted packet occurred 3 to 4 seconds apart with the Odyssey client, but only 1 and 2 seconds apart with the ACU client. Although ACU sent more packets (because of the LLC transaction), it completed about 1 to 2 seconds faster than Odyssey. From these traces we can then conclude that the differences between the two clients is due solely to idle time parameters between requests. Figure 7 shows the results of measurements while the 2img workload was transferring, the client adapter was configured with the Odyssey client, and the PDA had Pocket PC 2002 as its OS. This graph varies greatly from figure 5(a), and looks similar to figure 5(b). However, the cost of LEAP in figure 7 is almost double that of the cost in 5(b). We believe that the reason behind this result lies in the 802.1x support. PPC 2002 requires that a program called "802.1x Backport" be installed to use EAP authentication. However, Windows Mobile 2003 includes 802.1x support in the operating system.

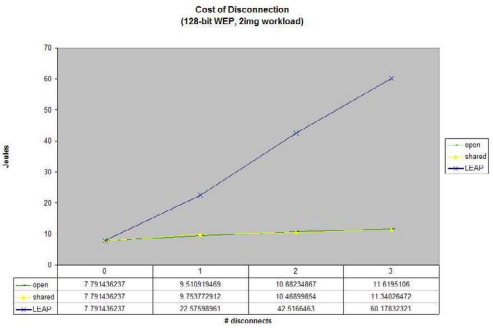
As discussed in the analysis, we can assume that multiple authentication exchanges may take place. In fact, a study of a campus WLAN[5] showed that 18% of sessions roam at least once. Of those sessions, 60% roamed within a subnet, which means that they had to reauthenticate with a new access point, but kept the same IP address. The remaining 40% had to undergo the complete association in addition to DHCP process.



(a) ACU client

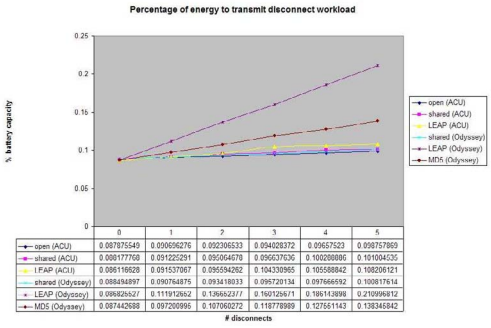
(b) Odyssey client

Figure 6: Transfer of disconnect workload with disconnection



	0	1	2	3
open	7.791436237	9.510919469	10.68234867	11.6195106
shared	7.791436237	9.753772912	10.46899854	11.34026472
LEAP	7.791436237	22.57688961	42.51666463	60.17832321

Figure 7: Transfer of 2img workload with disconnection (Pocket PC 2002, Odyssey client)



	0	1	2	3	4	5
open (ACU)	0.087875549	0.090696276	0.092306533	0.094028372	0.09657523	0.098757869
shared (ACU)	0.088177768	0.091222251	0.095064678	0.096537636	0.100208886	0.101004535
LEAP (ACU)	0.086116628	0.091537067	0.095594262	0.104330965	0.105588842	0.108206121
shared (Odyssey)	0.088494897	0.090764875	0.093418033	0.095720134	0.097666892	0.100617614
LEAP (Odyssey)	0.088626527	0.111912652	0.136622177	0.160120671	0.18511898	0.210996812
MD5 (Odyssey)	0.087442688	0.097200995	0.107060272	0.118778989	0.127651143	0.138346842

Figure 8: Percent of energy consumed by transfer of disconnect workload with deauthentication

7.3 Empirical Results - Effect on Battery Life

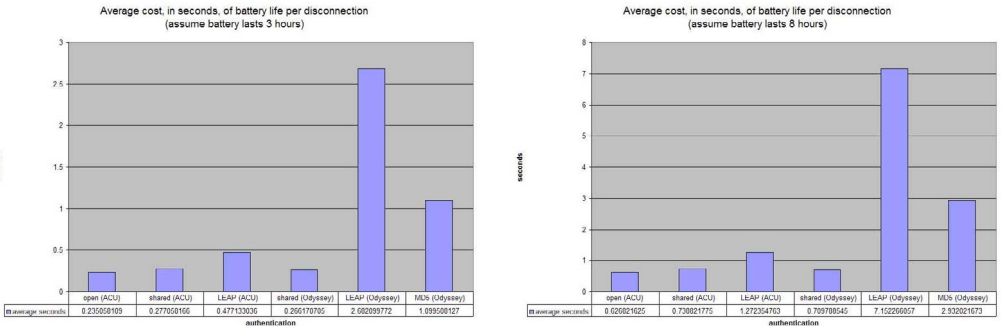
The primary battery on our handheld device has a life of 1400mAh. The use of the wireless card requires that the expansion pack also have a battery, which provides an additional 920mAh. Both are rated with 3.7V. This accounts for an energy capacity of 30,902.4 Joules. This computation of battery capacity holds true iff battery follows a linear dissipation rate. In practice the dissipation rate of a battery varies with discharge rate, temperature, and other critical factors. However, such variants do not have a significant impact in our analysis, hence. We will assume a linear dissipation rate. With these capacity values, we can now estimate the percentage of the battery that was consumed during our experiment. Because we do not have the discharge rate available, we will assume that the battery is at full capacity for each calculation.

	open (ACU)	shared (ACU)	LEAP (ACU)	shared (Odyssey)	MD5 (Odyssey)	LEAP (Odyssey)
% battery capacity	0.0021	0.0027	0.0046	0.0024	0.0102	0.0248

Table 3: Percent battery used per reauthentication

Figure 8 depicts the percentage of the battery's total energy consumed while transferring the disconnect workload, with 0 to 5 disconnections occurring. From these results, we can determine the approximate cost, in terms of battery percentage, for each reauthentication. These approximations are shown in table 3.

We can see that open authentication with the ACU client has the lowest energy cost, at 0.0021%. The client would have to be disconnected approximately 47,000 times in order for the entire battery to be used. On the other end of the spectrum, LEAP authentication with the Odyssey client uses 0.0248% of the battery for each authentication. Under this profile,



(a) Total battery life of 3 hrs

(b) Total battery life of 8 hrs

Figure 9: Impact of DisAssociations on a device with limited battery life

4,000 disconnections will utilize the entire battery. In practice, both of these numbers would be lower as the battery capacity will reduce with each disconnection, and the battery will discharge at a faster rate. However, we can still see that LEAP with the Odyssey client exhausts that battery in the order of 10 times faster than open authentication.

The cost of each disconnection, in terms of time, is dependent on the frequency of usage. A PDA, for example, may last 12 days without charging if it is not turned on. If it is in constant use, however, it may only last 3 hours. Figures 9(a) and 9(b) give estimates of the time cost of each disconnection, assuming 3 and 8 hours of battery life, respectively. These graphs show the average delta between disconnection measurements, not the cost of transferring the workload with disconnection. In this data, we see that the authentication profile that consumes the greatest amount of energy only takes seconds off the battery life. It also shows that the longer the battery life, the greater the energy impact of each reauthentication. Longer usage will all require more authentication, as authentication expires after a fixed amount of time. Therefore, authentication will tend to have a higher cost when the mobile device must be in use for longer periods of time.

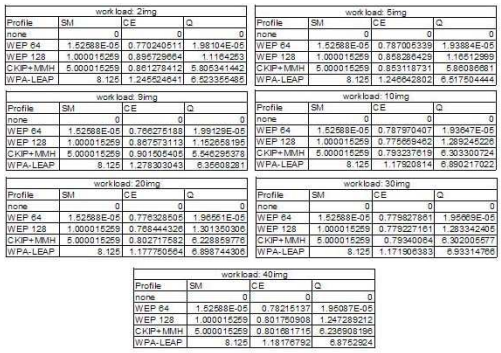
8 Trade-off Model as Applied to Wireless Protocols

In section 7, we measured the impact of the encryption protocol as well as that of re-authentications on the overall energy consumption of a mobile wireless device. These measurements become the foundation upon which our security-energy tradeoff model can be put to use. In Figure 9, the *C e ea e E e Q e (CEQ)*, Q_M, has been computed for the following security protocols: (1) open transmission, aka none, (2) WEP-64, (3) WEP-128, CKIP plus MMH, and WPA-LEAP. In all cases Q_M is computed for a single transaction composed of an authentication request followed by a single http transfer for each of our workloads. The WEP results assume shared key authentication. In all cases, the quotient follows our intuition in the sense that more secure profiles have higher countermeasure-energy quotient values. Of course, these results are highly dependent on our proxy, and trends may change with a more comprehensive and accurate measure of security.

Examining the results for workload "20img", we can see how putting restrictions on parameter values yields the most appropriate protocol. If the application at hand were to be limited to 1J per transaction, then CKIP with MMH would be the best choice, as it gives the most security for that energy constraint. On the other hand, if the application at hand required a minimum security profile with a value of 5 in our scale, then the best option would be WPA with LEAP authentication. Combining these two constraints for a given application so that both a minimum profile of 5 a maximum energy consumption of 1J were required, then CKIP+MMH would be the only option available to that application. Similar results to these were found when Q_M was computed where transaction were based on text-only workloads.

9 Summary and Future Work

In this manuscript, we reviewed the current limitations of security protocols associated with 802.11 networks. In addition, we applied the general model



workload: 2img

Profile	SM	CE	Q
none	0	0	0
WEP 64	1.52588E-05	0.770240511	1.98104E-05
WEP 128	1.000015259	0.895729664	1.1164253
CKIP+MMH	5.000015259	0.861278412	5.805341442
WPA-LEAP	8.125	1.245524541	6.523355485

workload: 5img

Profile	SM	CE	Q
none	0	0	0
WEP 64	1.52588E-05	0.787006339	1.93884E-05
WEP 128	1.000015259	0.858286429	1.16512969
CKIP+MMH	5.000015259	0.853118731	5.86086681
WPA-LEAP	8.125	1.246642802	6.517504444

workload: 9img

Profile	SM	CE	Q
none	0	0	0
WEP 64	1.52588E-05	0.766275188	1.99129E-05
WEP 128	1.000015259	0.867573113	1.152658195
CKIP+MMH	5.000015259	0.901505405	5.548295378
WPA-LEAP	8.125	1.278303043	6.35608281

workload: 10img

Profile	SM	CE	Q
none	0	0	0
WEP 64	1.52588E-05	0.787970407	1.93647E-05
WEP 128	1.000015259	0.775669452	1.289246226
CKIP+MMH	5.000015259	0.793237619	6.303300724
WPA-LEAP	8.125	1.17920814	6.890217022

workload: 20img

Profile	SM	CE	Q
none	0	0	0
WEP 64	1.52588E-05	0.776328505	1.96551E-05
WEP 128	1.000015259	0.768444326	1.301350306
CKIP+MMH	5.000015259	0.802717582	6.228859776
WPA-LEAP	8.125	1.177756564	6.898744306

workload: 30img

Profile	SM	CE	Q
none	0	0	0
WEP 64	1.52588E-05	0.779827861	1.95669E-05
WEP 128	1.000015259	0.779227161	1.283342405
CKIP+MMH	5.000015259	0.79340064	6.302005577
WPA-LEAP	8.125	1.171906383	6.93314766

workload: 40img

Profile	SM	CE	Q
none	0	0	0
WEP 64	1.52588E-05	0.782151327	1.95087E-05
WEP 128	1.000015259	0.801760908	1.247289212
CKIP+MMH	5.000015259	0.801681715	6.236908196
WPA-LEAP	8.125	1.18176792	6.8752924

Figure 10: Trade-off model as applied Image Intensive workloads

presented in [2] to help us understand how the current set of security related protocols, such as WEP, TKIP, AES, as well as several authentication schemes being actively considered, affect the energy consumption of the devices. Preliminary results confirmed our initial hypothesis that the effect of the encryption algorithm alone would not have a significant effect on the total energy consumed by the protocol across varying workloads. However, the cost of authentication, due in great part to dis-associations, did have a significant impact. Amongst all protocols, EAP methods which are considered to provide a higher level of security tend to have the highest energy consumptions costs.

The most significant result of our works points out the flaws associated with adopting security mechanisms from the wired-world in an effort to increase security. Such an approach could potentially have detrimental effects on the utility of the wireless device. Namely, it accelerates the depletion of battery life. Our work suggests that such consideration should be of importance moving forward in this area.

9.1 Future Work

The work presented raises several follow-up questions. Fundamental to this work, is the basic idea of cost/benefit analysis. Unfortunately, while several mechanisms exist (analytical tools, simulation, and empirical measurement) to quantify the costs (in terms of energy), measuring the benefits is significantly more difficult. For example, how does one go about answering the question how secure is the system, or how secure is the cryptographic protocol (not the algorithm itself)? Clearly, formal proofs can help in this area.

References

[1] Balachandran, A., Voelker, G. M., Bahl, P., and Rangan, P. V. Characterizing user behavior and network performance in a public wireless lan. In *P cee e ACM SI - MET ICS e a a c e e ce Mea e- e a e c e e* (2002), ACM Press, pp. 195–205.

[2] Fernando C. Colón Osorio, E. A., and McKay, K. Measuring tradeoffs between energy and security in wireless networks. In *P cee e I e a a Pe a ce C a C ca C e e ce, A - , - P e , A a* (April 2004), IEEE.

[3] Henderson, T., Kotz, D., and Abyzov, I. The changing usage of a mature campus-wide wireless network, 2004.

[4] Karri, R., and Mishra, P. Optimizing the energy consumed by secure wireless sessions: wireless transport layer security case study. *M b. Ne . A . , 2* (2003), 177–185.

[5] Kotz, D., and Essien, K. Analysis of a campus-wide wireless network. In *P cee e a a e a a c e e ce M b e c - a e* (2002), ACM Press, pp. 107–118.

[6] Lahiri, K., Raghunathan, A., Dey, S., and Panigrahi, D. Battery driven system design: a new frontier in low power design, 2002.

[7] Potlapally, N. R., Ravi, S., Raghunath, A., and Jha, N. K. Analyzing the energy consumption of security protocols. In *P cee e e a a L e e ec- c a e* (2003), ACM Press, pp. 30–35.

[8] Saroiu, S., Gummadi, K. P., Dunn, R. J., Gribble, S. D., and Levy, H. M. An analysis of internet content delivery systems. In *P cee - e S O e a S e De a I e e a* (Dec 2002), USENIX Association.

[9] Tang, D., and Baker, M. Analysis of a local-area wireless network. In *P cee e a - a e a a c e e ce M b e c a e* (2000), ACM Press, pp. 1–10.