Trade-offs Between Energy and Security in Wireless Networks[1]

By
Fernando C. Colon Osorio and Kerry McKay
Wireless Systems Security Research Laboratory
420 Lakeside Avenue
Marlborough, MA 01752
Phone: 508-490-7600, Fax: 490-07611
{fcco, kerrym} @ cs.wpi.edu

ABSTRACT

As the popularity of wireless networks increases, so does the need to protect them. In recent years, many researchers have studied the limitations of the security mechanisms that protect Wireless networks. There has also been much research in the power consumption introduced by the network card. Technologies such as CPU and memory are increasing and so is their need for power, but battery technology is increasing at a much slower rate, forming a ”battery gap” Because of this, battery capacity plays a major role in the usability of the devices. Although the effect of the network communication on a mobile device’s battery has been widely researched, there has been less research on the effect of the security profile on energy usage. In this manuscript, we examine a method for analyzing trade-offs between energy and security. This work extends previous work on the relationship between energy and the security of wireless communications in battery-constrained devices.

1. INTRODUCTION

The use of wireless networks has seen explosive grow in the last few years. 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 limitation is battery capacity. While memory and processor technologies roughly double every semiconductor generation, battery technology is increasing at the much slower rate of 5%-10% per year[1]. 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.

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. In this manuscript, we will use a model proposed by Colon Osorio et al.[2] to understand how security protocols affect the energy consumption of a mobile device. More specifically, we attempt to quantify how much additional power is expended in order to achieve a given security profile. This model will be used to evaluate WEP, WPA, 802.1x/EAP, and CCMP, see section 6. The protocols are first evaluated by analytical methods, 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. Security of the Wireless Channel: 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

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

phases: authentication, authorization, and access control; 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 transferred. This, leads to greater utilization of scarce resources. As we point out in section 3, an approach to get around this limitation is to investigate security from the perspective of effective resource utilization.

Power Limitations of Mobile Devices and their Impact on Security

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. 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, et al [3]. In their work, they examined the energy consumed by a PDA to communicate with a secure connection via wireless network.. Karri et al.[4] also had a related work, although they did not attempt to perform any trade-offs 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., [2], 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, and in a metropolitan area network [5], [6].

The key problems in this area are twofold. First, the problem of how to measure security is a difficult one. 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 we briefly present the security-energy tradeoffs model. In section 4, the major contributions of our work are presented, while in section 8, a summary of the results and future work is presented.

3. 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. Colon 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 *Countermeasure*

Energy Quotient (CEQ), $Q_{M,}$ was 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, 2, 3 and 4, and is in effect their security-energy tradeoff model.

$$C^E = \sum_i C^E(M_k, V_i) \qquad (1)$$

$$Q_{M,} = R_M \,/\, C^E \qquad (2)$$

$$C^E = \sum_i p(A^V_i | E)\, C^E(M_k, V_i, A). \qquad (3)$$

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

Here, $C^E(M_k, V_i, A).$, represents the amount of energy spend by a countermeasure M_k against a protocol vulnerability V_i, under a specific attack. Further, $p(A^V_i |E)$ represents the probability that an attack A on vulnerability V_i has occurred given some evidence, E. In the general case, Equation 4, the model is expanded to include classes of attacks $S_{j.}$

3.1 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 $C^E(K_{length}, V_1)$ = f (# computations in RC4). 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 5, below:

$$\text{Energy}_{\text{Total}} = K_0 + \alpha_1 E_{\text{cryp}} + \ldots$$
$$\ldots + \alpha_2 E_{\text{SendRcvd }\{ap\}} + \alpha_3 E_{\text{SendRcvd }\{rags\}} \qquad (5)$$

3. 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 *Mathematical Theory of Cryptography*. 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{"Breaking the System"} = 1- ε. Conversely, if P {"Breaking The System" } = ε, where $\varepsilon \to 0$.

The problem of defining such a measure of security across multiple protocols layers is more difficult. 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 evaluate the energy consumption associated with different services that the protocol provides using Equations 4,5. 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 4, and hence, need a method for measuring the security profile.

4.1 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 *ordinal*, 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.

5.0 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 authentication 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 would be those associated with authentications. Similarly, we speculated that there would 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.

5.1 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. Details of the experimental setup together with source files can be found on http://wssrl.org.

5.3 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. Here we will use the well-known “mice” (small objects that are transferred often, such as text messages) and “elephants” (large objects, such as multimedia files) model of Internet traffic to create a representative workload for our experimentation. This model together with results from empirical studies at the University of Washington, [7], yielded the workload presented here in Table 2.

6.0 EMPIRICAL RESULTS

6.1 Empirical Results - Encryption

Figure 3 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 after the client was authenticated and associated, so they convey only the cost of confidentiality and integrity countermeasures. 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.*

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 de-authenticate 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 de-authenticated 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 4(a) and 4(b), respectively. Both clients consume approximately the same amount of energy for open and shared authentication. However, in Figure 4(b), the cost of LEAP authentication is significantly greater than in Figure 4(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 disassociations from the access point a new workload needed to be created, the disconnect workload. 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 5(a) and 5(b). 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- (10) traces for each client during disconnection of the clients. The results showed that the differences between the two clients are due solely to idle time parameters between requests. Figure 6 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 4(a), and looks similar to Figure 4(b). However, the cost of LEAP in Figure 6 is almost double that of the cost in 4(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 re-authenticate 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.

6.2 Empirical Results - Effect on Battery Life

The primary battery on our handheld device has a life of 1400mAh, plus an additional 920 mAh due to the expansion pack. Both are rated at 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, 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. Lacking the discharge rate, we will assume that the battery is at full capacity for each calculation.

Figure 7 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 re-authentication. 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, 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.

7.0 Trade-off Model as Applied to Wireless Protocols

In section 6, 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. We computed the *Countermeasure Energy Quotient (CEQ)*, $Q_{\_M}$, 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. In examining the results for workload ``20img", we found that putting restrictions on parameter values yields the most appropriate protocol. For example, if the application at hand were to be limited to 1J per transaction, then our computations showed that 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 was 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.

8.0 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 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 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.

10. REFERENCES

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

[2] Fernando C. Colon Osorio, E. Agu., and McKay, K., Measuring tradeoffs between energy and security in wireless networks. In 24th International Performance Computing and.Communications Conf., April 7-9, 2005 - Phoenix, AZ.

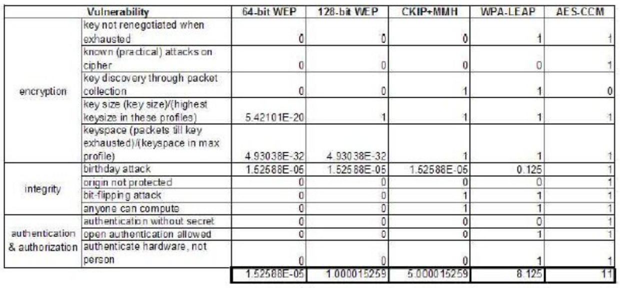
[3] Potlapally, N. R., Ravi, S., Raghunath, A., and Jha, N. K. Analyzing the energy consumption of security protocols. In Proceedings of the 2003 international symposium on Low power electronics and design (2003), ACM Press, pp. 30-35.

[4] Karri, R., and Mishra, P. Optimizing the energy consumed by secure wireless sessions: wireless transport layer security case study. Mob. Netw. Appl. 8, 2 (2003), 177-185.

[5] Kotz, D., and Essien, K. Analysis of a campuswide wireless network. In Proceedings of the 8th annual international conference on Mobile computing and networking (2002), ACM Press, pp. 107-118.

[6] Tang, D., and Baker, M. Analysis of a localarea wireless network. In Proceedings of the 6th annual international conference on Mobile computing and networking (2000), ACM Press, pp. 1-10.

[7] Saroiu, S., Gummadi, K. P., Dunn, R. J., Gribble, S. D., and Levy, H. M. An analysis of internet content delivery systems. In Proceedings of the 5th Symposium on Operating Systems Design and Implementation (Dec 2002), USENIX Association



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

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

	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: Percentage Battery capacity used per re-authentication

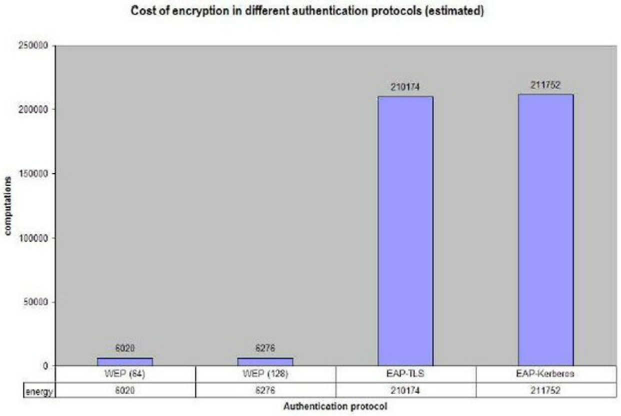


Figure 2: Costs associated with countermeasure of type: availability

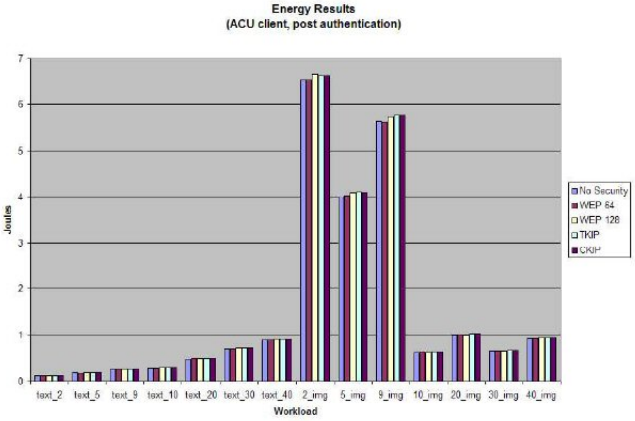
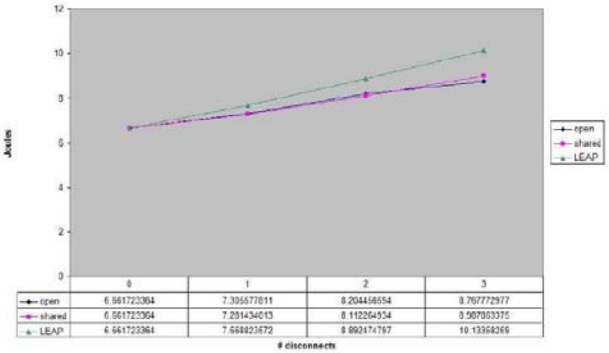
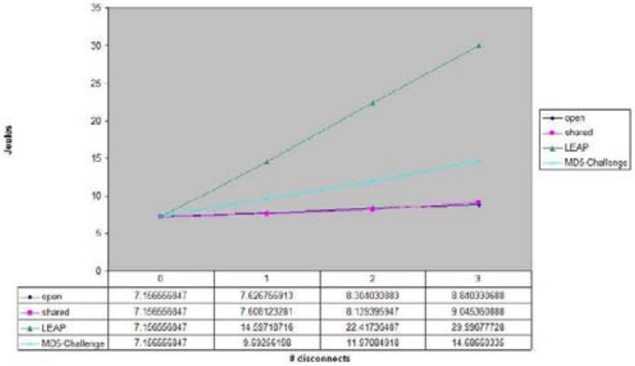


Figure 3: Energy used, post association, per workload



	0	1	2	3
open	6.661723364	7.305677811	8.204456654	8.767772977
shared	6.661723364	7.281434013	8.112264934	8.987863375
LEAP	6.661723364	7.668823672	8.892474797	10.13368269

Figure 4(a): Impact of dis-associations on 2img workload - ACU client



	0	1	2	3
open	7.156656847	7.626756913	8.304030883	8.840330688
shared	7.156656847	7.608123281	8.139395947	9.045360888
LEAP	7.156656847	14.59710716	22.41736487	29.99077728
MD5-Challenge	7.156656847	9.69256109	11.97084918	14.68660335

Figure 4(b): Impact of dis-associations on 2img workload - Odyssey client

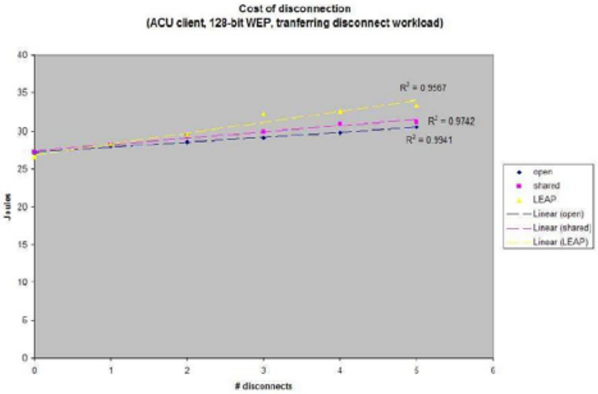


Figure 5(a): Effects of dis-associations on Disconnect Workload- ACU client

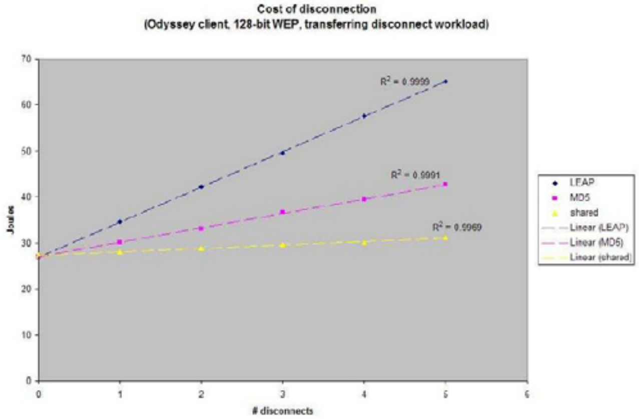
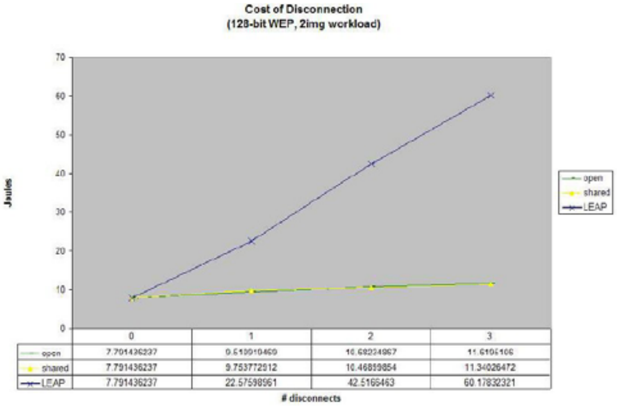


Figure 5(b): Effects of dis-associations on Disconnect Workload- Odyssey client



	0	1	2	3
open	7.791436237	9.510910469	10.68224967	11.6105106
shared	7.791436237	9.753772912	10.46859854	11.34026472
LEAP	7.791436237	22.57598961	42.5166463	60.17832321

Figure 6: Transfer of 2img workload with disconnection (Pocket PC 2002, Odyssey client)

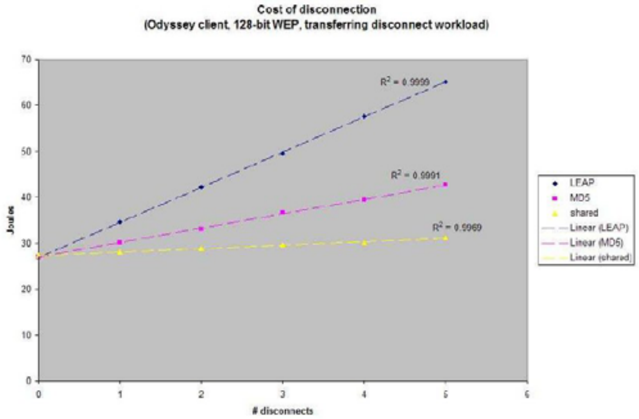


Figure 7: Percent of energy consumed by transfer of disconnect workload with de-authentication

Trade-Offs Between Energy and Security in Wireless Networks

Fernando C. Colon Osorio, Kerry McKay,
and Emmanuel Agu

WSSRL

Wireless System Security Research Laboratory

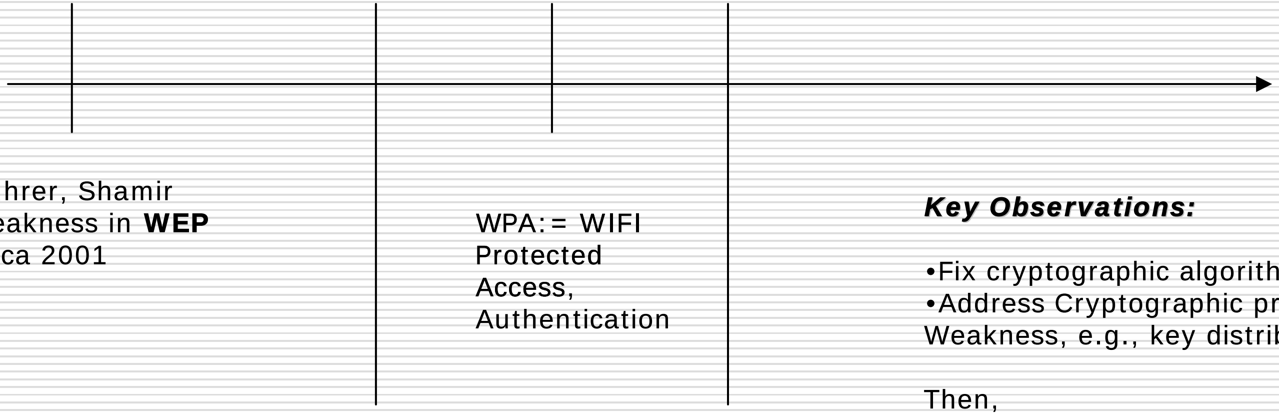
Outline

- The Problem
- Previous Work
- Our Approach
- Results

The problem

- □ Wireless devices are becoming more widespread
- □ Introduce insecurities not present in wired networks
  - Physical security
- □ Mobile device resources are limited
  - Less memory
  - Less processing power
  - Limited power supply (battery)
- □ Need to guarantee same security attributes as of those present in wired networks

Motivations



Fluhrer, Shamir
Weakness in **WEP**
Circa 2001

Quick, Fix it –
WEP 2 proposal,
Longer Keys

WPA:= WIFI
Protected
Access,
Authentication

802.11i –
Fix Key security
Problems:

Key Observations:

- Fix cryptographic algorithm
- Address Cryptographic protocol Weakness, e.g., key distribution

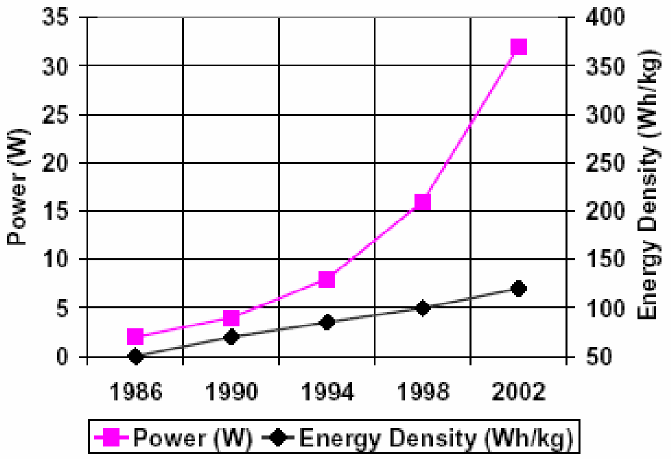
Then,

Throw everything at it:

- Radius Servers
- Public Keys
- AES
- More…

The problem (cont)

- Battery technology is increasing at a slower rate than technology
  - Causes a “battery gap” (Lahiri 2002)



- Need a way to make smart decisions about energy and security

Previous Work

- Stemm and Katz
  - Power use by wireless NIC in mobile handheld
  - Breakdown of transport-layer energy consumption

$Idle = I * b / B$

$Energy = SendRecv + Idle$

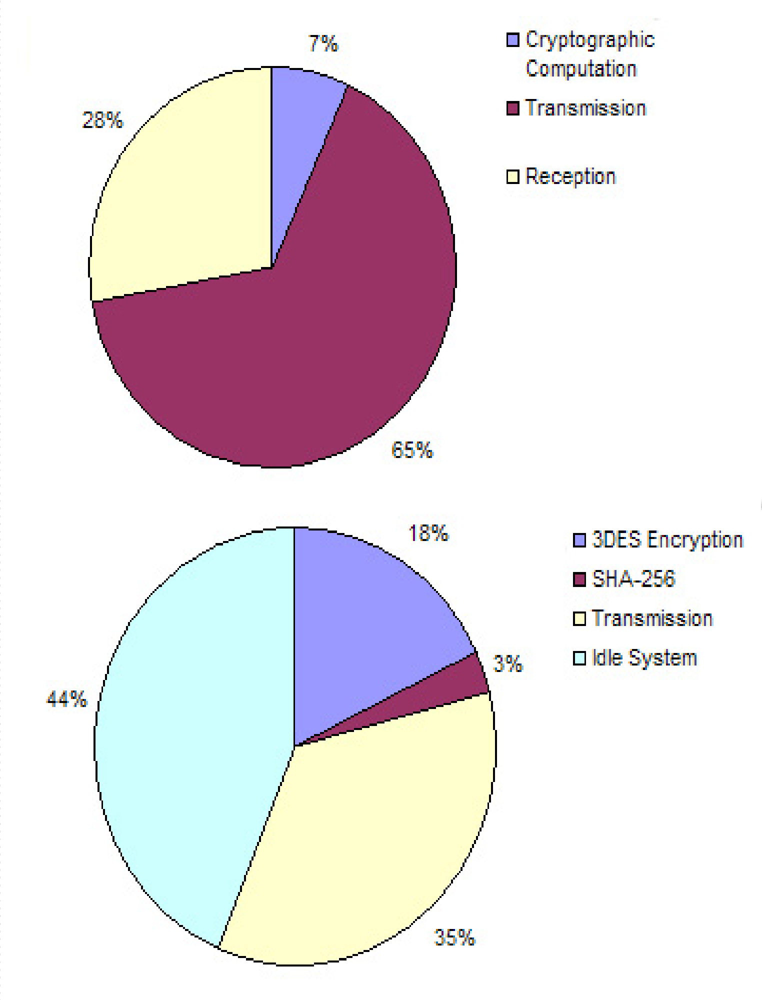
$SendRcv = aE_a + dE_d$

I = instantaneous power
b = # of bytes
B = bandwidth
a = # ack
E_a = energy to send a single ack
d = # data packets sent
E_d = energy to send a data packet

- Transmission the biggest source of power consumption
- Cost of reception very close to idle

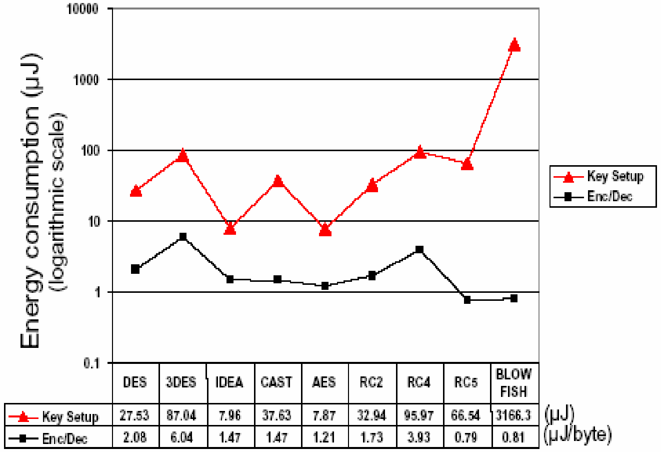
Previous Work (cont)

- Karri and Mishra
  - Examined energy consumed during secure wireless session
  - Energy breakdown during secure transaction (with 64KB data)
  - Effect of compression using DEFLATE algorithm
    - Cheaper to use energy to compress then encrypt than simply encrypt



Previous Work (cont)

- Potlapally et al.
  - Energy consumption of various cipher suites in a SSL transaction
  - Provided empirical measurements for a variety of ciphers, hash functions, and signature algorithms
  - Simple reasoning about energy-security tradeoffs (looked at key size only)



	DES	3DES	IDEA	CAST	AES	RC2	RC4	RC5	BLOW FISH	
Key Setup	27.53	87.04	7.96	37.63	7.87	32.94	95.97	66.54	3166.3	(μJ)
Enc/Dec	2.08	6.04	1.47	1.47	1.21	1.73	3.93	0.79	0.81	(μJ/byte)

Figure 3: Energy consumption data for various symmetric ciphers

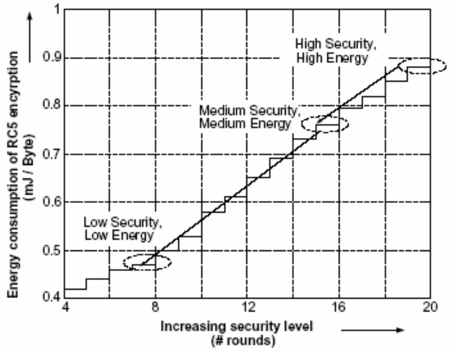


Figure 5: Energy consumption versus security trade-off for RC5 encryption

Approach

- □ Create a model for reasoning about energy-security tradeoffs
- □ Perform preliminary analytical study using current protocols
- □ Experiment
- □ Analyze empirical data

Energy-security tradeoff model

- Two parameters
  - C^E
    - Energy cost of implementing countermeasures to protect against vulnerabilities

$$C^E_{total} = \sum_i C^E(M_k, V_i)$$

Energy cost function

countermeasure

vulnerability

  - S_M
    - Security obtained by implementing countermeasures

Energy-security tradeoff model (cont)

- Countermeasure energy quotient
  - Assume upper limit on C^E, maximize quotient to find most secure profile to meet your battery needs
  - Assume lower limit on S_M, maximize quotient to find most energy-efficient profile (longest battery life) to meet your security needs

Security obtained by implementing countermeasures

$$Q_M = \frac{S_M}{C^E_{total}}$$

Countermeasure energy quotient

Cost of countermeasures

Energy-security tradeoff model (cont)

- A simplified model for our purposes

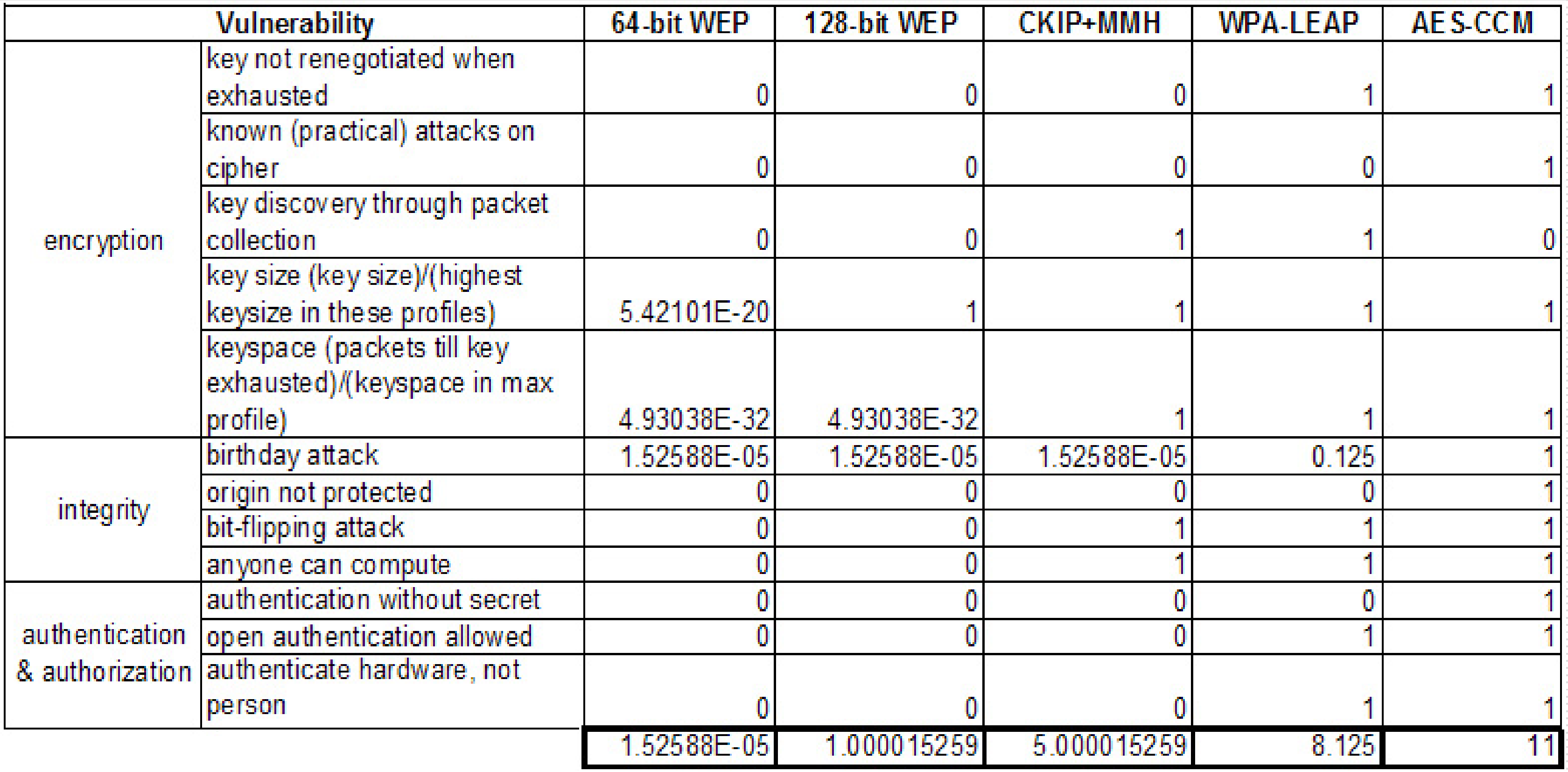
$$E_{total} = K_0 + \alpha_1 E_{cryp} + \alpha_2 E_{auth} + \alpha_3 E_{tgs}$$

- Assumptions
  - K_0 is constant for energy used in idle state and for bulk transmission
  - V_i from previous model are
    - Confidentiality or robustness of the encryption algorithm
    - Robustness of the integrity check
    - Robustness of authentication, authorization and access protocol

But how do we measure security?

- VERY hard
  - Unsolved problem
- Create a proxy
  - Create an ordinal scale on which to compare protocols
  - Identify classes of vulnerabilities
  - Evaluate whether or not a protocol protects against that weakness
    - 1 for yes or 0 for no
    - Value between 0 and 1 for weighted attributes
- Total each column, higher numbers are more secure

Security Proxy



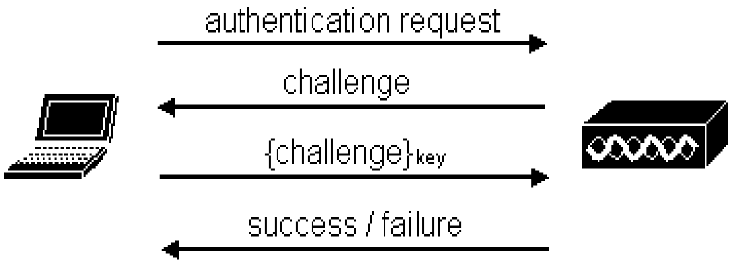
Vulnerability		64-bit WEP	128-bit WEP	CKIP+MMH	WPA-LEAP	AES-CCM
encryption	key not renegotiated when exhausted	0	0	0	1	1
	known (practical) attacks on cipher	0	0	0	0	1
	key discovery through packet collection	0	0	1	1	0
	key size (key size)/(highest keysize in these profiles)	5.42101E-20	1	1	1	1
	keyspace (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

Analytical study

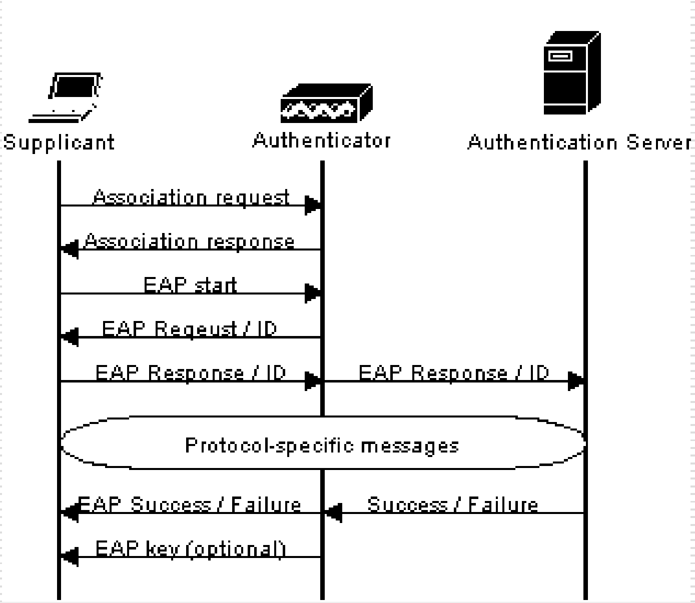
- Performed analytical using algorithms as specified in IEEE drafts and RFCs
- 802.11i was not officially defined at this point
- Looked at
  - WEP
  - WPA
  - 802.11i

Analytical study (cont)

- WEP been proved insecure
  - RC4 stream cipher
  - CRC integrity check
  - Poor authentication



- WPA enhanced security w/o hardware upgrade
  - RC4 w/key mixing
  - Michael
  - 802.1x



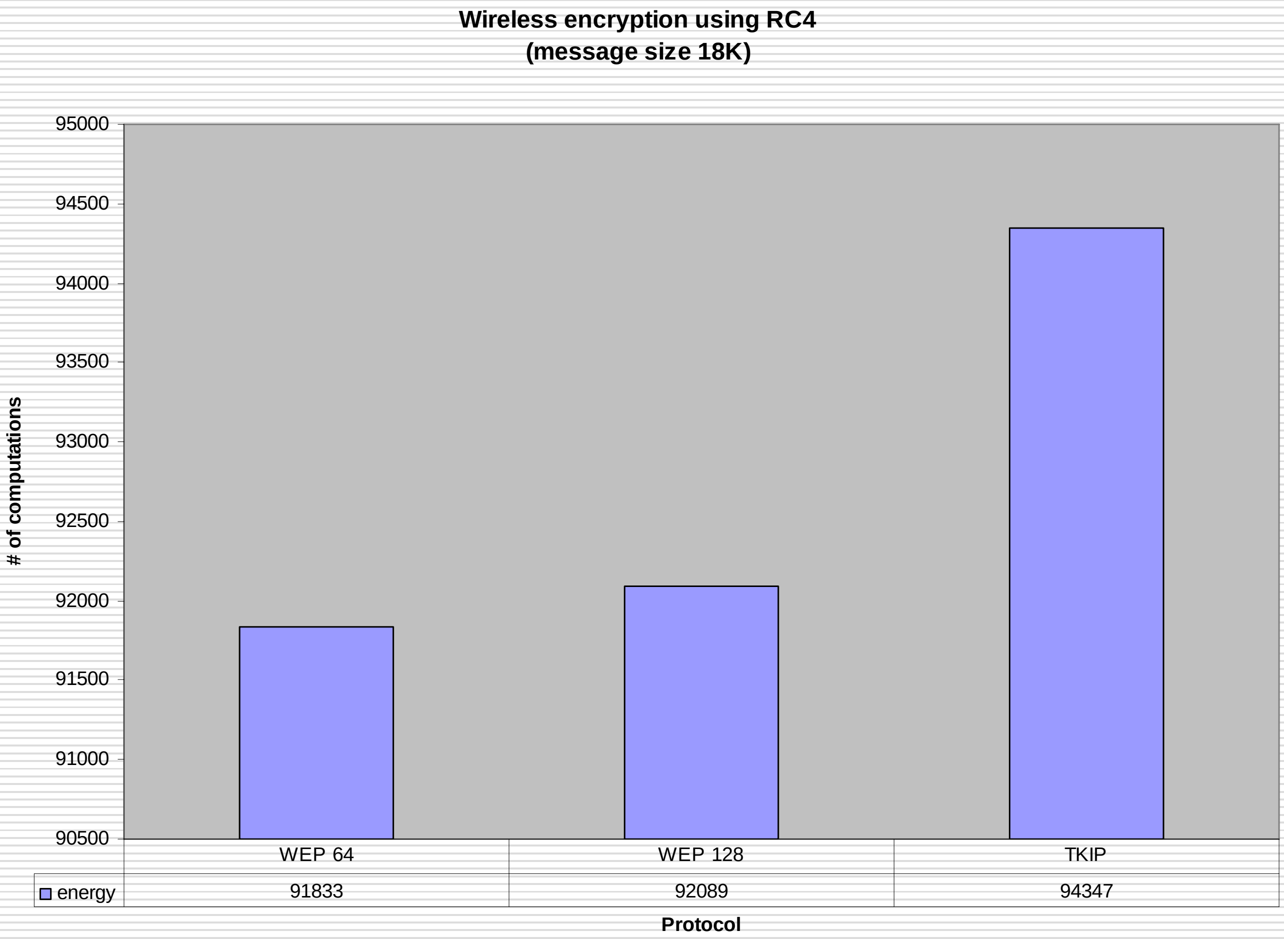
Analytical study (cont)

- 802.11i
  - AES-CCM
    - AES block cipher
    - CCM mode
    - 802.1x authentication
  - WPA
    - Backward compatibility

Analytical study (cont)

- Found:
  - Impact of encryption/decryption/MIC computation minimal
    - Approximately 2% increase from 128-WEP to TKIP
    - Improvement of AES varies by data, block, and key sizes
  - Cost of authentication rose greatly with the addition of 802.1x

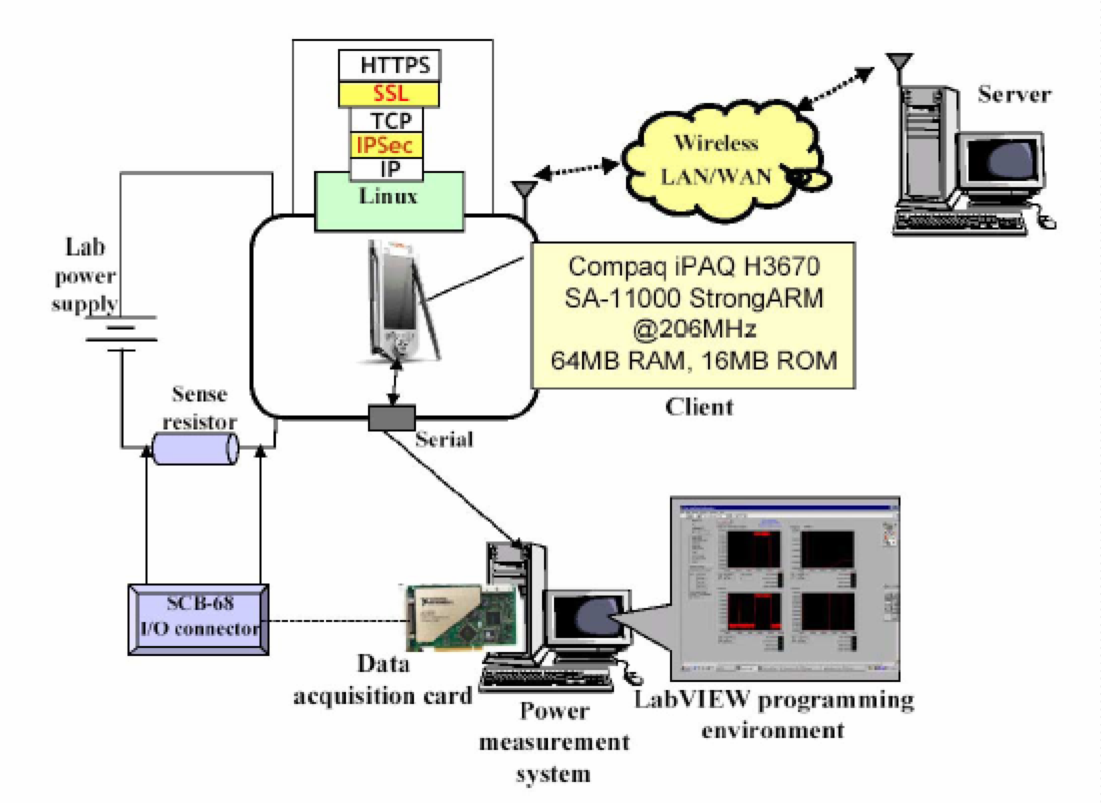
Analytical study (cont)



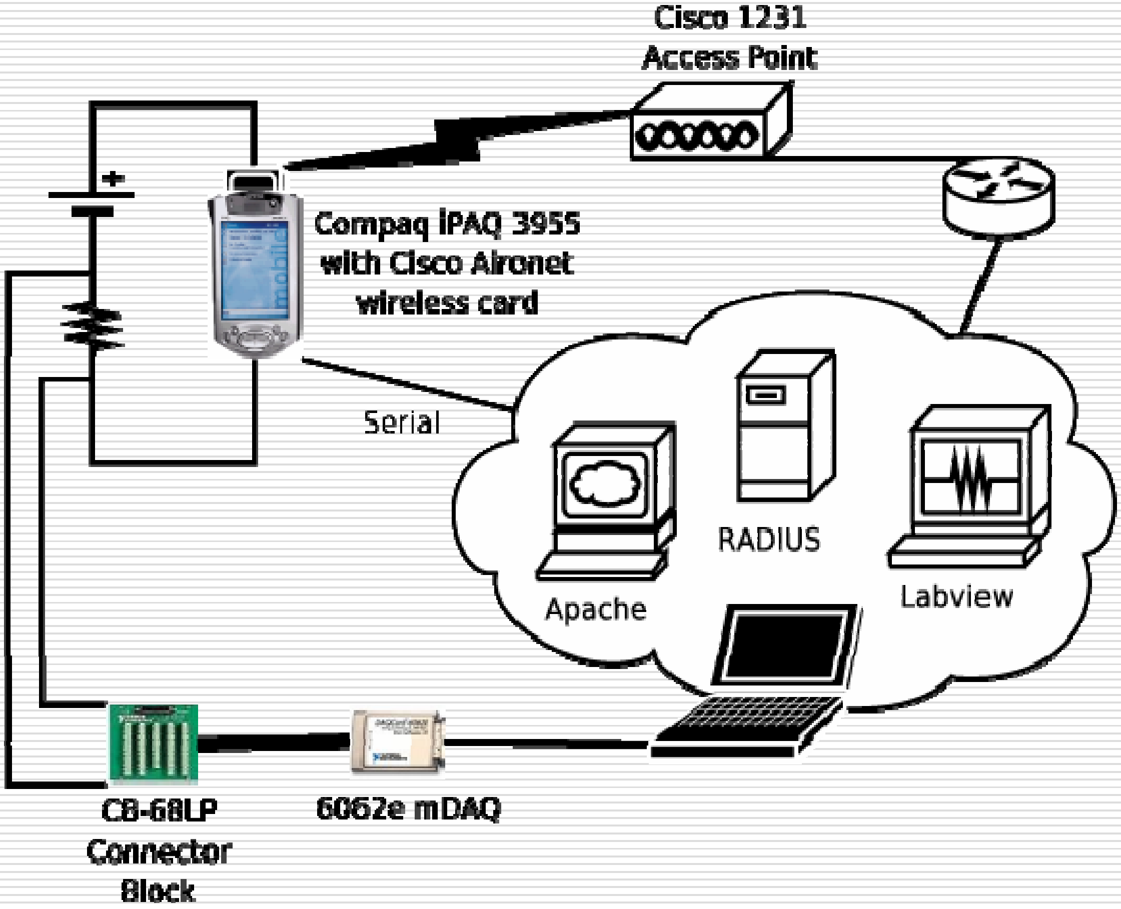
	WEP 64	WEP 128	TKIP
▨ energy	91833	92089	94347

Experiment

- Designed an experiment based on Potlapally et al.



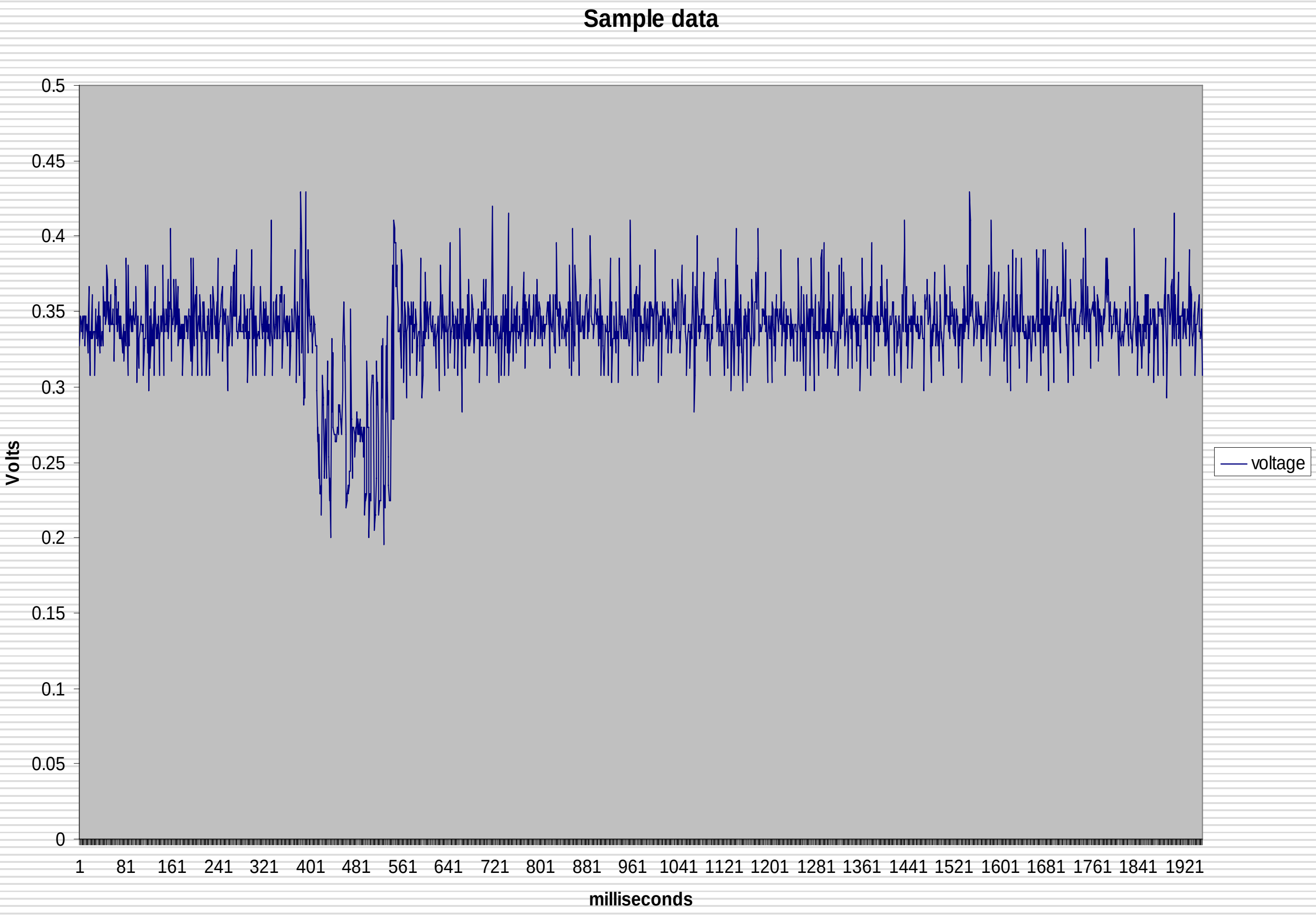
Experiment


Cisco 1231
Access Point
Compaq iPAQ 3955
with Cisco Aironet
wireless card
Serial
Apache
RADIUS
Labview
CB-68LP
Connector
Block
6062e mDAQ

Experiment details (cont)

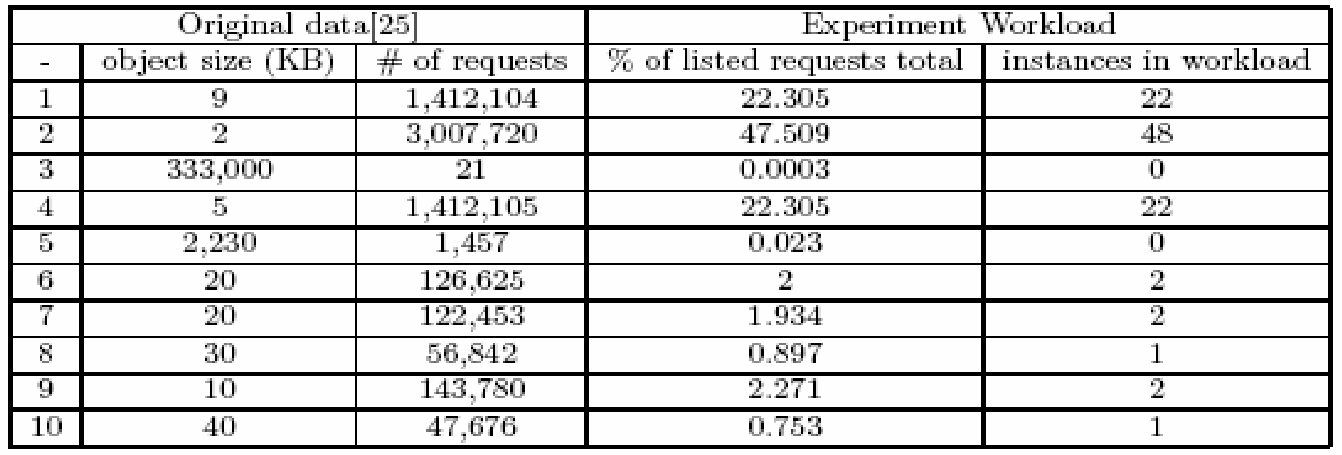
- Commercial Software
  - Funk Steel-Belted RADIUS
  - Funk Odyssey Client
  - Cisco Aironet Client Utility
  - Ethereal
  - Apache

Experiment details (cont)



Experiment details (cont)

- Workload
  - Mice and elephants
  - Used results from study of UW's campus network (Saroiu) to get sizes of mice and elephant objects
  - Created web pages based on these sizes
    - Text-only
    - Text with images

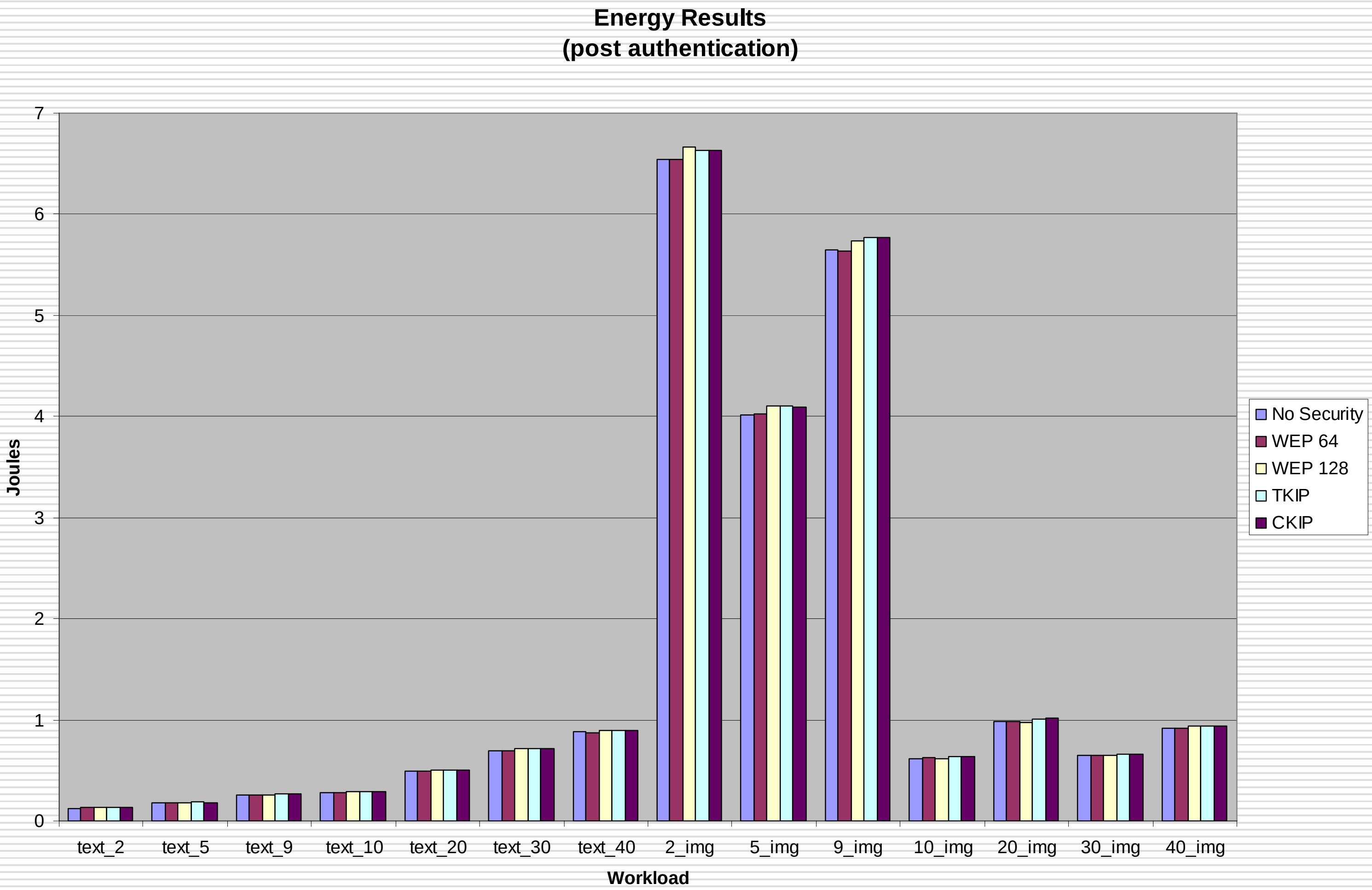


Original data[25]			Experiment Workload	
-	object size (KB)	# of requests	% of listed requests total	instances in workload
1	9	1,412,104	22.305	22
2	2	3,007,720	47.509	48
3	333,000	21	0.0003	0
4	5	1,412,105	22.305	22
5	2,230	1,457	0.023	0
6	20	126,625	2	2
7	20	122,453	1.934	2
8	30	56,842	0.897	1
9	10	143,780	2.271	2
10	40	47,676	0.753	1

Results

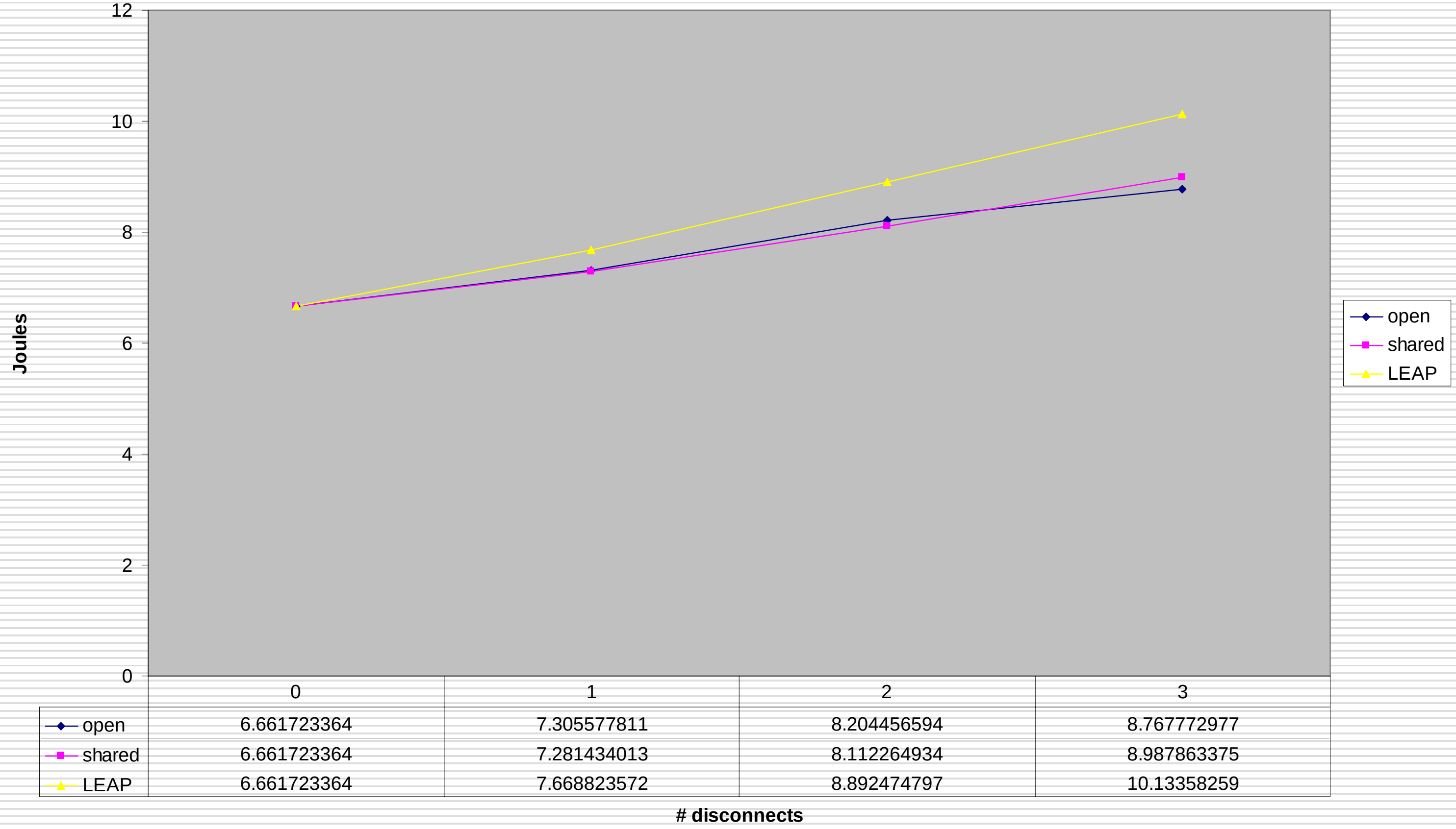
(thus far)

Results: Encryption



Results: Disconnection

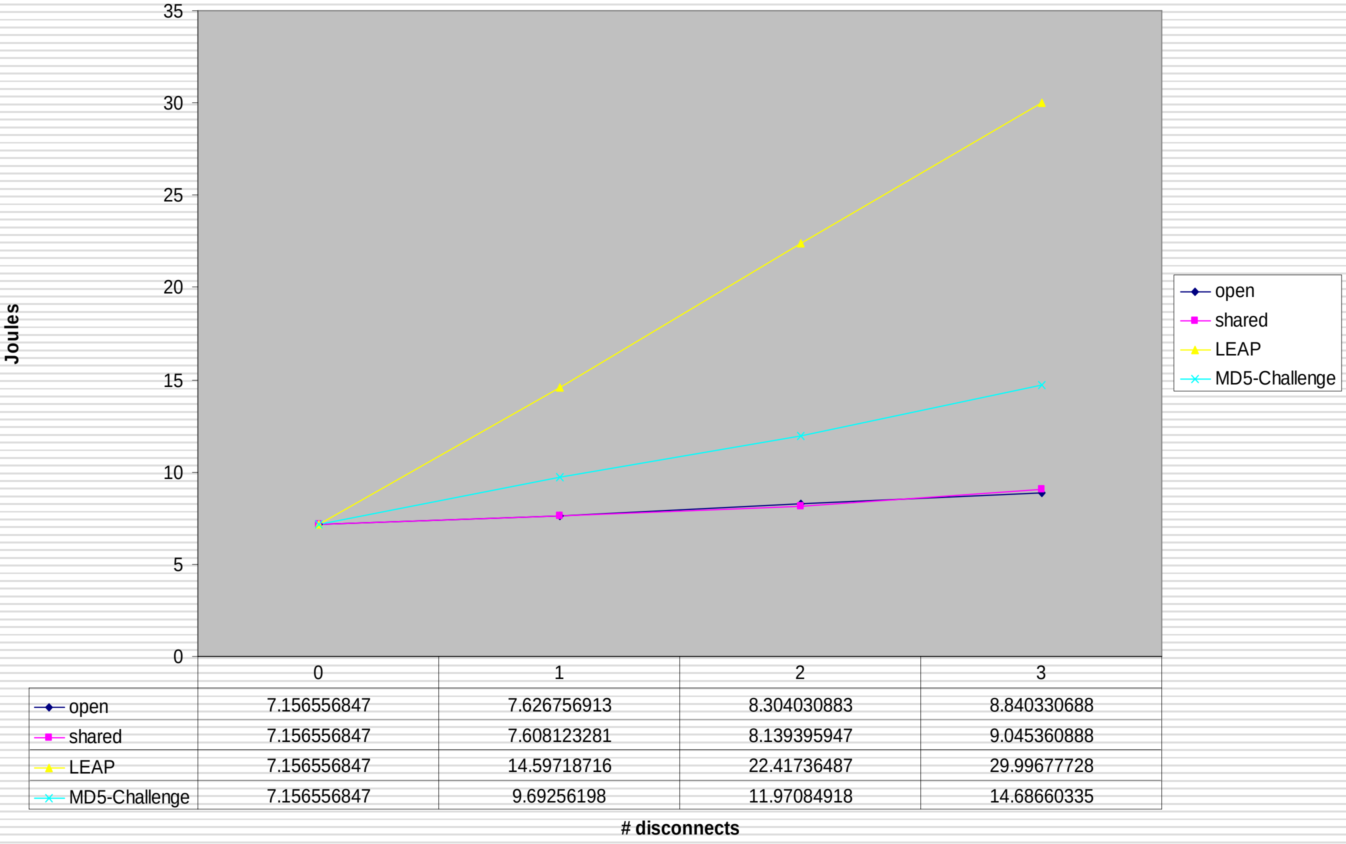
Cost of Disconnection
(ACU client, 128-bit WEP, transmitting 2img workload)



	0	1	2	3
open	6.661723364	7.305577811	8.204456594	8.767772977
shared	6.661723364	7.281434013	8.112264934	8.987863375
LEAP	6.661723364	7.668823572	8.892474797	10.13358259

Results: Disconnection

Cost of Disconnection
(Odyssey client, 128-bit WEP, transmitting 2img workload)



	0	1	2	3
open	7.156556847	7.626756913	8.304030883	8.840330688
shared	7.156556847	7.608123281	8.139395947	9.045360888
LEAP	7.156556847	14.59718716	22.41736487	29.99677728
MD5-Challenge	7.156556847	9.69256198	11.97084918	14.68660335

Results: Disconnection

- Open and shared authentication do not differ much
  - difference is a 128-bit challenge
- The cost of EAP authentication higher
  - More message transfer
  - More computation required for challenges
- Kotz and Essein study
  - 18% of sessions roam at least once
    - 60% authenticate with new AP, but still keep IP
    - 40% connection completely broken

Measurements applied to our model

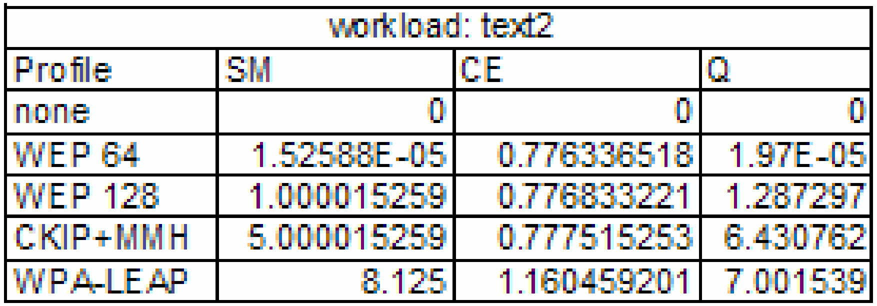
Security obtained by impleme
countermeasures

$$Q_M = \frac{S_M}{C^E_{total}}$$

Countermeasure energy quotient

Cost of countermeasures

- Limit the energy consumption to 1J for transfer of text2
  - Highest quotient is CKIP+MMH
- Require minimum security profile of 5
  - Select WPA with LEAP
- Require minimum security profile o 5 and maximum energy of 1J
  - Select CKIP+MMH



workload: text2			
Profile	SM	CE	Q
none	0	0	0
WEP 64	1.52588E-05	0.776336518	1.97E-05
WEP 128	1.000015259	0.776833221	1.287297
CKIP+MMH	5.000015259	0.777515253	6.430762
WPA-LEAP	8.125	1.160459201	7.001539

Summary

□ Smart tradeoffs between energy and security

□ Packet transfer and idle time are highest energy costs in secure communication

□ Deauthentication and disassociation add more energy overhead to secure transactions than encryption

□ More secure authentication methods use additional energy

Future Work

- For this work
  - Empirical data for
    - WPA key management
    - AES-CCM encryption
  - Improve security proxy
  - Difference between ACU and Odyssey LEAP authentication
- Future works
  - Further insights on disconnections per session
  - Move from infrastructure to ad-hoc environment

References

- □ Kotz, D., and Essien, K. Analysis of a campus-wide wireless network. In Proceedings of the 8th annual international conference on Mobile computing and networking (2002), ACM Press, pp. 107–118.
- □ Lahiri, K., Raghunathan, A., Dey, S., and Panigrahi, D. Battery driven system design: a new frontier in low power design, 2002.
- □ Potlapally, N. R., Ravi, S., Raghunath, A., and Jha, N. K. Analyzing the energy consumption of security protocols. In Proceedings of the 2003 international symposium on Low power electronics and design (2003), ACM Press, pp. 30–35.
- □ Saroiu, S., Gummadi, K. P., Dunn, R. J., Gribble, S. D., and Levy, H. M. An analysis of Internet content delivery systems. In Proceedings of the 5th Symposium on Operating Systems Design and Implementation (Dec 2002), USENIX Association.
- □ Stemm, M., and Katz, R. H. Measuring and reducing energy consumption of network interfaces in hand-held devices. In IEICE Transactions on Communications (Aug. 1997), vol. E80-B(8), pp. 1125–31.

Questions?