Polytechnic
UNIVERSITY

Minimizing Energy Consumption of Secure Wireless Session with QoS Constraints

Ramesh Karri, Piyush Mishra

April 2002

WICAT TR 02-002

WICAT

WIRELESS INTERNET
Center for Advanced Technology

MINIMIZING ENERGY CONSUMPTION OF SECURE WIRELESS SESSION WITH QOS CONSTRAINTS

Ramesh Karri   Piyush Mishra

Department of Electrical and Computer Engineering

Polytechnic University, Brooklyn, NY, US 11201

Abstract: In this paper we will investigate techniques to minimize the energy consumed by a secure wireless session without compromising the security of the session. While it has been shown in [8] that compressing the session negotiation messages, the protocol header, and the data reduces the energy consumed by a secure session [8], in this paper we show that matching the block size of compression to the data cache size of the device is important. We also investigate the choice of a bulk encryption algorithm (3DES vs. AES) and a key exchange protocol (Diffie-Hellman vs. RSA) based on the energy consumed by a secure session. These techniques yield energy savings of 1.3x during data transmission and 1.2x during data reception beyond that obtained by techniques in [8]. These techniques complement and supplement those proposed in [8] and when combined yield an overall energy savings of 2.1× during data transmission and 4.35× during data reception.

1. Introduction

The rapidly increasing trend of "anytime-anywhere" access of sensitive data together with the emerging m-commerce applications has fueled a tremendous growth of secure wireless sessions to ensure data integrity, privacy and authenticity over public networks [1, 2]. Such applications consume significant energy while (a) establishing the secure session, (b) performing the secure data transactions, and (c) periodically refreshing the session security parameters for higher security. Mobile computing and communication devices used for providing these services have limited computing resources and battery life. Therefore, a successful merger of shrinking device sizes and increasing secure wireless data access demands efficient management of battery energy.

A secure session is established between the client and the server using security protocols such as Secure Socket Layer (SSL) [24], Internet Security Protocol (IPSEC) [23] or Wireless Transport Layer Security protocol (WTLS) [3]. We extracted features common to these security protocols, such as the handshake for mutual authentication and for secret key exchanges, to study the performance and energy consumption characteristics of a secure session.

Client initiates the handshake by sending a list of cryptographic parameters it supports, such as the key exchange protocols, the private-key encryption algorithms and the message authentication code (MAC) algorithms. Server responds with the acceptable security association, authenticates itself to the client, sends necessary information for performing secret key exchange and requests authentication from the client. The client, in return, authenticates itself and sends the remaining information to complete the secret key

exchange. Finally, the client and the server exchange messages to activate the session with the negotiated security association, and encryption and MAC keys are generated independently at the server and the client using the exchanged secrets.

After successfully establishing the secure session, either the client or the server takes the plain text messages, computes the MAC, encrypts the data and transmits it. At the other end, the received data is decrypted and verified. Either end can terminate the session at any time. Periodically refreshing the encryption and the MAC keys (key refresh) and the secure session parameters (session refresh) enhances the security of the session.

There has been substantial research in the field of wireless communication energy management. Techniques to minimize the energy consumed by a communication unit include modulating the energy used by the mobile transmitter during active communication [5, 21], adapting communication according to the application requirements [18], suspending device operation during idle periods [6, 20] and transitioning between different modes of operation [7, 4]. Energy-aware network protocols optimize the WLAN card activities [22], reduce energy-expensive retransmission of lost messages [17] and employ energy-efficient error control schemes [19]. In this paper we extend the scope of this research to include security protocols and introduce techniques for reducing the energy consumed by secure wireless sessions carried over public networks.

2. Motivation

Energy consumed by secure wireless sessions on mobile devices is very significant. It is a function of the size of data transferred and the security level of the session, as shown in Figure 1.
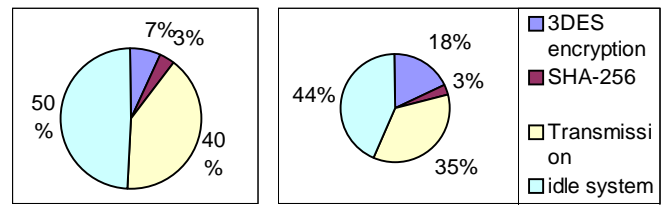

Figure 1: Energy consumed by secure wireless data transmission of 64 KB data using (a) DES and (b) 3DES encryption

Security of a private-key encryption algorithm is expressed in terms of user key size and the number of encryption rounds. 3DES encryption uses a 192-bit key as opposed to DES encryption that uses a 64-bit key and involved 3× more processing, thereby consuming significantly more energy.

We considered a Symbol PPT2800™ Pocket PC device (32-bit, 206 MHz StrongArm™ SA-1110 processor, 32 MB flash ROM, 32 MB RAM, 16 KB instruction cache and 8 KB data cache [16]) running Windows CE™ 3.0 operating system and equipped with an 11 Mbps Spectrum24™ wireless LAN adapter card [9], operating in the P1 polling mode, as the mobile test bed.

Table 1 summarizes the energy consumed by various tasks during a secure wireless session while transmitting and receiving 2.56 MB data[1]. We use Diffie-Hellman (DH) protocol for secret key exchange [25], triple-Data Encryption Standard (3DES) for encryption [15], SHA-256 for message authentication, a key refresh rate that entails regenerating the encryption and MAC keys every 128 KB of data and a session refresh rate that entails renegotiating the security association every 2 MB of data. Therefore, during this data transaction the security association is renegotiated once and the encryption and MAC keys are recomputed 19 times, as shown in Table 1. The idle system energy due to overheads, such as the back off period, channel access time and other network conditions is more than 40% of the entire system energy.

	Secure session energy (mJ)		
DH handshake	1062 mJ/handshake× ⌈2560/2000⌉	2124	(1)
SHA-256 sign SHA-256 verify	0.0552 μJ/bit × 2.56 × 10^6 × 8 bits	1130	(2)
3DES encrypt 3DES decrypt	0.3349 μJ/bit × 2.56 × 10^6 × 8 bits	6858	(3)
Transmit	0.6582 μJ/bit × 2.56 × 10^6 × 8 bits	13480	(4)
Receive	0.2833 μJ/bit × 2.56 × 10^6 × 8 bits	5803	(5)
Key refresh	12.895 mJ/key-refresh × (⌊2000/128⌋ + ⌊560/128⌋)	245	(6)
Idle system		16604	(7)
Total transmit	(1)+(2)+(3)+(4)+(6)+(7)	40441	
Total receive	(1)+(2)+(3)+(5)+(6)+(7)	32764	

Table 1: Energy consumed by tasks of a secure session

Table 2 shows the energy savings for the above data transfer using data and protocol header compression and protocol optimization techniques proposed in [8]. Due to the area restrictions of small mobile devices, such as the Symbol PPT 2800, we do not consider hardware implementation based techniques for energy minimization for this work. A combination of adaptive handshake and data and header compression operating on 64KB data block size (with compression parameters that

yield a compression ratio of 4.3) reduced the secure session energy by 1.59× during transmission and 3.49× during reception.

	Optimized session energy (mJ)		
DH Handshake[2]	724.3 mJ/handshake × ⌈(2560/4.3) /2000⌉	724.3	(1)
SHA-256 sign SHA-256 verify	0.0552 μJ/bit × 2.56 × 10^6 × 8 / 4.3 bits	261.2	(2)
3DES encrypt 3DES decrypt	0.3349 μJ/bit × 2.56 × 10^6 × 8 / 4.3 bits	1595	(3)
Transmit	0.6582 μJ/bit × 2.56 × 10^6 × 8/ 4.3 bits	3116	(4)
Receive	0.28335 μJ/bit × 2.56 × 10^6 × 8/ 4.3 bits	1342	(5)
Key refresh	12.895mJ/key-refresh × ⌊(2560/4.3) / 128⌋	51.56	(6)
Idle system	16604/4.3	3838	(7)
DEFLATE compr		15832	(8)
DEFLATE decomp		1590	(9)
Transmit	Total	(1)+(2)+(3)+(4)+(6)+(7)+(8)	25422.5
	Save		1.59 ×
Receive	Total	(1)+(2)+(3)+(5)+(6)+(7)+(9)	9402.5
	Save		3.49 ×

Table 2: Energy savings due to protocol optimization and compression of protocol header and data

3. Optimizing secure wireless session energy

In this section we will present three new techniques to further reduce the energy consumed by a mobile device during a secure wireless session while satisfying all the security requirements.

3.1 Matching compression block size to device data cache size

Data compression has been shown to reduce (a) the transmission, reception, encryption and decryption energy during a secure data transaction (b) the number of key refreshes required and the corresponding energy, and (c) the energy consumed by the idle system [8]. Energy consumed by a secure session is reduced if the energy savings due to compression and decompression are more than the energy consumed by compression and decompression. For a secure session operating on a fixed energy budget, compression improves security by affording larger encryption key size and higher key refresh rate.

Previous research [8] showed that an optimized C implementation of DEFLATE loss-less data compression algorithm [11] with medium compression level (level 5), medium memory level (level 5) and maximum history window size (15 bits) yields a compression ratio close to the best while consuming the least energy on a device with a large data cache.

	128 KB	64 KB	8 KB	1 KB
Energy (mJ)	709.62	395.79	31.69	14.76
Compression ratio	4.4815	4.3256	3.4782	2.8254

Table 3: Energy consumed by DEFLATE compression

---

[1] Refer to [8] for complete description of the mobile test bed and energy measurement methodology.

[2] Refer to [8] for detailed discussion of protocol optimization.

Table 3 summarizes the energy consumed by DEFLATE while compressing 1KB, 8 KB, 64 KB, and 128 KB block size benchmarks from Calgary corpus [12] on the Symbol device with an 8KB data cache.

Compression energy increases sharply as the compression data block size increases beyond the data cache size (8 KB). Matching the compression block size to the data cache size yields the optimum compression energy although it uses a low compression ratio. Table 4 shows that sacrificing the compression ratio by matching the compression block size to the data cache size reduces the energy consumed during data transmission. On the other hand, energy consumed by DEFLATE decompression is approximately one-tenth of the energy consumed by compression since decoding is simple and fast. Hence, sacrificing the compression ratio for compression energy while sending data to mobile device increases its energy consumption.

	Optimized session energy (mJ)		
DH Handshake	724.3 mJ/handshake × $\lceil(2560/3.4782)/2000\rceil$	724.3	(1)
SHA-256 sign SHA-256 verify	0.0552 µJ/bit × 2.56 × 10^6 × 8 / 3.4782 bits	324.9	(2)
3DES encrypt 3DES decrypt	0.3349 µJ/bit × 2.56 × 10^6 × 8 / 3.4782 bits	1972	(3)
Transmit	0.6582 µJ/bit × 2.56 × 10^6 × 8/ 3.4782 bits	3876	(4)
Receive	0.28335 µJ/bit × 2.56 × 10^6 × 8/ 3.4782 bits	1668	(5)
Key refresh	12.895mJ/key-refresh × $\lfloor(2560/3.4782)/128\rfloor$	64.45	(6)
Idle system	16604 / 3.4782	4773	(7)
DEFLATE compr		10141	(8)
DEFLATE decomp		1014	(9)
Transmit	Total	(1)+(2)+(3)+(4)+(6)+(7)+(8)	21862.8
	Save		1.16 ×
Receive	Total	(1)+(2)+(3)+(5)+(6)+(7)+(9)	10538.9
	Save		0.89 ×

Table 4: Impact of matching compression block size to device data cache size

Therefore, while transmitting data the compression block size should be matched to the device data cache size and while receiving data large compression block size (larger the better) should be used to reduce the client energy. Such an asymmetric compression arrangement can be agreed upon during the secure session negotiation.

3.2   Choice of a bulk encryption algorithm

Table 5 shows that the energy consumed by Advanced Encryption Standard (AES) [10] in software is 5× less than the energy consumed by 3DES. This is due to the elegant design of AES to better exploit features like pipelining and parallel processing and due to the larger data block size.

A client also has a choice of either reducing the encryption key size or the number of encryption rounds while increasing the key refresh rate or vice versa to reduce the system energy while maintaining the desired security level. The tradeoff depends upon the relative energy consumption of the key refreshes and the data encryption algorithm. For example, for a secure session transmitting 2.56 MB data using 3DES encryption, reducing the number of rounds of encryption by 2×, and correspondingly increasing the key refresh rate by 2× reduces the session energy by 1.05×. On the other hand, for a secure session using 192-bit key AES encryption session energy is reduced by 1.01× by increasing the encryption key size to 256 bits and reducing the key refresh rate by 2×.

Encryption software implementation				
	3DES (192-bit)	AES		
		128-bit	192-bit	256-bit
Energy/bit (µJ)	0.3349	0.0666	0.07	0.075
Throughput (Mbps)	4.976	25.963	24.58	24.1

Table 5: Energy consumed by optimized software implementations of 3DES and AES encryption

3.3   Choice of key exchange protocols

Energy consumed by the handshake protocol depends upon the level of security of the session (size of certificates and secret keys exchanged, size of encryption and MAC keys generated) and the number and size of messages exchanged.

A client using Deffie-Hellman key exchange protocol during handshake generates and exchanges large secret keys with the server. For example, for WTLS security protocol the size of these key exchange messages can be as large as 64KB. Therefore, a secure session using Deffie-Hellman key exchange protocol consumes 1062 milli Joules, 90% of which is consumed during the generation and exchange of the certificates and the secret keys, as shown in Table 6. Numbers in bold correspond to the client.

Messages Exchanged	Energy consumed (mJ)					
	D-H			RSA		
	Crypto-comp	Comm.		Crypto-comp	Comm.	
		Tx	Rx		Tx	Rx
Initiation	**0.01**	**16**	6.8	**0.01**	**16**	6.8
Server CERTIFICATE + KEY EXCHANGE	61.4	682	**294**	1.22	682	**294**
Client CERTIFICATE + KEY EXCHANGE	**61.9**	**677**	292	**19.21**	**34**	148
Activation	**-**	2.6	**1.3**	-	2.6	**1.3**
KEY$_{ENC+MAC}$ @ client	**12.33**	-	-	**12.33**	**-**	**-**
KEY$_{ENC+MAC}$ @ server	12.33	-	-	45.33	-	-
CLIENT	**74.3**	**693**	**295**	**31.55**	**358**	**295**
SERVER	73.8	685	298	46.55	685	154.8

Table 6: Energy consumed by handshake protocols using D-H and RSA key exchange protocols

On the other hand, for a system using a RSA [13] based handshake the server sends its public key to the client. The client encrypts a small random value (20 bytes for WTLS protocol) using the server public key and transmits the result back to the server. Table 6 shows that due to the small key exchange message size the handshake energy is reduced by 35% without compromising the session security.

Optimizing the handshake protocol and compressing the handshake messages, as suggested in [8], reduces the client energy by another 1.86×, as shown in Table 7. Reducing the session negotiation energy has significant impact upon short secure sessions involving relatively smaller data exchanges.

	Energy consumed by the RSA handshake protocol (mJ)	
	Un-optimized	Optimized
Transmit	358	20.9
Receive	295	83.392
Crypto-computations	31.554	31.554
Decompression	-	50.704
TOTAL	347.454	186.55
Energy saving factor		1.86 ×

Table 7: Energy saved by optimizing the handshake protocol

4. Summary

Let us study the overall impact of our previous work and these new techniques on the energy consumed by the secure session.

Let us consider the same secure session example from section 1 for securely transmitting and receiving 2.56 MB data. We assume a compression block size of 8KB (data cache size) at client and 64KB at the server, medium compression level (level 5), medium memory level (level 5) and maximum history window size (15 bits). DEFLATE compression with these configurations yields relatively lower compression but consumes significantly less energy, as shown in Table 3.

Session negotiation is carried out using RSA key exchange based optimized handshake protocol. The server looks up the client certificate from its own source and compresses the messages before transmitting them to the client. Besides, the optimized secure session uses 256-bit key AES encryption, SHA-256 MAC, key refresh rate that entails re-computation of the encryption and MAC key every 256 KB data and session renegotiation every 2 MB data.

Table 8 shows an energy savings of more than 1.3× during transmission and 1.25× during reception over [8] while satisfying all the security and performance requirements. Combining these techniques with those proposed in [8] results in an overall 2.1× energy savings in the transmit mode and 4.35× in the receive mode.

		Optimized secure session energy (mJ)		
Optimized RSA Handshake		186.55 mJ/handshake × ⌈(2560/3.4782) /2000⌉	186.5	(1)
SHA-256 sign SHA-256 verify		$0.0552\ \mu J/bit \times 2.56 \times 10^6 \times 8 / 3.4782$ bits	324.9	(2)
AES-192 encrypt AES-192 decrypt		$0.072\ \mu J/bit \times 2.56 \times 10^6 \times 8 / 3.4782$ bits	441.6	(3)
Transmit		$0.6582\ \mu J/bit \times 2.56 \times 10^6 \times 8 / 3.4782$ bits	3876	(4)
Receive		$0.28335\ \mu J/bit \times 2.56 \times 10^6 \times 8 / 4.3$ bits	1342	(5)
Key refresh		12.895mJ/key-refresh × ⌊(2560/3.4782) / 256⌋	32.22	(6)
Idle system		16604 / 3.4782	4181	(7)
DEFLATE compr			10141	(8)
DEFLATE decomp			1014	(9)
Transmit	Total	(1)+(2)+(3)+(4)+(6)+(7)+(8)	19177.3	
			1.33 ×	
Receive	Total	(1)+(2)+(3)+(5)+(6)+(7)+(9)	7516.3	
	Save		1.25 ×	

Table 8: Energy savings from optimized secure session

5. Acknowledgement

6. References
1. J. A. Senn, "The emergence of M-Commerce", IEEE Computer, December 2000, pp. 148-150.
2. D. Clark, "Encryption advances to meet Internet challenges", IEEE Computer online magazine, December 2000.
http://www.computer.org/computer/articles/August/techn ews800.htm
3. Wireless Application Protocol: Wireless Transport Layer Security Specifications, February 2000.
http://www.wapforum.org
4. S. Udani, J. Smith, "The power broker: Intelligent power management for mobile computers", Technical Report MS-CIS-96-12, CS Department, University of Pennsylvania, May 1996.
5. J. M. Rulnick, N. Bambos, "Mobile power management for maximum battery life in wireless communication networks", Proceedings, IEEE INFOCOM, 1996.
6. R. Kravets, P. Krishnan,"Power management techniques for mobile communication", Proceedings, ACM/IEEE MOBICOM, 1999.
7. A. Kamerman, L. Monteban, "WaveLAN-II: A high performance wireless LAN for the unliscensed band", Bell Labs Technical Journal, 1997.
8. R. Karri, P. Mishra, "Energy management of secure wireless session", Submitted to IEEE INFOCOM, 2002.
http://cad.poly.edu/publications/infocom2002.pdf
9. Spectrum24® High Rate LA 41X1 PC Card.
http://www.symbol.com/products/wireless/la41x1.html
10. http://csrc.nist.gov/encryption/aes

11. DEFLATE Compressed Data Format Specification version 1.3.
http://www.kblabs.com/lab/lib/rfcs/1900/rfc1951.txt.html

12. T.C. Bell, "Text compression", Prentice Hall, Englewood Cliffs, NJ, 1990.

13. R. L. Rivest, A. Shamir, L. M. Adelman, "A method for obtaining digital signatures and public key cryptosystems", Communications of the ACM, February 1978, Vol. 21, No. 2, pp. 120-126.

14. http://www.tektronix.com

15. National Bureau of Standards, NBS FIPS PUB 46, "Data Encryption Standard", National Bureau of Standards, U.S. Department of Commerce, January 1977.

16. Symbol PPT 2800 series portable pen terminal. http://www.symbol.com/products/mobile_computers/mobile_ppc_ppt2800.html

17. A. Chockalingam, M. Zorzi, "Energy consumption performance of a class of access protocol for mobile data networks", Proceedings, IEEE VTC, May 1998, Vol. 2, pp. 820-824.

18. R. Kravets, K. Calvert, K. Schwan, "Payoff adaptation of communication for distributed interactive applications", Journal on High Speed Networking: Special Issue on Multimedia Communications, July 1998.

19. M. Zorzi, R. R. Rao, "Error control and energy consumption in communications for nomadic computing", IEEE Transactions on Computers, Special Issue on Mobile Computing, March 1997.

20. S. Singh, C.S. Raghavendra, "PAMAS-Power aware multi-access protocol with signaling for ad-hoc networks", ACM Computer Communications Review, July 1998.

21. J. Ebert, B. Stremmel, E. Wiederhold, A. Wolisz, "An energy-efficient power control approach for WLANs", Journal of Communications and Networks, September 2000, Vol. 2, n. 3, pp. 197-206.

22. C. Rohl, H. Woesner, A. Wolisz, "A short look on power saving mechanisms in the wireless LAN standard draft IEEE 802.11", WINLAB Workshop on Third Generation Wireless Systems, NJ, March 1997.

23. IP Security Protocol (IPSEC) Charter. http://www.ietf.org/html.charters/ipsec-charter.html

24. Secure Shell Layer (SSL) Charter. http://www.ietf.org/html.charters/secsh-charter.html

25. W. Diffie, M. E. Hellman, "New directions in cryptography", IEEE Transactions on Information Theory, November 1976, Vol. 22, No. 6, pp. 644-654.