Encryption and Power Consumption in Wireless LANs[1]

N. Ruangchaijatupon and P. Krishnamurthy
Telecommunications Program
University of Pittsburgh
135, N. Bellefield Avenue, Pittsburgh, PA 15260
{nararatr,prashant}@mail.sis.pitt.edu

Security enforcement in wireless communication is considered necessary because of the inherent vulnerability of radio transmissions to eavesdropping. Encryption is being employed in wireless devices before data are transmitted over the air at the MAC/physical layers and the application layer. Current implementations at the MAC/physical layers are not very secure and application layer encryption becomes essential. However, encryption is computationally intensive and consumes energy and computational resources that are limited in wireless devices.

Different types of data need different levels of security. A major consequence of the advances in cryptography and development of encryption standards is that the strength of the encryption is dependent mostly on the size of the secret key. This is because encryption algorithms employed today are almost impossible to break except by brute force that involves searching through all possible keys (the key space). As the key space becomes larger, the time required to break an encryption scheme becomes so excessive that such attacks are meaningless. The rule of thumb today is to use algorithms with key sizes of 80 bits or more for secret key encryption (a search space of 2^{80} keys) and 1024 bits or more for public key algorithms like RSA. In summary, an algorithm's security depends on the encryption key size rather than the specific encryption algorithm today. A wireless network interface draws a significant fraction of total power consumed by a mobile device. Collisions and retransmissions also result in consumption of additional power. This is affected by the SNR and the number of contending nodes.

In order to effectively design energy efficient and secure protocols for mobile devices, there is a need to understand how encryption affects the consumption of battery power. In this work, we experimentally evaluate this by determining the major contributions to energy consumption. We investigate the rate of battery power consumption in wireless devices (laptops and handheld computers) under different scenarios such as with and without transmission over WLANs, at different SNRs, and varying the number of contending nodes. For this purpose, an IEEE 802.11b WLAN at 2.4 GHz is used. We examine three conventional encryption algorithms; CAST, IDEA, and Triple-DES, and two public key encryption algorithms; Diffie-Hellman and RSA. We focus on the security provided at the application level, which is the enhancement of the inadequate link-layer security provided by IEEE 802.11. Our results indicate that wireless transmissions and larger key sizes impact power consumption the most.

[1] This work has been partially supported by the University of Pittsburgh CRDF grant

Wireless Devices, LANs and PANs

- Local wireless networking is growing rapidly
  - IEEE 802.11 and 802.11b
  - IEEE 802.11a and HIPERLAN
  - Bluetooth
  - HomeRF
- Variety of devices connect to the network
  - Laptops
  - Handheld computers – WinCE devices
  - Palmtop computers – Palm, Handspring, Clie, etc.
  - Digital cameras, Camcorders, Home automation devices etc.

Security?

- Security in wireless networks is at best
  - Mediocre
    - 40-bit RC-4 in IEEE 802.11
      - Static keys!
    - Stronger encryption in Bluetooth but use of PINs that are weak
    - Somewhat stronger schemes in HomeRF-2
    - An overall well designed scheme in HIPERLAN-2
  - Non-existent
    - In most cases encryption is only an option
- Application layer security is strongly recommended

Energy Consumption in Handheld Devices

- Handheld devices rely on batteries, which have limited energy
  - Typical laptop battery lasts for 3-5 hours without network connectivity
- Previous studies show that energy consumption in handheld devices depends on several factors
  - Transmission of RF signals
  - Reception or monitoring of RF signals
  - Sleep modes
- *Major energy consumption in handheld devices is due to the wireless network interface*

Encryption and Power Consumption

- Encryption algorithms are computationally complex
  - Modular exponentiations
    - 1024 bit numbers in RSA
  - Several rounds of operations
    - 16 rounds in DES and 48 in 3-DES
- Requires several CPU cycles
- Requires memory
- Some algorithms are designed for resource constrained environments. but are not in widespread use

Energy efficient protocols

- Recent research work has focused on energy efficient communications protocols
- Example idea:
  - Transmissions consume energy
  - Transmissions may be wasted if the radio channel is bad
  - Design intelligent schemes to prevent transmissions unlikely to succeed
    - Send a short probe packet
    - If acknowledged, transmit large packet

Energy Efficient Security Protocols?

- Security of encryption algorithms today depend on the key size
  - Algorithms are virtually unbreakable except for brute force attacks
  - Larger the key size, larger the brute force search, and more secure the algorithm
- Large key size usually implies more operations ➔ more energy consumption
- Example idea:
  - Send non-critical information with less security
  - Send critical information with more security

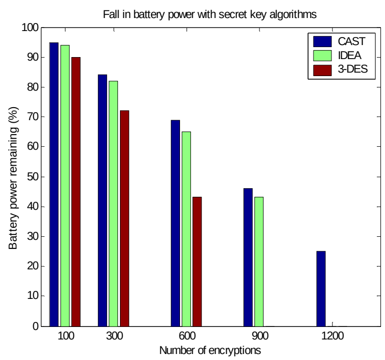
Need for experimental work

- How much does the key size affect battery consumption?
  - Does it make sense to switch from a 1024 bit key to a 32 bit key if they consume the same power?
- Is it environment dependent?
  - SNR can affect the success of transmissions
  - Increased number of users can increase collisions
  - Deployment can influence interference
- Is it platform dependent?
  - Laptop Vs Handheld computer

Experimental set-up

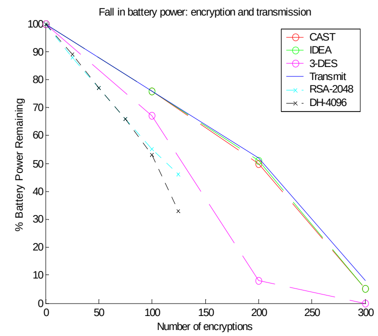
- IEEE 802.11b Wireless LAN in the School of Information Sciences Building
- Laptop computer
  - Windows 98, 64 Mb RAM, Pentium II processor
  - File encryption and encryption with transmission
    - Secret key and public key algorithms
    - CAST, IDEA, 3-DES, RSA and DH
  - Low and heavy traffic
  - Excellent, good, and marginal signal conditions
- Handheld computer
  - HP Jornada 720 running Windows CE
  - Blowfish encryption

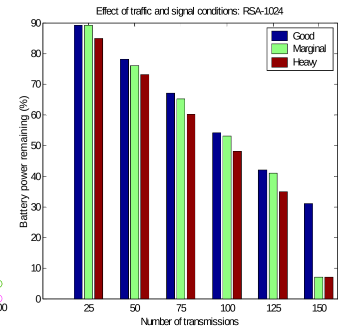
File Encryption on Laptops



- CAST and IDEA both have 128 bit keys
- 3-DES has 168 bit key but thrice the number of computations
- Beyond 900 encryptions, only CAST is able to carry on encryptions

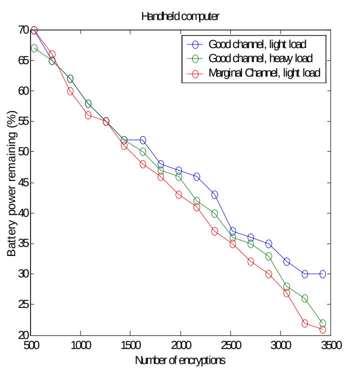
File Transmission with Encryption: Effect of Traffic and Signal Conditions





N. Ruangchaijatupon and P. Krishnamurthy
University of Pittsburgh Telecommunications Program
Partly funded by the University of Pittsburgh-CRDF grant

File Transmission with Encryption on Handheld Computers



- Used Blowfish algorithm
  - Implementations of other algorithms are scarce
  - 32 bit keys employed
- Suited for resource constrained environment
- Algorithm can employ varying key sizes but the net computational effort is not changed

N. Ruangchaijatupon and P. Krishnamurthy
University of Pittsburgh Telecommunications Program
Partly funded by the University of Pittsburgh-CRDF grant

Conclusions and Future Work

- Key size (computational steps) has an impact on battery consumption
  - Marked difference moving from CAST/IDEA to 3-DES
    - More steps in 3-DES
  - Public key algorithms are more computationally intensive and consume an order of magnitude more power
- Some impact of traffic and signal conditions
- Inconclusive results with handheld computers
  - Only one algorithm that is designed for resource constrained environments has been tested
- More experimental work and theoretical models for designing energy efficient security protocols

N. Ruangchaijatupon and P. Krishnamurthy
University of Pittsburgh Telecommunications Program
Partly funded by the University of Pittsburgh-CRDF grant