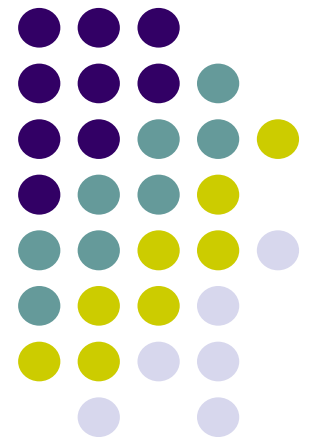


Energy Impact of Secure Computation on a Handheld Device

Zhiyuan Li Rong Xu

Department of Computer Science, Purdue University

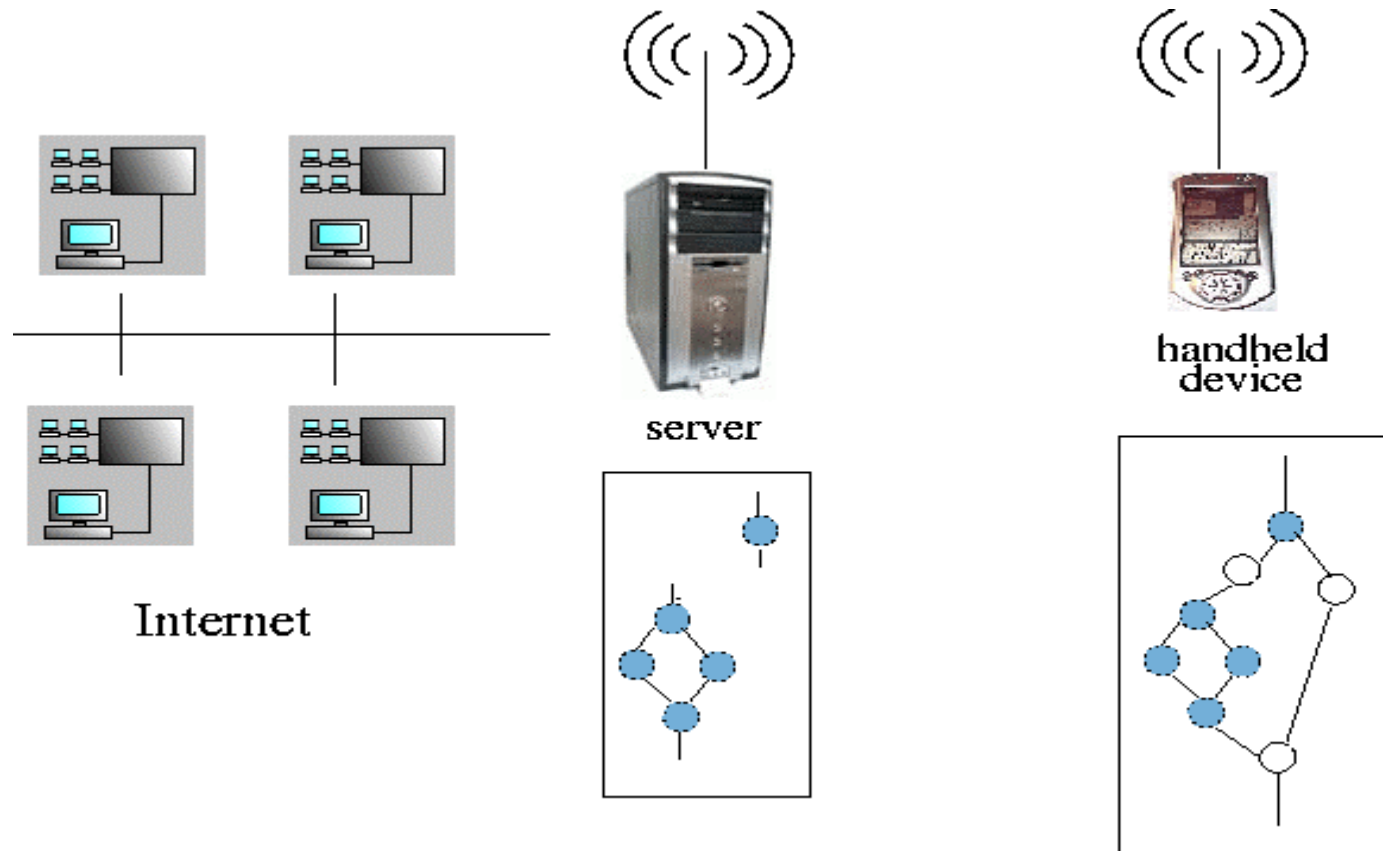


Handheld devices / wireless network

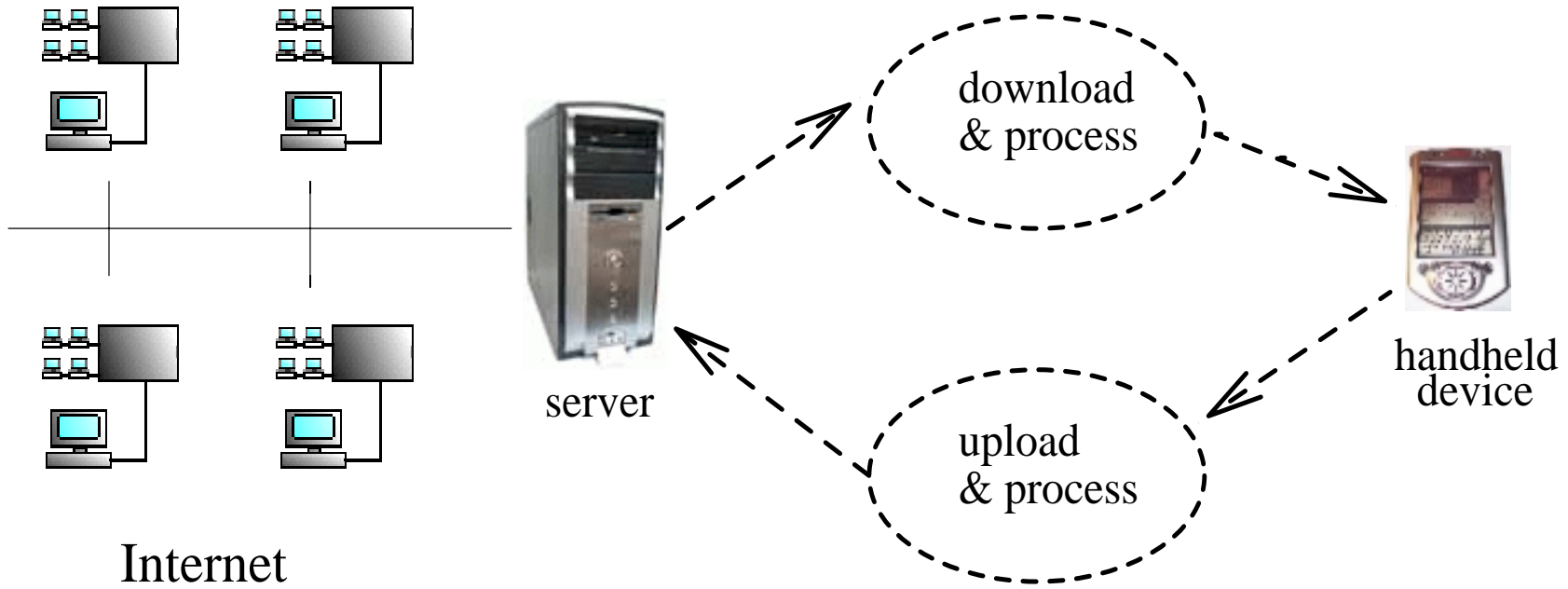


- More than an organizer ...
 - Computation on the move
 - Internet access on the move
 - Multimedia on the move
- Issues:
 - Battery life
 - Limited computation power
 - Limited memory

Offloading



Offloading





Security of wireless computation

- Wireless is not “safe”
- WEP is not enough
- Strong encryption mechanisms, such as IPSEC are needed
- What is the impact to offloading?

IPSec



- Protecting any traffic over IP layer
- Transparent to applications
- Authentication and encryption
- Option of compression

Execution Model



- Task Definition
 - Divide the normal program into tasks
 - Function call level tasks
- tasks mapping
 - Map tasks to server tasks or client tasks
 - Server tasks runs on the server
 - Client tasks runs on the handheld device
 - Static mapping using offline profiling information
 - Intrinsic client tasks
 - Some system calls, I/O



Energy Model

- Profiling Information
 - $s(i,j)$: size of data transfer from task i to task j .
 - $t_c(t)$: execution time for task t running on handheld device
 - $t_s(t)$: execution time for task t running on server
- Energy estimation
 - the energy consumed by executing task t as a client task,
$$e_c(t) = p_c t_c(t)$$
 - the energy consumed by executing task t as a server task,
$$e_s(t) = p_i t_s(t)$$
 - the energy consumed by transferring data d from client to server,
$$e_l(i,j) = p_s e(i,j) / b_s$$
 - the energy consumed by transferring data d from server to client,
$$e_r(i,j) = p_r s(i,j) / b_r$$

Secured Wireless LAN



- Commnucation cost increases
 - Extra energy to decrypt and encrypt
 - Packet expanded
 - Extra secure protocol traffic
- More tasks can be offloaded
 - Rsa_private_encrypt() in PGP
 - Sign a file digest with rsa private key
 - Not appropriate to offload in nonsecured environment since private key is needed for computation.



Experimentation setup

- Handheld device
 - Compaq iPAQ 3650, 206 MHz StrongArm SA 1100 processor, 32 MB RAM, 16 MB Flash Memory
- Supporting server
 - Pentium III 1.0 GHZ Dell Dimension 4100
- Wireless network
 - Lucent WaveLan Golden 11 Mb/s, covers up to 1750 feet



IPSec setup

- Linux FreeS/Wan 1.96
- Tunnel mode
- For each packet, encryption: 3DES, authentication: MD5
- RSA for host authentication
- The iPAQ and the server in the same subnet

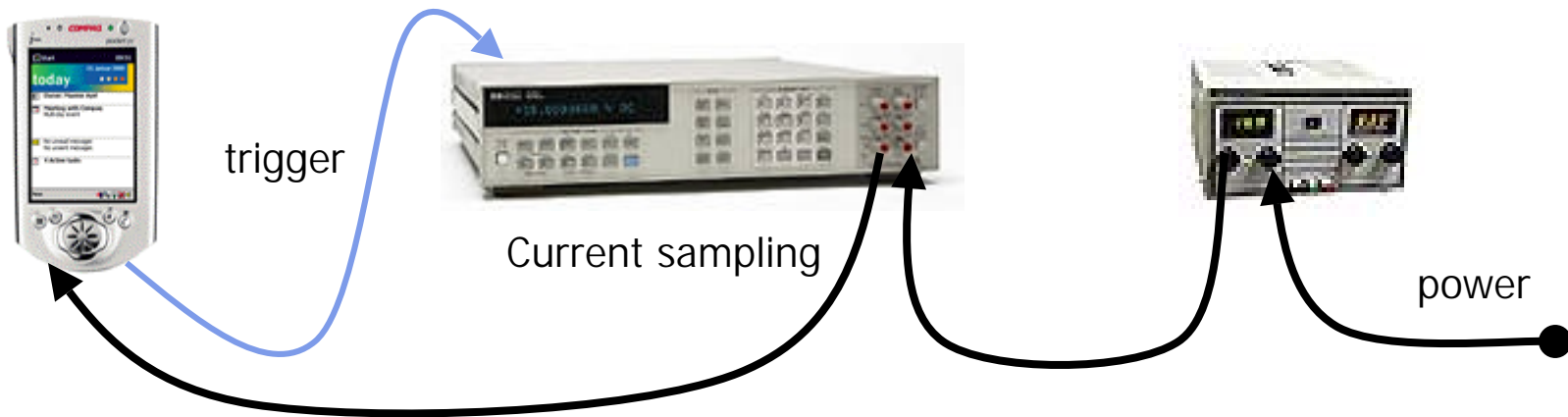
Physical Measurement



Compaq IPAQ 3650

HP 3458A Multimeter

AC power supply





Power parameters

- Power parameters

| iPAQ | Send/Recv | IPSec | Current(A) |
|------|-----------|-------|------------|
| Idle | No | - | 0.33 |
| Busy | No | - | 0.48 |
| - | Send | No | 0.44 |
| -- | Recv | No | 0.42 |
| -- | Send | Yes | 0.52 |
| -- | Recv | Yes | 0.45 |

- Effective bandwidth

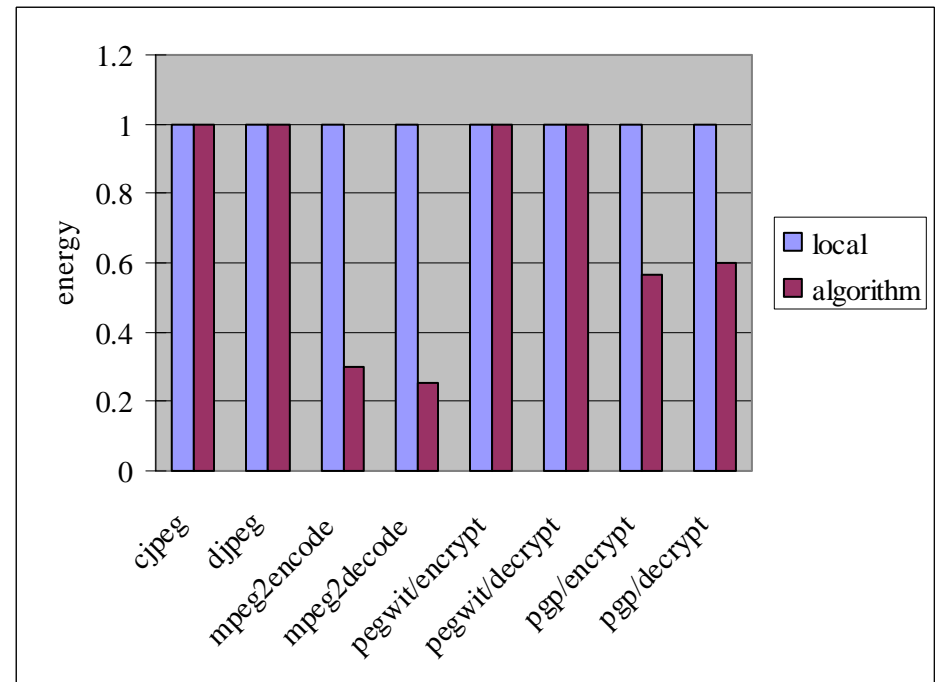
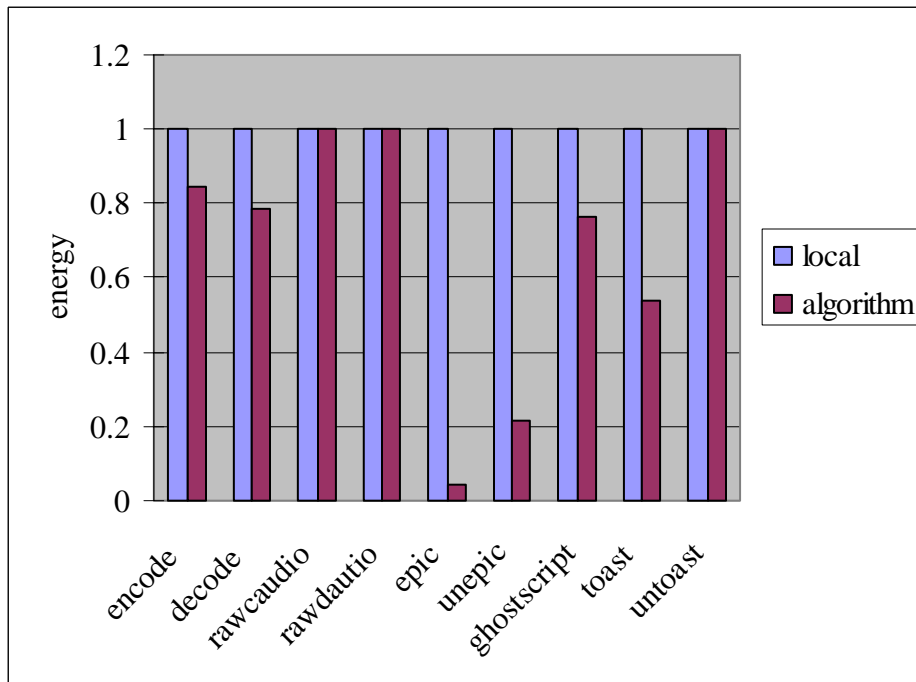
| Send/Recv | IPSec | Bandwidth (Mbps) |
|-----------|-------|------------------|
| Send | No | 5.0 |
| Recv | No | 5.1 |
| Send | Yes | 2.2 |
| Recv | Yes | 2.4 |



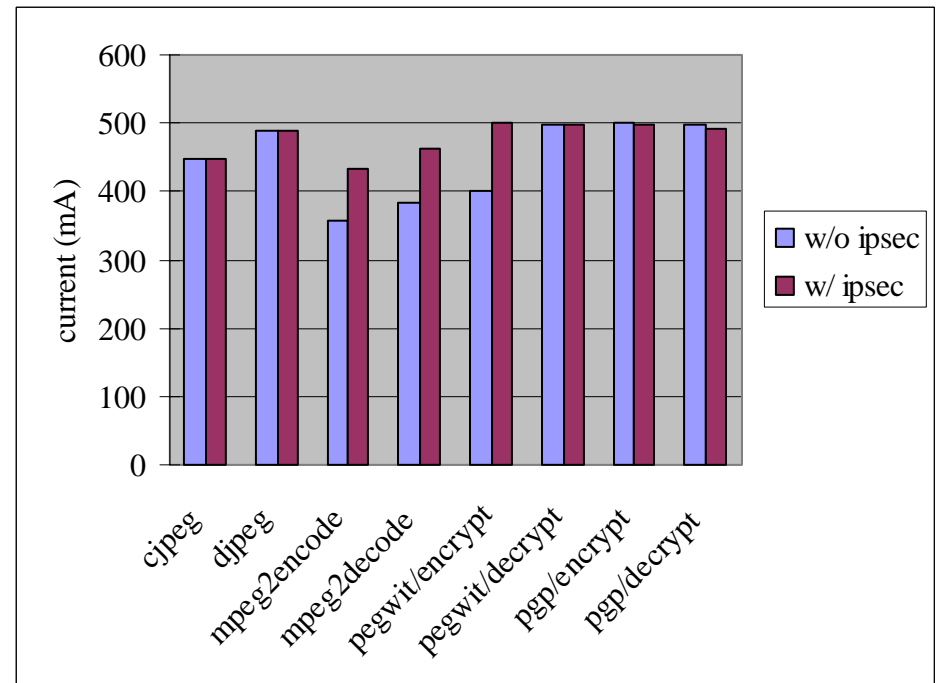
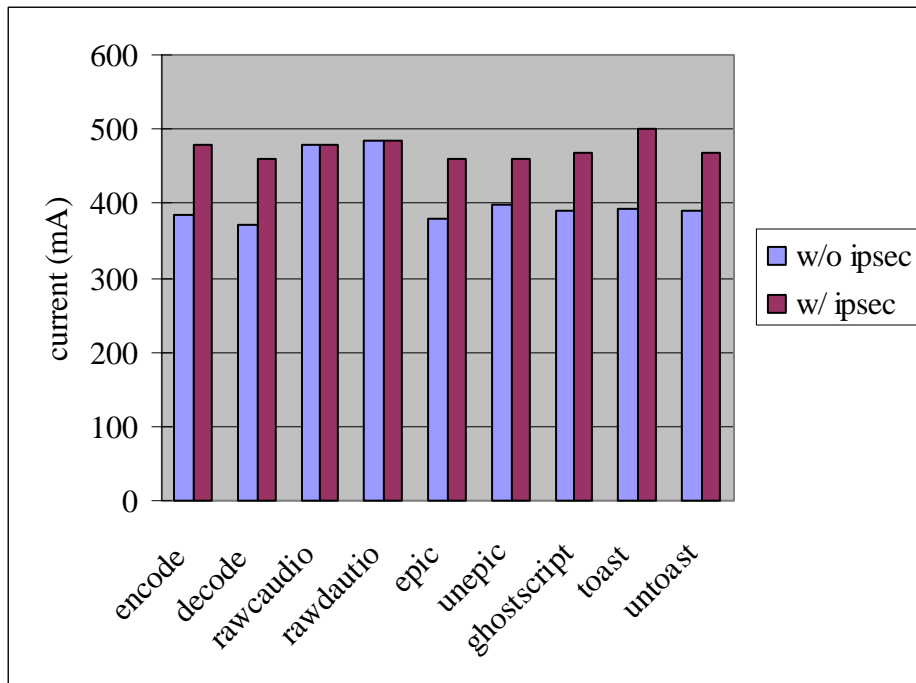
Mediabench programs

- Voice
 - GSM voice transcoding, G.721 voice compression/decompression, ADPCM
- Video/image
 - MPEG encoding/decoding, IJG JPEG compression/decompression, EPIC, GS
- Security
 - PGP and PEGWIT encryption/decryption

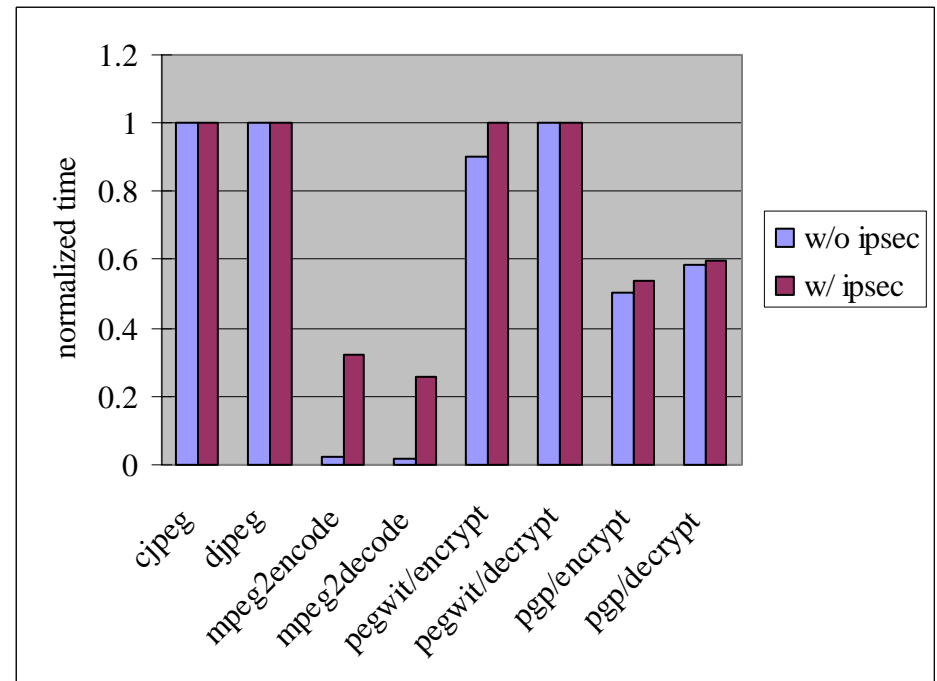
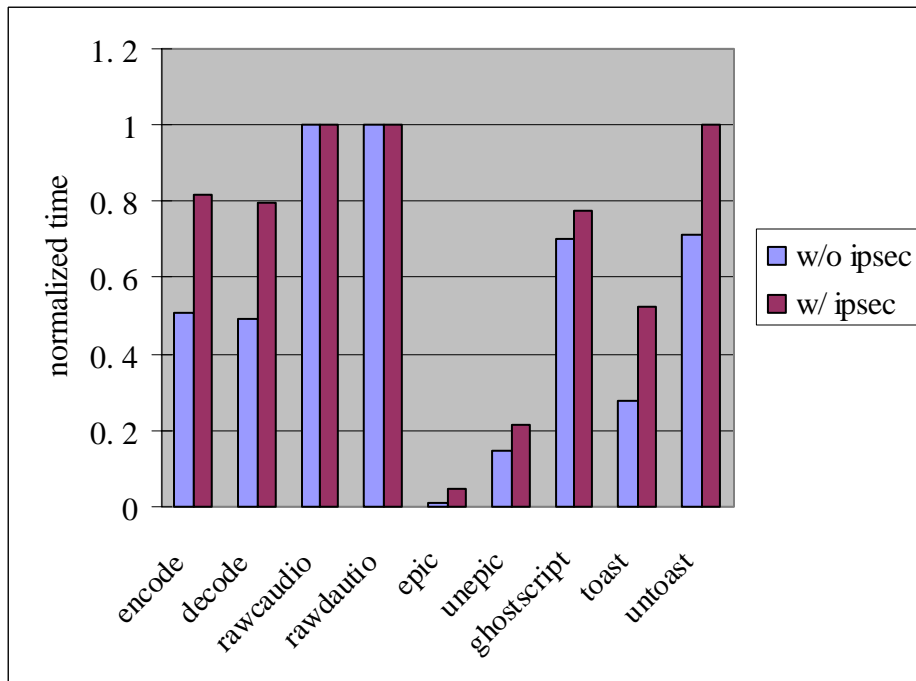
Normalized energy consumed on the handheld device (All data local)



Electrical current drawn in the handheld device (All data local)



Normalized running time on the handheld device (All data local)





Conclusion

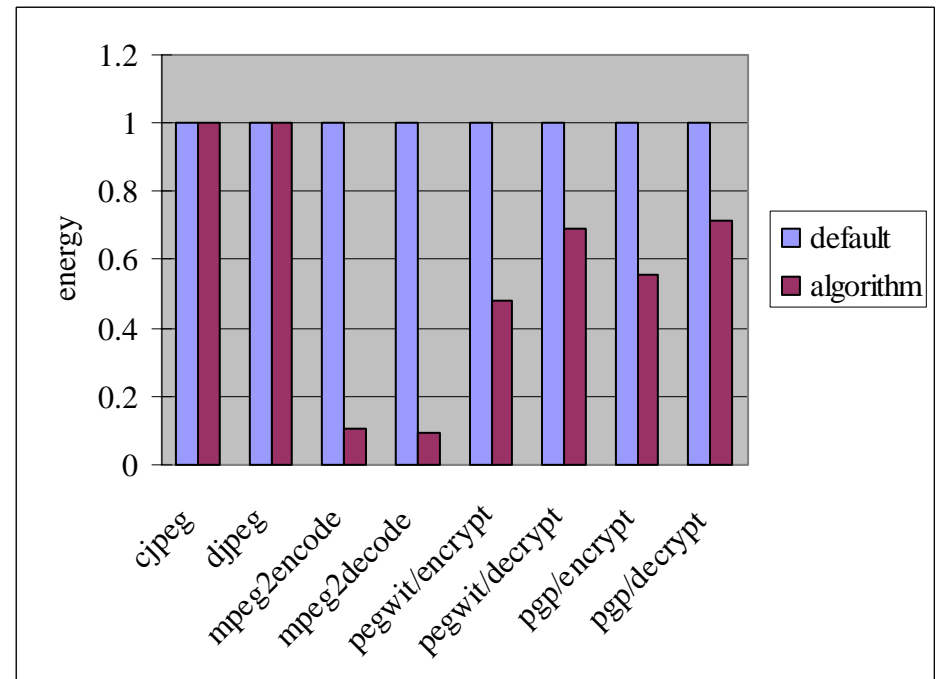
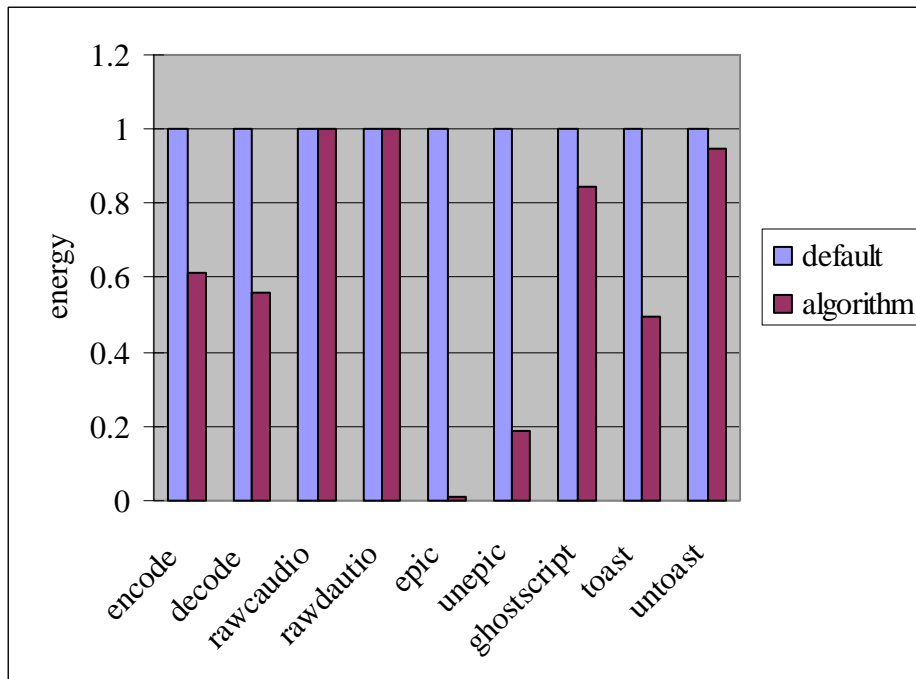
- Experiments are performed on a suite of multimedia benchmarks in a secured wireless LAN.
- Among 25 test cases which previously benefited from offloading, 23 of them remain to benefit. The average energy saving of offloading is 51% which decreases from the average of 70% in a nonencrypted environment.
- Despite the overhead of the security mechanism, offloading remains quite effective as a method for energy saving.

Distributed multimedia processing

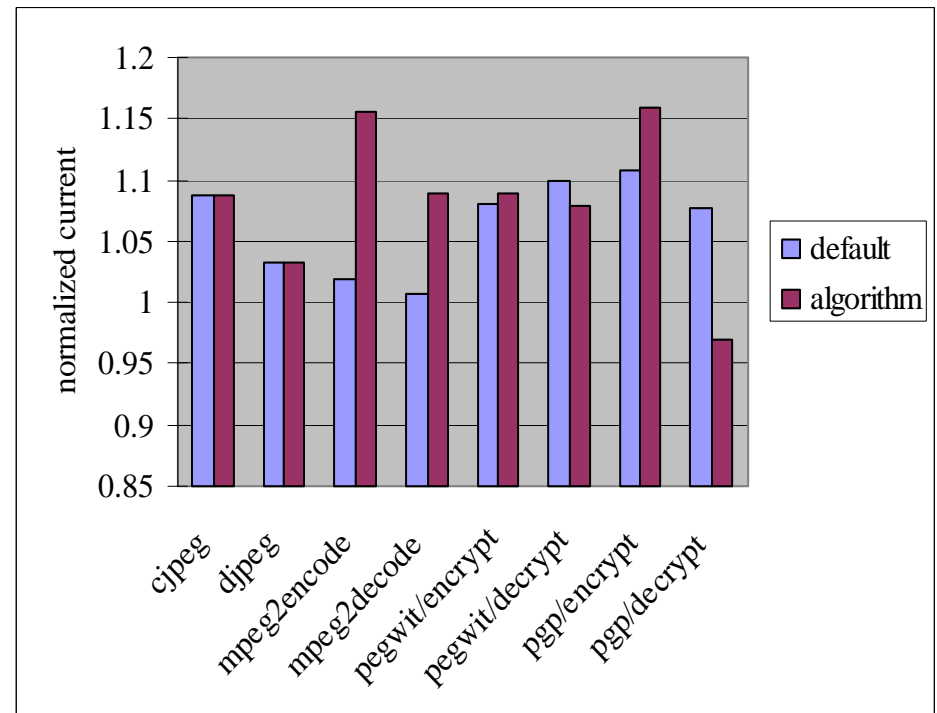
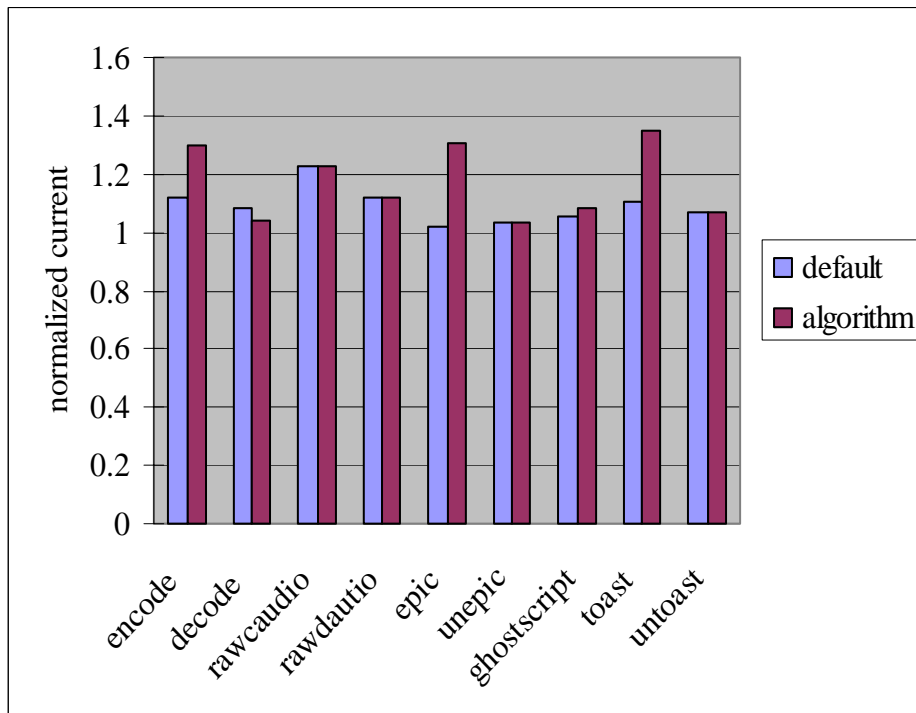


| progam | mode | program | mode |
|-------------|--------|----------------|--------|
| encode | c -> s | cjpeg | c -> s |
| decode | s -> c | djpeg | s -> c |
| rawcaudio | c -> s | mpeg2encode | c -> s |
| rawdaudio | s -> c | mpeg2decode | s -> c |
| epic | c -> s | pegwit/encrypt | c -> s |
| unepic | s -> c | pegwit/decypt | s -> c |
| ghostscript | s -> c | pgp/encrypt | c -> s |
| toast | c -> s | pgp/decrypt | s -> c |
| untoast | s -> c | --- | --- |

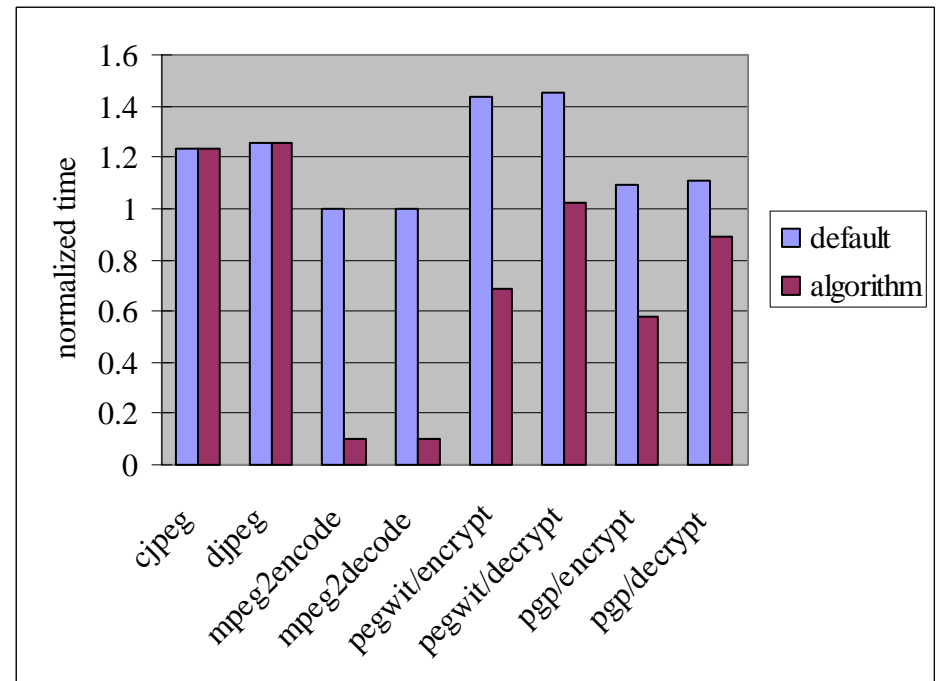
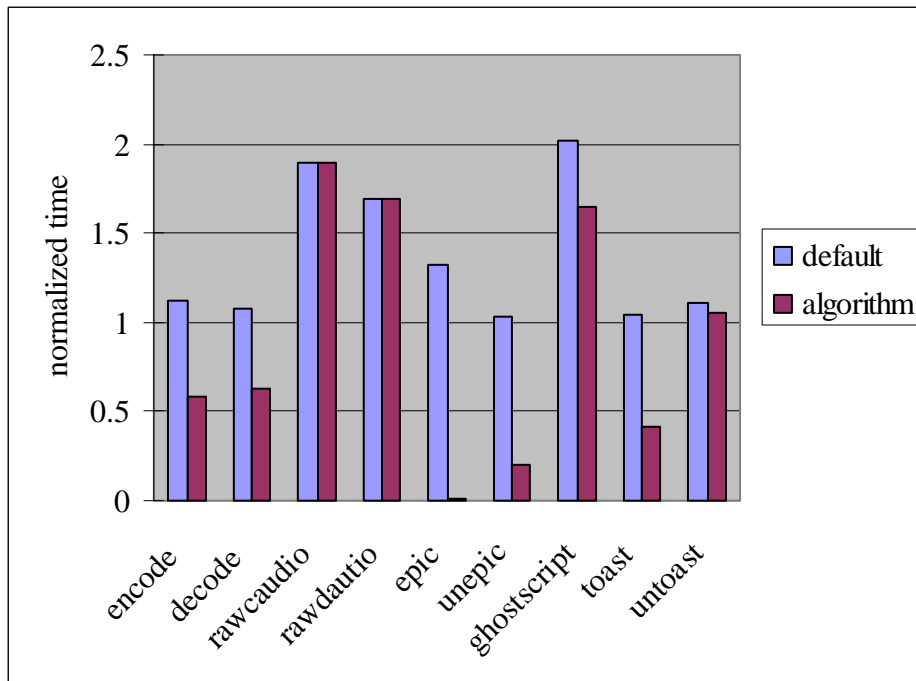
Normalized energy consumed on the handheld device (input & output separated)



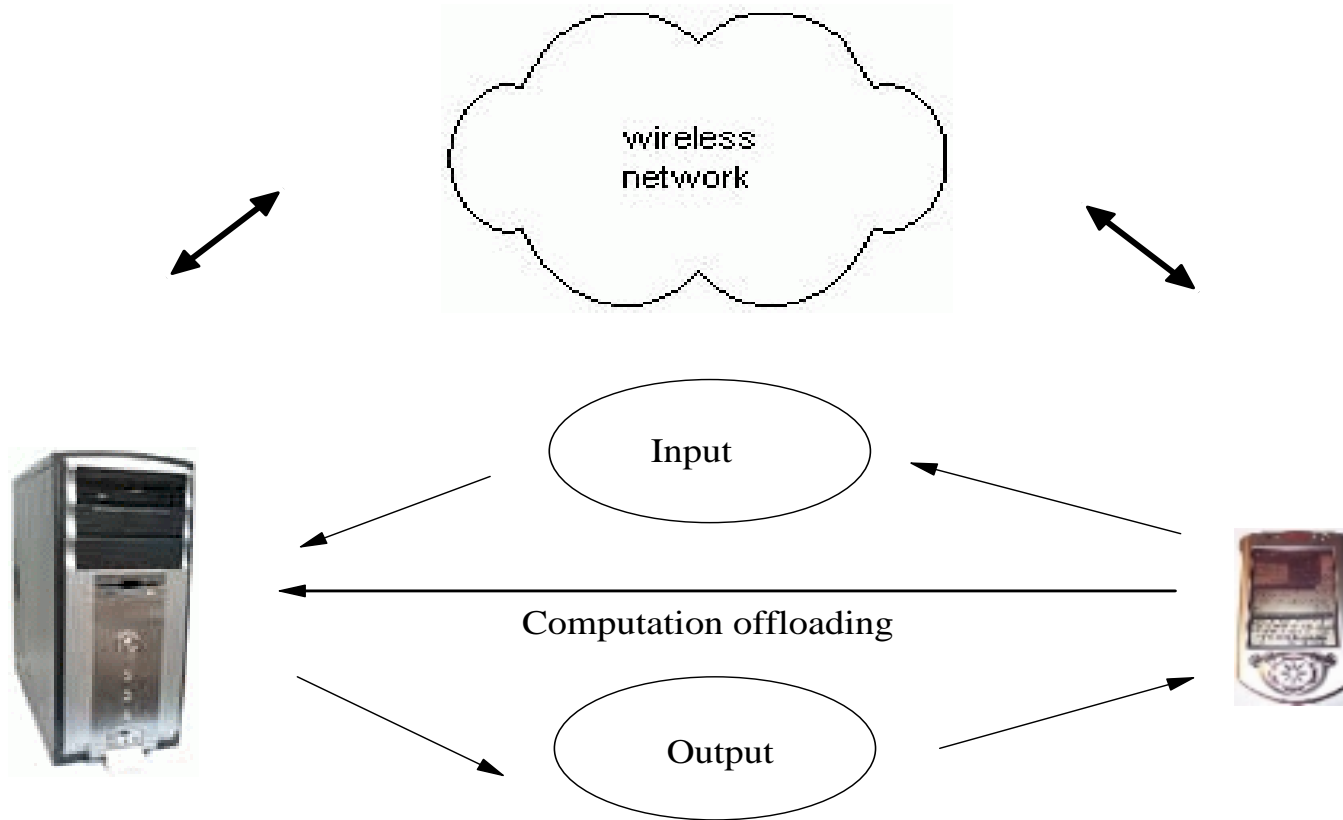
Electrical current drawn in the handheld device (input & output separated)



Normalized running time on the handheld device (input & output separated)



Offloading





Offloading

- Offload part or all computation to the Server
- Benefits
 - Reduce energy consumption
 - Enhance performance
 - Reduce memory requirement on handheld devices
- Not always gain
 - Extra energy consumed in sending/receiving
 - Energy on waiting results