QoS and Security in Energy-harvesting Wireless Sensor Networks

Antonio V. Taddeo, Marcello Mura,

<u>Alberto Ferrante</u>

ALaRI, Faculty of Informatics, University of Lugano

e-mail: ferrante@alari.ch

Università della Svizzera italiana

SECRYPT 2010

Advanced Learning and Research Institute

A. Ferrante – 1 / 24



Introduction

Security and QoS Management

Case Study



A. Ferrante – 2 / 24

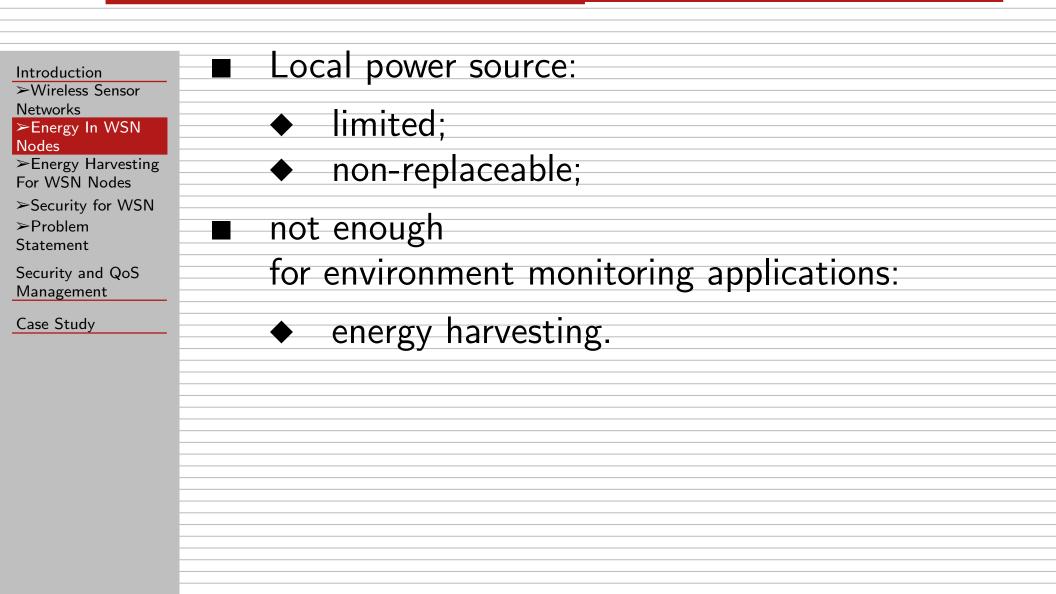
Wireless Sensor Networks

Introduction >Wireless Sensor Networks >Energy In WSN Nodes >Energy Harvesting For WSN Nodes >Security for WSN >Problem Statement Security and QoS Management Case Study	Composed of a large number of nodes: small; inexpensive; capabilities: sensing, processing, communication.
della Learning Svizzera Italiana Institute ALaRI	

SECRYPT 2010

A. Ferrante – 3 / 24

Energy In WSN Nodes



A. Ferrante – 4 / 24



Energy Harvesting For WSN Nodes

Introdu ≻Wire	iction less Sensor	Solar panels:
Nodes ≻Energ For WS	gy In WSN gy Harvesting SN Nodes rity for WSN	 the most used technology at the moment; they introduce a further level of uncertainty in the amount of energy available.
Statem	ient	
Securit Manag	y and QoS ement	
Case S	tudy	
Università	Advanced	
della Svizzera	Learning and Research	
italiana	Institute ALaRI	

A. Ferrante – 5 / 24

Security for WSN

Introdu	uction less Sensor	 Required by many applications;
Netwo		resource consuming;
Nodes		
≻Ener	gy Harvesting	 increases consumed energy;
	SN Nodes	■ static.
	rity for WSN	
≻Prob Statem		
Staten	iciti	
Securit	ty and QoS	
Manag		
Intanag		
Cons	باير، به	
Case S	study	
Università	Advanced	
della Svizzera	Learning and Research	
italiana	Institute ALaRI	
_		

A. Ferrante – 6 / 24

Problem Statement

Introduction	
≻Wireless Sensor	
Networks	th
≻Energy In WSN	
Nodes	
≻Energy Harvesting	
For WSN Nodes	
For VVSIN Modes	
≻Security for WSN	
≻Problem	
Statement	
Statement	
Security and QoS	
Management	
Management	
Case Study	
Case Study	

Università della Svizzera italiana Università della Learning and Research Institute ALaRI

SECRYPT 2010

There may be periods of time in which the energy available is very limited:

maximize node lifetime;

 maximize the number of packets sent with the energy available.

A. Ferrante – 7 / 24

Security and QoS Management

Introduction	
Security and QoS	
Management	
≻Security and QoS	-
Management	
≻Optimization	
Mechanism	
≻Energy Model	
≻Packet	
Characteristics	
≻Optimization	-
Strategies	
➤Possible Actions	
>Security	
Considerations	
	-
Case Study	

Change security settings dynamically to:

maximize security;

maximize the number of packets sent.

A. Ferrante - 8 / 24

Use QoS to:

increase the probability

of delivering critical packets.



Optimization Mechanism (1/2)

Introduction	
Security and QoS	
Management	
≻Security and QoS	
Management	
≻Optimization	
Mechanism	
≻Energy Model	
≻Packet	
Characteristics	
>Optimization	
Strategies	
≻Possible Actions	

➤Security Considerations

Case Study

Monitor-Controller-Adapter loop:

 Monitor: monitors available energy, packets to be sent;

Controller: decides which packets to send

A. Ferrante – 9 / 24

and the security suites to be used;

Adapter: actuates the decisions

taken by the Controller.



SECRYPT 2010

Advanced

Learning and Resea

Optimization Mechanism (2/2)

Introdu	uction	The <i>Monitor</i> requires:
Securit	y and QoS	
Manag	ement	
		an energy model;
≻Secu	rity and QoS	
Manag		
		packet characteristics.
≻Onti	mization	
Mechai	nism	
≻Energe	gy Model	
≻Pack	et	
Charac	teristics	
≻Optıı	mization	
Strateg		
Juareg	sies	
> Possi	ible Actions	
≻Secu	rity	
	erations	
Conside	erations	
Case S	tudy	
Cuse 5	tudy	
Università	Advanced	
della	Learning	
Svizzera italiana	and Research Institute	

A. Ferrante – 10 / 24

Energy Model



Security and QoS Management >Security and QoS Management >Optimization Mechanism

≻Energy Model

≻Packet
 Characteristics
 ≻Optimization
 Strategies

Possible Actions
 Security
 Considerations

Case Study

 Necessary to estimate the energy that will be used to send the packets in the queue;
 E_{packet} = E_{tx} + E_{errors}
 available energy updated with real data after the packets have been sent;
 in each transmission time slot ∑ E_{packet} must be below E_{frame}.

A. Ferrante – 11 / 24

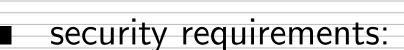


Packet Characteristics

Introduction	
Security and QoS	-
Management	
≻Security and QoS	
Management	
>Optimization	
Mechanism	
≻Energy Model	
≻Packet	-
Characteristics	
>Optimization	
Strategies	
➤Possible Actions	
≻Security	
Considerations	
Considerations	
Case Study	

Payload	size
priority:	

◆ 1-4;



choice of security suites

that fit the security needs

of the considered packets.





Optimization Strategies

Introduction
Security and QoS Management
≻Security and QoS
Management ≻Optimization
Mechanism ≻Energy Model
≻Packet
Characteristics > Optimization
Strategies
≻Possible Actions≻Security
Considerations

Case Study

Composition of actions to be performed to meet the energy constraint; two goals:

maximize the number

of high-priority packets delivered;

ensure that the security requirements

of packets are met.

Università Advanced della Learning Svizzera and Resear italiana Institute ALaRI

and Research Institute ALaRI

SECRYPT 2010

A. Ferrante – 13 / 24

Possible Actions

Introduction	
Security and QoS Management	
 Security and QoS Management Optimization Mechanism Energy Model Packet Characteristics Optimization 	
Strategies ≻Possible Actions	
 ➢ Security Considerations 	
Case Study	

Change the security suite used for packets;
 limit number of packets to be sent:

A. Ferrante - 14 / 24

 drop or delay packet transmission according to priorities.



Security Considerations (1/2)

	luction
Introc	luction
IIIUUU	IUCLIOII

Security and QoS Management →Security and QoS Management →Optimization Mechanism →Energy Model →Packet Characteristics →Optimization Strategies →Possible Actions →Security

Considerations

Case Study

The use of multiple cryptographic algorithms may lower global security:

A. Ferrante – 15 / 24

limited problem

when packets are independent;

the self-adaptation mechanism is designed to provide the highest security level

compatible with packet settings

and system conditions;



Security Considerations (2/2)

h+rod	uction
murou	uction

Security and QoS Management >Security and QoS Management >Optimization Mechanism >Energy Model >Packet Characteristics

≻Optimization Strategies

≻Possible Actions≻SecurityConsiderations

Case Study

the minimum level of security specified in the security requirements is always granted. our solution provides the ability to guarantee at least *some* security even when energy is scarce.



A. Ferrante – 16 / 24

Case Study (1/2)

Introduction

Security and QoS Management

Case Study

≻Case Study

≻Simulations

≻Results

≻Conclusions and

Future Work

7-node WSN;

802.15.4, beaconed mode;

star topology;

each node is equipped with:

♦ a solar cell;

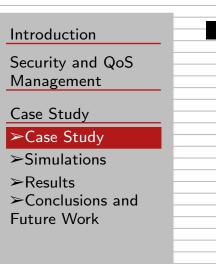
a super-capacitor of 310Farad;

node lifetime of 3 days without solar recharge;

A. Ferrante – 17 / 24



Case Study (2/2)



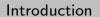
each node is equipped with a digital camera:

- it acquires an image every 30s;
- it sends the image to the base station;
- for every image:
 - 160 packets of 90 bytes;
 - pictures divided into 5 segments;
 - priorities uniformly assigned
 - to packets of the same segment.





Simulations



Security and QoS Management

Case Study

≻Case Study

≻Simulations

≻Results
 ≻Conclusions and
 Future Work

Case study simulated through a SystemC network simulator:

based on

an implementation-independent model;

- simulates node operations;
- simulates network operations;
 - annotates power consumption;
- manages

channel contention and retransmission.

A. Ferrante – 19 / 24



Results (1/4)

-	
Intro o	luction
Introc	luction

Security and QoS Management

Case Study

≻Case Study

≻Simulations

≻Results

➤Conclusions and Future Work Each node lasts 4 days instead of 3 when a limit on consumed energy is set;

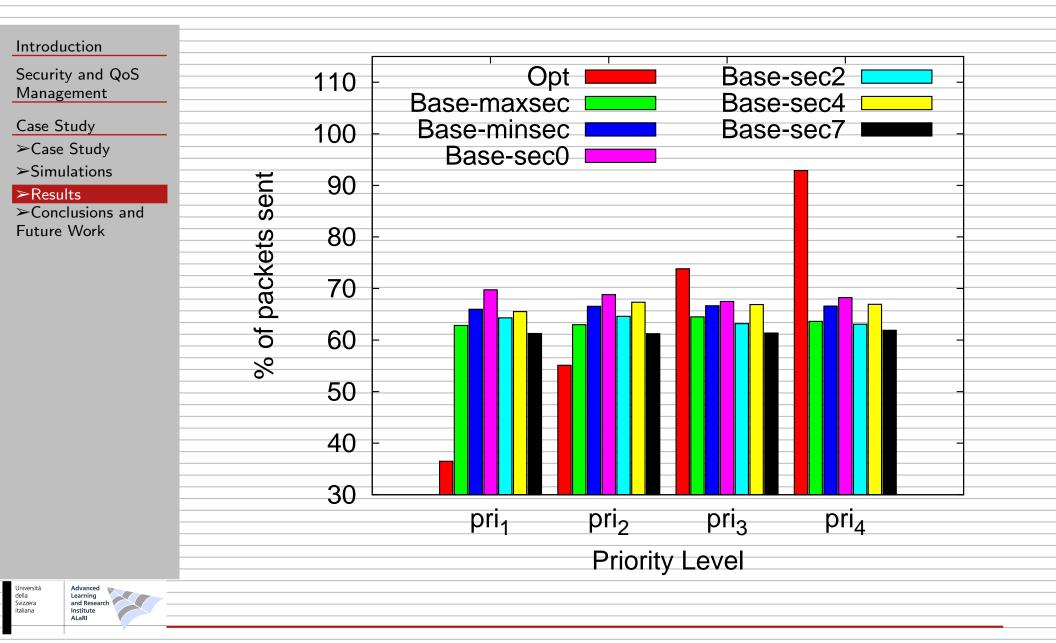
security adaptation improves security;

QoS improves the management

of important packets.



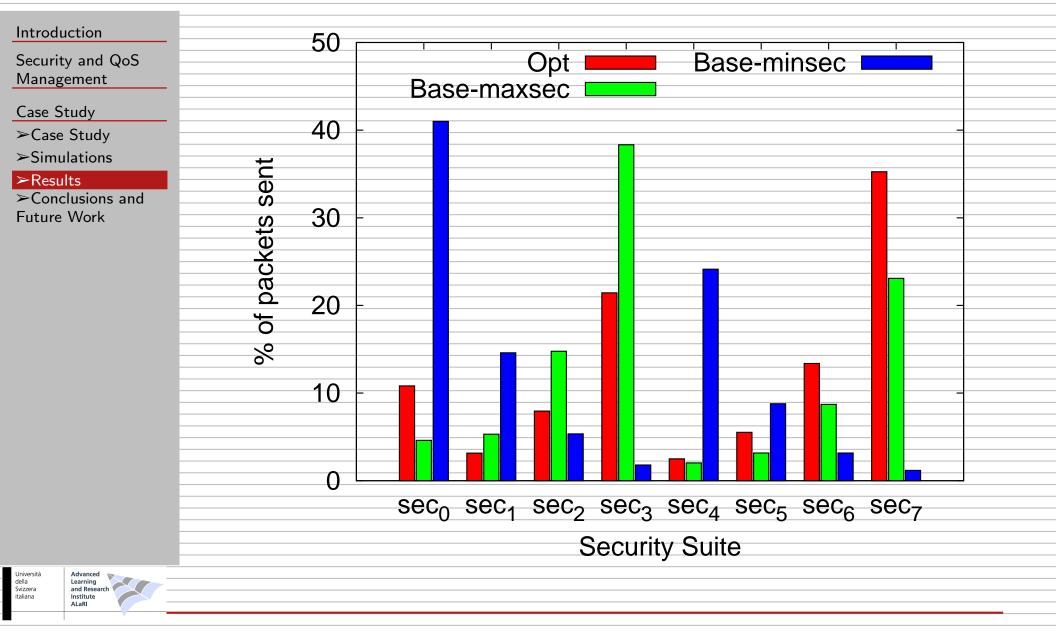




SECRYPT 2010

A. Ferrante - 21 / 24

Results (3/4)



SECRYPT 2010

A. Ferrante – 22 / 24



Introdu	uction		6				
Securit Manag	zy and QoS gement		U	Opt vs maxsec		Opt vs sec2 Opt vs sec4 Opt vs sec7	
<u>Case S</u> ≻Case			4	Opt vs minsec Opt vs sec0		Opt vs sec7	
	lations	byte					
	clusions and	per b <u>i</u>	2				
			0				
		energy					
		% of	-2				
			-4	_			
			-6		Syster	n	
Università della Svizzera italiana	Advanced Learning and Research Institute ALaRi				- ,		

SECRYPT 2010

A. Ferrante – 23 / 24

Conclusions and Future Work

Introduction		
Security and QoS Management		
Case Study		
≻Case Study		
≻Simulations		
≻Results		
➤Conclusions and		
Future Work		

 Conclusions:
 our mechanism changes security dynamically;
 it implements a QoS system to privilege important packets;
 our mechanism allows the nodes to manage packet transmission in an efficient way.

Future work:

refinement and extension of the methodology;
 implementation and testing in real nodes.

Università della Learning Svizzera and Resear italiana Institute ALaRI



A. Ferrante – 24 / 24