AAU Ph.D. Degree

Updated plan of research

Title:

Energy Efficient Authentication and Authorization for Multi-node Cooperative Connectivity and Reliability

PhD Candidate:

Vandana Rohokale

(vmr@es.aau.dk)

Supervisor

Prof. Ramjee Prasad

CTIF, Aalborg, Denmark

Co-supervisors

Assoc. Prof. Horia Cornean
AAU, Aalborg, Denmark

Prof. Debasis Saha
IIM, Kolkata, India

AALBORG UNIVERSITET

Updated PhD Study Plan

Ph.D. Programme: Wireless Communications

Project title: Energy Efficient Authentication and Authorization for Multi-node Cooperative Connectivity and Reliability

Ph.D. student: Mrs. Vandana Milind Rohokale Email: - vmr@es.aau.dk

Education: Master of Electronics Engineering (Mobile and Broadband Communication)

Institution: R.I.T. Sakharale, Maharashtra, India

Academic supervisor: Prof. Ramjee Prasad**,** CTIF, Aalborg, Denmark

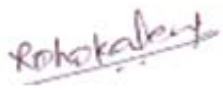
Co-supervisors: Horia Cornean, AAU, Aalborg, Denmark
Prof. Debasis Saha, IIM, Kolkata, India

Department: Institute of Electronic Systems

Date of enrolment: 15 Nov, 2009

Expected date of Completion: 14 Nov, 2012

Signature



Date: Ph.D. Student

Study plan approved

Date**:**	Academic Supervisor	Prof. Ramjee Prasad
Date	Head of Department	Prof. Børge Lindberg
Date	Head of PhD program	Gert Frølund Pedersen

Contents

Energy Efficient Authentication and Authorization for Multi-node Cooperative Connectivity and Reliability

SECTION 1: RESEARCH WORK SUMMARY/ ABSTRACT

The cooperative wireless communication (CWC) concept is more applicable to wireless sensor networks and Cognitive ad-hoc networks than that of cellular networks. In CWC, the active nodes may increase their effective QoS via cooperation. Cooperative diversity is a strong technique, which can provide the maximum throughputs. Opportunistic Large Array (OLA) is nothing but a cluster of network nodes, which use active scattering mechanism in response to the signal of the source called leader. The intermediate nodes opportunistically relay the messages from the leader to the sink. Cooperative OLA algorithms can improve the reliability as well as the energy efficiency of the communication.

Ensuring that the distributed public-keys are authentic is essential to security of the system and this issue is known as the "man-in-the middle attack." In cooperative wireless communication, security against man-in-the-middle type of attacks is very much essential. Security of private key cryptosystems depends on the secrecy of the secret key. In case of public key systems, it is infeasible to derive private key from the public key. Breaking of a public key is a complex and timely task. Wireless sensor nodes are inherently memory and energy constrained. Today's commonly utilized algorithms such as RSA, Diffie-Hellman, NTRU and Elliptic Curve Cryptography make use of large numbers multiplication in their encryption and decryption mechanisms. Due to their huge demand of memory and energy, these cryptographic algorithms can't be employed to wireless sensor nodes. This research work proposes a novel secure CoopMAC protocol making use of braid group based cryptography.

This report includes research activities and directions for PhD study in the area of Energy Efficient Authentication and Authorization for Multi-node Cooperative Connectivity and Reliability. First section explains the essentials of Cooperative Wireless Communication. In next section, state of the art in CWC related with energy efficiency and reliability is elaborated. After that the scope of the work is limited till authentication and authorization in Opportunistic Large Arrays in CWC-WSNs. Next section focuses on the challenges from literature survey, in the scope of the work. From those challenges, Energy Efficient Authentication and Authorization for Multi-node Cooperative Connectivity and Reliability are highlighted and finally drawn the conclusions and mentioned the future work based on the problem statement.

SECTION 2. SCIENTIFIC CONTENTS OF RESEARCH

a. Research Work Background

Wireless communication is a great revolution but it still suffers from limited battery life, broken connections from multi-path fading and insufficient coverage. Simple cooperation can make a big difference in coverage range, energy and battery life. In CWC, the active nodes may increase their effective QoS via cooperation. This research work proposes the development of an energy efficient novel approach for security mechanism for cooperative transmission of the information with peer to peer as well as centralized mutual authenticated communication. The comparison in between CT and DT is mentioned in table 1 below.

Table1: Differences between Direct and Cooperative Communication

	Cooperative Transmission	Direct Transmission
Components	Leader, Relay and Sink nodes	Source and destination
Communications	Cooperative	Single-hop or Multi-hop
Protocols	Cross layer (PHY+MAC)	Single layer
Mechanisms	Decode and forward, Amplify and forward, Coded Transmission	Simple transmission
Reliability	High reliability with less error probability	Less reliability due to increased error probabilities
Transmit Power	Less draining of power	Direct and Cooperative Communication
Coverage Area	Increased	Fixed
Shadowing	Resistant to large scale shadowing	Less resistance to shadowing

b. State-of –the-art for Research Work

In cooperative communication, the information overheard by neighboring nodes is intelligently used to provide the healthy communication between a source and the destination called as sink. The sink node or destination receives numerous editions of the message from the source, and relay(s) and it estimates these inputs to obtain the transmitted data reliably with higher data rates. Liu et.al.in [1], has explained the idea of integration of PHY cooperation with MAC sub layer for the improvements in throughput and interference. In cooperative resource allocation, each node transmits for multiple nodes. Effective QoS (different error measurements such as bit error rate, block error rates or outage probability) of the individual network nodes can be improved through cooperation [2].

Opportunistic Large Array (OLA) is nothing but a cluster of network nodes which use active scattering mechanism in response to the signal of the source called leader. The intermediate nodes opportunistically relay the messages from the leader to the sink [3]. The authors have suggested an optimal power allocation mechanism in [4]. It includes a class of diversity protocols for multi-node wireless network utilizing relaying strategies depending on the distance of relay either with source or sinks. Higher data rates at the reduced transmit power can be converted to an increase in cell coverage [5].

Relaying and cooperative diversity essentially creates a virtual antenna array. All of the cooperative diversity protocols are efficient in terms of full diversity achievement and optimum performance except fixed decode-and-forward approach. Although prior to Laneman [6], the work on relay and cooperative channels utilized full duplex approach, he has constrained the cooperative communication to employ half duplex transmissions. Also the Channel State Information (CSI) is employed in the receiver instead of transmitter.

Table 2. Security Implications of CoopMAC in wireless networks [15]

Wireless LAN Protocol	Data rate per stream (Mbps)	Modulation	Approx indoor range (m)	Approx outdoor range (m)	Pros	Cons	Security Provision
IEEE 802.11 The original 2.4 GHz wireless LAN protocol including infrared	1 , 2 , 10	FHSS			Also includes infrared communication.	Lowest data rates	
IEEE 802.11a The WLAN in 5 GHz UNII band.	6, 9, 12, 18, 24, 36, 48, 54	OFDM			The 5GHz UNII band consists of 3 sub-bands with a defined max output power.		
IEEE802.11b uses 2.4 GHz ISM band and uses the CSMA/CA media access method.	5.5, 11	DSSS	38	140	Lowest cost; signal range is good and not easily obstructed	slowest maximum speed; home appliances operating in the 2.4 GHz band may interfere on the unregulated frequency	It uses Wired Equivalent Privacy (WEP) security.
IEEE802.11g operates at a maximum physical layer bit rate of 54 mbps.	6, 9, 12, 18, 24, 36, 48, 54	OFDM, DSSS	38	140	Fast maximum speed; signal range is good and not easily obstructed	costs more than 802.11b; appliances may interfere on the unregulated	It uses WEP encryption with some companies including a Wi-Fi Protected Access (WPA) encryption supplement.
IEEE802.11i standard concentrates on resolving the security holes present in past standards.	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2	OFDM	70	250	802.11i has a pre-shared key mode (PSK), designed for home and small office networks that cannot afford the cost and complexity of an 802.1X authentication server.	Not suitable for cooperative wireless communication	The *802.11i* standard is meant to improve the security of data transfers (by managing and distributing keys, and implementing encryption and authentication). This standard is based on the *AES* (Advanced Encryption Standard).
IEEE802.11af Wi-Fi in TV spectrum white spaces and is more correctly known as power over ethernet (PoE).	144 Mbps	OFDM, DSSS	Upto 100 m	Upto 5 km	Very useful for the powering of VoIP and video data treams.Known as Super Wi-Fi.	Under development	Yet to be designed

In [7], the authors have proposed heuristic approximate algorithms with Cooperative Wireless Advantage (CWA) to provide suboptimal but scalable solutions for the minimum energy broadcasting approach. Since the wireless sensor nodes can switch in between active and sleep mode, the solution is based on the Long Preamble Emulation (LPE) MAC layer algorithm which emulates the asynchronous MAC protocol [12]. Liu et al. in [13], proposed the first cooperative MAC protocol called Coop MAC based on the well known IEEE 802.11 protocol.

Even though the cooperation is originating from physical-layer cooperation, all the above mentioned benefits cannot be fully realized until proper mechanisms have been incorporated at higher protocol layers (e.g., MAC, network) and the necessary information is made available from the lower layer (e.g., PHY). Indeed, a cross-layer approach has to be followed to reap all the benefits of cooperation. Through the cooperative MAC protocol, an additional three-way handshake procedure and a new signaling message have to be introduced to the MAC layer, and information on channel conditions for related wireless links should be made available to the upper layers so that the cooperation can be fully enabled. Another example of a cross-layer approach to cooperation, which involves interaction between the application layer and the physical layer, is provided in for transmission of video signals over wireless links [13]. Security Implications of CoopMAC in wireless networks are shown in Table 2.The CoopMAC protocol can be applied to the cooperative wireless sensor networks by taking into account the resource constrained radio sensor nodes.

Ensuring that the distributed public-keys are authentic is essential to security of the system and this issue is known as the “man-in-the middle attack.” In cooperative wireless communication, security against man-in-the-middle type of attacks is very much essential. Security of private key cryptosystems depends on the secrecy of the secret key. In case of public key systems, it is infeasible to derive private key from the public key. Breaking of a public key is a complex and timely task. Wireless sensor nodes are inherently memory and energy constrained. Today’s commonly utilized algorithms such as RSA, Diffie-Hellman, NTRU and Elliptic Curve Cryptography make use of large numbers multiplication in their encryption and decryption mechanisms. Due to their huge demand of memory and energy, these cryptographic algorithms can’t be employed to wireless sensor nodes.

b.1. Evaluation of the State of the Art Techniques

Table 3:- Comparison of OLA algorithms

Parameter/Technique	**Delay**	**Energy saving / life extension**	**Reliability**	**Node Density /Scalability**	**Authentication And Authorization**	**Merit/Demerit**
Basic OLA [6] The avalanche of responses to the leader node is like the ola in a sports stadium.	Guaranteed to be constant	5 dB compared to DIB algorithm	With increased SNR values, BER reduces.	Reasonable node density with high scalability	**NOT ADRESSED UPTILL NOW**	With cooperative Tx, reach-back problem is solved

OLA-T [7] The node participation in each OLA is controlled by the power transmission threshold in Rx.	Constant delay	32% of the transmitted energy as compared to Basic OLA	Highly reliable coop communication	For constant ϵ values, ρ=2.65 nodes/m^2 with less scalability as compared to basic OLA		With full flooding approach, energy saving is 50%
OLA-VT [7] OLA with variable threshold, which optimizes thresholds as a function of level.	Can be slightly variable	25% of the transmitted energy as compared to Basic OLA	**NOT CONCENTRATED ON RELIABILITY ISSUES**	Slightly less scalable as compared to basic OLA		
A-OLA-T [8] Broadcast protocol alters between the sets of OLAs for each broadcast.	Variable delay	Can offer a 17% life extension as compared to Basic OLA and OLA-T		Highly scalable		Almost double power as compared to OLA is required.
OLACRA [8] It exploits the concentric ring shapes of broadcast OLAs to limit flooding on upstream connection.		75% as compared to full flooding approach		Possesses highest scalability		Level Ganging
OLACRA-T [9] The criteria to be met for OLACRA & their received power is less than a specified threshold.				Highly scalable		

c. Research Work Objectives

Cooperative communication is a promising technique that would enhance the design of WSN. Nowadays everybody wish to use their wireless equipments to make wireless security sensitive transactions like online banking, stock trading and shopping. In such cases, the protection of personal and business data is very much important. When a receiver receives a message, it may be concerned about who is the real sender and whether the content of the message has been changed illegally by somebody in the transmission. These are two major points that the authentication of messages takes care of. The authentication problems as well as secrecy problem become the two important aspects of information security in modern times.

Ensuring that the distributed public-keys are authentic is essential to security of the system and this issue is known as the “man-in-the middle attack.” In cooperative wireless communication, security against man-in-the-middle type of attacks is very much essential. Security of private key cryptosystems depends on the secrecy of the secret key. In case of public key systems, it is infeasible to derive private key from the public key. Breaking of a public key is a complex and timely task. Lot of work is in progress in the direction of enhancement of energy efficiency. But certain issues such as Trusted, Authenticated and Reliable connectivity in multi-node cooperative communication networks in consultation with energy efficiency are the real forthcoming challenges. The energy savings in CWC are the result of cross-layer interactive cooperative communication. Routing functions are partially executed in the Physical layer as shown in Figure 3. The diversity

provided by MIMO space-time codes can improve performance at the MAC, Network and Transport layers.

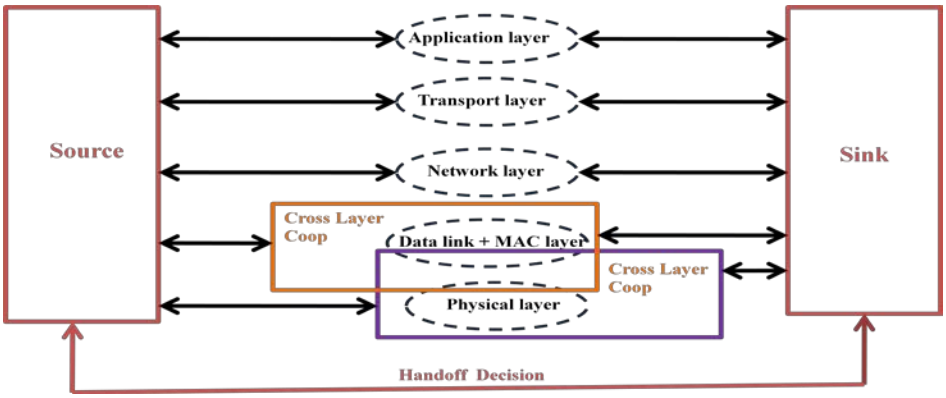


Figure 3: Cooperative Cross Layered Communication

c.1. Reliability and authenticity Issues in CWC

Due to signal enhancement in OLA, SNR_{CT} is much higher than SNR_{P2P} [3]. Due to increased SNR figures, highly reliable cooperative communication is possible (with less error probability). But since there are certain restrictions for further increase in SNR, some further study and experimentation is needed for reduction in error probability with considerable SNR values.

Authentication is the mechanism whereby systems may securely identify their users. Authentication systems provide answers to the questions:

- Who is the user?
- Is the user really who he/she represents himself to be?

Authorization, by contrast, is the mechanism by which a system determines what level of access a particular authenticated user should have to secure resources controlled by the system.

The importance of protecting the secrecy of sensitive messages has been realized by people since ancient times. By making use of strong techniques, the storage and transmission of information become cheap and simple in modern times. A huge amount of information is transformed in a way that almost anyone may access it. A lot of new problems related to cryptology appear. For example, an enemy might not only have the means to read transmitted messages, but could actually change them, or the enemy could produce and send a false message to the receiver and hope that this would initiate some action as shown in fig.5 below.

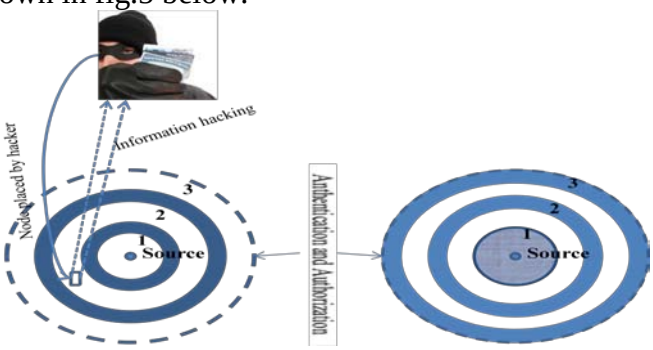


Figure 5: Authentication and Authorization issues in the OLAs. The colored strips represent the transmitting nodes (that form the OLAs) which alternate during each broadcast.

Now consider another example in which, we imagine a thief who has stolen an access to a bank's outgoing telephone line. When the thief visits the bank and deposits 100 Euros on his account, the bank sends a message to a central computer, telling the computer to add 100 Euros to the thief's account. By changing the content in the message, the thief can add a different amount, for example 1000 Euros, to his account. Another possibility would be to record the message transmitted by the bank and then send the same message several times, each time adding 100 Euros to the account. This example shows that it is necessary to have some mechanism to check that only messages sent by the bank will be accepted by the central computer. Here, the message needs to be authenticated.
In Cooperative Communication making use of Opportunistic Large Array approach, these issues like reliability, authentication and authorization are needed to be addressed and investigated in further research studies.

d. Key Methods

Following are some of the open areas in the related field

- Design Cooperative and Reliable MAC protocol
- Design efficient methodology for authentication using Group Based Cryptography.
- Develop an energy efficient novel approach for security mechanism for trustworthy transmission of the information.

When the OLAs are formed, the structure is assumed to be circular with different layers. The security, authentication and authorization issues come into picture either within one OLA or in between two OLAs during broadcast. In this work, it is planned to address the above mentioned issues with energy efficiency as well as to work on the design of reliable cooperative MAC protocol. Currently, the limited battery life of network nodes and restricted coverage area are the critical isues in the wireless sensor networks. With effective utilization of green energy sources and employing energy efficient routing mechanisms such as concentric OLAs, the proper solution could be achieved.

As per the state of the art described in Table 3, the shaded part clearly insists on some urgent issues to be taken care of. Accordingly, Energy Efficient Authentication and Authorization for Multi-node Cooperatively Connected and Reliable system is to be formulated and experimented with the help of some kind of simulation mechanisms. The key methods needed for the Research work fulfillment are:

1) Theoretical Studies: includes mathematical analysis and experimentation on MATLAB.
2) Empirical Studies: includes experimentation with the tools like NS-2.

e. Potential Significance and Applications

Cooperative communication is a promising technique that would enhance the design of WSN. In this context, we have to face new challenges in order to design a full functional system. One of these is to find a way to select a relay node that will efficiently forward packets in a cooperative way, in order to reach an improvement on channel capacity. Many researchers are working in the direction of enhancement of energy efficiency. But certain issues such as Trusted, Authenticated and Reliable connectivity in multi-node cooperative communication networks in consultation with energy efficiency are the real forthcoming challenges.

Applications Application areas will cover all sectors including Cognitive Radio Networks, Retail, Logistics, Pharmaceutical, Food, Health, Intelligent Home, Transportation, Military, etc.

f. Timeline

These are the milestones planning to achieve as part of my PhD with relative duration in months.

- **Milestone 1 (M3) :** Understanding literature of Cooperative wireless communication and IoT, Authentication analysis and requirement.
- **Milestone 2 (M3):** Determining motivations, questions and research challenges, direction and Problem specifications.
- **Milestone 3(M6):** Defining the functional requirements which will cover detailed study of risks and mitigations ,necessary extensions and novel developments and survey paper will be Published in conference and journal.
- **Milestone 4(M7):** Researching on different authentication and authorization mechanism.
- **Milestone 5 (M9):** Design of optimized Cryptographic algorithms and their efficient Implementation for low power, low complexity and spectrum efficient requirements.
- **Milestone 6 (M12):** Evaluating phases, defining of performance metrics and comparison with existing works.
- **Milestone 7 (M15):** To do few courses during this 6 month period and submission of conference /Journal Papers.
- **Milestone 8(M18):** Understanding literature of energy efficient security methods**.** Developing algorithm for authentic, authorized cooperative wireless communication, implementation and testing of these algorithms, Extending the algorithm with binding.
- **Milestone 9(M24) :** Devising techniques and methods for building framework for authentic, authorized cooperative wireless communication. Design of algorithm and devising cryptographic methods for cooperation.
- **Milestone 9 (M27):** To finish the courses and complete 30 ECTS and submission of Conferences/ Journal Paper.
- **Milestone 10 (M30):** To validate methods using system level simulation and try to combine all the previous work.
- **Milestone 11 (M33):** Understanding literature of authentication methods, developing algorithm for authentication and security, Implementation. Submission of Third Journal Paper.
- **Milestone 12 (M36) :** To start writing thesis and simultaneously do refinements towards finishing PhD, by the end of M34. Wind up the PhD work, and publish all the work done.

	Task	Year 1				Year 2				Year 3			
		M1 M2 M3	M4 M5 M6	M7 M8 M9	M10 M11 M12	M13 M14 M15	M16 M17 M18	M19 M20 M21	M22 M23 M24	M25 M26 M27	M28 M29 M30	M31 M32 M33	M34 M35 M36
1	Background Study												
2	Literature Survey												
3	Problem formulation												
4	Research direction and requirement												
5	Novel concept development												
6	Feasibility study												
7	Framework design and challenges												
8	Implementation												
9	Simulation and verification												
10	Result, conclusion, dissemination of the PhD study												
11	Refinement and optimisations												
12	Attending PhD courses **												
13	Publication (Journal and conferences)												
13	Writing of the Thesis												
14	Study abroad *												

**Planning still provisional: some of the PhD courses may be attended in India.

*Every year 3 month at AAU, Aalborg, Denmark and 9 months at GISFI Headquarters, SIT Lonawala, India.

g. Outline of the contents of Thesis

The thesis will be organized as a monograph.The outline of the thesis contents are as mentioned below.

1. Abstract
2. Introduction
3. State of the Art in Cooperative Wireless Communication

4. Light weight cryptography
    4.1 State of the Art in Light weight cryptography
    4.2 Group Based Public Key Cryptosystem
    4.3 Conclusion and Outlook
5. Authentication and authorization in CWC
    5.1 State of the Art
    5.2 Authentication and Authorization using Braided Group theory.
    5.3 Conclusion and Outlook
6. NS-2 experimentation platform
    6.1 CWC experimentation on NS2
    6.2 Security inclusive CWC
    6.3 Conclusion and Outlook
7. Conclusions
8. Bibliography

SECTION 3: AGREEMENT BETWEEN STUDENT AND SUPERVISOR

The student – supervisor agreement can be summarized within the following bullet points:

- The student and the supervisors are together responsible for time management in the project. Time plan for the Ph.D. study should be reviewed every six months.

- The student should be able to get access to lab equipment and technical assistance from both AAU and SIT. In cases when advanced equipments are required, the student should make a request at least one month in advance and the supervisors should help the student as much as they can.

- Telephone meetings every second week between the student and the AAU and Indian supervisors. Telephone conferences every two months for all PhD students, supervisors and managers. Workshops every six months. Meetings once a week between the student and the supervisors at India.

- Minutes will be made for telephone conferences and workshops.

- Minutes for telephone meetings are provided upon request on an ad hoc basis.

- Feedback regarding the progress and quality of work will be given during the meetings, conferences and workshops.

- Most meetings are scheduled and arranged jointly by the student and the supervisors. In case of special needs, both student and supervisors can call for a meeting.

- Agenda will be provided by the student one day prior to each meeting.

- Common documents will be distributed and maintained via e-mail and/or AFS servers at AAU. Large amount of data can be exchanged via optical disks or hard disks.

- The student is a staff member of both India and AAU and gets involved in group activities in both places.

- Group meetings at SIT are usually organized once a week.
- The student will present his/her work at biannual workshops.
- Paper writing is on the basis of collaboration between the student and the supervisors. In most of cases, the student prepares the first draft and the supervisors give feedback and comments timely.
- This agreement will be evaluated every six months.

SECTION 4: PhD COURSES PLAN

Courses	Place/ Organizer	Project course or General	Status	ECTS
Introduction to Internet of Things	Neeli Prasad, Albena Mihovska, Zheng Hua Tan, Ole Brun Madsen, Aalborg	Project Course	Completed	1
Intellectual Property Rights	Lisbeth Tved Linde		Completed	1
Vehicular Communication	Tatiana Kozlova Madsen and Hans-Peter Schwefel		Completed	3
Machine Learning	Zheng Hua Tan		Completed	3
Air Interface Design for Future Wireless Systems – Towards Real 4G and Cognitive Radio	Prof. Ramjee prasad Frederikson Suvra Shekhar Das Nicola Marchetti		Completed	4
Sensors and RFID Networks	Neeli Rashmi Prasad		Completed	3
Subtotal (Completed)				15
Cryptography	Hans Hüttel , Olav Geil	General	Planned (2011)	3
Special Courses for GISFI PhD Students	I4CT, India		Planned	3
Iterative techniques in wireless communications	Andreas Loeliger, Swiss FIT, Switzerland		Planned	2,5
Bayesian Statistics, Simulation and Software – with a View to application examples	Kasper K. Berthelsen, Associate Professor		Planned	4
Professional Communication	Professor Annette Kolmos		Planned	2,5
Subtotal				30

Note: The list of courses provided here is preliminary and may change after the addition of courses more relevant to the specific research topic. Some courses might be attended during stay in India.

SECTION 5: PLAN FOR DISSEMINATION OF KNOWLEDGE

Authentication, authorization and security in the cooperative wireless communication networks is an emerging research area that allows for novel research and publications in several related topics.

Journal

Submitted and Planned

[1] Vandana Rohoakale, Neeli Prasad, Ramjee Prasad," Secure Cooperative Communication and IoT: Towards Greener Reality", Springer Wireless Personal Communications Journal. (**Submitted**)

[2] Vandana Rohoakale, Neeli Prasad, Horia Cornean, Ramjee Prasad, "Secure Cooperative MAC Protocol using Group Based Cryptography (Working Title)", IEEE Journal on selected areas of Communications. (**Planned – End of 1st Quarter of 2011**)

[3] Vandana Rohoakale, Neeli Prasad, Horia Cornean, Ramjee Prasad, "Light Weighr Secure CoopMAC for Opportunistic Large Array based Cooperative Communication", (Working Title)", IEEE transactions on Personal Communications. (**Planned – End of 2nd Quarter of 2011**)

Conferences

Accepted & Published:

[1] Vandana Rohoakale, Nandkumar Kulkarni, Horia Cornean, Neeli Prasad, "Cooperative Opportunistic Large Array Approach for Cognitive Radio Networks", 8th IEEE International Conference on Communications, June 2010, Bucharest, Romania. (**Published**)

[2] Vandana Rohoakale, Neeli Prasad, "Receiver Sensitivity in Opportunistic Cooperative Internet of Things (IoT)", Second International Conference on Ad Hoc Networks August 2010, Victoria, British Columbia, Canada. (**Published**)

[3] Vandana Rohoakale, Neeli Prasad, Ramjee Prasad, "A Cooperative Internet of Things (IoT) for Rural Healthcare Monitoring and Control", Wireless Vitae 2011, 2nd International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology, Feb-Mar 2011, Chennai, India. (**Accepted**)

Planned

[1] Vandana Rohoakale, Neeli Prasad, Horia Cornean, Ramjee Prasad," Light Weight Cryptography for Opportunistic Large Array Based Cooperative wireles Communication using Group Theory", 3rd 7th International ICST Conference on Security and Privacy in Mobile Information and Communication Systems (Mobisec 2011), May 17-19, 2011 – Aalborg University, Denmark.

SECTION 6: AGREEMENTS ON IMMATERIAL RIGHTS TO PATENTS

The outcome of the research work will be registered for IPR and all the rights will be shared between the Aalborg University and the PhD student, following the standard procedures at AAU.

SECTION 7: PLANS FOR EXTERNAL COLLABORATION

It is planned to work along with research groups of Indian Institute of Management (IIM), Kolkata, India.

SECTION 8: FINANCIAL BUDGET FOR PHD PROJECT

CTiF, Alborg University will provide research facilities and Expenses for tution fees, lodging boarding and travelling will be borne by STES, Pune (India).

SECTION 9: LIST OF REFERENCES

[1] Pei Liu, Zhifeng Tao, Zinan Lin, Elza Erkip and Shivendra Panwa, "Cooperative Wireless Communications: A Cross Layer Approach", IEEE Wireless Communications August 2006

[2] Aria Nosratinia, Todd E. Hunter and Ahmadreza Hedayat, Cooperative Communication in Wireless Networks (ADAPTIVE ANTENNAS AND MIMO SYSTEMS FOR WIRELESS COMMUNICATIONS IEEE Communications Magazine • October 2004.

[3] A. Sendonaris, E. Erkip, and B. Aazhang, "User Cooperation – part i: System Description, part ii: Implmentation Aspects and Performance Analysis," IEEE Trans. Commun., vol. 51, no. 11, pp.1927– 48, Nov. 2003.

[4] J. N. Laneman, D. Tse, and G. W. Wornell,"Cooperative Diversitry in Wireless Networks: Efficient Protocols and Outage Behaviour,"IEEE Trans. Inf. Theory, vol. 50, no. 12, pp. 3063 80, Dec. 2004.

[5] Ahmed K. Sadek, Weifeng Su and K.J.Ray Liu," Multinode Cooperative Communications In Wireless Networks", IEEE TRANSACTIONS ON SIGNAL PROCESSING, VOL. 55, NO. 1, JANUARY 2007.

[6] Anna Scaglione and Yao-Win Hong, "Opportunistic Large arrays: Cooperative Transmission in Wireless Multihop Ad-Hoc Networks to Reach Far Distances", IEEE Transactions on Signal Processing, vol.51,no.8, August 2003.

[7] Arvind Kailas and Mary Ann Ingram,"Alternating Opportunistic Large arrays in Broadcasting for Network Lifetime Extension", IEEE Trans.Wireless Commun., vol. 8, no. 6, pp. June 2009.

[8] Lakshmi V. Thanayankizil, Aravind Kailas, Mary Ann Ingram, "Energy-Efficient Strategies for Cooperative Communications in Wireless Sensor Networks," sensorcomm, pp.541-546, 20 International Conference on Sensor Technologies and Applications (SENSORCOMM 2007).

[9] L. Thanayankizil, A. Kailas, and M. A. Ingram, "A simple cooperative transmission protocol for efficient broadcasting over multi-hop wireless networks", KICS/IEEE Journal of Communications and Networks, vol.10,no.2,pp.213-220, June 2008.

[10] Y. W. Hong and A. Scaglione, "Energy-efficient broadcasting with cooperative transmissions in Wireless sensor networks," IEEE Trans.Wireless Commun., vol. 5, no. 10, pp. 2844–55, Oct. 2006.

[11] Arvind Kailas, "Opportunistic Large Array-Based Cooperative Transmission Strategies", IEEE Trans.Wireless Commun 2008.

[12] Bastein Mainaud, Vincent Gauthier and Hossam Afifi, "Cooperative Communication for Wireless Sensors Network: A MAC Protocol Solution, 1st IFIP Wireless Days Conference, Date: NOV 24-27, 2008 Dubai U ARAB EMIRATES.

[13] P. Liu, Z. Tao, and S. Panwar. A cooperative MAC protocol for wireless local area networks.

In Proc.of the International Conference on Communications (ICC 2005), volume 5, pages 2962–2968, 2005.

[14] SecureRF White paper, “An Introduction to Cryptographic Security Methods and Their Role in Securing Low-Resource Computing Devices”, May 2010.

[15] Makda, S., Choudhary, A., Raman, N., Korakis, T., Zhifeng Tao, Panwar, S., “Security Implications of Cooperative Communications in Wireless Networks”, IEEE Sanrof Symposium 28-30 April 2008.