Cooperative Wireless Communications and Physical Layer Security: State-of-the-Art

Vandana Milind Rohokale, Neeli Rashmi Prasad and Ramjee Prasad

Center for TeleInFrastruktur, Aalborg University, Aalborg, Denmark;
e-mail: {vmr, np, prasad}@es.aau.dk

Abstract

One morning, we were waiting for our college bus. The Wipro industry bus was slowly passing nearby us looking for its employees. At the last moment, when the driver increased speed, one person stepped down from the auto rickshaw and shouted “stop the bus, stop the bus”. Voluntarily, whoever was present started shouting “stop, stop the bus”. The sound finally reached the bus driver who stopped the bus, and the employee could catch it in time. This analog from everyday realistic life simply depicts the spirit of cooperative wireless communication which utilizes the information overheard by neighbouring nodes to offer reliable communication between sender and receiver. Future converged wireless networks are expected to provide high data rate services with extension in coverage area. Also, the next generation networks should possess bandwidth efficiency, less power consumption ability with small sized mobile equipment. Multiple-input multiple-output (MIMO) system is the best technique for the provision of communication diversity wherein multiple antennas are installed at the sender and receiver. In today’s miniaturizing electronics era, the hardware implementation of MIMO in the mobile equipment is not feasible due to resource constraints. Cooperative wireless communication (CWC) is the upcoming virtual MIMO technique to combat fading and achieve diversity through user cooperation. Physical layer security (PLS) is the imminent security guarantee for the cooperative communication.

Journal of Cyber Security and Mobility, Vol. 1, 227–249.

Keywords: Multiple Input Multiple Output (MIMO), Cooperative Wireless Communication (CWC), Physical Layer Security (PLS).

1 Introduction

Currently, wireless communication and mobile computing are the buzz words for the telecom industry. For multimedia applications, the user needs higher data rates at which data transactions can take place efficiently. Gigabit wireless communication is the dream which is being chased by scientists and researchers. Capacity provided by single antenna systems is bounded by the Shannon limit. Diversity gains like capacity and high data rates are possible with the MIMO systems [1]. Diversity is nothing but a mechanism for reliability improvement in the transmitted message signal which makes use of two or more communication channels of different characteristics.

However today's booming wireless techniques, such as adhoc networks, wireless sensor networks and cognitive radio networks, make use of resource constrained miniature devices. The hardware implementation of the MIMO system poses problem due to size, weight and cost [2]. MIMO is the only key solution to bring spectrally efficient Gigabyte wireless communication in reality. Cooperative communication creates the scenario of virtual MIMO by utilizing the group communicating nodes antennas. Cooperation among the network node entities ensures the regulation of the network traffic whereas the traditional multi-hop networks generate contention in the traffic as depicted in Figure 1.

The cooperative broadcasting is prone to eavesdropping attacks due to its multi-node wireless connectivity. Nowadays everybody wishes to use their wireless equipment 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. Message secrecy problem become the important aspect of information security in modern times.

Security of private key cryptosystems depends on secrecy of the secret key. In case of public key systems, it is infeasible to extract private key from the public key. Breaking of a public key is a complex and timely task. Much 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

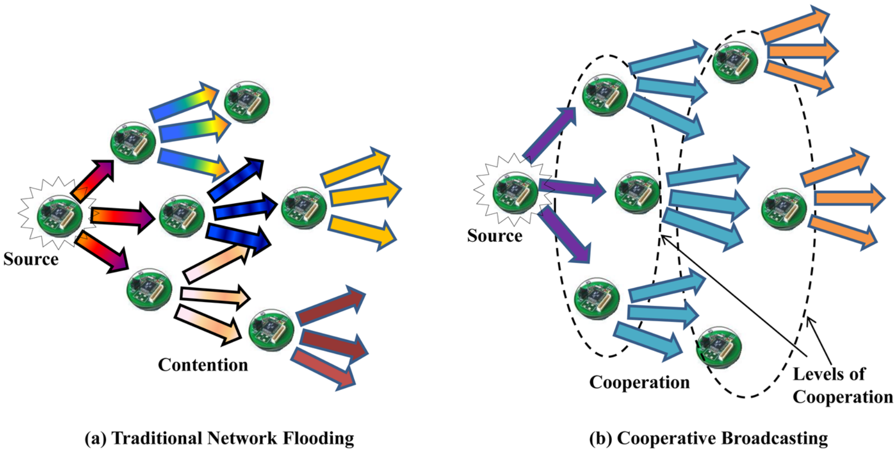
Source
Contention
(a) Traditional Network Flooding
Source
Cooperation
Levels of Cooperation
(b) Cooperative Broadcasting

Figure 1 Cooperative broadcasting vs. traditional network flooding.

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.

The traditional cryptographic algorithms namely, AES, DES, and NTRUE etc. include complex mathematical calculations. Since next generation networks like CRNs and WSNs are making use of resource constrained miniature network nodes, these traditional higher layered cryptographic solutions are not feasible for them. Physical layer security employing information theoretic source and channel coding techniques has potential to provide energy efficient security solutions for these networks.

This paper puts forward a physical layer security mechanism for the cooperative networks. In Section 2, related work in the fields of cooperative communication and physical layer security are described. Section 3 depicts the proposed secure cooperative scheme and the different techniques therein. Finally, Section 4 concludes the work.

2 Cooperative Wireless Communication (CWC)

The origin of cooperative communication concept dates back to the research work of Van der Meulen [3] and Cover and Gamal [4], where the concept of relay channel was introduced in between the traditional source-receiver communication. Three node network was considered for the analysis which consists of source, relay and destination. Total system under consideration

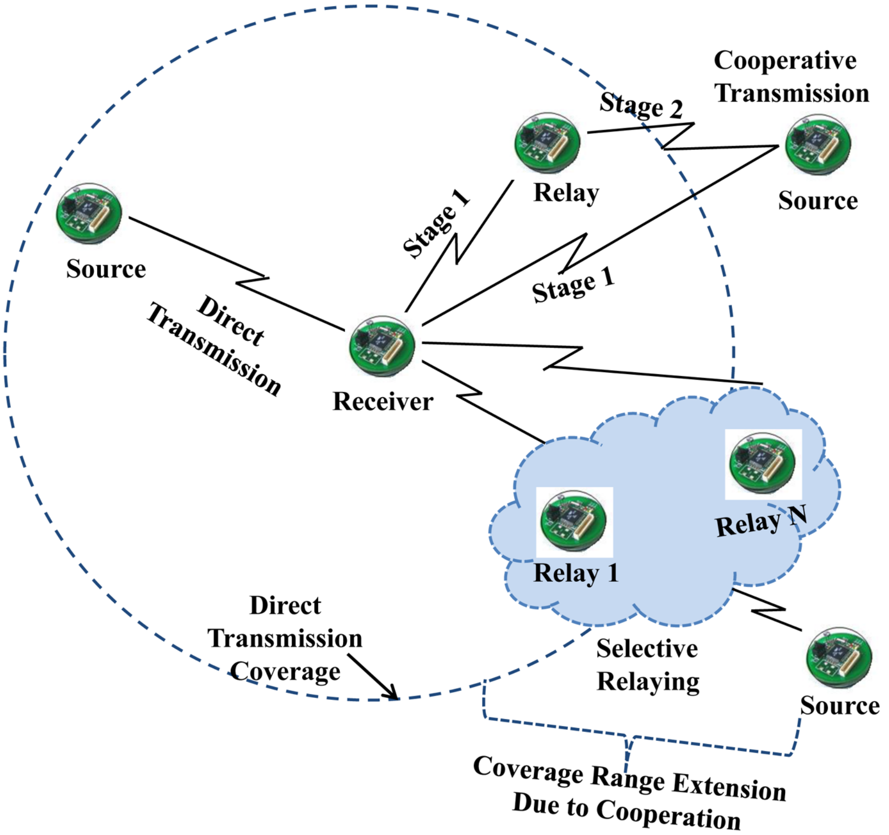

Figure 2 Illustration of direct transmission, cooperative relaying and selective relaying.

has a single bandwidth with broadcasting at the source node and multiple access at the receiver. Cooperation of mobile users with spatial diversity was studied in [5] wherein the network entities transmit their cooperative partner's data with their own data during different time slots. The network node functions as a source for the transmission of their own data and act as a relay for transmission of other nodes' data.

Misha Dohler et al. [6] have appropriately explained cooperation mechanism, wireless relay channel and their modelling, transparent relaying techniques, regenerative relaying techniques and hardware issues in the design of cooperative transceivers for different application scenarios like 3G UMTS Voice/HSDPA Relay and LTE/WiMAX Relay systems. They have also demonstrated some of the real implementations of cooperative diversity mechanisms. Some of the basic advantages of the cooperative relay techniques are depicted in Figure 2 like channel capacity and coverage range improvements.

Cooperative diversity in terms of distributed antenna system was first analyzed in the research work of Saleh et al. [7]. Here two or more information sources form a cooperative group and transmit common information to a single sink. The distributed antenna system was evolved initially for the cellular communication system. With spatial diversity, the advantages of the distributed antenna system are signal strength and channel capacity improvement. For making the transition from a traditional cellular system to a cooperative cellular network, Tao et al. [8] put forth new techniques such as distributed antenna system, multi-cell coordination, group cell mechanism including multiple point transmission and reception (CoMP). These are the stepping stones towards bringing 3GPP LTE-Advanced (LTE-A) into reality.

Research work in [9] has shown that with the coverage range enhancement and improvement in the channel capacity, the cooperative relaying can expressively increase the spectrum efficiency and overall performance of the system. Two intra-cell coordinated multipoint schemes for LTE-Advanced are taken into consideration and it is shown that the network capacity can be considerably improved with the cooperation. Since the transmissions in the cooperative communication are from the nodes at different locations, they may not be time or frequency synchronized. And it becomes difficult to achieve full diversity for the collocated MIMO systems. The work in [10] revisits the techniques for combating the time and frequency asynchronism in one-way as well as two-way cooperative communicating networks.

Reliable communication with reduced energy consumption is the hot issue in the resource constrained networks like WSN and CRN. Cross layer cooperation is the best suited solution for achievement of energy efficiency and reliability in wireless communication. In [11], distributed cross layer technique is proposed which makes use of opportunistic relaying mechanism to achieve quality of service (QoS) in the cooperative communications. Energy savings and low bit error rates can be achieved with the help of cross layer cooperation as shown in Figure 3. Some parts of the routing functions are executed at the physical layer. The diversity provided by the MIMO space time codes can help in the performance improvement at the MAC and upper layers [12]. Liu et al. [13] proposed a new CoopMAC protocol for IEEE 802.11 networks which has inbuilt receiver combining capability. Due to this, the physical layer system cooperates with higher layers in the protocol stack and gets benefits in terms of improvements in the system

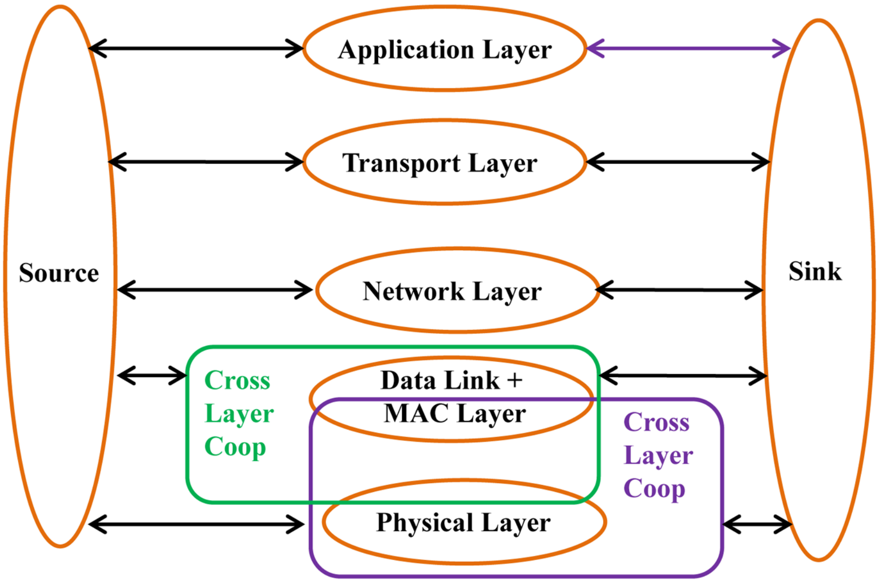

Figure 3 Cross layered cooperative communication [12].

robustness, throughput, delay and interference reduction with the coverage range extension.

The research work of Chen et al. [14] puts forth a new distributed weighted cooperative routing algorithm in which relay selection is based on the weights of the relays. The metrics used for the decision of relay weights are residual energy and channel state information (CSI) at each source-relay-receiver link. Here, the authors have made use of Destination Sequenced Distance Vector (DSDV) routing protocol with consideration of the difficulties due to time synchronization and data packet reduplication. To achieve energy efficient long range communication, cooperative beamforming is the ultimate solution. In the work of Dong et al. [15], a cross layer framework for cooperative communication is proposed which brings the concept of cooperative beamformimg. Here, the cooperative beamforming mechanism is applied for the analysis of the spectrum efficiency of the cooperative communication system. For the study of delay characteristics of the source messages, queuing theory is used.

Independent paths in between source and sink are generated by introducing relay channel in between them in the cooperative communication paradigm. Based on how the signal received form the source is processed at

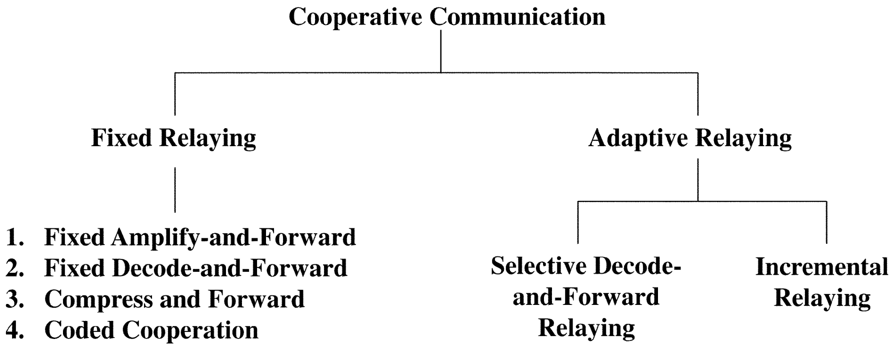
Cooperative Communication
Fixed Relaying
Adaptive Relaying
1. Fixed Amplify-and-Forward
2. Fixed Decode-and-Forward
3. Compress and Forward
4. Coded Cooperation
Selective Decode-and-Forward Relaying
Incremental Relaying

Figure 4 Cooperative relaying techniques.

relay, there are different cooperative communication protocols. Main classes include fixed and adaptive relaying mechanisms as depicted in Figure 4. In case of fixed relaying, the channel resources are distributed in between source and relay in deterministic way. All four techniques under the fixed relaying category work in the predefined deterministic or fixed manner [16]. Adaptive relaying technique containing selective and incremental relaying mechanisms has inbuilt flexibility in the sense that during the adverse conditions like severe channel fading or low SNR conditions, the relay can idle itself.

For optimum diversity gains, proper relay selection plays a vital role in the cooperative communication. The research work of Abdulhadi et al. [17] presents a survey of the distributed relay selection schemes for adhoc cooperative wireless networks. These relay selection schemes include opportunistic relaying, power aware relay selection, switched and examine node selection, opportunistic relaying with limited feedback, simple relay selection, geographical information based relay selection, threshold based relay selection for detect-and-forward, opportunistic AF relaying with feedback, incremental transmission relay selection, outage optimal relay selection, energy efficient relay selection, random priority based relay selection, receive SNR priority list based relay selection, fixed priority transmission protocol, generalized selection combining multiple relay selection scheme and output threshold multiple relay selection. Different performance metrics like objectives, mechanisms, performance, advantages and drawbacks of each of them are illustrated in the tabular way.

Ever-increasing traffic in the vehicular communication systems with safety and spectrum efficiency are the major current issues related to cooperative vehicular communication systems. In [18], the authors have analyzed congestion control and awareness control issues for the cooperative vehicular networks. These critical issues are heavily dependent on the frequency band allocation, medium access control technique being adopted and the availability of the wireless communication technology for particular vehicular communication system. These issues are needed to be researched again.

For the participation in cooperative communication, the network node entities does not get any incentives for their cooperation. Game theoretic cooperation approaches promise to provide proper incentives for the nodes cooperating to relay the information from sender to receiver [19]. Mainly, three types of behaviours are observed in the wireless networks like

1. *No Help (Egoistic Behaviour)*: If the network node has its own data to transmit, then it sends that data independently without any other node's help. If this node does not have its own data for transmission, it remains idle instead of helping other nodes in their data transmissions.
2. *Unidirectional Help (Supportive Behaviour)*: The network node acts only as a supporting relay for the source by helping it to transmit its data towards receiver. No any potential gain is there for such kind of supportive behaviour and that's why it is called as unidirectional help.
3. Mutual Help (Cooperative Behaviour): The network nodes mutually help each other in transmitting their own data as well as their neighbour's data to the intended recipients. The node acts both as source and relay [6].

There should be incentives for the cooperative behaviour and some punishments in terms of costs for the selfish behaviour or no help conditions. Game theory provides the modelling, analysis and solution for the cooperative and non-cooperative behaviours. Three primary techniques are designed for making the provision of cooperation incentives viz. reputation based, resource-exchange-based and pricing based techniques [19].

3 Physical Layer Security (PLS)

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 adversary might not only have the means to read transmitted messages, but could actually change them, or the enemy could produce and

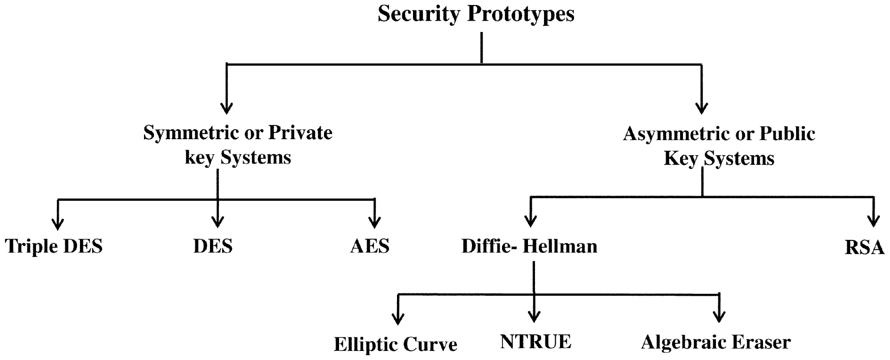

Figure 5 Classification of security mechanisms.

send a false message to the receiver and hope that this would initiate some action. The transactions with the help of wireless networks such as credit card transactions or banking related data exchange communications are prone to the malicious behaviour due to the open nature of wireless medium. Adversaries can easily get access to the wireless transactions and can modify the data therein [20].

Traditional cryptographic techniques include symmetric (private) and asymmetric (public) key systems which are further classified into different mechanisms such as DES, AES, RSA, Diffie–Hellman, etc., as shown in Figure 5. The main problem associated with these cryptographic techniques is that they include complex mathematical calculations which consume considerable part of the resources which are very much crucial for wireless sensor nodes or the consumer radio nodes of the cognitive radio networks.

For establishment of a communication link in between sender and receiver, traditional cryptographic encryption block making use of public and private keys is required at the transmitting end while at the receiving end, channel decoding and decryption blocks are separately used. With the help of information theoretic security, encryption and channel coding blocks are combined in a single secure encoding block as depicted in Figure 6. Also, at the receiving side, channel decoding and decryption blocks are combined to form decoding block. This greatly reduces resource consumption because of relief from the key management functionality which is most costly affair. With the basic wiretap channel, and variants of it like Gaussian, MIMP, compound wiretap, feedback wiretap and wiretap channel with side information are considered for the detail analysis in their work. They have further extended their work from basic wiretap channel to broadcast channels, multiple

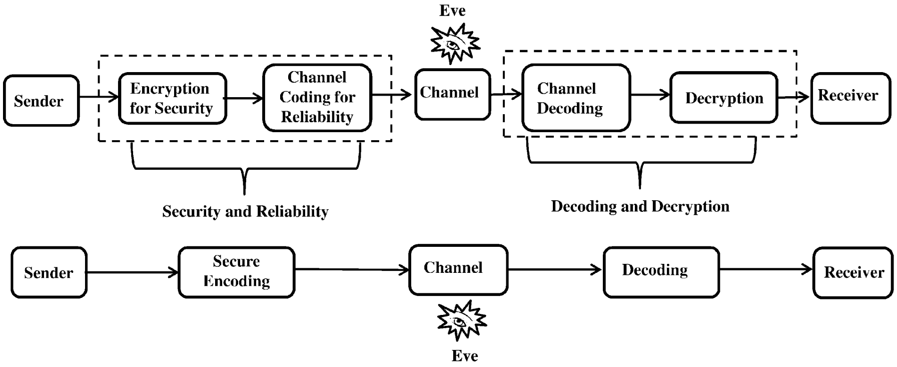

Figure 6 Information theoretic security combines security and reliability functions in a single block.

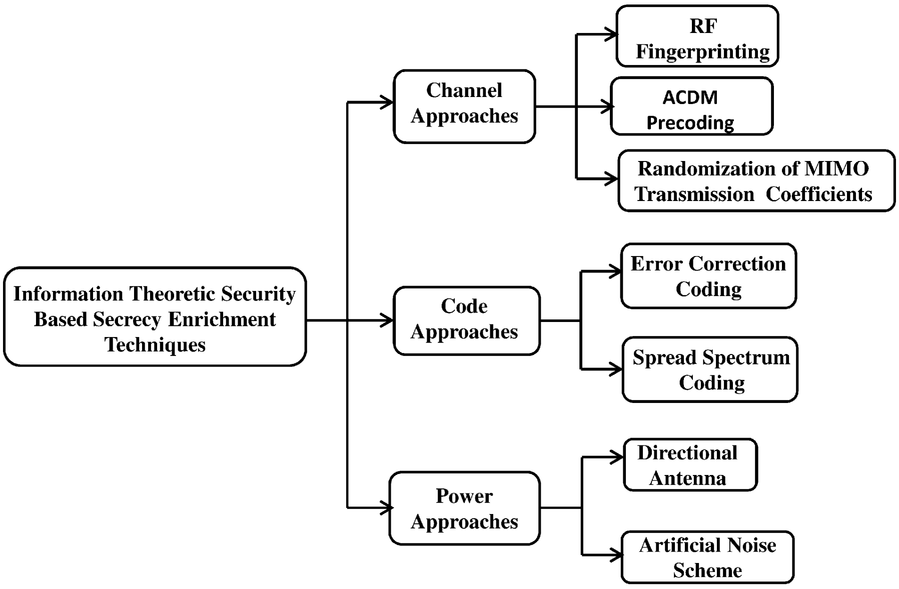

Figure 7 Security enhancement techniques based on information theoretic mechanisms.

access channels, interference channels, relay channels and two-way channels [21].

In the research work of [22], a tutorial is presented on the security improvement techniques at the physical layer in wireless networks. Depending on their characteristic features, these are classified into further subclasses as shown in Figure 7. Two metrics considered for the security analysis include secret channel capacities and computational complexities in comprehensive key search.

Built in physical layer security is nothing but the capacity of the transmission channel. It is called secret channel capacity. It is defined as information theoretic secrecy because the eavesdropper's received signal does not give any information about the original transmitted signal. It just keeps on purely guessing. Information theoretic secrecy is in fact equivalent to perfect secrecy. In the research work of Rohokale et al. [23], cooperative jamming technique is used to confound the eavesdropper and relay is cooperatively sending jamming signals towards the eavesdropper to confuse about the actual transmitted signal. Here, the secrecy capacity observed is almost equal to the perfect secrecy.

Traditional application layer cryptographic mechanisms cannot go beyond detection of signal corruption to determine the eavesdroppers. For the detection of malicious behaviour by the compromised relay node in the cooperative communication, Mao and Wu [24] proposed a cross-layer technique which makes use of adaptive signal detection at the physical layer with the statistical signal detection scheme making use of pseudorandom tracing symbols at the application layer. In [25], two different cooperative techniques are introduced viz. cooperative relaying and cooperative jamming for gaining the security. Power allocation of relay with cooperative relaying and jamming is studied for the achievement of optimum secrecy rate with the available source transmit power. Secrecy capacities of cooperative relaying and cooperative jamming techniques are compared with and without eavesdropper's channel state information.

Imperfect channel condition is the challenging issue for consideration of physical layer security in wireless communications. Cooperative decode and forward approach is considered to combat channel fading and achieve security in the information transmission in [26]. For the assumption of the presence of one eavesdropper, optimal solution is achieved with the help of iterative solution for transmit power minimization consideration. For the assumption of multiple eavesdroppers, due to the problem of secrecy capacity maximization with transmit power minimization, suboptimal solution is proposed by considering the restriction of complete nulling of signals at all the eavesdroppers.

Synergy MAC protocol for now a days Wi-Fi security framework is nothing but the extension of cooperative communication protocol at physical layer to the MAC sublayer. It results into the advantage of spatial diversity with increased transmission rates. For security adjustment in the cooperative scenario, two new security schemes are proposed for 802.11i viz. WPA and WPA2. Various security algorithms such as WEP, WPA and WPA2 are appropriately analyzed in [27] to function with Synergy MAC. The speciality of Synergy MAC is that it has multi-rate capability for packet transmission.

For establishing secure connection in between source and cell edge destination users in the presence of an eavesdropper, relay placement is observed to be more advantageous. Also when path loss is more severe, relay transmission is found to be beneficial. In the randomize-and-forward (RF) relaying mechanism, different randomization is introduced in each hop which is proved to be better physical layer security solution as compared to the traditional decode-and-forward (DF) relay technique [28]. For achievement of physical layer security, two cooperative relaying schemes are analyzed in [29], namely Decode-and-forward (DF) and Cooperative Jamming (CJ). For cell edge users, relays in between decode the received signal and again encoded and weighted signal is transmitted to the receiver. While the source is transmitting the weighted information signal to the receiver, some of the cooperating relay nodes are transmitting weighted noise signal to misperceive the eavesdropper. Two objectives are taken into consideration viz. maximization of the achievable secrecy rate and minimizations of total transmit power.

Due to open nature of multi-hop cooperative communication networks, they are inherently prone to the security threats such as impersonation attacks and message integrity at the receiving end. In [30], the authors have put forth a prevention based technique for secure relay selection for cooperative wireless communication which includes authentication protocol designed with hash chains and Merkle trees. The proposed security system can enhance the number of messages in the Merkle tree and at the same time it can appropriately select secure relay nodes for cooperative communication with significant improvement in the throughput QoS. Throughput attained by using this technique is observed to be higher than the systems without security provision.

In [31], secure cooperative transmission technique making use of physical layer security which considers the presence of passive eavesdroppers. The channels under consideration are frequency flat and frequency selective channels. By exploiting the local information available at individual nodes, full diversity and prevention against malicious behaviour is achieved by keeping intact the transmitter efficiency. The proposed protocol is named as Anti-Eavesdropping Space Time Network Coding (AE-STNC) which works on the principle of randomizing the signals being received at the eavesdroppers

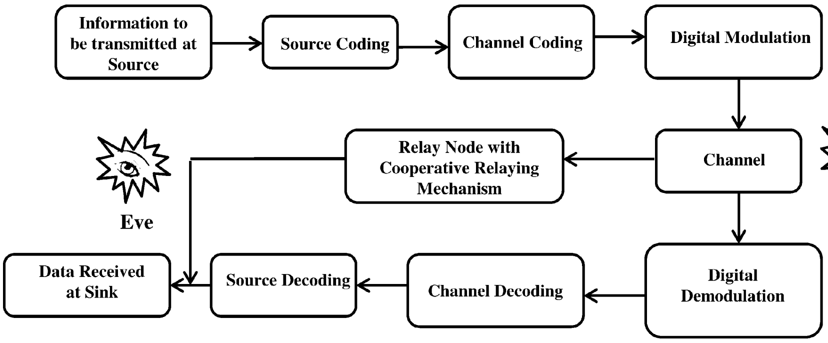

Figure 8 Information theoretically secure cooperative communication link.

with best channel quality so that it becomes difficult for the eavesdropper to capture the messages under transmission. The AE-SNTC protocol is extended further to design AE-STFNC for the broadcast asynchronous cooperative communication networks which is also provides the flexible diversity with security.

Due to highly mobile nature of the mobile adhoc networks, they suffer from imperfect channel conditions and frequently changing topology. The important network design parameters such as security and throughput are simultaneously analyzed in [32] for mobile adhoc networks. The authors have projected a topology control mechanism with authentication for throughput enhancement by combining higher layer security techniques with physical layer security techniques for CWC. The proposed system combines the authentication protocol technique from the upper layers in the protocol stack and transmission methodology from the physical layer to improve the overall cooperative system's throughput.

4 Proposed Secured Cooperative Scheme

Information theoretic source and channel coding techniques can be used with appropriate modulation techniques to achieve perfect secrecy capacities for the CWC. Today green energy is the buzz word and to achieve energy efficiency, we have to think about cost effective security measures. Data compression techniques under source coding mechanism provide high data rates ensuring less energy requirement. For achieving reliability of communication, channel coding methods are extremely useful. Physical layer security

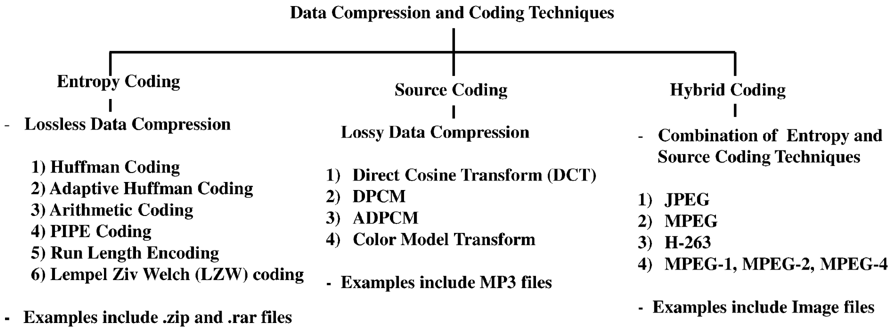
Data Compression and Coding Techniques
Entropy Coding
- Lossless Data Compression
1) Huffman Coding
2) Adaptive Huffman Coding
3) Arithmetic Coding
4) PIPE Coding
5) Run Length Encoding
6) Lempel Ziv Welch (LZW) coding
- Examples include .zip and .rar files
Source Coding
Lossy Data Compression
1) Direct Cosine Transform (DCT)
2) DPCM
3) ADPCM
4) Color Model Transform
- Examples include MP3 files
Hybrid Coding
- Combination of Entropy and Source Coding Techniques
1) JPEG
2) MPEG
3) H-263
4) MPEG-1, MPEG-2, MPEG-4
- Examples include Image files

Figure 9 Different data compression and coding techniques.

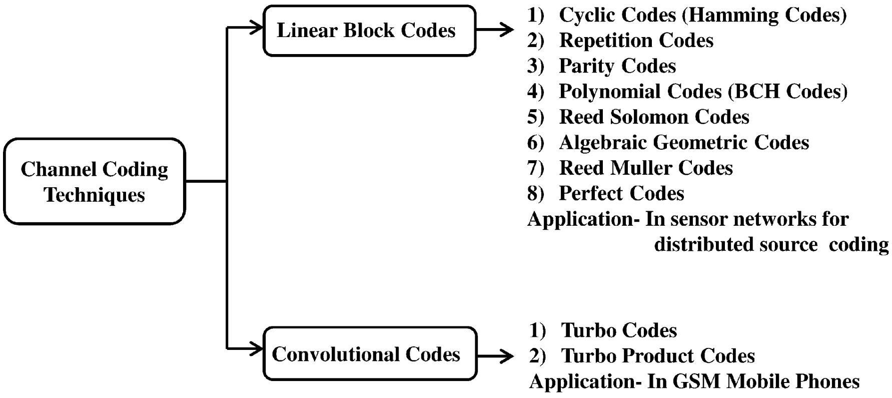
Channel Coding Techniques
Linear Block Codes
1) Cyclic Codes (Hamming Codes)
2) Repetition Codes
3) Parity Codes
4) Polynomial Codes (BCH Codes)
5) Reed Solomon Codes
6) Algebraic Geometric Codes
7) Reed Muller Codes
8) Perfect Codes
Application- In sensor networks for distributed source coding
Convolutional Codes
1) Turbo Codes
2) Turbo Product Codes
Application- In GSM Mobile Phones

Figure 10 Channel coding mechanisms.

making use of information theoretic techniques ensures security with minimal resource consumption. The proposed mechanism is depicted in Figure 8.

Generally, source coding is done for data compression and channel coding is performed for error detection and correction. For data compression, shortest average description length of a random variable is used. Variable length coding is applied for data compression in which short descriptions are allocated for most frequent outcomes and comparatively longer descriptions are assigned for less frequent outcomes. Data compression and coding techniques include entropy coding, source coding and hybrid coding as shown in Figure 9. It contains different subtypes of these main encoding techniques [33].

In order to achieve reliability of communication in terms of low bit error rate, error control coding or channel coding is the essential technique to detect

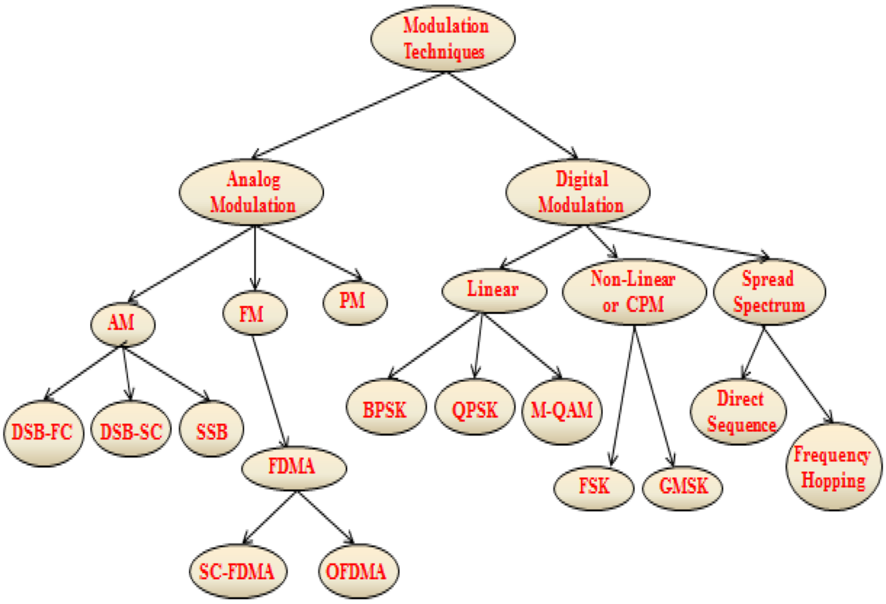

Figure 11 Classification of modulation techniques.

and correct the errors introduced in the channel due to noise [34]. Basic idea behind error correcting codes is nothing but addition of certain amount of redundancy to the message prior to transmission in a known manner. Various channel coding mechanisms are shown in Figure 10.

For conveying a message signal over long distance communication links, some parameters of a low frequency periodic waveform are varied according to high frequency carrier signal attributes [35], which is nothing but modulation. Each of the subclasses of analog modulation technique demand different bandwidth and power for their operation. Analog modulation technique has the disadvantage of more hardware and bandwidth requirement. Once, the noise gets added in the channel, it is carried out as it is till the receiving end since there is no any provision of error control coding for the analog modulation.

Digital modulation has advantages over analog modulation in terms of less hardware requirement, less interference, provision of the error control coding methods and less bandwidth demand. Different modulation techniques are illustrated in Figure 11. Design of a communication system is dependent on the application for which it is to be used. Two major criteria for choosing modulation technique are noise and bandwidth efficiency. Orthogonal frequency division multiplexing (OFDMA) is a good combination of modulation and multiplexing techniques wherein, available spectrum is divided into multiple carriers and each one of them is modulated at a low data rate. Each of these carriers are closely spaced and orthogonal to each other. Hence, OFDMA systems are immune to noise.

Trellis coded modulation (TCM) is a mechanism which combines coding and modulation in a one function. TCM makes use of various concepts of signal processing. Convolutional coding and PSK or QAM modulation schemes are combined in TCM. Ungerboeck's set portioning rules are used for portioning the PSK or QAM sets. TCM is proved to be a bandwidth efficient technique. It promotes highly efficient transmission of information over band limited channels such as telephone lines. It provides almost approximately 40% more spectral efficiency as compared to the popular Reed Solomon channel coding technique [36]. There are various fading channel model assumptions are available in digital communication system design including Nakagami fading, Log-normal shadow fading, Rayleigh fading, Ricean fading and Weibull fading channels. Mainly two channel assumptions are made while designing a communication system viz. Rayleigh and Ricean Fading channels. For line of sight (LOS) scenario, Ricean channel is a good choice and for long distance or non-line of sight case, Rayleigh fading channel is the better fading channel assumption.

5 Information Theoretic Security Measures

1. Entropy of the source $H(X)$ – Entropy is a measure of the uncertainty of a random variable.

$$H(X) = -\sum_{i=1}^{n} p(x_i) \log p(x_i) \tag{1}$$

2. Entropy at the receiver $H(Y)$ – average information per character at the destination.

$$H(Y) = -\sum_{j=1}^{m} p(y_j) \log p(y_j) \tag{2}$$

3. Entropy of the total communication system as a whole $H(X, Y)$ – average information per pairs of transmitted and received characters.

$$H(X, Y) = -\sum_{i=1}^{n}\sum_{j=1}^{m} p(x_i, y_j) \log p(x_i, y_j) \tag{3}$$

4. Conditional Entropy $H(Y|X)$ – a specific character x_k being transmitted and one of the permissible y_j may be. $H(Y|X)$ gives an indication of the noise (errors) in the channel.

$$H(X/Y) = H(X, Y) - H(X) \tag{4}$$

5. Conditional Entropy $H(X/Y)$ – a specific character y_j being received; this may be a result of transmission of one of the x_k with a given probability (a measure of information about the source, where it is known what was received). $H(X/Y)$ gives a measure of equivocation (how well one can recover the input content from the output).

$$H(Y/X) = H(X, Y) - H(Y). \tag{5}$$

   The mutual information for main channel is given by

$$I(X; Y) = H(X) - H(X/Y). \tag{6}$$

   Similarly, mutual information for the Eavesdropper's channel is given by

$$I(X; E) = H(X) - H(X/E) \tag{7}$$

6. The maximum amount of mutual information is nothing but the secrecy capacity for that particular channel.

$$C_{SM} = \max[I(X; Y)] \tag{8}$$

For security in cooperative communication, we should be able to prove that $H(E/X) > H(Y/X) > H(R/X)$ and $C_{SE} < C_{SM} < C_{SR}$, where C_{SE} is the Secrecy capacity of the Eavesdropper's channel, C_{SM} is the Secrecy capacity of the main or Direct (Main) channel, and C_{SR} is the Secrecy capacity of the Relay channel.

The maximum amount of eavesdropper's equivocation (uncertainty of eavesdropper about the source message) indicates the system security. According to Ciszar and Korner [37], the special case in which the eavesdropper is less capable, that is

$$I(X; E) \leq I(X; Y). \tag{9}$$

Then the Secrecy capacity of a communication link can be given by

$$C_s = \max_{P_x}[I(X;Y) - I(X;E)] \tag{10}$$

6 Conclusions and Future Scope

This research article puts forth a ready reference for the researchers working on cooperative wireless communication and physical layer security. Virtual MIMO or cooperative wireless communication with information theoretic security aspects can prove a cost effective physical layer security solution for today's mobile computing applications. Depending on the application, source coding, channel coding and modulation techniques can be selected which can give satisfactory data rates with ensured secure communication. This work can be extended further for various applications and security measures. Instead of applying channel coding and modulation blocks separately, one can combine both the techniques with a single Trellis Coded Modulation (TCM) block for the added advantage of bandwidth efficiency with higher data rates. Different eavesdropper locations and assumptions may result into better information theoretic security results. Selective relaying mechanism can be considered with relay weights and polarizations for getting transmit power efficiency.

References

[1] P. Liu, Z. Tao, Z. Lin, E. Erkip, and S. Panwar. Cooperative wireless communications: A cross layer approach. IEEE Wireless Communications, 13(4):84–92, August 2006.

[2] H. Katiyar, A. Rastogi, and R. Agarwal. Cooperative communication: A review. IETE Tech. Review, 28:409–417, 2011.

[3] E.C. van der Meulen. Three-terminal communication channels. Advances in Applied Probability, 3:120–154, 1971.

[4] T.M. Cover and A.A.E. Gamal. Capacity theorems for the relay channel. IEEE Transactions on Information Theory, 25(5), 1979.

[5] A. Sendonaris, E. Erkip, and B. Aazhang. Increasing uplink capacity via user cooperation diversity. In Proceedings of IEEE International Symposium on Information Theory (ISIT), August, p. 156, 1998.

[6] Misha Dohler and Yonghui Li. Cooperative Communications: Hardware, Channel and PHY. John Wiley and Sons, 2010.

[7] A. Saleh, A. Rustako, and R. Roman. Distributed antennas for indoor radio communications. IEEE Trans. Commun., 35(12):1245–1251, December 1987.

[8] Xiaofeng Tao, Xiaodong Xu, and Qimei Cui. An overview of cooperative communications. IEEE Communications Magazine, 50(6):65–71, June 2012.

[9] Li Qian, R.Q. Hu, Qian Yi, and Wu Geng. Cooperative wireless communications for wireless networks: Techniques and applications in LTE-advanced systems. IEEE Wireless Communications, 19(2):22–29, April 2012.

[10] Hui Ming Wang and Xiang Gen Xia. Asynchronous cooperative communication systems: A survey on signal Designs. Science China Information Sciences, 54(8):1547–1561, August 2011.

[11] Chen Yongrui, Yang Yang, and Yi Weidong. A cross layer strategy for cooperative diversity in wireless sensor networks. Journal of Electronics, China, 29(1/2), March 2012.

[12] Vandana Rohoakale and Neeli Prasad. Receiver sensitivity in opportunistic cooperative Internet of Things (IoT). In Proceedings of Second International Conference on Ad Hoc Networks, Victoria, British Columbia, Canada, August 2010.

[13] Pei Liu, Zhifeng Tao, Zinan Lin, Eiza Erkip, and Shivendra Panwa. Cooperative wireless communications: A cross-layer approach. IEEE Wireless Communications, August 2006.

[14] Chao Chen, Baoyu Zheng, Xianjing Zhao, and Zhenya Yan. A novel weighted cooperative routing algorithm based on distributed relay selection. In Proceedings 2nd International Symposium on Wireless Pervasive Computing (ISWPC'07), 2007.

[15] Lun Dong, Athina P. Petropulu, and H. Vincent Poor. Cross-layer cooperative beamforming for wireless networks. In Proceedings of Cooperative Communication for Improved Wireless Network Transmission-IGI Global, 2010.

[16] K.J. Ray Liu, Ahmed K. Sadek, Weifeng Su, and Anders Kwasinski. Relay channels and protocols. In Cooperative Communication and Networking. Cambridge University Press, 2009.

[17] S. Abdulhadi, M. Jaseemuddin, and A. Anpalagan. A survey of distributed relay selection schemes in cooperative wireless ad hoc networks. Wireless Personal Communications, 63:917–935, 2012.

[18] Miguel Sepulcre, Jens Mittag, Paolo Santi, Hannes Hartenstein, and Javier Gozalvez. Cogestion and awareness control in cooperative vehicular systems. Proceedings of the IEEE, 99(7), July 2011.

[19] Dejun Yang, Xi Fang, and Guoliang Xue. Game theory in cooperative communications. IEEE Wireless Communications, 44–49, April 2012.

[20] C.S.R. Murthy and B.S. Manoj. Adhoc Wireless Networks Architecture and Protocols. Prentice Hall, Princeton, 2004.

[21] Yingbin Liang, H. Vincent Poor, and Shlomo Shamai (Shitz). Information theoretic security. Foundations and Trends in Communications and Information Theory, 5(4–5):355–580, 2009.

[22] Yi-Sheng Shiu, Shin Yu Chang, Hsiao-Chun Wu, Scott C.-H. Huang, and Hsiao-Hwa Chen. Physical layer security in wireless networks: A tutorial. IEEE Wireless Communications, April 2011.

[23] Vandana Rohokale, Neeli Prasad, and Ramjee Prasad. Cooperative jamming for physical layer security in wireless sensor networks. In Proceedings of 15th International Symposium on Wireless Personal Multimedia Communications, Taipei, Taiwan, September 24–27, 2012.

[24] Yinian Mao and Min Wu. Tracing malicious relays in cooperative wireless communication. IEEE Transaction on Information Forensics and Security, 2(2):198–212, June 2007.

[25] Ling Tang, Xiaowen Gong, Jianhui Wu, and Junshan Zhang. Secure wireless communication via cooperative relaying and jamming. IEEE GLOBECOM Workshop on Physical Layer Security, pp. 849–853, December 2011.

[26] Lun Dong, Zhu Han, Athina P. Petropulu, and H. Vincent Poor. Secure wireless communication via cooperation. In Proceedings of Fourty Sixth IEEE Annual Allerton Conference, USA, September 2008.

[27] Santosh Kulkarni and Prathima Agarwal. Safeguarding cooperation in Synergy MAC. In Proceedings of 42nd IEEE Southeastern Symposium on System Theory (SSST), USA, pp. 156–160, March 2010.

[28] Jianhua Mo, Meixia Tao, and Yuan Liu. Relay placement for physical layer security: A secure connection perspective. IEEE Communication Letters, 16(6), June 2012.

[29] Jiangyuan Li, Athina P. Petropulu, and Steven Weber. On cooperative relaying schemes for wireless physical layer security. IEEE Transactions on Signal Processing, 59(10), October 2011.

[30] Ramya Ramamoorthy, F. Richard Yu, Helen Tang, Peter Mason, and Azzedine Boukerche. Joint authentication and quality of service provisioning in cooperative communication networks. Elsevier Journal of Computer Communications, 35:597–607, 2012.

[31] Zhenzhen Gao, Yu-Han Yang, and K.J. Ray Liu. Anti-eavesdropping space-time network coding for cooperative communications. IEEE Transactions on Wireless Communications, 10(11):3898–3908, November 2011.

[32] Guan Quansheng, F.R. Yu, Jiang Shengming, and V.C.M. Leung. A joint design for topology and security in MANETs with cooperative communications. In Proceedings of IEEE International Conference on Communications (ICC), pp. 1–6, June 2011.

[33] Thomas M. Cover and Joy A. Thomas. Elements of Information Theory (second edition). Wiley-Interscience Publication, 2006.

[34] Shu Lin and Daniel J. Costello. Error control coding: Fundamentals & Applications (second edition). Prentice Hall Series in Computer Applications in Electrical Engineering. Prentice Hall, 2010.

[35] D.K. Sharma, A. Mishra, and Rajiv Saxena. Analog and digital modulation techniques: A review. TECHNIA International Journal of Computing Science and Communication Technologies, 3(1), July 2010.

[36] Gottfried Ungerboeck. Trellis coded modulation with redundant signal sets Part I: Introduction. IEEE Communications Magazine, 25(2):5–11, February 1987.

[37] I. Csiszar and J. Korner. Broadcast channels with confidential messages. IEEE Transactions on Information Theory, IT-24(3):339–348, May 1978.

Biographies

Vandana Milind Rohokale received her B.E. degree in Electronics Engineering in 1997 from Pune University, Maharashtra, India. She received her Masters degree in Electronics in 2007 from Shivaji University, Kolhapur, Maharashtra, India. She is presently working as Assistant Professor in Sinhgad Institute of Technology, Lonavala, Maharashtra, India. She is currently pursuing her PhD degree in CTIF, Aalborg University, Denmark. Her research interests include Cooperative Wireless Communications, AdHoc and Cognitive Networks, Physical Layer Security, Information Theoretic security and its Applications.

Neeli Rashmi Prasad, Ph.D., IEEE Senior Member, Director, Center For TeleInfrastructure USA (CTIF-USA), Princeton, USA. She is also, Head of Research and Coordinator of Themantic area Network without Borders, Center for TeleInfrastruktur (CTIF) headoffice, Aalborg University, Aalborg, Denmark.

She is leading IoT Testbed at Easy Life Lab (IoT/M2M and eHealth) and Secure Cognitive radio network testbed at S-Cogito Lab (Network Management, Security, Planning , etc.).

She received her Ph.D. from University of Rome "Tor Vergata", Rome, Italy, in the field of "adaptive security for wireless heterogeneous networks" in 2004 and M.Sc. (Ir.) degree in Electrical Engineering from Delft University of Technology, the Netherlands, in the field of "Indoor Wireless Communications using Slotted ISMA Protocols" in 1997.

She has over 15 years of management and research experience both in industry and academia. She has gained a large and strong experience into the administrative and project coordination of EU-funded and Industrial research projects. She joined Libertel (now Vodafone NL), The Netherlands in 1997. Until May 2001, she worked at Wireless LANs in Wireless Communications and Networking Division of Lucent Technologie, the Netherlands. From June 2001 to July 2003, she was with T-Mobile Netherlands, the Netherlands.

Subsequently, from July 2003 to April 2004, at PCOM:I3, Aalborg, Denmark. She has been involved in a number of EU-funded R&D projects, including FP7 CP Betaas for M2M & Cloud, FP7 IP ISISEMD ICt for Demetia, FP7 IP ASPIRE RFID and Middleware, FP7 IP FUTON Wired-Wireless Convergence, FP6 IP eSENSE WSNs, FP6 NoE CRUISE WSNs, FP6 IP MAGNET and FP6 IP Magnet Beyond Secure Personal Networks/Future Internet as the latest ones. She is currently the project coordinator of the FP7 CIP-PSP LIFE 2.0 and IST IP ASPIRE and was project coordinator of FP6 NoE CRUISE. She was also the leader of EC Cluster for Mesh and Sensor Networks and is Counselor of IEEE Student Branch, Aalborg. Her current research interests are in the area of IoT & M2M, Cloud, identity management, mobility and network management; practical radio resource management; security, privacy and trust. Experience in other fields includes physical layer techniques, policy based management, short-range communications. She has published over 160 publications ranging from top journals, international conferences and chapters in books. She is and has been in the organization and TPC member of several international conferences. She is the co-editor is chief of *Journal for Cyber Security and Mobility* by River Publishers and associate editor of *Social Media and Social Networking* by Springer.

Ramjee Prasad (R) is currently the Director of the Center for TeleInfrastruktur (CTIF) at Aalborg University (AAU), Denmark and Professor, Wireless Information Multimedia Communication Chair. He is the Founding Chairman of the Global ICT Standardisation Forum for India (GISFI: www.gisfi.org) established in 2009. GISFI has the purpose of increasing the collaboration between European, Indian, Japanese, North-American, and other worldwide standardization activities in the area of Information and Communication Technology (ICT) and related application areas. He was the Founding Chairman of the HERMES Partnership – a network of leading independent European research centres established in 1997, of which he is now the Honorary Chair.

Ramjee Prasad is the founding editor-in-chief of the Springer *International Journal on Wireless Personal Communications*. He is a member of the editorial board of several other renowned international journals, including those of River Publishers. He is a member of the Steering, Advisory, and Technical Program committees of many renowned annual international conferences, including Wireless Personal Multimedia Communications Symposium (WPMC) and Wireless VITAE. He is a Fellow of the Institute of Electrical and Electronic Engineers (IEEE), USA, the Institution of Electronics and Telecommunications Engineers (IETE), India, the Institution of Engineering and Technology (IET), UK, and a member of the Netherlands Electronics and Radio Society (NERG) and the Danish Engineering Society (IDA). He is also a Knight (“Ridder”) of the Order of Dannebrog (2010), a distinguishment awarded by the Queen of Denmark.