Relay Selection Aided Security in Cognitive Radio Networks

Nitheesh S B[#1], *R V Nagarajan*[#2]
.[#1] *M.E Communication System, Rohinni College of Engineering and Technology,*
.[#2]*AP, ECE Department, Rohinni College of Engineering and Technology*

Abstract: Cognitive radio is an emerging trend to solve the problem of scarce spectrum resources in the prosperous area of wireless communication. By dynamically utilizing unoccupied spectrums of primary (licensed) users, secondary (unlicensed) users can meet their own communication requirements. Consider a cognitive radio (CR) network consisting of a secondary transmitter (ST), a secondary destination (SD) and multiple secondary relays(SRs) in the presence of an eavesdropper, where the ST transmits to the SD with the assistance of SRs, while the eavesdropper attempts to intercept the secondary transmission. We rely on careful relay selection for protecting the ST-SD transmission against the eavesdropper with the aid of both single-relay and multi-relay selection. We evaluate the performance of the proposed relay selection schemes.

Keywords: Cognitive radio network, relay selection, eavesdropping attack, security threats.

I. INTRODUCTION

The security aspects of cognitive radio (CR) systems have attracted increasing attention from the research community.An illegitimate user may attempt to tap the communications of authorized users by eaves dropping, to intercept confidential information. CR networks face diverse security threats during both spectrum sensing [5], [6] as well as spectrum sharing [7],spectrummobility[8]andspectrummanagement[9]. Traditionally, cryptographic techniques are employed for guaranteeing transmission confidentiality against an eavesdropping attack. The existing cryptographic approaches are not perfectly secure and can still be decrypted byaneavesdropper(E). Physical-layer security [16], [17] is emerging as an efficient approach for defending authorized users against eavesdropping attacks by exploiting the physical characteristics of wireless channels.

Motivated by the above considerations, we explore the physical-layer security of a CR network comprised of a secondary transmitter (ST) communicating with a secondary destination (SD) with the aid of multiple secondary relays (SRs) in the presence of an unauthorized attacker. Basically, Cognitive Radio has four major functions, namely; Spectrum sensing, Spectrum sharing, Spectrum management and Spectrum mobility.

Spectrum sensing: Cognitive Radio has the ability to determine available spectrum and

© Journal - ICON All Rights Reserved

also sense the presence of Primary User (license user) in a channel. In spectrum management, two techniques exist; spectrum analysis and spectrum decision.

Spectrum Sharing: Spectrum sharing is to share some of the idle spectrum band to secondary users in such a way that the operation of primary users will not be affected in any way.

Spectrum Mobility: CR can change its operating frequency in order to use spectrum in a dynamic manner and make use of the best available frequency band.

II. RELAY SELECTION AIDED PROTECTION

A. System Model: As shown in Fig. 1, we consider a primary network in coexistence with a secondary network (also referred to as a CR network). The primary network includes a primary base station (PBS) and multiple primary users (PUs), which communicate with the PBS over the licensed spectrum. By contrast, the secondary network consisting of one or more STs and SDs exploits the licensed spectrum in an opportunistic way. Evesdropper attempts to intercept the secondary transmission from the ST to the SD.

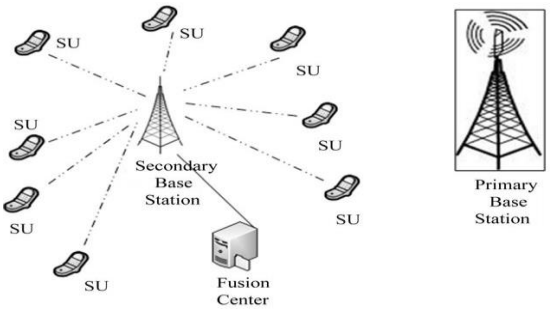


Fig.1 Cognitive Radio Network

For notational convenience, let H_0 and H_1 represent the event that the licensed spectrum is unoccupied and occupied by the PBS during a particular time slot, respectively. Moreover, let $\hat{}$ H denote the status of the licensed spectrum detected by spectrum sensing. Specifically, $\hat{}$ H = H_0 represents the case that the licensed spectrum is deemed to be unoccupied, while $\hat{}$ H = H_1indicates that the licensed spectrum is deemed to be occupied. The probability P_d of correct detection of the presence of PBS and the associated false alarm probability P_f are defined as $P_d = P_r(\hat{} H = H_1|H_1)$ and $P_f = P_r(\hat{} H = H_1|H_0)$, respectively. Due to the background noise and fading effects, it is impossible to achieve perfectly reliable spectrum sensing without missing the detection of an active PU and without false alarm, which suggests that a spectral band is occupied by a PU, when it is actually unoccupied.

Moreover, the missed detection of the presence of PBS will result in interference between the PU and SU. To guarantee that the interference imposed on the PUs is below a tolerable level, both the successful detection probability (SDP) Pd and false alarm probability (FAP) Pf should be within a meaningful target range. For example, the IEEE 802.22 standard requires $P_d > 0.9$ and $P_f < 0.1$. For better protection of PUs, we consider $P_d = 0.99$ and $P_f = 0.01$, unless otherwise stated.

B. Direct Transmission: Let us first consider the conventional direct transmission as a benchmark scheme.

C. Single-Relay Selection: We consider the cognitive relay network where both SD and E are assumed to be beyond the coverage

© Journal - ICON All Rights Reserved

area of the ST, and N secondary relays (SRs) are employed for assisting the cognitive ST-SD transmission. We assume that a common control channel (CCC) is available for coordinating the actions of the different network nodes and the decode-and-forward (DF) relaying using two adjacent time slots is employed.

More specifically, once the licensed spectrum is deemed to be unoccupied, the ST first broadcasts its signal xs to the N SRs, which attempt to decode xs from their received signals. For notational convenience, let D represent the set of SRs that succeed in decoding xs. Given N SRs, there are 2N possible subsets D, thus the sample space of D is formulated as

$$\Omega=\{/ \quad 0,D1,D2,\cdots,Dn,\cdots,D2N-1\}$$

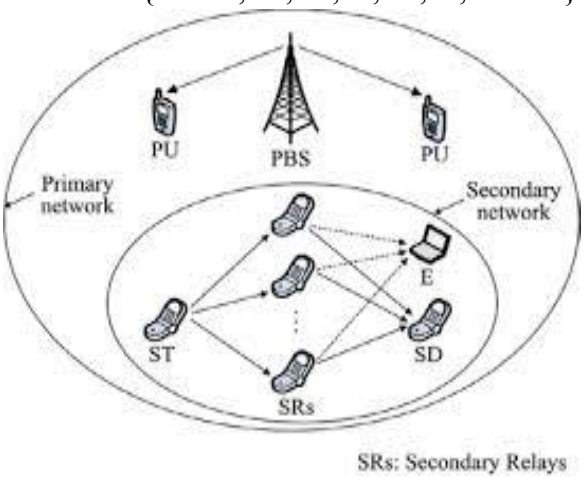


Fig.2 Relay Network

Hence, the signal received at a specific SRi is given by $y_i = h_{is}\sqrt{P_s}x_s + h_{pi}\sqrt{\alpha P_p}x_p + n_i$, where h_{si} and h_{pi} represent the fading coefficients of the ST-SRi channel and that of the PBS-SRi channel, respectively.

D. Multi-Relay Selection: This sub section presents a MRS scheme, where multiple SRs are employed for simultaneously forwarding the source signal x_s to SD. To be specific, ST first transmits x_s to N SRs over a detected spectrum hole. We denote by D the set of SRs that successfully decode x_s. IfD is empty, all SRs fail to decode x_s and will not forward the source signal, thus both SD and E are unable to decode x_s. If D is non-empty (i.e. $D = D_n$), all SRs within D_n are utilized for simultaneously transmitting x_s to SD. This differs from the SRS scheme, where only a single SR is chosen from D_n for forwarding x_s to SD. Considering that all SRs within D_n are selected for simultaneously transmitting x_s with a weight vector w, the signal received at SD is expressed as

$$y_{multi} = \sqrt{P_s}w^T H_d x_s + \sqrt{\alpha P_p}h_{pd}x_p + n_d, \quad (17)$$

where $H_d = [h_{1d}, h_{2d}, \cdots, h_{|Dn|d}]^T$.

III. COGNITIVE RADIO NETWORK ARCHITECTURE

There are three different architectures namely Infrastructure architecture, Ad-Hoc architecture and Mesh architecture.

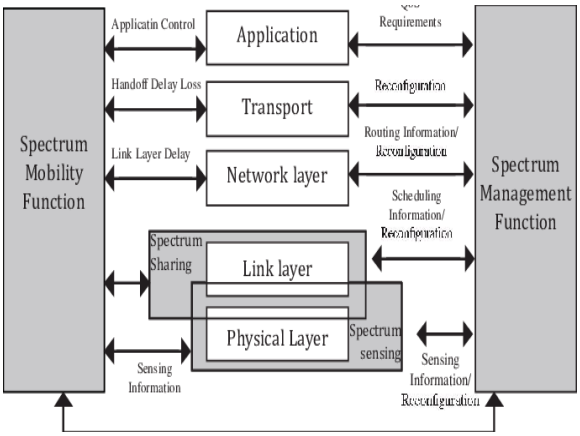


Fig.3 Layered architecture of cognitive radio

Infrastructure architecture: An infrastructure CRN consists of a base stations or access

© Journal - ICON All Rights Reserved

points which are devices having CR capabilities. The base stations communicate with other devices within its respective range through the base station itself. Communication between devices in cells other than itself is routed by the base stations.

Ad Hoc architecture: Ad-hoc CRNs consists of devices that do not need base stations, the devices can establish links between each other using different communication protocols.

Mesh architecture: Mesh architecture can be considered as a combination of infrastructure architecture and ad hoc architecture. In mesh architecture devices connect to the base stations through neighboring devices with the base stations working as routers forwarding packets.

IV. SECURITY THREATS

Security of CRN communications is one of the most critical issues to deal with. CRNs are more vulnerable to security threats originating from their open communication environment than wired networks. Attacks on wireless nodes privacy may involve different strategies including eavesdropping, impersonation and traffic analysis. These attacks may harm wireless networks in general and CRN among them.

A. **Eavesdropping and Impersonation:** In passive eavesdropping attack, the attacker silently listens to the CRN wireless communications to extract useful information about the sessions including the communicating parties, PUs, and SUs, and uses that information to launch a replay attack or an impersonation attack.

B. **Selective Forwarding Attack:** Within a selective forwarding attack, malicious CR nodes may refuse to forward certain messages originating from an authentic CR node or the BS, and possibly destroying them to ensure that they are not propagated any further beyond that real CR node.

C. **Sinkhole and Sybil Attack:** Attackers advertise incorrect information to other participating CR nodes. Sybil attack consists of a possible single CR node that pretends to be present at different locations of the network.

D. **Wormholes Attack:** Wormholes may convince two CR nodes to be neighbors when in fact they are far away from each other. This implies that identities and real addresses (locations) of such CR nodes will be disturbed.

E. **Hello Flood Attack:** In a Hello Flood attack, attackers can broadcast HELLO message to CR nodes to establish a connection and then advertise high-quality route to sink. This helps attackers to spoof acknowledgements to convince other nodes that a weak link between nodes or hops is strong or that a dead CR node is alive. As a result, a weak link may be designated for routing forcing packets sent through that link to other nodes to be lost or corrupted.

F. **Hardware Attacks:** Hardware attacks attempts to damage the hardware of some CR nodes or alter their functions. The impact of such attacks can range from totally shutting down a CR node, or leading it to transmit signals in a wrong frequency band.

G. **CR Software Attacks:** Like any other software, CR software is subject to various attacks. However, due to the

© Journal - ICON All Rights Reserved

specific characteristics of CRNs, attacks on their software will have even higher impact. Software attacks can completely paralyze CRNs.

H. **Primary User Emulation Attacks:** Using masquerading attacks or a PU Emulation Attack (PUE), a malicious adversary may masquerade a PU by replicating its characteristics and signal. This attack is uncomplicated to perform due to the flexibility of the cognitive radio of any CR node

I. **Jamming Disruption Attacks:** Jammers transmit a signal to the receiving antenna of the CR with the same frequency as that of an authorized transmitter, and thus thwarting the legitimate reception through the receiving antenna.

J. **Spectrum Sensing Data Attacks:** Counterfeiting spectrum sensing data is a high risk attack within the spectrum management process in charge of allocating appropriate bands to users. As a result of this attack, spectral analysis will be incorrect resulting in the wrong decisions of assigning improper bands to PUs and SUs

V. CRN SECURITY REQUIREMENTS

Availability: Within CRNs, the Base stations (BSs) should ensure the availability of spectrum needed by PUs and SUs. BSs should be equipped with the needed security measures to deter DoS attacks including distributed DoS.

Authentication: To ensure that CRN devices and components are communicating with a legal party, PUs, SUs, and other devices, authenticating them is essential. This applies to BS authenticating CRNs and CRNs authenticating each other.

Integrity: It is demanding to ensure that the messages sent by BS, CRN, PU, or SU have not been modified when arriving at their destination. Cryptographic hash functions and MACS need to be adopted to ensure message integrity.

Confidentiality/Privacy: PUs and SUs are interested in keeping their communications confidential.

VI. CRN SECURITY ENHANCEMENTS

1) For passive eavesdropping attack, messages need to be encrypted and time stamped to prevent replays. PUs and SUs will verify the message and only accept it if it is verifiable. To prevent impersonation attack, anonymous IDs are recommended.

2) To counter attack a selective forwarding attack, the CR node or BS can establish a timing limit. If this limit is exceeded and the PU or SU has not received the message, it will inform the BS through another secure node. The BS will then resend the message using that route or another one if needed.

3) To prevent an attacker from actually providing a false high quality route to a sink in case cognitive sensor networks are used, CR nodes can request certificates. These certificates could be issued by BS or by a Cognitive Radio Network Authority.

4) To counter measure the possibility of wormholes, the BS must provide each node with the anonymous IDs of the neighboring nodes and the distances from each one of

© Journal - ICON All Rights Reserved

these nodes. All this information must be encrypted.

5) For Hello Flood attack, certificates and authentication need to be enforced. Furthermore, routing protocols that use link layer acknowledgments must be replaced by more secure protocols.

6) To account for hardware attacks, hardware encryption must be provided.

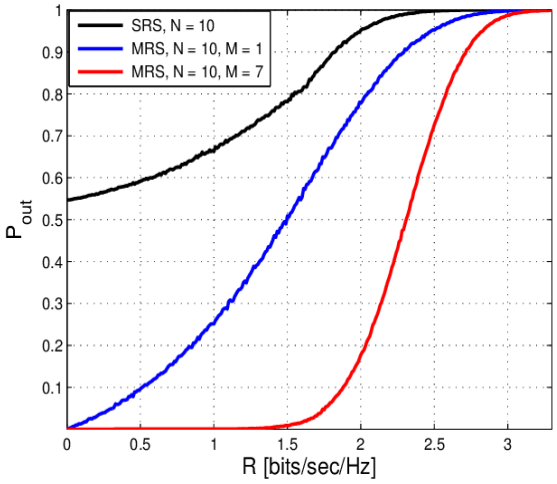
7) To resist software attacks, tamper-resistance, intrusion detection systems, and virus detection techniques should be incorporated to deter any malicious software installations.

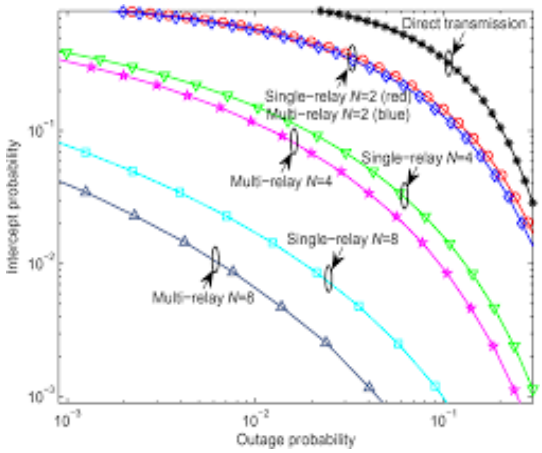
Further, the fusion center must verify any sensing information received from CR nodes in order to assess their integrity. Authenticating CR nodes can avoid receiving and using misleading information about PU activities, which can be disseminated by malicious nodes.

VII. SIMULATION RESULTS

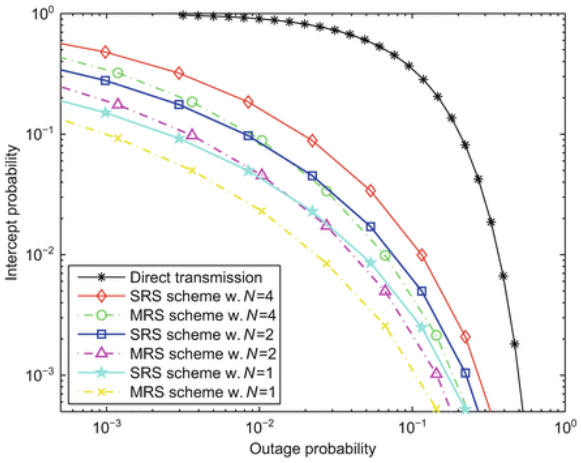
In this section, we present numerical tests by means of computer simulations. The observations made are: 1. One of the available relays in the secondary network is "randomly chosen" for both cooperative transmission and spectrum sensing. 2. The "best relay" for transmission is selected and used for both transmission and spectrum sensing tasks. 3. The "best relay" for spectrum sensing is selected and used for both tasks. 4. The proposed method of selecting the "optimum relay" for joint transmission and spectrum sensing.

Fig. 4 shows the simulated results of direct transmission for the SRS and MRS schemes. It can be seen from Fig. 4 that the IP of the direct transmission, the artificial noise based as well as of the proposed SRS and MRS schemes all improve upon tolerating a higher OP, implying that a trade-off exists between the IP (security) and the OP (reliability) of CR transmissions. Fig. 4 also shows that both the proposed SRS and MRS schemes outperform the direct transmission and the artificial noise based approaches in terms of their SRT, showing the advantage of exploiting relay selection against the eavesdropping attack. Moreover, the SRT performance of the MRS is better than that of the SRS.





© Journal - ICON All Rights Reserved



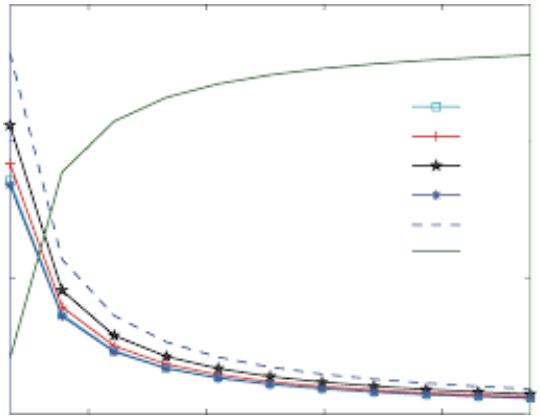


Fig.4 Simulation results of SRS and MRS schemes

AlthoughtheMRSachievesabetter SRT performance than its SRS-aided counterpart, this result is obtained at the cost of a higher implementation complexity, since multiple SRs require high-complexity symbol-level synchronizationforsimultaneouslytransmittingtotheSD,whereas the SRS does not require such elaborate synchronization. Upon increasing P_0, the licensed band becomes unoccupied by the PUs with a higher probability and hence the secondary users (SUs) have more opportunities for accessing the licensed band for their data transmissions, which leads to a reduction of the OP for CR transmissions.

Meanwhile, increasingP_0 maysimultaneouslyresultinanincreaseoftheIP , since the eavesdropper also has more opportunities for tapping the cognitive transmissions. However, in both the SRS and MRS schemes, the relay selection is performed for the sake of maximizing the legitimate transmission capacity without affecting the eavesdropper's channel capacity. Hence, upon increasing P_0, it becomes more likely that the reduction of OP is more significant than the increase of IP, hence leading to an overall SRT improvement for the SRS and MRS schemes.

CONCLUSION

Cognitive radio is a promising concept which uses the available spectrum more efficiently through opportunistic spectrum deployment. Security is one of most critical concerns in these networks because of their inherent vulnerabilities. In this paper, we proposed relay selection schemes for a CR network consisting of a ST, a SD and multiple SRs communicating in the presence of an eavesdropper. We examined the SRT performance of the SRS and MRS assisted secondary transmissions in the presence of realistic spectrum sensing, where both the security and reliability of secondary transmissions are characterized in terms of their IP and OP, respectively. We also analyzed the SRT of the conventional directtransmissionasabenchmark.Itwasillustratedthatasthe spectrumsensingreliabilityincreases,theSRTsofboththeSRS and MRS schemes improve.

© Journal - ICON All Rights Reserved

We also showed that the proposed SRS and MRS schemes generally outperform the conventional direct transmission and artificial noise based approaches in terms of their SRT. Moreover, the SRT performance of MRS is better than that of SRS.

REFERENCES

[1] Akyildiz,W.-Y. Lee, M. C. Vuran, and S. Mohanty,"A survey on spectrum management in cognitive radio networks," IEEE Commun. Mag., vol. 46, no. 4, pp. 40–48, Apr. 2008.

[2] Baldini, T. Sturman, A. R. Biswas, and R. Leschhorn, "Security aspects in software defined radio and cognitive radio networks: A survey and a way ahead," IEEE Commun. Surveys Tuts., vol. 14, no. 2, pp. 355–379,May 2012.

[3] Brown and A. Sethi, "Potential cognitive radio denial-of-service vulnerabilities and protection countermeasures: A multi-dimensional analysis and assessment," in Proc. 2nd Int. Conf. CROWNCOM, Orlando, FL,USA, Aug. 2007, pp. 456–464.

[4] Cabric,S. M. Mishra, and R. W. Brodersen, "Implementation issues in spectrum sensing for cognitive radios," in Proc. 38th Asil. Conf. Signal, Syst. Comput., Pacific Grove, CA, USA, Nov. 2004, pp. 772–776.

[5] Ghasemi and E. S. Sousa, "Fundamental limits of spectrum-sharing in fading environments," IEEE Trans Wireless Commun., vol. 6, no. 2,pp. 649–658, Feb. 2007.

[6] Lakshmanan, C. Tsao, R. Sivakumar, and K. Sundaresan, "Securing wireless data networks against eavesdropping using smart antennas," in Proc. 28th ICDCS, Beijing, China, Jun. 2008, pp. 19–27

[7] Li, "Cooperative spectrum sensing via belief propagation in spectrum heterogeneouscognitive radio systems," in Proc. IEEE WCNC, Sydney, N.S.W., Australia, Apr. 2010, pp. 1–6.

[8] Li and Z. Han, "Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems part I: Known channel statistics," IEEE Trans. Wireless Commun., vol. 9, no. 11, pp. 3566–3577,Nov. 2010.

[9] Ma, G. Zhao, and Y. Li, "Soft combination and detection for cooperative spectrum sensing in cognitive radio networks," IEEE Trans. Wireless Commun., vol. 7, no. 11, pp. 4502–4507, Nov. 2008.

[10] Southwell, J. Huang, and X. Liu, "Spectrum mobility games," in Proc.31st INFOCOM, Orlando, FL, USA, Mar. 2012, pp. 37–45.

[11]T.BrownandA.Sethi,"Potentialcognitive radiodenial-of-servicevulnerabilities and protection countermeasures: A multi-dimensional analysis and assessment," in Proc. 2nd Int. Conf. CROWNCOM, Orlando, FL, USA, Aug. 2007, pp. 456–464.

[12] S. Lakshmanan, C. Tsao, R. Sivakumar, and K. Sundaresan, "Securing wireless data networks against eavesdropping using smart antennas," in Proc. 28th ICDCS, Beijing, China, Jun. 2008, pp. 19–27.

[13] A. Olteanu and Y. Xiao, "Security overhead and performance for aggregation with fragment retransmission (AFR) in very high-speed wireless 802.11 LANs," IEEE Trans. Wireless Commun., vol. 9, no. 1, pp. 218– 226, Jan. 2010.

[14] Y. Xiao, V. K. Rayi, X. Du, F. Hu, and M. Galloway, "A survey of key management schemes in wireless sensor networks," Comput. Commun., vol. 30, no. 11–12, pp. 2314–2341, Sep. 2007.

[15] A. Mukherjee, S. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," IEEE Commun. Surveys Tuts., vol. 16, no. 3, pp. 1550–1573, Aug. 2014.

© Journal - ICON All Rights Reserved

[16] A. D. Wyner, "The wire-tap channel," Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355–1387, 1975.
[17] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel," IEEE Trans. Inf. Theory, vol. 24, no. 4, pp. 451–456, Jul. 1978.
[18] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in Proc. IEEE ISIT, Adelaide, SA, Australia, Sep. 2005, pp. 2152–2155.
[19] M. Bloch, J. O. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information theoreticsecurity,"IEEETrans.Inf.Theory,vol .54, no. 6, pp. 2515–2534, Jun. 2008.
[20] P. K. Gopala, L. Lai, and H. Gamal, "On the secrecy capacity of fading channels," IEEE Trans. Inf. Theory, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

© Journal - ICON All Rights Reserved