Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 4, April 2013, pg.223 – 226

RESEARCH ARTICLE

RELAY SELECTION FOR SECURE CO-OPERATIVE NETWORKS WITH JAMMING

Lakshmipraba.K[1], Nithya Devi.S[2], Praveen.P[3], Suresh Kumar.M[4], Mrs.V.Vennila[5]
[1,2,3,4]Department of Computer Science and Engineering, Anna University Chennai, India
[5]Assistant Professor, Department Of Computer Science and Engineering,
K.S.R. College Of Engineering, Tiruchengode, India

[1] lakshmiruthu@gmail.com; [2] snithyadevibe@gmail.com; [3] praveensft13@gmail.com;
[4] ssksuresh2010@gmail.com; [5] vennview@yahoo.co.in

Abstract— In this proposed system, we investigate joint relay and jammer selection in two-way cooperative networks, consisting of two sources, a number of intermediate nodes, and one eavesdropper, with the constraints of physical-layer security. Specifically, the proposed algorithms select two or three intermediate nodes to enhance security against the malicious eavesdropper. The first selected node operates in the conventional relay mode and assists the sources to deliver their data to the corresponding destinations using an amplify-and-forward protocol. The second and third nodes are used in different communication phases as jammers in order to create intentional interference upon the malicious eavesdropper. First, we find that in a topology where the intermediate nodes are randomly and sparsely distributed, the proposed schemes with cooperative jamming outperform the conventional non jamming schemes within a certain transmitted power regime. We also find that, in the scenario where the intermediate nodes gather as a close cluster, the jamming schemes may be less effective than their non-jamming counterparts. Therefore, we introduce a hybrid scheme to switch between jamming and non-jamming modes. Simulation results validate our theoretical analysis and show that the hybrid switching scheme further improves the secrecy rate.

Key Terms: - Cooperative jamming; friendly jammer selection; physical-layer security; relay selection, two-way relay

I. INTRODUCTION

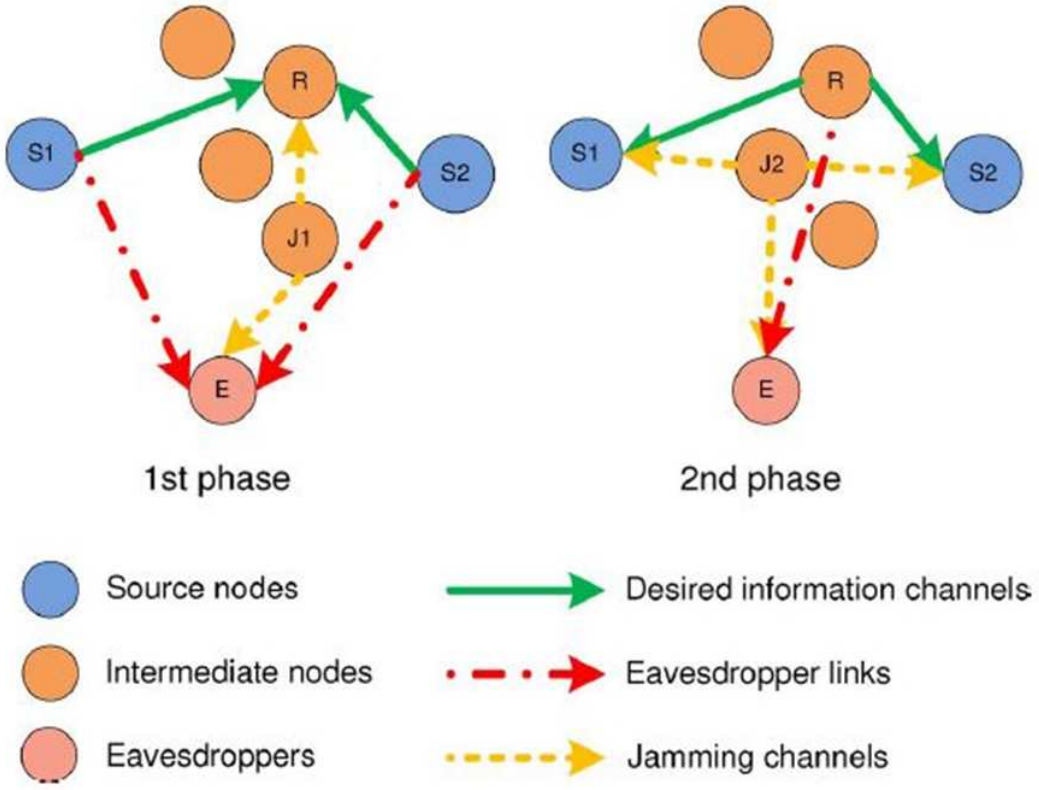
Traditionally security in wireless networks has been mainly focused on higher layers using cryptographic methods. The basic idea of physical-layer security is to exploit the physical characteristics of the wireless channel to provide secure communications. The security is quantified by the secrecy capacity, which is defined as the maximum rate of reliable information sent from the source to the intended destination in the presence of eavesdroppers. When the wiretap channel is a degraded version of the main channel, the source and the destination can exchange secure messages at a nonzero rate. Two-way communication is a common scenario in which two nodes transmit information to each other simultaneously. Recently, the two-way relay channel has attracted much interest from both academic and industrial communities, due to its bandwidth efficiency and potential application to cellular networks and peer-to-peer networks. In AF and DF protocols for one-way relay channels were extended to the general full-duplex discrete two-way relay channel and half-duplex Gaussian two-way relay channel, respectively. In network and channel coding were used in the two-way relay channel to increase the sum-rate of two sources.

The two-way memoryless system with relays, in which the signal transmitted by the relay is obtained by applying an instantaneous relay function to the previously received signal in order to optimize the symbol error rate performance. As for secure communications and role of feedback in secrecy for two-way networks, and

proved that the loss in secrecy rate when ignoring the feedback is very limited in a scenario with half-duplex Gaussian two-way relay channels and an eavesdropper. in a cooperative communication network, proper relay/jammer selection can have a significant impact on the performance of the whole system. Several relay selection techniques have been explored by far. The authors in proposed a non-jamming relay selection scheme for two-way networks with multiple AF relays in an environment without eavesdroppers, which maximized the worse received signal-to-noise ratio (SNR) of the two end users.

In several relay selection techniques were proposed in one-way cooperative networks with secrecy constraints. a scheme that can implement information exchange in the physical layer against eavesdroppers for two-way cooperative networks, consisting of two sources, a number of intermediate nodes, and one eavesdropper, with the constraints for physical-layer security. In which the relay selection is operated in an environment with no security requirement, our work takes into account the secrecy constraints. In contrast to, where many relay selections based on the DF strategy for one-way cooperative wireless networks were proposed and a safe broadcasting phase was assumed, the problem we consider here involves a non-security broadcasting phase, and the information is transferred bidirectional.

The principal question here is how to select the relay and the jammers in order to increase information security, and meanwhile protect the source messages against the eavesdropper. Several selection algorithms are proposed, aiming at promoting the assistance to the sources as well as the interference to the eavesdropper. The theoretical analysis and simulation results reveal that the proposed jamming schemes can improve the secrecy rate of the system by a large scale, but only within a certain transmitted power range. In some particular scenarios, the proposed schemes become less efficient than the conventional ones. We then propose a hybrid scheme with an intelligent switching mechanism between jamming and non-jamming modes to solve this problem.



II. TWO WAYS CO-OPERATIVE NETWORK

In this module, we can implement information exchange against eavesdroppers in two-way cooperative networks, consisting of two sources, one eavesdropper, and a number of intermediate nodes, with secrecy constraints.

Specifically, an intermediate node is selected to operate in the conventional amplify-and-forward (AF) relay mode and assists the sources to deliver data to the corresponding destinations. Meanwhile, another two intermediate nodes that perform as jamming nodes are selected and transmit artificial interference in order to degrade the eavesdropper links in the first and second phase of data transmission, respectively.

III. CONVENTIONAL SELECTION WITHOUT JAMMING

In this module, in a conventional cooperative network, the relay scheme does not have a jamming process. The conventional selection does not take the eavesdropper channels into account and the relay node is selected according to the instantaneous signal – to- noise ratio (SNR) of the links between *S*ource 1 to *S*ource 2.

IV. OPTIMAL SWITCHING

In this module, the original idea of using jamming nodes is to introduce interference on the eavesdropper links. However, it simultaneously degrades the links between the relay *R* and the destinations. In some specific situation is close to one destination, continuous jamming may decreases secrecy seriously, and acts as a bottleneck for the system. In order to overcome this problem, we introduce the idea of intelligent switching between two nodes.

V. OPTIMAL SWITCHING WITH JAMMING

In this module, the optimal selection with jamming assumes knowledge set and ensures a maximization of the sum of instantaneous to defined as the overall signal -to- interference-and-noise-ratio (SINR) of the channel The overall secrecy performance of the system is characterized by the ergodic secrecy rate that is the expectation of the sum of the two sources' secrecy rate for different types of channel feedback.

VI. SIMULATION RESULTS

The intermediate nodes spread randomly within the square space. It is clear that selection with jamming outperform their non-jamming counterparts within a certain transmitted power range. Outside this range the secrecy rate of OSJ converges to a power-independent value. Whereas the ergodic secrecy rate of OS continues to grow with a slope. This validates the analysis the suboptimal scheme SSJ performs almost the same as the optimal scheme OSJ. Furthermore, it can be seen from that OW provides better performance than any other selection techniques with or without continuous jamming. Within this configuration, we also compare the performance of different selection techniques measured by secrecy outage probability.

VII. CONCLUSIONS

This paper has studied joint relay and jammer selection in two-way cooperative networks with physical-layer security consideration. The proposed schemes achieve an opportunistic selection of one conventional relay node and one (or two) jamming nodes to enhance security against eavesdroppers based on both instantaneous and average knowledge of the eavesdropper channels. The selected relay node helps the information transmission between the two sources in an AF strategy, while the jamming nodes are used to produce intentional interference at the eavesdropper in different transmission phases. We found that the proposed jamming schemes (i.e., OS-MSISR, OS-MMISR, SS-MSISR, and SS-MMISR) are effective within a certain transmitted power range for scenarios with the intermediate nodes sparsely distributed. Meanwhile, the non-jamming schemes are preferred in configurations where the intermediate nodes are confined close to each other. The OSW scheme which switches intelligently between jamming and non-jamming modes is very efficient in providing the highest secrecy rate in almost the whole transmitted power regime in two-way cooperative networks, but it requires instantaneous eavesdropper channel knowledge. On the other hand, the SSW scheme, which is based on the average knowledge of the eavesdropper channel and thus much more practical, provides a comparable secrecy performance with the OSW scheme.

REFERENCES

[1] E. D. Silva, A. L. D. Santos, L. C. P. Albini, and M. Lima, "Identitybased key management in mobile ad hoc networks: Techniques and applications," IEEE Wireless Commun., vol. 15, no. 5, pp. 46–52, Oct. 2008.
[2] A. D. Wyner, "The wire-tap channel," Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
[3] 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.
[4] I. Csiszár and J. Körner, "Broadcast channels with confidential messages,"IEEE Trans. Inf. Theory, vol. 24, no. 3, pp. 339–348, May 1978.
[5] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in Proc. IEEE Int. Symp. Information Theory, Adelaide, Australia, Sep. 2005.
[6] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in Proc. IEEE Int. Symp. Information Theory, Seattle, WA, Jul. 2006.
[7] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.
[8] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," IEEE Trans. Inf. Theory, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.
[9] Y. Liang and H. V. Poor, "Generalized multiple access channels with confidential messages," in Proc. IEEE Int. Symp. Information Theory, Seattle, WA, Jul. 2006.
[10] Y. Liang and H. V. Poor, "Multiple-access channels with confidential messages," IEEE Trans. Inf. Theory, vol. 54, no. 3, pp. 976–1002, Mar.2008.
[11] I. Csiszár and P. Narayan, "Secrecy capacities for multiterminal channel models," IEEE Trans. Inf. Theory, vol. 54, no. 6, pp.2437–2452, Jun. 2008.
[12] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," IEEE Trans. Inf. Theory, vol. 54, no. 6, pp.2453–2469, Jun. 2008.
[13] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Secure wireless communications via cooperation," in Proc. 46th Ann. Allerton Conf.Communication, Control, and Computing, UIUC, Illinois, Sep. 2008.
[14] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Amplify-andforward based cooperation for secure wireless communications," in Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, Taipei, Taiwan, Apr. 2009.
[15] E. Tekin and A. Yener, "Achievable rates for the general Gaussian multiple access wire-tap channel with collective secrecy," in Proc. 44th Ann. Allerton Conf. Communication, Control, and Computing, Monticello, IL, Sep. 2006.

