International Journal of Modern Communication Technologies & Research (IJMCTR)
ISSN: 2321-0850, Volume-2, Issue-3, March 2014

Detection of Malicious Relays in Cooperative Wireless Communications

B. Vanmathi, P. Kuppusamy and S. Chandra

***Abstract*— A multi-relay network works spatial multifariousness by transmitting user's messages through multiple relay paths. Assume that all terminals are fully concerted and leave undone or leave out the effect of possibly existing malicious relay behaviors. In this paper, regards a multi relay network that originate of both cooperative and malicious relays, and point to obtain an improved cognition on the optimal behaviors of these two groups of relays via information-theoretic mutual information games. By modeling the set of cooperative relays and the set of malicious relays as two players in a zero-sum game with the maximum capable of existing rate as the utility, the optimal transmission scheme of both types of relays are derived by identifying the Nash equilibrium of the proposed game. Our main contributions are twofold. First, an inductive reasoning to previous works is obtained by allowing malicious relays to either listen or attack in Phase 1 (source-relay transmission phase). This is in direct contrast to previous works that only allow the malicious relays to listen in Phase 1 and to attack in Phase 2 (relay-destination transmission phase). The latter is shown to be suboptimal in this problem. Second, the impact of CSI knowledge at the end point on the optimal attack scheme that can be adopted by the malicious relays is identified. In particular, for the more practical scenario where the inter relay CSI is unknown at the destination, the unvarying attack is shown to be optimal as opposed to the normally considered Gaussian attack.**

***Index Terms*—Cooperative communications, malicious relay,**
Jamming, CSI, game theory, mutual information

I. INTRODUCTION

Cooperative or relay communications [1] - [5] allow users in a wireless system to transmit their messages through the relaying of multiple cooperative partners or relay stations. The relay paths provide spatial diversity that can be exploited to enhance communication reliability and throughput. Multi relay network consists of a source, destination and multiple relays that are including some malicious. The interaction of two or more person or organization directed toward a common goal, which is mutually promoting. I.e. joint action. When a node breaks any of the security principles and is therefore under any attack". Such nodes exhibit one or more of the following behavior:

Manuscript received Feb. 25, 2014.
B. Vanmathi, M.E/CSE, King College of Technology, Namakkal.
P. Kuppusamy, Associate Professor, CSE, King College of Technology, Namakkal, Tamilnadu, India.
S.Chandra, Assistant Professor, Computer Science, Selvam Arts and Science College, Namakkal, India.

- Packet Drop
- Bandwidth Consumption
- Malicious Node Entering
- Delay
- Denying from Sending Message
- Stealing Information

The information reports how a signal propagates from the sender to the receiver and corresponding the combined effect for example, sprinkling, fading, and power decay with distance. The CSI makes it possible to adapt transmissions to current channel conditions, which is crucial for achieving reliable communication with high data rates in multi antenna systems. The interaction between cooperative and malicious relays is modeled as a two-player zero-sum game .The goal of the two players is opposite to one another.

Here, two-player zero-sum game to model this cardinal problem. The source and the set of cooperative relays are viewed collectively as one player. The set of malicious relays are viewed as other player. The maximum code rate the beginning can transmit to ensure successful decoding at the destination. The maximum accomplishable rate is chosen as the utility measure. Malicious relays may utilize shared network information to advisedly, jam the reception at the receiver, and alter the messages that are to be forwarded. The main objective of the existing paper is to ascertain: Optimal signaling at the source, cooperative relays, and the malicious relay [6]-[11]. The optimal transmission strategies of different types of relays are derived by identifying the Nash equilibrium (NE). Malicious relays considered disrupting the communication between the source and the destination. The cooperative relays first receive signals from the source in Phase 1 and forward magnified versions of the received signal to the end in Phase 2.The malicious relays, on the other hand, may choose to both listen to the source in Phase 1 and utilize this information to emit busybodies signals in Phase 2 or emit jamming signals in both phases.

ADVANTAGES

A. Reliability

The probability that an item will perform a required function without failures understated conditions for a stated period of time.

B. Throughput

It is defined as how much data can be transferred from one location to another in a given period of time.

II. RELATED WORK

Regards a multirole network that consists of an origin, a destination and multiple relays in which some of the nodes are maybe malicious. A two-phase AF relay protocol is employed, where the relays first receive signals from the source in Phase1 and then forward amplified versions of these signals to the destination in Phase 2 [6]. Here, malicious relays may apply shared network information to intentionally jam the reception at the receivers or alter the messages that are to be forwarded [7]. Therefore, the source and the cooperative relays must design their transmission scheme to reduce the impact of these malicious behaviors. The main objective of this paper is to determine the optimal signaling at the source, the cooperative relays, and the malicious relays. Here the two-player zero-sum game theory [12] is modeled. Here, the source and the set of cooperative relays are viewed collectively as one player and the set of malicious relays as the other player. The maximum achievable rate (i.e., the mutual information between source and destination) is chosen as the utility measure. The optimal transmission strategies of different types of relays are derived by identifying the Nash equilibrium (NE) of the proposed game. The strategies are optimal in the sense that no single player can do better by unilaterally altering its own strategy. This paper furnishes a better discernment of the optimal signaling of both players. Note that the malicious relays considered in this work are those that purposely interrupt the communication between the source and the destination.
First, this paper views are more general set of attack strategies where the malicious relays to either listen to the source in Phase 1 utilize this information to transmit interfering signals in Phase2) or to directly emit jamming signals in both phases. The malicious relays were only allowed to listen in Phase 1 and attack in Phase 2. The results show that the optimal strategy taken by the malicious relays should be to jam rather than to listen in Phase 1. Secondly, the optimal attack strategy taken by the malicious relays are shown to depend on the CSI knowledge at the destination. This is different from *faulty* relays [13], where the relay behaviors may be incidental and are often irrational.

In [7], an AF relay network with one single-antenna cooperative relay and one single-antenna jammer (i.e., malicious relay) is examined. This paper can be viewed as a generalization of [7] to the case with multiple relays and more general attacking strategy. In [8] and in [9], the interaction between cooperative and malicious relays is examined for decode-and-forward (DF) networks. For DF networks, the source codebook is revealed to the relays and each relay is assumed to be able to successfully decode the source message. The problem in AF networks, as considered here, differs considerably forwarding of noise (and possibly also jamming signals) in Phase 2. The effect of malicious relays or jammers has also been examined in the context of multiple access channels in [6], [10], and in the context of secrecy channels with eavesdroppers in [14]–[17]. Not that, in contrast to the malicious relays (or jammers) considered in our work, the relays and jammers considered in [16] and [17] are friendly and work cooperatively to prevent eavesdropping by unauthorized receivers. The zero-sum game approach has also been applied to study jamming attacks in parallel slow fading channels in [11].

III. METHODOLOGY

The relay paths provide spatial diversity that can be exploited to raise communication reliability and throughput. Here, three modules are used:

A. Relay Node Deployment Scheme

The relay is chosen to forward a weighted version of its received signal. In timeserving relay chatting, in the first phase, the source transmits information, and the best relay listens. At the same time, a chatting group is formed from the remaining relays to perform cooperative jamming, is designed to create no interference at the best relay. In the second phase, the best relay forwards the weighted version of its received signal, and at the same time, a new chatting group performs cooperative jamming, designed to avoid interference at the end.

B. Cooperative Jamming and Gaming Relays

The origin and the cooperative relays have a common objective to increase the system throughput. The malicious relays, on the other hand, are antagonists that aim to make a break in the communication between the source and the destination. The problem was explicated as a zero-sum game and the optimal transmission strategies for the source, the cooperative relays, and the malicious relays were found by identifying the NE of the game. When full CSI is available at the destination, it shows that the optimal strategy for malicious relays is to emit Gaussian jamming signals in both phases.

C. Entropy Identification

The source-eavesdropper channel is a degenerate version of the source-destination channel, there exists a rate secret cipher such that dependable transmission at up to cipher at destination is possible in just about perfect secrecy. The equivocation rate equals the entropy of the data source. Along this line of work, secret communications through broadcast channels. We derive the optimal transmission strategies for the case where full CSI is available at the destination [6]-[10]. We obtain the selective information between source and destination. Theoretical studies on jammer or malicious relay behaviours have been considered in [14], [15].

This paper considers a more general set of attack strategies where the malicious relays are given the freedom of choosing to either listen to the source so that it can utilize this information to transmit interfering signals or to directly emit jamming signals that are independent of the source message in both phases. The optimal attack strategy taken by the malicious relays are shown to depend on the CSI knowledge at the destination. Specifically, when full CSI is available at the destination, it shows that the optimal attack strategy that can be taken by malicious relays is to emit Gaussian jamming

signals in both phases. The relays and jammers considered [16] and [17] are friendly can work cooperatively to prevent eavesdropping by unauthorized receivers.

IV. PERFORMANCE EVALUATION

A. Metrics

The utility of Player 1 versus the number of concerted relays is shown for the case with Full CSI, the case with Unknown H (mc) and the case with no vicious relays. Here, the number of cooperative relays is varied from 0 to 7.
The number of malicious relays is smaller than the number of cooperative relays. The advantages of increasing cooperative relays impregnate rapidly since for large cooperative relays, the jamming signals emitted by the malicious relays become the dominant source of noise and, thus, the effective receive SNR no longer increases with cooperative relays.

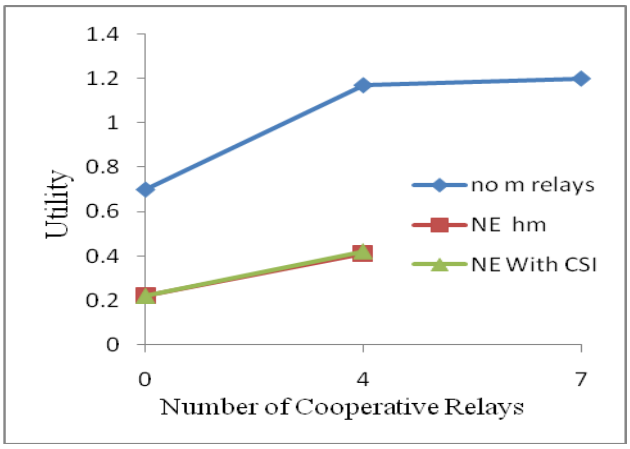

Fig. 1. Cooperative Relays

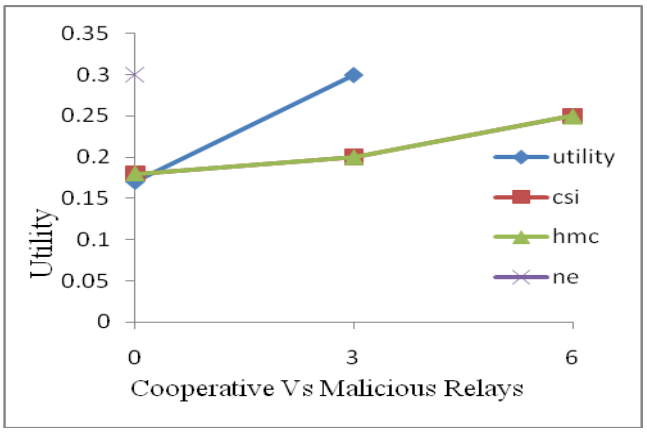

Fig.2 Cooperative Vs Malicious Relays

The advantages of increasing cooperative relays saturates rapidly since for large cooperative relays, the jamming signals emitted by the malicious relays become the dominant source of noise and, thus, the effective receive SNR no longer increases with cooperative relays.

The utility of Player 1 is shown versus increasing power constraints at the cooperative relays. The utility of Player 1 increases as power constraints increases, but the advantage saturates rapidly since the power of the jamming signal is magnify proportionally as power constraints increases and thus, becomes the dominant origin of noise.

V. CONCLUSION

In this paper, an aim to furnish an improved understanding of the interaction between cooperative and malicious relays inane AF multirole network examine with previous works. The problem was formulated as a zero-sum game and the optimal transmission strategies for the source, the cooperative relays, and the malicious relays were found by identifying the NE of the game.

In the two-phase transmission protocol under circumstance, malicious relays can either listen in Phase 1 or attack in Phase 2 or simply attack in both phases. When full CSI is available at the destination, it proves that the optimal scheme for malicious relays is to emit Gaussian jamming signals in both phases. However, if the interlay channel is not known at the destination, the malicious relays should alternatively attack with a constant jamming signal in Phase 1 and a Gaussian jamming signal in Phase 2. In both cases, the source should employ Gaussian signaling and all depots should transmit with full power.

REFERENCES

[1] T. Cover and A. El Gamal, "Capacity theorems for the relay channel,"*IEEE Trans. Inf. Theory*, Sep. 1979, vol. 25, no. 5, pp. 572–584.
[2] J. N. Laneman, D. N. C. Tse, and G.W.Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inf. Theory*, Dec. 2004, vol. 50, no. 12, pp. 3062–3080.
[3] A. Sendonaris, E. Erkip, and B. Aazhang, "User cooperation diversity. Part I. System description," *IEEE Trans. Commun.*, Nov. 2003, vol. 51, no. 11, pp.1927–1938.
[4] Y.-W. Hong,W.-J. Huang, F.-H. Chiu, and C.-C. J. Kuo, "Cooperative communications in resource-constrained wireless networks," *IEEE Signal Process. Mag.*, May 2007, vol. 24, no. 3, pp. 47–57.
[5] Y.-W. P. Hong, W.-J. Huang, and C.-C. J. Kuo, *Cooperative Communications and Networking: Technologies and System Design*. New York, NY, USA: Springer, 2010.
[6] S. Farahmand, G.B. Giannakis, and X.Wang, "Max-min strategies for power-limited games in the presence of correlated jamming," in *Proc.41st Annu. Conf. Inf. Sciences and Syst. (CISS)*, 2007, pp. 300–305.
[7] T. Wang and G. B. Giannakis, "Mutual information jammer-relay games," *IEEE Trans. Inf. Forensics Security*, Jun. 2008,vol. 3, no. 2, pp. 290–303.
[8] A. Kashyap, T. Basar, and R. Srikant, "Correlated jamming on MIMO Gaussian fading channels," *IEEE Trans. Inf. Theory*, Sep. 2004, vol. 50, no. 9, pp. 2119–2123.
[9] M.-H. Chen, S.-C. Lin, and Y.-W. Peter Hong, "A game theoretic approach for the cooperative network with the presence of malicious relays," in *Proc. IEEEGlobal Commun. Conf. (Globecom)*, Houston,TX, USA, 2011.
[10] S. Shafiee and S. Ulukus, "Mutual information games in multiuser channels with correlated jamming," *IEEE Trans. Inf. Theory*, Oct. 2009, vol. 55, no. 10, pp. 4598–4607.
[11] S.Wei, R. Kannan, V. Chakravarthy, and M. Rangaswamy, "CSI usage over parallel fading channels under jamming attacks: A game theory study," *IEEE Trans. Commun.*, Apr.2012, vol. 60, no. 4, pp. 1167–1175.
[12] M. J. Osborne and A. Rubinstein*," A Course in Game Theory"* Cambridge, MA, USA: MIT Press, 1994.

[13] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *IEEE J. Sel. Areas Commun.*, Oct. 2007, vol. 25, no. 8, pp. 1557–1568.

[14] A. Mukherjee and A. L. Swindlehurst, "Equilibrium outcomes of dynamic games in MIMO channels with active eavesdroppers," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Cape Town, South Africa, 2010.

[15] A. Yuksel, X. Liu, and E. Erkip, "A secure communication game with a relay helping the eavesdropper," *IEEE Trans. Inf. Forensics Security*, Sep. 2011,vol. 6, no. 3, pp. 818–830.

[16] R. Zhang, L. Song, Z. Han, and B. Jiao, "Distributed coalition formation of relay and friendly jammers for secure cooperative networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kyoto, Japan, 2011.

[17] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Trans. Veh. Technol.*, Oct. 2012, vol. 61, no. 8, pp. 3693–3704.