ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 12, December 2014

Preventing the falsified data injection attack through multiple relay network

M.Priyanka[1],G.PremaPriya[2]

PG Student, Department of CSE, Sri Shakthi College Of Engineering AndTechnology, Coimbatore, Tamilnadu [1]

Assistant Professor, Dept of CSE, Sri Shakthi College Of Engineering And Technology , Coimbatore, Tamilnadu [2]

Abstract: A relay network is a broad class of network topology commonly used in networks, where the source and destination are interconnected by means of some nodes. In such a network the source and destination cannot communicate to each other directly because the distance between the source and destination is greater than the transmission range of both of them, hence the need for intermediate node(s) to relay. The problem of detecting malicious relay nodes in single source, multi-relay networks has been studied in the literature for different relaying strategies. Relay nodes in apply network coding while those in and follow the decode-and-forward protocol. The authors consider a peer-to-peer (P2P) network in which peers receive and forward a linear combination of the exogenous data packets.

To check the integrity of the received packets, a signature vector is generated at the source node and broadcasted to all nodes where it is used to check the integrity of the received packets. In and several information theoretic algorithms for mitigating falsified data injection effects are proposed. The network model used in these works is composed of a single source, multiple intermediate nodes which apply network coding. We consider a multiple access relay network where multiple sources send independent data to a single destination through multiple relays, which may *inject* falsified data into the network. To detect the malicious relays and discard (erase) data from them, tracing bits are embedded in the information data at each source node.

Keywords –Multiple Access Relay Network, Tradeoff Between Reliability And Security, Falsified Data Injection Attack

I. Introduction

A. COOPERATIVE RELAYING

The cooperative relaying approach has a great potential to provide substantial benefits in terms of reliability (diversity gain) and rate (bandwidth or spectral efficiency) following a wireless relay network composed of single source, single relay, and single destination. In this network, the transmission occurs in two phases. In the first phase, the source sends its message to the destination. Because of the broadcast nature of the wireless channel, the relay hears the first phase transmission. In the second phase, the relay assists the source by forwarding the received signal to the destination. In order to decode the source's message, the destination combines the signals received from the source and the relay.

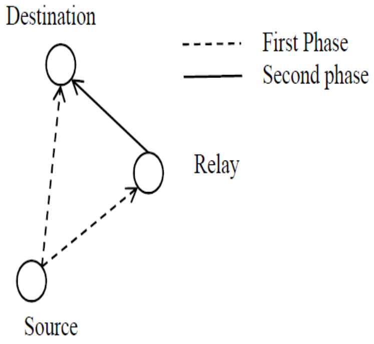

Figure 1.1 Single source, single relay and single destination

1.2 MULTIPLE ACCESS RELAY NETWORKS

Multiple access relay network. In multiple-access relay network (MARN), multiple sources communicate with a single destination in the presence of relay nodes. Examples of such networks include hybrid LAN/WAN networks and sensor and ad hoc networks where cooperation between sources is either undesirable or notpossible, but one can use intermediate relay nodes to aid communication between the sources and the destination.

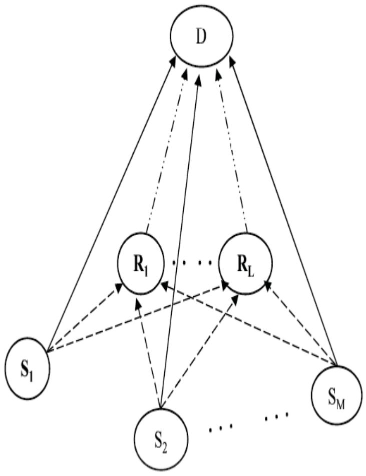

Figure 1.2 N Source, R Relay and one Destination

DOI 10.17148/IJARCCE

1.3 SECURITY ISSUES IN MARN

In multiple access relay networks, relay nodes may combine the symbols received from different sources to generate parity symbols (packets) and send them to the destination. Then, the destination may use the network generated parity symbols (packets) to enhance the reliability of decoding. While this technology is promising in improving communication quality, it also presents a new challenge at the physical layer due to the dependency of the cooperation. That is, reliance on implicit trust relationship among participating nodes makes it more vulnerable to falsified data injection. Although this might also occur in a traditional system without cooperative communication, its effect is far more serious with cooperative communication. If a false packet is injected into the buffer of a node, the output of the node will become polluted, and this may soon propagate to the entire network.

1.4 GENERAL PROJECT DETAILS

Consider exploiting the information on the presence of attack in enhancing the reliability of decoding by erasing (discarding) the data received from adversarial nodes and correcting the erasures. The motivation is that erasures can be corrected twice as many as errors. However, the information on the presence of attack may not be perfect in practice. The false alarm results in an erasure of correct bit, while the miss detection may result in an error in place of an erasure. Since the probability of false alarm and that of miss detection depend on the amount of tracing bits and the errors-and-erasures correction capability depends on the amount of parity bits, we expect there exists an optimal allocation of the redundancy between tracing bits and parity bits that minimizes the probability of decoding error at the destination. Here, the tracing bits are to identify the malicious relay nodes and erase the data received from them, while the parity bits are to the correct errors caused by channel and noise.

For a given redundancy, more parity bits (more reliability) implies less tracing bits (less security), and vice versa. That is, there exists a tradeoff between reliability and security. Once the malicious relay nodes are identified, some security measures such as en-route filtering and/or containment may be applied to limit the spread of false data. We investigate the optimal allocation of a given amount of redundancy (tradeoff) between tracing bits and parity bits and the resulting performance gain in terms of the probability of decoding error and the throughput. To overcome the drawbacks, we enhance the proposed system to achieve more scalability. If any sources update any file location, it needs to update the location information which maintain in the relay system thus overcome the false routing. If any source goes offline i.e. disconnect from the relay systems thus is must indicate offline mode in the relay node if so it must not consider for routing. By implementing these steps as our enhancement with the proposed system, we overcome the drawbacks and get the high scalability as well as certain information about the source mode status and files location.

II LITERATURE SURVEY

2.1 Distributed Cooperative Transmission with Unreliable and Untrustworthy Relay Channels

Cooperative transmission is an emerging wireless communication technique that improves wireless channel capacity through multiuser cooperation in the physical layer. It is expected to have a profound impact on network performance and design. However, cooperative transmission can be vulnerable to selfish behaviors and malicious attacks, especially in its current design. In this paper, we investigate two fundamental questions Does cooperative transmission provides new opportunities to malicious parties to undermine the network performance? Are there new ways to defend wireless networks through physical layer cooperation? Particularly, we study the security vulnerabilities of the traditional cooperative transmission schemes and show the performance degradation resulting from the misbehaviors of relay nodes.

Then, we design a trust-assisted cooperative scheme that can detect attacks and has self-healing capability. The proposed scheme performs much better than the traditional schemes when there are malicious/selfish nodes or severe channel estimation errors. Finally, we investigate the advantage of cooperative transmission in terms of defending against jamming attacks. A reduction in link outage probability is achieved.

The majority of work on cooperative transmission focuses on communication efficiency, including capacity analysis, protocol design, power control, relay selection, and cross layer optimization. In those studies, all network nodes are assumed to be trustworthy. Security threats are rarely taken into consideration.

- well known that malicious nodes can enter many wireless networks due to imperfectness of access control or through node compromising attack. In cooperative transmission, the malicious nodes have chances to serve as *relays* (i.e., the nodes help the source node by forwarding messages). Instead of forwarding correct information, malicious relays can send arbitrary information to the destination.
- Cooperative transmission can also suffer from selfish behavior. When the wireless nodes do not belong to the same authority, some nodes can refuse to cooperate with others, that is, not working as relay nodes, for the purpose of saving their own resources.
- In cooperative transmission, channel information is often required to perform signal combination and relay selection at the destination. The malicious relays can provide false channel state information, hoping that the destination. The security vulnerabilities of traditional cooperative transmission significantly damage the performance. Presence of implementation overhead.

2.2 Joint Network-Channel Coding in the Multiple-Access Relay Channel: Beyond Two Sources

The combination of log-likelihood ratio (LLR) quantization and network coding was previously shown to be a promising compress and forward strategy for the multiple access relay channel with two sources. In this paper, we generalize this approach to the case of more than two sources. Our proposed relay scheme consists of a scalar LLR quantizer for each source followed by a network coding (NC) step that suitably combines the quantizer outputs. We use the information bottleneck method to design the quantizers and the NC function. At the destination, an iterative message-passing decoder is used to jointly decode all source messages.

The proposed relay scheme consists of a scalar LLR quantizer for each source followed by a network coding (NC) step that suitably combines the quantizer outputs. We use the information bottleneck method to design the quantizers and the NC function. At the destination, an iterative message-passing decoder is used to jointly decode all source messages. Numerical simulations demonstrate the effectiveness of the proposed transmission strategy and its suitability for asymmetric source-relay channel conditions. Proposed a scalable CF-based transmission scheme for the MARC with more than two sources. This scheme performs optimal LLR quantization and NC based on the IBM at the relay. We have shown that the system performance can be improved substantially by adding more sources. The proposed scheme also achieves excellent performance for asymmetric source-relay channel conditions. We have furthermore analyzed the convergence behavior of the iterative joint network-channel decoder for which we proposed to use a serial message-passing schedule. Finally, simulation results confirm that the proposed scheme simultaneously achieves a diversity order of two for all sources in quasi-static fading channels. The proposed schedule clearly outperforms in the iterative joint network-channel decoder.

2.3 Cooperative Diversity in the Presence of a Misbehaving Relay: Performance Analysis

Cooperative wireless communications offers a new dimension of diversity by emulating transmit antenna diversity to provide reliable communications. In cooperative diversity, single-antenna radios behave as relays between a source and destination, and the performance improvements are due to cooperation of the source and the relay. However, a misbehaving relay can degrade the envisaged performance improvements severely. In practice, there are no mechanisms to ensure adherence of the relay to cooperation strategy. Due to this dependency on relay’s behavior cooperative diversity presents a new security challenge at the physical layer. In this paper, we investigate performance of cooperative diversity in the presence of a semi-malicious relay which does not conform to rules of cooperation at all time.

Due to lack of a mechanism to enforce cooperation, cooperative diversity presents a new security challenge at the physical layer. Thus, cooperative communication systems introduce a new form of vulnerability at the physical layer. As this vulnerability is inherent to the system, it presents formidable challenges to the performance improvement envisaged by cooperative wireless communication systems. However, a misbehaving relay can degrade the envisaged performance improvements severely. In practice, there are no mechanisms to ensure adherence of the relay to cooperation strategy. Due to this dependency on relay’s behavior cooperative diversity presents a new security challenge at the physical layer. In this paper, we investigate performance of cooperative diversity in the presence of a semi-malicious relay which does not conform to rules of cooperation at all time. The relay behavior is characterized by a probabilistic cooperation model which exploits the uncertainty in the wireless channel. Based on this model, we obtain the performance degradation in cooperative diversity both by analysis and simulation. In this paper we identify the inherent vulnerability of cooperative diversity in the presence of misbehaving relays. This vulnerability arises due to a lack of mechanism to ensure relay’s adherence to the rules of cooperation. To determine the performance penalty in the absence of such mechanism, we consider a semi-malicious relay which behaves in a probabilistic manner. However, in a practical setting, relays might exhibit malicious or selfish behavior. A supporting mechanism is also required to enforce cooperation.

2.4 Signatures for Content Distribution with Network Coding

Recent research has shown that network coding can be used in content distribution systems to improve the speed of downloads and the robustness of the systems. However, such systems are very vulnerable to attacks by malicious nodes, and we need to have a signature scheme that allows nodes to check the validity of a packet without decoding. In this paper, we propose such a signature scheme for network coding. Our scheme makes use of the linearity property of the packets in a coded system, and allows nodes to check the integrity of the packets received easily. We show that the proposed scheme is secure, and its overhead is negligible for large files. The server breaks the file to be distributed into small blocks, and whenever a peer requests a file, the server sends a random linear combination of all the blocks. As in BitTorrent, a peer acts as a server to the blocks it has obtained. However, in a linear coding scheme, any output from a peer node is also a random linear combination of all the blocks it has already received. A peer node can reconstruct the whole file when it has received enough degrees of freedom to decode all the blocks. This scheme is completely distributed, and eliminates the need for a scheduler, as any block transmitted contains partial information of all the blocks that the sender possesses. It has been shown both mathematically and through live trials that the random linear coding scheme significantly reduces the downloading time and improves the robustness of the system.

Security problem is a main obstacle in the implementation of content distribution networks using random linear network coding. To tackle this problem, instead of trying to fit an existing signature scheme to network coding based systems, in this paper, we proposed a new signature scheme that is made specifically for such systems. We introduced a signature vector for each file distributed, and the signature can be used to easily check the integrity of all the packets received for this file. The computation complexity of this solution is quite high and the overhead for the scheme is not negligible for large files.

2.5 A Stochastic Model for Misbehaving Relays in Cooperative Diversity

Existing cooperative diversity protocols are designed with the inherent assumption that users exhibit cooperative behavior all the time. However, in a practical cooperative wireless system users may misbehave in malicious or selfish manner. Thus existing cooperative diversity protocols are inherently vulnerable to misbehaving users as they lack a mechanism to detect the presence of such users. In this paper we examine the physical layer consequences of a malicious user which exhibits cooperative behavior in a stochastic manner. We assume that the malicious user exploits the inherent uncertainty of the wireless channel to hide its malicious behavior. We consider a malicious user which exhibits cooperative and malicious behaviors according to first order Markov chain. Based on the stochastic relay model, we characterize the performance penalty incurred due to the absence of a mechanism to detect malicious relays in cooperative DF. We show both analytically and by simulation the severe degradation in bit error rate (BER) and diversity performance.
Characterize the inherent vulnerability of cooperative diversity in the presence of a misbehaving relay. This vulnerability arises as a result of the assumption that relays conform to the cooperation strategy at all times. However, in practice there are no mechanisms to ensure that a relay adheres to the rules of cooperation. To characterize the performance penalty due to the lack of such mechanism, we consider a relay which mimics the underlying Markov property of slow fading channels. Analytically that a malicious relay significantly degrades the cooperative diversity gain and lack in parameters to trust the relays.

2.6 Mitigation of Forwarding Misbehaviors in Multiple Access Relay Network

Proposed a physical layer approach to detect the relay node that injects false data or adds channel errors into the network encoder in multiple access relay networks. The misbehaving relay is detected by using the maximum a posteriori (MAP) detection rule which is optimal in the sense of minimizing the probability of incorrect decision (false alarm and miss detection). The proposed scheme does not require sending extra bits at the source, such as hash function or message authentication check bits, and hence there is no transmission overhead. The side information regarding the presence of forwarding misbehavior is exploited at the decoder to enhance the reliability of decoding. We derived the probability of false alarm and miss detection and the probability of bit error, taking into account the lossy nature of wireless links. The MAP approach in detecting the misbehaving relay that injects false data or adds channel errors into the network encoder in multi-access relay networks. The proposed scheme does not require sending extra bits at the source, such as hash function or message authentication check bits, hence there is no transmission overhead. In addition, it makes an instantaneous decision about whether a relay node is behaving properly without a long term observation. The side information regarding the presence of forwarding misbehavior is exploited at the probability of bit error, taking into account the lossy nature of wireless links. We found that the proposed decoder and the MAP decoder with the aid of the MAP detection are effective in mitigating the forwarding misbehaviors in multiple access networks with network coding.

CONCLUSION

In this proposed work characterize the inherent vulnerability of cooperative diversity in the presence of a misbehaving relay. This vulnerability arises as a result of the assumption that relays conform to the cooperation strategy at all times. However, in practice there are no mechanisms to ensure that a relay adheres to the rules of cooperation. To characterize the performance penalty due to the lack of such mechanism to ensure relay's adherence to the rules of cooperation. Found that there exists an optimal allocation of redundancy between tracing bits and parity bits that minimizes the probability of decoding error or maximizing the throughput. When the total amount of redundancy (sum of tracing bits and parity bits) is fixed, more redundancy should be allocated to the tracing bits for higher probability of being malicious and less on the tracing bits for lower SNR.

ACKNOWLEDGMENT

It‘s a great pleasure to thank my guide Mrs.G.Premapriya, AssistantProfessor, Department of Computer Science and Engineering for her valuable technical suggestion and continuous guidance throughout this project work Finally, I take this opportunity to extend our deep appreciation to my family and friends for all that they meant to us during the crucial times of the completion of our project into a successful one.

REFERENCES

[1] A. N. C. Tse, and G. Wornell, J. N. Laneman, “Cooperative diversity in wireless networks: Efficient protocols and outage behavior,” IEEE Trans. Inf. Theory, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.

[2] A. Nosratinia, and A. Hedayat, T. E. Hunter, “Cooperative communication in wireless networks,” IEEE Commun. Mag., vol. 42, no. 10, pp. 74–80, Oct. 2004.

[3] B. W. Kim, “Cooperative spatial multiplexing in mobile ad hoc networks,” in Proc. IEEE Int. Conf. Mobile Ad Hoc Sensor Syst. Conf., Washington, DC, USA, Nov. 2005, pp. 387–395.

[4] C. Host-Madsen and A. Nosratinia, “The multiplexing gain of wireless networks,” in Proc. IEEE ISIT, Adelaide, SA, USA, Sep. 2005, pp. 2065–2069.

[5] F. Kishore, Y. Chen and J. Li, “Wireless diversity through network coding,” in Proc. IEEE WCNC, Las Vegas, NV, USA, Apr. 2006, pp. 1681–1686.

[6] I. Li and X. Bao, “Matching code-on-graph with networks-on-graph: Adaptive network coding for wireless relay networks,” in

Proc. Allerton Conf. Commun., Control Comput., Champaign, IL, USA, Sep. 2005, pp. 1–10.

[7] K. Hausl and P. Dupraz, "Joint network-channel coding for the multipleaccess relay channel," in Proc. 3rd Annu. IEEE Commun. Soc. Sensor Ad Hoc Commun. Netw., Reston, VA, USA, Sep. 2006, pp. 817–822.

[8] M. W. Kim, S. G. Kim, and B. K. Yi, "Decentralized random parity forwarding in multi-source wireless relay networks," in Proc. IEEE Global Telecommun. Conf., Washington, DC, USA, Nov. 2007, pp. 3937–3941.

[9] P. Zhao, T. Kalkert, M. Medard, and K. J. Han, "Signatures for content distribution with network coding," in Proc. IEEE Int. Symp. Inf. Theory, Nice, France, Jun. 2007, pp. 556–560.

[10] R. Leong ,T. Ho, R. Koetter, M. Medard, M. Effros, and D. R. Karger, "Byzantine modification detection in multicast networks with random network coding," IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2798–2803, Jun. 2008.

[11] S. Katabi ,S. Jaggi, M. Langberg, S. Katti, T. Ho, M. Medard, et al., "Resilient network coding in the presence of Byzantine adversaries," IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2596–2603, Jun. 2008.

[12] T.Y. and Mao Wu , "Tracing malicious relays in cooperative wireless communications," IEEE Trans. Inf. Forensics Sec., vol. 2, no. 2, pp. 198–212, Jun. 2007.

[13] T. Dehnie, H. T. Sencar, and S. Memon, "Detecting malicious behavior in cooperative diversity," in Proc. 41st Annu. CISS, Baltimore, MD, USA, Mar. 2007, pp. 895–899.

[14] V. Lin and D. J. Costello, Error Control Coding, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[15] V. Goldsmith, Wireless Communications. Cambridge, U.K.: Cambridge Univ. Press, 2005.