International Journal of Computer Applications Technology and Research
Volume 3– Issue 11, 682 - 684, 2014, ISSN: 2319–8656

Ensure Security and Scalable Performance in Multiple Relay Networks

V.Eswaramurthy
Computer Science and Engineering
V.S.B Engineering College
Karur,India

A.P.V Raghavendra
Computer Science and Engineering
V.S.B Engineering College
Karur,India

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 a some nodes. In such a network the source and destination cannot transmit to each other directly because the distance between the source and destination is greater than the transmission range of both of them, hence the demand 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 schemes. 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 out the integrity of the received packets, a key 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 modeling used in these works is composed of a single source, multiple intermediate nodes which utilize network coding. We consider a multiple access relay network where multiple sources send independent data to a single destination through multiple relays, which may interject falsified data into the network. To detect the malevolent relays and dispose (efface) data from them, trace bits are embedded in the information data at each source node.

Keywords: Multiple access relay network, trade-off between reliability and security, falsified data injection and forward error correction**.**

1. INTRODUCTION

Multiple access relay networks, relay nodes may combine the packets received from different sources to generate parity symbols (packets) and send them to the destination. Then, the destination may usage the network generated parity symbols (packets) to enhance the reliability by decoding. While this technology is promising in improving communication quality, it also represents 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 traditionalistic system without cooperative communication, its effect is far-off more serious with cooperative communication. If a false packet is interjected into the buffer of a node, the output of the node will become improve, and this may soon propagate to the full network.

The problem of detecting malevolent relay nodes in single-source, multi-relay networks has been studied in the literature for different relaying schemes. Relay nodes in apply network coding while those in follow the decode-and-forward protocol. In 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 out the integrity of the received packets, a key signature vector is generated at the source node and broad-casted to all nodes where it is used to check the integrity of the received packets. In lot of information theoretic algorithms for mitigating falsified data injection effects are proposed. The network modeling used in these works is composed of a single source, multiple intermediate nodes which utilize network coding.

In all algorithms proposed in there are two fundamental assumptions. First, all exogenous data packets are known at a single node to generate the hash or the signature vector. Therefore, these algorithms cannot be applied in multi-source scenarios because each source generates independent packets and thus the packets of all sources are not available at a single node. Second, each received packet is decrypted independently, and then the integrity from the decoded packet is checked using the hash or the signature vector. However, when the received packets are combined before decoding, a different approach needs to be developed to check the credibility (integrity) of the received packets. For example, in three-terminal cooperative diversity systems, the packets of the source and that from the relay are combined (e.g. using maximal ratio combining (MRC)) before decoding the message packet and then the integrity is checked on the decoded message packet. In the authors consider inserting a number of tracing bits in the data stream at the source in a cryptographically secure manner in single source scenario. The receiver then calculates the ground truth of the tracing bits and compares them with the tracing bits received from the relay path to determine whether a relay node is adversarial or cooperative. If the correlation coefficient between them is above a threshold then we decide that the relay node is cooperative and, otherwise, it is malevolent. The threshold can be chosen to achieve a target false alarm, misdetection, or error probability. The authors of propose a statistical detection technique in order to mitigate malevolent behavior in adaptive decode-and-forward (DF) cooperative diversity.

To exploit the detection outcome to enhance the reliability of decoding by erasing (discarding) the data received from the adversarial nodes and correcting the erasures. The motivating is that erasures can be corrected twice as many as errors. However, the information in the presence of attack may not be perfect in practice. The false alarm results in an erasure of correct bit, while the miss detecting may result in an error in place of an erasure. Since the chance 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 require 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 malevolent relay nodes and erase the data received by them, while the parity bits are to the correct errors caused by channel and noise. For a given redundance, more parity bits (more reliability) implies less tracing bits (less security), and vice versa. That is, there exists a trade-off between reliability and security. We enquiry the optimal allocation of a given amount of redundancy (trade-off) between tracing bits and parity bits.

ARCHITECTURE DIAGRAM

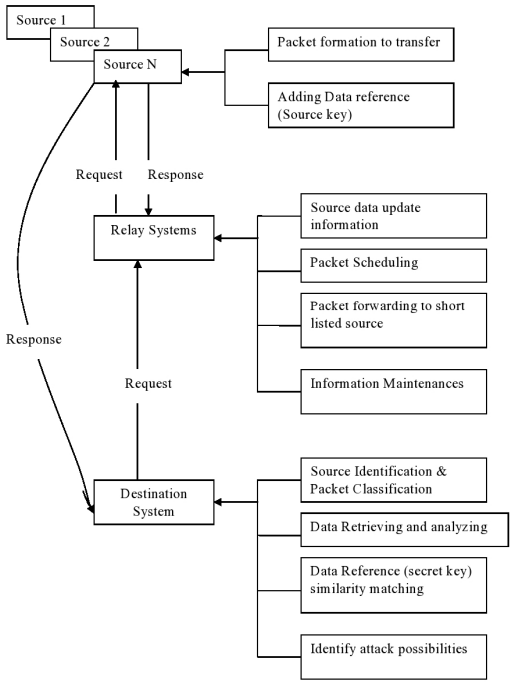

Fig. 1 Architecture Flow Diagram

2. RELATED WORK

2.1 Multiple Access Relay System

A multiple access relay network where multiple sources send independent data to a single destination through multiple relays. Multiple relay systems maintain the current information of the sources connection details and the respective files details. As per request and response relay system communicate with the source systems. In multiple access relay networks, relay nodes may combine the information's received from different sources to generate scheduling process as per destination request and forward the request to respective short listed source.

2.2 Source Response System

As per relay node request each source send the periodic update information about its connection status and the files information. The source generates independent packets after get the file request from the relay node then generate source key which is based on the contents in the file like

- Mitigation by Forwarding Misbehaviors in Multiple access relay network

reference/tracing bits. Then classify the destination system form the request packet and route the file to the destination system. At each source, the tracing bits are embedded in the k message bits using a position key κp which is common for all sources and is known to all source nodes and the destination. The generation and position keys are assumed to be unknown to the relay nodes. So, even if a relay is compromised the information on the tracing bits cannot be released to the attacker.

2.3 Destination Request System

To detect the malevolent relays and discard (erase) data from them, tracing bits are embedded in the data at each source node. The destination node then computes the ground truth of the tracing bits and compares them with the tracing bits received from the relay path to determine whether a relay node is adversarial or cooperative. Destination system sends the file request to the relay node and waits till the file gets download. After getting download request from the source system, the destination system accept the download request and classify the packet for to identify any false data may injected and identify the malevolent relay node.

2.4 False Data Injection Attack Detection

This module exploit the detection outcome to enhance the reliability of decoding by erasing (discarding) the data received from the adversarial nodes and correcting the erasures. Here, the tracing bits are to identify the malevolent relay nodes and erase the data received from them. Generate the data references for the content in the received file and calculate the distance between the data and find the similarity than compare with threshold, finally identify the malevolent activity of relay node and the injected data's.

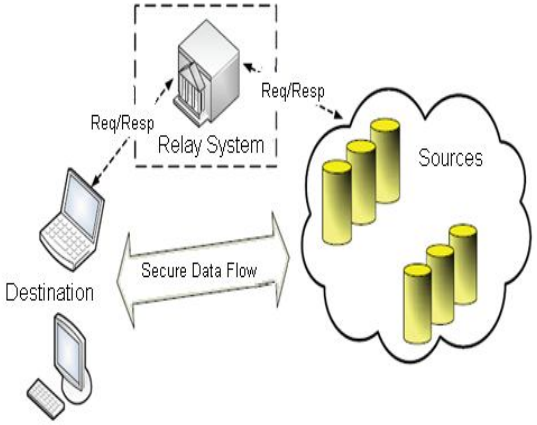

Fig. 2 Architecture Design

3. SECURE AND SCALABLE SCHEDULING PROCESS IN RELAY NETWORKS

We believed a multiple access relay network and investigated the following three processes:

- Trade-off between reliability and security under falsified data injection attacks
- Prioritized analog relaying

In the first process, a multiple access relay network where multiple sources send independent data to a single destination

through multiple relays which may inject a falsified data into the network. To detect the malevolent relays and discard (erase) data from them, tracing bits or secure key or data reference are embedded in the data at each source node. The performance metrics gains provided by the update optimal allocation/scheduling of data forwarding and the tradeoff between reliability and security are analyzed.

In the second process, a multiple access relay network where multiple sources send independent data simultaneously to a common destination through multiple relay nodes. Relay systems maintain update information about the source and its data. As per destination request relay system schedule the source and send the request packet to the respective source.

In the third process, a destination 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 source key or data reference detection rule which is optimal in the sense of minimizing the probability of incorrect decision (false alarm and miss detection). The proposed schema does not require sending extra bits at the source, such as hashish function or message authentication check bits, and hence there is no more transmission overhead. The side data regarding the presence of forwarding misbehavior is exploited at the decoder to enhance the reliability of decoding.

4. CONCLUSION

Optimal allocation of redundancy between tracing bits and parity bits that minimizes the probability of decoding error or maximizing the throughput. The generation and position keys are assumed to be unknown to the relay nodes. So, even if a relay is compromised the information on the tracing bits cannot be released to the attacker. 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. Analyzed the energy gain (saving) and the throughput gain provided by the optimal redundancy allocation.

5. FUTURE ENHANCEMENT

To overcome the drawbacks, enhance the 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 system, we overcome the drawbacks and get the high scalability as well as certain information about the source mode status and files location.

6. REFERENCES

[1] Taha A. Khalaf, Sang Wu Kim, and Alaa E. Abdel-Hakim, "Tradeoff Between Reliability and Security in Multiple Access Relay Networks Under Falsified Data Injection Attack" *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, VOL. 9, NO. 3, MARCH 2014.

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

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

[4] S. 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.

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

[6] Y. Chen, S. Kishore, and J. Li, "Wireless diversity through network coding," in *Proc. IEEE WCNC*, Las Vegas, NV, USA, Apr. 2006,pp. 1681–1686.

[7] X. Bao and J. Li, "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.

[8] C. 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.