THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

Secure Routing Algorithm to minimize the number of Intermediate Nodes in Unicast Network with Multiple Streams

S. Saravanya
PG Scholar, Department of CSE, MAM College of Engineering
Tiruchirapalli, Tamil Nadu, India
V. Pugazhenthi
Associate Professor, Department of CSE, M.A.M college of Engineering
Tiruchirapalli, Tamil Nadu, India

Abstract:
Linear Network coding is a technique which can be used to improve the network's efficiency, throughput and scalability as well as resilience to attacks and eavesdropping. Instead of relaying the packets of information received, the intermediate nodes of a network take several packets and combine them together for transmission thereby attaining maximum information flow in the network. However for secure data transmission, minimizing the number of intermediate nodes on multiple streams between the same source and destination pair is a real challenge. This paper aims to develop a secure routing algorithm that minimizes the number of intermediate nodes and maximizing transmission data rate using random linear transformation. This paper also focuses on utilizing the network coding scheme for defending active attacks particularly a wormhole attack using dynamic redundancy algorithm.

Key words*: Linear Network Coding, Random linear transformation, Intermediate nodes, Wormhole attack, Dynamic Redundancy Algorithm*

1. Introduction

Linear network coding is a promising technology that can maximize the throughput capacity of communication network, reduce delays and increase network robustness. In Linear network coding, algebraic algorithms are practiced with the data to accumulate the various transmissions. In traditional routing methods, packets are stored and forwarded to destinations. If a router node receives two packets from two different sources it forwards the packets one after another and queues the other packets even if both are headed for the same destination. Hence traditional routing method requires separate transmissions for every message delivered, which decreases network efficiency. In linear network coding, algorithms are used to merge two different messages at the same time and forwarded to the destination. After receiving the accumulated message, checking is done to detect whether it had received the correct message from the correct source.

Despite the salient features there are still many challenges to be addressed and security is clearly one of the most important challenges. In general, secure network coding is designed against two kinds of attacks: wiretapping and Wormhole attack. For passive attack such as wiretapping attack, Linear Network Coding provides confidentiality because Linear Network Coding tends to utilize more links and nodes to maximize the transmission rate. The wiretapping attack means some adversary can wiretap some communication signals with the purposes of curiosity or recovering the messages. In traditional transmission, packets are generally encrypted against wiretapping. Using network coding one can transmit the messages securely without the use of cryptographic approaches.

To defend against passive attacks a Network coding scheme called random network coding is proposed which is a simple yet powerful encoding scheme for secure network coding and protect from wiretapping attack, where the broadcast transmission schemes allows optimal throughput. There are two types of linear network coding Deterministic Linear Network coding and Random Linear Network coding. In Deterministic Linear network coding the packets are transmitted in a fixed and predetermined path. The path in which the message is to be transmitted is found and stored in a matrix format. The adversaries can easily gain the information since the path is fixed priory.

In Random Linear Network Coding the nodes transmit in random linear combinations of packets they receive that is current data, with coefficients chosen from a Galois field and broadcast to other nodes in the network. The advantages of random linear network coding over routing are distributed network operation and networks with dynamically varying connections. The implementation of secure network coding with random linear network coding involves two steps. First construct a transmission topology that includes a set of nodes and links to use and secondly design secure network coding scheme based on the constructed transmission topology. The transmission topology determines the maximum transmission rate that can be achieved with certain

security requirements. The unicast routing topology can significantly affect the maximum secure transmission rate under certain security requirements. Suppose that a transmission topology has been chosen to support a unicast flow, the messages obtained by every intermediate node should be limited to defend against passive attacks.

For launching a wormhole attack which is an active attack, an adversary uses wormhole links which connects two distant points in the network using a direct low-latency communication link. The wormhole link is established by variety of means like a Ethernet cable for long-range wireless transmission or an optical link. After that the adversary captures transmissions and sends them through the wormhole link and replays them at the other end. The wormhole attack can be prevented by using Redundancy Algorithm which detects the link and overcomes this attack.

Linear Network coding is also perceived to be useful in wireless mesh networks, messaging networks, multicast streaming networks, peer-to-peer networks and other networks where the same data needs to be transmitted to a number of destination nodes.

The paper focuses on addressing the design of secure linear network coding. Particularly, the network coding design that can both satisfy the weakly secure requirements and maximize the transmission data rate of multiple unicast streams between the same source and destination pair is investigated.

The paper is organized as follows. In section 2 the previous work of random linear network coding is dicussed. In section 3 The notations of Linear Network Coding is described. In section 4 a Topology called the Secure Unicast Routing Topolgy is constructed. In section 5 describes the path in which the messages is to be transmitted is selected by Random Linear Transformation. In section 6 alternate path is chosen if traffic is detected or wormhole attack is detected. In section 7 the size of finite field is reduced by reducing the number of intermediate nodes.

2. Related Works

With respect to passive attacks, there are two different models are existed weakly secure and Information theoretical secure. In Information theoretic model the adversary simply does not have enough information to break the encryption, so these cryptosystems are considered cryptanalytically unbreakable.

Weakly secure is that it is possible to transmit at a higher rate without the eavesdropper getting any meaningful information which cannot be done by Information theoretical secure. Random Linear Network Coding provides weakly secure model.

In [9] when the number of independent messages available to the eavesdropper is less than the multicast capacity, secure communication is possible without any loss in rate. Random Linear Network coding is used in weakly securing the network with large field size. In [7] a controlled amount of information is gained by the eavesdropper when the wiretapped links in wiretap network is larger than the maximum flow in the network from source to sink. In [8] for a multicast linear network coding problem secret sharing technique is used to provide security. Certain constraints should be met to follow secret sharing techique. It requires large field size.

In [10] Network coding security does not focus on threat posed by external wire tapper but the threat posed by intermediate nodes. This setup differs from previously considered wiretapping scenarios and a natural algebraic security criterion is developed. Algebric Security criterion is the level of security provided by random linear network coding is measured by the number of symbols that an intermediate node has to guess in order to decode *one* of the transmitted symbols. In complete acyclic directed graphs, the secure max-flow, as well as the minimum number of symbols required for algebraic security is determined. In [12] an acyclic delay-free networks has a bound on error probability in terms of the number of receivers and random coding output links which decreases exponentially with code length. For any acyclic network, a tighter bound on the probability of connection feasibility in a related network problem with unreliable links is found. Link failure probability and amount of redundancy affect randomized coding success probability.

Random Linear Network Coding can also be used for byzantine attack. In [5] a signature scheme is used that allows packet-level Byzantine detection. This scheme checks the membership of a received packet in the valid vector space. It saves bandwidth and allows one-hop containment of the contamination. Random Linear Network Coding is used to avoid passive attack like wiretapping attack and makes the syatem weakly secure.

In the previous work the finite field parameter is not considered as a main feature and the field size is large. In the proposed system the finite field size is reduced.

In [7], [8], [9], [10] the traffic pattern are discussed in multicast. Based on this Secure Unicast Routing Algorithm is studied and developed for Unicast with Multiple Streams.

3. LNC Scheme

In a directed acyclic network with set of nodes N and set of edges E is considered. A time-division multiplexing scheme is applied and the whole time horizon is partitioned into fixed size time slots. In unicast network with multiple streams L is the number of unicast flows from source s to destination d. k is the number of messages sent from source to destination. T is the time slot. K = kT. If L = 1, there is no weakly secure linear network code. For a single unicast stream there is no secret information is shared between source and destination nodes.

To encode the packets, LNC is applied, in which a total of (K x L) packets are coded and delivered to destination node d. Let M = $[m_{1,1},m_{1,2}, \ldots ,m_{1,K},m_{2,1}, \ldots ,m_{L,K}]T$ represent the data packets to be encoded at node s. Let Mi = $[m_{i,1},m_{i,2}, \ldots , mi ,K]T$ represent the set of data packets from stream i.

For link e and time slot t, vector $f_e(t)$ with length (K x L) is the global encoding vector (GEV), so that the coded data packet transmitted on e is f_e (t)M. Let In(v_i) and Out(v_i) be the set of input and output links of a given node vi, respectively. For the source node s, there are L virtual trunks, each of which represent one data stream and consist of k links with unit capacity.

4. Secure Unicast Routing Topology

In Secure Unicast with Multiple Streams (SUMS) senerio the Secure Unicast Routing (SUR) is done by Random Linear Network Coding. The Secure Unicast Routing Problem is equal to the link disjoint path problem. It is proven theoretically by a theorem.

For all link-disjoint paths and each intermediate node from source to destination in the network, the number of different paths passing through it is no more than the product of messages and Link - 1. It is referred as weakly secure k x L link-disjoint paths. The intermediate node does not cooperate with each other. After it is proven that it is equal to link disjoint path then an efficient algorithm is developed called the Secure Unicast Routing Algorithm.

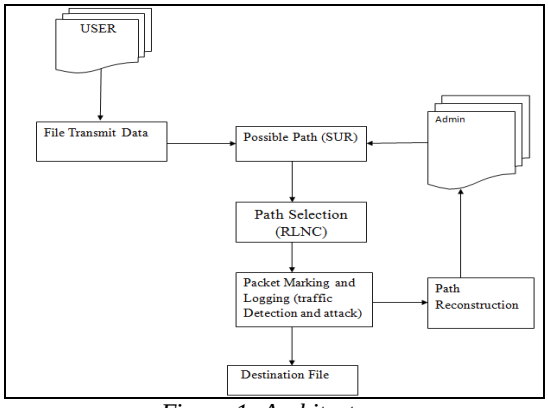

Figure 1: Architecture

In SUR Algorithm the node capacity is found out and then it checks whether a link to destination is available. Then it finds the possible path with maximum transmission rate as in figure 1.

5. Path Selection

In Random Linear Network Coding the messages are combined and sent in random path in random manner. The coding operations are only done at the nodes source s and destination d. The discrepancy in Random Linear Network coding from other LNC is instead of calculating the transformation matrix B which has the coefficients of messages and the path in matrix format, the elements in B are randomly chosen from the finite field Fq.

Once the SUR topology is formed, the secure network coding scheme is intended to achieve the maximum secure data transmission rate. After finding the possible path the messages are sent in one of the possible path using Real Time Scheduling Algorithm.

6. Packet Marking And Logging

If any traffic is detected then alternate path is found out and messages are sent in that path. The traffic is detected using Packet Marking Algorithm. The Real Time Scheduling and sensors are used to choose the best path without traffic and provide security from wormhole attack

6.1. Real Time Scheduling Algorithm

The characteristics and constraints of real-time tasks should be scheduled to be executed. There may be unexpected or irregular events and these must also receive a response. In all cases, there will be a time bound within which the response should be delivered. The ability of the computer to meet these demands depends on its capacity to perform the necessary computations in the given time. If a number of events occur close together, the computer will need to schedule the computations so that each response is provided within the required time bounds.

The Real Time Scheduler chooses the best path among the possible path before sending the messages by detecting traffic free link with maximum transmission rate and sends the messages.

6.2. Secure from Wormhole Attack

A user would issue a file and expect a response to be returned within the deadline. The use of fault tolerance mechanisms through redundancy improves query reliability. The system lifetime depends on the function of system parameters including the “source” and “path” redundancy levels. Redundancy management utilizing multipath routing to answer user queries and detect wormhole links in wormhole attack.

In this approach, each source node selects a path which can satisfy performance requirements of the intended application for transmitting its traffic towards the sink node. Although path discovery through path routing approach can be performed with minimum computational complexity, the limited capacity of a single path highly reduces the achievable network throughput .We applied our analysis results to the design of a dynamic redundancy management. The best design parameter settings at runtime in response to environment changes to prolong the system lifetime.

7. Size of the Finite Field

The field size is a significant parameter because it reduces both implementation complications and communication overhead. The field size value can be reduced if the unicast flows can put up with additional coding delay and the value of q can be abridged if the number of intermediate nodes in the Secure Unicast Routing topology decreases. Hence to reduce q, a SUR topology that can accomplish the maximum secure transmission rate and has the minimum number of intermediate nodes is found.

To reduce q URMI problem is studied. That is in a network with flow capacity, the product of messages and Links and node capacity the product of messages and Links – 1 the URMI problem is to find a unicast routing topology with the least number of intermediate nodes, which can provide link-disjoint paths from s to d, and for each intermediate node, the number of different paths passing through it is no more than node capacity. The URMI problem is NP Complete.

Based on this an efficient heuristic algorithm is developed called as UMI Algorithm(Unicast Routing Topology with minimum number of Intermediate Nodes) which gives w disjoint paths from s to d with the minimum number of links in the network. It also gives a feasible solution to URMI Problem.

8. Conclusion

Linear network coding (LNC) for secure unicast with multiple streams investigated the optimal LNC design issue for weakly SUMS between the same source and destination nodes. The design aims to satisfy the weakly secure requirements, maximize the transmission data rate, and minimize the size of the finite field which is satisfied using Secure Unicast Routing Algorithm. The usage of random linear code is investigated for weakly secure unicast and proved a lower bound for the probability that the random linear code is weakly secure. Extensive simulation results show the effectiveness of the proposed algorithms.

9. References

1. R. Ahlswede, N. Cai, S.-Y. Li, and R. Yeung, "Network Information Flow," IEEE Trans. Information Theory, vol. 46, no. 4, pp. 1204-1216, July 2000.
2. R. Koetter and M. Medard, "An Algebraic Approach to Network Coding," IEEE/ACM Trans. Networking, vol. 11, no. 5, pp. 782-795, Oct. 2003.
3. S.-Y.R. Li, R.W. Yeung, and N. Cai, "Linear Network Coding," IEEE Trans. Information Theory, vol. 49, no. 2, pp. 371-381, Feb.2003.
4. T. Ho, B. Leong, R. Koetter, M. Medard, M. Effros, and D. Karger, "Byzantine Modification Detection in Multicast Networks Using Randomized Network Coding," Proc. IEEE Int'l Symp. Information Theory, p. 144, 2004.
5. M. Kim, L. Lima, F. Zhao, J. Barros, M. Medard, R. Koetter, T. Kalker, and K.J. Han, "On Counteracting Byzantine Attacks in Network Coded Peer-to-Peer Networks," IEEE J. Selected Areas in Comm., vol. 28, no. 5, pp. 692-702, June 2010.
6. S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, and M. Medard, "Resilient Network Coding in the Presence of Byzantine Adversaries," Proc. ACM INFOCOM, pp. 616-624, 2007.
7. N. Cai and R. Yeung, "Secure Network Coding," Proc. IEEE Int'l Symp. Information Theory, p. 323, 2002.
8. J. Feldman, T. Malkin, C. Stein, and R.A. Servedio, "On the Capacity of Secure Network Coding," Proc. 42nd Ann. Allerton Conf. Comm., Control, and Computing, 2004.
9. K. Bhattad and K.R. Narayanan, "Weakly Secure Network Coding," Proc. First Workshop Network Coding, Theory, and Applications (NetCod), 2005.
10. L. Lima, M. Medard, and J. Barros, "Random Linear Network Coding: A Free Cipher?" Proc. IEEE Int'l Symp. Information Theory (ISIT), pp. 546-550, 2007.
11. T. Ho, R. Koetter, M. Medard, D. Karger, and M. Effros, "The Benefits of Coding over Routing in a Randomized Setting," Proc. IEEE Int'l Symp. Information Theory (ISIT), p. 442, 2003.
12. T. Ho, M. Medard, J. Shi, M. Effros, and D.R. Karger, "On Randomized Network Coding," Proc. 41st Ann. Allerton Conf. Comm. Control and Computing, vol. 41, pp. 11-20, 2003.
13. D. Silva and F. Kschischang, "Universal Weakly Secure Network Coding," Proc. IEEE Information Theory Workshop Networking and Information Theory (ITW), pp. 281-285, 2009.