A Review on Effective Algorithm to Secure Network Coding Systems against Wormhole Attack

Amruta Zanwar[1], Smita Ponde[2]

[1]Student, ME Department of Computer Science and Engineering, BAMU University
Deogiri Institute of Engineering and Management Studies, Aurangabad, Maharashtra, India

[2]Assistant Professor, Department of Computer Science and Engineering, BAMU University
Deogiri Institute of Engineering and Management Studies, Aurangabad, Maharashtra, India

Abstract: In wireless systems, network coding *has demonstrated a powerful approach in expanding system performance. Beside this if we consider the practical scenario; there are numerous security concerns which hinder its wide sending. Other than the very much contemplated pollution attacks, there is another serious risk of wormhole attacks. This attack collapses the execution increase of network coding. As the qualities of network coding are particularly not quite the same as traditional wireless networks. Subsequently the effect of these attacks and countermeasures are obscure. In this paper we analyzed the various techniques to detect as well as prevent wormhole attack and comparison between them. Consequently, we will take a review on centralized algorithm to find wormhole in the network.*

Keywords: Wormhole attack, RLNC-Random Linear Network Coding, Traditional wireless system, Wormhole detection techniques

1. Introduction

In wireless networks, network coding has demonstrated a powerful approach in increasing system performance. Network coding is a technique in which transmitted data is encoded and decoded to enhance network throughput, reduce delays and construct a more robust network. As the qualities of network coding are particularly not quite the same as traditional wireless networks. The methodology took after by network coding is on a very basic level not the same as traditional wireless network systems, where in between nodes store and forward parcels as original. In network coding forwarders are permitted to apply encoding schemes on what they receive and hence they themselves create and transmit new parcels. Contemplating blending or mixing packets on every node takes great advantage of opportunity multiplicity and broadcast characters of wireless systems, fundamentally enhances the system performance.

However network coding system confronts new difficulties. And among these difficulties the wormhole attack is the one. The attacker can forward each packet using wormhole link without encoding the packet and hence some nodes will think that they are close to the attacker. This changes the complete network topology hence diminishing the system performance.

As in wireless network coding systems the routing and packet forwarding procedures are different from those in traditional wireless networks such as-
1) In traditional systems, routing is simply establishing connection between source and destination and sending information over the connection.
2) Network coding is widely known as RLNC- Random linear network coding system, in which encoding schemes are used to transfer information from source to destination.
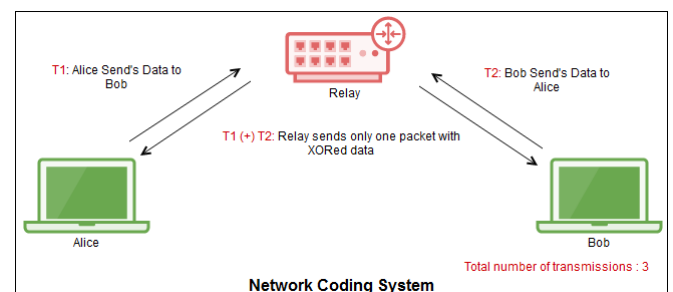
2. Difference: Traditional v/s RLNC systems

1. Traditional wireless systems
- Establishes connection between source and sink.
- Routing occurs between nodes.
- Each node in a given route acts as a switch.

Traditional Network System
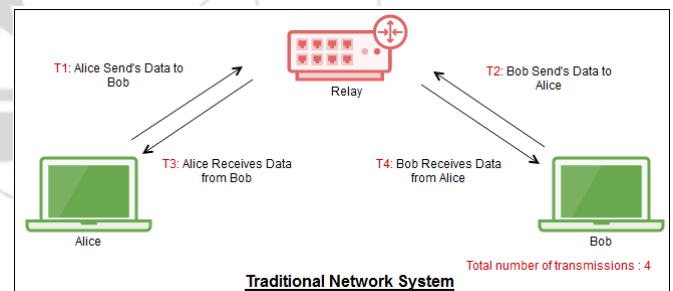
2. RLNC
- It is Random linear network coding.
- It applies coding schemes at nodes.
- It increases performance of system.

Network Coding System

Code on utilizations a restrictive calculation, Random Linear Network Coding (RLNC), to empower a scope of Network Coding applications for systems, stockpiling and portability applications. The key contrasts in the middle of RLNC and other, conventional codes are caught in the underneath table.

Paper ID: NOV161983

808

Code capabilities	RLNC	Rate-less codes	Block codes	Characteristics/ Benefits
Erasure Correction	Yes	Yes	Yes	Corrects missing or corrupted data packets
Carry code through each packet	Yes	No	No	Eliminates the tracking overhead
Distributed Operation	Yes	No	No	Enables/activates stateless management
Adding incremental Redundancy	Yes	No	No	Redundancy get added to the system whenever it is necessary
Encoding in sliding window	Yes	No	No	Flexible integration with protocols for greater efficiency

3. Literature Survey

Linear network coding - S. Li, R. Yeung, and N. Cai
In this paper [1], considered a communication network in which certain source nodes multicast information to other nodes on the network in the multihop fashion where each node can pass on any of its received data to others. They calculated how fast each node can receive the complete information, or equivalently, what the information rate arriving at each node is. Allowing a node to encode its received data before passing it on, the question involves optimization of the multicast mechanisms at the nodes. Among the simplest coding schemes is linear coding, which regards a block of data as a vector over a certain base field and allows a node to apply a linear transformation to a vector before passing it on. They formulate this multicast problem and prove that linear coding suffices to achieve the optimum, which is the max-flow from the source to each receiving node by using butterfly model.

Topological detection on wormholes in wireless ad hoc and sensor networks - D. Dong, Y. Liu, X. Li, and X. Liao
Wormhole attack is a severe threat to wireless ad hoc and sensor networks [2]. Most existing countermeasures either require specialized hardware devices or make strong assumptions on the network in order to capture the specific symptom induced by wormholes. Those requirements and assumptions limit the applicability of previous approaches. In this paper, presented the attempt to understand the impact and inevitable symptom of wormholes and develop distributed detection methods by making as few restrictions and assumptions as possible. They fundamentally analyzed the wormhole problem using a topology methodology and propose an effective distributed approach, which relies solely on network connectivity information, without any requirements on special hardware devices or any rigorous assumptions on network properties. They formally prove the correctness of this design in continuous geometric domains and extend it into discrete domains. They evaluate its performance through extensive simulations.

Opportunistic routing in multihop wireless networks - S. Biswas and R. Morris
This system describes Extremely Opportunistic Routing (ExOR), a new unicast routing technique [3] for multi-hop wireless networks. ExOR forwards each packet through a sequence of nodes, deferring the choice of each node in the sequence until after the previous node has transmitted the packet on its radio. ExOR then determines which node, of all the nodes that successfully received that transmission, is the node closest to the destination. That closest node transmits the packet. The result is that each hop moves the packet farther (or average) than the hops of the best possible pre-determined route. The ExOR design addresses the challenge of choosing a forwarding node after transmission using a distributed algorithm. First, when a node transmits a packet, it includes in the packet a simple schedule describing the priority order in which the potential receivers should forward the packet. The node computes the schedule based on shared measurements of inter-node delivery rates. ExOR then uses a distributed slotted MAC protocol for acknowledgements to ensure that the receivers agree who the highest priority receiver was. The efficacy of ExOR depends mainly on the rate at which the reception probability falls off with distance. Simulations based on measured radio characteristics suggest that ExOR reduces the total number of transmissions by nearly a factor of two over the best possible pre-determined route.

Xors in the air: practical wireless network coding - S. Katti, H. Rahul, W. Hu, D. Katabi
This system proposes COPE [4], a new architecture for wireless mesh networks. And also DCAR[5], as another method of packet forwarding, which more general case of COPE architecture.

In addition to forwarding packets, routers mix packets from different sources to increase the information content of each transmission. They show that intelligently mixing packets increases network throughput. Their design is rooted in the theory of network coding. It is explained by following example:
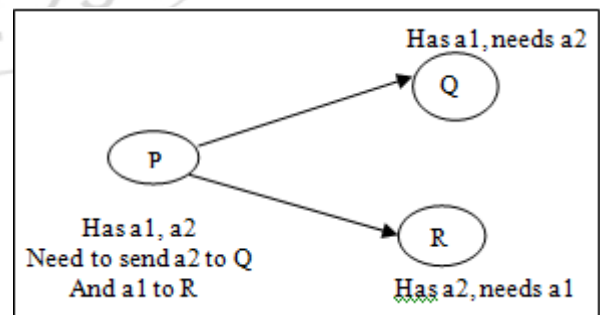

Example: Node P can broadcast a1ExOR a2 to allow Q and R to decode the packet and retrieve a2 and a1, respectively. COPE [4] applies network coding for immediate neighboring nodes. In general, node Q and R can be several hops away from P. As long as they have one of the packets, they can still decode the combined packet to retrieve the other packet. DCAR [5] considers this more general case.

Prior work on network coding is mainly theoretical and focuses on multicast traffic. This paper aims to bridge theory

with practice; it addresses the common case of unicast traffic, dynamic and potentially bursty flows, and practical issues facing the integration of network coding in the current network stack. They evaluated the design on a 20-node wireless network, and discuss the results of the first test bed deployment of wireless network coding. The results show that using COPE at the forwarding layer, without modifying routing and higher layers, increases network throughput.

4. Overview of Network coding based wireless systems

The Butterfly Network Example:
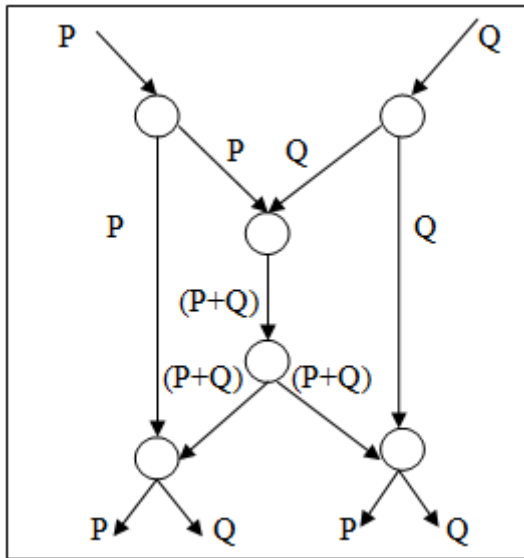
The butterfly network is often used to illustrate how linear network coding can outperform routing. Two source nodes (at the top of the picture) have information P and Q that must be transmitted to the two destination nodes (at the bottom), which each want to know both P and Q. Each edge can carry only a single value. If only routing were allowed, then the central link would be only able to carry P or Q, but not both. Suppose we send P through the center; then the left destination would receive P twice and not know Q at all. Sending Q poses a similar problem for the right destination. We say that routing is insufficient because no routing scheme can transmit both P and Q simultaneously to both destinations. Using a simple code, as shown, P and Q can be transmitted to both destinations simultaneously by sending the sum of the symbols through the center – in other words, we encode P and B using the formula "P+Q". The left destination receives P and P+Q, and can calculate Q by subtracting the two values. Similarly, the right destination will receive Q and P+Q, and will also be able to determine both P and Q.

Random linear network coding is a simple yet powerful encoding scheme, which in broadcast transmission schemes allows close to optimal throughput using a decentralized algorithm. Nodes transmit random linear combinations of the packets they receive, with coefficients chosen from a Galois field. If the field size is sufficiently large, the probability that

the receiver will obtain linearly independent combinations and therefore obtain innovative information.

In this section, we present the general frameworks for network coding systems for wireless mesh networks. There are two general approaches for applying network coding to wireless mesh networks, intra-flow network coding and inter-flow network coding. Both approaches exploit the broadcast advantage and opportunistic listening in wireless networks to reduce transmissions and improve performance. However, these benefits are realized differently: Intra-flow network coding systems mix packets within individual flows, while inter-flow network coding systems mix packets across multiple flows.

1) Intra-flow network coding:
In intra-flow network coding systems [6], packets are delivered in batches. Each node forwards linear combinations of the packets in a batch, which are referred to as coded packets. The source node continuously broadcasts linear combinations of packets from the current batch until an acknowledgment (ACK) for this batch is received from the destination, at which point the source begins transmitting the next batch of packets. It mainly includes-
- Forwarding node selection and rate assignment
- Data packet forwarding
- Acknowledgment delivery

2) Inter-flow network coding:
Inter-flow network coding abuses shrewd listening and remote show with entrepreneurial coding at middle of the nodes [7]. The key thought is that when a node has an arrangement of bundles for various streams to be conveyed to various next bounce nodes, rather than unicasting each bundle independently to its comparing next bounce node, the node consolidates the parcels together and broadcasts the consolidated parcel once for all the following bounce nodes.
In this manner, inter-flow network coding lessens various individual unicast transmissions to stand out to show as only once broadcast transmission. It includes-
- Discovery of coding opportunities
- Transmission of coded packets
- Routing integration

4.1 Challenges in Safe Design Wireless Network Coding System

In this section, we introduce potential security dangers that current system coding frameworks and the difficulties faced in tending to the security dangers. We concentrate mainly on attacks on the system coding framework that intend to disturb the information conveyance process.
- **Link quality modification:** In this the attacker node claims wrong metrics for its own adjacent links. It also modifies the original link qualities. They can be prevented by authentication like- digital signatures.
- **Packet pollution attack:** These Packet pollution attacks [7] are the most understood and most examined attacks against system coding framework. In this, the aggressor hub infuses ruined packets into the system. Since each forwarder hub consolidates got packets to frame new

coded packets, such attacks can bring about scourge impact, where the defiled packets from one influenced legitimate hub further influence other fair hubs. Accordingly, by infusing even a couple defiled packets, the aggressor can corrupt the execution essentially.

- **ACK Modification, Dropping and Delay:** These are three different attacks related to ACK. In first, ACK modification, the attacker forces a bogus or modified ACK packet to the source to move on next packet prematurely. In second, ACK Dropping, the attacker drops all the ACK packets by attacking on the ACK delivery path; it can be done using wormhole attacks. In third, ACK Delay, attacker node delays delivery of ACK packet causing high degradation in system throughput.

- **Wormholes:** These attacks can introduce fictitious links between honest nodes, and distort their perception of network topology. Although existing wormhole solutions, such as packet leashes and True Link can be applied, they typically incur substantial overhead, which can potentially destroy the performance gain of network coding. Designing a secure and efficient link state protocol is a challenging task. Still now, there is no existing solution that ensures correct link state propagation in wireless networks in the presence of colluding attackers. As in wireless network coding systems the routing and packet forwarding procedures are different from those in traditional wireless networks.

4.2 Effects of wormhole attack on network coding system as follows.

- If wormhole attacks are launched in routing, the nodes close to attackers will receive more packets than they should and be considered as having a good capability in help forwarding packets. Thus they will be assigned with more responsibility in packet forwarding than what they can actually provide.

- Furthermore, other nodes will be correspondingly contributing less. This unfair distribution of workload will result in inefficient resource utilization and reduce system performance.

- Wormhole attacks launched during the data transmission phase can also be very harmful. First, wormhole attacks can be used as the first step towards more sophisticated attacks, such as man-in-the-middle attacks and entropy attacks.

- Secondly, the attackers can periodically turn on and off the wormhole links in data transmissions, confusing the system with fake link condition changes and making it unnecessarily rerun the routing process.

5. Conclusions

Wireless Network coding systems is a wide area in which security is major challenge. In this paper, we have analyzed the difference between traditional and random linear network coding systems (RLNC) and how it is more efficient, we have investigated the negative impacts of wormhole attacks on wireless network coding systems Also types of attacks, how they are responsible for degrading the performance of the network, various techniques such as COPE and DCAR are studied to detect and prevent wormhole attack, detection is done without support of any hardware.

References

[1] S. Li, R. Yeung, and N. Cai, "Linear network coding," IEEE Transactions on Information Theory, vol. 49, no. 2, 2003.

[2] J. Eriksson, S. V. Krishnamurthy, and M. Faloutsos, "Truelink: A practical countermeasure to the wormhole attack in wireless networks," in Proc. IEEE ICNP, 2006, pp. 75–84.

[3] S. Biswas and R. Morris, "Opportunistic routing in multihop wireless networks," in ACM SIGCOMM, September 2004.

[4] S. Katti, H. Rahul, W. Hu, D. Katabi, M. M´edard, and J. Crowcroft, "Xors in the air: practical wireless network coding,"in Proc. of ACM SIGCOMM '06, 2006.

[5] J. Le, J. C. S. Lui, and D. M. Chiu, "DCAR: Distributed codingaware routing in wireless networks," in Proc. of ICDCS '08, 2008.

[6] S. Chachulski, M. Jennings, S. Katti, and D. Katabi, "Trading structure for randomness in wireless opportunistic routing," in Proc. of ACM SIGCOMM '07, 2007.

[7] Z. Yu, Y. Wei, B. Ramkumar, and Y. Guan, "An efficient signature-based scheme for securing network coding against pollution attacks," in Proceedings of INFOCOM 08, 2008.

Paper ID: NOV161983