

# Wormhole Attack Detection in Wireless Networks

## Chitra. G, Krithika. S, Monisha.K. R, P. Deivendran

Department of Information Technology, Velammal Institute of Technology, Chennai, India

### ABSTRACT

Wormhole attacks can destabilize or disable wireless sensor networks. In a typical wormhole attack, the attacker receives packets at one point in the network, forwards them through a wired or wireless link with less latency than the network links, and relays them to another point in the network. We first propose a centralized algorithm to detect wormholes and show its correctness rigorously. For the distributed wireless network, we propose DAWN, Distributed detection Algorithm against Wormhole in wireless Network coding systems, by exploring the change of the flow directions of the innovative packets caused by wormholes. We find that the robustness depends on the node density in the network, and prove a necessary condition to achieve collision-resistance. Our solutions only depend on the local information that can be obtained from regular network coding protocols, and thus the overhead that our algorithms introduce is acceptable for most applications.

**Keywords:** Wireless Networks, Random Linear Network Coding, Wormhole Attack, Expected Transmission Count.

### I. INTRODUCTION

In the efforts to improve the system performance of wireless networks, network coding has been shown to be an effective and promising approach and it constitutes a fundamentally different approach compared to traditional networks, where intermediate nodes store and forward packets as the original. In contrast, in wireless network coding systems, the forwarders are allowed to apply encoding schemes on what they receive, and thus they create and transmit new packets. The idea of mixing packets on each node takes good advantages of the opportunity diversity and broadcast nature of wireless communications, and significantly enhances system performance.

The wormhole attack is one of these attacks. In a wormhole attack, the attacker can forward each packet using wormhole links and without modifying the packet transmission by routing it to an unauthorized remote node. Hence, receiving the rebroadcast packets by the attackers, some nodes will have the illusion that they are close to the attacker. With the ability of changing network topologies and bypassing packets for further manipulation, wormhole attackers pose a severe threat to many functions in the network, such as routing and

localization. To investigate wormhole attacks in wireless network coding systems, we focus on their impact and countermeasures in a class of popular network coding schemes: the random linear network coding (RLNC) system.

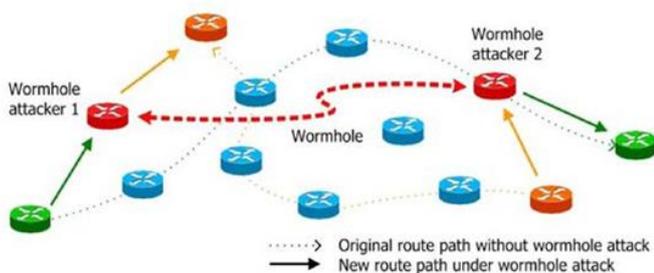
The main objective of this work is to detect and localize wormhole attacks in wireless network coding systems. The major differences in routing and packet forwarding rule out using existing countermeasures in traditional networks. In network coding systems like MORE, the connectivity in the network is described using the link loss probability value between each pair of nodes, while traditional networks use connectivity graphs with a binary relation (i.e., connected or not) on the set of nodes. For this reason, prior works based on graph analysis cannot be applied. Some other existing works rely on the packet round trip time difference introduced by wormhole attacks to detect them.

Unfortunately, this type of solutions cannot work with network coding either. They require either to use an established route that does not exist with network coding, or to calculate the delay between every two neighbouring nodes which will introduce a huge amount of error in network coding systems.

In this system, in order to best utilize resources, before data transmissions, routing decisions (i.e., how many times of transmissions a forwarder should make for each novel packet) are made based on local link conditions by some test transmissions.

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. For example, by retransmitting the packets from the wormhole links, some victim nodes will have to process much more non-innovative packets that will waste their resources; these constitute entropy attacks. Second, 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.

The main objective of this paper is to detect and localize wormhole attacks in wireless network coding systems. The major differences in routing and packet forwarding rule out using existing countermeasures in traditional networks is described using the link loss probability value between each pair of nodes, while traditional networks use connectivity .



**Figure 1:** Illustration of Wormhole attack in a Network

In this paper, we first propose a centralized algorithm to detect wormholes leveraging a central node in the network. For the distributed scenarios, we propose a distributed algorithm, DAWN, to detect wormhole attacks in wireless interflow network coding systems. The main idea of our solutions is that we examine the order of the nodes to receive the innovative packets in the network, and explore its relation with a widely used metric, expected transmission count (ETX), associated with each node. Our algorithms do not rely on any location information, global synchronization assumption or special hardware/middleware. Our solutions only

depend on the local information that can be obtained from regular network coding protocols, and thus the overhead that our algorithms introduce is acceptable for most applications.

The centralized algorithm concentrates the computation workload to the central node, and thus each normal node will suffer much less workload than DAWN. Since the transmissions between each node and the central node are unicast, the caused communication overheads of the centralized algorithm are lower than DAWN, which broadcasts the reports.

## II. METHODS AND MATERIAL

### 2. Technical Preliminaries

#### 2.1 Existing System

In existing system, the wormhole attack is one of these attacks. In a wormhole attack, the attacker can forward each packet using wormhole links and without modifies the packet transmission by routing it to an unauthorized remote node. Hence, receiving the rebroadcast packets by the attackers, some nodes will have the illusion that they are close to the attacker. With the ability of changing network topologies and bypassing packets for further manipulation, wormhole attackers pose a severe threat to many functions in the network, such as routing and localization.

#### 2.2 Proposed System

In this paper, we first propose a centralized algorithm to detect wormholes leveraging a central node in the network. For the distributed scenarios, we propose a distributed algorithm, DAWN, to detect wormhole attacks in wireless intra-flow network coding systems. The main idea of our solutions is that we examine the order of the nodes to receive the innovative packets in the network, and explore its relation with a widely used metric, Expected Transmission Count (ETX), associated with each node. Our algorithms do not rely on any location information, global synchronization assumption or special hardware/middleware. Our solutions only depend on the local information that can be obtained from regular network coding protocols, and thus the overhead that our algorithms introduce is acceptable for most applications.

## 2.3 Architecture

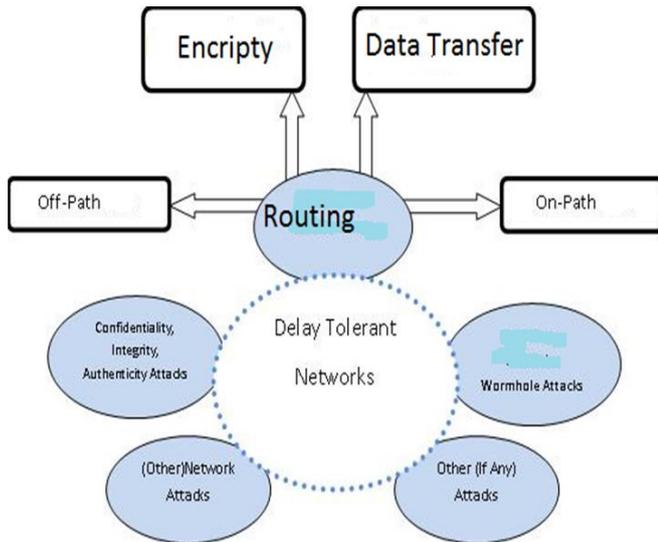


Figure 2 : Representation of Architecture

## 3. Modules:

1. Random Linear Network Coding.
2. Expected transmission count (ETX).
3. Wormhole Attack Model.

### 3.1 Modules Description

#### 3.1.1 Random Linear Network Coding

Linear Network Coding (LNC), especially Random Linear Network Coding (RLNC), owns numerous applications. Linear network coding permits each node in the network to pass on the combinations of the received data, in order to optimize the information capacity. In network coding, every node except the recipient applies a random linear mapping from the inputs to outputs over the field  $GF(2^k)$ . Each packet contains a vector in the  $m$ -dimensional code vector space  $V$ . particularly; each packet sent by the source node contains a basis of the code vector space  $V$ . If one intermediate node receives a packet which is linearly independent from previous packets, this packet is called an innovative packet. Essentially, an innovative packet must contain at least one basis that the node has not received, and the arrival of an innovative packet will increase the rank of the received packets by one. However, since the packet can derive various forms during the transmissions in network coding, when the wormhole attack is initiated, it is difficult to apply some

traditional solutions (i.e. tracing the timestamps of a particular packet) to defend. Thus, the wide applications of network coding push us to find another way to defend against wormhole attack.

#### 3.1.2 Expected Transmission Count (ETX)

ETX has extensive applications in network coding systems. The ETX of a node  $u$  in the network coding system denotes the expected total number of transmissions (including retransmissions) that the source node should make, in order to make the node  $u$  receive one innovative packet successfully. A node of high ETX means it is difficult to make it heard from the source, usually because the node is far from the source and the links between them are very lossy. Thus, the metric of the ETXs is a good representation of the network structure. The ETXs are calculated based on the probabilities of packet loss between each pair of the nodes in the network.

#### 3.1.3 Wormhole Attack Model

In wormhole attacks, the attackers between distant locations transmit packets using a Out-of-band tunnel. The transmission tunnel is called a wormhole link. The packet loss rate on the wormhole link is negligible. The kinds of the wormhole links can be various, such as an Ethernet cable, an optical link, or a secured long-range wireless transmission. When the wormhole attack is initiated, the attackers can capture data packets on either side, forward them through the wormhole link and rebroadcast them on the other node.

$$ETX(v) = \frac{1}{p(u,v)}$$

## 4. The Centralized Algorithm

In this section, we propose the centralized algorithm, which utilizes the ETX metric and the order of rank increment to detect wormhole attacks. In order to protect the validity of our method, we also introduce the public cryptographic scheme for the network. For the proposed algorithm, we not only perform the analysis of its correctness, but also discuss its technical details in this section.

## 4.1 The Centralized Algorithm

Input:  $T$  : the reports from all the nodes  $V$  in the network  
 $G$ ;  $D$ : the number of dimensions of the code vector space;  
Normal: the normal distance; Threshold: the threshold of alert

Output: whether there exists a wormhole attack in the network  $G$ ; the updated Normal

- 1: Randomly select a rank  $r$  s.t.  $r \geq 1$  and  $r$  should be small enough, i.e.,  $1 \leq r \leq 5$ .
- 2: Let  $T_r$  be the set of the reports whose rank increments are from  $r - 1$  to  $r$ .
- 3: Sort  $T_r$  into a sequence  $T_r^e$  s.t. the values of ETX in  $T_r^e$  are ascending.
- 4: Let  $L_e$  be the sequence of ascending ETXs in  $T_r$
- 5: Sort  $T_r$  into a sequence  $T_r^e$  s.t. the values of time in  $T_r$  are ascending.
- 6: Let  $L_e$  be the sequence of ETXs in  $T_r^e$  while preserving the order.
- 7: Distance  $\leftarrow$  CALCULATE-DISTANCE( $L_e, L_t, |V|$ )
- 8: if Distance - Normal > Threshold then
- 9: Find out the addresses of the nodes with the most aberrant ETXs.
- 10: Release a warning of wormhole attack.
- 11: end if
- 12: Update the value of Normal using k-means

## 5. The Distributed Detection Algorithm

In this section, we consider a practical scenario where centralized authority cannot be found. We propose DAWN, a distributed algorithm to detect wormhole attacks in wireless network coding systems. We will perform rigorous analysis on the detection rate of our algorithm and its resistance against collusions one with lower ETX is supposed to receive novel packets earlier than the other one with high probabilities. In other words, innovative packets are transmitted from low ETX nodes to high ETX nodes with high probabilities.

### 5.1 Algorithm:

The distributed detection algorithm for wormholes in wireless network coding systems (dawn) on node  $U$

Input:  $R$ : the set of reports recognized in the last batch;  
 $N(u)$ : the set of  $u$ 's neighbors;  $s_j$ : the local observation result of each neighbor  $j \in N(u)$ ;  $\delta$ : the threshold.  
Output: Detected wormhole attacker in  $N(u)$ , if any.

- 1: for Each report  $r(i; j; k) \in R$  do
- 2: if  $ETX(j) - ETX(i) \leq \delta$  OR  $i \in N(j)$  then
- 3: Discard this report;
- 4: else
- 5: if  $j \in N(u)$  then
- 6:  $s_j \leftarrow s_j + 1$ ;
- 7: end if
- 8: if  $k < 2$  then
- 9: Forward this report  $r(i; j; k + 1)$ ;
- 10: end if
- 11: end if
- 12: end for
- 13: for each  $v \in N(u)$  do
- 14: Let  $C(v) = \{i | i \in N(v) \text{ s.t. } ETX(v) - ETX(i) > \delta\}$
- 15: if  $s_v \geq \lceil (C(v) + 1) / 2 \rceil$  then
- 16: Mark  $v$  as a detected wormhole attacker, and block any traffic from or to node  $v$  in future batches.
- 17: end if
- 18: end for

## 6. Input Design

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

- What data should be given as input?
- How the data should be arranged or coded?
- The dialog to guide the operating personnel in providing input.
- Methods for preparing input validations and steps to follow when error occur.

### III. RESULTS AND DISCUSSION

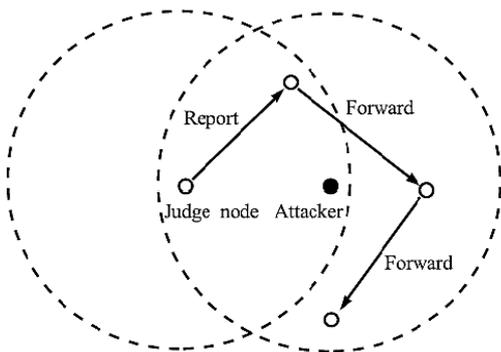
#### A. Output Design

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.
2. Select methods for presenting information.
3. Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.

- ❖ Convey information about past activities, current status or projections of the
- ❖ Future.
- ❖ Signal important events, opportunities, problems, or warnings.
- ❖ Trigger an action.
- ❖ Confirm an action.



**Figure 3.** Illustration of Report Forwarding

#### B. System Study

##### Feasibility Study

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are

- ◆ Economical Feasibility
- ◆ Technical Feasibility
- ◆ Social Feasibility

##### a) Economical Feasibility

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

##### b) Technical Feasibility

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

##### c) Social Feasibility

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of

training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

#### IV. CONCLUSION

In this paper, we have investigated the negative impacts of wormhole attacks on wireless network coding systems. We have proposed two algorithms that utilize the metric ETX to defend against wormhole attacks. We have proposed a Centralized Algorithm that assigns a central node to collect and analyze the forwarding behaviors of each node in the network, in order to react timely when wormhole attack is initiated. We have proven the correctness of the Centralized Algorithm by deriving a lower bound of the deviation in the algorithm. We have also proposed a Distributed detection Algorithm against Wormhole in Wireless Network coding systems, DAWN. In DAWN, during regular data transmissions, each node records the abnormal arrival of innovative packets and share this information with its neighbors. This algorithm is efficient and practical without strong assumptions. Furthermore, we theoretically prove that DAWN guarantees a good lower bound of successful detection rate.

#### V. REFERENCES

- [1] S. Li, R. Yeung, and N. Cai, "Linear network coding," *IEEE Trans. Inf. Theory*, vol. 49, no. 2, pp. 371–381, Feb. 2003.
- [2] T. Ho, M. Medard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," *IEEE Trans. Inf. Theory*, vol. 52, no. 10, pp. 4413–4430, Oct. 2006.
- [3] S. Biswas and R. Morris, "Opportunistic routing in multihop wireless networks," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 34, pp. 69–74, Sep. 2004.
- [4] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Medard, and J. Crowcroft, "XORs in the air: Practical wireless network coding," in *Proc. Conf. Appl., Technol., Archit. Protocols Comput. Commun.*, 2006, pp. 243–254.
- [5] S. Chachulski, M. Jennings, S. Katti, and D. Katabi, "Trading structure for randomness in wireless opportunistic routing," in *Proc. Conf. Appl., Technol., Archit. Protocols Comput. Commun.*, Aug. 2007, pp. 169–180.
- [6] D. Dong, Y. Liu, X. Li, and X. Liao, "Topological detection on wormholes in wireless ad hoc and sensor networks," *IEEE Trans. Netw.*, vol. 19, no. 6, pp. 1787–1796, Dec. 2011.
- [7] J. Kim, D. Sterne, R. Hardy, R. K. Thomas, and L. Tong, "Timingbased localization of in-band wormhole tunnels in MANETs," in *Proc. 3rd ACM Conf. Wireless Netw. Security*, 2010, pp. 1–12.
- [8] S. R. D. R. Maheshwari, J. Gao, "Detecting wormhole attacks in wireless networks using connectivity information," in *Proc. IEEE 26th Int. Conf Commun.*, 2007, pp. 107–115.
- [9] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Wormhole attacks in wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 370–380, Feb. 2006.
- [10] R. Poovendran and L. Lazos, "A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks," *Wireless Netw.*, vol. 13, no. 1, pp. 27–59, 2007.
- [11] A. J. Newell, R. Curtmola, and C. Nita-Rotaru, "Entropy attacks and countermeasures in wireless network coding," in *Proc. 5th ACM Conf. Security Privacy Wireless Mobile Netw.*, 2012, pp. 185–196.
- [12] W. Wang, B. Bhargava, Y. Lu, and X. Wu, "Defending against wormhole attacks in mobile ad hoc networks: Research articles," *Wireless Commun. Mobile Comput.*, vol. 6, no. 4, pp. 483–503, Jun. 2006.
- [13] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: A defense against wormhole attacks in wireless networks," in *Proc. IEEE 23rd Annu. Joint Conf. IEEE Comput. Commun.*, Mar. 2003, pp. 1976–1986.
- [14] W. Wang and B. Bhargava, "Visualization of wormholes in sensor networks," in *Proc. 3rd ACM*

- Workshop Wireless Security, Oct. 2004, pp. 51–60.
- [15] J. Eriksson, S. Krishnamurthy, and M. Faloutsos, “Truelink: A practical countermeasure to the wormhole attack in wireless networks,” in Proc. IEEE Int. Conf. Netw. Protocols, 2006, pp. 75–84.
- [16] S. \_Capkun, L. Butty\_an, and J.-P. Hubaux, “Sector: Secure tracking of node encounters in multi-hop wireless networks,” in Proc. 1st ACM Workshop Security Ad Hoc Sensor Netw., 2003, pp. 21–32.
- [17] D. S. J. D. Couto, D. Aguayo, J. Bicket, and R. Morris, “A highthroughput path metric for multi-hop wireless routing,” *Wireless Netw.*, vol. 11, no. 4, pp. 419–434, 2005.
- [18] A. G. Dimakis, P. B. Godfrey, Y. Wu, M. J. Wainwright, and K. Ramchandran, “Network coding for distributed storage systems,” *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4539–4551, Sep. 2010.
- [19] A. S. Avestimehr, S. N. Diggavi, and D. N. Tse, “Wireless network information flow: A deterministic approach,” *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 1872–1905, Apr. 2011.
- [20] B. Nazer and M. Gastpar, “Compute-and-forward: Harnessing interference through structured codes,” *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6463–6486, Oct. 2011.
- [21] P. Santi, “Topology control in wireless ad hoc and sensor networks,” *ACM Comput. Surv.*, vol. 37, no. 2, pp. 164–194, 2005.
- [22] F. Wu, T. Chen, S. Zhong, L. E. Li, and Y. R. Yang, “Incentive-compatible opportunistic routing for wireless networks,” in Proc. 14th ACM Int. Conf. Mobile Comput. Netw., 2008, pp. 303–314.
- [23] S. Lloyd, “Least squares quantization in PCM,” *IEEE Trans. Inf. Theory*, vol. IT-28, no. 2, pp. 129–137, Mar. 1982.
- [24] C. Cortes and V. Vapnik, “Support vector machine,” *Mach. Learn.*, vol. 20, no. 3, pp. 273–297, 1995.
- [25] W. Hoeffding, “Probability inequalities for sums of bounded random variables,” *J. Amer. Statist. Assoc.*, vol. 58, no. 301, pp. 13–30, 1963.
- [26] Beecrypt [Online]. Available: <http://sourceforge.net/projects/beecrypt.com>