IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 6, June 2016
ISSN (Online) 2348 – 7968 | Impact Factor (2015) - 4.332
www.ijiset.com

# Efficient Detection of Wormhole Attacks Using ETX Algorithm in Wireless Network Coding Systems

**Kashibai G Biradar[1], Deepak N Biradar[2]**

[1]PG Student, Department of Computer Science and Engineering,
[2]Assistant Professor, Department of Computer Science and Engineering,
Lingaraj Appa Engineering College, Bidar, Karnataka State, India.
adarsh.uttarkar7@gmail.com

***Abstract*— The wireless network coding system is an efficient method to improve the performance of a wireless network. These systems have become more popular among the wireless networks. But this system also faces serious threats in the form of Wormhole attack. The wormhole attack degrades the performance of the network coding systems. In order to overcome this problem various methods have been presented. For networks with centralized authority, a centralized algorithm is used. In this algorithm, a central node gathers the information from all the nodes in the network and evaluate whether there present a wormhole link. This algorithm ranks the series of the nodes that gains the innovative packet, and uses the machine learning method to differentiate the wormhole cases. For distributed method DAWN, a Distributed detection Algorithm against Wormhole in wireless Network coding systems is used. In DAWN, during proper data transmissions, each node reports the irregular appearance of innovative packets and shares this with its neighbours. Moreover, DAWN assure a good successful detection rate. This existing method is more energy saving and hence decrease the implementation and communication costs.**

***Keywords*— *WSN, DAWN, Wormhole attack, ETX, Certificate authority*.**

## 1. INTRODUCTION

In the efforts to improve the system performance of wireless networks, network coding has been shown be an effective and promising approach and it constitutes a fundamentally different approach com- pared to traditional networks, where intermediate nodes store and forward packets as the original. In contrast, in wire- less 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 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 To investigate wormhole attacks in wireless network coding systems, we focus on their impact and countermeasures in a class of popular network coding scheme 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 .

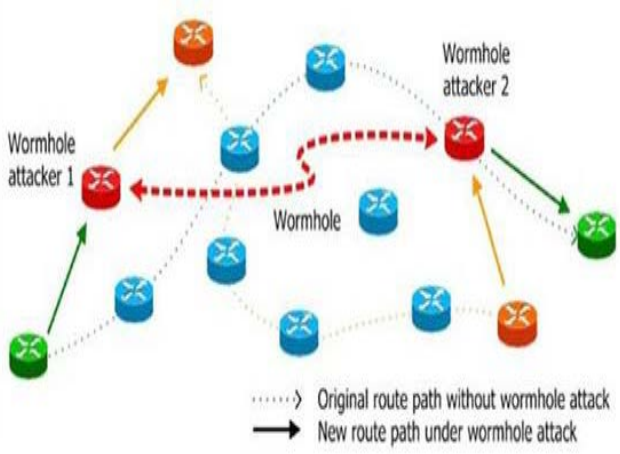


Fig.1: Illustration of Wormhole attack in a Network

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.

## 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.

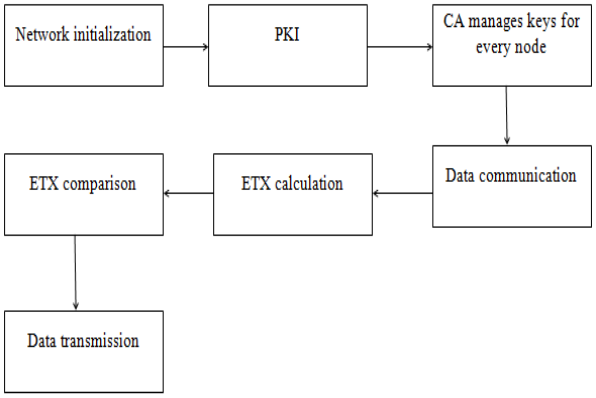


Fig. 2 Block diagram of Proposed System

## 3. 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 (2k). 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.

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

## 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 ≥ 1 and r should be small enough, i.e., 1 ≤ r ≤ 5.
2: Let Tr be the set of the reports whose rank increments are from r − 1 to r.
3: Sort Tr into a sequence Tre s.t. the values of ETX in Tre are ascending.
4: Let Le be the sequence of ascending ETXs in Tr
5: Sort Tr into a sequenceTre s.t. the values of time in Tr are ascending.
6: Let Le be the sequence of ETXs in Tre while preserving the order.
7: Distance ← CALCULATE-DISTANCE(Le,Lt, |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; sj: the local observation result of each neighbor j ∈ N (u); δ: the threshold. Output: Detected wormhole attacker in N (u), if any.

1: for Each report r(i; j; k) ∈ R do
2: if ETX(j) − ETX(i) ≤δ OR i =∈ N(j) then
3: Discard this report;
4: else
5: if j ∈ N(u) then
6: sj ← sj + 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 ∈ N(u) do
14: Let C(v)={i |i ∈ N(v) s.t. ETX(v) − ETX(i) >δ}
15: if sv ≥ ⌜ ( C(v) +1)/2⌝ 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

### 5.2 IMPLEMENTATION OF DAWN APPROACH

In this module, the forwarder nodes are selected based on Expected Transmission Count value. The ETX of a node 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 loss. DAWN uses public key infrastructure (PKI) is in place to implement the public key cryptographic techniques. The identity and the public key of each user are managed by the certificate authority (CA), which is a trusted entity.

## 6. RESULTS

After implementing the proposed system on NS2 platform, the results obtained are as follows:

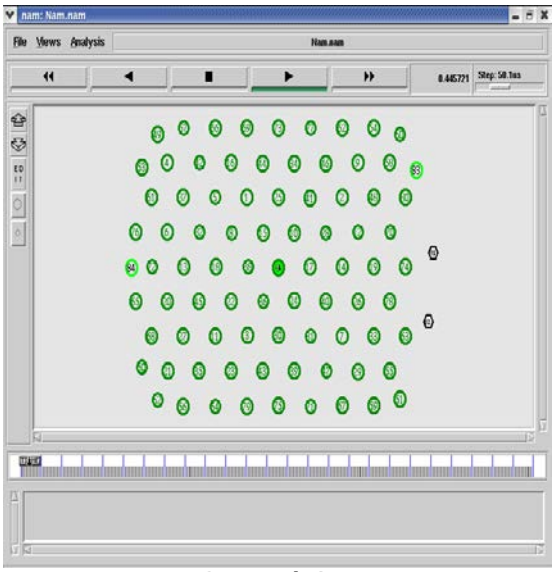


Fig. 3 Network Creation

In figure 3 the network is going to be created. Mainly it defines the topology of the system.

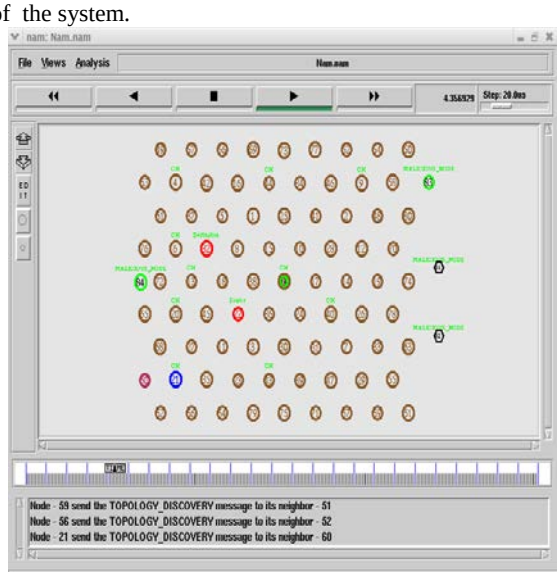


Fig. 4 Network Configuration

In figure 4 the network is going to configured, that is nodes are identified as source node, destination node and also the network is divided into different clusters.
The figure also shows the presence of malicious nodes, which are going to attack the network and going to disturb the communication.

The figure 5 shows the operation where malicious nodes are attacking the path and distrubing the communication of nodes and the proposed approach going to select an alternate path and going to continue the communication.

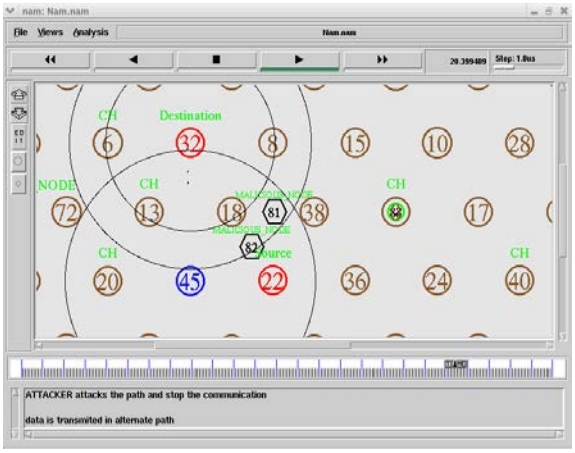


Fig. 5 Alternate path selection stage

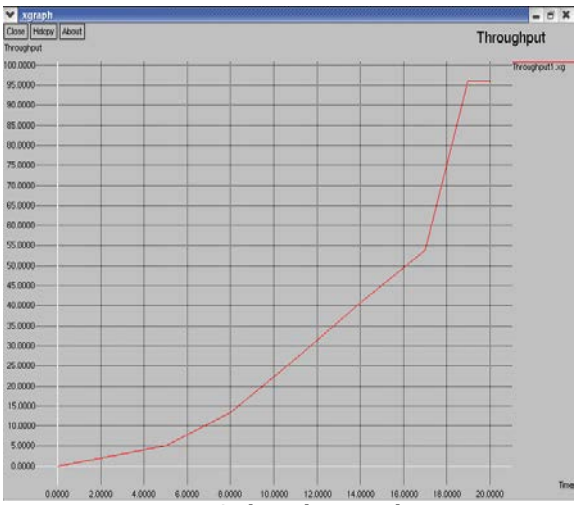


Fig. 6 Throughput graph

Figure 6 shows performance of proposed system by drawing throughput parameter using Xgraph function.

## 7. 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 net-

work, 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 detec- tion 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.

## 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. Buttyan, 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.