ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

Providing Immunity against Wormhole Attack in Wireless Network Coding System

Irin Sherly.S, Dhanalakshmi.G

Assistant Professor, Dept. of I.T., Panimalar Institute of Technology, Chennai, India

Assistant Professor Grade -I, Dept. of I.T., Panimalar Institute of Technology, Chennai, India

ABSTRACT: To improve the system performance of wireless Network, network coding is shown to be effective approach and it is totally different from traditional network. 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 .So, other nodes will be correspondingly contributing less. This unfair distribution of workload will result in inefficient resource utilization and reduce system performance. Here we detect and thus defend wormhole attack using Expected Transmission count technique, a centralized algorithm and DAWN algorithm. For data transfer we use Random linear Network coding (RLNC) System.

KEYWORDS*:* DAWN algorithm; RLNC system; Expected Transmission count

I. INTRODUCTION

When improving the 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 senders 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. 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 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.

II. RELATED WORK

Since in wireless network coding systems the routing and packet forwarding procedures are different from those will the wormhole attack cause a serious interruptions to network functions and downgrade system performance? Actually no matter what procedures are used, wormhole attacks severely imperil network coding protocols. In particular, 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 an 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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

The main aim of this paper is to detect and locate 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, traditional networks use connectivity graphs. But earlier 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. But this type of solutions cannot work with network coding systems. They require either to use an established route that does not exist with network coding, or to calculate the delay between every two neighboring nodes which will introduce a huge amount of error in network coding systems.

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 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. Different wireless networks have different characteristics and requirements. Some wireless networks have central controller, while others are highly distributed without any centralized authority. It is desirable to apply different solutions based on the network types. Our centralized algorithm is inspired by the fact that the wormhole link can significantly change the network topology, which can be measured by ETX.This idea is also heuristic to our distributed solution DAWN,which emphasizes on the scenario where no central administration node exists. Thus, our algorithms can address different scenarios. We first present the centralized solution and then discuss the distributed one, for a clear logic flow. On the other hand, compared with our distributed algorithm DAWN,our centralized algorithm also owns several advantages. 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. The centralized algorithm leverages the global information of the flows, and thus it can detect the wormhole link efficiently,and the resulted warnings can be delivered to each node more quickly than DAWN.

III. PROPOSED 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 each forwarding node in RLNC network, receiving the innovative packet will cause the rank of the previously received packets increase by one. We also find that the nodes with lower ETXs will be more likely to receive innovative packets (i.e., increase the rank) earlier than other nodes. On the other hand, wormhole links will make some nodes receive innovative packets (i.e., increase the rank) much earlier that they should. Thus, in the proposed centralized algorithm, we explore the order of rank increments in order to detect the wormhole links. Basically, in RLNC, when an innovative packet is sent from the source node, the nodes near the source node are more likely to receive the innovative packets earlier than the nodes that are far from the source node. Thus, the nodes with low ETXs can probably receive the innovative packets earlier. However, the existence of wormhole link intuitively changes the normal network topology since the innovative packets can be transmitted through the wormhole link directly and safely, and thus the nodes around the remote side of the wormhole link can receive the novel packets earlier than expected.

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 net-work 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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

4: Let L_e be the sequence of ascending ETXs in T_r^e.
5: Sort T_r into a sequence T_r^t s.t. the values of time in T_r^t are ascending.
6: Let L_t be the sequence of ETXs in T_r^t while preserving the order.
7: *Distance* ← 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.

CALCULATE-DISTANCE
Input: L_1; L_2: two lists; n: the number of nodes
Output: the distance between L_1 and L_2
1: Set up two n-dimensional vectors X and Y .
2: $d \leftarrow 0$
3: for i from 1 to n do
4: $d \leftarrow d + (L_1[i] - L_2[i])^2$
5: end for
6: return d

2.THE DISTRIBUTED DETECTION ALGORITHM

In this section, we consider a scenario where a central authority cannot be found. We propose a distributed algorithm to detect wormhole attacks in wireless network coding systems.
The basic idea of DAWN is that any two nodes in the neighborhood, the 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. In particular, DAWN has two phases on each node: 1) *Report* packets direction observation results to its neighbors and 2) *Detect* whether any attackers exist .The *Detect* phase is based on the received results from neighbors during the *Report* phase.

1. Random Linear Network Coding (RLNC)

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, inorder to optimize the information capacity. Let *r*1*; r*2;.. *; rn* denote the received data and the *s* will be the encoded data to be passed to the another node. We obtain the combination *f* based on received data based on Equation (1).

$$s = f(r1; r2.... ; rn) \quad (1)$$

For RLNC, *f* in Equation (1) is a random linear combination
in the field $GF(2k)$.

$$f(r1; r2; ...; rn) = \sum_{I=1}^{N} E_I R_I \quad (2)$$

Here, *i* is a randomly generated coefficient. 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. When the destination receives m innovative packets, whose vectors are linearly independent from each other, it can restore the source information S based on the received data R.

$$S = C-1R \quad (3)$$

Here C is the matrix of the coefficients of the received packets. Since each received packet is essentially a linear Combination of the original packets from the source, we can perfectly restore the original messages by multiplying the inverse of C.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

2. Expected transmission count (ETX)

ETX has extensive applications in network coding systems. In this paper, 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 in success. 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. In existing works the ETXs are calculated based on the probabilities of packet loss between each pair of the nodes in the network. Let *u* and *v* be two nodes, and *p*(*u v*) be the probability of successful transmissions between node *u* and *v*. For simplest case, if the network only has a sender *u* and a recipient *v*, then the ETX of the sender *u* is 1.0, and the ETX of *v* is shown as Equation (4).

$$ETX(v) = \frac{1}{p(u\ v)} \quad (4)$$

The probability *p*(*u; v*) can be estimated based on the previous transmission record, using some statistical models like weighted means and window-based observation[5]. Based on (4), if the link between the nodes is very lossy, the ETX of *v* can be very high, indicating that it is difficult to deliver messages through the link.

Algorithm to Determine ETX:
Input: the entire network *G* with nodes *V* and their locations *L*, and the source node *vs* Output: the ETXs for all the nodes in the network *G*
Output: ETXs for all the nodes in network *G*
1: $ETX(vs) \leftarrow 1{:}0$
2: for each node *vi* in *V* , except *vs* do
3: $ETX(vi) \leftarrow +\infty$
4: end for
5: repeat
6: *ETX*updated ← false
7: for each node *vi* in network *G*, than *vs* do
8: Let *N* be the set of the neighbors of *vi* s.t.
$ETX(vk) < +\infty$ for any $vk \in$
9: if $ETX(vi) < \frac{1}{1-\pi_{v1 \in N} \frac{1}{ETX(v1)}(1-P(v1-v2))}$ then
10: $ETX(vi) \leftarrow \frac{1}{1-\pi_{v1 \in N} \frac{1}{ETX(v1)}(1-P(v1-v2))}$
11: *ETXupdated* ← true
12: end if
13: end for
14: until *ETXupdated* = false
15: return the ETXs for all the nodes

IV. SIMULATION RESULTS

The proposed energy efficient algorithm is implemented with Network Simulator. We have a RLNC simulation and Figuress demonstrate the orders of rank increments with and without wormhole link. Here we have 100 nodes in the network, and we run Algorithm to calculate the ETXs. In the figures, the red curve denotes the ascending ETXs of the nodes. Then we start the network coding transmission. The source node sends out an innovative packet, and for each node, receiving the innovative packet will result in rank increment from 0 to 1. We collect the time stamps of rank increments on the nodes during the whole transmission, and find out the time order of rank increments. That is the blue line, which denotes the ETXs of the nodes based on the ascending time order of rank increments. We find that the blue line deviates from the red line when the wormhole link exists. For the centralized algorithm, we set up a central node, which owns the authority to gather information from all the nodes in the network, and we run a wormhole detection

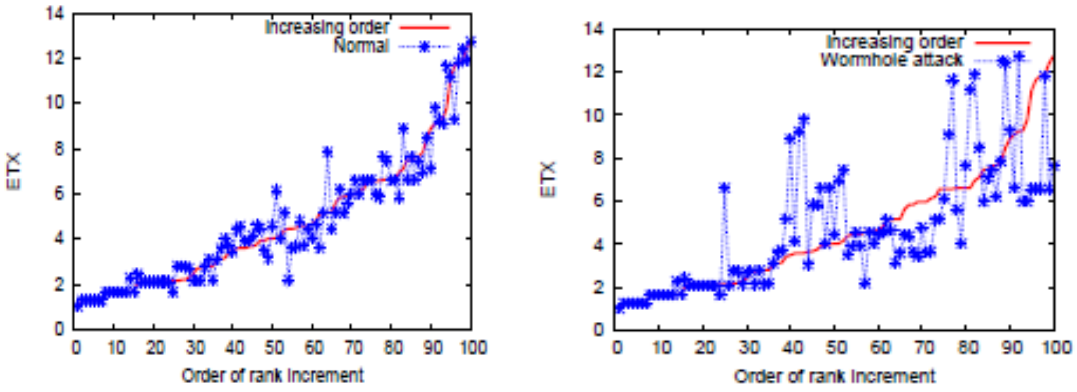
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

algorithm based on the rank increasing information on the central node. Each node is responsible to record the time when the rank of the received packets increases and then generates a report, which includes the details such as the time, the node address, and the rank. Each node delivers the reports to the central node via common unicast. At last, we update the bound of the distance for the next detection, in order to make our algorithm adaptive.



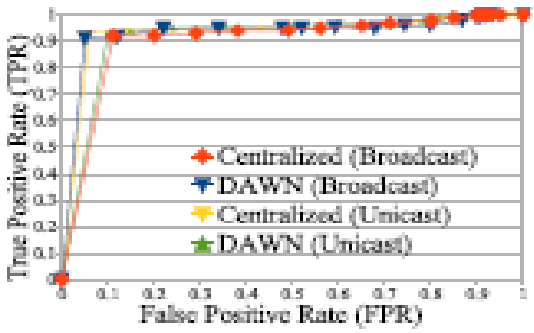


Fig: The ROC diagram of Centralized Algorithm and DAWN

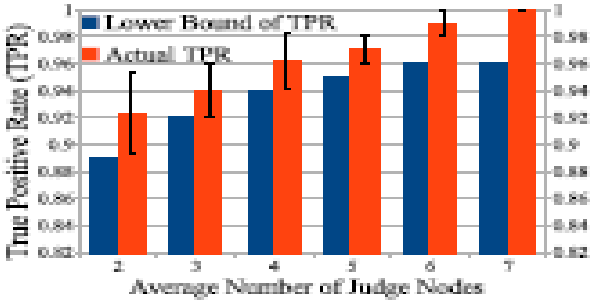


Fig: The TPR increases as the number

V. CONCLUSION AND FUTURE WORK

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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

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. DAWN is totally distributed for the nodes in the network, eliminating the limitation of tightly synchronized clock. DAWN is efficient and thus it fits for wireless sensor network. For both centralized and distributed algorithms, we have utilized the digital signatures to ensure every report is undeniable and cannot be forged by any attackers. The simulations have shown that the proposed algorithms can detect the malicious nodes participating in wormhole attack with high successful rate and the algorithm is efficient in terms of computation and communication overhead. As the performance of the proposed algorithm is analyzed in future with some modifications in design considerations the performance of the proposed algorithm can be compared with other energy efficient algorithm.

REFERENCES

1. S. Li, R. Yeung, and N. Cai, "Linear network coding," *IEEE Transactionson Information Theory*, vol. 49, no. 2, 2003.
2. T. Ho, M. Medard, R. Koetter, D. R. Karger, M. Effros, J. Shi, andB. Leong, "A random linear network coding approach to multicast,"*IEEE Transactions on Information Theory*, vol. 52, no. 10, 2006.
3. S. Biswas and R. Morris, "Opportunistic routing in multihop wirelessnetworks," in *ACM SIGCOMM*, September 2004.
4. S. Katti, H. Rahul, W. Hu, D. Katabi, M. Medard, and J. Crowcroft,"Xors in the air: practical wireless network coding," in *ACM SIGCOMM*,September 2006.
5. S. Chachulski, M. Jennings, S. Katti, and D. Katabi, "Trading structurefor randomness in wireless opportunistic routing," in *SIGCOMM*, August2007.
6. D. Dong, Y. Liu, X. Li, and X. Liao, "Topological detection onwormholes in wireless ad hoc and sensor networks," *IEEE Transactions on Networking*, vol. 19, 2011.
7. Y.-C. Hu, A. Perrig, and D. B. Johnson, "Wormhole attacks in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 24,no. 2, 2006.
8. R. Poovendran and L. Lazos, "A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks," *Wireless Network*,vol. 13, no. 1, 2007.

BIOGRAPHY

Irin Sherly.S is a Assistant Professor in the Information Technology Department, Panimalar Institute of Technology, Chennai. She received Master of Engineering degree in Computer Science in 2007 from affiliated college of Anna University, Chennai, India. She had around 8 years of teaching experience and presented many papers in National and International conferences. Her research interests are Computer Networks (wireless Networks), Cloud Computing,Network Security etc.

Dhanalakshmi.G is a Assistant Professor Grade-I in the Information Technology Department, Panimalar Institute of Technology, Chennai. She had around 12 years of teaching experience and presented many papers in National and International conferences. Her research interests are Computer Networks , Cloud Computing etc.