Modified Approach to Detect Wormhole Attack in Wireless Network Coding Systems

[1]Amruta Zanwar, [2]Smita Ponde

[1]PG 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. But Practically if we see there are numerous security concerns which hinder its wide sending. Other than the very much contemplated black-hole attacks, pollution attacks, there is another serious risk of wormhole attacks. Wormhole 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. . 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 associated with each node. In this paper we analyzed Distributed Detection algorithm to detect wormhole attack in wireless network coding which is a modified one. It considers the energy factor of the node. Energy of node is the capacity of sending and receiving number of packets in the network.

Index Terms **– Wireless Network coding, Expected Transmission Count, Modified Distributed Approach.**

I. INTRODUCTION

In the area of wireless networks lots of efforts are taking place to improve the system performance, 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 [1], [2]. 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. However, practical wireless network coding systems face new challenges and attacks, whose impact and countermeasures are still not well understood because their underlying characteristics are different from well-studied traditional wireless networks. 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 [3], [4], [5] and bypassing packets for further manipulation, wormhole attackers pose a severe threat to many functions in the network, such as routing and localization. The main objective of this project is to detect and localize wormhole attacks in wireless network coding systems. Different wireless networks have different characteristics and requirements. Some wireless networks have central controller, while others are highly distributed without any centralized authority. 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. In this algorithm decentralized that is distributed method is followed where one new factor energy of node is also considered. Trust and willingness of node is considered for sending packets from one node to another which is a very secure one, it gives a proper way of sending packets by detecting wormhole attack.

II. RELATED WORK

Some of routing protocols and other methods of detecting wormhole attack are discussed. Linear Network coding [1] and wireless network are two different networking areas in which this attack can occur. Recent years have experienced an explosion of the wormhole attack and its countermeasures. Besides, the parameters that are considered till date, in network coding systems to study the performance

of the network are varying time to time[2], [3], the results of the performance of the network has been shown in the graphical format.

Shuo-Yen Robert Li, Ning Cai [1], in this paper they have used communication network in which certain source nodes multicast information to other nodes on the network in the multihop fashion where every node can pass on any of its received data to others. 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.

Achuthan P. aramanathan, Ulrik W. Rasmussen [3], they have proposed an energy model and energy measurements for network coding enabled wireless meshed networks based on IEEE 802.11 technology. The energy model and the energy measurement testbed is limited to a simple Alice and Bob scenario. For this toy scenario they compare the energy usages for a system with and without network coding support. For high load scenarios we see that the energy consumption for with network coding is slightly higher due to the computational power it requires, but as the throughput increases with network coding, the energy per bit ratio is improving so that the gain per Joule is higher.

Zhiwei Li, Di Pu [4], the author has proposed detection of wormhole attacks with physical layer network coding that is a new mechanism based on physical layer network coding to detect wormhole attacks. When two signal sequences collide at the receiver, the starting point of the collision is determined by the distances between the receiver and the senders. Therefore, by comparing the starting points of the collisions at two receivers, we can estimate the distance between them and detect fake neighbour connections via wormholes.

Jinsub Kim, Dan Sterne [6], proposed the problem of localizing in-band wormhole tunnels in MANETs is considered. In an in-band wormhole attack, colluding attackers use a covert tunnel to create the illusion that two remote network regions are directly connected. This apparent shortcut in the topology attracts traffic which the attackers can then control. They begins with binary hypothesis testing, which tests whether a suspected path is carrying tunnelled traffic.

Lijun Qian, Ning Song [8], proposed the effects of routing attacks on multi-path routing have not been addressed. In this paper, the performance of multi-path routing under wormhole attack is studied in detail. The results show that multi-path routing is vulnerable to wormhole attacks. There are different types of wormholes, wormhole attacks can be recognized

1) Open wormhole attack
2) Half Open wormhole attack
3) Closed wormhole attack

The application of multi-path routing (MR) reduces the damages of unreliable wireless links and the constantly changing network topology. This inefficiency can be avoided by having multiple paths available and a new route discovery is needed only when all paths break and the categories given as above.

III. SYSTEM ARCHITECTURE

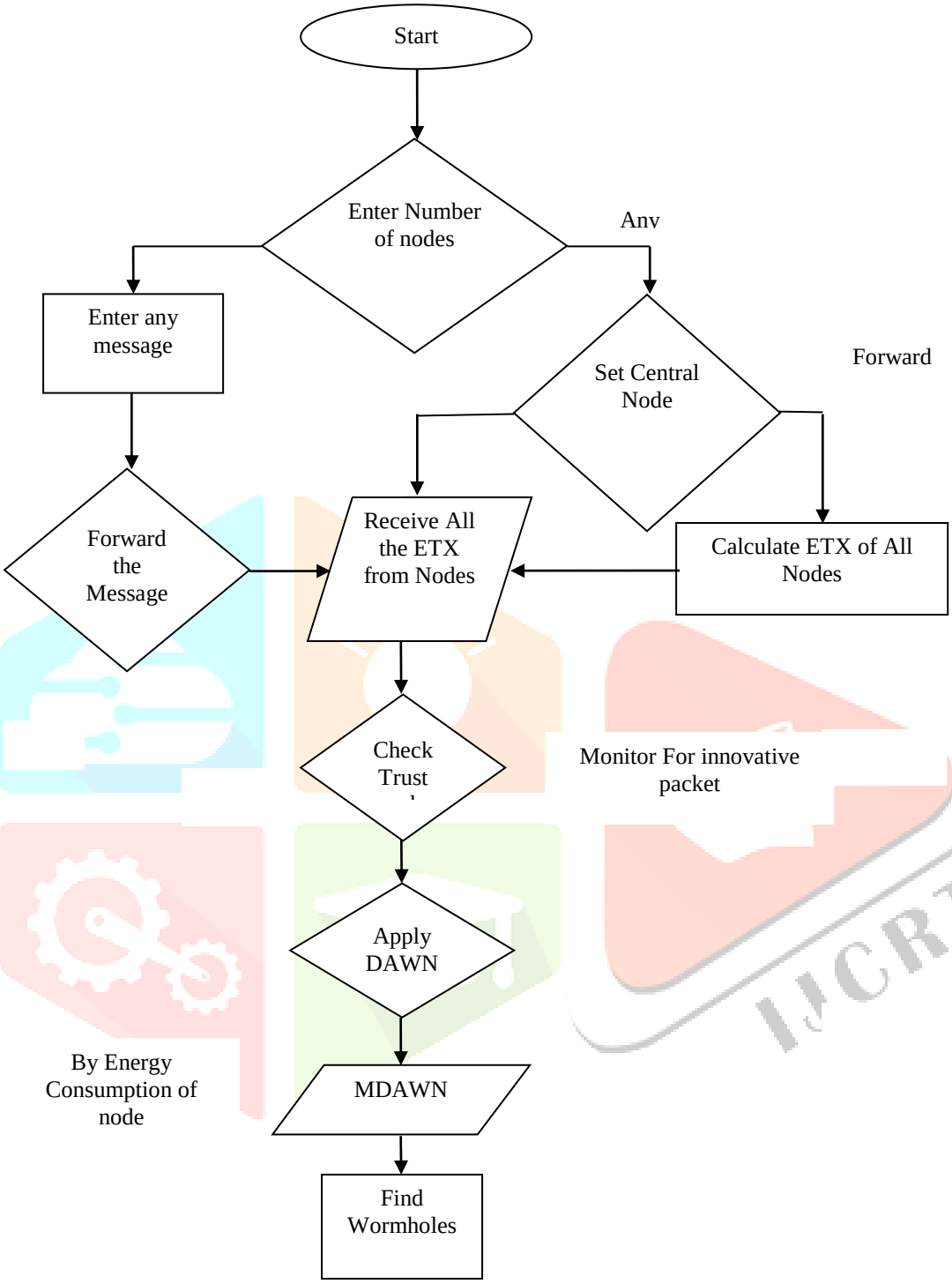


Figure 1: System Flow Diagram

Steps to detect Wormhole Attack

Step 1: Enter number of nodes and any random message. You can enter as many number of nodes as you wish.

Step 2: Apply centralized algorithm to calculate distance between nodes.

Step 3: Distributed approach is further used which gives more precise distances by considering X and y locations of nodes.

Step 4: It is a final step which is modified distributed approach in which trust parameter of node is considered to calculate distances.

Step 5: If any wormhole, it is detected.

Network Model:

In this model, we consider a wireless network with a set of consistent nodes operating network coding protocols. Nodes are coupled via lossy wireless links. For any two pair of nodes say u and v in the network such that the fortunate transmission rate between u and v, p (u, v) > 0, then we say u and v are neighbors. We imagine that ETXs are computed to specify the network topology, and are measured regularly to guide routing functions. Each node receives its own ETXs and its neighbors' ETXs. In the wireless network systems, we imagine that trust of node is calculated by considering the energy consumption of that node. For the wireless network, we mark all individual nodes as a user who has a pair of public and private keys. The identity and the public key of each user are maintained by the certificate authority (CA), which is a trusted party. If node A needs to securely communicate with node B, A has to demand B's public key from the CA. After the transmission, node B has to demand A's public key from the CA in order to check the message from A. CA is also constrained to pre distribute and call back the key pairs of the nodes. We also further apply DAWN distributed algorithm for wireless network coding system by calculating distances between nodes which can assure that no node can fake records from other nodes.

Detection of Wormhole Attack:

In the wormhole attacks, the attackers between different places send packets using a out-of-band channel. This transmission channel is called a wormhole link. The packet loss ratio on the wormhole link is small. The type of the wormhole links can be varying, such as an Ethernet cable, an optical link, or a secured long-range wireless transmission. When the wormhole attack is triggered, the attackers can catch data packets on both sides, transmit them through the wormhole link and rebroadcast them on the other node. Wormhole attack can have huge impact on wireless network coding systems. Based on different launching time, wormhole attacks can heavily degrade the system performance and can cause each independent node to deal with many non-innovative packets and ruin their resources.

Role of Central Node:

In this method, we use a centralized algorithm for detecting the wormhole link. For the centralized algorithm, we maintain a central node, which gains an influence to collect information from all nodes in the network, and we run an algorithm based on the rank increment information on the central node. Each node is bounded to report the time. When the rank of the collected packets increases and then generates a report, which includes the information such as the time, the node address, and the rank. Each node provides its reports to the central node via common uncast. The central node chooses an action of rank change, i.e., the rank increases from i to i + 1, and then searches the received reports to find all the related ones. Then we relate the time order of ETXs with the ascending ETX order and then determine the distance between them. If the distance breaks the threshold, we declare then there remains wormhole attack, and then release the

warning. At last, we update the bound of the distance for the next detection, in order to make our algorithm a robust one. 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 transmission between nodes u and v. For the 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 :

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

Distributed Approach:

In this section, we recognize a practical scenario where the central authority is found to be absence. In this we propose a DAWN, a distributed algorithm to detect wormhole attacks in wireless network coding systems. We will bring accurate analysis on the detection ratio of our algorithm and its resistance against collusions. The main plan of DAWN is that for any two nodes in the neighborhood, the one with lower ETX is assumed to gain new packets prior than the other one with high probabilities. In other words, the innovative packets are forwarded from low ETX nodes to high ETX nodes with high probabilities. In order to monitor the innovative packets transmission direction, all nodes will work together. Basically, DAWN has two phases on each node for the detection: 1) Report packets and 2) Detect whether any attackers exist.

Modified Distributed Approach:

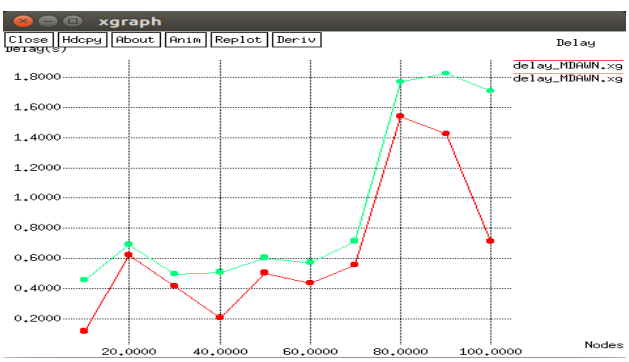
In this section after taking results from DAWN, now we consider other parameters of our nodes. The most favorable parameter for any networking node is considering trust of that node. In modified DAWN approach we consider trust of the node that means the energy consumption of node as well as mobility of that node. Trust is the most important parameter of a node which gives us assurance about whether to forward our packet through that node or not to forward through that node. This parameter is new and considered in our algorithm only. MDAWN finally helps us to find whether the node is wormhole node or a secure node to forward our packets.

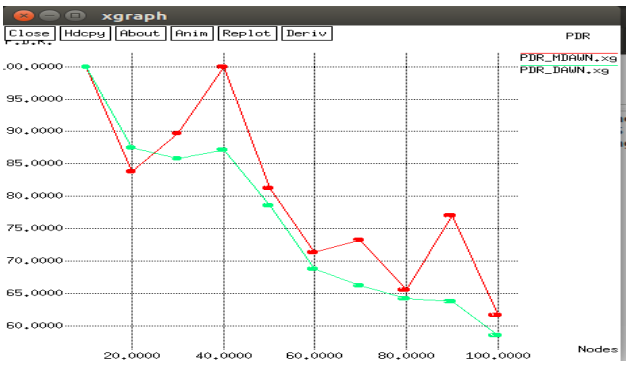
AODV protocol used for network coding systems, such as :

1) This protocol is reliable for the wireless mesh networks. AODV is loop free and does not require any cartelized system to handle routing process for wireless mesh networks.
2) AODV can respond very quickly to the topological changes that affect the active routes because of the availability of dynamic networks.
3) AODV can support both unicast and multicast packet transmissions, even for nodes in constant movement.
4) AODV has lower setup delay for connection and detection of routes.

IV. RESULTS

In this section, we evaluate the effectiveness of the proposed system by simulating it using network simulator. We have considered different parameters to check the performance of the network. Finally, the graphs of the simulation get produced which shows how the performance varies with number of nodes.





Graph 1: Delay Graph 2: PDR

As shown in above graphs we can see the variation in delay and packet delivery ratio with increase in number of nodes. For comparison we have considered the previous distributed algorithm for wormhole detection. Our algorithm that is modified approach towards wormhole detection shows good packet delivery ration as compare to previous one.

V. CONCLUSION

The negative impacts of wormhole attacks on wireless network coding systems are examined. Here algorithms that uses the metric ETX to prevent against wormhole attacks. Distributed detection Algorithm against wormhole in wireless network coding systems, MDAWN. MDAWN is totally distributed for the nodes in the network, eliminating the limitation of tightly synchronized clock. MDAWN is more powerful and thus it suits for network coding systems. For both centralized and distributed algorithms, considered trust and willingness as the major parameter of node. Hence, Wormhole is detected on the basis of a new parameter. MDAWN works in Best manner for stable networks. MDAWN with updated ETX algorithm by considering energy factor.

REFERENCES

[1] S. Li, R. Yeung, 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. Inference Theory, volume 52, Issue 10, pp. 4413–4430, October 2006.

[2] Stephan A. Rein, Frank H.P. Fitzek, "Energy Consumption Model and Measurement Results for Network Coding-enabled IEEE 802.11 Meshed Wireless Networks", IEEE Trans. Volume 5, Issue 4, April 2012.

[3] T. Ho, B. Leong, R. Koetter, M. Medard, M. Effros, and D. Karger, "Byzantine modification detection in multicast networks using randomized network coding," in Proc. IEEE Int. Symp. Inference Theory, Jan. 2004, p. 143.

[4] D. Dong, Y. Liu, X. Li, and X. Liao, "Topological detection on wormholes in wireless ad hoc and sensor networks," IEEE Trans. Network, volume 19, number 6, pp. 1787–1796, Dec. 2011.

[5] 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.

[6] 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.

[7] T. Ho, B. Leong, R. Koetter, M. Medard, M. Effros, and D. Karger, "Byzantine modification detection in multicast networks using randomized network coding," in Proc. IEEE Int. Symp. Inf. Theory, Jan. 2004, p. 143.