International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 03 Issue: 01 | Jan-2016 www.irjet.net p-ISSN: 2395-0072

A DISTRIBUTED APPROACH FOR DETECTING WORMHOLE ATTACK IN WIRELESS NETWORK CODING SYSTEM

Ms. Nivethitha N, Mr. NandhaKumar S, Ms. Meenadevi M

Student, Dept. of Comp. Sci., Dhanalakshmi Srinivasan Engineering College,Tamilnadu,India
Professor, Dept. of Comp.Sci., Dhanalakshmi Srinivasan Engineering College,Tamilnadu,India
Student, Dept. of Comp. Sci., Dhanalakshmi Srinivasan Engineering College,Tamilnadu,India

---

Abstract - *Wireless Network Coding System is the promising approach to improve the performance of a wireless network. It allows the forwarders to apply encoding schee on what they receive, and they can 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. However, wireless networks suffer from a variety of problems such as packet drops, low throughput and routing problems. The major threat in wireless network is wormhole attack. The wormhole attackers can severely disturbs the routing of a network and sends the packet to the distant location. In existing system, connectivity based graph analysis and Timing Based algorithm are used to detect the wormhole attack. These algorithms have difficulty in packet tracking and it does not localize the attacker node in wireless network coding system. Hence, it shows less efficiency in detecting wormhole attack. In this paper, ETX (Expected Transmission Count) is used to calculate the capacity of a node and also the expected total number of transmissions that are needed for a node to transmit the packet successfully. The DAWN algorithm is based on the ETX to detect and report the wormhole attack in wireless network. For each node in the detect phase, it uses the ETX metrics obtained by the node and based on that it detect the attacker node exist in the network. In the report phase, the DAWN algorithm forwards the report about an attacker node that exists in the network to other node.*

Key Words: *Network Coding, DAWN, Expected Transmission Count, Wormhole attack.*

1. INTRODUCTION

Mobile computing is human–computer interaction by which a computer is expected to be transported during normal usage. Mobile computing involves mobile communication, mobile hardware, and mobile software. Communication issues include ad hoc and infrastructure networks as well as communication properties, protocols, data formats and concrete technologies. Providing security services in the mobile computing environment is challenging because it is more vulnerable for intrusion and eavesdropping. The open nature of the wireless medium makes it easy for outsiders to listen to network traffic or interfere with it. Lack of centralized control authority makes deployment of traditional centralized security mechanisms difficult, if not impossible. Lack of clear network entry points also makes it difficult to implement perimeter-based defense mechanisms such as firewalls. Finally, in a MANET nodes might be battery-powered and might have very limited resources, which may make the use of heavy-weight security solutions.

In the efforts to improve the system performance of wireless networks, network coding has been shown to be an effective and promising approach [1],[2] 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. 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 actually no matter what procedures are used, wormhole attacks severely imperil network coding protocols [4], [5]. 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 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 [3]. 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. 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.

The main objective of this paper is to detect and localize wormhole attacks in wireless network coding systems. A distributed algorithm, DAWN, to detect wormhole attacks in wireless interflow network coding systems. The main idea of the solutions is that by examining the order of the nodes to receive the packets in the network, and explore its relation with a widely used metric, expected transmission count (ETX), associated with each node [6], [7].

In DAWN, during regular data transmissions, each node records the abnormal arrival of packets and shares this information with its neighbours. DAWN has two phases on each node: 1) Detect whether any attackers exist the network and 2) Report attacker to the other node. Both of the algorithms are running on every node in the network [8]. In wireless network coding systems, where no fixed routes exist, ETX, the expected number of the packets for the source node to transmit so that the target node (intermediate node or recipient) receives the packet, provides a way to portray the topological structure of the network and the relations among nodes.

2. SYSTEM MODEL

In this section we consider the existing system design and the proposed system.

2.1 Existing System

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. A graph theoretic framework for modeling wormhole links was implemented and it derives the necessary and sufficient conditions for detecting and defending against the wormhole attacks. Based on this framework, it shows that any candidate solution preventing wormholes should construct a communication graph that is a subgraph of the geometric graph defined by the radio range of the network nodes. Making use of this framework, a cryptographic mechanism was proposed based on local broadcast keys in order to prevent wormholes. This solution does not need time synchronization or time measurement, requires only a small fraction of the nodes to know their location, and is decentralized. Hence, it is suitable for networks with the most stringent constraints such as sensor networks [9].

Some other existing works rely on the packet round trip time difference introduced by wormhole attacks to detect them [10]. Unfortunately, this type of solutions cannot work with network coding. The fundamental reason is that with network coding, the packets being transmitted on each hop are different. 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.

Problems Identified:

- They detect only the presence of a wormhole, but do not provide the location of the attacker.
- It cannot find a solution to the dropping of the data packet by the attacker node.
- The detections which rely on Connection based detection leads to the false report when the network changes.

2.2 Proposed System

The main objective of this paper is to detect and localize wormhole attacks in wireless network coding systems. A distributed algorithm, DAWN, to detect wormhole attacks in wireless interflow network coding systems. The main idea of the solutions is that examining the order of the nodes to receive the packets in the network, and explore its relation with a widely used metric, expected transmission count (ETX), associated with each node. In DAWN, during regular data transmissions, each node records the abnormal arrival of packets and shares this information with its neighbours. DAWN has two phases on each node: Detect whether any attackers exist in the network and in the report phase, the DAWN algorithm forwards the report about an attacker node that exists in the network to other node. The Detect phase is based on the received results from the ETX. Both of the algorithms

are running on every node in the network. The DAWN algorithm successfully detects and reports the wormhole attack.

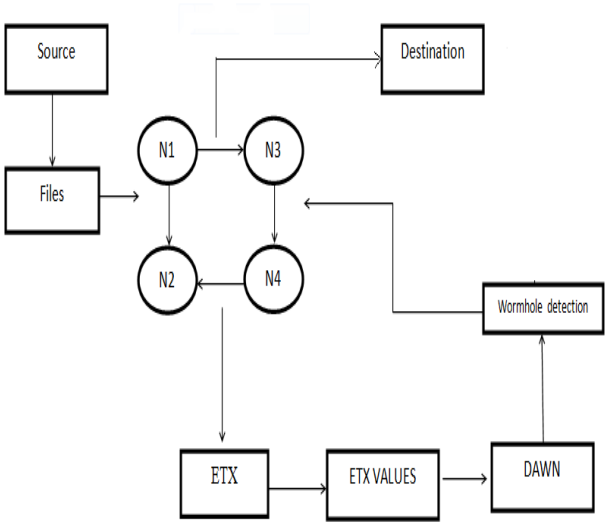

Fig -1 : Wormhole attacker detection

Benefits:

- DAWN algorithm successfully detects the wormhole attacks and also localizes the malicious node.
- Increases the reliability by continuous monitoring of the network.
- DAWN is totally distributed for the node in the network, eliminating the limitation of the tightly synchronized clock.
- It provides the collusion resistance for legitimate node against attacker nodes in the network.

3. DESIGN CONSTRUCTION

This section describes the modules to find the wormhole attack in wireless network.

3.1 Neighbour List

A neighbour node is any node that falls within the transmission range. The wireless network engages in a neighbourhood discovery process. This gives each node's information about which node it can communicate directly. In this, each node broadcast the neighbour request NREQ message. The NREQ receiving node responds to the neighbour with a neighbour reply message (NREP). The requesting node constructs the neighbour lists based on the received NREP messages and counts its neighbour number to forward the packets. After finding the neighbours, the sender node initiates the route request to neighbour for finding the destination.

3.2 Route Finding

The sender selects the data which is to be transmitted and convert them into packets. The forwarding decision is generally made by using the routing process. In this project, Dynamic Source Routing (DSR) algorithm is used to establish a path between the source and destination. Each node is responsible to construct the hierarchical routing tree to other nodes in the network.

- When node S wants to send a packet to node D, but does not know a route to D, node S initiates a route discovery.
- Source node S floods Route Request (RREQ) to the neighbour node and followed by other nodes in the network till it finds the destination.
- Each node appends own identifier when forwarding RREQ. Destination D on receiving the first RREQ sends a Route Reply (RREP).
- RREP is sent on a route obtained by reversing the route appended to receive RREQ.
- RREP includes the route from S to D on which RREQ was received by node D.
- Node S on receiving RREP, caches the route included in the RREP.

When node S sends a data packet to D, the entire route is included in the packet header. Intermediate nodes use the source route included in a packet to determine to whom a packet should be forwarded. Routes maintained only between nodes that need to communicate. Route caching can further reduce route discovery overhead.

3.3 Expected Transmission Count

Expected Transmission Count is used to calculate the total number transmission that a node should make in order to make the other node to receive the packet successfully. A node of low ETX means it is nearer to the source and it may not be the wormhole attacker node. 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 or it may be the attacker node which leads the high ETX values. Thus, the metric of the ETXs is a good representation of the network structure.

ETX is also used to calculate the capacity of the intermediate nodes in a network to check whether the node has the capacity to forward the packet to the

receiver node. It can be used as the first line of defense for reducing the possibilities of wormhole attacks in the network.

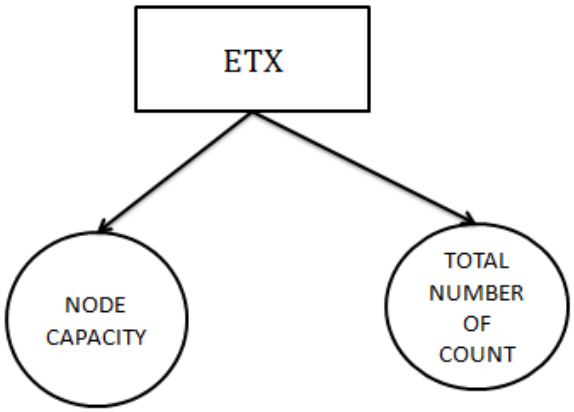

Fig -2 : ETX Results

3.4 Wormhole Attack Detection

It is needed to present the order of the nodes receiving the packets in the network, and explore its relation with a widely used metric, Expected Transmission Count (ETX), associated with each node. DAWN (a Distributed detection Algorithm against Wormhole in wireless Network coding systems) is totally distributed for the nodes in the network. DAWN is efficient and thus it fits for wireless network. DAWN has two phases on each node: detect wormhole attackers exist in the network and report the attacker to the other node.

- For each node in the detect phase, it uses the ETX metrics obtained by the node and based on that it detect the attacker node exist in the network.
- In the report phase, the DAWN algorithm forwards the report about an attacker node that exists in the network to other node.
- Since any node can modify the report when forwarding it, it is needed to apply cryptographic techniques to protect the integrity of the reports. Digital signatures are used to defend against malicious modification of the report.

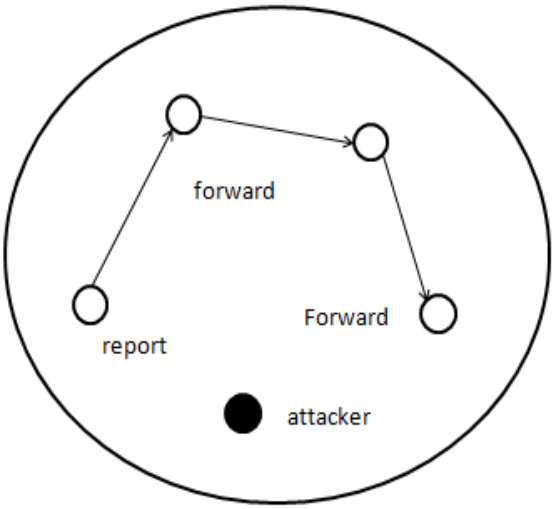

Fig -3 : Attacker Detection

ETX and DAWN algorithm 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.

4. PERFORMANCE EVALUATION

For each node, the detection algorithm will suspect that one neighbor is an attacker if it receives packets from the neighbor but the ETX of this neighbor is much higher than that of itself. It sends its judgment as a report to its neighbors. A node is called a judge node of a neighbor if the difference between their ETXs is greater than the threshold. We use digital signatures of the reports to defend against malicious modification, and abstract of the packet for administrative verification. It first examines whether a report is from a valid judge node. If so, it will forward the report unless it has already been forwarded twice. The detection algorithm on each node accumulates and calculates the number of its judge nodes who send report about the reported potential attacker in the current batch. If the number of judge nodes composes the majority, the node will make the decision that the attacker is involved in a wormhole attack.

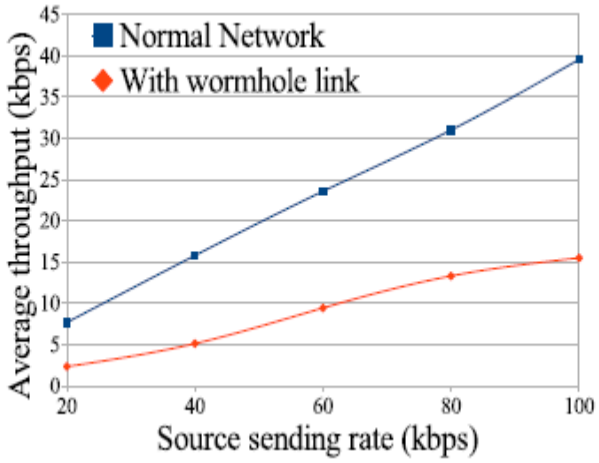

Fig -3 : Average throughput for source sending rate with or without wormhole attack.

In order to examine the capability of DAWN in resisting collusions among judge nodes, we test our algorithm in the scenarios with different numbers of colluding judge nodes. We observe the True Positive Rates with different number of colluding nodes. It verifies that DAWN has strong resistance against the colluding attacks.

For DAWN, Fig -5 shows the average computation time cost per node and per batch with various node densities. We can observe that our algorithm costs more time, when there are more nodes in the network and correspondingly more events to monitor and report. Overall it shows the computation time cost of DAWN is tolerable for most wireless network applications, with a few milliseconds at most.

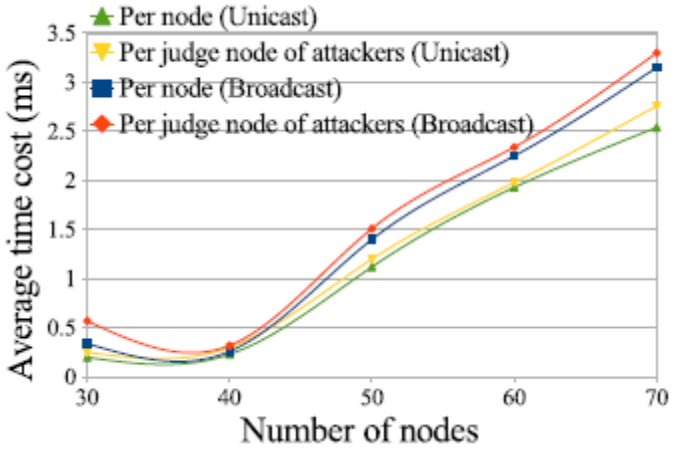

Fig -5 : Average time cost

5. CONCLUSION

Two algorithms, ETX and DAWN are proposed to defend against wormhole attacks. Expected Transmission Count is used to calculate the total number counts that a node should make in order to make the other node to receive the packet successfully. To examine the order of the nodes which receive the packets in the network, and explore its relation, expected transmission count (ETX), associated with each node is used. ETX is also used to calculate the capacity of the intermediate nodes in network to check whether the node has the capacity to forward the packet to the receiver node. In DAWN, during regular data transmissions, each node records the transmission of packets and shares this information with its neighbours. DAWN algorithm successfully detects the wormhole attacks and also localizes the malicious node. It also forwards the attacker report to the other node in the network. ETX and DAWN efficiently detect and localize the wormhole attack in the networks. In the future work, the attacker node can be avoided from participating in packet transmission.

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] 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.

[4] 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.

[5] 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.

[6] 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.

[7] D. S. J. D. Couto, D. Aguayo, J. Bicket, and R. Morris, "A high throughput path metric for multi-hop wireless routing," Wireless Netw., vol. 11, no. 4, pp. 419–434, 2005.

[8] Shiyu Ji, Tingting Chen, and Sheng Zhong,(2015.) "Wormhole Attack Detection Algorithms in Wireless Network Coding Systems", IEEE Trans.

Mobile Computing, vol. 14, no.3, pp.660-674, Mar. 2015.

[9] 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.

[10] 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.