Cognitive Approach to Detect the Wormhole Attacks in MANET

Nagendran.K
Assistant professor / Department of Information Technology
Sri Krishna College of Engineering & Technology
Coimbatore
knagendrancse@gmail.com

Manojee.K.S
Assistant Professor
Department of Computer Science
Mahendra Engineering College
Namakkal
Manojee.suri@gmail.com

Abstract— Wireless networks are recognized to be liable to a assortment of Dos and DDOS attacks such as wormhole which reduces the quality of service in normal network operations. Lot of methods have been developed to identify and to preserve these kind of attacks. But these solutions mainly focus on attack-resilient rather than rooting out the source of attacks. Wormhole attacks can weaken or disable wireless sensor networks. MANET is severely affected by Distributed Denial of Service (DDoS) attacks which are the major problem for users of computer systems connected to the Internet. The wormhole attack is possible even if all communication provides legitimacy and secrecy. In the wormhole attack, an attacker slash packets at one location in the network, tunnels them to another location, and retransmits them there into the network. This can form a serious threat in wireless networks, including many ad hoc network routing protocols and location-based wireless security systems. An unique solution is developed to handle this integrity verification by forming the distributed and centralised wormhole detection algorithm for wireless networks. In this paper, we quantify wormhole's demoralizing harmful crash on network coding system performance through experiments**.**

Keywords— *MANET, DDoS, DoS, wormhole effect*

*****

I. Introduction

A wireless network is a network that uses wireless data connection for connecting nodes. Wireless networking is a method of connecting home networks; telecommunication networks and business installation avoid the expensive process of introducing cable, or as a connection between different locations. Wireless network attacks have significantly increased in the past few years. Every wireless network attack has its own crash on network function. The intruder will attack the packets which are sent as plain text or in encrypted form, "Confidentiality Attacks" will interrupt the data packets sent over the wireless network. Attackers are getting smarter along with the passage of time. A wormhole attack can be easily done by capturing the packets from one node to another node without having knowledge of the network or any other node. It is a severe threat in mobile ad hoc network applications. The Intruder receives packets at one point in the network, forwards them through a wireless tunnel and relays them to another point in the network. This paper describes distributed and centralized wormhole detection algorithm for wireless networks.

II. Problem Statement

In a wormhole attack, an invader receives packets at one node in the network, "tunnels" them to another node in the

network, the distance formed by "tunneling" is longer than the normal transmission range of a single hop, the work attacker is simple to make the tunneled packet appear with better metric than a normal multihop route. The attacker forwards each bit over the tunnel directly, without waiting for an entire packet to be received.

:

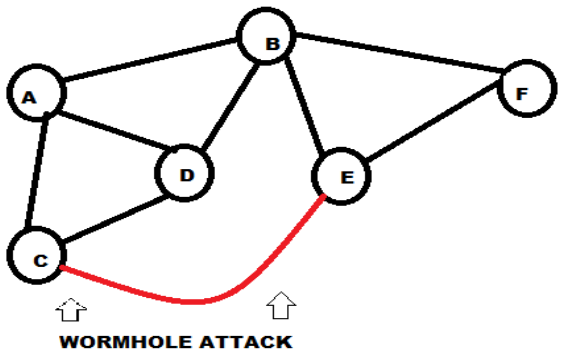

Figure 1: Wormhole Attack

The attacker accepts the rebroadcast packets. In wireless networks, some nodes will have the delusion that they are close to the attacker. It has the ability of changing network topologies and bypassing packets for further exploitation.

The wormhole has been created and posed in three different ways:

a) Tunneling the packets.

b) The Distance of Long Range tunnel.

c) Tunnel creation.

The wormhole attack replay packets already existing on the network so the attack cannot be overwhelmed by network security, which pass all cryptographic check. The first step of the wormhole attacks are more complicated attacks, such as man-in-the-middle attacks and other DoS attacks. Some nodes in the network will waste their resources by retransmitting the packets from the wormhole link and processing some non-innovative packets. Second, the intruder may have the ability

to turn off and on the wormhole tunnel in the data transmission. This makes the network system unable to find the counterfeit transmission link in data transmission. The main objective of this paper is to detect and localize wormhole attacks. A centralised and distributed algorithm is proposed to detect the attack in MANET.

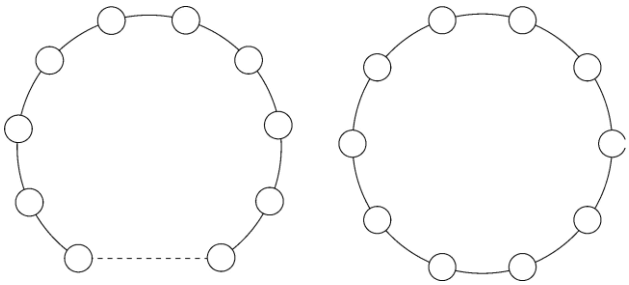

Figure 2: Dotted Lines- "Tunneling" path created by two malicious node

Packet leash is a general mechanism for detecting and defensive against wormhole attacks. A leash is defined as any information that is added to a packet designed to restrict the maximum allowed transmission distance of a particular packet.

III. The Dawn Algorithm

The DAWN algorithm is designed using the Transmission Count. The ETX metric, or expected transmission count, is defined as the measure of the value of a path between two nodes in a wireless packet data network. ETX is the number of expected transmissions of a packet to be received without error at its destination. The Expected Transmission Count (ETX) metric is an sophisticated routing metric used for finding high-throughput. Among the neighbor nodes, the one with lower ETX is supposed to receive new packets earlier than the other one whose probability is high. In order to supervise the new packets transmission direction, nodes have to work collaboratively. DAWN consists of two phases on each node:

a) Observation of packet direction and report its results to its neighbors and

b) Detection of attackers, if any.

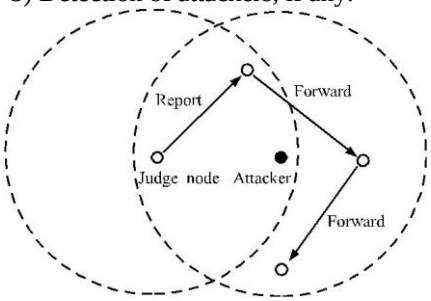

Figure 3: Judge Node in wireless network

The Detect phase is mainly based on the results which are received from neighbours during the Report phase. Both of the algorithms are running simultaneously on every node in the network.

Report phase, Each node will think that its neighbor is an attacker if it receives new packets from the neighbor and the ETX of this neighbour is greater than the threshold. A node is called a judge node of a neighbor if their ETXs metric is higher than the threshold. It sends its opinion as a report to its neighbours.

Detect phase, the judge node sends the report to each node in the detect phase. After receiving the report from the judge node, it analyses the report i.e. whether it is from valid judge node or not. Next, it sends the report from the valid judge node to all the remaining nodes in the network and helps to detect the malicious node. Each node accumulates and calculates the number of its judge nodes who forward report about the reported possible attacker in the current batch. The decision will be based on the majority report which are generated from the judge node and confirms the attacker is involved in a wormhole attack and block it from future data transmission.

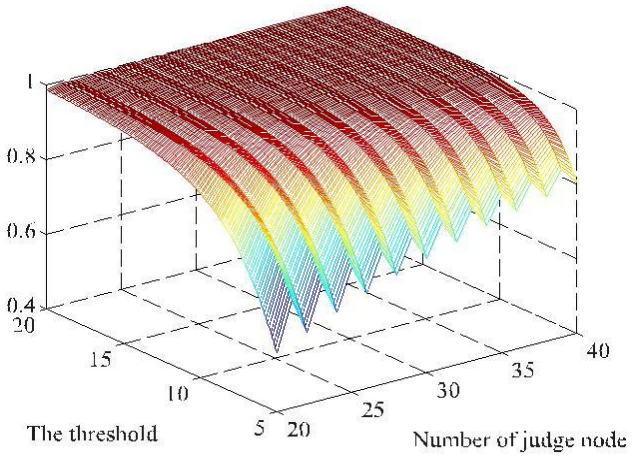

Figure 4: Successful Probability in DAWN

IV. The centralized Algorithm

In the centralized algorithm, we investigate the order of rank increments to identify the wormhole links. Mostly, when a new packet is sent from the source node, the nodes that are near the source node are expected to receive the new packets earlier than the nodes that are distant from the source node.

On the other hand, the existence of wormhole link instinctively changes the regular network topology since the new packets can be transmitted through the "tunnel" directly and safely, and thus the nodes in the region of the remote side of the "tunnel" can receive the new packets earlier than expected. This significantly changes the order of the rank increments among the nodes. The source node sends a new packet, and each node receiving the new packet will result in rank increment varies from 0 to 1. The time stamps of rank increments on the nodes throughout the whole transmission are collected and by using these time stamps the order of rank Increments are found.

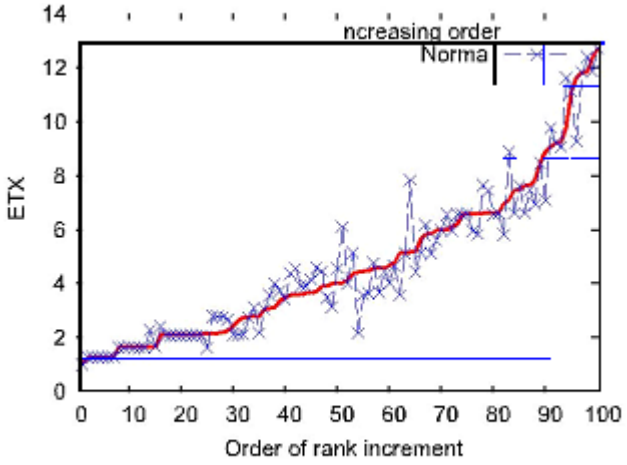

Figure 6: rank increment order of node in normal network

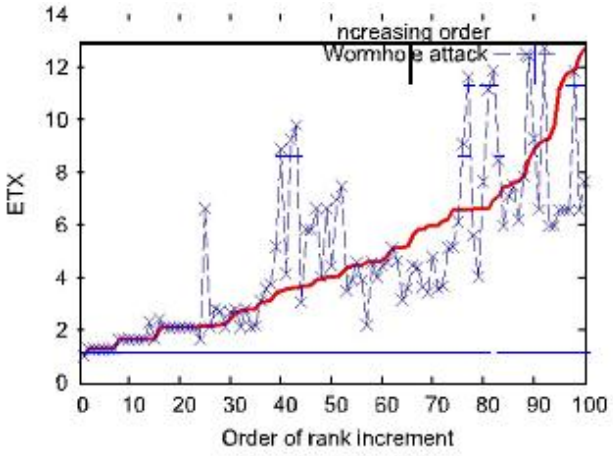

Figure 6: rank increment order of node in worm hole attack network

The ETXs of the nodes based on the ascending time order of rank increments are denoted by blue lines. Later, we find that when the wormhole link exists the blue line automatically deviates from the red line. It is true that the wormhole truly changes the network topology and also the transmission flows. It is easy to observe the time order of rank increments, and send alerts when the deviation of the order exceeds the bound.

The range of the nodes which involved in wormhole attack also determined. We set up a central node in the centralised algorithm and it owns the authority to collect information from all the nodes in the network. Wormhole detection Algorithm will be based on the rank increasing information on the central node. The responsibility of each node is to record the time when the rank of the received packets increases and then it generates a report that contains the details of the time, the node address, and their rank. Each node sends the reports to the central node through common unicast.

V. Conclusion

We have investigated about the wormhole attacks on wireless network system and proposed two algorithms that make use of the metric ETX to safeguard against wormhole attack.In proposed Centralized Algorithm, it assigns a central node to collect and examine the forwarding behaviors of each node in the network, to react well-timed when wormhole attack is initiated. The correctness of the Centralized Algorithm was proven by deriving a lower bound of the deviation in the algorithm. We have proposed a Distributed detection Algorithm against Wormhole in wireless Network systems, DAWN. DAWN is distributed algorithm for the nodes in the network, eliminating the restriction of firmly synchronized clock. DAWN is efficient and it fits for wireless network. Both centralized and distributed algorithms, we have utilized the digital signatures to make sure every report is indisputable and cannot be forged by any attackers. the proposed algorithms can sense the malicious nodes participating in wormhole attack with high booming rate and the algorithm is proficient in terms of computation and communication overhead.

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,” inProc. 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,” inProc. 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 high throughputpath 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 sensornetworks," 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/
[27] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21, no. 2, pp. 120–126, 1978.
[28] R. Rivest, "The md5 message-digest algorithm," RFC 1321, 1992.
[29] J. Dong, R. Curtmola, and C. Nita-Rotaru, "Practical defences against pollution attacks in intra-flow network coding for wireless mesh networks," in Proc. ACM Conf. Security Privacy Wireless Mobile Netw., Mar. 2009, pp. 111–122.
[30] 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.
[31] Z. Li, D. Pu, W. Wang, and A. Wyglinski, "Forced collision: Detecting wormhole attacks with physical layer network coding," Tsinghua Sci. Technol., vol. 16, no. 5, pp. 505–519, 2011.
[32] I. Khalil, S. Bagchi, and N. B. Shroff, "Liteworp: A lightweight counter measure for the wormhole attack in multihop wireless networks," in Proc. Int. Conf. Dependable Syst. Netw., Jul. 2005,pp. 612–621.
[33] L. Qian, N. Song, and X. Li, "Detection of wormhole attacks in multi-path routed wireless ad hoc network: A statistical analysisapproach," J. Netw. Comput. Appl., vol. 30, no. 1, 2007.
[34] L. Buttyan, L. Dora, and I. Vajda, "Statistical wormhole detection in sensor networks," in Proc. Eur. Workshop Security Privacy Ad-Hoc Sensor Netw., Jul. 2005, pp. 128–141.