IJRSET AUGUST 2016 Volume 3, Issue 8 Pages: 1-8

ISSN 2394-739X

International Journal for Research in Science Engineering and Technology

DETECTION OF BLACKHOLE AND GREYHOLE ATTACKS ALONG WITH WORMHOLE ATTACKS IN WIRELESS SENSOR NETWORKS

[1] Shibila U
[1] M.Tech Scholar
[1] Department of ECE
[1] MEA Engineering College Kerala, India

[2] Praveen P N
[2] Asst. Professor
[2] Department of ECE
[2] MEA Engineering College Kerala, India

ABSTRACT - The wireless network coding system is one of the effective ways to improve the performance ofthe wireless network. But this system also knop various kind of threats in the wormhole attack. The wormhole attack debases the performance of the network coding systems. In order to conquer this issue various methods and techniques have been presented. For networks that have centralized authority, a centralized algorithm is used. In this algorithm, the central node is responsible for collect all information about surrounding nodes. It has received the contemporary packets from the nodes and it will analyze the wormhole cases. But the network coding systems also suffer from selective black hole attacks i.e. black hole nodes and grey hole attacks. To overcome this problem, a new approach called Advanced Detection Protocol (ADP) is used to detect and remove both black hole and grey hole attacks. In this method, the IDS nodes are set in promiscuous mode only when required, to detect the irregular activities through the data packets, which are forwarded by the node. When any anomaly is detected, the nearbyIDS node announces the block message, informing all nodes on the network to cooperatively isolate the attacker node from the network. In this approach, the destination node detects the presence of malicious attackers in the route based on the momentous difference between the number of data packets the source node had sends and the number of data packets it actually receives that has been monitor. The suspicion nodes are then informed to the IDS nodes to isolate the attacker nodes that launch the black hole attack and grey hole attack, from the network. The proposed method is more energy efficient and hence reduces the computation and communication costs.

Keywords-[Wireless networks, Linear network coding, Wormhole attack, Expected transmission count]

1. INTRODUCTION

When improving the achievement of wireless networks, network coding system has been shown to be a promising and effective approach and it was basically different approach compared to other network approaches. In contrast, in wireless network coding systems (WNCS), the senders grand to substitute encoding schemes on what they receive, and thus they are responsible to create and transmit new packets. The idea of mixing packets on each node takes good influence of the opportunity diversity and broadcast nature of wireless communications network, and

much upgraded system are have a good performance. During the wormhole attack, the attackers can easily forwarded each data packets using wormhole links and without modifies any packet transmission during the routing to an unauthorized node. Hence, receiving the rebroadcast packets by the attackers, some nodes will have the delusion that they are close to the attacker. With the capability of modifying network topologies and bypassing packets for further control, wormhole attackers pose a distribute attack to many functions in the network, such as routing and localization.

Black hole and Grey hole attack are different attack in MANET. In black hole attack, source node broadcast the route request message to the nodes. But request is listened by the attacker node and then malicious node claim that it has a shortest path to the destination minimum hop count and maximum sequence number. Then the malicious node takes all the routes towards itself and it doesn't allow forwarding the packets to the others nodes. Gray-hole attack is a kind of black hole attack. In gray hole attack packets that are transmitted from one node to other are dropped with some probability. It drop packet coming from (source) and going to certain specific node in a network while forwarding all packet from onenode to another. The grey hole attack is more difficult to be detected than the black hole attack.

2. PRELIMINARIES

In this paper, a new technique is introduced which is called Advanced Detection Protocol (ADP) for detecting the black hole and grey hole attacks in the network coding systems. In this method, firstly cluster the network using weighted based clustering algorithm. A Random Linear Network Coding Approach to Multicast [1] is distributed linear network coding approach which asymptotically achieves capacity. The analysis uses insights from network flows and bipartite matching which then lead to a new bound on required field size for centralized network coding.

A Random Linear Network Coding Approach to Multicast Impressive packet loss conservation scheme joint deterministic network coding (DNC) [2] and the random linear network coding (RLNC) used for H.264/AVC video transmission. It considers the complexity of the RLNC algorithm for the transmission scheme should make some improvement. Comparison of Traditional and Opportunistic Multi hop Routing in the Wireless Networking Scalability [3], a discrete event simulator is applied to examine the performance of network with two classes of routing protocols: traditional vs. opportunistic. It obtains that the opportunistic routing can better utilize network redundancies, as compared to an upper bound of traditional routing based on global route optimization.

XORs in the Air: Practical Wireless Network Coding [4] addresses the normal case of unicast traffic, dynamic and potentially burst flows, and practical issues facing the integration of network coding in the current network stack. Improved Power-Delay Trade-off in Wireless Ad Hoc Networks Using Opportunistic Routing [5] opportunistic routing can exhibit better power delay trade-off than the conventional routing which provide a logarithmic boost in the scaling law. In Privacy in opportunistic network contact graphs [6], contact graph is then used to give a utility to each node (e.g., based on their centrality), thereby defining a ranking of the nodes' values for carrying a message.Topological Detection on Wormholes in Wireless Ad Hoc and Sensor Networks [7] understand the impact and inevitable symptom of wormholes and develop distributed detection methods by making as few restrictions and assumptions as possible[8]. In-Band Wormholes and Countermeasures in OLSR Networks [9] are an important threat since they do not require specialized hardware and can be launched by any node in the MANET. Preventing

Wormhole Attacks on Wireless Ad Hoc Networks-A Graph Theoretic Approach [10] is an important defense mechanism based on local broadcast keys that supports for detection of wormhole attack in a network.

3. PROPOSED WORK

In the existing method, novel methods are presented to overcome the devastating harmful effects of the Wormhole attacks in the wireless network coding systems. The algorithm leverages the order of the nodes to receive the ingenious packet and utilizes the machine learning techniques to distinguish the wormhole cases. The centralized algorithm and the digital signatures are used to ensure every report is undeniable and cannot be forged by any attackers. Black hole and grey hole attacks are not considered in that system. Security issues increases when attackers capture neighbor nodes. To overcome this problem Advanced Detection Protocol (ADP) is proposed for detecting the black hole and grey hole attacks in the network coding systems.

In this method, firstly cluster the network using weighted based clustering algorithm. It assess a weight for each node and the cluster heads are chosen among the best suitable nodes in terms of node degree, area between neighbors node, mobility and energy possible. In terms of energy consumption, the algorithm tries to achieve the greater durable cluster architecture, meaning after the first iteration the algorithm is executed only when there is an appeal. This minimizes system updates and hence computation and communication costs. In this approach, the destination node detects the presence of malicious attackers in the route based on the significant difference between the number of data packets that source node sends and the number of data packets it absolutely receives. The suspected nodes are then inform to the IDS nodes to avoid the malicious nodes that launch the black hole attack and grey hole attack, from the network. This method is more efficient in detecting the attacks. The figure 1 shows the block diagram of system process.

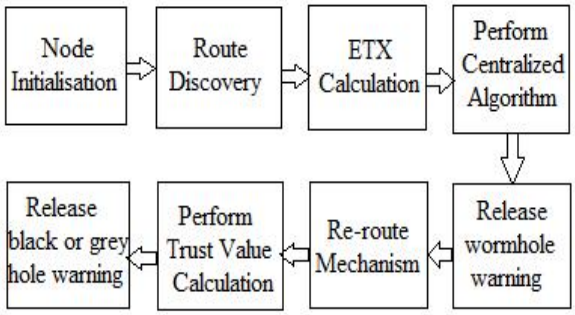

Figure 1- System Process

3.1 Initialization

The first step in the algorithm is the initialization of the population of N nodes where each node represents a candidate solution. An objective function is associated with the brightness of the firefly and is directly proportional to the brightness. The figure 2 shows the node initialization where 30 different nodes are positioned in X and Y, fixed range and are randomly generated in that range of nam window. The transmission range for each node is 250metres and the node in blue color is set as the certificate authority as used in the centralized algorithm for wormhole detection.

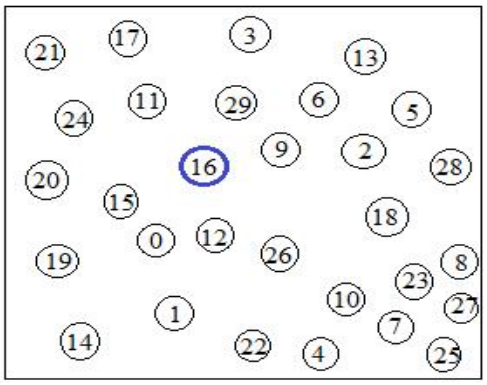

Figure 2- Node Initialization

3.2 Wormhole Detection

A path from source to the destination node is created by choosing the shortest distance from one node to the other. Then, all valid nodes register with the public register before packet transmission. In this work, worm hole detection approach is found by

using the parameter called the ETX (Expected transmission count). The ETX is nothing but the probability of number of packets that can be send or receive by the nodes. Node of high ETX means it is difficult to make it hear from the source usually because the node is far from the source and the links between them are much loss. Thus, the metric of the ETXs is a good representation of the network structure. Let u and v be two nodes and p (u v) be the probability of successful transmissions between node u and v. For simple 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:

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

The probability p (u; v) is estimated based on the previous transmission record, using some statistical models like weighted means or window-based observation. It is assumed that, whenever the data's are forwarded from one node to another node, it must receive innovative packets. Innovative packets are nothing but the new packets which cannot be found in the previously received packet values. Wormhole detection in the existing mechanism is done in two phases. Those are

- Report phase
- Detect phase

Report phase will find the existence of wormhole link and Detect phase will ensure worm hole is present and will block in the future.

In the report phase, ETX count of all the nodes will be calculated. When sender node sends the packet to the receiver node it will also inform about the ETX count. By receiving the packets from sender, the receiver node will check whether the innovative packets present. If it is present then it will compare its ETX rate with the sender node ETX rate. If the sender node has higher ETX rate than the receiver node then, receiver will mark it as wormhole node. Then it will create the report contains that the sender node id which is found as malicious along with signature values. This report would be encrypted which will then be forwarded to all the neighboring nodes.

In the detect phase, nodes will receive the report which contains the information about the worm hole nodes from all judge nodes present in the environment in the encrypted format. Then it will be verified whether these information are received from the valid node or not by getting identity information from the public server. If it receives the information about the malicious nodes from majority of judge nodes then it will be concludes that the worm hole is present then those transmission of packets through those nodes would be avoided in the future.

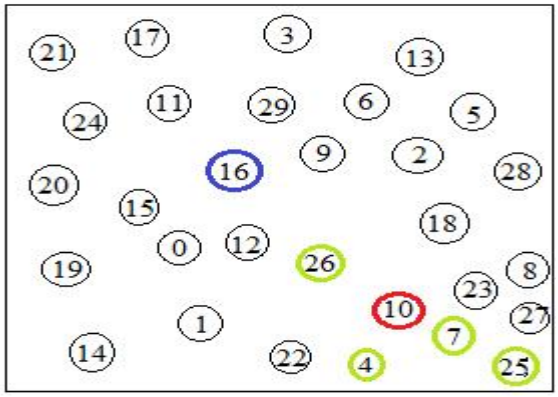

Figure 3- Wormhole Detection

The figure 3 shows wormhole detection at node 10, shown in red color. The nodes in green color represent the path for packet transmission.

3.3 Advance Detection Protocol (ADP)

This framework is widely used in mobile ad hoc networks (MANET). The different kind of misbehavior a node may exhibit is selfishness. A misbehaving node need to protect itself assets, when using the processes of others and consuming their assets. One way of preventing selfishness in a MANET is a detection and exclusion mechanism. In this method, the network is clustered. It assess a weight for each node and the cluster heads are chosen among the best suitable nodes in terms of node degree, area between neighbors node, mobility and energy possible. . The selected CH is an IDS node in

the intrusion detection system. The IDS nodes are set in promiscuous mode only when required, to detect the abnormal diversity in the number of data packets being forwarded by a node. When any anomaly is detected, the nearby IDS node shows the block message, informing all nodes on the network to cooperatively isolate the malicious node from the network. In this approach, the destination node detects the presence of malicious attackers in the route based on the significant difference in the number of data packets the source node sends and the number of data packets it absolutely receives.

3.4 Trust Mechanism

This section provides the overview of the proposed scheme to detect the malicious node that is implementing the grey hole and black hole attack. The method to calculate the trust value of the node is given below. To calculate the trust value every node will monitor the behavior of the cluster head. And then calculate the trust value using the data collected by monitoring the behavior of the node. In wireless sensor network all the packets are actually broadcasted therefore it is easy for all other node to listen the packet transmitted to cluster head. Due to the presence of adversary cluster head may drop some packed instead of forwarding. Thus by finding out how many packet the cluster head has forwarded can find out how much task the cluster head has completed. Beside this every node will observe the number of packet forwarded by the cluster head. Let Ui be the number of the packet transmitted by node i to CH, and Fi be the number of packet belonging to node i forwarded by CH to BS. Therefore the trust value of CH calculated by node j for node i on bases of task completion is given by following equation:

$$Trustvalue = \frac{F_i}{Ui} * 100 \quad (2)$$

Once the node has calculated the trust value of its cluster head, node will now determine whether the cluster head is malicious or not. For this node will compare its calculated trust value with the predetermine threshold TH. Every node in cluster will compare both its node level trust values and the cluster level trust value with threshold. If any node discovers the trust value below TH then that respective node will raise alert message. For this consider two threshold value TH1, TH2 such that TH1<TH2. If the trust value is less than TH1 then the node is malicious and said to be affected by black hole attack. If the trust value is greater than or equal to TH1 but less than TH2 then there is uncertainty. This case detects a malicious node being affected by grey hole attack and if the trust value is greater than or equal to TH2 then the node is normal.

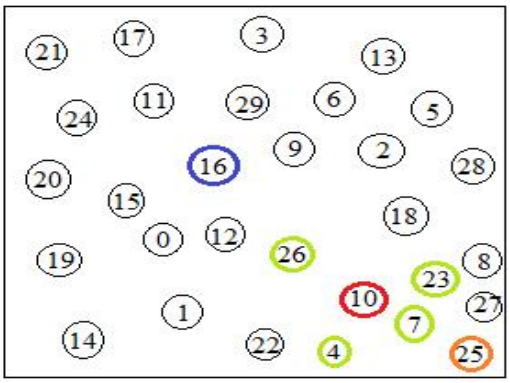

Figure 4- Black hole or Grey hole Detection

The figure 4 shows the animated output of trust mechanism. In this, a new path is created after wormhole detection and the trust mechanism is performed on this new path. It shows the case of a black hole attack in orange color. Similarly the gray whole attack detection is set to be in grey color.

If any node discovers the trust value below TH then that respective node will raise alert message claiming that the cluster head may be malicious node implementing the gray hole attack and node will directly broadcast to BS. The attack detection is done by base station and nodes only calculate the trust value and forward it to base station. Thus energy required by the node for the attack detection will be reduced. Also a better secure system without being affected by any attack is obtained.

4. PERFORMANCE EVALUATION

The simulation is done on an event based simulator called NS-2. In this mechanism, the network includes 30 nodes deployed randomly in a 500meters × 500meters and the transmission range is 250 meters.There is no movement of nodes and traffic is generated randomly by a random generator provided by NS-2. Thefollowing section shows the simulation parameters and results and comparison performance of the proposed system. Table 1 shows the simulation parameters of the proposed method.

Parameter	Value
Field size	1000×1000 m
Number of sensor nodes	30
Propagation type	Two ray ground
Routing type	AODV
Channel	Wireless channel
Simulation time	85.0 s

Table 1- Simulation Parameters

In this section the performance of the protocol is compared with the existing method in terms of packet delivery ratio, end to end delivery and the throughput.

Figure 5- PDR Plot

Above graph shows the comparison of existing and proposed attacks detecting scheme in terms of packet delivery ratio (PDR). From figure 5, the whole ratio of the number of packets being delivered from the source to the destination is found to be increased as compared with the detection of a single attack in the network.

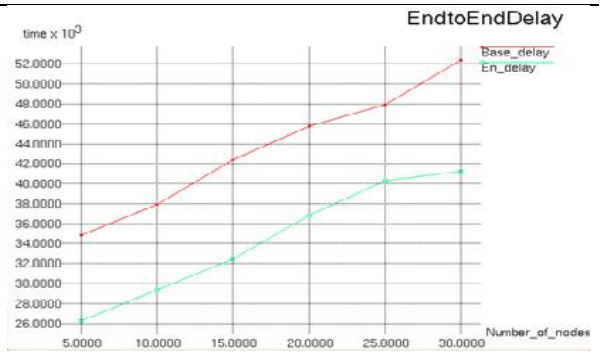

Figure 6- End to End Delay Plot

Above graph shows the comparison of previous technique and proposed routing framework in terms of end to end delay. In figure 6, the average time delay caused by a data packet to reach at the destination is found to be low as compared with the previous scheme.

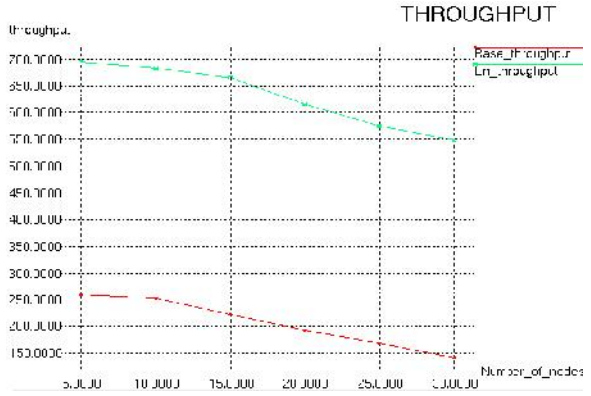

Figure 7- Throughput Plot

Above graph shows the comparison of previous technique and proposed routing framework in terms of end to end delay. In figure 6, the average time delay caused by a data packet to reach at the destination is found to be low as compared with the previous scheme.

CONCLUSION

This paper proposed Advance Detection Protocol (ADP) detecting the black hole and grey hole attacks in the network coding systems. The IDS nodes are set in immoral mode only when required, to find the irregular difference in the number of data packets being forwarded by a node. The suspected nodes are then informed to the IDS

nodes to isolate the malicious nodes that launch the black hole attack and grey hole attack, from the network. This method is more efficient in detecting the attacks. IDS evaluates a weight for each node and the cluster heads are chosen among the best suitable nodes in terms of node position, bandwidth from nearby nodes, movements and enough power. In terms of energy consumption, the technique tries to achieve the highly unmovable group structure, define than the first iteration the algorithm is executed only when there is an appeal. Thus decreases processes modernize and counting transmission costs.

REFERENCE

[1] Tracey Ho, Member, IEEE, Muriel Médard, Senior Member, IEEE, Ralf Koetter, Senior Member, IEEE, David R. Karger, Associate Member, IEEE, Michelle Effros, Senior Member, IEEE, Jun Shi, and Ben Leong" A Random Linear Network Coding Approach to Multicast" in 10, OCTOBER 2006.

[2] Cuiping Jing, Xingjun Zhang, Yifei Sun, Huali Cui and Xiaoshe Dong "A Packet LossProtection Scheme Joint Deterministic Network Coding and Random Linear Network Coding for H.264/AVC" in 2011.

[3] PetrosSpachos, Liang Song and DimitriosHatzinakos "Comparison of Traditional and Opportunistic Multihop Routing in Wireless Networking Scalability" in 2012.

[4] SachinKatti, Hariharan Rahul, Wenjun Hu,Dina Katabi, Muriel Médard "XORs in the Air: Practical Wireless Network Coding" in 2008.

[5] Won-Yong Shin, Sae-Young Chung, and Yong H. Lee "Improved Power-Delay Trade-off in Wireless Ad Hoc Networks Using Opportunistic Routing" in 2007.

[6] Bernhard Dist, TheusHossmannl"Privacy in opportunistic network contact graphs"

[7] A. J. Newell, R. Curtmola, and C. Nita-Rotaru, "Entropy attacks and countermeasures in wireless network coding,"

[8] Dezun Dong, Member, IEEE, MoLi,Member, IEEE, Yunhao Liu, Senior Member, IEEE, Xiang-Yang Li, Senior Member, IEEE,and Xiangke Liao "Topological Detection onWormholes in Wireless Ad Hoc and Sensor Networks"

[9] Peter Kruus, Dan Sterne, Richard Gopaul, Michael Heyman, and Geoff Lawler, "In-Band Wormholes and Countermeasures in OLSR Networks"

[10] L. Lazos1, R. Poovendran, C. Meadows, P.Syverson, L.W.Chang, "Preventing Wormhol Attacks on Wireless Ad-Hoc Networks: A Graph Theoretic Approach"

[11] Yih-Chun Hu, Member, IEEE, Adrian Perrig, Member, IEEE, and David B. Johnson, Member, IEEE "Wormhole Attacks in Wireless Networks".

[12] Shiyu Ji, Tingting Chen and Sheng Zhong," Wormhole Attack Detection Algorithms in Wireless Network Coding Systems", IEEE transactions on mobile computing, vol. 14, no. 3, march 2015

[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. 3rdACM 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] MitaliKhandelwal, SachinUpadhyay," Detecting and Preventing Black hole and Grey Hole Attacks for Trust Management in Wireless Sensor Networks", International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 5, May 2016

[17]Weichao Wang, Aidong Lu, "Interactive Wormhole Detection in Large Scale Wireless

Networks," IEEE Symposium On Visual Analytics Science And Technology 2006
[18] Youngho Cho, Gang Qu, Yuanming Wu. "Insider Threats Against Trust Mechanism With Watchdog And Defending Approaches In Wireless Sensor Networks." IEEE Symposium On Security And Privacy Workshops, 2012, Pp. 134-141
[19] ShilaDevuManikantan, Cheng Yu, Anjali Tricha." Channel-Aware Detection Of Gray Hole Attacks In Wireless Mesh Networks." in: IEEE Global Telecommunications Conference, December 2009. P. 1–6
[20] William Potnis, and C S Rajeshwari, "Wireless Sensor Network: Challenges, Issues And Research", Proceedings Of 2015 International Conference On Future Computational Technologies (Icfct'2015), Pp. 224-228, March 29-30, Singapore, 2015