Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 3– No.3, October 2015 – www.caeaccess.org

Modified Hop Count Analysis Algorithm (MHCAA) for Preventing Wormhole Attack in WSN

Mosmi Tiwari
M.Tech Scho
Oriental University, Indore

Amrita Tiwari
Assistant Professor
Oriental University, Indore

Deepak Sukheja
Assistant Professor
Oriental University

ABSTRACT

Wormhole attack is one of severe security threat may apply on network layer. It is a passive attacks aims to drop packets by creating illusion of shortest path from source to destination. Wormhole nodes attempt to attract the genuine nods by showing an illusion of shortcut from source to destination and registered themselves as next hop at source routing table. When source consider wormhole tunnel as shortest route and transfer packet to wormhole node they start dropping packet respectively. This paper considers this problem as severe issue an attempt to derive a mechanism to detect and prevent wormhole node in mobile ad-hoc networks.

The objective of this paper is to study various ways to create wormhole attack and develop techniques to detect and prevent wormhole node using AODV routing protocol.

Keywords

WSN, Worm-Hole, AODV

1. INTRODUCTION

The Wireless Sensor Network (WSN) is a kind of wireless network that consist of thousands of sensor nodes deployed in the open field. WSN provides the solution to the real world application like military and civilian tasks at very low cost with absolute performance. Further, Small data storage capacity, low power battery, low bandwidth and low computational power make it more complex and vulnerable to many security threats.

Wormhole attack is very difficult to detect in the network because it neither require MAC protocol information nor need to crack the encryption key. In order to implement wormhole attack, attacker either compromised the existing node or introduces a malicious node in existing scenario between source and destination. Afterwards, when packets reach to compromise node, it drops the packet rather than forwarding.

. These nodes have the ability to configure themselves and because of their self configuration ability, they can be deployed urgently without the need of any infrastructure which is shown in Figure 1.1.

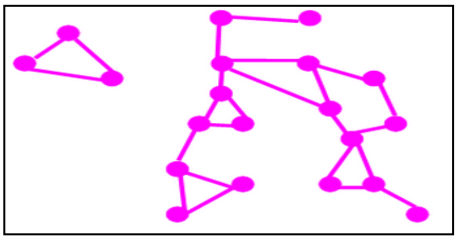

Figure 1.1: WSN

2. WORMHOLE ATTACK

The wormhole attack is one of the most severe attacks of WSN.. Wormhole attack is a type of the Denial-of-Service attacks effective on the network layer. It affects network routing, and especially location based wireless security. The wormhole attack is basically launched by a pair of collaborating nodes. In wormhole attack two collaborating attacker nodes occupy strong strategic locations in two different parts of the network. By occupying dominant positions in a network these two nodes can cover complete network and advertise to have the shortest path for transmitting data. The two attacker nodes are connected to each other using a link which is called wormhole tunnel. At one end of wormhole tunnel, one node overhears the packets in its local area and forwards them to the other node which replays them to its local area.

The wormhole tunnel can be established to obtain a direct low latency communication link between two distant nodes (attacker nodes) using private high speed network for example using an Ethernet cable or optical link. If these two nodes forward all the packets legitimately then in a way they are supporting the faster communication and routing within the network. However, this is not the case as these attacker nodes either drop or selectively forwards the packets or alter them.

Here the target node sends RREQ packets all over the network to find out the possible legitimate routes. As the attacker 1 receives the RREQ packet sent by the target node it forwards it to the attacker 2 over the wormhole link between them. As the colluding attacker 2 receives the RREQ packet, transmit it to the destination node. The destination node on its part sends a RREP packet back to the target node over the wormhole link between the colluding attackers. In order to present them as a legitimate route, the colluding attackers forward the RREP packet to the target node. After they are picked up by the target node for the transfer of the data as authentic users within MANET, the attackers can intercept the data flow, i.e. receive the information and does not forward it to the end user (destination node), or selectively forward data packages in order to not being caught.

Many numbers of techniques have been proposed on securing routing protocols along idea range of security threat attacks. A study of these techniques is given in this section.

A. Vani and D. Rao proposed a scheme that combines three techniques based on hop count, decision anomaly and neighbour list count methods. In hop count based mechanism if the difference between the numbers of hops of the two routes is greater than a certain value called the Threshold value, the sender assumes that a wormhole exists. In anomaly detection, neighbouring nodes of a wormhole node notice that the wormhole node has extreme capacity of competition in path discovery. In Neighbour List Based Detection method secure neighbour discovery from source to destination is obtained by neighbour list and detect the anomaly if attack is present.

R. Maheshwari et al. presented an algorithm that uses connectivity information and look for forbidden substructures in connectivity graph. The presence of wormhole influences the network connectivity by creating long links between two sets of nodes located potentially far away. The resulting connectivity graph thus deviates from the true connectivity graph. The algorithm uses local connectivity information which means that every node looks into connectivity of its k-hop neighbours.

L. Hu and D. Evans used directional antennas to prevent wormhole attacks. They present cooperative protocol called neighbour discovery protocol in which nodes share directional information to prevent wormhole endpoints from behaving as false neighbours. The approach to detect wormhole attacks depends on nodes maintaining accurate sets of their neighbors. An important property of directional antennas is that a node can get approximate direction information based on received signals. From this information assumptions about the network can be done. As directional information is combined with effective protocols, attacks become increasingly difficult to execute successfully.

V. Kumar and A. Kush presented a new secure routing protocol known as Worm Secure protocol. The basic idea of the Worm Secure protocol is to detect the wormhole node using an algorithm to find alternative routes to a target node that does not pass through the wormhole. This approach is based on hop count analysis. In Worm Secure protocol after getting the route from the source to destination in routing table, sender will set a second hop node as a target node from the route which is stored in routing table. One hop neighbours find alternate paths to target node, if the hop count of alternate path is greater than threshold then it is considered as wormhole.

K. Win [14] presented algorithm that combines method used in the DaW –Defence against Wormhole security model, monitoring nodes and calculation of trust for wormhole detection. Whenever routing takes place in the network, analysis of the frequencies of links in different routes is done. If any of the links are suspicious, then the available trust information is used to check if the link is that of a wormhole. In the trust model used, nodes monitor their neighbours based on their packet drop pattern and not on the measure of number of drops.

3. PROBLEM STATEMENT

Previously the works done on security issues i.e. attack (Worm-Hole attack) involved in WSN were based on proactive routing protocol. Worm-Hole attack is studied under the AODV routing protocol and its effects are elaborated by stating how this attack disrupt the performance of WSN. Very little attention has been given to the fact to study the impact of Worm-Hole attack in WSN. There is a need to address both these types of protocols as well as the impacts of the attacks on the WSN for detecting and preventing security threat based on AODV routing protocol.

The AODV routing protocol is a popular reactive routing protocol in wireless networks, but AODV routing protocol designed for better performance of the network not for security of node, secure protocols are generally designed to have features such as authentication, integrity, confidentiality and non-repudiation. For security purpose AODV have vulnerabilities and it is easily manipulate by malicious node to destroy its network routing.

The open nature of wireless medium also makes it easy for outsider attackers to interfere and interrupt the legitimate traffic. This concept classifies the attacks into two broad categories, namely Passive and Active attacks. In Passive attack, the adversary only eavesdrop upon the packets content, while packets may get dropped or altered on way in case of Active attacks. Worm-hole attack is one of the Denial of Service attacks effective on the network layer, that can affect network routing, data aggregation and location based wireless security. The Worm-hole attack may be launched by a single or a pair of collaborating nodes. In commonly found two ended Worm-hole, one end overhears the packets and forwards them through the tunnel to the other end, where the packets are replayed to local area. It either drops or selectively forwards the packets, leading to network disruption. Worm-hole attack does not require MAC protocol information as well as it is immune to cryptographic technique. This makes it very difficult to detect. The main purposes are following as:

1. Analyze and simulate the AODV protocol in MANET.
2. Analyze and simulate the impact of Worm-hole attack on AODV in detail for various scenarios.
3. Propose a technique for detection of malicious node under Worm-hole attack in AODV.
4. Propose a technique for prevention of malicious node under Worm-hole attack in AODV and analyze its performance.
5. Simulate and analyze its performance of modified AODV and compare with the normal AODV.

4. PROPOSED TECHNIQUES (MODIFIED HOP COUNT ANALYSIS APPROACH)

This research work proposes an efficient technique to detect and prevent wormhole attack without the need for special hardware or strict location or synchronization requirements. The proposed technique makes use of variance in routing information between neighbors to detect wormholes. The detection technique uses an approach based on hop count. The wormhole affected routes are distinguished from legitimate routes by analyzing the hop count value of all paths. The basic idea of the technique is to discover alternative routes to the destination. These alternative routes will be extensively dissimilar in length i.e. the lengths of the alternative paths are invariably greater than the path including wormhole tunnel. The basic idea behind this approach is illustrated in below section.

The objective of this research was to detect and prevent wormhole attacks in AODV routing protocol which has been done in the proposed technique based on hop count analysis approach. The basic idea behind the proposed technique is using hop count as a parameter to distinguish paths containing wormhole tunnel.

The basic idea of hop count analysis is illustrated in figure 3.1. Mostly the routes contain larger hop count value for example hop count value is 5 and 6 in the network shown in figure, to establish connection between source node and destination node. While the hop count value of the path going through wormhole tunnel will be much smaller, in this case the value of hop count is 2. It can be explained as, consider a source node which wants to communicate with a destination node. If source node communicates through the wormhole tunnel then it encounters only 2 hops. But the other possible alternative routes comprise 5 or 6 hops to transfer a packet from the same source to destination nodes. Thus it can be a basic approach that the route path having too small hop count value or the path having invariably smaller number of hops may be unsafe. So the proposed technique is that by avoiding the route paths having too short hop count value the wormhole tunnel can be kept away.

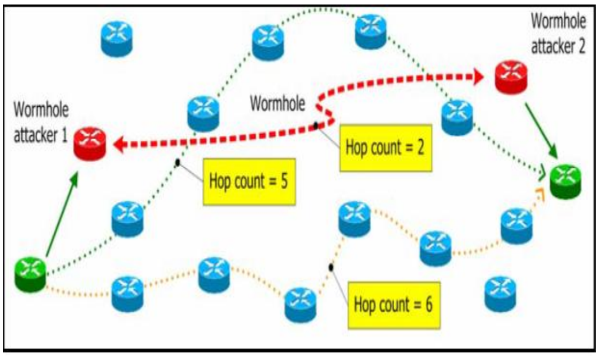

Figure 4.1 Compare hop count values of all availableroutes linking source node and destination node

In the proposed detection technique, hop count values of all the available route paths is calculated first. Source node then verifies the one hop neighbours and accordingly a threshold value is set, which is used for comparing the number of hops of the current route with the next available route. If the length of the new route differs extensively compared to the length of the preferred path followed by AODV then it can be concluded as a wormhole attack.

4.1 Algorithm of the proposed hop count based detection technique

In the proposed technique, any node not necessarily the source node, which is set in detect mode uses this hop count analysis approach to detect and prevent wormhole attack. Whenever any node sends the RREQ packets and in turn start receiving RREP packets, it follows the below mentioned algorithm using the checkpath( ) function module in AODV routing protocol implemented in ns-2.

The algorithm is repeatedly executed in ns-2 in every 0.1 seconds. The purpose of repeatedly checking the routes is to ensure that the wormhole attacker nodes should not get included in the selected path for packet transmission from source to destination because of the RREP packet sent by the malicious nodes. This is possible because the malicious node sets the highest sequence number and lowest hop count which is one in the RREP packet.

4.2 Modified Hop-count Analysis Algorithm (MHCAA):

1. To detect wormhole in AODV, all the available paths to the destination are checked one by one through routing table.
2. To check the paths, AODV determines number of hops and each one-hop neighbour is verified.
3. If there is one hop neighbour, it is legitimate and threshold is incremented by 1, otherwise it is decremented. This way a threshold value is set.
4. Then the next alternative path is checked in similar manner and number of hops is calculated which again defines a new threshold value.
5. Source node compares length of selected route with alternative path by comparing number of hops and threshold.
6. If the number of hops of the considered route is greater than the set threshold, it is concluded that wormhole exists.
7. On detecting malicious route, the corresponding next hop entry is deleted, so that now that suspected neighbour is not used for routing.
8. Similarly other paths are examined using the step 5 – 10.

The research work proposes a solution based on specification-based intrusion detection technique to monitor the AODV routing protocol and detect wormhole attack on AODV. The proposed approach involves the use of a counter for specifying correct AODV routing behavior and individual nodes monitor the routing behavior of their neighbours for detecting run-time violation of the specifications. In addition, one additional field, count in the RREP message is proposed to enable the monitoring. Another important modification is that RREP packets are broadcasted as opposed to unicast to the source in normal AODV.

5. SIMULATION OF PROPOSED TECHNIQUE

The simulation of the work completed in three scenarios. The configuration of scenarios is based on the number of nodes are deployed and the position of the source node and destination node. Initially all nodes in each scenario are normal and no malicious node is present in the scenario. The standard AODV routing algorithm is used at routing protocol on network layer. The scenarios are differentiated as per normal scenario, scenario with malicious nodes and scenario with proposed technique;

Scenario 1: It describes the normal situation of mobile ad-hoc networks with normal AODV routing protocols.

Scenario 2: It described impact of wormhole attack using Tunnel and impact of wormhole attack on performance of ad-hoc networks.

Scenario 3: it implements the proposed technique to detect and prevent wormhole attack in mobile ad-hoc networks.

Table 5.1 demonstrate the evaluated performance

TIME	NO. of Nodes	Throughput (kbps)	Packet delivery ratio	Packet drop ratio	End-to-End Delay (ms)
500 sec	100	27.28	27.45	72.55	100.7
	300	39.11	43.60	56.40	129.7
	500	45.48	49.48	43.6	121.2
750 sec	100	27.71	26.02	73.98	103.9
	300	39.26	43.73	56.27	143.1
	500	42.34	45.42	54.8	119
1000 sec	100	23.42	30.29	69.71	108.8
	300	39.37	43.43	56.67	167.2
	500	40.11	42.61	57.39	116.1

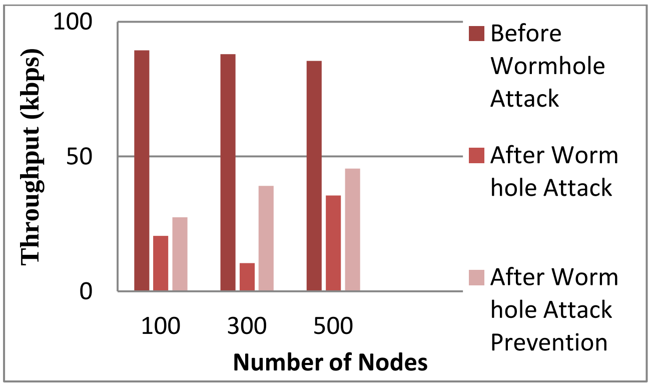

Figure 4.4: Throughput Analysis

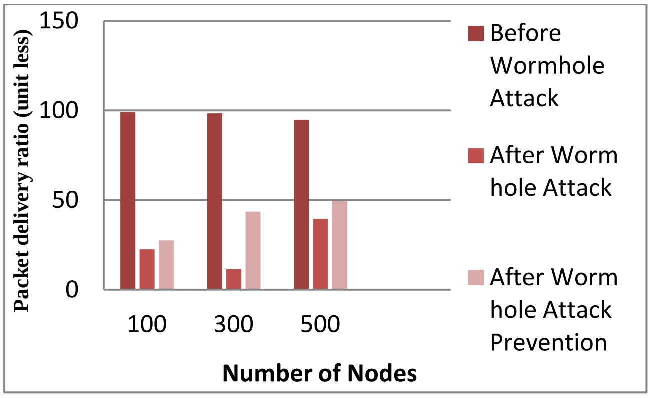

Figure 4.5: PDR Analysis

Above figure 4.4, 4.5, 4.6, 4.7 demonstrate that performance of WSN becomes less in case of wormhole attack. Furthermore, it rises by more than 60% in after integration of proposed mechanism. The complete work concludes that, proposed mechanism will not only detect malicious node but will also improve the performance on mobile ad-hoc network in case of wormhole attack.

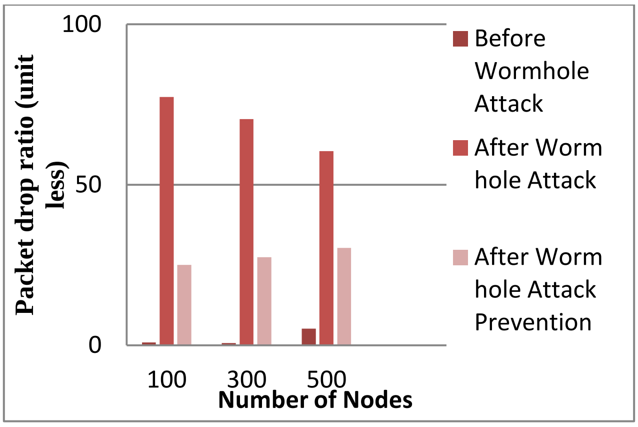

Figure 4.6: Packet Drop Ratio Analysis

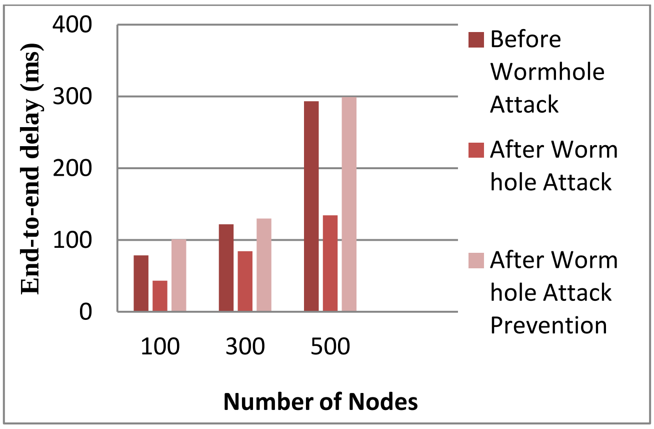

Figure 4.7: End-to-End Delay Analysis

6. CONCLUSIONS

This research work carried out the detailed study and analysis of AODV routing protocols and security issues and attacks in MANET theoretically and through simulation. This research work proposed techniques namely hop-count analysis and specification based intrusion detection for detecting and preventing wormhole attacks respectively. To evaluate the performance of proposed techniques, simulation of wormhole attacks along with the simulation of proposed techniques had been done. Simulation of security strategies provides the facility to select a good security solution for routing protocols and gives the knowledge how to use these schemes in hostile and compromised environments. Simulation results show that proposed techniques show superior performance as PDR and throughput increases however, average end-to-end delay also increases. In the analyzed scenario, it is found that the modified AODV has superior performance than AODV. Modified AODV is suitable to detect and prevent wormhole attack. It improves the PDR under attack conditions, with a minimal decrease in throughput and acceptable increase in end-to-end delay.

7. REFERENCES

[1] Tarek Mosbah Abdala “Performance Tradeoffs of Routing Protocols in Wireless Sensor Networks” International Conference on Network security &

Computer Science (ICNSCS-15) Feb. 8-9, 2015 Kuala Lumpur (Malaysia).

[2] Zainab Dalaf Katheeth "Performance Evaluation with Throughput andPacket Delivery Ratio for Mobile Ad-hoc Networks" International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 5, May 2014.

[3] R.Sherine Jenny "Simulation based performance comparison of aodv, dsr, fsr routing protocol with wormhole attack." IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501 Vol.3, No1, February 2013

[4] Kapil Raghuwanshi "An Enhanced Integrated Solution for Identification and Elimination of Wormhole Attack in MANET" International Journal of Computer Applications (0975 – 8887) Volume 110 – No. 7, January 2015.

[5] A.Vani and D. S. Rao, "A Simple Algorithm for Detection and Removal of Wormhole Attacks for Secure Routing in Ad Hoc Wireless Networks", International Journal on Computer Science and Engineering (IJCSE) ISSN: 0975-3397 Vol. 3, No. 6, 2011.

[6] L. Hu and D. Evans "Using Directional Antennas to Prevent Wormhole Attacks" , In Network and Distributed System Security Symposium (NDSS 2004), San Diego, California, USA. February 2004.

[7] D. B. Roy, R.Chaki and N. Chaki, "A new cluster-based wormhole intrusion detection algorithm for mobile ad-hoc networks" International Journal of Network Security & Its Applications (IJNSA), Vol. 1, No.1, 2009.

[8] D. S. Kushwaha, A. Khare and J. L .Rana, "Improved Trustful Routing Protocol to Detect Wormhole Attack in MANET", in International Journal of Computer Applications, Vol. 62, No.7, 2013.

[9] S. Yi, P. Naldurg and R. Kravets, "Security-Aware Ad-hoc Routing for Wireless Networks", Report No.UIUCDCS-R-2002-2290, UIUC, 2002

[10] H. Deng, W. Li, and D. P. Agrawal, "Routing Security in Wireless Ad Hoc Networks", Telecommunications Network Security, IEEE Communications Magazine, Vol. 40, No. 10, pp 70-75, 2002.

[11] Z. Alishahi, J. Mirabedini and M. K. Rafsanjani, "A new method for improving security in MANETs AODV Protocol", Management Science Letters 2 (2012) 2271–2280.

[12] K. S. Win, "Analysis of Detecting Wormhole Attack in Wireless Networks", World Academy of Science, Engineering and Technology 24, 2008.

[13] Maurice Chu International Journal of High Performance Computing Applications, Scalable Information-Driven Sensor Querying and Routing for Ad Hoc Heterogeneous Sensor Networks

[14] S.M. Jen, C.S. Laih, and W.C. Kuo, "A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET", Sensors 2009.

[15] K. Win, "Analysis of Detecting Wormhole Attack in Wireless Networks", World Academy of Science, Engineering and Technology 24, 2008.

[16] L. Qian, N. Song and X. Li, "Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks through Statistical Analysis of Multi-path"

[17] Xu Su Rajendra V. Boppana, "On Mitigating In-band Wormhole Attacks in Mobile Ad Hoc Networks", in proceedings of IEEE Communications Society, ICC 2007.

[18] R. Maheshwari, J. Gao and S. R Das, "Detecting Wormhole Attacks in Wireless Networks using Connectivity Information",

[19] V. Kumar and A. Kush, "Worm Secure Protocol for Wormhole Protection in AODV Routing Protocol", International Journal of Computer Applications, Vol. 44, No.4, 2012.

[20] K. Win, "Analysis of Detecting Wormhole Attack in Wireless Networks", World Academy of Science, Engineering and Technology 24, 2008.

[21] X. Wang and J. Wong, "An End-to-end Detection of Wormhole Attack in Wireless Ad-hoc Networks"