International Journal of Computer Security & Source Code Analysis
(IJCSSCA), 2017, Vol3, Issue3, ISSN (O): 2454-5651

Detection and Prevention of Wormhole Attack in Wireless Sensor Network using Beacon Node

Rahul Jain, Varsha Namdev
RKDF Institute of Science & Technology, Bhopal (MP)
rahul.jain1300@gmail.com

Abstract: The wormhole attack is considered a serious threat to the security in multi-hop ad hoc networks. In wormhole attack, the attacker makes the tunnel from one end to another network, the nodes are in a different place at both ends of the tunnel believe are true neighbors and gets the conversation through the wormhole link . Unlike many other ad hoc routing attacks, worm hole attack cannot be prevented by cryptographic solutions because intruders or create new or modify existing packages, but before existing. In this thesis a simple technique to effectively detect attacks wormholes without any special hardware and / or location or timing of the stringent requirements proposed. The proposed technique allows the use of the variance in routing information between neighbors to detect wormholes. Basic thesis is to find the alternative path from the source to the second jump and calculate the number of hops to detect wormhole.

Keywords: MANET, IDS, Network security, Active Attack, Passive Attack, K-Means, Clustering, Game Theory.

I. INTRODUCTION

Sensor Network is a temporary network and a set of wireless mobile nodes without the use of central access, infrastructure or central administration. There are many features in custom mobile networks that have real features like dynamic network topology, limited bandwidth and network power restrictions. The main reason for this is the constant change in the topology of the network, due to the high degree of mobility node [14].

A number of protocols have been developed to accomplish this task. Some of them are DSP and UDF routing protocols. To maintain communication on the network must be able to feel and discover with neighbouring nodes, but the transfer of MANET network interfaces is very limited. Therefore, to exchange data within the node in the network, multiple network "jumps" may be required.

One of the simple ways of routing is to send packets to the destination of the source node through the media nodes using engineering information for all nodes in the network. Obtaining accurate engineering information is still not easy. Where, one is from another stretch of road that has been actively identified to request all neighbours to obtain information on the shortest route to the destination [5-9].

II. Mobile Ad-hoc Network

Sensor network are communication networks that all mobile contracts and communicate with each other through wireless communication. There is no fixed infrastructure. All nodes are the same and there is no central control or overview. No specific routers: All nodes can act as routers with each other, and node-to-node data packets are sent in multi-hop mode.

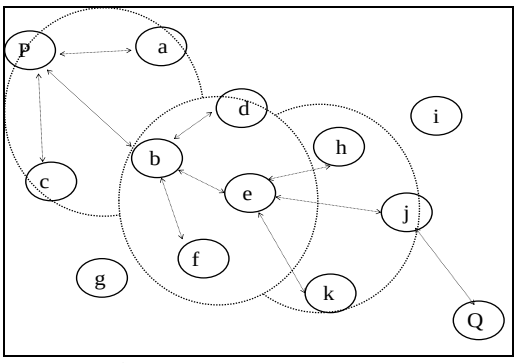

Figure 1: MANET Structure

Sensor network is a type of dedicated wireless network that is a self-configuring network of mobile routers connected by wireless connections - a federation that forms an arbitrary topology. Routers, compromising nodes act as a router, are free to move randomly and arbitrarily managed. Therefore, the wireless network topology can change quickly and unpredictably. This network can operate independently, or it can be connected to the Internet morethere are many characteristics of MANET. Some of them are describe here-

- **Dynamic Topologies:** The contract is free to move arbitrarily. The network topology can change randomly and has no limits on the distance between it and other nodes. As a result of this random move, the entire topology changes in an unpredictable manner, this in turn leads to both unidirectional titles and links between the nodes.
- **Energy Constrained Operation:** Almost all nodes in a dedicated network rely on batteries or other integral means to power them. The battery runs out due to the extra time the node is making to survive the network. Therefore, energy conservation is a standard design improvement is important.
- **Bandwidth Constraint:** Wireless connections have much less capacity [10] than infrastructure networks. The production of wireless communications is much lower due to the effect of multiple access, fading, noise and interference conditions. As a result, congestion becomes an obstacle in the use of bandwidth.
- **Limited Physical Security:** Sensor Network are generally more prone to physical security threats than wireless networks because the ad hoc network is a distributed system and all the security threats relevant to such a system are pretty much present, as a result, there is an increased possibility of eavesdropping, spoofing, masquerading[16-20], and denial-of-service type attacks.
- **Scalability:** Networks can be large, typically more than 10 nodes and up to 1000 nodes in a sensor network. Consequently, routing protocols must be able to expand this amount. A number of algorithms have been proposed,

which can be classified as proactive or reactive protocols.

III. WORM HOLE ATTACK

In a wormhole attack, two attacker nodes join. An attacker node receives packets at one point and "tunnels" Forward to another node via a private network connection, and then played on the network.

Wormhole attack is a relay-based to attack the routing protocol is interrupted and thus interrupts or failure of a network and, for this reason, this attack is serious. We can use 4 steps to explain a general attack worm hole.

- An attacker has two trusted nodes in two different networks with a direct link between the two nodes places.
- Attacker logs packets to a location on a network.
- Tunnels Striker after packages stored in a different location.
- Attacker sends packet to the network location from step 1.

The simple wormhole in the network is shown in figure 2. Here, node 2 and node 8 create the tunnel in order to work as a malicious node. Both nodes give the illusion to another node that there is a shortest path. But this shortest path does not exist and attack can easily perform by the attacker.

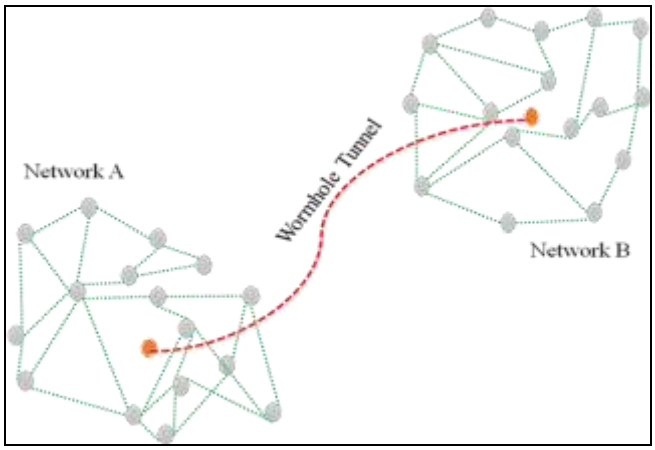

Figure 2: Example of Wormhole

IV. PROPOSED METHODOLOGY

Proposed methodology of wormhole detection and prevention is based on beacon node Based scheme [4] and neighbor node based solution of wormhole problem. The main theme of the proposed technique is to discover wormhole in the route suggest by AODV protocol by using the divide and conquer technique. In which, wormhole detection is performed between all the possible combination of node to its next to next node. Finally, decision will be taken on the basis of each and every possible combination.

If wormhole is detected in any of possible combination then whole suggested path is consider being as wormhole effect path. Elsewhere if all the combination is wormhole free then path is consider to be as worm hole free path. In proposed methodology every node responsible to find out, is there any worm hole between that nodes to it's next to next node.

For detection, every node find alternate route for its next to next node as suggested by AODV expect via AODV suggest. If number of hop count in any of alternate route is greater than threshold than that node reply wormhole detection signal between itself and its next to next node. Algorithm for wormhole detection is described below in algorithm 1.

Algorithm for Wormhole Detection and Prevention

Assumption-

1. $N^{i}_{MANIT} = Mobile\ adhoc\ network\ having\ i\ mobile\ node$
2. $M = \{X_i | X_i \text{ is } i^{th} \text{ mobile node} \in N^{i}_{MANIT}\}, Set\ of\ Mobile\ node$
3. $NN^{Xi} = \{Y_i | Y_i \text{ is } i^{th} \text{ neighbour node of } X_{ith} \text{ mobile node} \in N^{i}_{MANIT}\}$
4. X^{b}_{i}= Beacon node
5. X^{d}_{i} = Detecting node
6. N^{i}_{MHD} = Maximum hop distance X^{b}_{i} and X^{d}_{i}

Algorithms

1. {
2. Step 1:- Source node ($\mathbf{X_S}$) call AODV and broadcast RRP to all there $\mathbf{NN^{Xs}}$ path towards their desired destination ($\mathbf{X_D}$)
3. Step 2:- Every $\mathbf{NN^{Xs}}$ uni-cast Route reply packet (RRP) to $\mathbf{X_S}$
4. $Ri^{Xd}_{Xs} = X_s, Y_1, Y_{1+1}, Y_{1+1+1}, \ldots, X_d$
5. Step 3:- for every route Ri^{Xd}_{Xs}
6. Do ( )
7. {
8. Y_i Broadcast RRP for Y_{i+2}
9. neighbour node of Y_i reply hop distance Between Y_i & Y_{i+2}
10. MHD[i] = hop distance
11. While ($Y_i != X_d$)
12. }
13. If (MHD[i] > N^{i}_{MHD})
14. Then
15. Reply "Wormhole is present in route Ri^{Xd}_{Xs}"
16. Exit ( );
17. Else
18. Goto Step 3
19. }
20. "Reply route Ri^{Xd}_{Xs} is selected for transmission"
21. }

In proposed algorithm, all decision will be taken on the basis of value of maximum hop distance i.e. maximum number of hop distance in alternate route between every pair of beacon node and detecting node is discover by AODV. If it's greater than maximum hop distance, then it's declared there is wormhole between beacon node and detecting node, elsewhere not.

In proposed methodology main focus on how to calculate maximum hop distance of the network for a fixed number of node. Proposed methodology use an evolutionary model that use beacon node concept along with neighbor node concept. In beacon node concept every node have a GPS system to coordinate their position over the network but use very large amount of battery power, this is bottle nick of this system.

To overcome this demerit proposed methodology combine the feature of neighbor node information scheme with beacon node scheme in order to overcome the demerit of both being alone.

In proposed methodology, for calculating maximum hop distance each and every node behave like beacon node and

find the path having the largest number of node over the entire possible path between it and it's detecting node and consider average value highest hop distance of the entire node as maximum hop distance over the network as describe in algorithm 2.

Algorithm for Maximum hop distance between beacon node and detecting node (N^{i}_{MHD})

Assumptions-

1. $max_{hopcount} = 0$

Algorithms

1. {
2. $for\ (x_i = 1, x_i \leq n, x_{i++})$
3. {
4. Select neighbor node of x_i as y_i
5. $for\ (y_i = 1, y_i \leq m, y_{i++})$
6. {
7. Select neighbor node of y_i as z_i
8. $for\ (z_i = 1, z_i \leq k, z_{i++})$
9. {
10. X_i call AODV broadcast RRP for Z_i
11. AODV reply hop distance
12. $max^{i}_{hopcount}$ = hop distance
13. }
14. }
15. }
16. $N^{i}_{MHD} = \frac{\sum_{i=1}^{n} max^{i}_{hopcount}}{\sum_{i=1}^{n} x_i}$
17. }

V. SIMULATION DETAIL & PERFORMANCE MEASURE

To implement this concept, the aodv.cc file was modified. When the simulation is started, the command is called. Each setting is related to the hole in this function. The functions for creating mobile nodes are added by reading the file node ID in this functionality. The script calls this function to create the cluster game in the simulation.

Table 1: Simulation Detail

Parameters	Values	
Number of Nodes	Vary from 40 to 100	
Area	40	600*300
	50	600*300
	100	1000*800
Traffic	CBR	
Simulation Duration	100 Mili Seconds	
Packet Transmission Rate	1024 kbps	
Carrier sense threshold Used In Normal Nodes	200 Meter	

The performance metrics which are used to analyze the performances of routing protocols in heterogeneous ad hoc networks are discussed in the following: In the figure 5, it is shown that when the number of nodes increases the routing load is also increases.

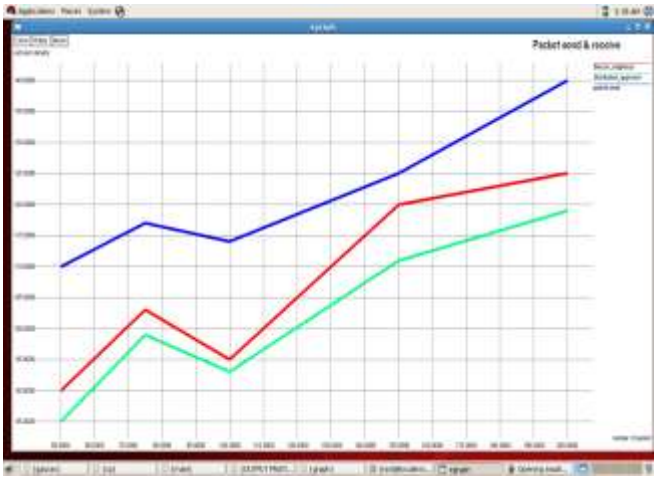

Figure 5: Packet Send & Receive Rate

In the second scenario the simulation will be done with 72 nodes with same assumptions. After that, we take same scenario with 84, 100 and 200 nodes. Also analysis the ratio of packet sends and receive rate of both proposed and existing technique as shows in figure 5.

Table 1: Number of packet received

Network Density	Packet Sent	Packet Received by Beacon	Packet Received by Distributed
50	110	90	85
100	117	103	99
125	114	95	93
150	125	120	111
200	140	125	119

Energy consumption: In proposed beacon & neighbor node mechanism wormhole recognition is perform over that path suggested by AODV over P-2 node if path having P hop distance. As per describe in distributed approach every intermediate hop required two joule for sending control packet via detecting wormhole. Distributed approach required additional one joule energy by every beacon node for sending and receiving their GPS coordinate. So total energy use to detect wormhole via distributed approach in worst case is O(P*3) joule.

Whereas, proposed beacon & neighbor node concept only P-2 hop play a role to detect wormhole along with that there is not any requirement to use GPS system. So total energy required to detect wormhole in worst case is O(P-2*2) joule .

Mitigation Percentage:-

The number of mitigate packets in different network density are shown in table 2.

Table 2: Number of Mitigate Packets

Network Density	Distributed	Beacon (Proposed)
50	11945	11956
100	12225	12233
125	12567	12679
150	12789	12678
200	13987	13598

The above observation shows that the detection technique works efficiently but having some overhead, control packet as mitigation percentage is also increases in the graph, but the benefit of this technique is that it detects the wormhole, and will serve as an advantage when added to the existing AODV protocol. The results of mitigation percentage are shown in figure 6.

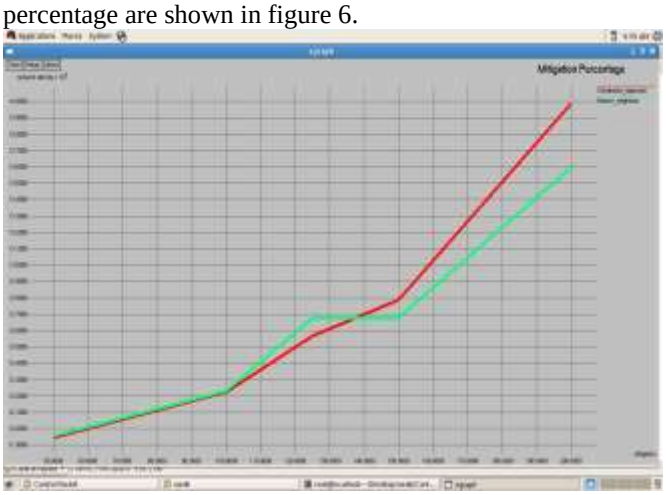

Figure 6: Comparison of Mitigation Percentile between Distributed and Beacon Neighbor Node Concept

It shows that when the number of nodes increases the value of mitigation percentage also being increases.

VI. CONCLUSION

The wormhole is a major problem in the field of wireless network. To take this problem as a challenge this work has proposed an approach to detect and prevent the wormhole attack from the network. This is some kind of defensive mechanism. This is beacon neighbor node approach to defense wormholes in mobile ad-hoc network. The approach uses the two methods having their own limitation. This work uses the positive points of these approached and combined it. The performance of proposed technique is depending upon network density, having lower FNR ratio with network having larger number of node. Along with that proposed technique required lower power backup for wormhole detection along with that its required lower mitigation percentile and higher packet send and receive ratio as compare to existing one.

REFERENCE

[1] N. Marchang, R. Datta and S. K. Das, "A Novel Approach for Efficient Usage of Intrusion Detection System in Mobile Ad Hoc Networks," in IEEE Transactions on Vehicular Technology, vol. 66, no. 2, pp. 1684-1695, Feb. 2017.

[2] Y. Zhang, et Al., "Artificial immune system based intrusion detection in a distributed hierarchical network architecture of smart grid," IEEE, Power and Energy Society General Meeting, San Diego, CA, pp. 1-8, 2014

[3] T. S. Bharati and R. Kumar, "Secure intrusion detection system for mobile adhoc networks," 2nd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, pp. 1257-1261, 2015.

[4] G. Indirani and K. Selvakumar, "A swarm-based efficient distributed intrusion detection system for mobile ad-hoc networks MANET", Int. J. Parallel Emerg. Distrib. Syst., Vol 29, Issue 1, pp. 90-103, Jan 2014.

[5] S. Sumit, D. Mitra and D. Gupta, "Proposed Intrusion Detection on ZRP based MANET by effective k-means clustering method of data mining," International Conference on Reliability Optimization and Information Technology (ICROIT), Faridabad, pp. 156-160, 2014.

[6] D. Du and H. Xiong, "A dynamic key management scheme for Sensor Network," Proc. of Cross Strait Quad-Regional Radio Science and Wireless Technology Conference, Harbin, pp. 779-783, 2011.

[7] A. Kumar, K. Gopal and A. Aggarwal, "A complete, efficient and lightweight cryptography solution for resource contrainst Mobile Ad-Hoc Networks," 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, Solan, pp. 854-860, 2012.

[8] S. Balfe, et Al. "Key Refreshing in Identity-Based Cryptography and its Applications in Sensor Network", IEEE, Military Communications Conference, Orlando, FL, USA, pp. 1-8, 2007.

[9] Z. Narmawala and S. Srivastava, "Survey of Applications of Network Coding in Wired and Wireless Networks" in Proc. of the 14th National Conference on Communications, pp. 153-157, February 2008.

[10] R. Sheikh, M. S. Chande and D K Mishra, "Security issues in MANET: A review", IEEE, pp 1-4, 2010.

[11] J P Anderson, "Computer security threat monitoring and surveillance" Technical report, James P. Anderson Company, Fort Washington, Pennsylvania, 1980.

[12] S. Sumit, D. Mitra, and D. Gupta, "Proposed Intrusion Detection on ZRP based MANET by effective k-means clustering method of data mining" IEEE, 2014.

[13] K. P. Karmore and M. S. Nirkhi, "Detecting Intrusion on AODV based Mobile Ad Hoc Networks by k-means Clustering method of Data Mining" International Journal of Computer Science and Information Technologies, Vol 2, Issue 4, pp. 1774-1779 2011.

[14] G. Indirani and K. Selvakumar, "A swarm-based efficient distributed intrusion detection system for mobile ad hoc networks (MANET)", International Journal of Parallel, Emergent and Distributed Systems, Vol 29, Issue 1, pp. 90-103, 2014.

[15] B. Y. Bhavsar and C. K. Waghmare, Intrusion Detection System Using Data Mining Technique: Support Vector Machine", International Journal of Emerging Technology and Advanced Engineering, Vol 3, Issue 3, pp. 581-586, 2013.

[16] S. S. Panwar and Y. P. Raiwani, "Data Reduction Technique to analyze NSL-KDD set", International Journal, Vol 5 Issue 10, pp.21-31, 2014.

[17] B. K. Nakayama, H. Y. Nemoto and N. Kato, "A survey of routing attacks in mobile ad hoc networks", IEEE, pp 85-91, 2007.

[18] M. K. Verma, S. Joshi and N. V. Doohan, "A survey on: An analysis of secure routing of volatile nodes in MANET", IEEE, pp 1-3, 2012.

[19] P. Papadimitratos and Z. J. Haas, "Secure Routing for

Mobile Ad Hoc Networks" in Proc. of CNDS, 2002.
[20] K. Sanzgiri, et Al., "A Secure Routing Protocol for Ad-Hoc Networks" Proc. of IEEE, ICNP, 2002.
[21] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing", IEEE, pp 25-26, 1999.
[22] M. Nouri, S. A. Aghdam and S. A. Aghdam, "Collaborative Techniques for Detecting Wormhole Attack in Sensor Network", IEEE, pp 1-6, 2011.
[23] A. Modirkhazeni, et Al., "Distributed Approach to Mitigate Wormhole Attack in Wireless Sensor Networks", IEEE, pp 122-128, 2011.
[24] A. A. Mariannne, "Wormhole Attacks Mitigation in Ad- Hoc Networks", IEEE, pp 561-568, 2011.
[25] Jin Guo, Zhi-yong Lei, "A Kind of Wormhole Attack Defense Strategy of WSN based on Neighbor Nodes Verification", IEEE, pp 564-568, 2011.

