International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 04
February 2018

Detection and Prevention of Wormholes Based on Range-Free Localization Scheme

Nnochiri I.U
Department of Computer Science Department,
Michael Okpara University of Agriculture, Umudike

ABSTRACT
Mobile ad-hoc networks (MANET) are particularly vulnerable to a severe attack known as the wormhole attack. A few existing protocols detect wormhole attacks but they require special hardware. This research paper aims at developing detection and prevention model against Wormhole attack based on a range free scheme which does not requires an addition costs.The proposed model is easy to deploy: it does not require any especial hardware, like, time synchronization or GPS; nor does it require any complex computation. The performance of this proposed model shows a high detection rate under various scenarios. Proposed model achieves a detection rate about 99.7% versus 99.2% for Secure-AODV model and a detection accuracy rate 98.4% versus 97.1 for Secure-Ad Hoc On demand Distance Vector (AODV).

Keywords: Mobile ad-hoc networks, Ad Hoc On demand Distance Vector (AODV), Wormhole, Free scheme

1 INTRODUCTION

With development of new technologies in the field of wireless communication, especially in wireless ad-hoc networks, mobile ad-hoc networks (MANET) have become an important research area nowadays. MANET is widely used in militarily monitoring, heath care, conference room, disaster relief, battle field communication and it is also useful also where infrastructure network deployment is either difficult or costly [1].

In most wireless networks, an attacker can easily inject bogus packets or impersonating another sender. An attacker can also easily eavesdrop on communication, record packets, and replay the packets that potentially altered. Due to the nature of wireless communications in MANET's and among the many attacks in wireless networks, a wormhole is one of dangerous and specific attacks, that attacker does not require to exploit nodes in the network, and it can be done via the route foundation method [2].

Many existing protocols attempt to solve the problem of determining a node's location within its environment. With regard to the mechanisms used for estimating location, it is divided into two categories: range-based and range-free. Solutions in range-free localization are being pursued as a cost-effective alternative to more expensive range-based approaches.

In the proposed model, a major contribution will made to the wormhole problem in MANETs; a new model proposed to tackle wormhole attack based on range-free scheme and a simulation will be conducted to validate the effectiveness of our proposed model.

2.0 MANET's

Mobile Ad hoc networks (MANET) are a new paradigm of wireless communication formobile hosts (nodes). In an ad hoc network, there is no fixed infrastructure such as mobileswitching centers or base stations. Mobile nodes that are within radio range can communicatebetween each other; while those that are out of range of wireless link depend on other nodes torelay messages as routers. Node mobility in ad-hoc networks are changing frequently causingchanges of the network topology. Figure 1 shows such an example: initially, nodes A and D havea direct link between them. When D moves out of A's radio range, the link is broken. However,the network is still connected, because A can reach D through C, E, and F.

In early days, Ad-Hoc research was mainly focused on military networks, but nowMANET's can be used in environments like conference room, disaster relief, battle fieldcommunication and it is also useful, where deployment of infrastructure network is either costlyor difficult [1].

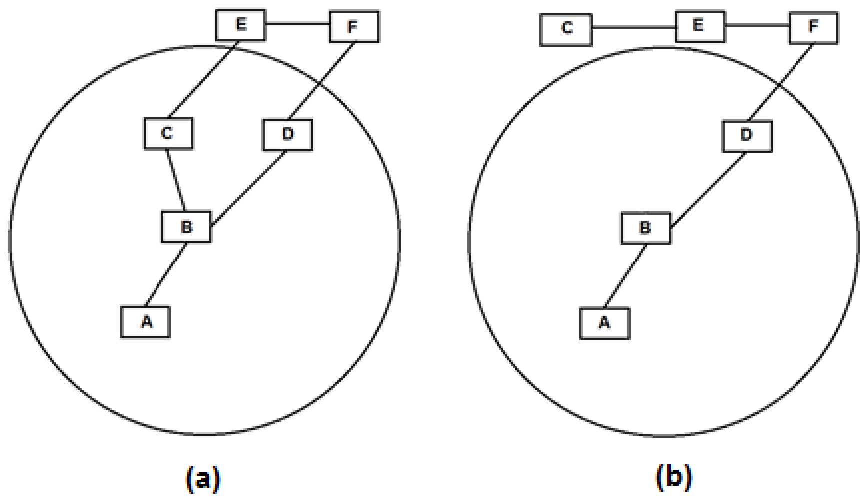

Figure 1: Topology Change in Ad-Hoc Networks [1](a) Before (b)After

MANET is a collection of mobile nodes or devices, such as mobile phones, personal dataassistant (PDA), laptops, etc. as shown in figure 2, these nodes are connected over a wirelessmedium [3]. Each node in MANET not only acts as host but also as router that route datafrom/to other nodes in network.
Use of wireless medium and inherent collaborative nature of the network protocols makesuch network vulnerable to various forms of attacks. In most wireless networks, an attackercan easily inject bogus packets or impersonating another sender. An attacker can also easilyeavesdrop on communication, record packets, and replay the packets that potentially altered[4].

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 04
February 2018

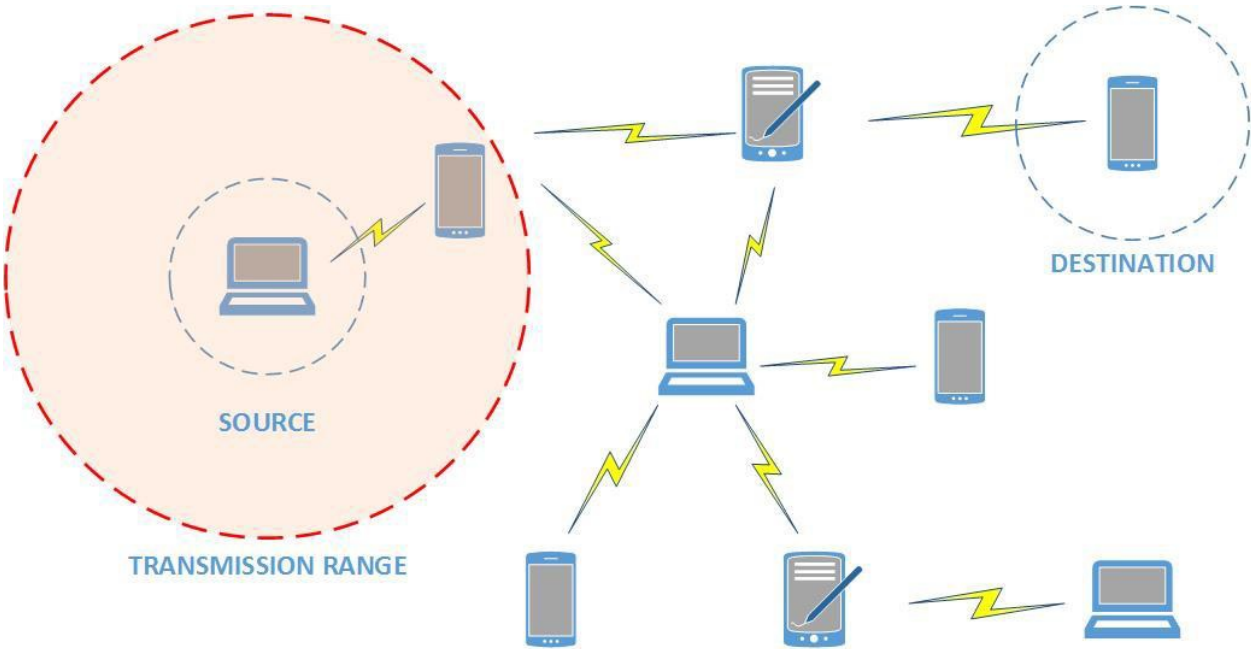

Figure 2: Mobile Ad-Hoc Network [3]

2.1 Security issues in MANET's

Developing foolproof security protocol for MANETs is tough task [5]. This is mainlybecause of certain uniqueness of Ad-hoc mobile network, namely, common broadcast radiochannel, insecure working environment, lack of central administration and limited availabilityof resources.

For instance, the early routing protocols, such as AODV and DSR protocols were notdesigned to provide or guarantee privacy and communication anonymity, rather they wereaimed at increasing network performance, efficiency, security, and reliability.

In general, the main security requirements in any system are: confidentiality, integrity,availability. Confidentiality ensures that eavesdroppers will not be able to intercept theinformation sent through the network which may be achieved by encryption mechanisms.

Integrity will insure that packets will not be altered or modified by adversaries. Finally,Availability implies that the network services must be available to all legitimate usersregardless of any malicious events. There are many different aspects to consider in order classifying attacks in MANET's [6]. They can be classified into passive and active attacksdepending on how much the attacker is involved. Also, these attacks can be classified dependson the domain of the attack. They can be classified into internal and external attacks.

3.0 METHODOLOGY

3.1 The Proposed Model Characteristics

The PROPOSED protocol has four main important characteristic which plays a role in ourprotocol to work effectively. These characteristics are listed as following:

1. Localization procedure: The localization process will maintain every node locationfor future routing need.

2. **Neighborhood table**: Every node in the network will maintain a neighborhood tablewhich will consists of node ID of the neighbor nodes. As the network we areimplementing is a uniform one hence the node will be in set in matrix format hence wecan easily get the neighborhood table.

3. **Trust factor**: Each node in neighborhood table given a trust value, it is measures theaccuracy and

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 04
February 2018

sincerity of the immediate neighboring nodes by monitoring theirparticipation in the packet forwarding mechanism.

4. **Detection and Prevention procedure**: The algorithm detects wormhole node and itscolluding node based on intermediate node trust factor value. Then, Wormhole andcolluding nodes IDs are now blacklisted.

Figure 3 shows how a packet in normal condition transmits from source S to destinationD, the packet will not travel out of its transmission range. If a packet from S is received by Aor B directly then there is a possibility of presence of wormhole in the network.

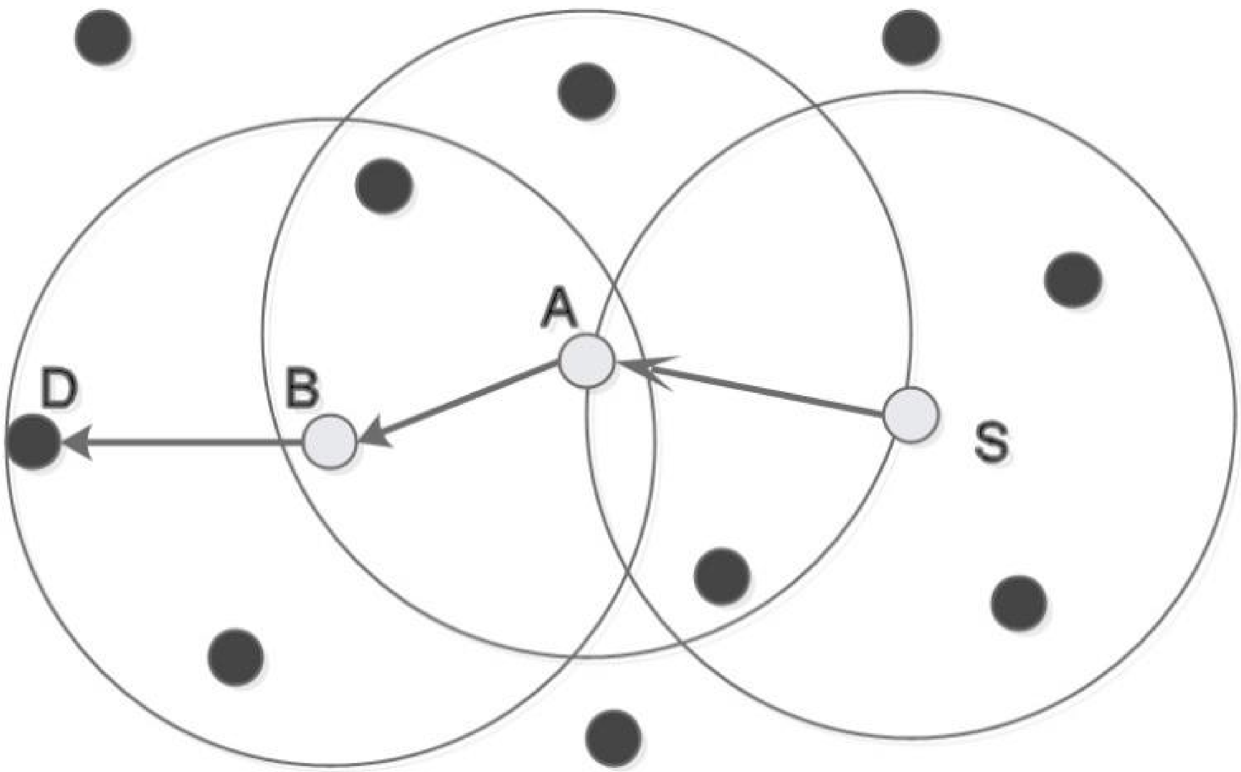

Figure 3: Normal packet transmission [6]

3.2 The Proposed Model - General Overview

A general overview of the proposed model is described in figure 4. The modelconsists of four main steps:

1. Localization Process.
2. Trust Factor Model.
3. Route Establishment.
4. Wormhole Detection and Prevention.

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 04
February 2018

Figure 5: Proposed Model for Wormhole Detection and Prevention [6]

3.2.1 Localization Process

1. Generate random nodes.
2. Choose anchor nodes randomly.
3. Localize all nodes using Selective 3-Anchor DV-hop algorithm.
4. Assign a trust value for all of anchors neighbors.

3.2.2 Build TFactor "Trust Factor Model"

5. Each anchor broadcast **HELLO**.
6. Neighbor nodes reply.
7. Each anchor build **Neighbor_list(anchor)** "Anchors' neighbor list"
8. Compare all anchors' neighbor lists and calculate common nodes.
9. Common nodes increment **TFactor**. More common nodes more **TFactor**value.

3.2.3 Route Establishment

10. Source nodes sends**RREQ** to all its neighbors.
11. Intermediate nodes forward **RREQ** until match destination address otherwise repeatuntil destination not found.
12. Destination node unicast **RREP**.
13. RREP Contains: **hop_count**, **Neighbor_list(Dest)** "Destination's neighbor list"
14. To check wormhole detection go to **STEP 17**.
15. Rout from source to destination established.
16. Source node stores **Neighbor_list(Dest)** and **hop_count**.

3.2.4 Wormhole Detection and Prevention

17. Check weather **Node location** within anchor communication Range.
18. If yes, wormhole may exist.
19. Check **Neighbour_list(Dest)**, if node **TFactor< threshold**.
20. If yes, wormhole exist.
21. Send Announce to all nodes.
22. Any node has wormhole id within **Routing_Table**, it removes it.
23. Re-initiate route establishment process in **STEP 10**, to find new route to destination.

4.0 RESULTS

To evaluate the proposedmodel, average hop-count, wormhole detection rate and wormhole detection accuracy rate isused. An analysis conducted through simulation by presenting proposed model to a non-adversarial model as proposed in most secure routing protocols [7], and provide adetailed analysis of the obtained simulation results.

4.1 Simulation Setup

We developed an event driven simulator by using Matlab [8]. The Matlab software usedto set up the simulation environment and to visualize the obtained results after computing theactions of all nodes between routing processes.

4.2 Simulation Parameters

In our simulations and as in [9], it isassume that physical layer has a fixedcommunication range pattern, i.e. two nodes can directly communicate with each othersuccessfully only if they are in each other communication range. We randomly deployed 50nodes within an area of 100 x 100 meters. A fraction of these nodes was randomly selected towormhole misbehave. The Trust Factor value of each node is initialized to TFactor = zero.

Simulations are implemented with one source node and one destination node. The source nodeis located at the most left-bottom region of the simulation area, while the destination node isplaced at the most right-upper area of simulation environment. This assumption ensures thatour results are representative of a long multi-hop path from source to destination; also, itpermits potential failures at various distances from the source. Each experiment was repeatedfor 100 random network topologies. A brief summary of the basic simulation parameters arelisted in Table 1.

Table 1: Simulation Environment

parameters	**values**
Simulation Area	1000 x 1000 (m)
Number of nodes	50
Number of wormhole nodes	1, 2, 4, 8, 16
Communication Range	250 m
Routing Protocol	Modified AODV
Node Speed	10 m/s

4.3 Performance Evaluation Metrics

The evaluation of the proposed model is measured in accordance to the following threemetrics:

i. **Average Hop-Count**: Average hop count per route refers to the Total Hop Count ofdemands over Number of demands as in [8].

$$\text{AverageHopCount} = \frac{\text{TotalHopCountOfDemand}}{\text{NumberOfDemand}} \quad (1)$$

ii. **Detection rate**: which is the ratio of the number of nodes that are possibly attacked by awormhole to the number of how many of them are successfully detected as in [9].

Equation 2 is used to determine the wormhole detection rate:

$$\text{DetectionRate} = \frac{\text{TotalDetectedWormholes}}{\text{TotalWormholes}} \quad (2)$$

iii. **Detection Accuracy**: It is the ratio of the number of links declared as attacked by awormhole to the number of how many of them are actually affected as in [9]. Thefollowing formula is used to determine the detection accuracy:

$$\text{DetectionAccuracy} = \frac{\text{TotalDetectedWormholes}}{\text{TotalActualWormholes}} (3)$$

4.3.1 First Scenario

The simulation parameters that used in first scenario are a MANET with different sizes.Here, we assume the network size are 20, 30, 40 and 50 nodes and are randomly distributed in1000m×1000m area. No wormhole nodes are considered in these experiments. The scenario issimulated for 100 times. Experiment results listed in table 2 and figure 6 shows the resultsof average hop-count according to different network size.

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 04
February 2018

Table 2: No-Wormhole Scenario

No. of Nodes	Average hop-count
20	5.6
30	6.3
40	6.65
50	**7.9**

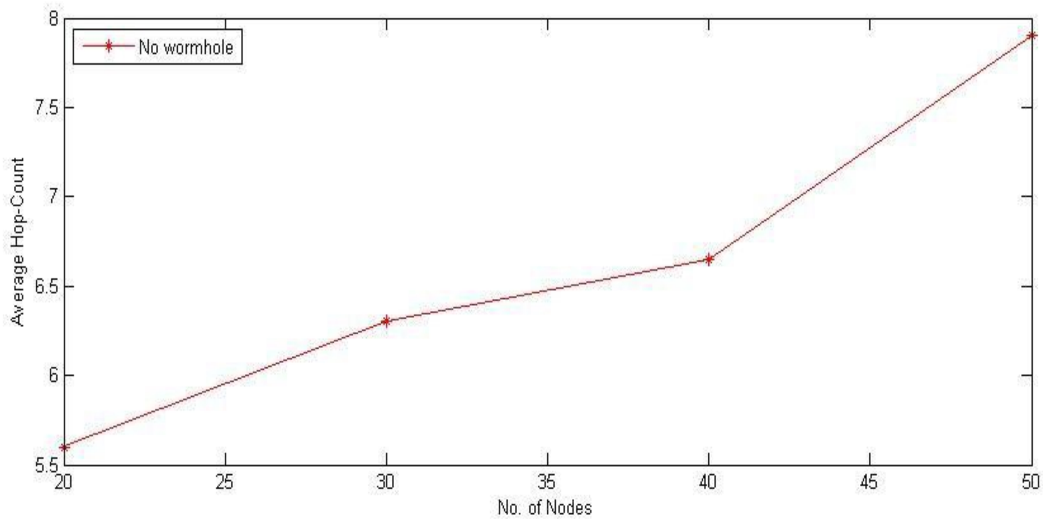

Figure 6: No-Wormhole Scenario

4.3.2 Second Scenario

A simulation conducted with same simulation parameters that used in above scenarioexcept that two wormhole nodes are considered. Results listed in table 3 and figure 7depicts the results of average hop count according to assumed parameters.

Table 3: Two Wormhole Nodes

No. of Nodes	Average hop-count
20	4.37
30	5.4
40	6
50	7.63

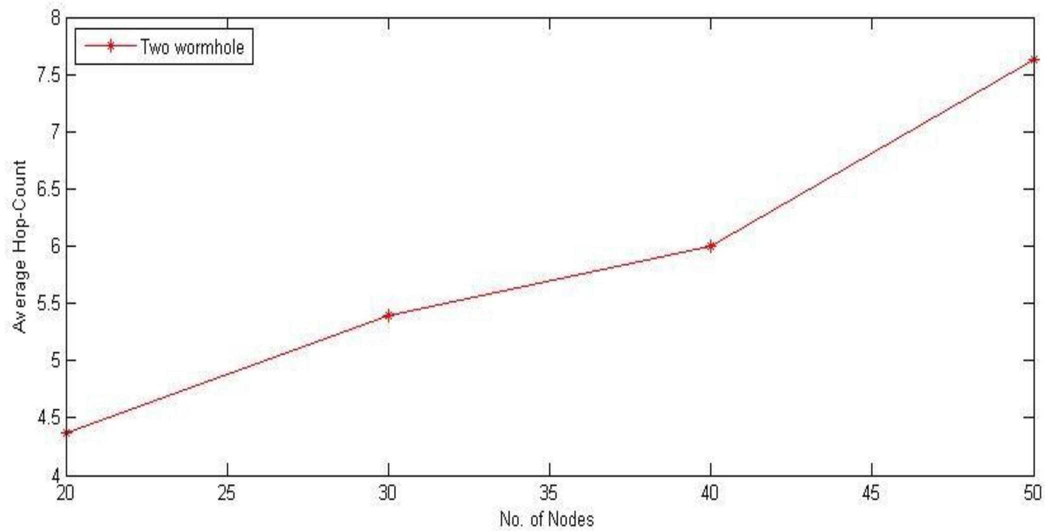

Figure 7: Two Wormhole Nodes Scenario

4
.3.3 Third Scenario

Another simulation results listed in table 4 and figure 8 depicts these results for aneight wormhole nodes. A significant change in average hop-count depicted compared to firstand second experiments and this lead us to a conclusion that hop-count play an important rolein detecting wormhole attack.

Table 4: Eight Wormhole Nodes

No. of Nodes	**Average hop-count**
20	3.2
30	4.18
40	5.75
50	7.01

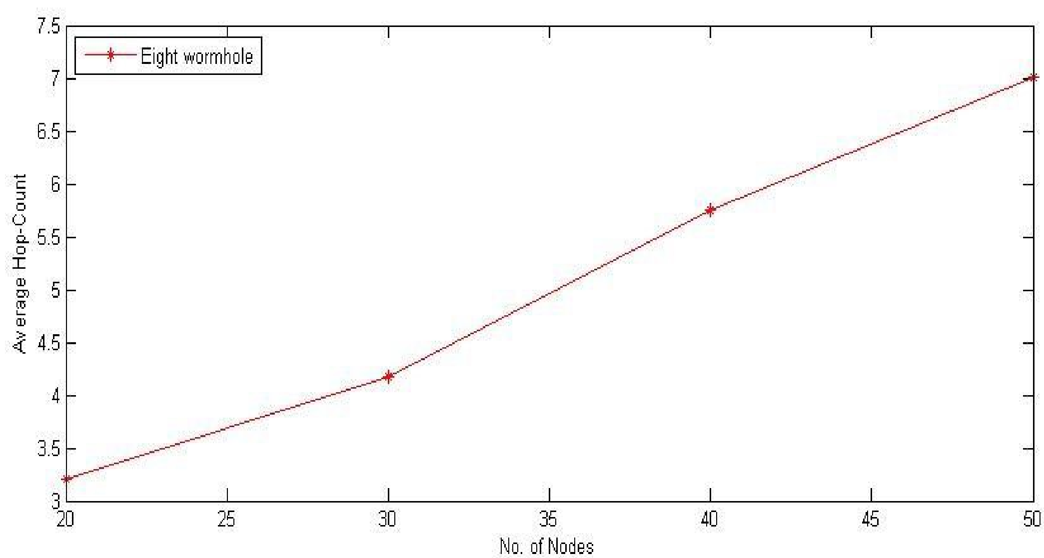

Figure 8: Eight Wormholes Nodes Scenario

4.4 Performance Evaluation

All scenarios with different network sizes are obtained. In the following graph, figure 9, x-axis represents number of nodes and y-axis representsthe average Hop-Count. A comparison between number of nodes and the average hop-countobtained for every different scenario presented. We change the number of nodes from 20 to50. We can find that as the number of wormhole increases, the average hop-count decreasesrapidly. Thus, Hop-count metric gives us a good pointer for an existence of wormhole.

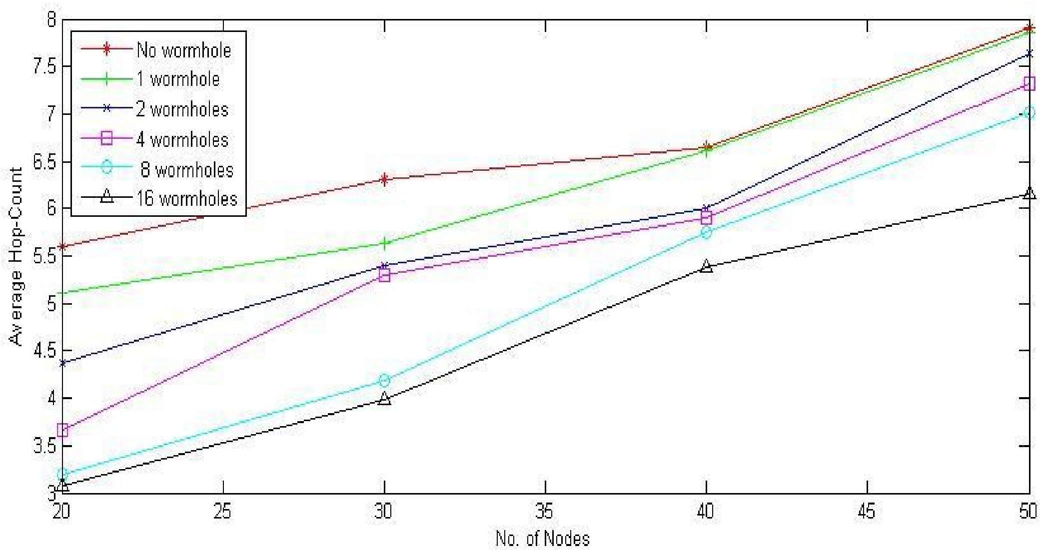

Figure 9: Relation between number of nodes and number of Hop-Count

Calculating Average Hop-Count Metric:

Average hop-count metric calculated by the equation 1, we obtain the total hop-count fordifferent number of wormholes in each routing model Secure-AODV and our proposed model.

In Secure-AODV, the total Hop-Count of demands was 685, 680, 615, 567 and 497 andnumber of demands was 100. So, the averages Hop-Count are 6.85, 6.8, 6.15, 5.67, and 4.97respectively. In the proposed model, the totals Hop-Count of demand were 779, 737, 712, 673and 596 and the number of demands was 100. So, the average hop-count are 7.79, 7.37, 7.12,6.73 and 5.96 respectively.

In table 5, i listed the experiments results obtained for different wormhole nodes tomeasure average hop-count. In figure 10, the performance of the proposed model is evaluated.

The performance of our proposed model is compared with AODV routing protocol and normalmode without any secure routing protocol. Non secure scenario, in blue line, shows the averageroute length in normal situation, and it will be used as a reference for the performance ofproposed model. With a detection and prevention to wormhole scenario in green used AODVrouting protocol, the graph shows a decrease in average hop-count. In the proposed model, thegraph shows an increase in average hop-count which indicates that now the nodes avoidingmalicious path effectively.

Table 5: Results obtained for different wormhole nodes

No. of Wormholes	Secure-AODV	Proposed Model
1	6.85	7.79
2	6.8	7.37
4	6.15	7.12
8	5.67	6.73
16	4.97	5.96

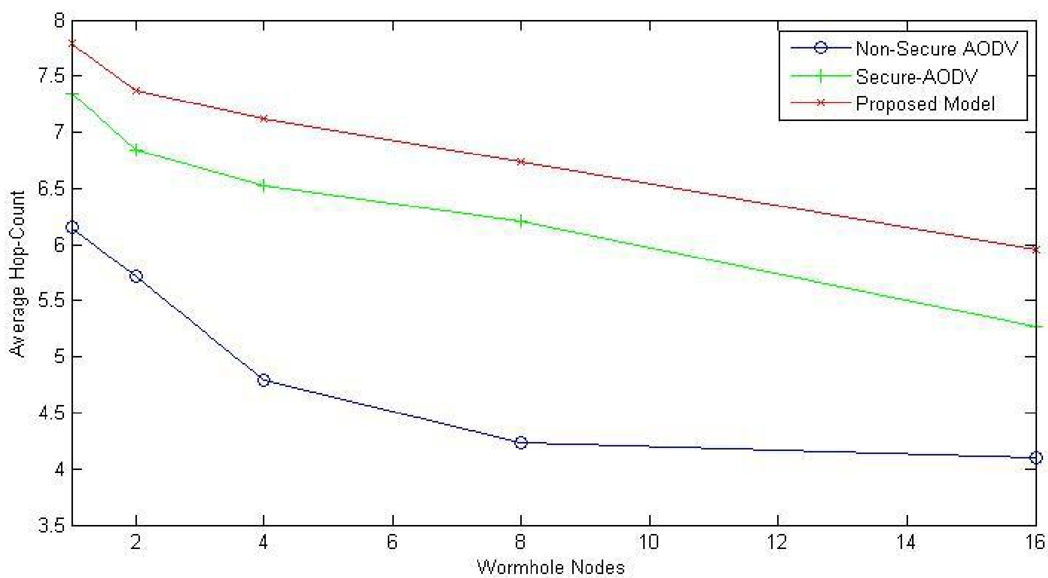

Figure 10: Number of wormholes vs Average Hop-Count

5.0 CONCLUSION

Wormhole attacks in MANET significantly degrade network performance and threat to network security. Wormhole attacks are severe attacks that can easily be launched even in networks with confidentiality and authenticity. Malicious nodes usually target the routing control messages related to topology or routing information. In this research, i have presented an effective model for detecting and preventing wormhole attacks in DVHOP. To detect wormhole tunnels, i used hop-count metric which inherited from routing protocol. The proposed model is easy to deploy: it does not require any especial hardware, like, time synchronization or GPS; nor does it require any complex computation. The performance of this proposed model shows a high detection rate under various scenarios. Proposed model achieves a detection rate about 99.7% versus 99.2% for Secure-AODV model and a detection accuracy rate 98.4% versus 97.1 for Secure-AODV.

REFERENCES:

[1] Zhou L. and Z. J. Haas, (2009).“Securing ad hoc networks,” IEEE Netw., vol. 13, no. 6, pp. 24–30, 2009.

[2] RoyerE. and C. Toh, (2010) “A review of current routing protocols for ad hoc mobile wireless networks,” Pers. Commun. IEEE, no.April, pp. 46–55, 2010.

[3]Yi S., P. Naldurg, and R. Kravets, (2011) "Security-aware ad hoc routing for wireless networks,"Symp. Mob.ad hoc Netw. 2011.
[4] KärpijokiV., (2012) "Security in ad hoc networks," Semin. Netw.Secur., pp. 1–16, 2012.
[5] HuY., A. Perrig, and D. Johnson, (2013)."Packet leashes: a defense against wormhole attacks in wireless networks," INFOCOM 2013.Twenty- …, vol. 00, no.C, 2013.
[6] PerkinsC. and E. Royer, (2009) "Ad-hoc on-demand distance vector routing," … WMCSA'2009. Second IEEE Work., 2009.
[7]Kong J. and X. Hong, (2010). "ANODR: anonymous on demand routing with untraceable routes for mobile ad-hoc networks," … Int. Symp.Mob.ad hoc Netw. …, pp. 291–302, 2010.
[8] ZhangY., W. Liu, W. Lou, and Y. Fang, (2016) "Mask: Anonymous on-demand routing in mobile ad hoc networks," Wirel. Commun.…, vol. 5, no. 9, pp. 2376–2385, 2016.
[9] DefrawyK. El and G. Tsudik, (2011)"ALARM: anonymous location-aided routing in suspicious MANETs," Mob. Comput.IEEE Trans. …, pp. 1–14, 2011.
[10] HeG., (2012"Destination-sequenced distance vector (DSDV) protocol," Netw. Lab. Helsinki Univ. 2012.

.