An Energy Efficient Approach for Wormhole Detection and Prevention

Gaurav Sharma
Department of Electronics & Communication Engineering,
SIRT, Bhopal

Mehajabeen Fatima
Department of Electronics & Communication Engineering,
SIRT, Bhopal

ABSTRACT
Now these day multi- hop wireless Ad-hoc network suffer from number of security threat namely wormhole attack. Wormhole attacks make an tunnel that attracted all the communication over the network in order either scan message over packet , drop the packet or for unwanted consumption of battery power of Ad-hoc network. In this paper a wormhole detection and prevention scheme has been proposed in order to save battery power. Proposed scheme upgrade neighbor node information scheme for wormhole detection by encapsulating hop count scheme. Basically in neighbor node scheme there is problem for selection of threshold value. Proposed methodology overcomes that problem by using hop count scheme under that decision. Recently research will focus over wormhole detection and prevention but existing technique having very higher false negative rate and battery consummation along with overloaded control packet and routing overhead. In this paper a wormhole detection and prevention technique has been proposed which is based neighbour node and hop count method.

Keywords
Adhoc network, Wormhole Attack, Statistics and Graph Based scheme, AODV

1. INTRODUCTION
Wireless network refers to a network, in which all the devices communicate without the use of wired connection. Wireless networks [1] are generally implemented with some type of remote information transmission system that uses electromagnetic waves, such as radio waves; for the carrier and this implementation usually takes place at the physical level or "layer" of the network. Mobile ad hoc network is a part of wireless network [2] which is a self-configuring network that is formed automatically by a set of mobile nodes without the help of a fixed infrastructure or centralized management.

The wormhole attack is a serious threat for mobile ad-hoc network. And it cannot be detected easily. For detection of the wormhole attack in MANET a technique has been proposed. In a wormhole attack, two attacker nodes join together. One attacker node receives packets at one point and "tunnels" them to another attacker node via a private network connection, and then replays them into the network [3]. The wormhole puts the attacker nodes in a very powerful position compared to other nodes in the network. In the reactive routing protocols such as AODV, the attackers can tunnel each route request packets to another attacker that is near to destination node [3,4]. When the neighbors of the destination hear this RREQ, they will rebroadcast this RREQ and then discard all other received RREQs in the same route discovery process.

As mentions in above paragraph wormhole attack have a best impact on the network, it must attract a large amount of network traffic which is done by giving a shortest route to destination in the network. Therefore, the routes going through the wormhole must be shorter than alternate routes through valid network nodes.

Also it is seen that most of the previous approaches for detection of wormhole shows dropped performance and have relative higher complexity [5,6,7,8,9]. As the mobile nodes operate on the limited power of battery therefore it becomes very necessary to develop a technique which can successfully defend against wormhole attacks while maintaining lesser complexity[10,11,12].The objective of this dissertation is to develop a new approach which can successfully defend against wormhole attacks.

2. PROPOSED SOLUTION
Proposed algorithms check the validity of route suggested by AODV protocol whether the route is infected by wormhole attack or not on the basis of some threshold value as show in figure1.If route suggested by AODV not infected by wormhole attack the it's selected for transmission otherwise rejected and generate an signal for AODV protocol to suggest another route
Proposed scheme use Statistics and graph Based scheme [4] for wormhole detection and prevention. In order to analysis weather there is wormhole tunnel in the route suggest by AODV or not every pair of continuous three node make a combination like {N1,N2,N3},{N2,N3,N4},…..(Nn-2,Nn-1,Nn) where first node of every pair responsible to check whether the wormhole is present between its next node and next to next node. If any node Ni detect there is wormhole between Ni+1 and Ni+2 then whole route is rejected to be consider as
Wormhole affected. Whereas if every pair of combination reply wormhole free message then route is selected for message communication otherwise rejected.

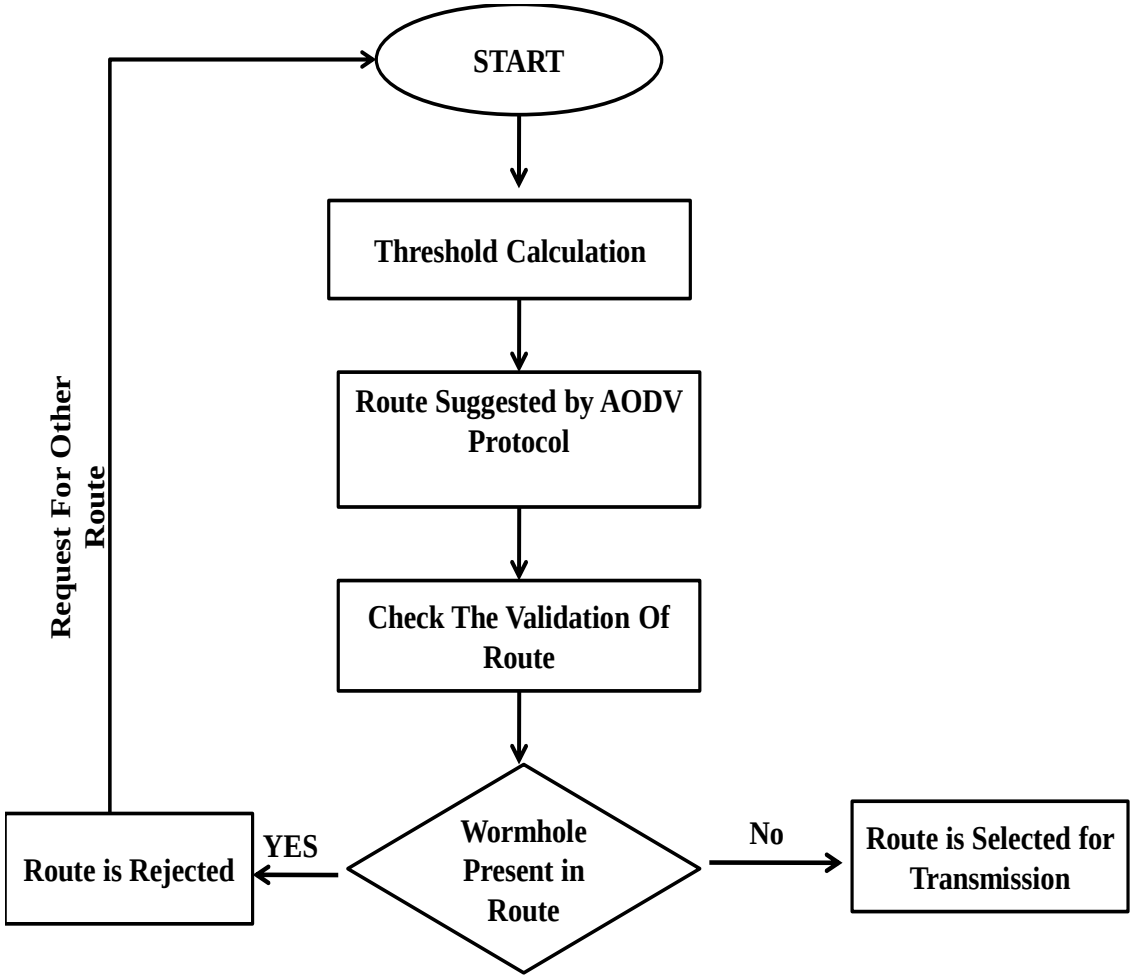

Figure 1: Flow Chart of Proposed Algorithm

In key hole of proposed scheme is value of threshold, what is the maximum number of node in between every pair radio node and neighbor of radio node.

Method for calculating value of threshold is based on fusion of hop count and neighbor node algorithm. In proposed scheme value of threshold is calculated on the basis of hop count methodology with the help of neighbor node information. For calculating threshold each and every node of network find the all the possible path between itself to its next to next node on the basis of hop count suggested by AODV select largest one . Finally average of hop count of every path is suggested as threshold as explain in algorithm 1.

Algorithm1 (Threshold for wormhole detection)
{
Assumption

1. TN total number of node in network
2. Ni any arbitrary node in network
3. R(Ni) = Set of node that comes under radio range of Ni
4. |S|= cardinality of any set
5. R(R(Ni)j)= Set of node that comes under radio range of radio node j of Ni
6. $M_{HP=}$maximum number of Hop count in any route initialed with $M_{HP}=0$
7. Sum of M_{HP} sum of maximum hop count for all pair of node in network

```
For (i=1; i<=TN ;i++)

{
For (k=1; k<=|R(R(Ni))J| ; k++)

{

For (J=1; J<=|R(Ni)| ; J++)
{
```

Step 1. Ni send an route request message to its radio node R(Ni)j for R(R(Ni)j)k

Step 2. The neighbor node reply the Route through route Reply packet to Ni in term of number of hop count 'Y'

Step 3. if ($Y>M_{HP}$)

$M_{HP}=Y$

}

Sum of M_{HP}= Sum of M_{HP}+ M_{HP}

}

Threshold = Sum of M_{HP}/N

}

Proposed scheme is based on neighbor node information ie every Ni node find out alternate route for Ni+2 and if minimum of alternate route is greater than threshold proposed scheme generate wormhole presence signal and discard that route .In order to avoid wormhole path proposed scheme suggest AODV find an alternate route between source and destination expect via Ni+1 node. Algorithm for wormhole detection prevention is describing below in algorithm 2.

Algorithm:2(Wormhole Detection and Prevention Algorithm)

Assumption
S_N=Source Node
D_N=destination node
N(N)= Set of Neighbors node of Node N
NNi where i=1,2,…….n
Ri= Route suggested by Aodv

Algorithms ( )
For (i=1 ; i<= n; i++)
{
Step 1:-Source node(S_N) call AODV protocol for the route to destination (D_N) via NNi
Step 2:- AODV reply route response message

Ri=N1,N2,N3,……..Nn

And

Set WH="N"

Where N1 is source node, Nn is destination Node and Ni for 2<=i<n is intermediate node

// Now every node in route suggested by AODV is responsible for detection of wormhole.

Step3:- for (Nj=1 ;Nj<=Nn-2 ; Nj++)
{

- Ni broadcast Route request message to every of its neighbor node expect Ni+1(in Ri) for route to Ni+2
- N(Ni) reply route response message in term of number of hop count select minimum among them as R(Ni,Ni+2)

If(R(Ni,Ni+2)> Threshold)
{
Reply (WH="Y")
Exit ()
}
}
Step 4:- if (WH="Y")
{
Reject the Route Ri //
there is wormhole
Goto step 1
Else
Route Ri selected for transmission
Exit ()
}
}

3.PERFORMANCE EVALUATION

For performance evaluation of our proposed methodology, it has been compared against E2SIW [13] in term of power consumption where both protocol simulated over AODV routing protocol in NS2 for mobile ad hoc networks.

(a) Simulation Setup

In order to authenticate the proposed methodology for wormhole detection verity of simulation experiments have been performed by using NS-2 by using 50 mobile nodes and use AODV protocol for routing.

In order to validate the proposed approach a number of simulation experiments have been performed by using network simulator version 2.32. Table 1 show the parameters used in the simulation experiments. The proposed approach is tested with wormhole using a rectangular scenario of 2000 × 1500 m square area; CBR traffic is used to generate UDP packets for the simulation. In the simulation, start on 0ms and end on the 100ms. The attack will start on 25ms in the simulation and re-check on 50ms. There are different packets sizes are used in the NS-2, for this simulation 1024KB packet is used. In the simulation the carrier sensing power is defined as 200m.The wormhole is randomly created somewhere between the sender and the receiver with a random length that is uniformly distributed between the nodes. The algorithm is implemented by modifying the original AODV source code in NS-2.

Simulation Area	**2000mx1500m**
Number of Nodes	Vary from 50 to 200
Traffic	CBR

Simulation Duration	100 Milliseconds'
Packet Transmission Rate	1024 kbps
Radio range for normal node	200 Meter

Table 1 Simulation Parameters

(b) Energy Consumed

Proposed methodology for wormhole detection and prevention is based on threshold value where threshold value has been calculated on the basis of neighbor node and hop count analysis method as explain in algorithm 2 in upper section. Whereas existing E2SIW use GPS system for threshold calculation that required additional energy along with that there is a need of neighbor list that consume 1 joule of additional energy which doesn't required in proposed technique.

As per E2SIW [13] assumption 2 joule of energy consume in establishment of handshaking , control packet , data packets and storage data in memory , where values depend upon simulation and network density.

Consider path suggested by AODV protocol over network in simple scenario without attack as show in figure 2

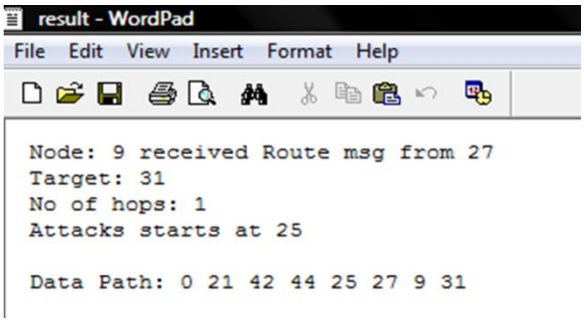

Figure 2:- Path Suggested by AODV protocol in simple scenario without attack

As

0 21 42 44 25 27 9 31

And after attack (there is tunnel between 21 and 9)

```
After Attacking :
Data Path: 0 21 9 31

Detection restart at 50

Node: 0 sending route msg to neighbours
Target to be identified 9
Data Path: 0 21 9 31
```

Figure 3:- Path Suggested by AODV protocol after attack

As

0 21 9 31

In proposed technique wormhole detection is perform over N-2 node if path having N hop count so If average 2 joule of energy consume at every node for wormhole detection then total energy consumption in AODV suggested path without attack as show in figure 2 is 12 joule in worst case is O(n-2*2)joule because path having 8 hop count and only 6 participate in taking decision .Where if wormhole present total 2 joule energy consume for wormhole detection in best case is O(2) joule this is because in best case first node catch wormhole between its next and next to next node.

Whereas in existing E2SIW wormhole detection technique is perform over total number of hop count and required additional 1 joule over each node for neighbor list so total 24 joule energy consume for wormhole detection and in E2WIS have same performance in both worst case and best case.

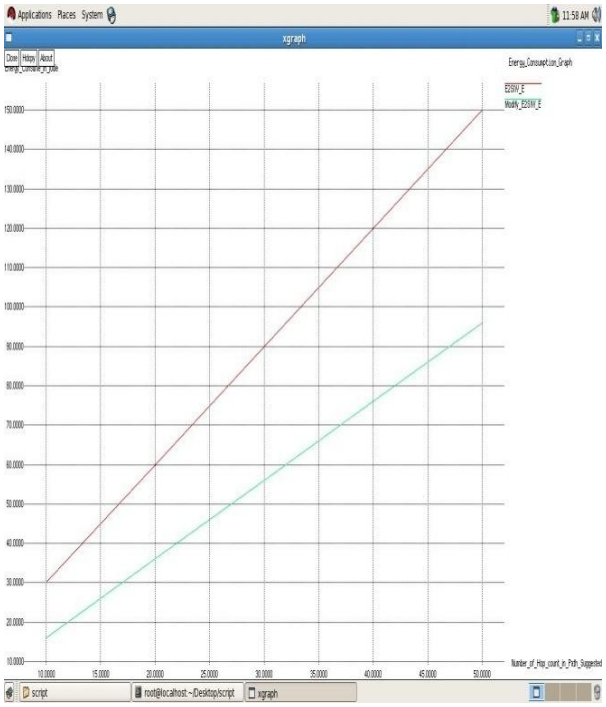

Figure 4:-Comparison graph between E2SIW and modify E2SIW for Energy Consumption

(c) False Negative Rate

False negative rate means if there is a wormhole in selected path but system generates no wormhole signal. It is need to minimized FNR ratio of any system. In proposed work accuracy depend upon density of network, highly dense lead to lower FNR ratio as show in figure 5.

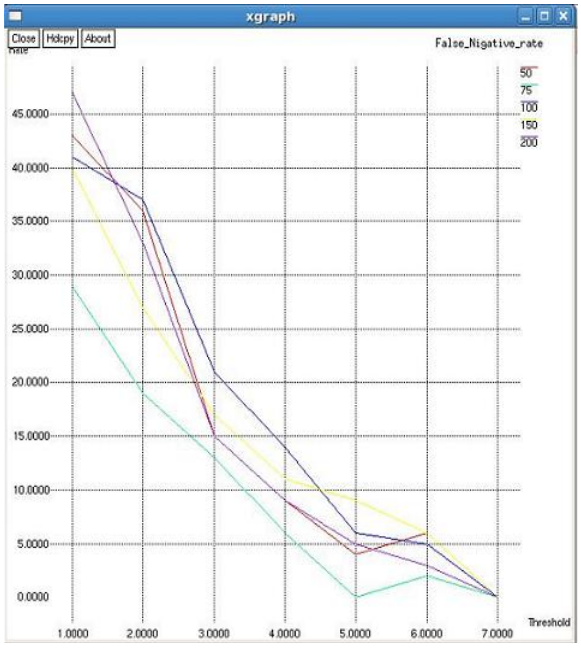

Figure 5:- False Negative Rate of Modify E2SIW in Different Scenario

(d) Control Packet

Control packet responsible for internodes communication and handshaking. Modify E2SIW required lower number of control packet as compare E2SIW because there is no need to maintain neighbor list so it is not to required to broadcast number of control packet for identification of neighbor node.

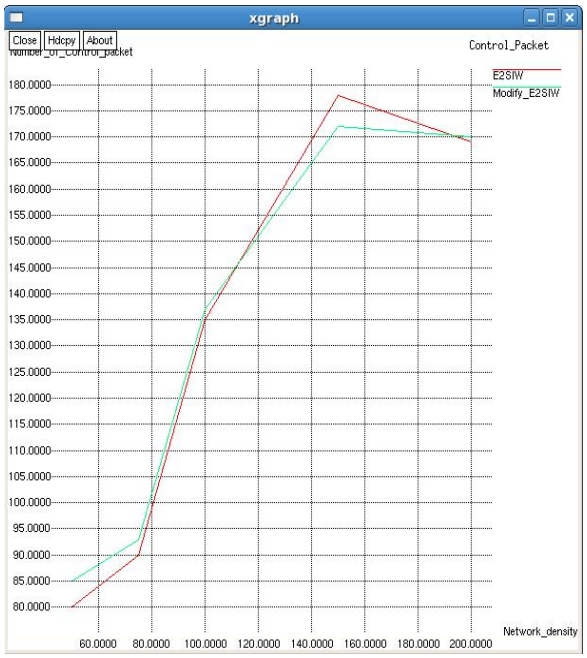

Figure 6: Comparison graph between E2SIW and modify E2SIW for number for control packet

4. CONCLUSIONS

In this paper a hybrid methodology for detecting wormholes and prevention in mobile ad hoc networks is presented. This method encapsulate advantage of two different predefine method in order to overcome their limitation. The performance of proposed technique is depending upon network density and use software approach to evaluate threshold in place of hardware used in existing technique. Along with that proposed technique required lower power backup for wormhole detection.

In order to detect wormhole proposed technique use larger number of control packet in future we will try negotiates that effect.

5. REFERENCES

[1] Maulik, R, Chaki, N. "A comprehensive review on wormhole attacks in MANET" IEEE 2010, Page 233-238.

[2] Jian Yin, Sanjay Madria, "A hierarchical secure routing protocol against black hole attack in sensor networks", IEEE SUTC, 2006.

[3] Xiangyang Li "Wireless Ad Hoc and Sensor Networks: Theory and Applications" Cambridge University Press 978-0-521-86523-4

[4] Sebastian Terence J , "Secure Route Discovery against Wormhole Attack in Sensor Networks using Mobile Agents", IEEE 2011, pp 110-115.

[5] C. Perkins, E. Belding-Royer, "Ad hoc On-Demand Distance Vector (AODV) Routing," The Internet Society 2003.

[6] Sang-min Lee, Keecheon Kim "An Effective Path Recovery Mechanism for AODV Using Candidate Node" springerlink, vol. 4331/2006, 2006.

[7] Mahajan, V. ;Natu, M. ; Sethi, A. , "Analysis of wormhole intrusion attacks in MANETS", IEEE 2008, Page 1-7.

[8] Keer, S. ;Suryavanshi, A., "To prevent wormhole attacks using wireless protocol in MANET" IEEE 2010, Page 159-163.

[9] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding- Royer, "A secure routing protocol for ad hoc networks," in Proc. of IEEE ICNP, 2002.

[10] Dang QuanNguyen ; Lamont, L., "A Simple and Efficient Detection of Wormhole Attacks", IEEE 2008, Page 1-5.

[11] KatrinHoeper, Guang Gong, "Pre-Authentication and Authentication Models in Ad Hoc Networks," Signals and Communication Technology, pp. 65-82, 2007.

[12] KanikaLakhani, Himanibathla, Rajesh Yadav "A Simulation Model to Secure the Routing Protocol AODV against Black-Hole Attack in MANET" IJCSNS International Journal of Computer Science and Network Security, vol. 10 No.5, May 2010.

[13] Sanjay Kumar Dhurandher and Isaac Woungang "E2SIW: An Energy Efficient Scheme Immune to Wormhole Attacks in Wireless Ad Hoc Networks" in 26th International Conference on Advanced Information Networking and Applications Workshops in IEEE,2012