IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 15, Issue 1 (Sep. - Oct. 2013), PP 51-58
www.iosrjournals.org

A Novel Approach to Detect & Prevent Wormhole Attack over MANET & Sensor n/w towards Lower Battery Power Consumption

Pratima Singh, Ashish Srivastava, Nitesh Gupta
Department of Computer Science and Engineering, NRI Institute of Information Science &Technology, Bhopal

Abstract: *In Mobile Ad hoc Network (MANET) mobile node is responsible for route establishment using wireless link where each node may behave like both as a host and router. MANET encounters number of security threats because of its open entrusted environment, with little security arrangement, security over MANET can be enhance up to some satisfactory level because of its inherent characteristics. Among some of the prominent security threats wormhole attack is considered to be a very serious security threat over MANET. In wormhole two selfish node which is geographically very far away to each other makes tunnel between each other to hide their actual location and give the illusion that they are true neighbours and attract other nodes to make conversation through the wormhole tunnel. Many researchers focused on detecting wormhole attack and its prevention mechanism. It seems that in the previous technique there is a need to improve their results in the brink of false negative rate, routing overhead etc. The present paper has proposed the hybrid model in order to detect and prevent the wormhole attack. This approach has been work with neighbour node and hop count method.*

Keywords: *Mobile Ad hoc Network, Selfish node, Malicious node, AODV*

I. Introduction

Mobile ad hoc network is a infrastructure less network that is self-configured automatically by mobile nodes without the help of any centralized management. In MANET nodes having special characteristics that each node in MANET behaves like receiver and transmitter and allow communicating with other nodes in its radio range. In order for a node to forward a packet to a node that is out of its radio range, the support of other nodes in the network is needed; this is known as multi-hop communication. Therefore, each node must act as both a host and a router at the same time. The network topology normally changes due to the mobility of mobile nodes in the network.

In MANET each node can communicate with the help of its neighbor node that's comes in its radio range each node forward their packet to their neighbor node towards destination where path for transmitting massage packet is suggested by routing protocol as shortest path.

Every routing protocol concentrates over shortest path where some malicious node over network use this greediness of routing protocol and present an illusion of shortest path between two end point of network and attack major traffic over the network.

Wormhole attack attract message packet and launch attack with that routing packet like scanning of confidential message, drop, corrupt and change transmitted message over network.

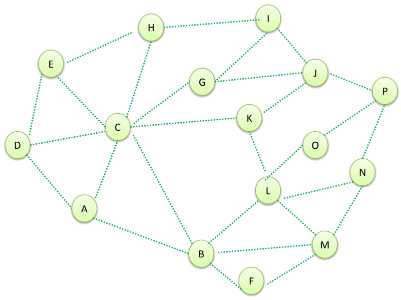

Figure 1: Mobile Ad-Hoc Network

Figure 1 shows the view of MANET where circle represent different node and connected dashes line shows wireless connection between any node to their respective radio node (neighbor node) and each node works as transmitter and receiver. So there is no need of any centralized device.

The remaining part of the paper is organized as follows: Section II discusses security issues of the Mobile Ad-hoc Network. Section III throws some light on wormhole attack and its type. Section IV gives the brief history of previous work. Section V presents problem statement. Our proposed solution is described in section VI. Finally the paper has concluded in section VII.

II. SECURITY CONSTRAINTS IN MANET

MANET is vulnerable to various types of attacks. Some attacks affect to general network, some affect to wireless network, and some are particular to MANETs. These security attacks can be classified according to different criteria, such as the domain of the attackers, or the techniques used in attacks [3]. These security attacks in MANET and all other networks can be generally classified by the following criteria: passive or active, internal or external, different protocol layer, stealthy or non-stealthy, cryptography or non-cryptography related. Among the classification of attacks, one of the prominent attack is wormhole attack.

III. WORMHOLE ATTACK

Wormhole attack is a serious threat in MANET, it attacks the traffic of network and either scan, change or drops the entire confidential message inside the packet in the time of journey of packet over the wormhole tunnel. As shown in Figure 2, during wormhole attack two malicious nodes of different network link together via some physical connection and form a tunnel and present an illusion that node X of network A is neighbor of node Y of network B. Generally wormhole puts their malicious nodes at powerful position within the network as compared to other nodes so its attract maximum traffic of network and prevents other routes instead of the wormhole from being discovered, and thus creates a permanent Denial-of-Service attack by dropping all the data, or selectively discarding or modifying certain packets as needed .

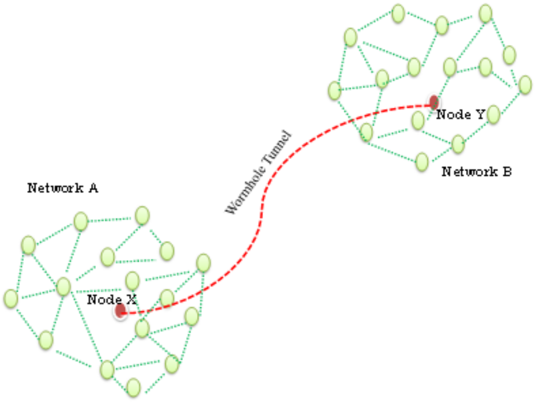

FIGURE 2: WORM HOLE

Wormhole attacks are organized in three different type namely closed, half open and open on the basis of visibility of malicious node [10] in the route discover by routing protocol. If both end point of wormhole tunnel not participate in hop count of route or hide them self then it is closed wormhole.

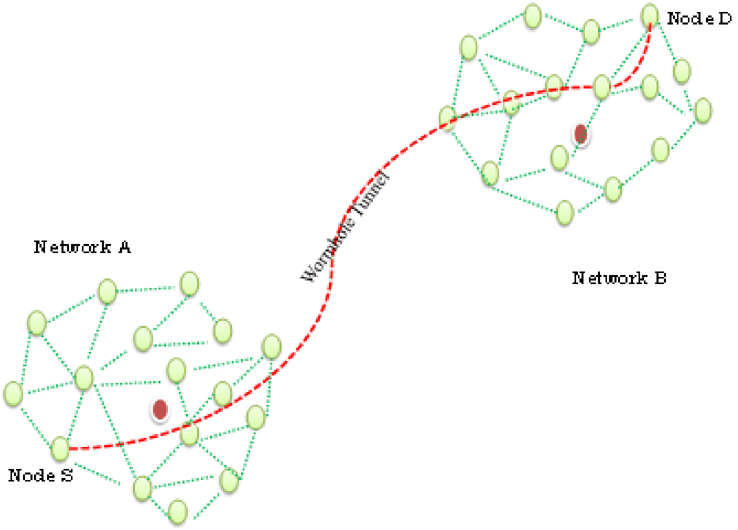

Figure 3: Closed Wormhole

Where if both end point of wormhole tunnel consider in counting of hop count or they are participate in route suggested by routing protocol, it is open wormhole.

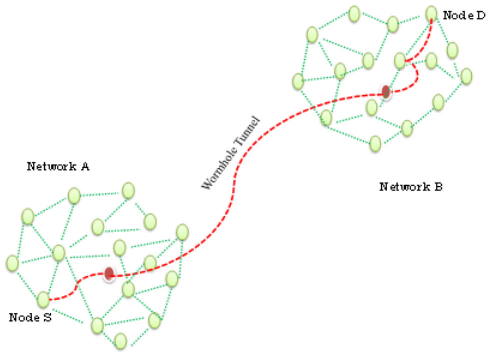

Figure 4: Open Wormhole

And if only one of either end of wormhole tunnel participate in route hop count then it is half open .

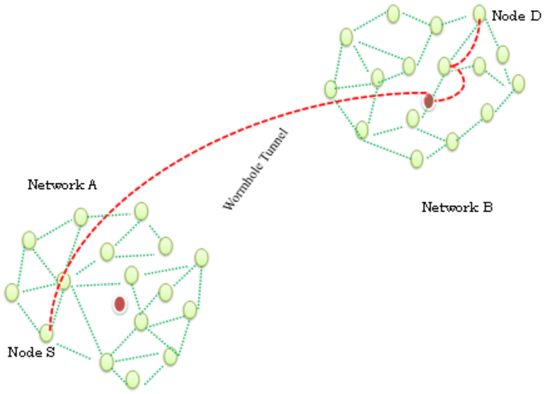

Figure 5: Half Open Wormhole

IV. RELATED WORK

Before starting this work there is a need to deep study about these methods. We had studied many research papers and found the various emerging technology and approaches. Some of them are discussed below:

Pallavi Sharma, et.al [1] proposed a solution to prevent wormhole attack that is the verification of digital signatures. In proposed solution, if sender wants to send the data to destination, firstly it creates a secure path between sender and receiver with the help of verification of digital signature. If there is presence of any malicious node in between the path then it is identified because malicious node does not have its own legal digital signature.

In [2] E2SIW, Sanjay Kumar Dhurandhar et.al use GPS system for Location information of nodes to detect the presence of a wormhole in network and finds secure alternate route for desirer destination. E2SIW can detect wormholes with a high detection rate, less overhead, and but consume large amount of energy to control GPS system .

Sebastian TerenceJ, et.al [3] in SeRWA provides secure route with false positive. Literature survey has been done on various techniques used to defence against wormhole attack, advantages and disadvantages of each also studied. Researchers have used some special hardware such as the directional antenna and the precise synchronized clock to defend the network from wormhole attack.

Bing Wu, Jianmin Chen, et.al [4] provides a countermeasures are features or functions that reduce or eliminate security vulnerabilities and attacks , give an overview of attacks according to the protocols stacks, an security attributes and mechanisms. Then they present preventive approaches following the order of the layered protocol stacks. They also put forward an overview of MANET intrusion detection systems (IDS), which are reactive approaches to thwart attacks and used as a second line of defence.

Rusheel Jain,et.al[5] suggested an efficient routing algorithm for mobile ad-hoc networks with a route establishment technique using Bayesian approach. They consider both time and space information to compute the route from source to destination. The results show that there is major improvement in delivery ratio, control packets overhead w.r.t. mobility and control packet overhead w.r.t. network size.

Fei Shi, Dongxu Jin,et.al [6] propose a time-based scheme for the purpose of preventing wormhole attacks in wireless ad hoc networks. The scheme includes two phases which are detection phase and location phase. By detection phase, the existence of wormhole attacks can be detected. By location phase, the wormhole nodes can be identified.

Binxiao Yu and Tongqiang Li,[7] present centralized and distributed algorithms for detecting wormhole attack in wireless sensor networks and require neither global topology information nor specialized hardware, but also can minimize wormhole related security risk by discriminating normal neighbours from illusive ones and removing the latter from neighbour lists. As only abnormal nodes get involved in detection procedures, compared with other approaches, sensor nodes in proposed schemes consume much less energy and algorithm complexity get further reduced , algorithms are able to detect wormhole attacks with 100% detection and 0% false alarm probabilities using proper parameters.

Ronggong Song, et.al[8] present a new method based on signal processing techniques, in which purposely shaped traffic is transmitted, analysed at the destination node by constructing the reception time data into a "signal", and then transforming this signal to the frequency domain using the Fast Fourier Transform (FFT). Using this technique, the wormhole attack can be quickly and accurately identified. They demonstrate in simulation and in a test-bed that the proposed methodology can be used to detect an attack within seconds. In addition, the detection mechanism proposed is agnostic of routing protocol and does not require any specialized hardware support.

V. PROBLEM STATEMENT

Previous approach for wormhole detection and prevention consume larger battery power that directly degrades the survival of MANET, Along with that previous approach having higher false negative rate and routing overhead that increase network packet in order to decrease network performance. The main goal of this paper is to develop a new approach which can successfully defend against wormhole attacks and consume lesser battery power in order to long survival of MANET and Sensor network.

VI. PROPOSED SOLUTION

Proposed methodology of wormhole detection and prevention is based on Statistics Based scheme [4] and graphical 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 an divide and conquer technique in which wormhole detection is performed between all the possible combination of node to its next to next node and 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 to be 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 node to its 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

Ni = Any arbitrary node in network where i = 1,2,3,……..n
Nb(Ni)j = Neighbor node of node Ni where j = 1,2,3,…..m
HC(Rx,y) = number of hop count in route from node x to node y as suggested by AODV
Th(HC) = Threshold hop count

Algorithms

```
{
Step 1:- Any arbitrary source node(S) call AODV for path towards their desired destination (D)
Step 2:-  AODV reply Route reply packet (RRP) with selected path that entitle with route R
R = n0, n1, n2,……, nn, nn+1
Where
n0 = source node
nn+1 = destination node
ni where i=1 to n is intermediate node
Step 3:-
For ( i = 0 ; i<= n-1 ; i++)
{
For ( j = 1 ; j<= m ; j++)
{
```

```
Node (ni) send RRP (route request message) for ni+2 via neighbour node Nb(ni)j
Nb(ni)j  reply as the number of hop count  HC(Rni,ni+2)
If (Th(HC) > HC(Rni,ni+2))
Then
Reply wormhole is present in route R
Goto Step 1
}//end of for loop j
}// end of for loop i
Reply route R is selected for transmission
}// algo end
```

In proposed algorithm all decision will take on the basis of value of threshold i.e. ,minimum number of node in alternate route between every pair of node to next to next node with the path discover by AODV is greater than or not. If it's greater than threshold, then it's declared there is wormhole between its next node and next to next node, elsewhere not.

Processer for evaluating the value of threshold is based on a hybrid model that encompasses both hop count and neighbour node algorithm. In hybrid approach value of threshold is calculated on the basis of hop count methodology with the help of neighbour node information. For calculating threshold each and every node of network find the path having the largest number of node over the entire possible path between it and it's next to next node and consider average value highest hop count of the entire node as threshold over the network as describe in algorithm 2.

Algorithm for Threshold

Assumption

```
Ni = Any arbitrary node in network where i = 1,2,3,……..n
Nb(Ni)j = Neighbor node of node Ni where j = 1,2,3,…..m
HC = Hop Count
T(HC) = Total hop count (initialized with zero)
Th(HC) = Threshold hop count (initialized with zero)
Initialized x=0
Initialized y=0
```

Algorithms

```
{
For ( i = 1 ; i<=n ; i++)
{
Max (HC)i = 0
For ( j = 1 ; j<=m ; j++)
{
// node arbitrary node N send RRP for their next to next node
Node (Ni) send route request packet for Nb[Nb(Ni)j]
Node { Nb[Nb(Ni)j] } reply as the number of hop count (HC)j
If ( Max (HC)i< HCj )
Then
Max (HC)i = HCj
x++
}// end of for loop j
T(HC) = T(HC) + Max (HC)i
y++
} // end of for loop i
Th(HC) = T(HC)/ x*y
}// algo end
```

VII. Simulation And Result Analysis

In order to authenticate the proposed methodology for wormhole detection variety of simulation experiments have been performed in NS-2 (2.32).

For performance and validation of proposed technique take different numbers of nodes in each scenario and consider a wormhole tunnels between any two nodes of that scenario for the simulation test.

(a) Simulation Setup

In order to analyze the proposed technique for wormhole detection number of simulation experiments have been performed by using NS-2 by using 50 mobile nodes with AODV protocol for routing.

Number of Nodes	Vary from 40 to 100	
Area	40	600*300
	50	600*300
	100	1000*800
	140	2000*1500
	170	2000*1500
Traffic	CBR	
Simulation Duration	100 Milliseconds	
Packet Transmission Rate	1024 kbps	
Carrier sense threshold Used In Normal Nodes	200 Meter	

Table 1 Simulation Parameters

Table 1 shows the parameters used in the simulation experiments. The proposed approach is tested with wormhole using a rectangular scenario of 600 × 300 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.

(b) False Negative Rate

For experimental verification proposed technique run over three different scenarios with 40, 50, 100,140 and 170 node density with same assumptions. As show in figure 6 false negative rate i.e. rate of wormhole detection depend on network density whereas threshold that is considered as keyhole for wormhole detection also depends on the network density.

After simulation with the help of tr file result can be observed which shows that FNR is fully depends on threshold value and network density i.e. when the nodes in the network are increased rate of detection of a true wormhole is also increase.

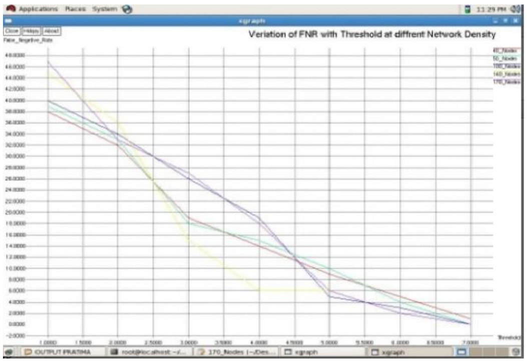

Figure 6:- False negative rate Vs threshold

(c) Control Packet

We consider the algorithm 2 for threshold calculation. Proposed technique is compared with the existing E2SIW[2] in many different factors like network overhead and number of control packet responsible for route hunting and handshaking over different node of network. Proposed technique may be increasing the number of control packet transmission as shown in figure 7.

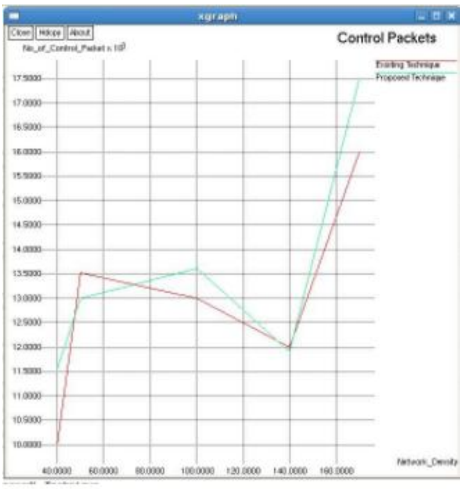

Figure 7: Control packet comparison

(d) Energy Consumed

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 in worst case is O(n-2*2)joule..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 and in E2SIW have same performance in both worst case and best case.

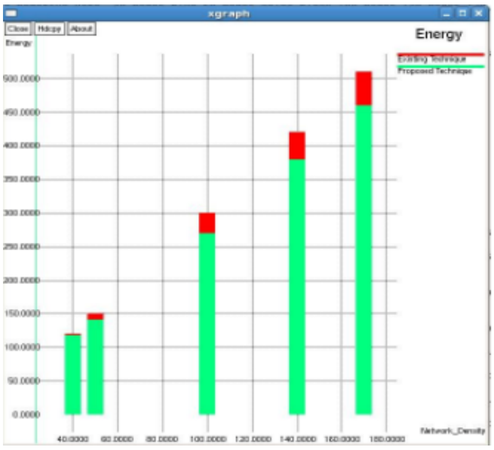

Figure 8: Energy Consumption Comparison

VIII. CONCLUSION AND FUTURE WORK

This paper gives a bird eye over MANET and their security threat mainly Wormhole attack. Wormhole is a very serious threat over MANET that present an illusion of shortest path and try to attack all the traffic over the network. This paper presents a hybrid approach that is based on hop count and neighbor node information scheme for wormhole detection and prevention with lower false negative rate and energy consumption. Backbone of Proposed technique is evaluation of threshold value i.e. maximum number of intermediate nodes between any node (N) to node (N+2) that describe in section VI.

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

REFERENCES

[1] Pallavi Sharma, Prof. Aditya Trivedi "An Approach to Defend Against Wormhole Attack in Ad Hoc Network Using Digital Signature" in IEEE ,2011

[2] 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

[3] Sebastian TerenceJ "Secure Route Discovery against Wormhole Attacks in Sensor Networks using Mobile Agents" in IEEE 2011

[4] Bing Wu, Jianmin Chen, Jie Wu and Mihaela Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", Springer Wireless/Mobile Network Security2007, pp 103-135

[5] Rusheel Jain, Murali Parameswaran and Chittaranjan Hota, "An Efficient On-Demand Routing Protocol for MANETs using Bayesian Approach", IEEE 2011

[6] Fei Shi, Dongxu Jin, Weijie Liu and JooSeok Song, "Time-based Detection and Location of Wormhole Attacks in Wireless Ad Hoc Networks" IEEE 2011, pp 1721-1726.

[7] Binxiao Yu and Tongqiang Li, "Study of Wormhole Attack Detecting Based on Local Connectivity Information in Wireless Sensor Networks", IEEE 2011, pp 3585-3588.

[8] Ronggong song, Peter c. Mason, Ming li "Enhancement of frequency-based wormhole attack detection" in military communications conference, 2011 - milcom ,ieee,2011

[9] Jin Guo, Zhi-yong Lei, "A Kind of Wormhole Attack Defense Strategy ofWSN Based on Neighbor Nodes Verification", IEEE 2011, 564-568.

[10] Mahdi Nouri, Somayeh Abazari Aghdam, Sajjad Abazari Aghdam "Collaborative Techniques for Detecting Wormhole Attack in MANETs" in International Conference on Research and Innovation in Information Systems (ICRIIS), 2011 ,IEEE

[11] Mariannne. A. Azer "Wormhole Attacks Mitigation" in Sixth International Conference on Availability, Reliability and Security ,2011,IEEE

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

[13] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, "Wormhole Attacks in Wireless Networks" citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.110.609

[14] W. Wang, B. Bhargava, Y. Lu, and X. Wu, "Defending against wormhole attacks in mobile ad hoc networks: Research articles," Wireless Communication Mobile Computing, vol. 6, no. 4, pp. 483–503, 2006.

[15] Ali Modirkhazeni , Saeedeh Aghamahmoodi , Arsalan Modirkhazeni , Naghmeh Niknejad "Distributed Approach to Mitigate Wormhole Attack in Wireless Sensor Networks" in 7th International Conference on Networked Computing (INC),IEEE,2011