International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-2 Issue-5, June 2013

Co-operative and Threshold Detection Method and Proposed Algorithm for Black Hole Attack

Shanu Singh, Shikha Chandana, Amit Kumar Pandey

Abstract - To avail the prospective of wireless communication now days, the complete communication should be flexible and supportive to various architectures. Now a days various prospective has been proposed to achieve the flexibility and minimize the losses. Various routing protocols has been proposed in case of Mobile and ad-hoc networks. Various optimized link and nodes for routing is insisted in this paper. This paper comes with a complete comparative study of various routing protocol, security issue and physical layers . In this paper an approach has been proposed for Black Hole Removal using Threshold and Co-operative Method. Co-operative detection method has been also proposed to identify the proper step. Over all this paper contains a comparative routing protocol and study of various security issue physical layer and proposed algorithm for co-operative detection method of Black hole Attack.

Index Terms—Routing protocol, security issue, physical layers, co-operative detection.

I. ROUTING PROTOCOL IN MANET

A. Routing protocol

A large number of routing protocols have been proposed in the literature for the ad-hoc wireless networks. These protocols can be categorized as table driven / proactive protocols and source initiated protocols / demand- driven or reactive protocols. In proactive routing protocols the optimized link state routing (OLSR), nodes obtain their routes by exchanging the topology information periodically. In reactive linking protocols, such as the ad hoc on demand distance vector protocol (AODV), nodes find routes only when they are in need.

B. On demand routing protocol

The On Demand routing protocols initiates the route discovery process within the network whenever there is a need of route to reach the destination. As soon as a route is discovered and established, it is maintained by the route maintenance procedure until any other destination by each node is inaccessible along every path or if the Route is no longer desired. Examples are: Ad-hoc On Demand Vector Routing (AODV), Dynamic Source Routing (DSR), Temporary Ordered Routing Algorithm (TORA) etc. Ad hoc On-Demand Distance Vector (AODV) is a reactive protocol so routes are only determined when they are needed. It is frequently adaptable to dynamic link and memory overhead and low network utilization conditions, low processing. It also determines unicast route from source to destination. It allows them to choose their new destination. One distinguishing feature of AODV is its use of a destination sequence number for each route entry. The IETF (Internet Engineering Task Force) defined RFC 3561 for AODV. Other example of on demand routing protocol is Dynamic Source Routing (DSR) used for multi hop wireless mobile ad-hoc networks. DSR protocol requires no administration by the network operator as it automatically discovers and maintains link in the network by storing source routes, discovered dynamically only when needed. All the nodes act as routers and participate in the packet forwarding process. Description of DSR is available in RFC 4728.

C. Security issue

In the physical layer, mobile nodes along with communication links are vulnerable to active and passive attacks. The mobile ad hoc networks are more prone to suffer from the malicious behaviors than the traditional wired networks because of their lack of secure boundaries. This unique characteristics of mobile ad-hoc networking present a new set of nontrivial challenges to security design. This challenges include open network infrasture, shared wireless medium, stringent resource constraints, and highly flexible network topology.

II. VULNERABILITIES OF MANET

If MANET are more vulnerable than wired networks therefore security is difficult to maintain in mobile ad hoc networks. Indexing are the various vulnerabilities [5] that exist in wireless ad-hoc networks.

A. Attack issues compromised node inside network

As mobile nodes are autonomous units they can leave or join the network with freedom. Due to the behavioral diversity of different nodes it is hard for nodes to prevent the possible malicious behavior of all nodes it communicates. It is very difficult to track the malicious behavior performed by the compromised nodes mainly in large scale ad hoc networks, as due to mobility of the ad hoc network the compromised nodes frequently change their attack target and perform malicious behavior to different nodes.

Manuscript published on 30 June 2013.
* Correspondence Author (s)
Ms Shanu Singh, Department Of Computer Science & Technology, Gurgaon Institute of Technology & Management, Gurgaon, India.
Ms. Shikha Chandana, Department Of Computer Science & Technology, Gurgaon Institute of Technology & Management, Gurgaon, India.
Mr. Amit Kumar Pandey, Department of Electronics and Communication Engineering, Skyline Institute Of Engineering and Technology, Greater Noida, India.

Therefore threats from the compromised nodes are far more difficult to detect. Example of this kind of threat is Byzantine Attack which encountered in the routing protocol. In this nodes or group of compromised intermediate nodes works in collusion and perform malicious behavior. The compromised nodes cannot be easily recognized so it is very harmful to ad hoc networks.

B. Lack of management centralized facility

The absence of centralized management makes the detection of attack very difficult as it is not easy to monitor the traffic in the highly dynamic large scale network. Due to this, failures happen such as path breakage, transmission impairment and packet dropping happens frequently. The absence of such management machinery can cause vulnerability that can influence several aspects of operations in the mobile ad hoc network. Absence of no centralized authority, and decision making in mobile ad hoc network is sometimes decentralized, the adversary which can make use of this vulnerability and perform some attacks that can break the cooperative algorithm. Black Hole attack [5] is one of the prominent attacks. It is a type of denial of service attack [6]. Black hole attack is difficult to detect in dynamic networks with mobile nodes entering and leaving the network. In the Figure-2.1, S is the Source node, and D is the destination node whereas A, B, C are the intermediate nodes. Here M is the malicious node. The malicious node M waits for the neighboring nodes to send RREQ messages. As soon as the malicious node receives the RREQ message, it immediately sends the false RREP message giving the route to destination through itself. Without checking its routing table it assigns a high sequence number to settle in the routing table of the victim node, before other nodes send justified route information. Therefore the requesting node thinks that his discovery process is completed so it stops replying RREP messages and begin to send packets to malicious node. The malicious node M attacks all RREP messages and takes over all the routes. Therefore all the packets are sent to node M which is not going to forward the packets anywhere. In this way the Black Hole node delay, drop of packet.

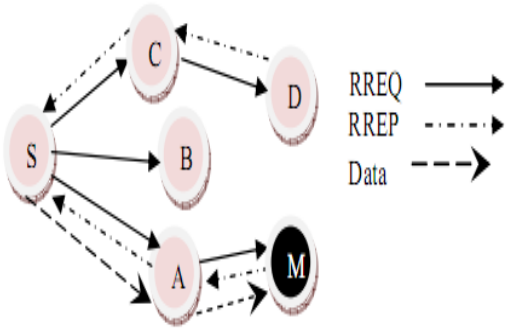

Figure 1 : Attacks Identified

III. ATTACK AT THE MAC LAYER

The denial of service attack aims to crab the availability of certain node or even the services of the entire ad hoc networks. Under traditional wired network, some kind of network traffic to the target so as to exhaust the processing power of the target the DoS attacks are carried out by flooding and make the services provided by the target become unavailable. To perform the traditional DoS attacks is not good idea in the mobile ad hoc networks because of the distributed nature of the services. Moreover, the mobile ad hoc networks are more vulnerable than the wired networks because of the interference-prone radio channel and the limited battery power. The attackers exactly use the radio jamming and battery exhaustion methods to conduct DoS attacks to the mobile ad hoc networks, which well correspond to the two vulnerabilities.

A. Attack of warm hole at network layer

In the wormhole attacks, a compromised node in the ad hoc networks colludes with external attacker to create a short path in the networks. By obtaining this shortcut, they may or may not trick the source node to fetch in the route discovery process and after this they launch interception attacks. Packets from suh two colluding attackers are usually transmitted using wired connection to create the fastest route from source to the destination node(DN). In addition, if the worm-hole nodes consistently maintain the bogus routes, they can disable permanently deny other routes from being established. The intermediate nodes reside along that denied routes are unable to participate in the network operations.

B. Attack of link spoofing at data link layer

In a link spoofing attack, a malicious node advertises fake links with non-neighbors to disrupt routing operations. As in OLSR protocol, an attacker can advertise a fake link with a target's two-hop neighbors. This makes the target node to select the malicious node to be its MPR. A malicious node can then manipulate data or routing traffic, for example, updating or dropping the routing traffic or performing other types of DoS attacks. Figure 2 shows an example of the link spoofing attack in an OLSR MANET.

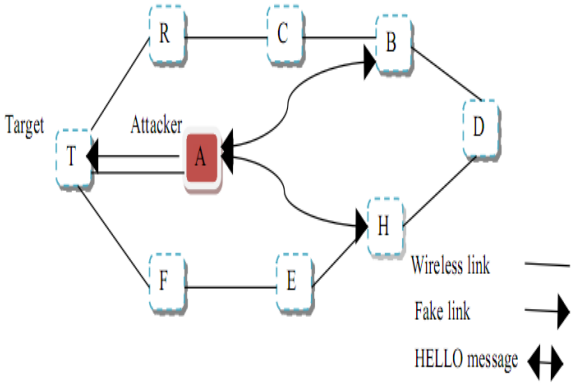

Fig 2 Link Spoofing Attack

In the figure 2, an assumption is made that node A is the attacking node [9], and node T is the target to be attacked. Before the attack, both nodes A and E are MPRs for node T. During the link such a slang attack, node A express a fake link with node T's two-hop neighbour, that is, node D. By following the path to the OLSR protocol, node T will select the malicious node A as its only MPR since node A is the least set that reaches node T's two-hop neighbours. Node A can then drop or withhold the routing traffic produced by node T by being node T's only MPR.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

C. *Eavesdropping at physical layer*

Eavesdropping is another kind of attack usually happens at physical layer. The goal of eavesdropping is to obtain some confidential information that should be kept secret during the communication [4]. The confidential information may include the location, , private key, even passwords public key of the nodes. Because these data are very important to the security state of the nodes, to prevent away from the unauthorized person to access.

D. *Impersonation at physical layer*

Impersonation attack is a severe threat to the security of mobile ad hoc network. In few case where proper authentication mechanism among the nodes is not possible, the opponent can capture some nodes in the network and make them look like benign nodes. In this way, the separated nodes can join the network as the normal nodes and begin to conduct the malicious behaviors such as propagate fake routing information and gain inappropriate priority to access some confidential information.

IV. BLACK HOLE REMOVAL USING THRESHOLD AND CO-OPERATIVE METHOD

A. *Cooperative detection to confirm the malicious behavior of nodes in Black List*

Once the list of possible black hole nodes is maintained with the help of Threshold Value, **the cooperative detection procedure is activated**. The cooperative fetching procedure is initiated by the initial detection node, which proceeds by primarily broadcasting and notifying all the one-hop neighbors of the possible suspicious node to cooperatively participate in the decision process confirming that the node in question is indeed a malicious one.

B. *Cooperative detection to confirm the malicious behavior of nodes in Black List*

Once the list of possible black hole nodes is maintained with the help of Threshold Value, **the cooperative detection procedure is activated**. The cooperative fetching procedure is initiated by the initial detection node, which proceeds by preceding broadcasting and notifying all the one-hop neighbors of the possible suspicious node to cooperatively participate in the decision process confirming that the node in question is indeed a malicious one.

C. *Cooperative detection Procedure*

1) **First of all Call Neighbor List (Node_id) algorithm,** as defined above, with Node_id of first suspicious called SN (1) node as argument to the algorithm to find out the Neighbor List of suspicious node.
2) Now find out the common nodes in the two neighbor lists , one is list of nodes which are at distance of 1 hop from source node (also called initial detection node) , this list is called IN1H and other is the neighbor list (SN1H) of SN (1) or first suspicious node by taking the intersection of both the lists. We call the final list as INSN1H, i.e list of nodes which are at distance of both the nodes, IN as well as SN.
3) After finding out the nodes with 1 hop distance from both, the source and the first suspicious node in last step, source node will broadcast the cooperative detection message to all nodes in INSN1H list.
4) Now every node in INSN1H list will broadcast the RREQ_pkt with destination node being set to IN (initial detection node).
5) Upon receiving the RREP_pkts from different nodes do the following :

5.1) If the RREP_pkt is from SN then

- Send check packet intentionally to IN via SN.
- Send Notification of this check packet to IN directly (as its at only 1 hop distance from IN)

5.2) Else, if the packet is not from SN simply discard the packet as it doesn't require any further processing.

6) IN will wait till Waiting Time (pre-defined) time to collect the notification packets from nodes in INSN1H list.
7) IN will also maintain a table known Voter Table (written as VT). VT includes of 2 fields.
8) Put the Node_id of sender of notification packet to "Voter" field of VT.
9) IN waits for two WT for check packet from SN. If IN receive check packet from SN , mark " False" to the "Suspicious Value" field and send Notification to cooperative node that CP is received.
10) After waiting for two WT for check packet, if IN doesn't receive any check packet from SN , mark "True" to the "Suspicious Value" field of VT

Table1 : Format of Voter table:

Voter	Suspicious Value
2	True
3	True
4	True
5	True

11) If all the entries in VT's Suspicious Value are TRUE then its surely a malicious node and ALARM packet is sent to all its neighbors to warn them against malicious node.
12) If all the entries in VT's Suspicious Value are FALSE then its not a malicious node, remove it from Black List.
13) If some values are TRUE and some are False in VT's Suspicious Field then decision is taken on the basis of voter's count in favour and against that particular node.

V. PROPOSED ALGORITHM

Notations :
IN : Initial detection node (source node) , SN : Suspicious Node , DN : Destination Node ,IN1H : IN's 1 Hop Neighbor node list , SN1H : SN's 1 Hop Neighbor node list, VT : Voter Table, WT : Waiting Time.

1 Begin

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

```
2  Find out the common nodes of IN1H and SN1H, i.e
   IN1H ^ SN1H and store it in list called INSN1H i.e
   the list of nodes which are at 1 hop distance to both
   ,IN as well as SN.
3  IN Broadcasts cooperative detection message to all
   nodes of INSN1H list.
4  For each x Є INSN1H
5      {
6       Broadcast RREQ_pkt ( with DN being set to IN )
7       Upon receiving RREP_pkts
8            If( received RREP_pkt is from SN )
9             {
10             Send a check packet(CP) to IN via this
   route and
                  a notification of this CP to IN
11            }
12           Else
13            {
14             Discard the RREP_pkt( as it doesn't require
   further processing)
15            }
16     }
17 IN waits for WT to collect the Notification packets
   from nodes of INSN1H list.IN waits for two WT for
   CP from SN.
18     {
19       If IN receives CP from SN
20            {
21             Mark "False" to the "Suspicious Value"
   field of VT and send
   notification packet to cooperative node.
22            }
23       Else
24            {
25             Mark "True" to the "Suspicious Value"
   field of VT.
26            }
27     }
28 If (All the entries of "Suspicious Value" field are
   "True")
29  {
30   It's a Black Hole in the network.
31  }
32 End
```

Fig. 3 Algorithm for Co-operative Detection

VI. GRAPH TO SHOW PERFORMANCE OF PROPOSED ALGORITHM

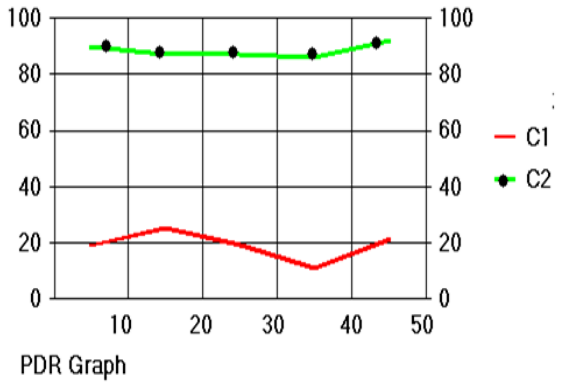

Fig. 4 Performance of Proposed Algorithm (BRTCM)

VII. CONCLUSION

This paper presents an approach for minimizing of black hole attack by using an algorithm called co-operative detection architecture. Such a system presents various detection procedure which is achieved in this paper. The comparative study is perform of routing protocol to minimize security issue. To make paper more meaning full the algorithms and procedure listed stepwise. The performance of proposed algorithm graph is provided for achievement of better results. Black hole attack in various layer is given to minimize the search of researchers.

REFERENCES

[1] Michele Nogueira Lima, Aldri Luiz dos Santos and Guy Pujolle, "A Survey of Survivability in Mobile Ad Hoc Networks", IEEE Communications Surveys and Tutorials COMSUR), Volume 11, Number 1, 2009, pp 1-3.

[2] Nishu Garg and R.P Mahapatra, "MANET Security Issues", International Journal of Computer Science and Network Security (IJCSNS), Volume 9, Number 8, 2009, pp. 241-246.

[3] Wenjia Li and Anupam Joshi, "Security Issues in Mobile Ad Hoc Networks - A Survey", Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County, 2006.

[4] Kamanshis Biswas and Md. Liakat Ali, "Security Threats in Mobile Ad Hoc Network", Master Thesis Computer Science, Thesis no: MCS-2007:07, 22nd March, 2007.

[5] Rashid Hafeez Khokhar, Md Asri Ngadi and Satria Mandala, "A Review of Current Routing Attacks in Mobile Ad Hoc Networks", International Journal of Computer Science and Security, Volume 2, Number 3, 2008, pp 18-29.

[6] Sheenu Sharma and Roopam Gupta,"Simulation study of Black Hole Attack in the Mobile Adhoc Network", Journal of Engineering Science and Technology, Volume 4, Number 2, 2009, pp 243-250.

[7] Hao yang, Haiyun Luo, Fan Ye, Songwu Lu and Lixia Zhang, "Secuirty in Mobile Ad hoc Networks: Challenges and Solutions", IEEE Wireless Communications Journal, Volume 11, Number 1, 2004, pp 38-47.

[8] Payal N. Raj and Prashant B. Swadas, "DPRAODV: A dynamic learning system against black hole attack in AODV based MANET", International Journal of Computer Science Issues (IJCSI), Volume 2, Number 3, 2009, pp 54-59.

[9] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, "Prevention of cooperative black hole attack in wireless ad hoc networks," International Conference (ICWN'03), Las Vegas, Nevada, USA, 2003, pp 570-575.

[10] Mohammad Al-Shurman, Seong-Moo Yoon and Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks", ACM Southeast Regional Conference , Proceedings of the 42nd annual Southeast regional conference, 2004, pp 96-97 .

[11] Chang Wu Yu, Tung-Kuang, Wu, Rei Heng, Cheng and Shun Chao Chang, "A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Networks", PAKDD 2007 International Workshop, May 2007, Nanjing, China, pp 538–549.

[12] Hesiri Weerasinghe, "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation", Proceedings of the Future Generation Communication and Networking, Volume 2, 2007, pp 362-367.

[20] Mehdi Medadian, M.H. Yektaie and A.M Rahmani, "Combat with Black Hole Attack in AODV routing protocol in MANET", First Asian Himalayas International Conference on Internet (AH-ICI2009), 3-5th Nov, 2009.

[21] Bo Sun Yong, Guan Jian Chen and Udo W. Pooch, "Detecting Black-hole Attack in Mobile Ad Hoc Networks", The Institution of Electrical Engineers (IEE),Volume 5, Number 6, 2003, pp 490-495.

[22] Elmar Gerhards-Padilla, Nils Aschenbruck, Peter Martini Marko Jahnke and Jens Tolle, "Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs", 32nd IEEE Conference on Local Computer Networks, 15-18th Oct 2007, Dublin, pp 1043-1050.
[23] Gao Xiaopeng and Chen Wei, "A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks", IFIP International Conference on Network and Parallel Computing – Workshops, 18-21 Sep 2007, Dalian, China, pp 209-214.
[24] Ming Yu, Mengchu Zhou and Wei Su, "A Secure Routing Protocol Against Byzantine Attacks for MANETs in Adversarial Environments", IEEE Transactions on Vehicular Technology, Volume 58, Number 1, pp 449-460, 2009.
[25] K. Lakshmi et al. "Modified AODV Protocol Against Blackhole Attacks in MANET" International Journal of Engineering and Technology Vol.2 (6), 2010, 444-449.
[26] Mohammad Al-Shurman and Seong-Moo Yoo "Blackhole Attack in mobile ad-hoc networks" Electrical and Computer Engineering Department The University of Alabama in Huntsville Huntsville, Alabama 35899.

Ms. Shanu singh is a student of Master of Technology from Gurgaon Institute Of Technology and Management Gurgaon . She is presenting her work over cooperative black hole attack issue as similar her thesis work. Her area of interest is Agile development, mobile technology and s/w project management.

Ms. Shika chandana a student of master of technology from Gurgaon Institute of Technology and Management gurgaon. She had presented many paper related computer science diagnosis .

Mr. Amit Kumar Pandey had done his bachelor of Technology in Electronics And Communication Engineering from Skyline institute of engineering and Technology. He is working as a lecturer under ECE department in BMCTM from past two years. His area of Publications are Wireless communication.

.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)