# An Approach to protect the Cluster Attacks in Ad-hoc Network Security

**[a]Pradosh Chandra Patnaik, [b]M V Ramana Muthy, [c]S B Kishor**
[a]Associate Professor, Dept. Of Computer Science, ASTRA, Hyderabad
[b]Professor, Dept. of Mathematics & Computer Science, Osmania University, Hyderabad, India.
[c]Head, Dept. of Computer Studies and Research, S.P College, Chandrapur, Maharsashtra, India,

## Abstract

Wireless network technology is most frequently used network technology. A number of variants are available on the basis of traditional wireless networking such as WSN, WMN, MANET and others. In all the variants of wireless networks routing plays the essential role. Additionally the attackers are mainly targeting the routing strategies for performing the malicious activities. In order to secure the wireless ad hoc network a new kind of security system is proposed in this presented paper. The proposed security architecture provides the security against the malicious attackers namely black-hole, wormhole, grey-hole and DDOS attacks. Additionally able to improve the performance of network in normal conditions as well as under attack conditions. The given paper includes the proposed system design and the concepts that are help to support the proposed security infrastructure.

**KEYWORDS:** Ad-hoc Network, Wireless network, attacks

## I.INTRODUCTION

Wireless ad hoc network is a kind of wireless network with additional properties that improve the adoptability of network for different applications such as military operations and others. In this network the network devices are known as nodes and the connectivity among them is called the links. In such network the connectivity, availability and power is fluctuating with the geographical positioning and their mobility of nodes. Thus in order to scale the network performance and resource provisioning the clustering approaches are adopted. These approaches are help to identify the efficient routers from the network nodes and the most promising nodes are working as key service provider routers.

In this proposed work WCA (weighted clustering) algorithm is investigated and explored. The basic concept behind the utilization of WCA algorithm is to obtaining the efficient routers by which the resource consumption and efficiency is maintained in communication. And after implementing the WCA concept the security concepts are added to the network functioning. Therefore the entire design concept is required to demonstrate. In addition of that this paper also provides the attack models investigation and issues encountered during the design of secure cluster oriented routing protocol.

### *A. Wormhole*

## II. BACKGROUND

In this section the different attack models that are incorporated for finding solution and implementation objectives.
Wormhole attacks can cause (i) tunneling of the packets at the application layer, (ii) tunneling of the packets through a long range wormhole tunnel using high power transmitters and (iii) tunneling the packets via external wired infrastructure [1]. In our work, the third case is considered to secure WANETs against wormhole attacks. A representative feature of wormhole attacks consists of relatively longer packet latency than the normal wireless propagation latencies on a single hop. The load on a single route can also increase, leading to typically longer queuing delays. However, this is not a sufficient condition for the existence of a wormhole attack, because packet transmission is affected by various factors like congestion and traditional processing [2].

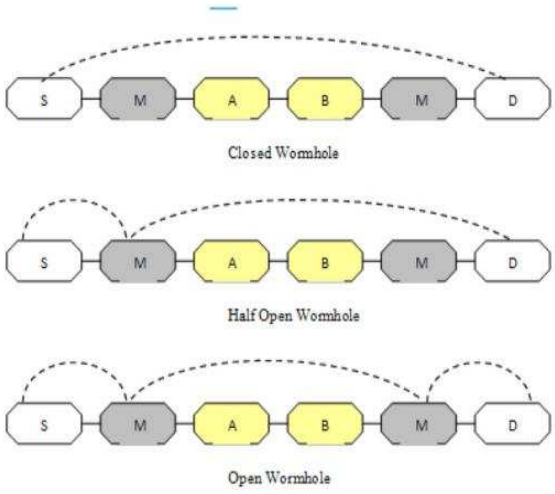


Figure 1 worm hole attack and types

In a wormhole attack more than one malicious nodes are join the network and according to the nodes they are connected thorough high speed data buses by which they promises to send data from source to sink, the formation of attack is driven as a malicious node can record packets at one location in the network and tunnel them to another location through a private network shared with a colluding malicious node. Wormhole attack can be done with one node also, but generally two or more attackers connect via a link called wormhole link. Wormhole attack is of three types: Closed Wormhole, Half Open Wormhole, and Open Wormhole [3].

***B. Black hole attack***

A Black hole is formed during the week routing infrastructure. When a malicious node joins the network this problem arises. This node falsely replies for route requests without having an active route to the destination and exploits the Routing Protocol to advertise itself as having a good and valid path to a destination node. Actually in AODV routing for find the path between source and sink RREQ packets are flood and all the path replies with RREP packets if malicious node RREP is arrive first then the requester node suppose the provided information is correct and reply with the data packets [4].

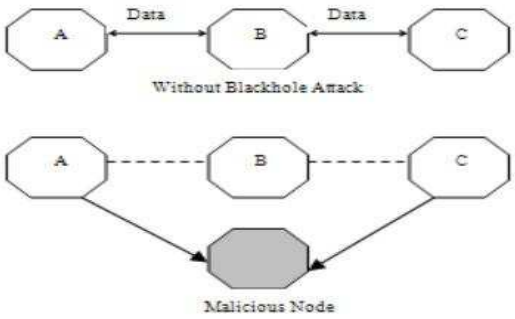


Figure 2 black hole attack

Thus the black hole attack deployed using the malicious attacker in network and the malicious attacker drop all the packets received.

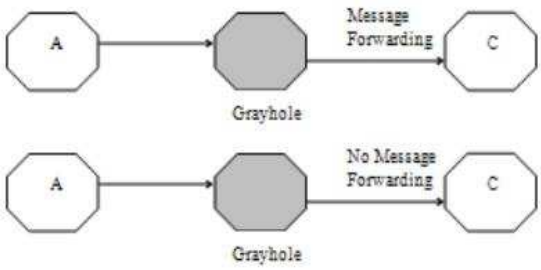


Figure 3gray-hole attack

### *C. Gray-hole attacks*

A Gray-hole attack is much similar to the two attack black hole and wormhole attack. In this attack nodes forward all packets to certain nodes but may drop packets coming from or destined to specific nodes as shown in Figure 3. In this type of attack, node may behave maliciously for some time but later on it behaves absolutely normally. This type of attacks is more difficult compared to black hole attack. Because of the malicious attacker drops the selected packets therefore sometimes that is also called selective forwarding attack. Therefore the basic packet delivery ratio is not much affected according to the performance aspect but the data recovery from the network at the target end is difficult.

### *D. Ad Hoc Flooding Attack*

Flooding RREQ packets in the whole network will consume a lot of resource of network. To reduce congestion in a network, the AODV protocol adopts some methods. A node cannot originate more than RREQ_RATELIMIT RREQ messages per second. After broadcasting a RREQ, a node waits for a RREP. If a route is not received within round-trip milliseconds, the node may try again to discover a route by broadcasting another RREQ. Repeated attempts by a source node at route discovery for a single destination must utilize a binary exponential back-off. The first time a source node broadcasts a RREQ, it waits roundtrip time for the reception of a RREP. If a RREP is not received within that time, the source node sends a new RREQ. When calculating the time to wait for the RREP after sending the second RREQ, the source node MUST use a binary exponential back-off. Hence, the waiting time for the RREP corresponding to the second RREQ is 2 * round-trip time. The RREQ packets are broadcast in an incrementing ring to reduce the overhead caused by flooding the whole network [5].

In the Ad Hoc Flooding Attack the attack node violates the above rules to exhaust the network resource. Firstly, the attacker selects many IP addresses which are not in the networks if he knows the scope of IP address in the networks. Because no node can answer RREP packets for these RREQ, the reverse route in the route table of node will be conserved for longer. The attacker can select random IP addresses if he cannot know scope of IP address. Secondly, the attacker successively originates mass RREQ messages for these void IP addresses. The attacker tries to send excessive RREQ without considering RREQ_RATELIMIT within per second. The attacker will resend the RREQ packets without waiting for the RREP or round-trip time, if he uses out these IP addresses. The TTL of RREQ is set up to a maximum without using expanding ring search method. In the Flooding Attacks, the whole network will be full of RREQ packets which the attacker sends. The communication bandwidth is exhausted by the flooded RREQ packets and the resource of nodes is exhausted at the same time. If mass RREQ packets are coming to the node in a little time, the storage of route table in the node will exhaust so that the node cannot receive new RREQ packet. As a result, the legitimate nodes cannot set up paths to send data [5].

| Name | SYN flooding attack | Ad hoc flooding attac k |
|---|---|---|
| Attack method | TCP connectio n request with spoofed source address | Flooding mass RREQ packets |
| Victim | Host | a Mobile d hoc network |
| Protoco l | TCP/I P | On routin demand g protocol |
| Protoco l layer | Transport layer | Network layer |
| Goal | DOS in host | DO S in whole network |

Table 1 flooding attack and summary

## III. PROPOSED WORK

The main objective of the proposed work is to develop more stable and efficient cluster head selection algorithm by which the performance of network is significantly increases and security constrains are implementable. Therefore the modular development strategy is presented in this section.

### *A. Node Quality*

In order to find the stable and more efficient network cluster the following solutions are suggested to implement.

1. **Energy:** the node which having higher remain

   battery power having long life and able to participate in communication.

2. **Connectivity:** Maximum numbers of nodes are in connected through this node causes the more serving capability.

3. **Buffer length:** buffer length demonstrate the low load on node, therefore less loaded node can serve better.

4. **Mobility:** low mobile nodes are able to form more

   stable clusters.

***B. Clustering Algorithm***

In this section proposed clustering approach are discussed in detail. The proposed WCA algorithm that include fresh route information is described in two different modules first the primary calculation and secondly the cluster head selection.

***Weight Calculation Algorithm***

1. For each node in network
2. Find remain energy E
3. Find mobility using
4. find buffer remain for all nodes as B
5. find number of neighbour nodes as C
6. calculate the weights

***Cluster Head Selection Algorithm***

1. Find the memory, buffer, connectivity and mobility for each node
2. Find weights for all the nodes
3. For each node in network
4. If node weight is maximum than
   a. cl-head =1
5. Else
   a. cl-head=0
6. End if

7. End for
8. Broad cast the massage to neighbor nodes where cl-head=1
9. Mobile nodes
10. Determine new role of nodes
11. Repeat process to step 1

***C. Security Integration***

In this section the layered detection and removal of different kinds of targeted attacks are provided. During security integration first the entire network nodes are evaluated on the basis of their number of request broadcasts. Thus using the previous sessions the broadcasting threshold is prepared. That can be evaluated using the given formula.

The estimated threshold is used to remove the DDOS flooding based malicious attacker in network. thus if at the time of receiving request from another node if any node send RREQ packets more than estimated threshold than add these nodes to blacklist and do not receive any request from this node. After implementing the desired first phase security checks the nodes are evaluated for the further checks.

Thus the following procedure is utilized to detect and prevent an attacker in ad hoc network.

1. Source node S broadcast RREQ for route discovery and store sending time t
2. If S receive RREP form destination then capture time t'
3. S calculate $Alt=t'-t$
4. If $Alt$
5. Nodes may be malicious;
6. Run algorithm 2.
7. Else
8. S considers the route among source and destination is safe and sends data.
9. End if

In above given algorithm steps the Node TT is the maximum expected wireless propagation latency on a single hop [1].The second algorithm consumes the DH algorithm for cryptographic solution of the secure data transmission and remaining node identification for Gray hole, Black hole and Wormhole detection.

Now when the route contains the malicious nodes than the cryptographic technique is utilized for secure data transmission and therefore Diffie–Hellman key exchange technique is utilized for securing the communication and prevention of targeted attack. That is a specific method of securely exchanging cryptographic keys over a public network. D–H is one of the earliest practical examples of public key exchange implemented within the field of cryptography. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communication channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher. And the second algorithm for identifying the attacker is taken place in the following manner.

1. Sender sends dummy packets
2. For five dummy packets
3. Send encrypted packet by using sender key
4. Wait for 6*Node TT
5. If send get RREP from other route
6. If time of receiving and sending vary by number of hops
7. Node is malicious wormhole attack detected
8. Add in blacklist
9. Else if get reply = 0
10. Black-hole attack detected
11. Else if get reply <= 3
12. Gray hole attack detected
13. End if
14. End if
15. End for

After locating the entire attackers in network the network becomes secure and trustworthy thus the proposed secure cryptographic weighted clustering scheme for secure communication is prepared. The next section provides the conclusion and future extension of the proposed work.

## IV.CONCLUSION AND FUTURE WORK

The proposed work is intended to investigate the security in ad hoc networks. Therefore different kinds of attacks are investigated and the crucial attacks namely Black hole, Gray hole, wormhole and DDOS attacks are targeted for finding the solution. Additionally that is found the performance of the network is decreases when the malicious attackers are deployed in network. Therefore performance scaling is also required in network.

Thus in this paper a weighted clustering scheme is proposed for implementation with the cryptographic solution and detection of attackers. In near future the proposed concept is implemented by modifying the AODV routing protocol. And the simulation is demonstrated using the network simulator 2 environment.

## REFERENCES

[1] Emmanouil A. Panaousis, LevonNazaryan, Christos Politis, “Securing AODV against Wormhole Attacks in Emergency MANET Multimedia Communications”, Mobimedia, London, U.K., Vol - 09, pp (7-9), Sept 2009.

[2] F. Nait-Abdesselam, B. Bensaou, and T. Taleb, “Detecting and avoiding wormhole attacks in wireless ad hoc networks”, IEEE Communications Magazine, vol. 46, no. 4, pp. (127– 133), April 2008.

[3] Pratik Gite & Sanjay Thakur, “Different Security Issues Over MANET”, International Journal of Computer Science Engineering and Information Technology, Research Vol. 3, Issue 1, pp. (233-238), Mar 2013.

[4] Pankaj Solanki, Deepak Shukla, “Detection and Prevention of Black Hole Attack To Improve Network Performance By Using Fidelity and ECARP Algorithms”, International Journal Of Engineering And Computer Science, Vol. - 3, Issue 2, pp. (3884-3890), February 2014.

[5] Ping Yia, , Yafei Houc, YipingZhongb, Shiyong Zhangb, Zhoulin Daib, “Flooding attack and defence in Ad hoc networks”, Journal of Systems Engineering and Electronics, Vol. 17, Issue 2, pp. (410-416), June 2006.