ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 2, pp: (69-75), Month: April - June 2016, Available at: www.researchpublish.com

Packet Estimation Algorithm to Prevent Collaborative Attacks in Manet

Mr.S.Narayanan[1], C.Kokila[2], N.Kowsalya[3], C.Madurambiga[4]

Assistant Professor[1], B.Tech-IT Final Year Students[2 3 4], Department Of Information Technology,
Valliammai Engineering college, Kattankulathur, Kanchepuram, Tamilnadu, India

Abstract: **Mobile Ad hoc Networks also called infrastructure less networks are complex distributed systems consist of wireless links between the nodes and each node also works as a router to forwards the data on behalf of other nodes, MANETs have been widely used for various important applications such as military crisis operations and emergency preparedness and response operations. The dynamic topology feature of MANETs makes these networks highly vulnerable to various attacks. We propose a detection scheme called the cooperative bait detection scheme, which aims at detect and prevent malicious nodes launching black and gray hole attacks in MANETs. By using CBDS its only prevent the black-hole attack, There is no possibilities to detect and prevent the gray-hole attack. So, The Packet Estimation Algorithm to Calculate packet delivery rate per hop count determine trustworthiness, To prevent both the attacks in the wireless communication. Main Advantages are preventing (or) avoiding an attack in its initial stage, Hidden attack is not possible and Qos is maintained.**

Keywords: **CBDS, Packet estimation, RREQ, RREP.**

1. INTROUDCTION

An ad-hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any stand-alone infrastructure or centralized administration. Mobile Ad-hoc networks are self-organizing and self-re-configuring multi-hop wireless networks, where the structure of the network changes dynamically.

Types of attacks: DATA traffic attacks: Black hole attack, Cooperative block hole attack, Gray whole attack, Jellyfish attack. Control traffic attacks: Worm whole attack, Hello flood attack, Bogus registering attack, Sybil's attack, Black mail attack. These are attacks in Manet. In this proposed system, there are two kinds of attacks (Black and Gray hole attacks) are prevented by using Packet Estimation Algorithm.

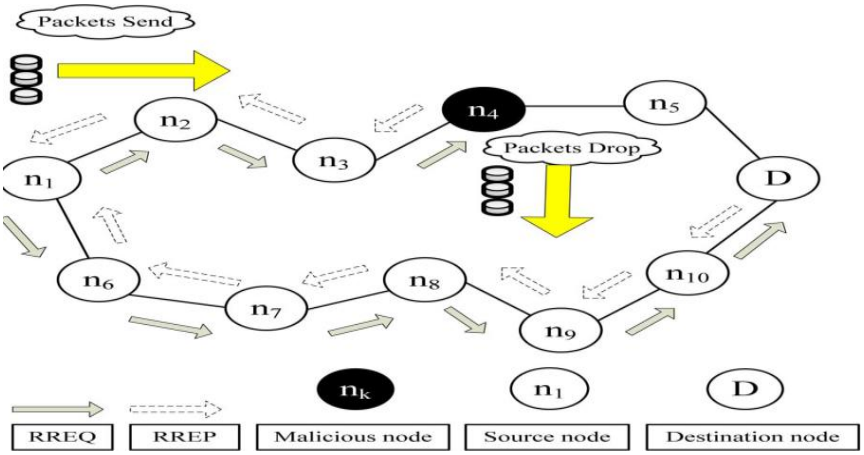

Fig 1. Black hole attack–node *n*4 drops all the data packets

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 2, pp: (69-75), Month: April - June 2016, Available at: www.researchpublish.com

In black hole attacks (see Fig. 1), a node transmits a malicious broadcast informing that it has the shortest path toward the destination, with the goal of intercepting messages. [6]

AODV involves two main processes: route discovery and route reply. To execute the route discovery phase, the source node broadcasts a Route Request (RREQ) packet through the network. If an intermediate node wants to communicate with the source node, it send the RREP to the source node. When the RREQ is forwarded to the destination node, the node adds its address information on the route record in the RREQ packet. When the destination receives the RREQ, it can know each intermediary node's address among the route. To properly send the RREP to the source node.

The destination node relies on the collected routing information among the packets in order to send a reply RREP message to the source node along with the whole routing information on the established route. AODV does not have any detection mechanism, but the source node can get all route information about the nodes on the route. In our approach, we make use of this feature. In this paper, a mechanism [so-called Packet Estimation Algorithm (PEA)] is used to prevent the collaborative attacks (Gray and Black hole attack) in Manet. In our scheme, We are estimating the packet rate per hop count. Now consider the threshold value is 1.000 is maintained in each neighboring node at the time of transaction. This value is calculated per hop count. The value is reduced to 0.5482 at the two hop count that node is represented as malicious node. Then the source node search the nearest shortest path in the network.

Fundamental characteristics such as MANET allow nodes to join and leave the network at any point of time. It has rendered it vulnerable to security attacks. It does not depend on pre-existing infrastructure (or) base station.

The structure of MANET may vary from a small, static network, mobile, dynamic network. Fundamental characteristics such as Open medium, Dynamic topology, Distributed cooperation and constrained capability. [4]

Black hole attack malicious node acts like a black hole, dropping all data packets passing through it as like matter and energy disappears from our universe into a black hole. A black hole has two properties: Firs, the node exploits the Ad-hoc Routing Protocol. Second, the node consumes the intercepted packets. [1]

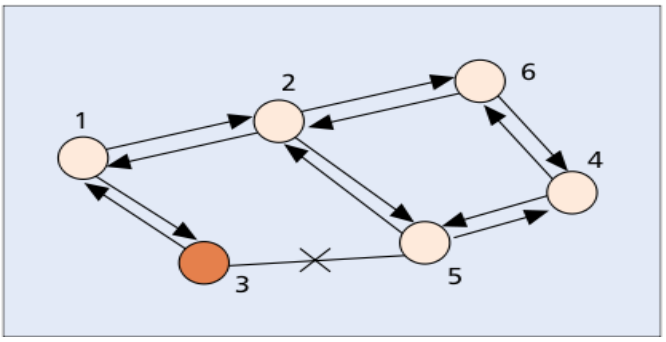

Fig 2.black hole detection

The Gray hole attack has its own characteristic's behavior. It too drops data packets. The gray hole attack is also called hidden attack. In gray hole attack, Its not drop all the data packets, It randomly accesses the data packet send by the source node. It has two types: Node dependent attack: Drops data packets destined towards a certain victim node. Time dependent attack: Drops data packets based on some predetermined trigger time. Malicious node can attract all data packets by using forged route reply (RREP) packets to falsely claim that "fake" shortest route to the destination and then discard data packets without forwarding to the destination. [6]

2. LITERATURE SURVEY

S. Ramaswamy et al (2003) proposed the "Prevention of cooperative black hole attacks in wireless ad-hoc networks," In this paper, characteristic of MANET has rendered it vulnerable to security attacks. In this system, it is dynamic topology to connect and leave the network at any point of time, Address of the problem in this paper is coordinated attack by multiple black holes. The solution of this problem by implementing AODV techniques to identify multiple black holes cooperating with each other and a solution to discover a safe route avoiding cooperative black hole attack. [1].

K. Liu, et al (2007) Proposed the method "An Acknowledgement based approach in the detection of routing misbehavior in MANETs," In this paper ,the selfish node (misbehavior node) is participating in the route discovery and maintenance

processes, But it forget to forward data packets. So solution of this paper is to propose the 2ACK scheme that serves as an add-on technique for routing schemes to detect routing misbehavior order to reduce additional routing overhead by using received data packets are acknowledged in the 2ACK scheme.

P.-C. Tsou, et al (2011) have proposed, "CBDS: A cooperative bait detection schemes to prevent malicious node for MANET based on hybrid defense architecture," Problem of this paper, AODV don't have the related mechanism about detection and response. The DSR mechanism is used to detect malicious nodes launching black/gray hole attacks and cooperative black hole attacks, known as Cooperative Bait Detection Scheme (CBDS).By using the address of the adjacent node as the bait destination address, The solution of this problem is to baits malicious nodes to reply to RREP and detects the malicious nodes by proposing reverse tracing program to prevents their attacks.

W. Wang, et al (2009) have proposed "Defending against collaborative packet drop attacks on MANETs,", In this paper, Detecting packet drop attack by using random audit based mechanism, But it cannot detect collaborative attacks. The solution for this attack by proposing hash function to generate node behavioral proofs that contain information from both data traffic and forwarding paths. The new method is robust against collaborative attacks. We investigate the security of the proposed approach and design schemes to further reduce the overhead.

S. Marti, et al (2000) proposed this paper "Mitigating routing misbehavior in mobile ad-hoc networks," In this paper, The network containing nodes that agree to forward packets, but fail to do. The dynamic measurement is used to monitor all the nodes in the network. The watchdog scheme that identifies misbehaving nodes and a path-rater that helps routing protocol to avoid these nodes. The result of the watchdog and path rather use the packet throughput, percentage of overhead transmissions, Is used to detect misbehavior node.

3. PROBLEM IDENTIFICATION

In MANET is a cooperative communication among nodes. It is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. Each device in MANET is free to move independently in any direction. In the presence of the malicious nodes, this requirement may cause security problems like a gray hole and black hole attacks. To resolve these attacks, we proposed Packet Estimation Algorithm, in this approach received packet information collected from destination, which reply to the source about intruders if it is not receiving predefined packets. Consider the threshold value is 1.000 is maintained in each neighboring node at the time of data packet transaction. This value is calculated per hop count. The value is reduced to 0.5482 at the two hop count that node is represented as malicious node. Then the source node searches the nearest shortest path in the network.

4. PROPOSED SYSTEM

In this system the packet estimation algorithm is used to prevent attacks in Manet, Packet estimation is done by calculating the packet send form source node to destination through the number of nodes between the source and destination.

The AODV (Ad Hoc On demand Distance Vector Routing) protocol is used for this communication. It does not maintain any record about this network communication and it is represented as reactive protocol, it means that it establishes a route to a destination only on demand.

Route discovery:

The AODV protocol is used for discovering the routes between the node , that is established only when it is required by a source node for transmitting a data packet. The destination sequence number is used to identify the shortest path to the destination node.

And the source and destination stores the hop count information according to the flow of packet transmission.

Route.

Route reply:

Route reply is used to identify the interested node for this communication that node is referred as destination node. In this type of communication sometimes the intermediate node act as a malicious node to access and drop all the data packet sent by the source node. That node is identified by using the fake route request. The source will generate a fake request with destination address as cooperating neighbor. Source already knows the information, for Freq no reply. But in case if there is a reply from any node, then that node will be identified as malicious by using the source routing mechanism.

Detection:

In detection mechanism, The DSR (dynamic source routing) it does not have any security for the packet delivery, So the CBDS method is used for fetching the malicious node between the source and destination, The CBDS for fetching the node act as a hacker (black and gray hole attack) in the network, the Only detection process is possible in these CBDS mechanisms. CBDS disconnects the path containing malicious node between the source and destination.

***Detection Algorithm*:**

Initialize the Hello timer
If Hello timer expires
Send hello message
If the node has data
If loop checking not yet over
Get the random neighbor from table
Send the req to the neighbor node
Else
Send the req to destination
If the packet received
If the packet is hello packet
If the sender is not malicious
If the node is unknown node
Add details in table
`Else
Update the expire time
Else
Ignore the packet
If the packet is Req packet
did basic packet filtering and updating operation
If the current node is destination && sender is a neighbor
Set packet as Freq
Ignore the packet
If the current node is a malicious node
Send reply
If the node is destination
Send reply
If the packet is a reply packet
If the current node is the destination of reply packet && source is the neighbor
Set packet final node is malicious
Ignore the packet
Else
Do normal filtering and updating operation

5. PREVENTION

Packet Estimation Algorithm is used for calculating the packet rate, the estimation fully depends upon the source. Reply (alarm) of proper destination is an essential thing to calculate the packet delivery rate. The fack reply message of a malicious node is identified by the threshold value calculation between each node from source to destination. The Packet Estimation Algorithm still successfully detects those malicious nodes while keeping the threshold value of a packet delivery ratio is 1.000.Each and every node is monitored by using this threshold value. The threshold value is calculated between every hop count. That value getting reduced more than one hop count at any node (0.6890 or 0.5670) that node is considered as malicious node.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 2, pp: (69-75), Month: April - June 2016, Available at: www.researchpublish.com

Diagram:

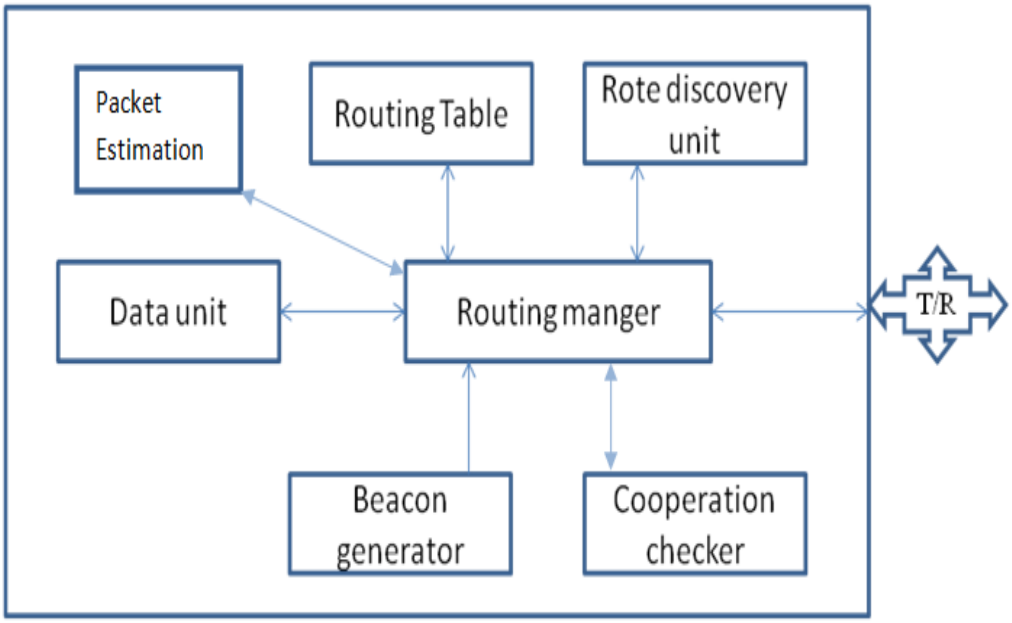

Fig 3. Architecture Diagram

ALGORITHM:

Packet Estimation Algorithm:

If the packet is the data type

Data transfer to the shortest path

Initialize for every nodes in a fine path

Check per every hop count ()

Calculated value updated to Rtable ( )

If Update node detail into the malicious list

Break link

Generate RREQ to find a new route without a hacker

Once again data transfer in another route

Else transfer regular data

6. PERFORMANCE METRIC

Packet Delivery Ratio:

The packet delivery ratio is used to calculate the number of data packets send from source node to the destination node and it's also used to monitor the time taken to send the data packet to the destination node. The below graph represent the packet delivery ratio between the existing and the proposed system (Packet Estimation Algorithm)

$$\mathbf{PDR} = \frac{\text{Number of Packet Receive}}{\text{Number of Packet Send}}$$

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 2, pp: (69-75), Month: April - June 2016, Available at: www.researchpublish.com

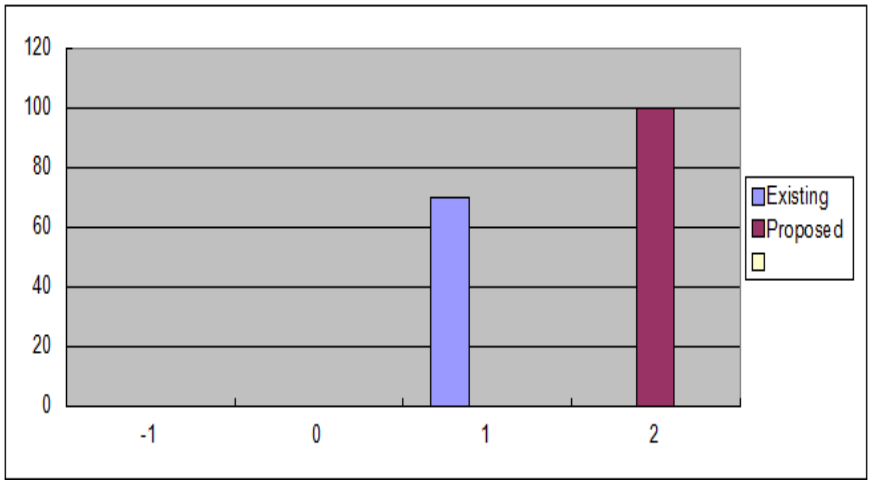

Fig 4.Packet Delivery Ratio

Routing Overhead:

In the Proposed system the overhead is minimized then the existing system. The overhead represents the extra information or unwanted information it increases the time of data transmission. It may also cases, some collision and data re transmission in the network.

Average End to end delay:

The average end to end delay used to represent the average time taken to transfer the information from source to destination node. The quality of an rout and time period is used to calculate the delay rate between each node.

Throughput:

It is used to refer the destination to get the final packet from the source node. It transfers the data packet per second to the neighboring node. It also monitors the data packet send from the source to the destination.

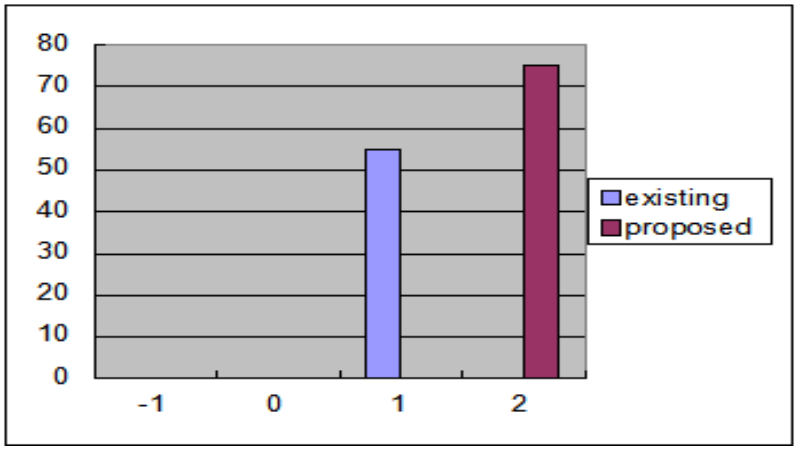

Fig 5. threshold

7. CONCLUSION

In this paper we have proposed a new mechanism (called Packet Estimation Algorithm) for preventing black and gray hole attacks(collaborative attacks) in MANET .The packet Estimation Algorithm is enhance the feature of an existing system(Cooperative bait detection scheme).The delay, throughput and overhead is minimized by using(PEA) this mechanism and The threshold value is used to monitor the data packet send from source to destination, Consider the threshold value is 1.000 is maintained in each neighboring node at the time of transaction. This value is calculated per hop count. The value is reduced to 0.5482 at two hop count that node is represented as malicious node. Then the source node search the nearest shortest path in the network.

REFERENCES

[1] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, "Prevention of cooperative blackhole attacks in wireless ad hoc networks," in Jun. 2003, pp. 570–575.

[2] K. Liu, D. Pramod, K. Varshney, and K. Balakrishnan, "An Acknowledgement based approach for the detection of routing misbehavior in MANETs," vol. 6, no. 5, pp. 536–550,May 2007.

[3] D. Johnson and D. Maltz, "Dynamic source routing in ad hoc wireless networks," . pp. 153–181, 1996.

[4] P.-C. Tsou, J.-M. Chang, H.-C. Chao, and J.-L. Chen, "CBDS: A cooperative bait detection scheme to prevent malicious node forMANET based on hybrid defense architecture," in *Proc. 2nd Intl. Conf. Wireless Commun., VITAE*, Chenai, India, Feb. 28–Mar., 03, 2011, pp. 1–5.

[5] W.Wang, B.Bhargava, and M.Linderman, "Defending against collaborative packet drop attacks on MANETs," in, New Delhi, India, Sep. 2009.

[6] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. 6th Annu. Intl. Conf. MobiCom*, 2000, pp. 255–265.

[7] W. Kozma and L. Lazos, "REAct: resource-efficient accountability for node misbehavior in ad hoc networks based on random audits," in, 2009, pp. 103–110.

[8] A. Baadache and A. Belmehdi, "Avoiding blackhole and cooperative blackhole attacks in wireless ad hoc networks," *Intl. J. Comput. Sci. Inf. Security*, vol. 7, no. 1, 2010.

[9] Y. Xue and K. Nahrstedt, "Providing fault-tolerant ad hoc routing service in adversarial environments," *Wireless Pers. Commun.*, vol. 29, pp. 367– 388, 2004.

[10] QualNet Simulaton Tool, Scalable Network Technologies. (Last retrieved March 18, 2013).

[11] H. Deng, W. Li, and D. Agrawal, "Routing security in wireless ad hoc network,", vol. 40, no. 10, Oct. 2002

[12] W.Wang, B.Bhargava, and M.Linderman, "Defending against collaborative packet drop attacks on MANETs," in, New Delhi, India, Sep. 2009.