International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) ISSN: 2395-5325
Volume 3, Special Issue 2 (March '2017)
Proceeding of - National Conference on Recent Trends in Information Technology and Communication,
Conference held at Velammal Engineering College,Chennai,India.

ENSURING SECURITY IN MANET USING PACKET DELIVERY BASED CBDS TECHNIQUE

A.Vijayan,
Assistant Professor,
Velammal Engineering College,
Chennai,India.

Prathiba Kalidass,
B.Tech Information Technology,
Velammal Engineering College,
Chennai,India.

Vani Masilamani,
B.Tech Information Technology,
Velammal Engineering College,
Chennai,India.

Sridevi Murugesan,
B.Tech Information Technology,
Velammal Engineering College,
Chennai,India.

Abstract: In MANET the primary requirement is co-operative communication among nodes. The malicious nodes may cause security problems like gray hole and collaborative attacks. To resolve these attack propose designing DSR mechanism, which is referred as cooperative bait detection scheme (CBDS) that integrate the advantage of both the proactive and the reactive defence architecture. In black hole and grey hole attacks, a node broadcasts a fake message informing that it has the shortest path to the destination, with the goal of intercepting messages. In this case, a black hole node can attract all the packets by using forged Route Reply (RREP) packet to falsely claim that "fake" shortest route to the destination and then drop these packets and not forwarding them to the destination. In gray hole attack, the malicious node is not initially recognized as such since it turns malicious only at a later time and preventing the trust-based security solution from detecting its presence within the network. It then selectively drops/forwards the data packets when packets go through it. In this we focus is on detecting gray hole and collaborative black hole attacks using the dynamic source routing (DSR)-based routing technique.

Keywords: Cooperative Bait Detection Scheme(CBDS), black hole attacks, wireless network, infrastructure network dynamic source routing protocol, malicious node, mobile ad hoc network(MANET).

I.INTRODUCTION

Communication is the process in which two or more people exchange their ideas, facts, information in ways that each gains a common understanding of the intent,meaning and use of messages. The term "communication" origins from the Latin word "communism" - meaning common. Thus, communication is to share the information, ideas, attitudes, and the like with others. In short, it is the process of getting a sender of the message and a receiver of the message synchronized together for a particular message, or a series of messages. For two or more people associated in a common, co-operative effort, they must be able to communicate with each other. In computerized technology, we need to transfer the data from one person to another without any problem like security and quality. To improve the communication in MANET ,we need to test our proposed method is working good or not by using system modeling. System modeling refers to representing an actual system in a simply way.

System modeling is very much important in system design and development, since it gives the concept of how the system would perform if it actually implemented.

What does security mean?

Ability for two nodes to communicate effectively even in the presence of active adversaries in the network

1. Ability to find routes
2. Availability of service
3. If an "honest" path exists

Network security consists of certain number of provisions and policies which is proposed by network administrator to protect and monitor unauthorized access, misuse, modification and user-accessible resources. Network security involves the mechanism of providing authorization of access to data in a network, which is controlled by network administrator. Users are provided with an ID and password or other authenticating information that allows users to access information within their authority.

Mobile Ad-hoc Networks: An adhoc network is a collection of wireless mobile hosts which forming a temporary network without the aid of any stand-alone infrastructure or centralized administration. Mobile Ad-hoc network is a self-organizing and self re-configuring multihop wireless networks where structure of the network changes dynamically. This is mainly due to the mobility of the nodes. Nodes in those networks utilize the same random access wireless channel, cooperating in some friendly manner to engage themselves in the multihop forwarding. The nodes in the network not only act as hosts but also as routers that route data to and from other nodes in network. In mobile ad-hoc networks where there is no infrastructure support as it is the case with wireless networks, and since the destination node in the network might be out of range of a source node transmitting packets; a routing procedure is always be

needed to find a path so as to forward the packets appropriately between source and the destination. Within the cell, a base station can reach all mobile nodes without the routing through broadcast in common wireless networks. In the case of ad-hoc networks, each and every node must be able to forward data for other nodes. This creates some additional problems along with the problems of dynamic topology that is unpredictable connectivity changes.

MANETS rely on wireless transmission, so a secured way of message transmission is important to protect the privacy of data. An insecure ad-hoc network at the edge of an existing communication might potentially cause the entire network to become vulnerable to security breaches. In MANET, there is no central administration to take care of detection and prevention of anomalies.There are two sources of threats to the routing protocols. The first comes from external attackers. By injecting erroneous routing information in the network, replaying old routing information, or distorting routing information, an attacker could successfully partition the network or introduce a traffic overload by causing retransmission and inefficient routing. The second but also more severe kinds of threat comes from compromised nodes, which might (i) misuse routing information to other nodes or (ii) act on applicative data in order to induce service failures.

Characteristics: Mobile Adhoc Network is a collection of independent mobile nodes,they can communicate to each other via radio waves. These networks are fully distributed, and can work at any place without help of any infrastructure. This property makes these networks highly exible and robust.Generally, the communication terminals have a mobility nature which makes the topology of the distributed networks time varying. The dynamic nature of network topology increases the challenges of the design of ad hoc networks. The energy consumption is one of the critical issue in the design of the ad hoc networks.The mobile devices usually have a limited storage and low computational capabilities. They heavily depend on the other hosts and resources for data access and information processing. A reliable network topology is one that should be assured through an efficient and secure routing protocols for Ad Hoc networks.

AODV (AdHoc Ondemand Distance Vector Routing): It is a reactive routing protocol, means that it establishes a route to a destination only on demand. In contrast, the most common routing protocols in the Internet are proactive, means that they find routing paths independently of the usage of the paths. AODV is, as the name indicates, a distance-vector routing protocol. AODV avoids the counting-to-infinity problem of other distance vector protocols by using their sequence numbers on route updates, a technique pioneered by DSDV. AODV is capable of both unicast and multicast routing.

Working: In AODV, the network is silent until a connection is needed. At that point the network node that needs a connection broadcasts a request for connection. Other AODV nodes forwards this message, and it record the node that they heard it from, creating an explosion of temporary routes back to the needy node. When a node receives such a message but already has a route to the desired node, it sends the message backwards through a temporary route to the requesting node. The needy node then begins using the route that has the least number of hops through other the nodes in the network. Unused entries in the routing tables are recycled after a time. When a link fails, the routing error is passed back to a transmitting node, and the process repeats. Most of the complexity of the protocol is to lower the number of messages to conserve the capacity of the network. For example, each request for a route has a sequence number. Nodes use their sequence number so that they do not repeat route requests that they have already passed.One of the feature is that if a route request fails, another route request might not be sent until twice as much as time has passed as the timeout of the previous route request. The advantage of AODV is, it creates no extra traffic for communication along existing links. Also, distance vector routing is simple, and don't require much memory or calculation. However AODV requires more time to establish the connection, and the initial communication to establish a route is heavier than some other approaches.

II.LITERATURE SURVEY

1) "**Detection/Removal of Cooperative Black Hole and Gray Hole Attack in Mobile Ad-Hoc Networks**", **Sukla Banerjee, July 22, 2008.**

A mobile ad hoc network is a collection of wireless nodes, they can be set up dynamically anytime and anywhere without using any pre-existing network infrastructure. Protecting the mobile ad-hoc network from malicious attacks is important and challenging issue. In this paper we discuss the problem of packet forwarding misbehavior and propose a mechanism to detect and remove the black and gray-hole attacks. Our approach consists of an algorithm which behaves as follows. Instead of sending the total data traffic at a time we should divide the total traffic into some small sized blocks. So that the malicious nodes can be detected and removed in between transmission of two such blocks by ensuring an end-to-end checking. Source node sends a prelude message to the destination node before the start of sending any block to alert it about incoming data block. Flow of the traffic is monitored by the neighbors of the each node in the route. After the end of the transmission the destination node sends an acknowledgement through a postlude message containing the no of data packets received by destination node. Source node uses this information to check whether the data loss during the transmission is within tolerable range, if not then the source node initiate the process of detecting and removing malicious node by aggregating the response from monitoring nodes and the network.

This Proactive detection schemes are the schemes that need to constantly detect or monitor nearby nodes. In these schemes, regardless of existence of malicious nodes, the

overhead of the detection is constantly created, and the resource used for detection is constantly wasted.

2) "An Acknowledgement based approach for the detection of misbehavioring of routing in MANETs," IEEE K. Liu, D. Pramod, K. Varshney, and K. Balakrishnan, May 2007.

In this proposed a 2ACK scheme for the detection of routing misbehavior in Mobile Adhoc Networks. In this scheme, two-hop acknowledgement packets are sent in opposite direction of the routing path to indicate that the data packets have been successfully received. The parameter acknowledgment ratio, i.e., Rack is also used to control the ratio of the received data packets for which acknowledgment is required. This type of scheme belongs to the class of proactive schemes and, hence, produces additional routing overhead regardless of the existence of malicious nodes.

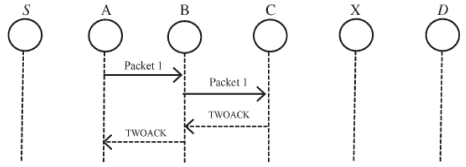


Fig. 1. TWOACK scheme: Each node is required to send back an acknowledgment packet to the node that is two hops away from it.

The TWOACK scheme successfully solves receiver collision and limited transmission power problems posed by the Watchdog. However, the acknowledgment process is required in every packet transmission process adds a significant amount of the unwanted network overhead. Due to the limited battery power nature of the MANETs, such redundant transmission process can easily degrade the life span of the entire network. However, many of the research studies are working in energy harvesting to deal with this problem

3) "Routing Security in Wireless Ad Hoc Networks", Hongmei Deng, 2002.

The primary advantage of a wireless network is the ability of the wireless node to communicate with the rest of the world while being mobile. In this article we study the routing security issues of MANETs, and analyze the detail one type of attack — the "black hole" problem — `that can easily be employed against the MANETs. We also propose a solution for black hole problem for ad hoc on-demand distance vector routing protocol. One of the possible solution to the black hole problem is to disable the ability to reply in the message of an intermediate node, so all the reply messages must be sent out only by the destination node. Using this method the intermediate node cannot reply, so in some sense we may avoid the black hole problem and implement a secured AODV protocol. But there are two associated demerits. First, the routing delay is greatly increased, especially for a large network. Second, the malicious node can take further action such as fabricate the reply message on behalf of the destination node. and another method is considered in this paper and in that method the source node will verify the each next node information by forming a new route, but in this method, the overhead will increase.

Existing System:

- In a MANET, each node not only works as a host but can also act as a router.
- While receiving data, nodes also need cooperation with each other to forward the data packets, thereby forming a wireless LAN.
- These great features also come with serious drawbacks from a security point of view.
- The presence and collaboration of malicious nodes in the network may disrupt the routing process, leading to the malfunctioning of the network operations.
- The lack of infrastructure leads to attacks like black hole and gray hole.

Disadvantages:

- Node transmits a malicious broadcast message informing that it has the shortest path to the destination.
- Malicious nodes discard these packets without forwarding them to the destination.
- Malicious node can attract all packets by using forged Route Reply.

Proposed System:

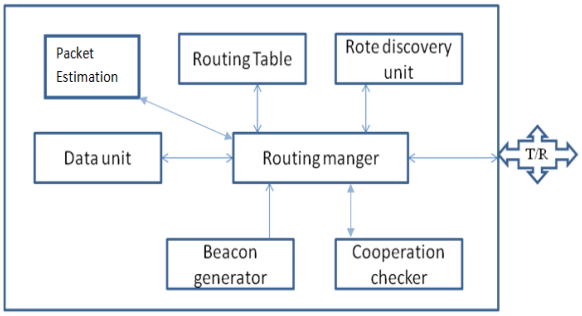
- DSR involves two main processes: route discovery and route maintenance.
- DSR does not have any detection mechanism, but the source node can get all the route information concerning the nodes on the route.

Advantages:

- Help in preventing or avoiding an attack in its initial stage.
- It can identify all the addresses of nodes in the selected routing path from the source to destination after the source has received the RREP message.

The reverse tracing program in the next step would be initiated in order to detect this route

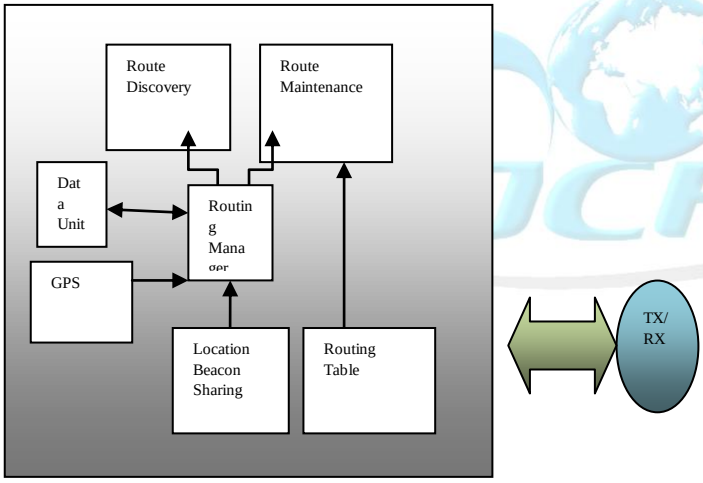
Diagram:



Network design:
In our project, we are mainly dealing with the security side, to check our protocol strength we have to design the attacker and defender nodes. The attacker node able to check the route request and can give the fake reply to source and attacker can identify the data packet and it will drop. Legitimated nodes can make the cooperation with neighbor and can make the communication, and forwards the data from one node to other nodes, and can try to defend from attacker.

Cooperative Checker:
In this module, we have used the timer to keep the time expire and intimates to generate periodic packet. The beacon generator can generate the packet and that packet can be read by any neighbor node, the beacon life is only for one hop. The work of neighbor management unit is to store the neighbor information into the table when it receives the beacon packet from the neighbor. If the time is got expire the neighbor node info will be deleted from the table

Block Diagram:



Route Discovery:

Normally the source node can find the route when the data is waiting in buffer without route by using the route request and route reply. In our project also we are going to use same method with different style, such as creating a fake route request. The source will generate fake request with destination address as cooperating neighbor. Source already knows the information,for Freq no reply. But incase if there is any reply from any of the nodes, then that node will be identified as malicious by using the source routing mechanism.Packet estimation of this process finding the RREQ source can transfer from data to destination. In periodic interval rate, every hop count we can determine how much transmits or receives the data or information.We have to monitor the estimated value, if any node values below threshold value. The node will be noticed by malicious node.The malicious node details it will be updated to all other neighbor nodes. Once again we can generate another RREQ without the malicious node, we can transfer the information.

Route Maintenance:
In this module, if route is failed means the intermediate node will share the error message. Based on the error messge,the source node will find another route to destination.

Algorithm:
1)Initialize the Hello timer
2)If Hello timer expires
a.Send hello message
3)if node has data
a.If coop checking not yet over
Get the random neighbour from table
2.Send the req to the neighbour node
b.Else
1.Send the req to destination
4)If packet received
a.If the packet is hello packet
1.If sender is not malicious
a.If node is unknown node
add details in table
b.Else
update the expire time
2.Else
Ignore the packet

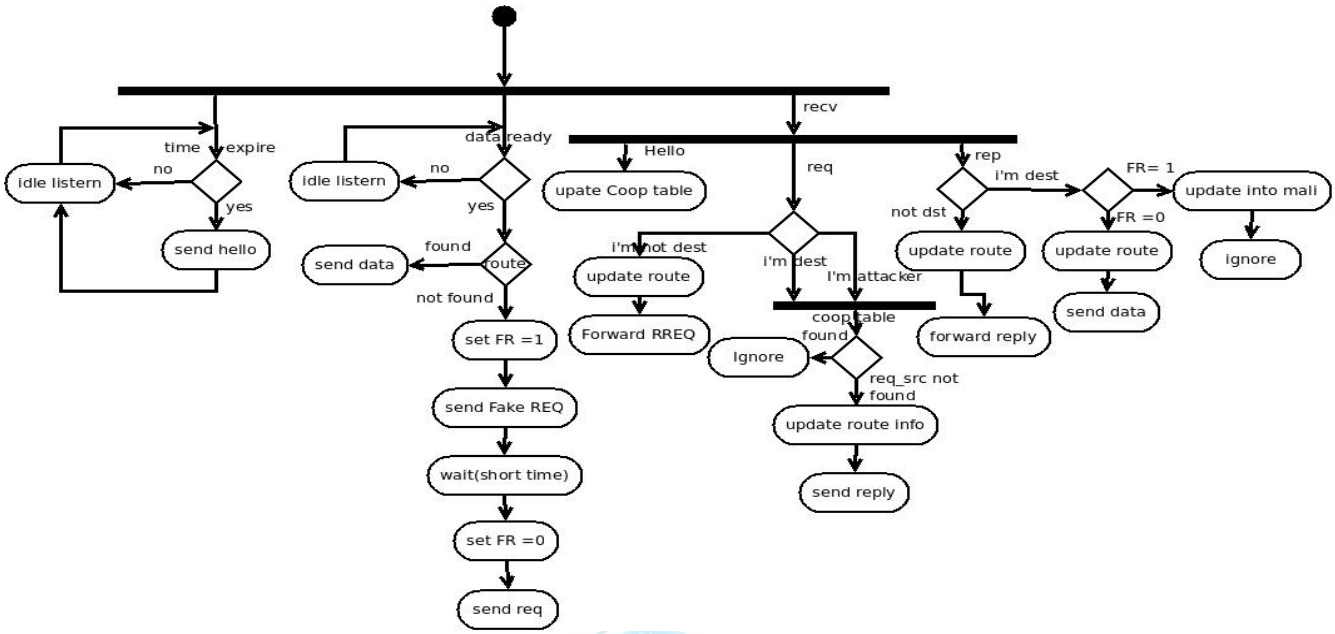
b.If packet is Req packet
1.Do basic packet filtering and updating operation
2.If current node is destination && sender is neighbor
a.Set packet as Freq
b.Ignore the packet
3.If current node is malicious node
Send reply
4.If node is destination
Send reply

c.If packet is reply packet
1.If current node is destination of reply packet && source is neighbor
a.Set packet final node is malicious
b.Ignore the packet
2.Else
Do normal filtering and updating operation

Enhanced Algorithm:
1.If packet is data type
a.Data transfer to the shortest path
b.Initialize Trust=1.000 for every nodes in a find path
c.Check per every hop count(Trust=Rx/(Tx*100))

d.Calculated value update to Rtable(Trust U Rtable)
1.If Trust < 0.75 && < 0.25
Update node detail into malicious list
Break link
Generate RREQ to find new route without hacker
Once again data transfer in another route
2.Else transfer regular data

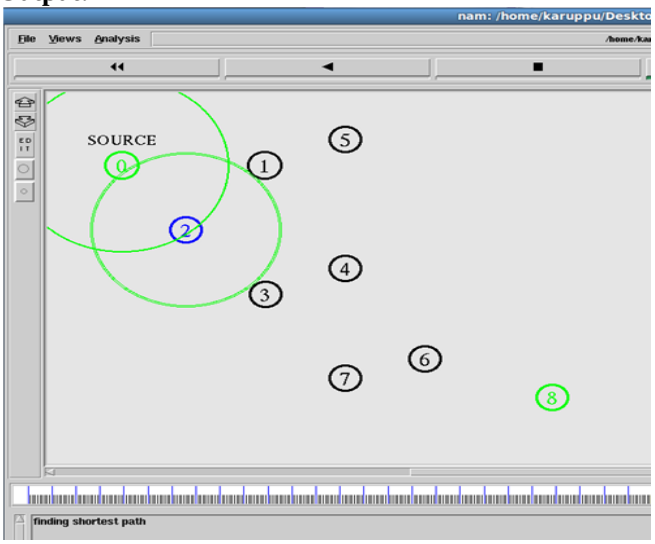
Flowchart CBDS:



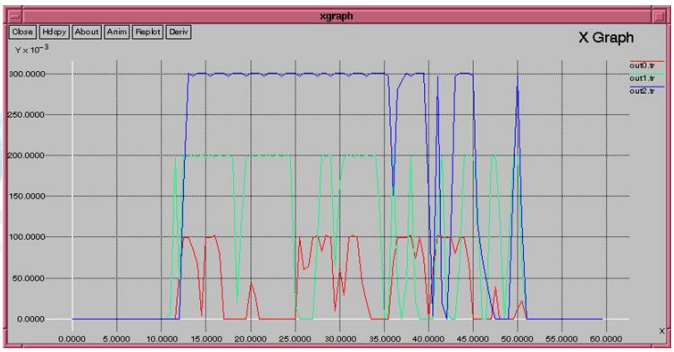
Reply Attack:

Initially in MANET, source node will send route request and respectively destination send Route Reply. After that the data will send by source to destination. Reply attack is warm attack it will attack the network in starting phase. It is difficult to identify the attacker node. When the source node generates the route request, the attacker node will try to receive the request and it will generate the fake route reply. Source always wait for the route reply from destination. Because in MANET, it should be prefer shortest path in every network. Once getting the route reply it will establish the route to that attacker node. While receive the data it will also generates the fake acknowledgement. We can detect the attacker node by cryptosystem or authentication schemes.

Output:



XGRAPH:



FUTURE WORK:

Therefore using the proposed system we can able to avoid boh black hole and replay attack in MANET and it also improves the data quality of the transferred packet by calculating the trust values of each and every node with the help of packet delivery based CBDS technique.

REFERENCES:

[1]. 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.

[2]. S. Corson and J. Macker, RFC 2501, Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, Jan. 1999. (Last retrieved March 18, 2013). [Online]. Available: http://www.elook.org/computing/rfc/rfc2501.html

[3]. C. Chang, Y.Wang, and H. Chao, "An efficientMesh-based core multicast routing protocol onMANETs," *J. Internet Technol.*, vol. 8, no. 2, pp. 229– 239, Apr. 2007.
[4]. D. Johnson and D. Maltz, "Dynamic source routing in ad hoc wireless networks," *Mobile Comput.*, pp. 153–181, 1996.
[5]. I. Rubin, A. Behzad, R. Zhang, H. Luo, and E. Caballero, "TBONE: A mobile-backbone protocol for ad hoc wireless networks," in *Proc. IEEE Aerosp. Conf.*, 2002, vol. 6, pp. 2727–2740.
[6]. 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.
[7]. S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks," in *Proc. 6th Annu. Intl. Conf. MobiCom*, 2000, pp. 255–265.
[8]. K. Vishnu and A. J Paul, "Detection and removal of cooperative
black/gray hole attack in mobile ad hoc networks," *Int. J. Comput. Appl.*, vol. 1, no. 22, pp. 28–32, 2010.
[9]. K. Liu, D. Pramod, K. Varshney, and K. Balakrishnan, "An Acknowledgement based approach for the detection of routing misbehavior in MANETs," *IEEE Trans. Mobile Comput.*, vol. 6, no. 5, pp. 536–550, May 2007.

